

Filing # 108740376 E-Filed 06/11/2020 02:52:52 PM

IN THE 15TH JUDICIAL CIRCUIT OF FLORIDA

AO ALFA-BANK

Plaintiff,

v.

JOHN DOE *et al.*

Defendants.

Civil Action No. _____

COMPLAINT FOR DAMAGES

1. This is an action arising under the Florida Civil Remedies for Criminal Practices Act (“Florida RICO”), Fla. Stat. Ann. § 772.101 *et seq.* Plaintiff AO Alfa-Bank (“Alfa Bank”) seeks damages for injuries caused by the unknown John Doe defendants’ pattern of criminal activity.

INTRODUCTION

2. Alfa Bank brings this action to seek redress from the unknown actors who perpetrated a sustained series of highly sophisticated cyberattacks against it in 2016 and 2017. This action is in no way related to U.S. or international politics, nor is it an attempt to support or harm, or to align Alfa Bank with, any candidate or political party. As a victim of deliberate, malicious, and damaging cyberactivity, Alfa Bank seeks simply to recoup its losses by identifying the unknown actors who carried out the cyberattacks, obtaining complete relief from those actors, and restoring its global reputation as the leading private bank in Russia.

3. The unknown John Doe defendants (“Defendants”) executed a highly sophisticated cyberattacking scheme to fabricate apparent communications between Alfa Bank, one of Russia’s largest privately owned commercial banks, and the Trump Organization, President Donald

Trump's namesake company, in the months leading up to and immediately following the 2016 U.S. Presidential election. Upon information and belief, Defendants' efforts were part of a broader disinformation campaign aimed at improperly linking Alfa Bank to President Trump's electoral campaign; sowing confusion and polarizing the U.S. public by pitting the predominant political parties against one another; and, ultimately, leading the U.S. public to question the legitimacy of the results of the 2016 election.

4. Upon information and belief, Defendants are members of a group who share a common purpose of using offensive cyber capabilities to develop and execute disinformation campaigns with the intent to disrupt the activities of governments, corporations, and individuals.

5. Upon information and belief, Defendants fraudulently manufactured and manipulated the Domain Name System ("DNS") resolution process, discussed below, to create the false appearance of a covert communication channel between Alfa Bank and the Trump Organization, in at least two separate and distinct ways.

6. First, from at least May 2016 through at least September 2016, Defendants sent "spoofed" emails purporting to come from the Trump Organization to Alfa Bank. Tricked into thinking that the emails were authentic, Alfa Bank's servers responded by sending DNS "lookups" to request information from the Trump Organization server. Observers interpreted the resulting exchange of network traffic between Alfa Bank servers and a Trump Organization server as evidence of secret communications between Alfa Bank employees and members of the Trump Organization. This scheme of cyberattacks involved a series of up to 100 or more separate but related attacks.

7. As part of this scheme, upon information and belief, computer scientists and researchers who have access to and monitor nonpublic DNS activity "discovered" the manipulated

and curated data showing the apparent exchange of DNS data between Alfa Bank and the Trump Organization. Upon information and belief, Defendants alerted these scientists and researchers to the DNS data, with the intent that the scientists and researchers publicize the data. And, indeed, this is precisely what happened. The scientists and researchers who obtained the nonpublic DNS data deliberately leaked portions of that data to other scientists and researchers and, ultimately, to the media. Critically, the DNS data showed Alfa Bank's communication relationships, including the number and frequency of emails between Alfa Bank and unique third parties, and the number and frequency of visits from Alfa Bank to unique websites owned by third parties. This data revealed highly sensitive and confidential information, including Alfa Bank's clients, business partners, suppliers, trade secrets, and unique software used for internal services. Defendants' actions thus proximately caused a data breach that exposed Alfa Bank's business information.

8. Second, upon information and belief, Defendants carried out an independent but related scheme of cyberattacks in February and March 2017 to further bolster the alleged evidence of covert connections between Alfa Bank and the Trump Organization. On February 18, 2017; March 11, 2017; and March 13, 2017, Defendants sent Alfa Bank over 20,000 DNS requests that appeared to combine a Trump Organization domain name with an Alfa Bank domain name purposefully to create the illusion of secret communications between the two entities. Upon information and belief, Defendants perpetrated these cyberattacks to bolster their disinformation campaign that sought falsely to tie Alfa Bank to President Trump's electoral efforts.

9. Beginning in October 2016 and persisting through the present day, media outlets have interpreted the manipulated and curated DNS log data as explosive evidence that Alfa Bank illegally interfered in the 2016 U.S. presidential election on behalf of then-candidate Trump and continued illicit communications with President Trump throughout the presidential transition and

the beginning of the new administration. Journalists have pointed to the alleged covert communication channel between Alfa Bank servers and the Trump Organization server as the mechanism through which then-candidate Trump's campaign and the Russian government coordinated their efforts to increase the likelihood that President Trump prevailed in the election.

10. Alfa Bank in fact engaged in no communications with the Trump Organization in 2016 or 2017 beyond the falsely generated and inauthentic DNS queries. Indeed, Alfa Bank has never had any business dealings with the Trump Organization. Three prominent U.S. cybersecurity firms have reviewed all available evidence and found nothing suggesting any intentional or covert communications directed by the Trump Organization and Alfa Bank. The Federal Bureau of Investigation ("FBI"), moreover, investigated supposed links between Alfa Bank and the Trump Organization and ultimately concluded that there were "no such links." Special Counsel Robert S. Mueller, III likewise testified that allegations of ties between Alfa Bank and the Trump Organization were "not true."

11. Nevertheless, despite these definitive findings, the narrative that Alfa Bank communicated with the Trump Organization to coordinate election-interference efforts—falsely created and shaped by Defendants—persists in media circles and the public consciousness. As a direct and reasonably foreseeable result of Defendants' unlawful conduct, Alfa Bank has suffered damage to its business and property. Among other things, Alfa Bank has been forced to hire legal counsel and expend considerable resources to defend itself against the baseless allegations stemming from Defendants' actions, and it has suffered a loss of income through disruption to existing and prospective business transactions caused by Defendants' actions. Alfa Bank seeks to recoup the monetary losses that it has suffered as a direct result of Defendants' unlawful scheme.

PARTIES

12. Plaintiff Alfa Bank is a major banking institution, registered and licensed in the Russian Federation. Its registered office is located at 27 Kalanchevskaya Street, Moscow, Russia 107078. Alfa Bank has a branch network consisting of approximately 750 offices across Russia, as well as a subsidiary bank in the Netherlands and financial subsidiaries in the United Kingdom and Cyprus.

13. Defendants John Doe *et al.* are the unknown persons or entities who are members of the association in fact (“Disinformation Enterprise”) that perpetrated cyberattacks against Alfa Bank in 2016 and 2017 designed to produce data purporting to show communications between Alfa Bank and the Trump Organization. Defendants themselves conducted or participated in the Disinformation Enterprise as outlined in this Complaint. Upon information and belief, the Disinformation Enterprise preexisted the events that form the basis of this action and remains in existence to this day. Upon information and belief, the objective of the Disinformation Enterprise is to spread disinformation and disrupt the activities of governments, corporations, and individuals.

14. Alfa Bank has conducted a reasonable search to determine the actual names of Defendants, but Defendants’ identities remain unknown to Alfa Bank. The John Doe designation is fictitious and serves as a placeholder until Alfa Bank is able to conduct discovery and uncover the actual names of Defendants.

JURISDICTION, VENUE, AND CHOICE OF LAW

15. This Court has subject-matter jurisdiction over this action because the claims arise under Florida law. *See Fla. Stat. Ann. §§ 772.101 et seq., 815.01 et seq.*

16. Upon information and belief, the Court has personal jurisdiction over Defendants pursuant to Fla. Stat. Ann. § 48.193.

17. Upon information and belief, venue is proper in this Court pursuant to Chapter 47, Florida Statutes, because some or all of the causes of action accrued in Palm Beach County, Florida.

18. Florida law applies to Alfa Bank's claims because Defendants' wrongful conduct is chargeable by indictment or information under Florida statutory provisions. *See Fla. Stat. Ann.* §§ 772.102(1)(a)(21), 910.005.

FACTS

I. Network Infrastructure

19. Internet Protocol ("IP") addresses are the bases for communications on the internet. IP addresses are numerical codes (such as 66.216.133.29) that are often assigned and correspond to word-based domain names (such as "trump-email.com"). The DNS serves as a global directory that converts, or "resolves" the domain names (which are more easily used by humans) into an IP address (which are used by machines). The DNS is necessary for facilitating communication on the internet, as it takes the domain name input by a human user and resolves it into the corresponding IP address that is needed to send the communication to the appropriate recipient.

20. When a domain on one server searches for a domain name on another server, there is a "lookup" or "ping" between the two servers indicating that communication was attempted. This lookup (which is referred to as a "DNS request" or "DNS query") does not mean that a substantive communication actually occurred—e.g., that an email was sent and received—but merely that one server was looking for a specific IP address on another server. Domains and domain names are hosted by DNS servers. The appropriate DNS server fields the lookup and tries to resolve the DNS request by locating the correct IP address.

21. Critically, data logs of these DNS requests can reveal highly sensitive and confidential information. A reviewer with knowledge of DNS data can take the raw data from DNS logs and extract meaningful, substantive information. With respect to a business like Alfa Bank, for instance, an elementary analysis of raw DNS data could reveal a company's website traffic, email traffic, business partners, suppliers, trade secrets, and other similarly sensitive information. A reviewer could use the data to identify a company's communication relationships, including the number and frequency of emails between a company and unique third parties, and the number and frequency of visits from the company to unique websites owned by third parties. DNS data also could reveal software used by a company for various internal services.

22. In each of the two schemes, Defendants improperly manipulated and fabricated DNS lookups between Alfa Bank servers (located in Russia) and a Trump Organization server (located in the United States).

23. Cendyn, LLC ("Cendyn") is a Boca Raton, Florida-based marketing company that administered the Trump Organization domain that allegedly communicated with Alfa Bank servers—i.e., "trump-email.com." In June 2007, the Trump Organization retained Cendyn as its "exclusive marketing agency." (Ex. 1, *Cendyn is Tapped for Interactive Marketing Services by the Trump Organization*, Cision PRWeb (June 21, 2007), <https://www.prweb.com/releases/2007/06/prweb535089.htm> (last visited June 11, 2020).) In this capacity, among other tasks, Cendyn distributed marketing emails. Prior to its announcement of a business relationship with the Trump Organization, Cendyn had registered the generic domain "contact-client[.]com" in its own name. (Ex. 2, Ankura Consulting Group, *Covert Channel Allegation: New Data Analysis Results* (Apr. 2020) at 4 (hereinafter "Ankura Report"); Ex. 3, Mandiant, *Alfa-Bank Investigation Report* (Nov. 4, 2016) at 9 (hereinafter "Mandiant Report").)

In August 2009, Cendyn registered the domain “trump-email.com” in the Trump Organization’s name but listed itself as the administrator. (Ex. 3, Mandiant Report at 6–8.) Two months later, Cendyn coordinated the hosting of two related domains (“trump1.client-contact.com,” which was a subdomain of “contact-client.com,” and “mail1.trump-email.com,” which was a subdomain of “trump-email.com”) on a server with the IP address 66.216.133.29. (Ex. 2, Ankura Report at 5.) GoDaddy, Inc. (“GoDaddy”) hosted both parent domains and their corresponding subdomains.

24. GoDaddy used three DNS servers (“ns1.cdservices.com,” “ns2.cdservices.com,” and “ns3.cdservices.com”) to process DNS requests. (Ex. 3, Mandiant Report at 3.) Notably, all three DNS servers are located in Boca Raton, Florida, in Palm Beach County. Each time any computer on the internet (including those connected to Alfa Bank’s servers) sent a DNS request to try to resolve the IP address for those Trump Organization domains, the actual network traffic was directed by GoDaddy to one of the three DNS servers in Palm Beach County, Florida.

25. Cendyn contracted certain marketing functions to Listrak, a Pennsylvania-based company that provides digital marketing platforms and that distributed marketing emails on behalf of Trump Hotels. Listrak owned the server with the IP address 66.216.133.29, which housed the Trump Organization domains registered and administered by Cendyn. That server is located in Lititz, Pennsylvania. Reports indicate that the Listrak server continued to “reverse resolve[] the IP address 66.216.133.29 as ‘mail1.trump-email.com’” through and following the last known cyberattack committed by Defendants against Alfa Bank. (Ex. 4, Robert Graham, *Pranksters gonna prank*, Errata Security at 2 (Mar. 19, 2017), <https://blog.erratasec.com/2017/03/pranksters-gonna-prank.html#.XpjCWKhKiUn> (last visited June 11, 2020).)

26. Although the Trump Organization retained Serenata CRM (a German firm now doing business as NextGuest Technologies) to perform its marketing services in March 2016, the

business relationship between Cendyn and the Trump Organization continued for another year. Specifically, on June 29, 2016, Cendyn extended the registration for the “trump-email.com” domain for one year and remained the administrator of that domain until March 8, 2017, when it transferred the domain to the Trump Organization. (Ex. 2, Ankura Report at 10.) At least one team of researchers, moreover, identified “thousands of e-mails between Trump and Cendyn through the entire period that Alfa Bank was looking up the Trump server,” such that the business relationship persisted throughout the duration of Defendants’ cyberattacks. (Ex. 5, Dexter Filkins, *Was There a Connection Between a Russian Bank and the Trump Campaign?*, THE NEW YORKER, Oct. 8, 2018, <https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign> (hereinafter “Oct. 8, 2018 *New Yorker* article”).)

27. Notably, one of the cybersecurity expert firms that reviewed the evidence related to the cyberattacks concluded that the manner in which Cendyn configured the Trump Organization domains made them vulnerable to manipulation. Specifically, the expert concluded that the domains “trump-email.com” and “contact-client.com” were set up in such a way that “a threat actor could send spoofed emails or inauthentic DNS queries masquerading as these domains” to other domains, such as those hosted on Alfa Bank servers. (Ex. 2, Ankura Report at 4.) “As a result, this inauthentic activity could force Alfa-Bank servers to repeatedly query DNS records for both of these domains even if Alfa-Bank never received a legitimate marketing email” or other communication. (*Id.*) As explained further below, Defendants exploited this vulnerability to fabricate “evidence” of a purported secret communication channel between Alfa Bank and the Trump Organization.

II. Defendants' Cyberattacks Against Alfa Bank

28. Defendants orchestrated a coordinated series of cyberattacks against Alfa Bank that took place over the course of at least ten months, and potentially longer. Upon information and belief, Defendants perpetrated these cyberattacks as part of a disinformation campaign aimed at falsely linking Alfa Bank to President Trump's electoral campaign, thereby pitting the predominant political parties against one another, leading the U.S. public to question the legitimacy of the results of the election, and undermining trust in the U.S. democratic system.

29. Upon information and belief, the Disinformation Enterprise is a highly skilled group with robust cyber offensive capabilities, as highlighted by the sophisticated nature of the attacks and the manipulation of the specialized DNS infrastructure. Indeed, only a subset of malicious cyber actors would have been capable of funding, organizing, and carrying out the attacks on Alfa Bank. Executing the cyberattacks against Alfa Bank would have required understanding precisely how the Alfa Bank servers were constructed and demanded a concerted effort over a significant amount of time. Upon information and belief, Defendants are part of a well-trained and well-funded group that existed before the cyberattacks committed against Alfa Bank, continues to exist today, and carries out cyberattacks against a range of targets. It is likely that Defendants and the Disinformation Enterprise will continue their efforts to spread disinformation and undermine U.S. institutions, including through cyber campaigns aimed at disrupting the upcoming 2020 U.S. Presidential election.

30. Upon information and belief, Defendants exploited the DNS request process to manufacture the purported connection between Alfa Bank and the Trump Organization for multiple reasons. Because DNS data is a reliable indicator of communications between two sources, upon information and belief, Defendants knew that third parties would interpret the

fraudulent DNS data as highly compelling evidence that Alfa Bank in fact communicated with the Trump Organization, thereby posing particularly acute risks to Alfa Bank's business and reputation. Upon information and belief, moreover, Defendants sought to take advantage of the inherent complexities and difficulties of collecting and interpreting historic DNS data. To take just one example, different sources of DNS records often contradict each other in material ways such that focusing on a "single point of collections or DNS historical data" can lead to overlooking "clarifying context." (Ex. 2, Ankura Report at 7.) Thus, upon information and belief, Defendants expected that no observers would be able to detect their manipulations, which produced the DNS activity falsely evidencing communications between Alfa Bank and the Trump Organization, until well after the 2016 U.S. Presidential election, if ever. In the meantime, Defendants anticipated that at least some individuals who reviewed the data would promote Defendants' concocted narrative of illicit communications because they would be expected to "miss[], ignore[]," or lack "access to a complete record of DNS history." (*See id.* at 19.)

A. The 2016 Cyberattack Scheme

31. As Ankura Consulting Group ("Ankura"), one of the cybersecurity experts who studied the evidence, concluded, a "likely scenario" is that Defendants "artificially created DNS activity to make it appear as though a connection" between Alfa Bank servers and a Trump Organization server "existed, for 'discovery' later." (Ex. 2, Ankura Report at 3.) Indeed, from at least May 4, 2016 until September 21, 2016, Defendants improperly connected to server networks and manipulated data on a regular basis to fool Alfa Bank's servers into looking up a domain registered to the Trump Organization—when, in the absence of this activity, Alfa Bank's servers would not have done so. Through this scheme, Defendants caused traffic on U.S.-based computer

servers and networks and created the illusion of two-way communication between Alfa Bank and the Trump Organization.

32. Applying their sophistication and deep knowledge of arcane DNS infrastructure, Defendants exploited a vulnerability in the configuration of the Trump Organization servers operated by Cendyn and Listrak. In the normal course, an “SPF TXT record” accompanies an email when that email is sent. An SPF TXT record is used to confirm that emails actually have been sent by the identified sender, and not by someone falsely claiming to be the sender. An SPF TXT record performs this authentication by “specifying which hostnames, IP addresses, and/or IP ranges are permitted to send emails on behalf of a domain.” (Ex. 2, Ankura Report at 13.) In the case of the Trump Organization domains, the SPF TXT records contained a list of IP ranges that it deemed legitimate, all of which are associated with hotel and hospitality companies. (*Id.* at 13–16.) Critically, however, these SPF TXT records ended with an “~all flag,” which directed the recipient of an email from the “trump-email.com” domain that originated from an IP address *not* included in the verified SPF TXT record to “identify [the email] as spam but allow it at” the recipient’s direction. (*Id.* at 13, 15.) In other words, recipients did not necessarily reject emails that claimed to be from one of the Trump-related domains but originated from IP addresses not associated with those domains. This “~all flag” gateway thus allowed emails from non-Trump-related domains to appear as though they were from Trump-related IP addresses when they actually were not. Accordingly, the configuration “could . . . [have] allow[ed] an attacker”—such as Defendants—“to bypass spam identification and deliver mail into an organization” as though the mail originated from the Trump Organization. (*Id.* at 13.)

33. And Defendants in fact exploited this vulnerability to manufacture purported communications between Alfa Bank and the Trump Organization, “essentially tricking” Alfa Bank

servers “to perform a DNS query for a domain [they] never visited or received a legitimate email from.” (Ex. 2, Ankura Report at 18.) Ankura concluded that the DNS traffic patterns that formed the basis for alleging that Alfa Bank servers had been communicating with a Trump Organization server could have been caused by Defendants’ sending “spoofed emails masquerading as trump1.contact-client[.]com to Alfa-Bank,” in which case “these spoofed emails would force Alfa Bank’s email servers to request SPF records from contact-client[.]com.” (*Id.*) When Alfa Bank’s servers requested these records, the network traffic was routed to the appropriate DNS servers in Boca Raton, Florida. These original spoofed emails sent by Defendants to Alfa Bank, when combined with DNS requests sent by Alfa Bank servers to a Trump Organization server, created the false illusion of secret communications between Alfa Bank and the Trump Organization.

34. Defendants’ first cyberattack scheme took place over the span of nearly five months in 2016, from at least May through September. As experts have concluded, the varied timing and volume of DNS lookups suggest that they were the product of human action, not automation. (*See, e.g.,* Ex. 6, Franklin Foer, *Was a Trump Server Communicating with Russia*, SLATE, Oct. 31, 2016, at 8, http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html (hereinafter “Oct. 31, 2016 *Slate* article”).) Defendants would have needed to sustain this scheme with near-daily manual lookups to create this pattern of activity. In other words, the 2016 scheme of cyberattacks in fact comprised a series of up to 100 or more separate but related attacks.

35. Upon information and belief, Defendants intended that computer scientists and researchers “discover” the DNS data purportedly showing communications between Alfa Bank and the Trump Organization, monitor the traffic themselves, and then publicize that data to create a narrative that Alfa Bank was illegally coordinating with President Trump’s campaign and

interfering in the 2016 election. Some computer scientists and researchers have access to nonpublic DNS data for purposes of cybersecurity research and monitoring. Upon information and belief, Defendants alerted one or more of these scientists or researchers to DNS data showing the manufactured exchange of network traffic between Alfa Bank servers and Trump Organization servers, with the expectation that these scientists or researchers would publicly disclose this data and its purported significance as alleged evidence of a covert communication channel between Alfa Bank and the Trump Organization.

36. Through this scheme, Defendants caused a breach of Alfa Bank's confidential business information. Upon information and belief, Defendants caused third parties to obtain, analyze, distribute, and publicize Alfa Bank's DNS data. Alfa Bank's DNS data, in turn, contained confidential business information, including information related to Alfa Bank's business partners, suppliers, trade secrets, and unique software used for internal services. The DNS data, more broadly, revealed Alfa Bank's communication relationships, including the number and frequency of emails between Alfa Bank and unique third parties, and the number and frequency of visits from Alfa Bank to unique websites owned by third parties.

B. The 2017 Cyberattack Scheme

37. Defendants carried out a separate campaign of cyberattacks against Alfa Bank over three days in 2017. As with the 2016 cyberattacks, this scheme also was designed to create the false impression of illicit communications between Alfa Bank and the Trump Organization. Upon information and belief, these attacks were intended to bolster Defendants' disinformation efforts by linking Alfa Bank with President Trump's campaign, pitting the predominant political parties against one another, delegitimizing the results of the 2016 presidential election, and undermining faith in U.S. democracy. In separate attacks on February 18, 2017; March 11, 2017; and March

13, 2017, Defendants manufactured and sent over 20,000 DNS requests for invalid domain names to Alfa Bank. (Ex. 7, Stroz Friedberg LLC, *Summary of Cyber Incident Investigation* (Jul. 19, 2017) at 1 (hereinafter “Stroz Friedberg Report”); Ex. 8, *Press Statement: Alfa Bank confirms it has sought help from U.S. authorities, and discloses new cyberattacks linked to Trump hoax* (Mar. 17, 2017), at 3, <https://alfabank.com/news/press-statement-alfa-bank-confirms-it-has-sought-help-from-u-s-authorities-and-discloses-new-cyberattacks-linked-to-trump-hoax/> (last visited June 11, 2020) (hereinafter “Mar. 17, 2017 Alfa Bank Press Release”).) Those invalid domain names appeared to combine a purported Trump Organization domain name with a purported Alfa Bank domain name. (Ex. 7, Stroz Friedberg Report at 1.) When Alfa Bank’s servers sent DNS requests in response to these queries, the network traffic was routed to the appropriate DNS servers in Boca Raton, Florida

38. On February 18, 2017, Defendants sent Alfa Bank at least sixteen suspicious DNS queries. Specifically, Defendants queried the domain name “mail.trump-email.com.MOSCOW.Alfaintra.net” from external IP addresses. (Ex. 7, Stroz Friedberg Report at 1.) This invalid domain name combines two valid domain names associated with the Trump Organization and Alfa Bank: “mail.trump-email.com” and “moscow.alfaintra.net.” Defendants intended that these DNS queries create the impression of an exchange of communications between Alfa Bank and the Trump Organization. Notably, these lookups were virtually identical to unverified DNS data that L. Jean Camp, a computer science professor at Indiana University, posted on her website in early November 2016. (Ex. 9, L. Jean Camp, “Intra Net DNS Leakage,” <http://ljean.com/NetworkRecords/intranet/index.html> (last visited June 11, 2020).)

39. On March 11 and March 13, 2017, Defendants sent 20,000 more of these DNS requests for the same domain name. (Ex. 7, Stroz Friedberg Report at 1; Ex. 8, Mar. 17, 2017 Alfa

Bank Press Release at 3.) Significantly, this exponential uptick in attacks began the day after CNN published an article stating that the FBI continued to investigate an “‘odd’ computer link between [a] Russian bank and [the] Trump Organization.” (See Ex. 10, Pamela Brown & Jose Pagliery, *Sources: FBI investigation continues into ‘odd’ computer link between Russian bank and Trump Organization*, CNN (Mar. 10, 2017), <https://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/index.html> (last visited June 11, 2020).)

40. An expert retained by Alfa Bank to review evidence related to the 2017 cyberattacks, Stroz Friedberg LLC (“Stroz Friedberg”), concluded that the data was consistent with DNS traffic produced by cyberattackers. (Ex. 7, Stroz Friedberg Report at 3.)

III. “Discovery” of Defendants’ Manufactured Data

41. As Defendants intended, computer scientists “discovered” Defendants’ fabricated DNS data in the summer of 2016.

42. After the publication of news reports in June 2016 that Russian hackers had infiltrated the Democratic National Committee’s (“DNC”) computer network and looted the DNC’s opposition research on then-candidate Trump, a “tightly knit community of computer scientists” worked together to uncover evidence of other network intrusions related to the upcoming U.S. Presidential election. (Ex. 6, Oct. 31, 2016 *Slate* article at 2; Ex. 5, Oct. 8, 2018 *New Yorker* article at 2.) This group, which has been described as a “Union of Concerned Nerds” or an “elite group of malware hunters,” includes both academics and professionals, some of whom reportedly worked at cybersecurity firms with close ties to federal agencies and accordingly had unparalleled access to “nearly comprehensive logs of communications between servers.” (Ex. 6, Oct. 31, 2016 *Slate* article at 2–3.)

43. In late July 2016, one member of this group, who has identified himself using the pseudonym “Tea Leaves,” uncovered what he initially thought was malware emanating from Russia destined for a domain with “Trump” in the domain name. Thereafter, to augment this data, Tea Leaves “began carefully keeping logs of the Trump server’s DNS activity” and periodically circulated the data to the other group members. (Ex. 6, Oct. 31, 2016 *Slate* article at 3.) At least six of these computer scientists, including Tea Leaves and another member who uses the pseudonym “Max,” started to comb through the data looking for abnormalities. (*Id.*; Ex. 5, Oct. 8, 2018 *New Yorker* article at 4.) The identities of these researchers, including Tea Leaves and Max, remain a mystery.

44. The researchers ultimately collected what they claimed were portions of Alfa Bank’s historical DNS records spanning approximately five months, presumably using commercial databases available to them because of the nature of their employment and expertise. The researchers subsequently distributed, first among their group and later to the press, Alfa Bank’s DNS logs, which allegedly showed two servers belonging to Alfa Bank pinging a hostname, “mail1.trump-email.com,” that was registered to the Trump Organization and associated with the IP address 66.216.133.29. The nonpublic DNS data, which includes approximately 2800 DNS logs dated from May 4, 2016 to September 23, 2016, was circulated in a text file, the source of which was never verified. (Ex. 6, Oct. 31, 2016 *Slate* article at 8.)

45. The researchers asserted that “[t]he irregular pattern of server lookups actually resembled the pattern of human conversation—conversations that began during office hours in New York and continued during office hours in Moscow.” (*Id.* at 4.) They theorized that the pattern of activity “wasn’t an attack, but a sustained relationship between a server registered to the Trump Organization and two servers registered to an entity called Alfa Bank.” (*Id.*)

46. The researchers sought to bolster their theory that the DNS data evidenced a covert communication channel between Alfa Bank and the Trump Organization. First, they plotted the DNS logs against a timeline of campaign events and concluded that there were upticks in the number of pings during significant campaign events, such as the party conventions. (Ex. 6, Oct. 31, 2016 *Slate* article at 10.) Second, the researchers claimed that the Trump server was disabled after two journalists from *The New York Times* met with Alfa Bank representatives on September 21, 2016 to discuss the server allegations. (*Id.* at 11.) According to the researchers, the Trump Organization shut down the server after Alfa Bank informed it that journalists had discovered the connection between the servers. (*Id.*) Third, the researchers determined that on September 27, 2016, the Trump Organization had established a new host name, trump1.client-contact.com, that used the same IP address as the mail1.trump-email.com host name, and that an Alfa Bank server was the first to look up the new host name—an act that one journalist reported is “never random.” (*Id.*)

47. Upon information and belief, Defendants flagged the fabricated DNS data for one or more of the researchers. It is unlikely that the researchers could have identified the data without knowing to look for it, given the sheer volume of DNS data. (*See, e.g.*, Ex. 6, Oct. 31, 2016 *Slate* article at 3 (describing discovery of the data as “pure happenstance—a surprising needle in a large haystack of DNS lookups”.) Indeed, Max, one of Tea Leaves’ colleagues, provided a forensic team with the 37 million DNS logs that the researchers had at their disposal. (Ex. 5, Oct. 8, 2018 *New Yorker* article at 8.) Particularly given that only 2800 of the 37 million logs showed the alleged communications between Alfa Bank servers and Trump Organization servers, it is likely that Defendants pointed Tea Leaves or other researchers in the direction of the planted evidence.

IV. Publication of Defendants' Manufactured Data

48. Just as Defendants had intended, the researchers who “discovered” the fabricated data allegedly showing communications between Alfa Bank and the Trump Organization promptly moved to disclose that data to other researchers and journalists.

49. Notably, the DNS log data that the researchers reviewed is not public information. Rather, some companies, after de-duplicating the raw data and removing critical details, amass the processed DNS logs in databases that they offer commercially on a subscription basis. Other specialized entities collect and review the raw DNS data to ensure that the DNS process works effectively. Researchers and cybersecurity professionals use this nonpublic data to look for evidence of misconfigurations, outages, manipulation, malicious activity, and surveillance. As Ankura explained with specific reference to Alfa Bank, “only entities with specialized and non-public access to DNS infrastructure would know that Alfa-Bank . . . [was] sending repeated DNS queries to Trump associated domains.” (Ex. 2, Ankura Report at 11.)

50. Despite the nonpublic nature of DNS data, the researchers disclosed excerpts of their underlying data to news media outlets, including *The New York Times*, *Washington Post*, *Reuters*, *Daily Beast*, *Vice*, *The Intercept*, and *Slate*. (Ex. 11, Sam Biddle, Lee Fang *et al.*, *Here's the Problem with the Story Connecting Russia to Donald Trump's Email Server*, THE INTERCEPT, (Nov. 1, 2016) at 1–3, <https://theintercept.com/2016/11/01/heres-the-problem-with-the-story-connecting-russia-to-donald-trumps-email-server/> (last visited June 11, 2020) (hereinafter “Nov. 1, 2016 *The Intercept* article”); Ex. 6, Oct. 31, 2016 *Slate* article at 4.) Specifically, the researchers provided each media outlet with three documents: (i) an “academia-style white paper” about the so-called Trump server; (ii) an analysis of the white paper; and (iii) a “sprawling dossier on Alfa Bank,” described as having been “compiled with the exhaustive detail of a political oppo[sition]

team, not a university researcher.” (Ex. 11, Nov. 1, 2016 *The Intercept* article at 4.) Tea Leaves himself reportedly posted data on the dark web, *id.* at 6, and an unnamed researcher using the handle “LeavesTeaLeaves” posted the data in a Reddit thread. (Ex. 6, Oct. 31, 2016 *Slate* article at 11.) Then, on October 5, “leavestea” created a post on a WordPress blog that indicated that then-candidate Trump and Russia’s largest bank communicated via a “hidden server.” (Ex. 12, *Trump’s Russian Bank Account*, WordPress (Oct. 5, 2016), <https://gdd53.wordpress.com/2016/10/05/first-blog-post/>.) *Slate* published Franklin Foer’s explosive, yet false story of secret server communication on October 31, 2016—eight days before the Presidential election. Scores of additional news outlets subsequently reported that same story, making Alfa Bank a household name across the U.S. population, synonymous with Russian election interference.

51. Foer’s article relied on interviews with Tea Leaves and two unnamed accomplices, as well as the opinions of well-known experts in the cybersecurity field who had received and examined the logs. Among these experts was L. Jean Camp, a computer science professor at Indiana University. Camp had access to the researchers’ DNS log data and reportedly knows the identity of Tea Leaves and the author of the so-called Alfa Bank dossier. (Ex. 6, Oct. 31, 2016 *Slate* article at 4; Ex. 11, Nov. 1, 2016 *The Intercept* article at 3.) Since the publication of the *Slate* story, Camp has spoken out in support of the threat actors’ theory of secret server communication and the authenticity of the source data. (See, e.g., Ex. 13, Franklin Foer, *Trump’s Server, Revisited*, SLATE (Nov. 2, 2016), at 5, <https://slate.com/news-and-politics/2016/11/the-trump-server-evaluating-new-evidence-and-countertheories.html> (last visited June 11, 2020).) On November 2, 2016, shortly after the publication of Foer’s article and in the wake of ensuing criticism, Camp posted the DNS logs that she had in her possession to her personal website. (Ex. 14, *Some Network*

Data, Transparent Network Data, <http://ljean.com/NetworkData.php> (last visited June 11, 2020).)

In addition to Camp, Foer relied on the opinions of cybersecurity experts Paul Vixie (who also received the nonpublic DNS logs directly from the researchers), Richard Clayton, Christopher Davis, and Nicholas Weaver. (Ex. 6, Oct. 31, 2016 *Slate* article at 5, 7–8.)

52. News articles relying on the fabricated DNS data to link Alfa Bank to illegal efforts to interfere in the 2016 U.S. Presidential election continued unchecked for years—and, indeed, persist to this day. To take one particularly notable example, Dexter Filkins published a lengthy exposé on the server allegations in *The New Yorker* in October 2018. (Ex. 5, Oct. 8, 2018 *New Yorker* article at 3.) Similar stories continue to surface with the effect of dredging up the false and discredited narrative that Alfa Bank maintained a secret communication channel with the Trump Organization in 2016 and 2017.

V. Initiation of Investigations Into Alfa Bank

53. After receiving purported leads from several sources, the FBI began investigating allegations of a secret communication channel between Alfa Bank and the Trump Organization in August and September 2016. In particular, at least three primary sources provided the FBI with information underpinning its investigation.

54. First, Max’s attorney contacted the FBI in September 2016 to alert officials to a potential upcoming story in *The New York Times* about the server allegations. (Ex. 5, Oct. 8, 2018 *New Yorker* article at 3.)

55. Second, also in September 2016, Michael Sussmann, an attorney representing the DNC and Hillary Clinton’s campaign, gave FBI General Counsel James Baker information about a purported “surreptitious channel of communications” between a part of then-candidate Trump’s business and a Russian organization allegedly associated with the Russian government. (Ex. 15,

House Comm. on Judiciary & Comm. on Gov't Reform & Oversight, U.S. H.R., Interview of James A. Baker, 105 Cong., at 119–23 (Oct. 18, 2018).) Sussmann similarly delivered a briefing and supporting documents to an intelligence agency. (Ex. 16, Permanent Select Comm. on Intelligence, U.S. H.R., Interview of Michael Sussmann, at 28–30, 52–54, 60–61 (Dec. 18, 2017).) Sussman obtained this information in the summer of 2016 from an unidentified client. (*Id.* at 53–56, 60–61.)

56. Third, Glenn Simpson, co-founder of Fusion GPS (“Fusion”), a commercial research and strategic intelligence firm in Washington, DC, provided information that ultimately was shared with the FBI. The DNC had engaged Fusion to conduct opposition research on then-candidate Trump. Fusion, in turn, retained Christopher Steele and Steele’s company, Orbis Business Intelligence Ltd., who shared information with Simpson that related to purported communications between Alfa Bank servers and the Trump Organization server. Steele discussed the server allegations with Bruce Ohr, a senior official at the U.S. Department of Justice (“DOJ”), on September 23, 2016. (Ex. 17, Office of Inspector Gen., U.S. Dep’t of Justice, *Review of Four FISA Applications and Other Aspects of the FBI’s Crossfire Hurricane Investigation*, Oversight and Review Division Report 20-012 (Dec. 2019), at 274–75 (hereinafter “OIG Report”).) Simpson later indicated that “people” had given his group “information” that he described as “a bunch of data” “beyond [his] competence.” (Ex. 18, Sen., Judiciary Comm., U.S. S. Interview of Glenn Simpson at 304:21–305:13 (Oct. 18, 2018).)

57. On September 19, 2016, Steele provided election reporting to the FBI. (Ex. 17, OIG Report at vi (finding that Steele’s reporting “played a central and essential role in the FBI’s and [DOJ’s] decision to seek the FISA order”).) Thereafter, in October 2016, Steele met with two officials at the U.S. Department of State: Kathleen Kavalec, Deputy Assistant Secretary in the

Bureau of European and Eurasian Affairs; and Jonathan Winer, Deputy Assistant Secretary in the Bureau of International Narcotics and Law Enforcement Affairs. (*Id.* at 117.) In her notes from that meeting, Kavalec recounted that “Peter [sic] Aven of Alfa Bank has been the conduit for secret communications between the Kremlin and Manafort; messages are encrypted via TOR software and run between a hidden server managed by Alfa Bank.” (Ex. 19, Rowan Scarborough, *Dossier author Christopher Steele breaks silence with IG report rebuttal*, WASH. TIMES (Dec. 19, 2019) at 5, <https://www.washingtontimes.com/news/2019/dec/16/christopher-steele-trump-dossier-author-rebuts-ig/> (last visited June 11, 2020) (hereinafter “Dec. 16, 2019 *Washington Times* article”); Ex. 17, OIG Report at 117.) On October 13, 2016, Kavalec reportedly downloaded Steele’s summary of the server allegations from a private cloud storage service and transmitted it to FBI section chief Stephen Laycock. (Ex. 20, John Solomon, *Christopher Steele’s nugget of fool’s gold was easily disproven—but FBI didn’t blink an eye*, THE HILL (May 21, 2019), at 2, <https://thehill.com/opinion/white-house/444884-christopher-steeles-nugget-of-fools-gold-was-easily-disproven-but-fbi> (last visited June 11, 2020); Ex. 17, OIG Report at 119.) In addition, Simpson reportedly met with Ohr and shared information regarding the alleged server link in December 2016. (Ex. 19, Dec. 16, 2019 *Washington Times* article at 5; Ex. 21, John Solomon, *Move over ‘grassy knoll,’ the Trump-Russia bank tale joins unproven conspiracies list*, THE HILL (Oct. 14, 2018) at 2, <https://thehill.com/opinion/white-house/411209-move-over-grassy-knoll-the-trump-russia-bank-tale-joins-unproven> (last visited June 11, 2020).) Simpson also pitched the false server story to multiple journalists.

58. The FBI reportedly used these sources of information to seek a warrant from the Foreign Intelligence Surveillance Court authorizing it to wiretap the server in Trump Tower for the purpose of investigating Alfa Bank and another Russian bank, including those banks’ possible

connections to the Trump campaign. The court granted the FBI's request in October 2016. (*See generally* Ex. 17, OIG Report at i–xix; *see also* Ex. 22, Louise Mensch, *EXCLUSIVE: FBI 'Granted FISA Warrant' Covering Trump Camp's Ties to Russia*, HEAT STREET (Nov. 7, 2016) at 1–2, <https://archive.is/xFqPB> (last visited June 11, 2020).)

59. At around the same time, FBI agents visited Listrak's offices to obtain information from the company. (Ex. 23, Tim Mekeel, *FBI gets Lititz firm's help in probe of Russian bank's 'odd' interest in Trump Hotels marketing emails*, LANCASTER ONLINE (Mar. 10, 2017), at 1, https://lancasteronline.com/news/local/fbi-gets-lititz-firm-s-help-in-probe-of-russian/article_ef5d5ed0-05ae-11e7-a003-471e5543b26a.html (last visited June 11, 2020); Ex. 5, Oct. 8, 2018, *New Yorker* article at 7.) Ross Kramer, Listrak's CEO, told reporters that he “gave them everything they asked for.” (Ex. 5, Oct. 8, 2018, *New Yorker* article at 7.)

60. The FBI's investigation continued into 2017. In March 2017, for instance, FBI agents met with Daniel Jones, the president of the Penn Quarter Group and a former FBI investigator and Senate aide. (Ex. 24, Rowan Scarborough, *FBI refuses to say if it has received Daniel Jones' anti-Trump research*, WASH. TIMES (May 8, 2019), at 2, <https://www.washingtontimes.com/news/2019/may/8/fbi-refuses-reveal-if-daniel-jones-alfa-bank-serve/> (last visited June 11, 2020).) Jones reportedly told the FBI that the Penn Quarter Group was funded by seven to ten wealthy donors in New York and California and had retained Steele and Fusion GPS to explore alleged Russian interference in the 2016 election. (*Id.*) Jones and the Penn Quarter Group planned to share any information that they obtained with policymakers on Capitol Hill, the mainstream media, and the FBI. (*Id.* at 3.) At the same time that he was assisting the FBI, Jones assembled a team of computer scientists to review the computer data compiled by Max's group, which an unnamed Democratic Senator disclosed to Jones and

requested him to analyze. Jones assembled two teams of computer scientists, both of which consulted with Camp and Max. (Ex. 5, Oct. 8, 2018 *New Yorker* article at 7.) The findings of those teams were the backbone of the October 8, 2018 article in *The New Yorker* that concluded that the DNS data in fact was evidence of a covert communication channel between Alfa Bank and the Trump Organization.

VI. Exoneration of Alfa Bank

61. Law enforcement officials and cybersecurity experts who reviewed all available evidence of purported communications between Alfa Bank and the Trump Organization concluded that there were no such communications. These officials and experts determined that Alfa Bank did not communicate with the Trump Organization in 2016 and 2017 through their respective servers or otherwise.

62. In September 2016, Alfa Bank engaged Mandiant, a preeminent U.S. cybersecurity consulting firm, to investigate the allegations that recently had surfaced. Mandiant determined that there was no evidence of communications between Alfa Bank and the Trump Organization. (Ex. 3, Mandiant Report.)

63. In the wake of the 2017 cyberattacks, Alfa Bank retained a second elite cybersecurity expert group, Stroz Friedberg, to review evidence related to those attacks. Stroz Friedberg concluded that its investigation had “revealed no actual connections or communications between Alfa-Bank and President Trump or the Trump Organization.” (Ex. 7, Stroz Friedberg Report at 3; *accord id.* at 2 (“find[ing] no evidence of any connections or communications between Alfa-Bank and the Trump Organization occurring in 2017”).) Stroz Friedberg further determined that the server traffic from February and March 2017 was “consistent with the type of traffic often

seen coming from . . . attackers checking or testing a company's security.” (*Id.* (“[I]t is likely that the suspicious queries came from researchers and/or would-be attackers . . .”).)

64. Most recently, Alfa Bank retained a third cybersecurity consulting firm, Ankura, to review all of the evidence related to the purported communications between Alfa Bank and the Trump Organization. As described above, Ankura found no “support whatsoever for the allegation of a ‘secret server’ or covert ‘cyber links’ between Alfa Bank and the Trump Organization.” (Ex. 2, Ankura Report at 3.) Instead, Ankura concluded that malicious actors likely manipulated DNS traffic to create the false illusion of communications between Alfa Bank and the Trump Organization. (*Id.*)

65. The Special Counsel’s Office, whose mandate included investigating Russian efforts to interfere in the 2016 U.S. Presidential election, also reviewed allegations that Alfa Bank and the Trump Organization had orchestrated a secret communication channel through the use of their servers. Special Counsel Robert Mueller testified before Congress that his “belief at this point” was that the server allegations were “not true.” (Ex. 25, *Former Special Counsel Robert S. Mueller III on the Investigation into Russian Interference in the 2016 Presidential Election*, U.S. H.R., Permanent Select Comm. on Intelligence, 116 Cong. (July 24, 2019) at 64.)

66. In December 2019, the Office of the Inspector General of the DOJ released its review into the FBI’s investigation into Russian efforts to interfere in the 2016 election. The final report noted that “[t]he FBI investigated whether there were cyber links between the Trump Organization and Alfa Bank, but had concluded by early February 2017 that there were no such links.” (Ex. 17, OIG Report at 119 n.259.)

CAUSES OF ACTION

I. Count One: Florida Civil Remedies for Criminal Practices Act (Primary Violation) (Fla. Stat. Ann. § 772.101 *et seq.*)

67. All preceding paragraphs are repeated, re-alleged, and incorporated as if fully set forth herein.

68. Florida RICO provides that “[i]t is unlawful for any person . . . [e]mployed by, or associated with, any enterprise to conduct or participate, directly or indirectly, in such enterprise through a pattern of criminal activity or the collection of an unlawful debt.” Fla. Stat. Ann. § 772.103(3). The statute further provides a private right of action to “[a]ny person who proves by clear and convincing evidence that he or she has been injured by reason of any violation of the provisions of s. 772.103.” *Id.* § 772.104(1).

69. Defendants are employed by, or associated with, the Disinformation Enterprise. Fla. Stat. Ann. § 772.103(3). The Disinformation Enterprise is a partnership, corporation, business trust, or other legal entity, or any unchartered union, association, or group of individuals associated in fact although not a legal entity. *Id.* Upon information and belief, Defendants are members of the Disinformation Enterprise, an ongoing organization whose various associates function as a continuing unit. Upon information and belief, Defendants have associated together and with others to form a group with the common purpose of orchestrating and executing disinformation campaigns to disrupt the activities of governments, corporations, and individuals. Upon information and belief, the Disinformation Enterprise preexisted the perpetration of cyberattacks against Alfa Bank in 2016 and 2017 and continues to exist.

70. Defendants conducted or participated, directly or indirectly, in the affairs of the Disinformation Enterprise. *See* Fla. Stat. Ann. § 772.103(3). Defendants, separately and collectively, participated in the operation or management of the Disinformation Enterprise itself.

Specifically, Defendants developed and executed, in whole or in part, the 2016 and 2017 cyberattacks directed at Alfa Bank.

71. Defendants conducted or participated, directly or indirectly, in the affairs of the Disinformation Enterprise through “criminal activity.” Fla. Stat. Ann. § 772.103(3). From at least May 2016 through March 2017, Defendants committed; attempted to commit; or solicited, coerced, or intimidated another person to commit crimes chargeable by indictment or information under the Florida Computer Crimes Act (“FCCA”). *Id.* § 772.102(1)(a)(21) (citing Chapter 815). Defendants, through the scheme outlined above, willfully, knowingly, and without authorization introduced a computer contaminant or modified or rendered unavailable data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, computer network, or electronic device. *Id.* § 815.04(1). Alternatively, or in addition, Defendants, through the scheme outlined above, willfully, knowingly, and without authorization or exceeding authorization accessed or caused to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized or the manner of use exceeds authorization; disrupted or denied or caused the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another; destroyed, injured, or damaged any computer, computer system, computer network, or electronic device; or introduced any computer contaminant into any computer, computer system, computer network, or electronic device. *Id.* § 815.06(2).

72. Alfa Bank’s servers and the other servers discussed herein are computers, computer networks, computer systems, or electronic devices within the meaning of Fla. Stat. Ann. §§ 815.03(2), (4), (7), and (9).

73. Defendants conducted or participated, directly or indirectly, in the affairs of the Disinformation Enterprise through a “pattern” of criminal activity, as defined in the preceding paragraphs. Fla. Stat. Ann. § 772.103(3). Defendants’ cyberattacks against Alfa Bank in 2016 and 2017 qualify as at least two incidents of criminal activity that have the same or similar intents, results, accomplices, victims, or methods of commission or that otherwise are interrelated by distinguishing characteristics and are not isolated incidents, and the last of such incidents occurred within five years after a prior incident of criminal activity. *Id.* § 772.102(4).

74. As the direct and proximate result of Defendants’ unlawful acts, Alfa Bank was injured in its business or property in an amount to be proven at trial.

II. Count Two: Florida Civil Remedies for Criminal Practices Act (Conspiracy) (Fla. Stat. Ann. § 772.101 *et seq.*)

75. Paragraphs 1–66 are repeated, re-alleged, and incorporated as if fully set forth herein.

76. Florida RICO provides that “[i]t is unlawful for any person . . . [t]o conspire or endeavor to violate any of the provisions of subsection (1), subsection (2), or subsection (3)” of section 772.103. Fla. Stat. Ann. § 772.103(4). The statute further provides a private right of action to “[a]ny person who proves by clear and convincing evidence that he or she has been injured by reason of any violation of the provisions of s. 772.103.” *Id.* § 772.104(1).

77. Defendants are employed by, or associated with, the Disinformation Enterprise. Fla. Stat. Ann. § 772.103(3). The Disinformation Enterprise is a partnership, corporation, business trust, or other legal entity, or any unchartered union, association, or group of individuals associated in fact although not a legal entity. *Id.* § 772.102(3). Upon information and belief, Defendants are members of the Disinformation Enterprise, an ongoing organization whose various associates function as a continuing unit. Upon information and belief, Defendants have associated together

and with others to form a group with the common purpose of orchestrating and executing disinformation campaigns to disrupt the activities of governments, corporations, and individuals. Upon information and belief, the Disinformation Enterprise preexisted the perpetration of cyberattacks against Alfa Bank in 2016 and 2017 and continues to exist.

78. Defendants conspired or endeavored to conduct or participate, directly or indirectly, in the affairs of the Disinformation Enterprise. Fla. Stat. Ann. § 772.103(3). Defendants, separately and collectively, conspired or endeavored to participate in the operation or management of the Disinformation Enterprise itself. Specifically, Defendants conspired or endeavored to develop and execute, in whole or in part, the 2016 and 2017 cyberattacks directed at Alfa Bank. Defendants knew of the overall objectives of the Disinformation Enterprise and agreed to further its purpose or, alternatively, committed at least two predicate acts of criminal activity themselves.

79. Defendants conspired or endeavored to conduct or participate, directly or indirectly, in the affairs of the Disinformation Enterprise through “criminal activity.” Fla. Stat. Ann. § 772.103(3). From at least May 2016 through March 2017, Defendants conspired to commit crimes chargeable by indictment or information under the FCCA. *Id.* § 772.102(1)(a)(21) (citing Chapter 815). Defendants, through the scheme outlined above, conspired or endeavored to willfully, knowingly, and without authorization introduce a computer contaminant or modified or rendered unavailable data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, computer network, or electronic device. *Id.* § 815.04(1). Alternatively, or in addition, Defendants, through the scheme outlined above, conspired or endeavored to willfully, knowingly, and without authorization or exceeding authorization access or cause to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized or the manner of use exceeds authorization;

disrupt or deny or cause the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another; destroy, injure, or damage any computer, computer system, computer network, or electronic device; or introduce any computer contaminant into any computer, computer system, computer network, or electronic device. *Id.* § 815.06(2).

80. Alfa Bank’s servers and the other servers discussed herein are computers, computer networks, computer systems, or electronic devices within the meaning of Fla. Stat. Ann. §§ 815.03(2), (4), (7), and (9).

81. Defendants conspired or endeavored to conduct or participate, directly or indirectly, in the affairs of the Disinformation Enterprise through a “pattern” of criminal activity, as defined in the preceding paragraphs. Fla. Stat. Ann. § 772.103(3). Defendants’ cyberattacks against Alfa Bank in 2016 and 2017 qualify as at least two incidents of criminal activity that have the same or similar intents, results, accomplices, victims, or methods of commission or that otherwise are interrelated by distinguishing characteristics and are not isolated incidents, and the last of such incidents occurred within five years after a prior incident of criminal activity. *Id.* § 772.102(4).

82. As the direct and proximate result of Defendants’ unlawful acts, Alfa Bank was injured in its business or property in an amount to be proven at trial.

JURY TRIAL DEMAND

Alfa Bank requests a trial by jury on all issues so triable.

RELIEF REQUESTED

WHEREFORE, Alfa Bank respectfully prays that this Court enter judgment against Defendants for the following:

1. Treble monetary damages in an amount to be proven at trial;
2. Costs and attorneys' fees incurred in this action;
3. Pre- and post-judgment interest to the extent permitted by law; and
4. Such other relief as the Court may deem just and proper.

Dated: June 11, 2020

Respectfully submitted,

/s/ Terrance Anderson, Jr.

Terrance Anderson, Jr. (Bar No. 27426)
NELSON MULLINS RILEY & SCARBOROUGH LLP
Lynn Financial Center
1905 NW Corporate Blvd., Ste. 310
Boca Raton, FL 33431
(561) 218-8862
tw.anderson@nelsonmullins.com

Jonathan Etra (Bar No. 686905)
NELSON MULLINS RILEY & SCARBOROUGH LLP
2 South Biscayne Blvd., 21st Floor
Miami, FL 33131
(305) 373-9447
jonathan.etra@nelsonmullins.com

Margaret E. Krawiec (*pro hac vice* motion forthcoming)
Michael A. McIntosh (*pro hac vice* motion forthcoming)
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
1440 New York Ave. NW
Washington, DC 20005
(202) 371-7000
margaret.krawiec@skadden.com
michael.mcintosh@skadden.com

EXHIBIT 1

NOT A CERTIFIED COPY

PRWeb

LOGIN

CREATE A FREE ACCOUNT

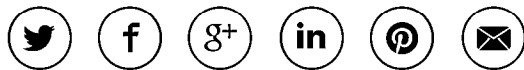
HOME **NEWS CENTER** **BLOG**

Monday, June 8, 2020



Cendyn is Tapped for Interactive Marketing Services by the Trump Organization

Share Article



Cendyn, the leader in interactive marketing for the hospitality industry, has been selected as The Trump Organization's exclusive interactive marketing agency.

BOCA RATON, FL (PRWEB) JUNE 21, 2007

Cendyn, the leader in interactive marketing for the hospitality industry, has been selected as The Trump Organization's exclusive interactive marketing agency. Implementation of Cendyn's products and services will enhance The Trump Organization's global online presence which includes the website <http://www.trump.com>, along with more than 50 private label websites for Trump owned properties and investments (real estate, golf and hotel).

The Trump Hotel Collection, which includes Trump International Hotel & Tower in New York and soon to open hotels in Las Vegas and Chicago, will feature Cendyn's CRM Suite: eInsight™, eConcierge™ and eSurvey™ which allows hoteliers to effectively manage the entire view of each guest from a single platform. The Trump Hotel Collection will also feature Cendyn's award-winning ePresence™ for website design, eVisibility™ for Search Engine / Pay-per-Click Marketing and eProposal™ system, for delivery of custom proposals in less than 60 seconds to meeting planner clientele.

"In selecting Cendyn as our interactive marketing firm, we know we are availing ourselves of innovative products that speak to the



During the presentation to The Trump Organization, I had the opportunity to meet the management team and learn

needs and interests of our all-important customers. With their help, we look forward to making it easy and rewarding to interact with us," commented Jim Petrus, Chief Operating Officer, The Trump Organization.

All Trump real estate and golf interests will utilize Cendyn's eInsight™ system for guest intelligence and central management of prospect, member and customer information. Cendyn's ePresence™ will capture the outstanding attributes of the Trump Chicago and Trump Las Vegas residences, as well as all Trump Golf Courses in new website designs to be launched later this year.

"During the presentation to The Trump Organization, I had the opportunity to meet the management team and learn about the company's five-star philosophy. Their commitment to customer service excellence is impressive. The company is visionary and Cendyn is excited to be on board." said Charles Deyo, Cendyn's President.

With Cendyn's expertise and proven track record, The Trump Organization has a partner providing interactive marketing solutions that enable Trump personnel to provide guests with high touch and memorable experiences at all Trump properties around the globe.

About Trump Hotel Collection – <http://www.trump.com>

Trump Hotel Collection is currently comprised of Trump International Hotel and Tower (New York City), Trump International Hotel & Tower (Chicago, opening December 2007) and Trump International Hotel & Tower (Las Vegas, opening spring 2008). Additional hotels and resorts are under development in several North American markets, including New York, Florida, Hawaii, Louisiana and Ontario (Canada) and in strategic markets around the world including Mexico, Panama, the Dominican Republic and Dubai.

About Cendyn – <http://www.cendyn.com>

Cendyn is a full-service interactive marketing firm established in 1996. Cendyn has won several prestigious industry awards for its design, innovation and marketing efforts.

Specializing in turnkey solutions for the travel and hospitality industry as well as other business-to-business and consumer-focused industries, the innovative products of this Boca Raton, Florida-based company are in use by more than 6,000 hotels worldwide. Cendyn provides highly personalized customer service and its comprehensive range of services include website marketing, website design and development, search engine marketing, branding and logo development, along with many other interactive products such as eProposal™, eConcierge™, eSurvey™, eInsight™, eContact™, eConnectivity™, eBooker™, eMenus™ eMail/Direct Mail™ and eVisibility™ among others. For a complete list of products and services, please visit our website <http://www.cendyn.com>. Let Cendyn show you how far an idea can go!

For more information about Cendyn, contact Robin Deyo, Executive Vice President by email [rdeyo\(at\)cendyn.com](mailto:rdeyo(at)cendyn.com) or phone 561.314.3212.

about the company's five-star philosophy. Their commitment to customer service excellence is impressive. The company is visionary and Cendyn is excited to be on board.

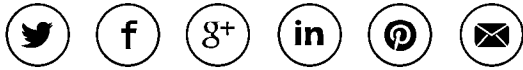
**Past News
Releases**



Contact:
Sarah E. Flynn
Willcaro Communications LLC
sarahf(at)willcarocomm.com
561.243.1922 (EST)

###

Share article on social media or email:



View article via:

PDF **PRINT**

Contact Author

SARAH E. FLYNN

Cendyn
561-243-1922
Email >

VISIT WEBSITE

News Center

PRWeb



Questions about a news article you've read?

Reach out to the author: contact and available social following information is listed in the top-right of all news releases.

Questions about your PRWeb account or interested in learning more about our news services?

Call PRWeb:1-866-640-6397



[CREATE A FREE ACCOUNT](#)

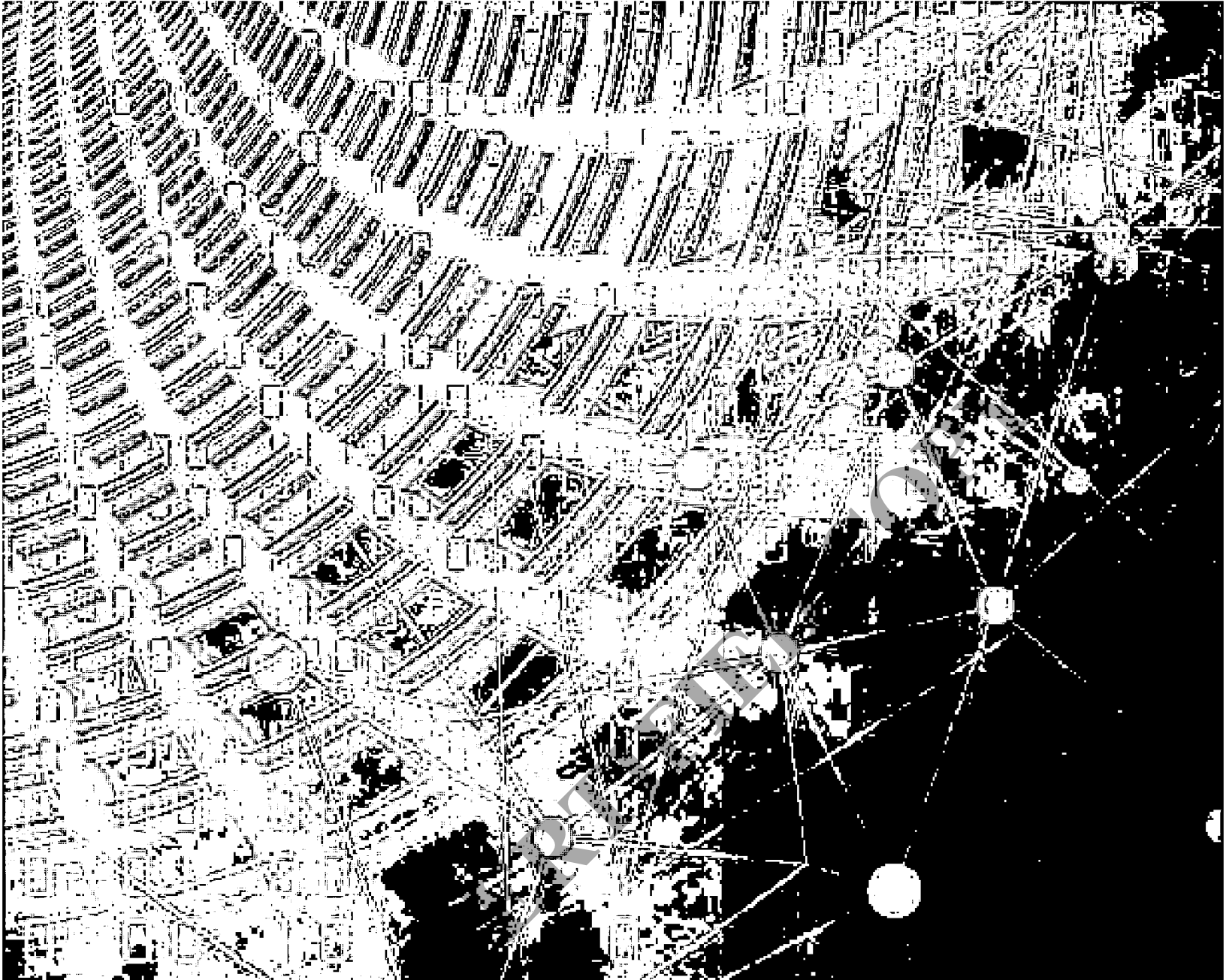
CISION

©Copyright 1997-2015, Vocus PRW Holdings, LLC. Vocus, PRWeb, and Publicity Wire are trademarks or registered trademarks of Vocus, Inc. or Vocus PRW Holdings, LLC.

NOT A CERTIFIED COPY

EXHIBIT 2

NOT A CERTIFIED COPY



Covert Channel Allegation: New Data Analysis Results

APRIL 2020

ankura 

TABLE OF CONTENTS

INTRODUCTION 3

EXECUTIVE SUMMARY 3

Overview..... 3

Key Considerations 4

MULTI-THREADED DNS ANALYSIS 4

Timeline 4

Marketing Infrastructure Details..... 8

Root Cause Analysis..... 18

CONCLUSION 19

Observations..... 19

APPENDIX A..... 21

Domains hosted on 198.91.42.0/23 21

Domains hosted on 63.251.151.0/24 34

Domains hosted on 64.135.26.0/24 35

Domains hosted on 64.95.241.0/34 36

Domains hosted on 69.25.15.0/24 37

APPENDIX B 39

DNS Testing For External Query Activity (DNS Forgery) 39

NOT A CERTIFIED COPY

INTRODUCTION

Kirkland & Ellis LLP, on behalf of Alfa-Bank JSC (Alfa-Bank), engaged Ankura Consulting Group to investigate and independently review newly identified evidence regarding the historical DNS records of servers alleged to have operated as a "secret server" back channel for Russian interest access to the Trump Organization, during the run-up to the 2016 U.S. Presidential election. In its recent review of the FBI's "Crossfire Hurricane" Investigation, the U.S. DOJ Inspector General (IG) stated: "The FBI investigated whether there were cyber links between the Trump Organization and Alfa Bank, but had concluded by early February 2017 that there were no such links."¹ While the IG's report is clear with respect to the FBI's finding on this issue, the report did not include the underlying technical evidence and analysis supporting this conclusion.

Ankura's detailed review of this matter, including newly identified data, sheds new light on the server allegations and includes findings supporting the FBI's conclusion debunking the alleged covert cyber links between Alfa-Bank and the Trump Organization. Additionally, Ankura's analysis of the DNS records and the overt nature of the DNS activity, suggest that a likely scenario is that threat actors may have artificially created DNS activity to make it appear as though a connection existed, for "discovery" later. If true, this would constitute a potential violation of various US federal laws.

This document summarizes the analysis that Ankura's Cyber Threat Analysis and Pursuit Team (CTAPT) undertook to assess the data provided by Kirkland & Ellis along with other information sourced by Ankura, including open source data, information obtained from various passive Domain Name System (DNS) data providers, threat intelligence analytics, and Internet Protocol (IP) registrations.

EXECUTIVE SUMMARY

OVERVIEW

For this investigation Ankura's CTAPT relied on recently identified SecurityTrails DNS records, DomainTools passive DNS databases, and PassiveTotal archives for inquiry into Cendyn, Internap, Listra, and Trump related entities. CTAPT concluded that the available DNS records do not provide any support whatsoever for the allegation of a "secret server" or covert "cyber links" between Alfa-Bank and the Trump Organization. The three sources of DNS records reflect that servers attributed to the Trump Organization were actually owned and operated by a hotel marketing related company named "Central Dynamics" (Cendyn). DNS records also show Cendyn was engaged in legitimate marketing activity for numerous global hotel chains, including Trump Hotels.

CTAPT's investigation discovered the Cendyn company and its servers have a long history of providing marketing solutions for hotel chains. Relevant here, the relationship between Cendyn and Trump Hotels goes back to at least 2009. We come to this understanding after considering multiple passive DNS sources, reviewing previous reporting, and assessing the original allegations as reported via multiple news outlets and blogs.

¹<https://www.justice.gov/storage/120919-examination.pdf>

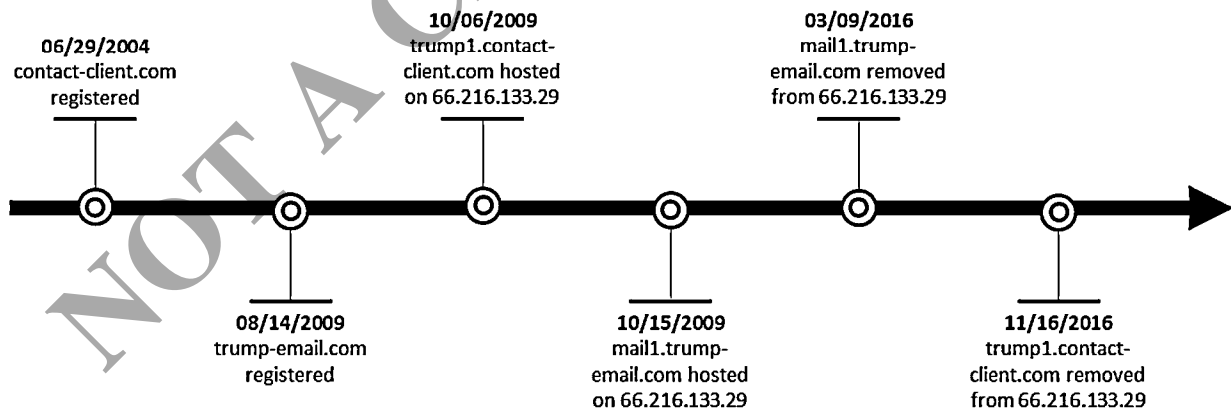
Cendyn's Trump Organization related marketing activity, including the activity alleged in 2016 to be associated with covert communications, was in fact hardly confidential. Available DNS records clearly attribute Cendyn activities to publicly resolvable domain names and IP address registrations to Trump related entities, with no effort to conceal the connection. Alfa-Bank's publicly attributable domains and IPs were also clearly in the DNS and IP registration records, which is the opposite of secret or covert. Additionally, CTAPT's research and analysis demonstrate it is possible -- indeed likely -- that threat actors may have conducted some inauthentic DNS activity to force a "connection" between Alfa-Bank and the Trump Organization, only to then later "discover" the connection.

KEY CONSIDERATIONS

- The DNS query and response process typically involves an entity sending a domain query to a name server and, in return, receiving the hosting IP addresses where the domain of interest can be found. The DNS lookup process does not necessarily connect to the domain being translated to an IP address. The system originating the query may or may not use that delivered IP from the DNS process to then navigate to the IP address. DNS queries are not evidence of an actual communication taking place between a DNS requestor and the requested domain. One fallacy that is common is to assume the DNS lookup process connects with the domain of interest.
- The Sender Policy Framework (SPF) records for both trump-email[.]com and contact-client[.]com were configured in a way that a threat actor could send spoofed emails or inauthentic DNS queries masquerading as these domains to Alfa-Bank. As a result, this inauthentic activity could force Alfa-Bank servers to repeatedly query DNS records for both of these domains even if Alfa-Bank never received a legitimate marketing email.

MULTI-THREADED DNS ANALYSIS

TIMELINE



Historical DNS records were collected from a total of three (3) sources for DNS entries related to *trump-email.com and *contact-client.com. CTAPT analysis of multiple DNS sources, data available published online, and other research activities revealed no evidence that mail1.trump-email[.]com and trump1.contact-client[.]com were used by Alfa-Bank and the Trump Organization for covert communications.

SecurityTrails^{2,3}, Domaintools^{4,5}, and PassiveTotal^{6,7} were queried for all available historical DNS data for both *.trump-email[.]com and *.contact-client[.]com domains. However, the historical DNS data retrieved from SecurityTrails did not match completely with what was retrieved from additional passive DNS providers, namely PassiveTotal and DomainTools. This issue highlights why attempting to make assertions using only one DNS source can lead to analysis errors. DNS record discrepancies exist because different passive DNS providers often leverage unique sensors and data points to collect and populate their DNS data. For example, PassiveTotal utilizes a variety of open and proprietary sensors and sources including 360CN, Emerging Threats, Farsight, Kaspersky, Mnemonic, OpenDNS, Pingly, RiskIQ, and Virustotal:

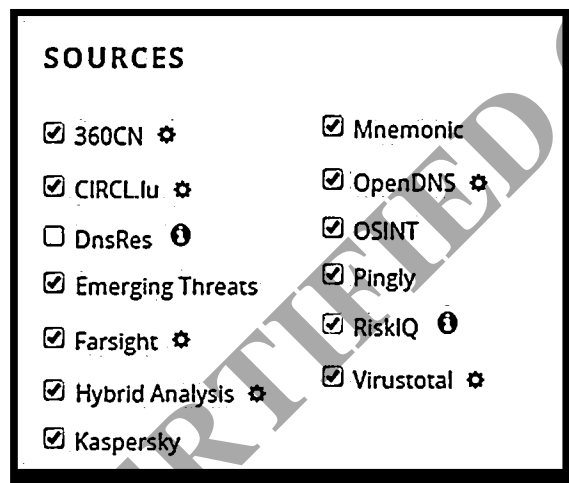


Figure 1: Screenshot showing PassiveTotal user options for passive DNS source

Mail1.trump-email[.]com

During review of the *.trump-email[.]com DNS artifacts, we noted an example of DNS discrepancies related to this domain's "A" record. A key data point missing from SecurityTrails, yet available from other sources, was that mail1.trump-email[.]com did, in fact, have an A record prior to 03/08/2017, the first date that SecurityTrails identified it as having an A record. PassiveTotal records show that this fully qualified domain name (FQDN) had an A record pointing to 66.216.133[.]29 beginning on 10/15/2009 and running through 03/09/2016. This fact illustrates the historical and overt use of Cendyn infrastructure for Trump Hotel related marketing. The PassiveTotal information listing the A record expiration in March 2016 also supports the timeline in the New Yorker article⁸ that Cendyn was

²<https://securitytrails.com/domain/trump-email.com/history/a>

³<https://securitytrails.com/domain/contact-client.com/history/a>

⁴<https://research.domaintools.com/iris/search/?q=trump-email.com>

⁵<https://research.domaintools.com/iris/search/?q=contact-client.com>

⁶<https://community.riskiq.com/search/trump-email.com>

⁷<https://community.riskiq.com/search/contact-client.com>

⁸<https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign>

no longer used by the Trump Organization as a marketing provider after March 2016. However, this new observation challenges the same New Yorker article’s claim that mail1.trump-email[.]com was removed from 66.216.133.29 on or about September 23, 2016, after the story surfaced in the media. The article states: “The Trump domain vanished from the Web on the morning of Friday, September 23rd, two days after the Times presented its data to B.G.R., Alfa Bank’s lobbyists in Washington, but before it called Trump or Cendyn.” The Trump related domain did not actually vanish, after the Times presented its data, but was changed months before. According to multiple passive DNS sources, the domain actually “vanished” from the web on March 9, 2016. The change was more likely done in accordance with marketing activity, as the New Yorker pointed out, because Cendyn was no longer used by the Trump organization in March 2016. Cendyn corroborated this when it told CNN that it “stopped sending e-mails for the Trump Organization in March 2016, before the peculiar activity began.”⁹

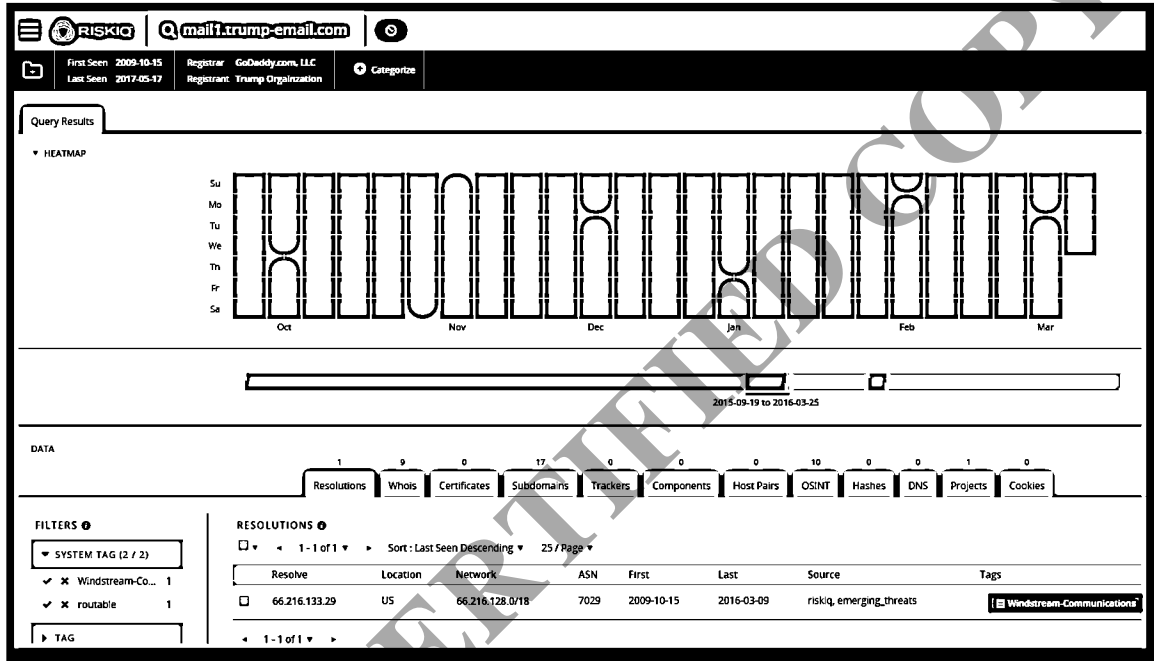


Figure 2: Screenshot from PassiveTotal showing A record for mail1-trump-email[.]com

Additionally, DomainTools passive DNS records show different dates pertaining to A records for mail1.trump-email[.]com. DomainTools queries different sources and sensors for DNS records. DomainTools passive DNS history shows the following records:¹⁰

Query	Type	Source	Response	First Seen	Last Seen
mail1.trump-email.com	A	B	66.216.133.29	2014-12-04, 20:07	2016-09-13, 01:47
mail1.trump-email.com	A	A	66.216.133.29	2014-12-04, 19:54	2016-09-23, 13:45
mail1.trump-email.com	A	D	66.216.133.29	2010-07-02, 19:02	2016-09-13, 01:47
mail1.trump-email.com	A	D	66.216.133.29	2017-03-08, 04:32	2017-07-16, 20:53

⁹<https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign>

¹⁰<https://research.domaintools.com/iris/investigations/464456/search/dc3e5548-e445-4756-ba19-9397bcfc816e/fb0a15ed-ea6d-440e-9d1f-29aa59a338c4>

The records above demonstrate the challenges of relying on one source for DNS analysis. If the original "researchers" and news media outlets used a single point of collections or DNS historical data, it is likely they missed additional clarifying context, or chose the data source that best met the intended message.

Trump1.contact-client[.]com

Another key data point to consider is that one of the DNS providers did not return any records for the trump1.contact-client[.]com domain.¹¹ If analysis relied solely on this source, the results would reflect that an A record for this FQDN never existed, as potentially seen in the New Yorker article¹² which stated that trump1.contact-client[.]com "does not appear to have been previously active." The article states: "On the night of Tuesday, September 27th, ten minutes after the bank made its last failed attempt, it looked up the domain name trump1.contact-client.com—which was, it turned out, another route to the same Trump server. The alternative domain name does not appear to have been previously active; no one has produced an e-mail sent from it. So how did Alfa find it?" In contrast, PassiveTotal records show that trump1.contact-client[.]com did have an A record pointing to 66.216.133[.]29 from 10/06/2009 through 11/16/2016. Both mail1.trump-email[.]com and trump1.contact-client[.]com had the same A record IP address over most of the same time span¹³ and answers the question about how an Alfa-Bank DNS request "found it."

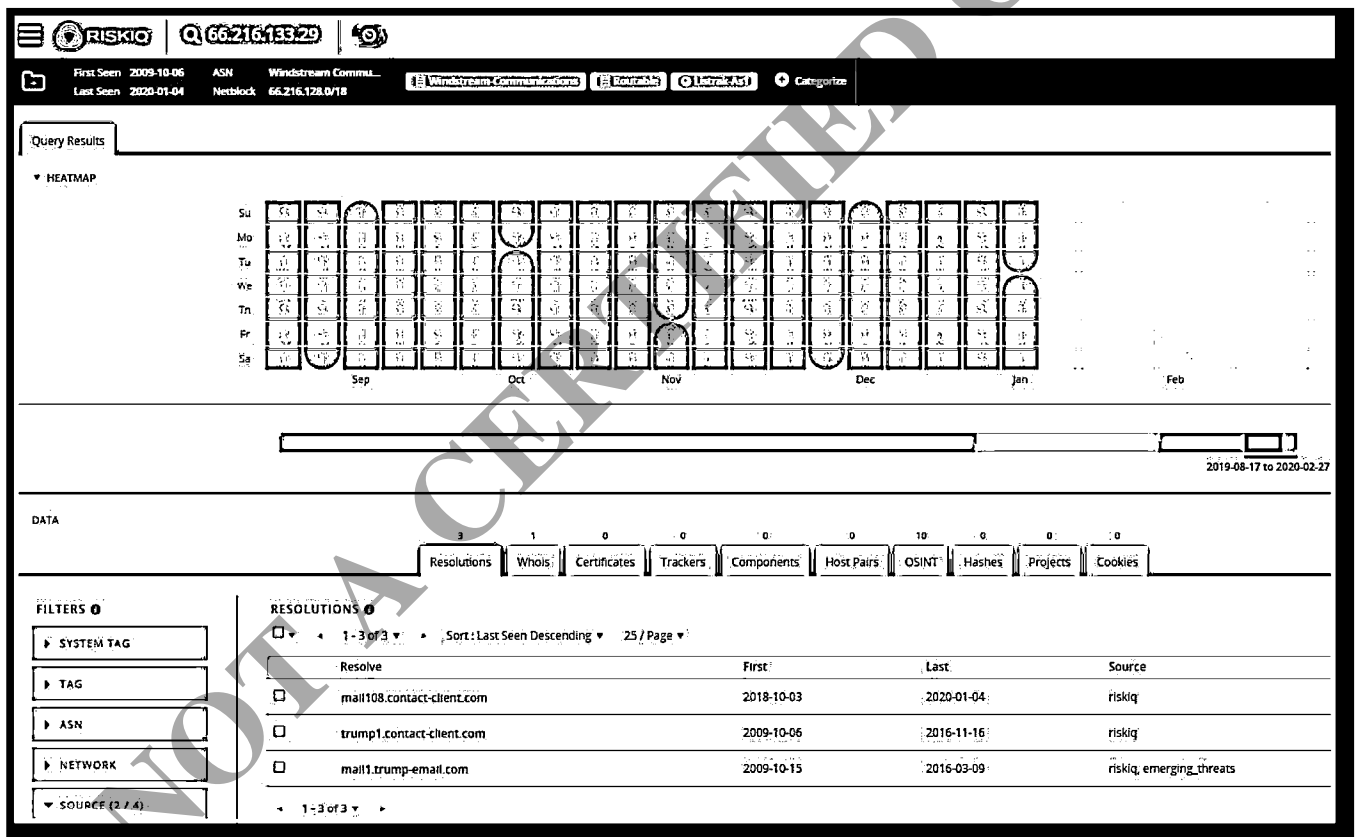


Figure 3: Screenshot from PassiveTotal showing overlap between trump1.contact-client[.]com & mail1.trump-email[.]com

¹¹ <https://securitytrails.com/domain/contact-client.com/history/a>

¹² <https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign>

¹³ <https://community.riskiq.com/search/66.216.133.29>

MARKETING INFRASTRUCTURE DETAILS

CTAPT's review of the publicly available SecurityTrails¹⁴ DNS records concluded that Cendyn server DNS configurations were consistent with marketing infrastructure for the hotel industry, including Trump Hotels. However, SecurityTrails doesn't tell as complete a picture as DomainTools and PassiveTotal both do. One example of SecurityTrails' lack of resolution is where additional sources prove Cendyn was operating in a marketing capacity for the Trump Organization as far back as 2009, countering key claims of some of the initial DNS analysis in the press. For example, mail1.trump-email[.]com and trump1.contact-client[.]com, both registered by Cendyn and both hosted on the same Listrak IP address beginning in 2009 through 2016, were according to DNS records, reachable for nearly seven (7) years. This type of static activity is typically employed by marketing entities to avoid interruptions and misconfiguration impacts when emails are marked as spam or websites become unreachable.

Cendyn company (Central Dynamics) infrastructure and configuration management played key roles for both trump-email[.]com and contact-client[.]com. Cendyn is reported to be a services and software company focused on serving the global hospitality industry. According to their website, they serve clients in 143 different countries and have delivered over 1.5 billion communications on behalf of their customers every year.¹⁵

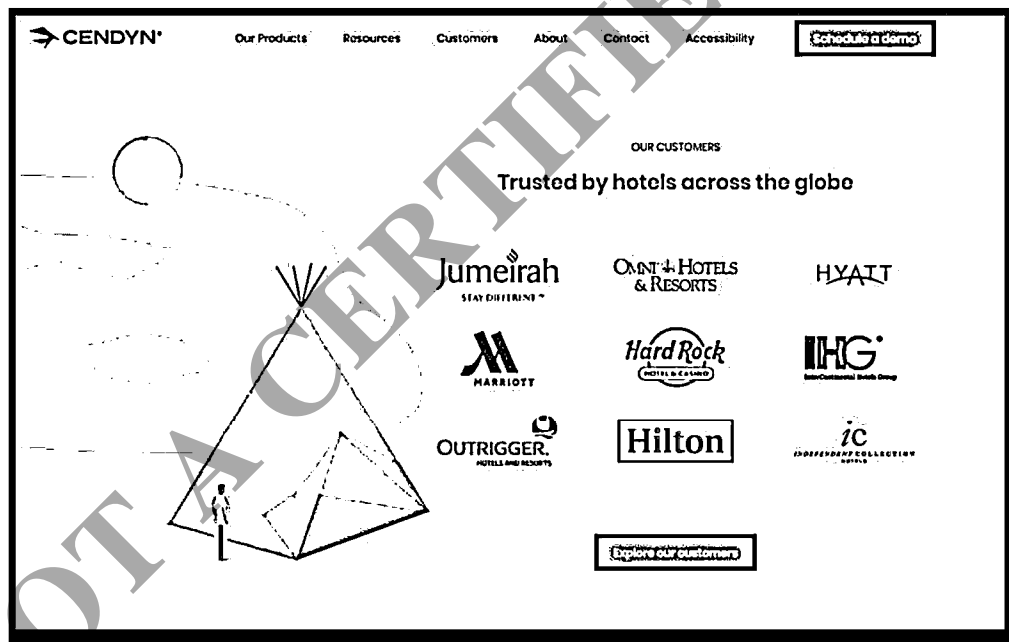


Figure 4: Screenshot of Cendyn's website listing some of their hospitality clients.

CTAPT review of DomainTools' historical WHOIS records shows that both trump-email[.]com and contact-client[.]com domains were registered to and owned by Cendyn related entities into 2016. Specifically, Trump1.contact-client[.]com was active and discoverable before and during the time that the alleged "secret" server was in operation.

¹⁴<https://securitytrails.com/domain/contact-client.com/history/a>

¹⁵<https://www.cendyn.com/company/>

2016-02-27	2016-07-01
1 Domain Name: CONTACT-CLIENT.COM	1 Domain Name: CONTACT-CLIENT.COM
2 Registry Domain ID: 123705252_ECMAN_CCM-VRSN	2 Registry Domain ID: 123705252_ECMAN_CCM-VRSN
3 Registrar WHOIS Server: whois.godaddy.com	3 Registrar WHOIS Server: whois.godaddy.com
4 Registrar URL: http://www.godaddy.com	4 Registrar URL: http://www.godaddy.com
5 Update Date: 2011-07-18T04:28:07Z	5 Update Date: 2011-07-18T04:28:07Z
6 Creation Date: 2004-06-29T14:41:05Z	6 Creation Date: 2004-06-29T14:41:05Z
7 Registrar Registration Expiration Date: 2021-06-28T14:41:05Z	7 Registrar Registration Expiration Date: 2021-06-28T14:41:05Z
8 Registrar: GoDaddy.com, LLC	8 Registrar: GoDaddy.com, LLC
9 Registrar IANA ID: 146	9 Registrar IANA ID: 146
10 Registrar Abuse Contact Email: abuse@godaddy.com	10 Registrar Abuse Contact Email: abuse@godaddy.com
11 Registrar Abuse Contact Phone: +1.4806242505	11 Registrar Abuse Contact Phone: +1.4806242505
12 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited	12 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
13 Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited	13 Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
14 Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited	14 Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
15 Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited	15 Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
16 Registry Registrant ID: Not Available From Registry	16 Registry Registrant ID: Not Available From Registry
17 Registrant Name: Charles Deyo	17 Registrant Name: Charles Deyo
18 Registrant Organisation:	18 Registrant Organisation:
19 Registrant Street: 1515 N. Federal Hwy	19 Registrant Street: 1515 N. Federal Hwy
20 Registrant City: Boca Raton	20 Registrant City: Boca Raton
21 Registrant State/Province: Florida	21 Registrant State/Province: Florida
22 Registrant Postal Code: 33422	22 Registrant Postal Code: 33422
23 Registrant Country: US	23 Registrant Country: US
24 Registrant Phone:	24 Registrant Phone:
25 Registrant Phone Ext:	25 Registrant Phone Ext:
26 Registrant Fax:	26 Registrant Fax:
27 Registrant Fax Ext:	27 Registrant Fax Ext:
28 Registrant Email: nocontactsfound@secureserver.net	28 Registrant Email: nocontactsfound@secureserver.net
29 Registry Admin ID: Not Available From Registry	29 Registry Admin ID: Not Available From Registry
30 Admin Name: Charles Deyo	30 Admin Name: Charles Deyo
31 Admin Organisation:	31 Admin Organisation:
32 Admin Street: 1515 N. Federal Hwy	32 Admin Street: 1515 N. Federal Hwy
33 Admin City: Boca Raton	33 Admin City: Boca Raton
34 Admin State/Province: Florida	34 Admin State/Province: Florida
35 Admin Postal Code: 33422	35 Admin Postal Code: 33422
36 Admin Country: US	36 Admin Country: US
37 Admin Phone: 561-555-3142	37 Admin Phone: 561-555-3142
38 Admin Phone Ext:	38 Admin Phone Ext:
39 Admin Fax:	39 Admin Fax:
40 Admin Fax Ext:	40 Admin Fax Ext:
41 Admin Email: emcmullin@cendyn.com	41 Admin Email: emcmullin@cendyn.com
42 Registry Tech ID: Not Available From Registry	42 Registry Tech ID: Not Available From Registry
43 Tech Name: Charles Deyo	43 Tech Name: Charles Deyo
44 Tech Organisation:	44 Tech Organisation:
45 Tech Street: 1515 N. Federal Hwy	45 Tech Street: 1515 N. Federal Hwy
46 Tech City: Boca Raton	46 Tech City: Boca Raton
47 Tech State/Province: Florida	47 Tech State/Province: Florida
48 Tech Postal Code: 33422	48 Tech Postal Code: 33422

Figure 5: Screenshot of historical WHOIS record history for contact-client[.]com¹⁶

Figure 5 shows two (2) side by side WHOIS records for contact-client[.]com, dated 02/27/2016 and 07/01/2016. These dates were chosen because the earlier date is before the alleged “secret” server activity began and the later date is after the alleged activity commenced. No ownership changes were documented during this activity or at any other time during the domain’s existence.

¹⁶<https://research.domaintools.com/research/whois-history/search/?q=contact-client.com#changes>

2016-05-03	2016-06-29
1 Domain Name: TRUMP-EMAIL.COM	1 Domain Name: TRUMP-EMAIL.COM
2 Registry Domain ID: 1565681491_DCMAN_CCM-VRSN	2 Registry Domain ID: 1565681491_DCMAN_CCM-VRSN
3 Registrar WHOIS Server: whois.godaddy.com	3 Registrar WHOIS Server: whois.godaddy.com
4 Registrar URL: http://www.godaddy.com	4 Registrar URL: http://www.godaddy.com
5 Update Date: 2015-06-26T17:27:59Z	5 Update Date: 2016-06-25T14:27:44Z
6 Creation Date: 2009-08-14T20:06:37Z	6 Creation Date: 2009-08-14T20:06:37Z
7 Registrar Registration Expiration Date: 2016-07-01T03:59:59Z	7 Registrar Registration Expiration Date: 2017-07-01T03:59:59Z
8 Registrar: GoDaddy.com, LLC	8 Registrar: GoDaddy.com, LLC
9 Registrar IANA ID: 146	9 Registrar IANA ID: 146
10 Registrar Abuse Contact Email: abuse@godaddy.com	10 Registrar Abuse Contact Email: abuse@godaddy.com
11 Registrar Abuse Contact Phone: +1.4906242505	11 Registrar Abuse Contact Phone: +1.4906242505
12 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited	12 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
13 Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited	13 Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
14 Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited	14 Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
15 Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited	15 Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
16 Registry Registrant ID: Not Available From Registry	16 Registry Registrant ID: Not Available From Registry
17 Registrant Name: Trump Orgainsation	17 Registrant Name: Trump Orgainsation
18 Registrant Organisation: Trump Orgainsation	18 Registrant Organisation: Trump Orgainsation
19 Registrant Street: 725 Fifth Avenue	19 Registrant Street: 725 Fifth Avenue
20 Registrant City: New York	20 Registrant City: New York
21 Registrant State/Province: New York	21 Registrant State/Province: New York
22 Registrant Postal Code: 10022	22 Registrant Postal Code: 10022
23 Registrant Country: US	23 Registrant Country: US
24 Registrant Phone: +1.2129322000	24 Registrant Phone: +1.2129322000
25 Registrant Phone Ext:	25 Registrant Phone Ext:
26 Registrant Fax:	26 Registrant Fax:
27 Registrant Fax Ext:	27 Registrant Fax Ext:
28 Registrant Email: emcmullin@cendyn.com	28 Registrant Email: emcmullin@cendyn.com
29 Registry Admin ID: Not Available From Registry	29 Registry Admin ID: Not Available From Registry
30 Admin Name: Emily McMullin	30 Admin Name: Emily McMullin
31 Admin Organisation: Cendyn	31 Admin Organisation: Cendyn
32 Admin Street: 1515 N Federal Highway	32 Admin Street: 1515 N Federal Highway
33 Admin Street: Suite 419	33 Admin Street: Suite 419
34 Admin City: Boca Raton	34 Admin City: Boca Raton
35 Admin State/Province: Florida	35 Admin State/Province: Florida
36 Admin Postal Code: 33432	36 Admin Postal Code: 33432
37 Admin Country: US	37 Admin Country: US
38 Admin Phone: (561) 750-3173	38 Admin Phone: (561) 750-3173
39 Admin Phone Ext:	39 Admin Phone Ext:
40 Admin Fax:	40 Admin Fax:
41 Admin Fax Ext:	41 Admin Fax Ext:
42 Admin Email: ssl.admin@cendyn.com	42 Admin Email: ssl.admin@cendyn.com
43 Registry Tech ID: Not Available From Registry	43 Registry Tech ID: Not Available From Registry
44 Tech Name: Emily McMullin	44 Tech Name: Emily McMullin
45 Tech Organisation: Cendyn	45 Tech Organisation: Cendyn
46 Tech Street: 1515 N. Federal Highway	46 Tech Street: 1515 N. Federal Highway
47 Tech Street: Suite 419	47 Tech Street: Suite 419
48 Tech City: Boca Raton	48 Tech City: Boca Raton
49 Tech State/Province: Florida	49 Tech State/Province: Florida

Figure 6: Screenshot showing historical WHOIS history record for trump-email[.]com¹⁷

The screenshot above shows two (2) side by side WHOIS records for trump-email[.]com, dated 05/03/2016 and 06/29/2016. These dates were chosen because the earlier date is before the alleged “secret” server activity began and the later date was after the alleged activity commenced. The only change showing is an extension of domain ownership for an additional year. This is likely the result of Cendyn extending the domain ownership on behalf of the Trump Organization for another year. As seen in the screenshot below, an ownership change was made on 03/08/2017, which shows that the Trump Organization took full control of the domain.¹⁸

¹⁷<https://research.domaintools.com/research/whois-history/search/?q=trump-email.com>

¹⁸<https://research.domaintools.com/research/whois-history/search/?q=trump-email.com#changes>

2017-03-06	2017-03-08
1 Domain Name: TRUMP-EMAIL.COM	1 Domain Name: TRUMP-EMAIL.COM
2 Registry Domain ID: 1565681491_DOMAIN_COM-VRSN	2 Registry Domain ID: 1565681491_DOMAIN_COM-VRSN
3 Registrar WHOIS Server: whois.godaddy.com	3 Registrar WHOIS Server: whois.godaddy.com
4 Registrar URL: http://www.godaddy.com	4 Registrar URL: http://www.godaddy.com
5 Update Date: 2016-06-29T14:27:44Z	5 Update Date: 2016-06-29T14:27:44Z
6 Creation Date: 2009-09-14T20:06:37Z	6 Creation Date: 2009-09-14T20:06:37Z
7 Registrar Registration Expiration Date: 2017-07-01T02:59:59Z	7 Registrar Registration Expiration Date: 2017-07-01T02:59:59Z
8 Registrar: GoDaddy.com, LLC	8 Registrar: GoDaddy.com, LLC
9 Registrar IANA ID: 146	9 Registrar IANA ID: 146
10 Registrar Abuse Contact Email: abuse@godaddy.com	10 Registrar Abuse Contact Email: abuse@godaddy.com
11 Registrar Abuse Contact Phone: +1.4806242505	11 Registrar Abuse Contact Phone: +1.4806242505
12 Domain Status: clientTransferProhibited http://www.icann.org/epp/clientTransferProhibited	12 Domain Status: clientTransferProhibited http://www.icann.org/epp/clientTransferProhibited
13 Domain Status: clientUpdateProhibited http://www.icann.org/epp/clientUpdateProhibited	13 Domain Status: clientUpdateProhibited http://www.icann.org/epp/clientUpdateProhibited
14 Domain Status: clientRenewProhibited http://www.icann.org/epp/clientRenewProhibited	14 Domain Status: clientRenewProhibited http://www.icann.org/epp/clientRenewProhibited
15 Domain Status: clientDeleteProhibited http://www.icann.org/epp/clientDeleteProhibited	15 Domain Status: clientDeleteProhibited http://www.icann.org/epp/clientDeleteProhibited
16 Registry Registrant ID: Not Available From Registry	16 Registry Registrant ID: Not Available From Registry
17 Registrant Name: Trump Orgainsation	17 Registrant Name: Trump Orgainsation
18 Registrant Organization: Trump Orgainsation	18 Registrant Organization: Trump Orgainsation
19 Registrant Street: 725 Fifth Avenue	19 Registrant Street: 725 Fifth Avenue
20 Registrant City: New York	20 Registrant City: New York
21 Registrant State/Province: New York	21 Registrant State/Province: New York
22 Registrant Postal Code: 10022	22 Registrant Postal Code: 10022
23 Registrant Country: US	23 Registrant Country: US
24 Registrant Phone: +1.2122322000	24 Registrant Phone: +1.2122322000
25 Registrant Phone Ext:	25 Registrant Phone Ext:
26 Registrant Fax:	26 Registrant Fax:
27 Registrant Fax Ext:	27 Registrant Fax Ext:
28 Registrant Email: emcmullin@cendyn.com	28 Registrant Email: generalcounsel@trumporg.com
29 Registry Admin ID: Not Available From Registry	29 Registry Admin ID: Not Available From Registry
30 Admin Name: Emily McMullin	30 Admin Name: The Trump Organisation
31 Admin Organization: Cendyn	31 Admin Organization: The Trump Organisation
32 Admin Street: 1515 N Federal Highway	32 Admin Street: 725 Fifth Avenue
33 Admin Street: Suite 419	33 Admin City: New York
34 Admin City: Boca Raton	34 Admin State/Province: New York
35 Admin State/Province: Florida	35 Admin Postal Code: 10022
36 Admin Postal Code: 33432	
37 Admin Country: US	36 Admin Country: US
38 Admin Phone: (561) 750-3173	37 Admin Phone: +1.2122322000

Figure 7: Screenshot showing trump-email[.]com ownership change

Analysis of both Trump associated domains during the time period that the alleged "secret" servers were communicating with one another shows that both domains utilized Cendyn name servers. This means that any DNS query would ultimately be handled by one of those name servers. Since Cendyn registered these domains and pointed them at Cendyn name servers for resolution requests, only entities with specialized and non-public access to DNS infrastructure would know that Alfa-Bank and Spectrum Health were sending repeated DNS queries to Trump associated domains, making this tactic a very improbable communications channel.

CTAPT performed analysis on the MX and SPF TXT DNS records collected from several passive DNS providers for both trump-email[.]com and contact-client[.]com:

Trump-email[.]com

The following MX DNS records for trump-email[.]com were examined by Ankura:

Source	Mail Servers	Organization	First Seen	Last Seen
Domain Tools	incoming.cdcservices[.]com	Central Dynamics	2015-04-27	2016-09-23
SecurityTrails	incoming.cdcservices[.]com	Central Dynamics	2011-11-14	2016-09-24

These MX DNS records indicate that all incoming emails to the trump-email[.]com domain would be routed to incoming.cdcservices[.]com. According to historical WHOIS records, cdcservices[.]com was registered by Cendyn and used the same Cendyn name servers as trump-email[.]com and contact-client[.]com.

```

Domain Names: CDCSERVICES.COM
Registry Domain ID: 164281674_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2011-08-25T21:24:38Z
Creation Date: 2003-09-29T16:54:15Z
Registrar Registration Expiration Date: 2020-09-29T16:54:15Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.480.242.5855
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Emily McMullin
Registrant Organization: Cendyn
Registrant Street: 1515 North Federal Highway, Suite 419
Registrant City: Boca Raton
Registrant State/Province: Florida
Registrant Postal Code: 33432
Registrant Country: US
Registrant Phone: +1.5617503173
Registrant Phone Ext:
Registrant Fax: +1.5617506795
Registrant Fax Ext:
Registrant Email: ssl.admin@cendyn.com
Registry Admin ID: Not Available From Registry
Admin Name: Emily McMullin
Admin Organization: Cendyn
Admin Street: 1515 North Federal Highway, Suite 419
Admin City: Boca Raton
Admin State/Province: Florida
Admin Postal Code: 33432
Admin Country: US
Admin Phone: +1.5617503173
Admin Phone Ext:
Admin Fax: +1.5617506795
Admin Fax Ext:
Admin Email: ssl.admin@cendyn.com
Registry Tech ID: Not Available From Registry
Tech Name: Emily McMullin
Tech Organization: Cendyn
Tech Street: 1515 North Federal Highway, Suite 419
Tech City: Boca Raton
Tech State/Province: Florida
Tech Postal Code: 33432
Tech Country: US
Tech Phone: +1.5617503173
Tech Phone Ext:
Tech Fax: +1.5617506795
Tech Fax Ext:
Tech Email: ssl.admin@cendyn.com
Name Server: NS1.CDCSERVICES.COM
Name Server: NS2.CDCSERVICES.COM
Name Server: NS3.CDCSERVICES.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
    
```

Figure 8: Screenshot showing historical WHOIS record from DomainTools¹⁹

The MX DNS records show that Cendyn controlled the routing for all inbound emails sent to *.trump-email[.]com. This type of configuration adheres to how a legitimate marketing organization would construct their infrastructure. Essentially, any email sent back to *.trump-email.com would be routed through Cendyn infrastructure.

The following SPF TXT DNS records for trump-email[.]com were examined by Ankura:

¹⁹<https://research.domaintools.com/research/whois-history/search/?q=cdcservices.com>

trump-email.com	TXT	A	1	"v=spf1,ip4:198.91.42.0/23,ip4:64.135.26.0/24,ip4:64.95.241.0/24,ip4:206.191.130.0/24,ip4:63.251.151.0/24,ip4:69.25.15.0/24,mx,-all"	2016-02-11, 01:08	2016-09-23, 13:48
trump-email.com	TXT	A	0	"Internet.Solution.from.Cendyn.com"	2015-12-03, 14:18	2016-01-31, 12:29
trump-email.com	TXT	D	10	"Internet.Solution.from.Cendyn.com"	2014-11-14, 11:17	2016-09-23, 12:59
trump-email.com	TXT	D	10	"v=spf1,ip4:198.91.42.0/23,ip4:64.135.26.0/24,ip4:64.95.241.0/24,ip4:206.191.130.0/24,ip4:63.251.151.0/24,ip4:69.25.15.0/24,mx,-all"	2014-11-14, 11:17	2016-09-23, 12:59

Figure 9: Screenshot showing relevant TXT records extracted from DomainTools²⁰

A SPF TXT record is an email authentication technique that is typically used to mitigate email spoofing by specifying which hostnames, IP addresses, and/or IP ranges are permitted to send emails on behalf of a domain. The SPF TXT record captured in the screenshot above will be broken down below to better understand it.

- "v=spf1"
 - This identifies the TXT record as an SPF string. It also indicates the version of SPF being used.
- "ip4:198.91.42.0/23,ip4:64.135.26.0/24,ip4:64.95.241.0/24,ip4:206.191.130.0/24,ip4:63.251.151.0/24,ip4:69.25.15.0/24"
 - This identifies the IP ranges that are authorized to send emails on behalf of trump-email[.]com. When an email from *.trump-email[.]com is delivered to an email server, that server will retrieve the TXT record from trump-email[.]com to examine the SPF record. If the IP address used to send the email from *.trump-email[.]com is in the SPF record, the email should be tagged as genuine and not SPAM. Analysis of these IP address ranges indicate nothing more than typical marketing activity. A breakdown of ownership for these IP address ranges are below. An evaluation of how these IP addresses are currently being utilized can be found in Appendix A.
- "mx"
 - Any domain that hosts email has at least one MX record. These MX records identify which email servers should be used when relaying email. By including "mx" in the TXT record, the servers identified in the MX DNS record for trump-email[.]com are automatically approved and avoids having to re-list them in the TXT record.
- "~all"
 - This indicates that emails sent from an IP address not included in the SPF record should be accepted by the recipient marked as an SPF failure.

The SPF records demonstrate that for the trump-email[.]com domain, any email sent using the trump-email[.]com domain and originating from one of the IP ranges or MX domains included above are to be considered legitimate by the recipient of the email. However, this SPF configuration also allows for a spoofed email to successfully masquerade as an email from trump-email[.]com. The "~all" flag, also known as a "soft fail"²¹ indicates that if a recipient receives an email from trump-email[.]com but it originates from an IP address not included in the SPF record, the recipient should identify it as spam but allow it at their discretion. This option could allow a marketing organization to keep sending legitimate marketing emails in case of a DNS configuration error. It could also allow an attacker to bypass spam identification and deliver mail into an organization. That email could then have links in the body of the message, that could also force DNS lookups if delivered.

The following IP ranges (Figure 10) were explicitly allocated to Cendyn and/or host Cendyn related domains:

²⁰<https://research.domaintools.com/iris/investigations/463262/search/72fe1f25-d27f-4078-979b-e41c59702f54/7b459b7b-3581-43d6-b2f0-d866198e0d90>

²¹<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing?view=o365-worldwide>

IP Range	Ownership Record	Purpose
198.91.42.0/23	Central Dynamics 980 N Federal Hwy Suite 200 Boca Raton, FL 33432	Cendyn has helped hotels around the world drive marketing and sales for over 20 years. ²²
64.135.26.0/24	BroadbandONE, Inc 3500 NW Boca Raton BLVD Boca Raton, FL 33431	Broadband One is an Internet Service Provider located in Boca Raton, Florida. ²³
64.95.241.0/24	Internap Corporation 50 NE 9 th Street Miami, FL 33030	Internap (INAP) is a publicly traded internet service provider. According to WHOIS records, this net range is allocated to private INAP customers.
206.191.130.0/24	Internap Corporation 50 NE 9 th Street Miami, FL 33030	Internap (INAP) is a publicly traded internet service provider. According to WHOIS records, this net range is allocated to private INAP customers.
63.251.151.0/24	Internap Corporation 50 NE 9 th Street Miami, FL 33030	Internap (INAP) is a publicly traded internet service provider. According to WHOIS records, this net range is allocated to private INAP customers.
69.25.15.0/24	Internap Corporation 50 NE 9 th Street Miami, FL 33030	Internap (INAP) is a publicly traded internet service provider. According to WHOIS records, this net range is allocated to private INAP customers.

Figure 10: Ownership of IP ranges identified in TXT record for trump-email[.]com

Analysis discovered many of the domains pertain to large hotel or hospitality related companies. Please refer to Appendix A for a list of domains found to be associated with the IPs in Figure 10.

Contact-client[.]com

The following MX DNS records for contact-client[.]com were examined by Ankura:

Source	Mail Servers	Organization	First Seen	Last Seen
PassiveTotal	incoming.cdcservices[.]com	Central Dynamics	2011-11-15	2020-02-27
SecurityTrails	incoming.cdcservices[.]com	Central Dynamics	2011-11-14	2017-05-25
SecurityTrails	incoming.cdcservices[.]com	Central Dynamics	2017-05-25	2020-02-27

These MX DNS records indicate that all incoming emails to the contact-client[.]com domain would be routed to incoming.cdcservices[.]com, the same email server that handled incoming emails for trump-email[.]com. This type of configuration adheres to how a legitimate marketing organization would construct their infrastructure. Essentially, any email sent back to *.contact-client.com would be routed through Cendyn infrastructure.

The following is the SPF TXT record for contact-client[.]com:

²²<https://www.cendyn.com/company/>

²³<https://www.linkedin.com/company/broadband-one-inc.>

TXT Values:	First Seen	Last Seen	Duration Seen
v=spf1 include:spf.contact-client.com ~all google-site-verification=6hjrhTYNB12EL88q-Jla9PsvagOMgmLnH4gAEF7FAbs	2017-05-11 (2 years ago)	2020-02-26 (19 hours ago)	2 years
v=spf1 include:spf.contact-client.com ~all google-site-verification=6hjrhTYNB12EL88q-Jla9PsvagOMgmLnH4gAEF7FAbs	2016-06-28 (3 years ago)	2017-05-11 (2 years ago)	10 months
v=spf1 ip4:198.91.42.0/23 ip4:64.135.26.0/24 mx include:listsak.com include:sendgrid.net include:spf.maropost.com ~all google-site-verification=6hjrhTYNB12EL88q-Jla9PsvagOMgmLnH4gAEF7FAbs	2015-11-06 (4 years ago)	2016-06-28 (3 years ago)	7 months

Figure 11: Screenshot showing relevant SPF records for contact-client[.]com extracted from SecurityTrails

The various records are detailed below for clarity:

- "v=spf1"
 - This identifies the TXT record as an SPF string. It also indicates the version of SPF being used.
- "ip4:198.91.42.0/23,ip4:64.135.26.0/24"
 - This identifies the IP ranges that are authorized to send emails on behalf of trump-email[.]com. When an email from *.contact-client[.]com is delivered to an email server, that server will retrieve the TXT record from contact-client[.]com to examine the SPF record. If the IP address used to send the email from *.contact-client[.]com is in the SPF record, the email should be tagged as genuine and not SPAM. Analysis of these IP address ranges indicate nothing more than typical marketing activity. The two IP ranges included in these SPF records overlap with those found in trump-email[.]com SPF record.
- "mx"
 - Any domain that hosts email has at least one MX record. These MX records identify which email servers should be used when relaying email. By including "mx" in the TXT record, the servers identified in the MX DNS record for contact-client[.]com are automatically approved and avoids having to re-list them in the TXT record.
- "include"
 - This includes the SPF record for these domains as valid sending sources. In this particular case, the SPF records for listsak[.]com, sendgrid[.]com, and maropost[.]com are to be included in the SPF record for contact-client[.]com. A breakdown of ownership for these domains is below.
- "~all"
 - This indicates that emails sent from an IP address not included in the SPF record should be accepted by the recipient but marked as an SPF failure.
- "google-site-verification"
 - This identifies that the webmaster has verified ownership with Google.

The SPF records demonstrate that for the contact-client[.]com domain, any email sent using the contact-client[.]com domain and originating from one of the IP ranges or MX domains included above are to be considered legitimate by the recipient of the email. However, this SPF configuration also allows for a spoofed email to be masquerading as contact-client[.]com from an IP address not approved by Cendyn. The "~all" flag, also known as a "soft fail"²⁴, indicates that if a recipient receives an email from contact-client[.]com but it originates from an IP address not included in the SPF record, the recipient should identify it as spam but allow it at their discretion. This option could allow a marketing organization to keep sending legitimate marketing emails in case of a DNS configuration error. It could also allow an attacker to bypass spam identification and deliver mail into an organization. That email could then have links in the body of the message, that could also force DNS lookups if delivered.

²⁴<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing?view=o365-worldwide>

The following is a list of domains that were seen in the “include” section of the SPF record for contact-client[.]com. As explained above, these domains were approved to send emails on behalf of *.contact-client[.]com, to include trump1.contact-client[.]com.

Domain	Ownership	Purpose
Listrak[.]com	Jeff McDonald 529 E. Main Street Lititz, PA 17543	A retail digital marketing automation platform trusted by leading brands for email marketing, mobile messaging, customer insights and cross-channel orchestration.
Sendgrid[.]com	Sendgrid, Inc. 1401 Walnut Street Boulder, CO 80302	Offers automated workflows that leverage automation triggers to set up automated, recurring emails or drip series to customers.
Maropost[.]com	Maropost, Inc. 200 University Avenue Toronto, Ontario	Offers an email marketing platform to create unique experiences for customers. Allows for the segmentation, scheduling, and development of dynamic content based on unified customer data.

Figure 12: Description of domains found in the SPF record for contact-client[.]com

CTAPT’s analysis of the domains included in the table above concluded that all of them appear to be legitimate entities utilized by numerous companies for marketing purposes. It should be noted that Listrak also owns the IP address (66.216.133[.]29) that hosted both mail1.trump-email[.]com and trump1.contact-client[.]com. Figures 11-13 are screenshots copied from these platform websites highlighting Listrak customers:

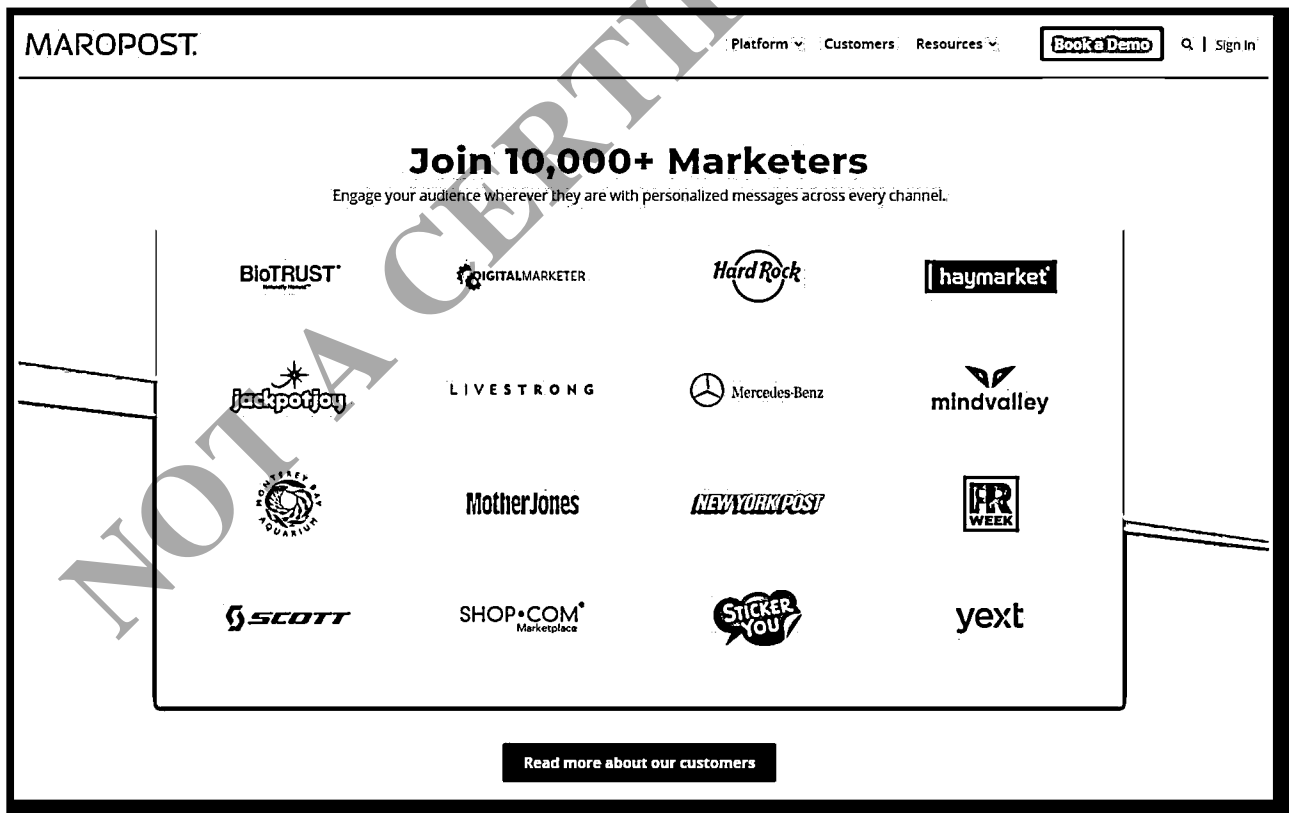


Figure 13: Screenshot from Maropost[.]com

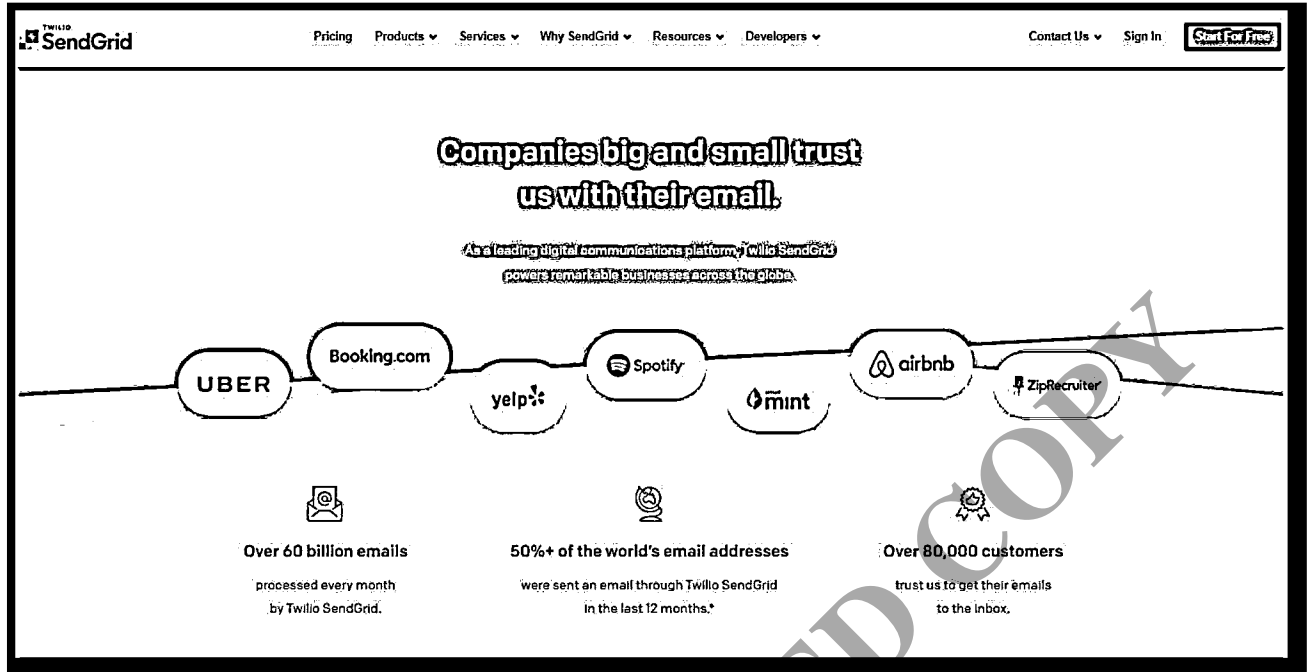


Figure 14: Screenshot from Sendgrid[.]com

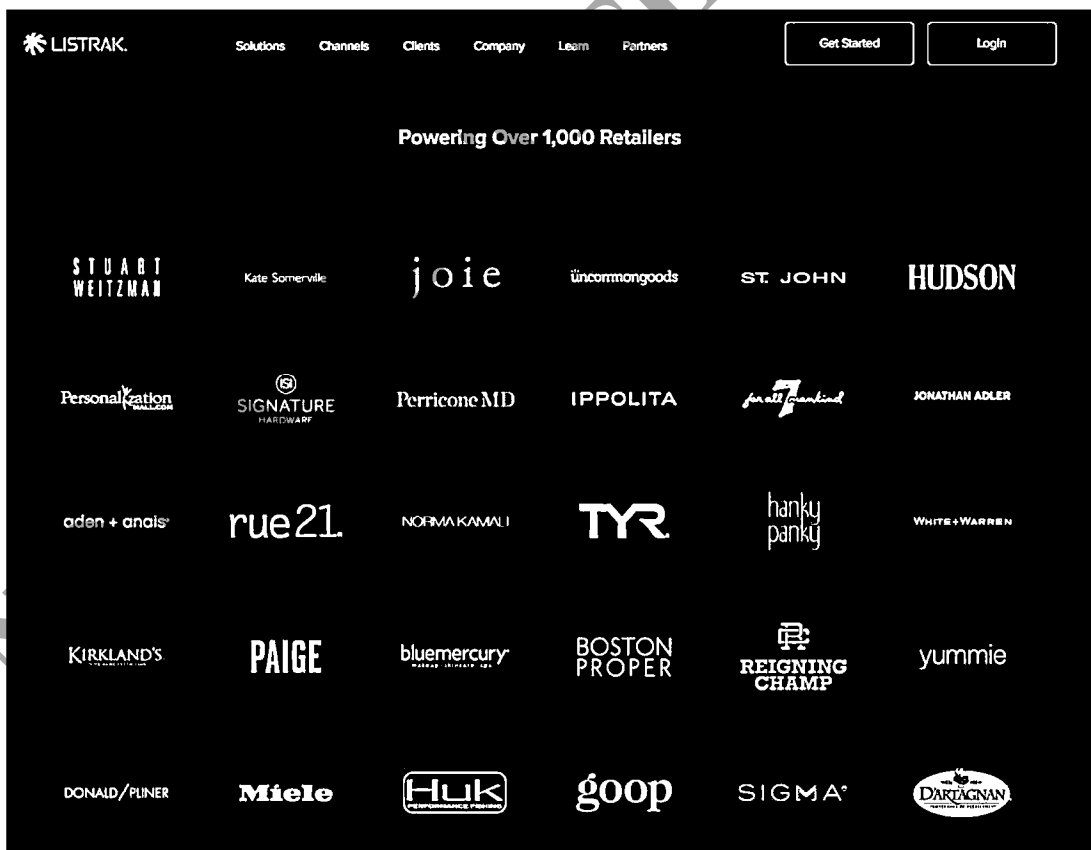


Figure 15: Screenshot from Listrak[.]com

We stress that the analysis performed by CTAPT did not find any support for allegations that either mail1.trump-email[.]com or trump1.contact-client[.]com were ever used as a covert communications channel. Newly identified historical DNS data obtained from SecurityTrails as well as our review of DomainTools and PassiveTotal, clearly strengthen the conclusion that these two domains were used for legitimate marketing purposes beginning as early as 2009.

Moreover, the fact that the SPF records for both domains included "~all" made it possible for malicious actors to have sent crafted SPAM emails, to both Alfa bank and Spectrum Health, spoofing either the mail1.trump-email[.]com or trump1.contact-client[.]com domain as the source. This would likely force the receiving entity's infrastructure to send a DNS record request to Cendyn nameservers to validate that the IP address used to send the email was verified, as per the stored DNS records on the Cendyn servers. These spoofed emails could have been sent at any time.

The passive DNS records specifically challenge the claim made in the New Yorker²⁵ that Alfa-Bank's servers found trump1.contact-client[.]com on September 27, 2016 as "evidence of direct contact between Alfa-Bank and Trump" since the DNS record shows that the DNS process was working as intended; when the mail1.trump-email[.]com did not resolve, the DNS process resolved to trump1.contact-client[.]com, which was assigned the same IP address. There are a number of scenarios that could be responsible for repeated DNS queries in this case, speculation includes the DNS activity could have been caused when Alfa-Bank blocked the IP address at their firewall and/or flagged that IP address as a source of SPAM. Or if a threat actor, also noticing that mail1.trump-email[.]com no longer resolved to an IP address, began sending spoofed emails masquerading as trump1.contact-client[.]com to Alfa-Bank, these spoofed emails would force Alfa-Bank's email servers to request SPF records from contact-client[.]com. Another possible scenario is a threat actor redirected DNS queries for both mail1.trump-email[.]com and trump1.contact-client[.]com through both Alfa-Bank and Spectrum Health DNS servers, to appear as if those DNS queries originated from Alfa-Bank and Spectrum Health and not the actual sender. This is demonstrated in Appendix B.

ROOT CAUSE ANALYSIS

CTAPT analysis of available DNS records identified the following potential causes for Alfa-Bank servers conducting DNS lookups for Trump related domains:

SPAM Email

As mentioned previously, SPF records for both email-trump[.]com and contact-client[.]com included the string "~all". This mechanism allows for spoofed emails received by an entity like Alfa-Bank, to compare validated IP addresses from Cendyn and pass them through, since Cendyn servers were configured to respond with a "Softfail"²⁶ instead of a "Hardfail." This Cendyn configuration forces the recipient of a marketing or spoof email (Alfa-Bank) to request the SPF DNS record for the alleged sending domain, essentially tricking a recipient of an email to perform a DNS query for a domain it never visited or received a legitimate email from.

DNS Forgery

The CTAPT conducted a test that explored the idea that an outside entity could push a DNS request query to Alfa-Bank's DNS servers. Additionally, network traffic validation was achieved by capturing network traffic generated from a test DNS server, to see the activity associated with execution of the DIG command.

²⁵<https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign>

²⁶<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing?view=o365-worldwide>

To conduct the test, CTAPT used an open source tool named “Scapy” used by penetration testers to craft custom packets. Scapy is often used to bypass restrictive firewalls and other security measures to gain access to targeted networks. Using Scapy we crafted packets to manipulate our test server (mimicking Alfa-Bank’s DNS server) to conduct DNS DIG requests for “Ankura.com.” Our testing confirms it is possible to make an externally crafted request to a DNS server belonging to an entity like Alfa-Bank, and then forcing that server to fulfill the request, making it appear as if Alfa-Bank’s server requested it. Please review Appendix B for details.

Although media stories made numerous assumptions about how Alfa-Bank’s DNS servers were configured in 2016, the findings above, the Stroz Friedberg Investigation Summary dated 07/19/2017,²⁷ and our testing, support the view that Alfa-Bank’s systems may have been manipulated into sending the DNS requests noted by Tea Leaves, or others.

CONCLUSION

OBSERVATIONS

CTAPT’s investigation relied on recently identified SecurityTrails DNS records, DomainTools passive DNS databases, and PassiveTotal archives for inquiry into Cendyn, Internap, Listra, and Trump related entities. When considered together, the data affirms that the anonymous researchers who initially raised the covert Cyber connection allegation against the Trump Organization and Alfa-Bank, missed, ignored, or didn't have access to a complete record of DNS history. The multiple sources of DNS records the CTAPT reviewed demonstrate that the server alleged to be secret, was in fact an overt email marketing system. Ankura's analysis does not support either mail1.trump-email[.]com or trump1.contact-client[.]com being used as a covert communications channel. Newly identified historical DNS data obtained from SecurityTrails, as well as our review of DomainTools and PassiveTotal, actually strengthen the conclusion that these two domains were used for marketing purposes beginning as early as 2009 through 2016.

Ankura's analysis doesn't find any support for the allegation of a "secret server" or covert "cyber links" between Alfa-Bank and the Trump Organization and is consistent with the conclusions of the FBI, as reported in the IG's report concerning the FBI's "Crossfire Hurricane" investigation.²⁸ The three sources of DNS records indicate that servers attributed to the Trump Organization were actually owned and operated by a hotel marketing related company named "Central Dynamics" (Cendyn). DNS records show that Cendyn was engaged in legitimate marketing activity for numerous global hotel chains, including Trump Hotels.

CTAPT's detailed review of DNS records demonstrates that the configuration of Cendyn servers may have enabled a threat actor to send spoofed emails or inauthentic DNS queries that could have generated DNS requests to Trump Organization affiliated domains, from Alfa-Bank and Spectrum Health IP addresses.

Additionally, CTAPT's research did not find evidence of open source reporting from the Information Security (INFOSEC) community, either before or after this allegation arose, that would suggest DNS lookup activity as described by the anonymous researchers offers a means for covert or secret communications. The updated passive DNS analysis coupled with the timing of the underlying allegations, suggest that Alfa-Bank servers may have been

²⁷ <http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf>

²⁸ <https://www.justice.gov/storage/120919-examination.pdf>

unwitting sources of the DNS requests at the direction of some entity to create a connection between Alfa-Bank and the Trump Organization. If true, this may constitute a violation of one or more U.S. federal criminal laws.

NOT A CERTIFIED COPY

APPENDIX A

DOMAINS HOSTED ON 198.91.42.0/23

IP Address	Domain	Whois Record URL
198.91.42.175	70parkhotelrewards.com	https://whois.domaintools.com/70parkhotelrewards.com
198.91.42.8	95cordova.com	https://whois.domaintools.com/95cordova.com
198.91.42.56	accorproposal.com	https://whois.domaintools.com/accorproposal.com
198.91.42.25	acehotelandswimclubconcierge.com	https://whois.domaintools.com/acehotelandswimclubconcierge.com
198.91.42.25	acehotellondonconcierge.com	https://whois.domaintools.com/acehotellondonconcierge.com
198.91.42.25	acehotellosangelesconcierge.com	https://whois.domaintools.com/acehotellosangelesconcierge.com
198.91.42.25	acehotelnewyorkconcierge.com	https://whois.domaintools.com/acehotelnewyorkconcierge.com
198.91.42.43	acmehotelcompanychi.com	https://whois.domaintools.com/acmehotelcompanychi.com
198.91.42.25	affiniaconcierge.com	https://whois.domaintools.com/affiniaconcierge.com
198.91.42.26	airliecenteremenus.com	https://whois.domaintools.com/airliecenteremenus.com
198.91.42.30	aloftemenus.com	https://whois.domaintools.com/aloftemenus.com
198.91.42.56	aloftproposal.com	https://whois.domaintools.com/aloftproposal.com
198.91.42.25	americantradedhotelconcierge.com	https://whois.domaintools.com/americantradedhotelconcierge.com
198.91.42.165	amesbostonconcierge.com	https://whois.domaintools.com/amesbostonconcierge.com
198.91.42.43	anantara.info	https://whois.domaintools.com/anantara.info
198.91.42.26	andazemenus.com	https://whois.domaintools.com/andazemenus.com
198.91.42.76	aocmetals.com	https://whois.domaintools.com/aocmetals.com
198.91.42.43	arlohotels.co	https://whois.domaintools.com/arlohotels.co
198.91.42.24	atlantisproposal.com	https://whois.domaintools.com/atlantisproposal.com
198.91.42.43	avanihotels.info	https://whois.domaintools.com/avanihotels.info
198.91.42.56	avtebrochure.com	https://whois.domaintools.com/avtebrochure.com
198.91.42.24	avtproposal.com	https://whois.domaintools.com/avtproposal.com
198.91.42.26	bacaraemenus.com	https://whois.domaintools.com/bacaraemenus.com
198.91.42.26	bayviewcollection.international	https://whois.domaintools.com/bayviewcollection.international
198.91.42.26	bayviewhotels.international	https://whois.domaintools.com/bayviewhotels.international
198.91.42.24	benchmarkproposal.com	https://whois.domaintools.com/benchmarkproposal.com
198.91.42.25	bernarduslodgeconcierge.com	https://whois.domaintools.com/bernarduslodgeconcierge.com
198.91.42.26	bernssalongeremenus.com	https://whois.domaintools.com/bernssalongeremenus.com
198.91.42.3	bestwesternebrochure.com	https://whois.domaintools.com/bestwesternebrochure.com
198.91.42.26	bestwesternemenus.com	https://whois.domaintools.com/bestwesternemenus.com

198.91.42.27	bestwesternplanner.com	https://whois.domaintools.com/bestwesternplanner.com
198.91.42.1	bestwesternnews.com	https://whois.domaintools.com/bestwesternnews.com
198.91.42.26	beverlyheritagehotelemenus.com	https://whois.domaintools.com/beverlyheritagehotelemenus.com
198.91.42.26	beverlyhillshotelemenus.com	https://whois.domaintools.com/beverlyhillshotelemenus.com
198.91.42.24	biltmoreproposal.com	https://whois.domaintools.com/biltmoreproposal.com
198.91.42.26	boarsheadinnemenus.com	https://whois.domaintools.com/boarsheadinnemenus.com
198.91.42.8	bohemianhotelbiltmorevillage.com	https://whois.domaintools.com/bohemianhotelbiltmorevillage.com
198.91.42.26	bonnetcreekemenus.com	https://whois.domaintools.com/bonnetcreekemenus.com
198.91.42.23	bookmeeting.com	https://whois.domaintools.com/bookmeeting.com
198.91.42.25	borgataconcierge.com	https://whois.domaintools.com/borgataconcierge.com
198.91.42.164	brasstownvalleyconcierge.com	https://whois.domaintools.com/brasstownvalleyconcierge.com
198.91.42.26	broadmooremenus.com	https://whois.domaintools.com/broadmooremenus.com
198.91.42.24	broadmoorproposal.com	https://whois.domaintools.com/broadmoorproposal.com
198.91.42.43	brushcreekluxurycollection.com	https://whois.domaintools.com/brushcreekluxurycollection.com
198.91.42.43	brushcreekluxurycollections.com	https://whois.domaintools.com/brushcreekluxurycollections.com
198.91.42.26	buenavistaemenus.com	https://whois.domaintools.com/buenavistaemenus.com
198.91.42.56	bwiproposal.com	https://whois.domaintools.com/bwiproposal.com
198.91.42.24	cafeproposal.com	https://whois.domaintools.com/cafeproposal.com
198.91.42.8	casinoroyalehotel.com	https://whois.domaintools.com/casinoroyalehotel.com
198.91.42.1	cdcservices.com	https://whois.domaintools.com/cdcservices.com
198.91.42.24	celebrationproposal.com	https://whois.domaintools.com/celebrationproposal.com
198.91.42.2	cendyn-econcierge.com	https://whois.domaintools.com/cendyn-econcierge.com
198.91.42.56	cendynaccess.com	https://whois.domaintools.com/cendynaccess.com
198.91.42.3	cendynadvertising.com	https://whois.domaintools.com/cendynadvertising.com
198.91.42.43	cendyncommunity.com	https://whois.domaintools.com/cendyncommunity.com
198.91.42.24	cendynebrochure.com	https://whois.domaintools.com/cendynebrochure.com
198.91.42.1	cendynecard.com	https://whois.domaintools.com/cendynecard.com
198.91.42.20	cendyneconcierge.com	https://whois.domaintools.com/cendyneconcierge.com
198.91.42.56	cendyneproposal.com	https://whois.domaintools.com/cendyneproposal.com
198.91.42.3	cendynesalessuite.com	https://whois.domaintools.com/cendynesalessuite.com
198.91.42.3	cendynhotelqa.com	https://whois.domaintools.com/cendynhotelqa.com
198.91.42.36	cendynsource.com	https://whois.domaintools.com/cendynsource.com
198.91.42.3	cendynvoice.com	https://whois.domaintools.com/cendynvoice.com
198.91.42.26	chateaurrestaurantemenus.com	https://whois.domaintools.com/chateaurrestaurantemenus.com
198.91.42.24	cheecalodgebrochure.com	https://whois.domaintools.com/cheecalodgebrochure.com
198.91.42.158	choctawcasinoconcierge.com	https://whois.domaintools.com/choctawcasinoconcierge.com
198.91.42.2	chrco.ca	https://whois.domaintools.com/chrco.ca
198.91.42.210	chrco.com	https://whois.domaintools.com/chrco.com

198.91.42.156	client-qa-10.com	https://whois.domaintools.com/client-qa-10.com
198.91.42.236	clubproposal.com	https://whois.domaintools.com/clubproposal.com
198.91.42.43	cme-alcronhotel.com	https://whois.domaintools.com/cme-alcronhotel.com
198.91.42.43	cme-revolutionhotel.com	https://whois.domaintools.com/cme-revolutionhotel.com
198.91.42.43	cmte-hotellora.com	https://whois.domaintools.com/cmte-hotellora.com
198.91.42.43	cmte-lorahotel.com	https://whois.domaintools.com/cmte-lorahotel.com
198.91.42.43	cmte-villaroyalehotel.com	https://whois.domaintools.com/cmte-villaroyalehotel.com
198.91.42.43	cmte-woodlarkhotel.com	https://whois.domaintools.com/cmte-woodlarkhotel.com
198.91.42.24	coastproposal.com	https://whois.domaintools.com/coastproposal.com
198.91.42.20	conferenceplanningresources.biz	https://whois.domaintools.com/conferenceplanningresources.biz
198.91.42.20	conferenceplanningresources.info	https://whois.domaintools.com/conferenceplanningresources.info
198.91.42.20	conferenceplanningresources.net	https://whois.domaintools.com/conferenceplanningresources.net
198.91.42.20	conferenceplanningresources.org	https://whois.domaintools.com/conferenceplanningresources.org
198.91.42.26	connecticutconventioncenteremenu.com	https://whois.domaintools.com/connecticutconventioncenteremenu.com
198.91.42.26	conrademenu.com	https://whois.domaintools.com/conrademenu.com
198.91.42.136	conradmenu.com	https://whois.domaintools.com/conradmenu.com
198.91.42.5	coral-hospitality.com	https://whois.domaintools.com/coral-hospitality.com
198.91.42.5	coralbeachhotelsandclubs.com	https://whois.domaintools.com/coralbeachhotelsandclubs.com
198.91.42.5	coralcollection.com	https://whois.domaintools.com/coralcollection.com
198.91.42.5	coralhospitality.com	https://whois.domaintools.com/coralhospitality.com
198.91.42.9	corporatecup.org	https://whois.domaintools.com/corporatecup.org
198.91.42.5	courtyardmarriottpueblo.com	https://whois.domaintools.com/courtyardmarriottpueblo.com
198.91.42.24	coveproposal.com	https://whois.domaintools.com/coveproposal.com
198.91.42.210	crescenthotels.com	https://whois.domaintools.com/crescenthotels.com
198.91.42.1	crescentintranet.com	https://whois.domaintools.com/crescentintranet.com
198.91.42.26	crowneplazaemenu.com	https://whois.domaintools.com/crowneplazaemenu.com
198.91.42.56	crowneplazaproposal.com	https://whois.domaintools.com/crowneplazaproposal.com
198.91.42.26	crowneventsemenu.com	https://whois.domaintools.com/crowneventsemenu.com
198.91.42.43	cte-alcronhotel.com	https://whois.domaintools.com/cte-alcronhotel.com
198.91.42.43	cte-revolutionhotel.com	https://whois.domaintools.com/cte-revolutionhotel.com
198.91.42.26	curioemenu.com	https://whois.domaintools.com/curioemenu.com
198.91.42.43	cwresorts.com	https://whois.domaintools.com/cwresorts.com
198.91.42.24	davidsonproposal.com	https://whois.domaintools.com/davidsonproposal.com
198.91.42.8	delraysands.com	https://whois.domaintools.com/delraysands.com
198.91.42.209	delraysandsresort.com	https://whois.domaintools.com/delraysandsresort.com
198.91.42.24	destinationproposal.com	https://whois.domaintools.com/destinationproposal.com
198.91.42.24	disneyproposal.com	https://whois.domaintools.com/disneyproposal.com

198.91.42.24	dolceproposal.com	https://whois.domaintools.com/dolceproposal.com
198.91.42.26	doralgolfresortemenus.com	https://whois.domaintools.com/doralgolfresortemenus.com
198.91.42.24	dorchestercollectionproposal.com	https://whois.domaintools.com/dorchestercollectionproposal.com
198.91.42.26	doubletreemenus.com	https://whois.domaintools.com/doubletreemenus.com
198.91.42.24	doubletreeproposal.com	https://whois.domaintools.com/doubletreeproposal.com
198.91.42.26	drakehotelenus.com	https://whois.domaintools.com/drakehotelenus.com
198.91.42.24	dtebrochure.com	https://whois.domaintools.com/dtebrochure.com
198.91.42.20	e-confirmations.com	https://whois.domaintools.com/e-confirmations.com
198.91.42.25	eaglemountainhouseconcierge.com	https://whois.domaintools.com/eaglemountainhouseconcierge.com
198.91.42.20	eagleresortandspa.com	https://whois.domaintools.com/eagleresortandspa.com
198.91.42.20	eagleridgeinnresort.com	https://whois.domaintools.com/eagleridgeinnresort.com
198.91.42.20	eagleridgeresortonline.com	https://whois.domaintools.com/eagleridgeresortonline.com
198.91.42.26	eaglewoodresortemenus.com	https://whois.domaintools.com/eaglewoodresortemenus.com
198.91.42.25	eattacheservice.com	https://whois.domaintools.com/eattacheservice.com
198.91.42.26	ectcemenus.com	https://whois.domaintools.com/ectcemenus.com
198.91.42.30	elementemenus.com	https://whois.domaintools.com/elementemenus.com
198.91.42.56	elementproposal.com	https://whois.domaintools.com/elementproposal.com
198.91.42.43	email-hotelmodera.com	https://whois.domaintools.com/email-hotelmodera.com
198.91.42.43	email-montagehotels.com	https://whois.domaintools.com/email-montagehotels.com
198.91.42.43	email-pendryhotels.com	https://whois.domaintools.com/email-pendryhotels.com
198.91.42.43	email-rlhc.com	https://whois.domaintools.com/email-rlhc.com
198.91.42.43	email-sagehotelscollection.com	https://whois.domaintools.com/email-sagehotelscollection.com
198.91.42.26	embassysuitesemenus.com	https://whois.domaintools.com/embassysuitesemenus.com
198.91.42.26	embassysuiteshotelsemenus.com	https://whois.domaintools.com/embassysuiteshotelsemenus.com
198.91.42.136	embassysuitesmenus.com	https://whois.domaintools.com/embassysuitesmenus.com
198.91.42.201	emenusaccess.com	https://whois.domaintools.com/emenusaccess.com
198.91.42.43	encoreatreunion.com	https://whois.domaintools.com/encoreatreunion.com
198.91.42.43	encoreatreunion.info	https://whois.domaintools.com/encoreatreunion.info
198.91.42.19	enrichingthespiritatsandpearl.com	https://whois.domaintools.com/enrichingthespiritatsandpearl.com
198.91.42.81	eplanneraccess.com	https://whois.domaintools.com/eplanneraccess.com
198.91.42.56	eproposalaccess.com	https://whois.domaintools.com/eproposalaccess.com
198.91.42.3	eproposalsupport.com	https://whois.domaintools.com/eproposalsupport.com
198.91.42.163	essexhouseconcierge.com	https://whois.domaintools.com/essexhouseconcierge.com
198.91.42.24	eventeproposal.com	https://whois.domaintools.com/eventeproposal.com
198.91.42.25	exeterinnconcierge.com	https://whois.domaintools.com/exeterinnconcierge.com
198.91.42.43	experience-copamarina.com	https://whois.domaintools.com/experience-copamarina.com
198.91.42.43	experience-hoteljoaquin.com	https://whois.domaintools.com/experience-hoteljoaquin.com
198.91.42.43	experience-studyhotels.com	https://whois.domaintools.com/experience-studyhotels.com

198.91.42.43	experience-theedwinhotel.com	https://whois.domaintools.com/experience-theedwinhotel.com
198.91.42.43	experiencehotelerwin.com	https://whois.domaintools.com/experiencehotelerwin.com
198.91.42.43	experienceinnatperrycabin.com	https://whois.domaintools.com/experienceinnatperrycabin.com
198.91.42.43	explorebrushcreekranh.com	https://whois.domaintools.com/explorebrushcreekranh.com
198.91.42.43	explorebrushcreekranhcollection.com	https://whois.domaintools.com/explorebrushcreekranhcollection.com
198.91.42.43	explorefrenchcreeksportsmensclub.com	https://whois.domaintools.com/explorefrenchcreeksportsmensclub.com
198.91.42.43	exploremageehomestead.com	https://whois.domaintools.com/exploremageehomestead.com
198.91.42.26	fairmontemenu.com	https://whois.domaintools.com/fairmontemenu.com
198.91.42.24	fairmonthotelvancouverebrochure.com	https://whois.domaintools.com/fairmonthotelvancouverebrochure.com
198.91.42.26	fallsviecasinoresortemenu.com	https://whois.domaintools.com/fallsviecasinoresortemenu.com
198.91.42.30	fourpointsemenu.com	https://whois.domaintools.com/fourpointsemenu.com
198.91.42.56	fourpointsproposal.com	https://whois.domaintools.com/fourpointsproposal.com
198.91.42.26	fourseasonsemenu.com	https://whois.domaintools.com/fourseasonsemenu.com
198.91.42.136	fourseasonsmenu.com	https://whois.domaintools.com/fourseasonsmenu.com
198.91.42.20	galenaresort.com	https://whois.domaintools.com/galenaresort.com
198.91.42.77	getfinancebyhilton.com	https://whois.domaintools.com/getfinancebyhilton.com
198.91.42.78	getfinancebyhiltonstaging.com	https://whois.domaintools.com/getfinancebyhiltonstaging.com
198.91.42.26	glencovemansionemenu.com	https://whois.domaintools.com/glencovemansionemenu.com
198.91.42.1	globalgds.com	https://whois.domaintools.com/globalgds.com
198.91.42.1	goard.com	https://whois.domaintools.com/goard.com
198.91.42.43	gohotelvic.com	https://whois.domaintools.com/gohotelvic.com
198.91.42.20	golfgalena.com	https://whois.domaintools.com/golfgalena.com
198.91.42.8	grandbohemiangalleries.com	https://whois.domaintools.com/grandbohemiangalleries.com
198.91.42.24	grandbrochure.com	https://whois.domaintools.com/grandbrochure.com
198.91.42.19	grandlucayanatyourservice.com	https://whois.domaintools.com/grandlucayanatyourservice.com
198.91.42.8	grandthemehotels.com	https://whois.domaintools.com/grandthemehotels.com
198.91.42.3	gravesresidences.com	https://whois.domaintools.com/gravesresidences.com
198.91.42.43	greystonehotelscme.com	https://whois.domaintools.com/greystonehotelscme.com
198.91.42.43	greystonehotelscte.com	https://whois.domaintools.com/greystonehotelscte.com
198.91.42.5	groupmeetingsnyc.com	https://whois.domaintools.com/groupmeetingsnyc.com
198.91.42.5	groupsnyc.com	https://whois.domaintools.com/groupsnyc.com
198.91.42.24	gwrproposal.com	https://whois.domaintools.com/gwrproposal.com
198.91.42.26	hamiltonparkemenu.com	https://whois.domaintools.com/hamiltonparkemenu.com
198.91.42.26	hamptonhotelsemenu.com	https://whois.domaintools.com/hamptonhotelsemenu.com
198.91.42.26	hamptoninnemenu.com	https://whois.domaintools.com/hamptoninnemenu.com
198.91.42.24	hamptoninnproposal.com	https://whois.domaintools.com/hamptoninnproposal.com

198.91.42.24	hardrockcafesproposal.com	https://whois.domaintools.com/hardrockcafesproposal.com
198.91.42.20	hardrockebrochure.com	https://whois.domaintools.com/hardrockebrochure.com
198.91.42.24	hardrockproposal.com	https://whois.domaintools.com/hardrockproposal.com
198.91.42.3	hgimagnificentmileebrochure.com	https://whois.domaintools.com/hgimagnificentmileebrochure.com
198.91.42.189	hhotellosangeles.com	https://whois.domaintools.com/hhotellosangeles.com
198.91.42.211	hi-nyc.com	https://whois.domaintools.com/hi-nyc.com
198.91.42.20	hiltonebrochure.com	https://whois.domaintools.com/hiltonebrochure.com
198.91.42.26	hiltonemenu.com	https://whois.domaintools.com/hiltonemenu.com
198.91.42.26	hiltongardeninnemenu.com	https://whois.domaintools.com/hiltongardeninnemenu.com
198.91.42.136	hiltongardeninnmenu.com	https://whois.domaintools.com/hiltongardeninnmenu.com
198.91.42.24	hiltonproposal.com	https://whois.domaintools.com/hiltonproposal.com
198.91.42.26	hiltonwwemenu.com	https://whois.domaintools.com/hiltonwwemenu.com
198.91.42.26	holidayinnemenu.com	https://whois.domaintools.com/holidayinnemenu.com
198.91.42.24	holidayinnproposal.com	https://whois.domaintools.com/holidayinnproposal.com
198.91.42.5	holidaysatthedel.com	https://whois.domaintools.com/holidaysatthedel.com
198.91.42.26	homewoodsuitesemenu.com	https://whois.domaintools.com/homewoodsuitesemenu.com
198.91.42.25	hooterscasinohotelconcierge.com	https://whois.domaintools.com/hooterscasinohotelconcierge.com
198.91.42.194	hospitalityupgrade.com	https://whois.domaintools.com/hospitalityupgrade.com
198.91.42.26	hotelbelairemenu.com	https://whois.domaintools.com/hotelbelairemenu.com
198.91.42.26	hotelchicagodowntownemenu.com	https://whois.domaintools.com/hotelchicagodowntownemenu.com
198.91.42.24	hotelemployee.com	https://whois.domaintools.com/hotelemployee.com
198.91.42.26	hotelirvinemenu.com	https://whois.domaintools.com/hotelirvinemenu.com
198.91.42.58	hotelmadisonalumni.com	https://whois.domaintools.com/hotelmadisonalumni.com
198.91.42.43	hotelmadisonva.com	https://whois.domaintools.com/hotelmadisonva.com
198.91.42.26	hotelmonteleoneemenu.com	https://whois.domaintools.com/hotelmonteleoneemenu.com
198.91.42.26	hotelnobuibizabay.com	https://whois.domaintools.com/hotelnobuibizabay.com
198.91.42.1	hotelorigami.com	https://whois.domaintools.com/hotelorigami.com
198.91.42.140	hoteltrio.com	https://whois.domaintools.com/hoteltrio.com
198.91.42.141	hotelvicrewards.com	https://whois.domaintools.com/hotelvicrewards.com
198.91.42.162	hotelvikingeconcierge.com	https://whois.domaintools.com/hotelvikingeconcierge.com
198.91.42.24	houseofbluesproposal.com	https://whois.domaintools.com/houseofbluesproposal.com
198.91.42.43	huntleyexclusives.com	https://whois.domaintools.com/huntleyexclusives.com
198.91.42.43	huntleyexperience.com	https://whois.domaintools.com/huntleyexperience.com
198.91.42.26	huntvalleyinnemenu.com	https://whois.domaintools.com/huntvalleyinnemenu.com
198.91.42.167	hutchinsonshores.com	https://whois.domaintools.com/hutchinsonshores.com
198.91.42.2	hyatt.gr	https://whois.domaintools.com/hyatt.gr
198.91.42.2	hyattbrochure.com	https://whois.domaintools.com/hyattbrochure.com
198.91.42.151	hyattcatering.de	https://whois.domaintools.com/hyattcatering.de

198.91.42.154	hyattmenus.com	https://whois.domaintools.com/hyattmenus.com
198.91.42.3	hyattfortheholidays.com	https://whois.domaintools.com/hyattfortheholidays.com
198.91.42.135	hyattmenus.com	https://whois.domaintools.com/hyattmenus.com
198.91.42.24	hyattproposal.com	https://whois.domaintools.com/hyattproposal.com
198.91.42.198	iclocalrewards.com	https://whois.domaintools.com/iclocalrewards.com
198.91.42.24	icproposal.com	https://whois.domaintools.com/icproposal.com
198.91.42.26	ihgemenus.com	https://whois.domaintools.com/ihgemenus.com
198.91.42.26	indigoemenus.com	https://whois.domaintools.com/indigoemenus.com
198.91.42.43	info-hrhguadalajara.com	https://whois.domaintools.com/info-hrhguadalajara.com
198.91.42.43	info-hrhlondon.com	https://whois.domaintools.com/info-hrhlondon.com
198.91.42.43	innatperrycabinreservations.com	https://whois.domaintools.com/innatperrycabinreservations.com
198.91.42.43	islabellabeachresortfl.com	https://whois.domaintools.com/islabellabeachresortfl.com
198.91.42.24	jcresortsproposal.com	https://whois.domaintools.com/jcresortsproposal.com
198.91.42.24	jumeirahproposal.com	https://whois.domaintools.com/jumeirahproposal.com
198.91.42.207	jupiterbeachresort.com	https://whois.domaintools.com/jupiterbeachresort.com
198.91.42.56	kempinskiproposal.com	https://whois.domaintools.com/kempinskiproposal.com
198.91.42.25	kesslerconcierge.com	https://whois.domaintools.com/kesslerconcierge.com
198.91.42.24	kesslerproposal.com	https://whois.domaintools.com/kesslerproposal.com
198.91.42.24	kimptonebrochure.com	https://whois.domaintools.com/kimptonebrochure.com
198.91.42.56	kimptonproposal.com	https://whois.domaintools.com/kimptonproposal.com
198.91.42.25	kittitianhillexperience.com	https://whois.domaintools.com/kittitianhillexperience.com
198.91.42.24	kslproposal.com	https://whois.domaintools.com/kslproposal.com
198.91.42.26	kyotogardenemenus.com	https://whois.domaintools.com/kyotogardenemenus.com
198.91.42.26	kyotograndemenus.com	https://whois.domaintools.com/kyotograndemenus.com
198.91.42.197	lakeplacidlodge.com	https://whois.domaintools.com/lakeplacidlodge.com
198.91.42.24	langhamproposal.com	https://whois.domaintools.com/langhamproposal.com
198.91.42.26	lansingcenteremenus.com	https://whois.domaintools.com/lansingcenteremenus.com
198.91.42.24	laquintaproposal.com	https://whois.domaintools.com/laquintaproposal.com
198.91.42.8	lathamhotelphiladelphia.com	https://whois.domaintools.com/lathamhotelphiladelphia.com
198.91.42.3	latorrettaebrochure.com	https://whois.domaintools.com/latorrettaebrochure.com
198.91.42.26	latorrettalakeresortemenus.com	https://whois.domaintools.com/latorrettalakeresortemenus.com
198.91.42.26	lecrystalhotelemenus.com	https://whois.domaintools.com/lecrystalhotelemenus.com
198.91.42.30	lemeridienemenus.com	https://whois.domaintools.com/lemeridienemenus.com
198.91.42.56	lemeridienproposal.com	https://whois.domaintools.com/lemeridienproposal.com
198.91.42.26	lexingtonhotelsemenus.com	https://whois.domaintools.com/lexingtonhotelsemenus.com
198.91.42.1	lfcdevelopment.com	https://whois.domaintools.com/lfcdevelopment.com
198.91.42.200	lidobeachresort.com	https://whois.domaintools.com/lidobeachresort.com
198.91.42.24	limevenueproposal.com	https://whois.domaintools.com/limevenueproposal.com

198.91.42.24	livenationproposal.com	https://whois.domaintools.com/livenationproposal.com
198.91.42.26	loewsemenus.com	https://whois.domaintools.com/loewsemenus.com
198.91.42.203	longboatkeyclub.com	https://whois.domaintools.com/longboatkeyclub.com
198.91.42.215	longreachhouse.com	https://whois.domaintools.com/longreachhouse.com
198.91.42.134	lostvalleyranch.com	https://whois.domaintools.com/lostvalleyranch.com
198.91.42.26	lowesemenus.com	https://whois.domaintools.com/lowesemenus.com
198.91.42.30	luxurycollectionemenus.com	https://whois.domaintools.com/luxurycollectionemenus.com
198.91.42.56	luxurycollectionproposal.com	https://whois.domaintools.com/luxurycollectionproposal.com
198.91.42.3	lynnfinancialcenter.com	https://whois.domaintools.com/lynnfinancialcenter.com
198.91.42.1	madsearch.com	https://whois.domaintools.com/madsearch.com
198.91.42.43	makemyplaceyourplace.com	https://whois.domaintools.com/makemyplaceyourplace.com
198.91.42.24	mandarinorientalproposal.com	https://whois.domaintools.com/mandarinorientalproposal.com
198.91.42.24	mansionproposal.com	https://whois.domaintools.com/mansionproposal.com
198.91.42.43	margaritavilleres.com	https://whois.domaintools.com/margaritavilleres.com
198.91.42.26	marketingnobuhotelibizabay.com	https://whois.domaintools.com/marketingnobuhotelibizabay.com
198.91.42.24	marriottbrochure.com	https://whois.domaintools.com/marriottbrochure.com
198.91.42.1	marriottcard.com	https://whois.domaintools.com/marriottcard.com
198.91.42.5	marriottmn.com	https://whois.domaintools.com/marriottmn.com
198.91.42.24	marriottproposal.com	https://whois.domaintools.com/marriottproposal.com
198.91.42.26	meadowoodnapavalleyemenus.com	https://whois.domaintools.com/meadowoodnapavalleyemenus.com
198.91.42.26	mebymeliaemenus.com	https://whois.domaintools.com/mebymeliaemenus.com
198.91.42.14	media-client.com	https://whois.domaintools.com/media-client.com
198.91.42.8	meetinglouisville.com	https://whois.domaintools.com/meetinglouisville.com
198.91.42.43	mekongkingdoms.info	https://whois.domaintools.com/mekongkingdoms.info
198.91.42.181	menusaccess.com	https://whois.domaintools.com/menusaccess.com
198.91.42.43	mhm-news.com	https://whois.domaintools.com/mhm-news.com
198.91.42.1	millenniumebrochure.com	https://whois.domaintools.com/millenniumebrochure.com
198.91.42.43	minorhotels.info	https://whois.domaintools.com/minorhotels.info
198.91.42.205	miravalspamonarchbeach.com	https://whois.domaintools.com/miravalspamonarchbeach.com
198.91.42.43	montagereservations.com	https://whois.domaintools.com/montagereservations.com
198.91.42.3	mountainlodgebrochure.com	https://whois.domaintools.com/mountainlodgebrochure.com
198.91.42.216	mrccoconutgrove.com	https://whois.domaintools.com/mrccoconutgrove.com
198.91.42.216	mrchotels.com	https://whois.domaintools.com/mrchotels.com
198.91.42.216	mrcseaport.com	https://whois.domaintools.com/mrcseaport.com
198.91.42.25	myaffiniaconciierge.com	https://whois.domaintools.com/myaffiniaconciierge.com
198.91.42.179	mybreakersstay.com	https://whois.domaintools.com/mybreakersstay.com
198.91.42.25	mybroadmoorconciierge.com	https://whois.domaintools.com/mybroadmoorconciierge.com
198.91.42.43	myhotelvic.com	https://whois.domaintools.com/myhotelvic.com

198.91.42.19	myladeraexperience.com	https://whois.domaintools.com/myladeraexperience.com
198.91.42.43	mymiravalstay.com	https://whois.domaintools.com/mymiravalstay.com
198.91.42.43	myplacehotelsreservations.com	https://whois.domaintools.com/myplacehotelsreservations.com
198.91.42.43	myplacestayrewarded.com	https://whois.domaintools.com/myplacestayrewarded.com
198.91.42.161	myroundhillexperience.com	https://whois.domaintools.com/myroundhillexperience.com
198.91.42.20	myterracewedding.com	https://whois.domaintools.com/myterracewedding.com
198.91.42.43	naladhu.info	https://whois.domaintools.com/naladhu.info
198.91.42.26	newmarketemenusdemo.com	https://whois.domaintools.com/newmarketemenusdemo.com
198.91.42.43	news-belovedhotels.com	https://whois.domaintools.com/news-belovedhotels.com
198.91.42.43	news-excellenceresorts.com	https://whois.domaintools.com/news-excellenceresorts.com
198.91.42.43	news-finestresorts.com	https://whois.domaintools.com/news-finestresorts.com
198.91.42.43	news-theexcellencecollection.com	https://whois.domaintools.com/news-theexcellencecollection.com
198.91.42.43	newstunehotels.com	https://whois.domaintools.com/newstunehotels.com
198.91.42.43	niyama.info	https://whois.domaintools.com/niyama.info
198.91.42.157	noblehouseconcierge.com	https://whois.domaintools.com/noblehouseconcierge.com
198.91.42.24	noblehouseproposal.com	https://whois.domaintools.com/noblehouseproposal.com
198.91.42.172	nyloloyals.com	https://whois.domaintools.com/nyloloyals.com
198.91.42.172	nylomembers.com	https://whois.domaintools.com/nylomembers.com
198.91.42.43	oakshotels.info	https://whois.domaintools.com/oakshotels.info
198.91.42.43	oceansedgehotelkw.com	https://whois.domaintools.com/oceansedgehotelkw.com
198.91.42.43	omnihotels-cme.com	https://whois.domaintools.com/omnihotels-cme.com
198.91.42.43	omnihotels-cte.com	https://whois.domaintools.com/omnihotels-cte.com
198.91.42.26	oneoceanresortemenu.com	https://whois.domaintools.com/oneoceanresortemenu.com
198.91.42.193	opalcollection.com	https://whois.domaintools.com/opalcollection.com
198.91.42.57	opalgrand.com	https://whois.domaintools.com/opalgrand.com
198.91.42.38	ovationsmanagement.com	https://whois.domaintools.com/ovationsmanagement.com
198.91.42.38	ovationsolutions.com	https://whois.domaintools.com/ovationsolutions.com
198.91.42.2	ownkaanapali.com	https://whois.domaintools.com/ownkaanapali.com
198.91.42.24	palaceproposal.com	https://whois.domaintools.com/palaceproposal.com
198.91.42.43	palazzoversace-mail.ae	https://whois.domaintools.com/palazzoversace-mail.ae
198.91.42.26	panpacificseattleemenu.com	https://whois.domaintools.com/panpacificseattleemenu.com
198.91.42.26	parkvistagatlinburgemenu.com	https://whois.domaintools.com/parkvistagatlinburgemenu.com
198.91.42.26	peabodyorlandoemenu.com	https://whois.domaintools.com/peabodyorlandoemenu.com
198.91.42.24	pebblebeachproposal.com	https://whois.domaintools.com/pebblebeachproposal.com
198.91.42.26	pelicangrandbeachresortemenu.com	https://whois.domaintools.com/pelicangrandbeachresortemenu.com
198.91.42.43	pendryreservations.com	https://whois.domaintools.com/pendryreservations.com
198.91.42.26	peppermillemenu.com	https://whois.domaintools.com/peppermillemenu.com

198.91.42.3	pganationalebrochure.com	https://whois.domaintools.com/pganationalebrochure.com
198.91.42.26	pganationalemenus.com	https://whois.domaintools.com/pganationalemenus.com
198.91.42.43	platinumpinkclub.com	https://whois.domaintools.com/platinumpinkclub.com
198.91.42.24	projectionproposal.com	https://whois.domaintools.com/projectionproposal.com
198.91.42.56	proposalaccess.com	https://whois.domaintools.com/proposalaccess.com
198.91.42.55	proposalaccesssandbox.com	https://whois.domaintools.com/proposalaccesssandbox.com
198.91.42.26	radissonbluemenus.com	https://whois.domaintools.com/radissonbluemenus.com
198.91.42.26	radissonblumallofamericamenus.com	https://whois.domaintools.com/radissonblumallofamericamenus.com
198.91.42.26	radissonbluroyalsinkiemenu.com	https://whois.domaintools.com/radissonbluroyalsinkiemenu.com
198.91.42.26	radissonmenus.com	https://whois.domaintools.com/radissonmenus.com
198.91.42.24	radissonproposal.com	https://whois.domaintools.com/radissonproposal.com
198.91.42.24	ramadaebrochure.com	https://whois.domaintools.com/ramadaebrochure.com
198.91.42.26	redlionemenus.com	https://whois.domaintools.com/redlionemenus.com
198.91.42.3	regentpalmsebrochure.com	https://whois.domaintools.com/regentpalmsebrochure.com
198.91.42.48	relaxandenjoyclub.com	https://whois.domaintools.com/relaxandenjoyclub.com
198.91.42.24	renaissanceproposal.com	https://whois.domaintools.com/renaissanceproposal.com
198.91.42.43	res-hrhdesaru.com	https://whois.domaintools.com/res-hrhdesaru.com
198.91.42.43	res-hrhguadalajara.com	https://whois.domaintools.com/res-hrhguadalajara.com
198.91.42.43	res-hrhlondon.com	https://whois.domaintools.com/res-hrhlondon.com
198.91.42.43	reservations-copamarina.com	https://whois.domaintools.com/reservations-copamarina.com
198.91.42.43	reservations-hoteljoaquin.com	https://whois.domaintools.com/reservations-hoteljoaquin.com
198.91.42.43	reservations-hotelmodera.com	https://whois.domaintools.com/reservations-hotelmodera.com
198.91.42.43	reservations-sagehotelscollection.com	https://whois.domaintools.com/reservations-sagehotelscollection.com
198.91.42.1	resortecard.com	https://whois.domaintools.com/resortecard.com
198.91.42.133	revelationconsultancy.com	https://whois.domaintools.com/revelationconsultancy.com
198.91.42.24	reverehotlebrochure.com	https://whois.domaintools.com/reverehotlebrochure.com
198.91.42.160	rockstarhostconciierge.com	https://whois.domaintools.com/rockstarhostconciierge.com
198.91.42.1	roktekservices.com	https://whois.domaintools.com/roktekservices.com
198.91.42.24	rosenproposal.com	https://whois.domaintools.com/rosenproposal.com
198.91.42.56	rosewoodproposal.com	https://whois.domaintools.com/rosewoodproposal.com
198.91.42.172	roundhillselect.com	https://whois.domaintools.com/roundhillselect.com
198.91.42.43	rsvp-belovedhotels.com	https://whois.domaintools.com/rsvp-belovedhotels.com
198.91.42.43	rsvp-excellenceresorts.com	https://whois.domaintools.com/rsvp-excellenceresorts.com
198.91.42.43	rsvp-finestresorts.com	https://whois.domaintools.com/rsvp-finestresorts.com
198.91.42.43	rsvp-theexcellencecollection.com	https://whois.domaintools.com/rsvp-theexcellencecollection.com
198.91.42.186	saddlebrooktennis.com	https://whois.domaintools.com/saddlebrooktennis.com
198.91.42.159	sagamoreconciierge.com	https://whois.domaintools.com/sagamoreconciierge.com

198.91.42.43	sales-hrhdesaru.com	https://whois.domaintools.com/sales-hrhdesaru.com
198.91.42.188	samoset.com	https://whois.domaintools.com/samoset.com
198.91.42.188	samosetresort.com	https://whois.domaintools.com/samosetresort.com
198.91.42.24	sandiaproposal.com	https://whois.domaintools.com/sandiaproposal.com
198.91.42.26	sandioresortandcasinoemenu.com	https://whois.domaintools.com/sandioresortandcasinoemenu.com
198.91.42.25	sandioresortexperience.com	https://whois.domaintools.com/sandioresortexperience.com
198.91.42.24	sanibelproposal.com	https://whois.domaintools.com/sanibelproposal.com
198.91.42.20	santuitinncapecod.com	https://whois.domaintools.com/santuitinncapecod.com
198.91.42.3	seasidebrochure.com	https://whois.domaintools.com/seasidebrochure.com
198.91.42.9	secretharborbeachfrontresort.com	https://whois.domaintools.com/secretharborbeachfrontresort.com
198.91.42.9	secretharborbeachfrontresortusvi.com	https://whois.domaintools.com/secretharborbeachfrontresortusvi.com
198.91.42.9	secretharborbeachresortusvi.com	https://whois.domaintools.com/secretharborbeachresortusvi.com
198.91.42.9	secretharborusvi.com	https://whois.domaintools.com/secretharborusvi.com
198.91.42.9	secretharbourbeachfrontresortusvi.com	https://whois.domaintools.com/secretharbourbeachfrontresortusvi.com
198.91.42.9	secretharbourbeachresortusvi.com	https://whois.domaintools.com/secretharbourbeachresortusvi.com
198.91.42.9	secretharbourbeachresortvi.com	https://whois.domaintools.com/secretharbourbeachresortvi.com
198.91.42.9	secretharbourusvi.com	https://whois.domaintools.com/secretharbourusvi.com
198.91.42.5	sedona-resorts.com	https://whois.domaintools.com/sedona-resorts.com
198.91.42.26	sequelresortsemenus.com	https://whois.domaintools.com/sequelresortsemenus.com
198.91.42.26	shangrilasrasasentosaemenu.com	https://whois.domaintools.com/shangrilasrasasentosaemenu.com
198.91.42.30	sheratonemenu.com	https://whois.domaintools.com/sheratonemenu.com
198.91.42.56	sheratonproposal.com	https://whois.domaintools.com/sheratonproposal.com
198.91.42.24	shirehotelproposal.com	https://whois.domaintools.com/shirehotelproposal.com
198.91.42.26	sonestabayfrontemenu.com	https://whois.domaintools.com/sonestabayfrontemenu.com
198.91.42.26	southseasemenu.com	https://whois.domaintools.com/southseasemenu.com
198.91.42.26	springhillemenu.com	https://whois.domaintools.com/springhillemenu.com
198.91.42.29	standarddowntownlaconciierge.com	https://whois.domaintools.com/standarddowntownlaconciierge.com
198.91.42.29	standardeastvillagenyconciierge.com	https://whois.domaintools.com/standardeastvillagenyconciierge.com
198.91.42.29	standardhighlineconciierge.com	https://whois.domaintools.com/standardhighlineconciierge.com
198.91.42.29	standardhollywoodconciierge.com	https://whois.domaintools.com/standardhollywoodconciierge.com
198.91.42.29	standardmiamibeachconciierge.com	https://whois.domaintools.com/standardmiamibeachconciierge.com
198.91.42.30	starwoodemenu.com	https://whois.domaintools.com/starwoodemenu.com
198.91.42.23	starwoodproposalaccess.com	https://whois.domaintools.com/starwoodproposalaccess.com
198.91.42.20	statability.com	https://whois.domaintools.com/statability.com
198.91.42.26	statlerhotelemenu.com	https://whois.domaintools.com/statlerhotelemenu.com
198.91.42.43	stay-hotelerwin.com	https://whois.domaintools.com/stay-hotelerwin.com

198.91.42.43	stay-rlhc.com	https://whois.domaintools.com/stay-rlhc.com
198.91.42.43	stay-studyhotels.com	https://whois.domaintools.com/stay-studyhotels.com
198.91.42.43	stayatflemings-hotel.com	https://whois.domaintools.com/stayatflemings-hotel.com
198.91.42.43	stayatsavigny-hotel.com	https://whois.domaintools.com/stayatsavigny-hotel.com
198.91.42.43	staybrushcreekranch.com	https://whois.domaintools.com/staybrushcreekranch.com
198.91.42.43	staybrushcreekranchcollection.com	https://whois.domaintools.com/staybrushcreekranchcollection.com
198.91.42.43	stayfrenchcreeksportsmensclub.com	https://whois.domaintools.com/stayfrenchcreeksportsmensclub.com
198.91.42.8	staygaybaltimore.com	https://whois.domaintools.com/staygaybaltimore.com
198.91.42.43	staymageehomestead.com	https://whois.domaintools.com/staymageehomestead.com
198.91.42.43	staytunehotels.com	https://whois.domaintools.com/staytunehotels.com
198.91.42.26	steinlodgeemenu.com	https://whois.domaintools.com/steinlodgeemenu.com
198.91.42.20	stonedriftingspa.com	https://whois.domaintools.com/stonedriftingspa.com
198.91.42.26	stpaulmeetingcenteremenu.com	https://whois.domaintools.com/stpaulmeetingcenteremenu.com
198.91.42.30	stregisemenu.com	https://whois.domaintools.com/stregisemenu.com
198.91.42.56	stregisproposal.com	https://whois.domaintools.com/stregisproposal.com
198.91.42.26	stretisemenu.com	https://whois.domaintools.com/stretisemenu.com
198.91.42.26	sundyhouseemenu.com	https://whois.domaintools.com/sundyhouseemenu.com
198.91.42.26	suninternationalemenu.com	https://whois.domaintools.com/suninternationalemenu.com
198.91.42.176	sunsetkeycottages.com	https://whois.domaintools.com/sunsetkeycottages.com
198.91.42.24	swissotelproposal.com	https://whois.domaintools.com/swissotelproposal.com
198.91.42.26	swissotelsydneymenu.com	https://whois.domaintools.com/swissotelsydneymenu.com
198.91.42.24	tajproposal.com	https://whois.domaintools.com/tajproposal.com
198.91.42.20	terracehotelweddings.com	https://whois.domaintools.com/terracehotelweddings.com
198.91.42.26	thayerhotelatwestpointemenu.com	https://whois.domaintools.com/thayerhotelatwestpointemenu.com
198.91.42.25	thebenjaminconciierge.com	https://whois.domaintools.com/thebenjaminconciierge.com
198.91.42.1	thebluedolphins.com	https://whois.domaintools.com/thebluedolphins.com
198.91.42.26	thebreweryemenu.com	https://whois.domaintools.com/thebreweryemenu.com
198.91.42.166	thebrownpalaceconciierge.com	https://whois.domaintools.com/thebrownpalaceconciierge.com
198.91.42.26	thecharleshotelemenu.com	https://whois.domaintools.com/thecharleshotelemenu.com
198.91.42.26	thecheshireemenu.com	https://whois.domaintools.com/thecheshireemenu.com
198.91.42.43	thedominickhotelsoho.com	https://whois.domaintools.com/thedominickhotelsoho.com
198.91.42.182	theharborsidehotel.com	https://whois.domaintools.com/theharborsidehotel.com
198.91.42.26	thekingedwardhotelemenu.com	https://whois.domaintools.com/thekingedwardhotelemenu.com
198.91.42.43	theparchotelny.com	https://whois.domaintools.com/theparchotelny.com
198.91.42.1	thepurpledolphins.com	https://whois.domaintools.com/thepurpledolphins.com
198.91.42.43	theredburyhotelny.com	https://whois.domaintools.com/theredburyhotelny.com
198.91.42.196	thesagamore.biz	https://whois.domaintools.com/thesagamore.biz
198.91.42.196	thesagamore.com	https://whois.domaintools.com/thesagamore.com

198.91.42.196	thesagamore.net	https://whois.domaintools.com/thesagamore.net
198.91.42.196	thesagamore.org	https://whois.domaintools.com/thesagamore.org
198.91.42.8	thesuitesatbeavercreeklodge.com	https://whois.domaintools.com/thesuitesatbeavercreeklodge.com
198.91.42.183	theweststreethotel.com	https://whois.domaintools.com/theweststreethotel.com
198.91.42.43	tivolihotels.info	https://whois.domaintools.com/tivolihotels.info
198.91.42.26	trubyhiltonemenu.com	https://whois.domaintools.com/trubyhiltonemenu.com
198.91.42.26	trubyhiltoneplanner.com	https://whois.domaintools.com/trubyhiltoneplanner.com
198.91.42.136	trubyhiltonmenu.com	https://whois.domaintools.com/trubyhiltonmenu.com
198.91.42.24	trumpproposal.com	https://whois.domaintools.com/trumpproposal.com
198.91.42.43	turnberryisleinfo.com	https://whois.domaintools.com/turnberryisleinfo.com
198.91.42.43	turnberryislereservations.com	https://whois.domaintools.com/turnberryislereservations.com
198.91.42.173	universalhollywoodevents.com	https://whois.domaintools.com/universalhollywoodevents.com
198.91.42.24	universalproposal.com	https://whois.domaintools.com/universalproposal.com
198.91.42.26	universalstudioshollywoodemenu.com	https://whois.domaintools.com/universalstudioshollywoodemenu.com
198.91.42.26	universityofwashingtonemenu.com	https://whois.domaintools.com/universityofwashingtonemenu.com
198.91.42.8	ushgradventure.com	https://whois.domaintools.com/ushgradventure.com
198.91.42.56	vfcasinoproposal.com	https://whois.domaintools.com/vfcasinoproposal.com
198.91.42.43	visitflemings-hotel.com	https://whois.domaintools.com/visitflemings-hotel.com
198.91.42.43	visitmohonk.com	https://whois.domaintools.com/visitmohonk.com
198.91.42.43	visitsavigny-hotel.com	https://whois.domaintools.com/visitsavigny-hotel.com
198.91.42.26	waldorfastoriaemenu.com	https://whois.domaintools.com/waldorfastoriaemenu.com
198.91.42.30	westinmenu.com	https://whois.domaintools.com/westinmenu.com
198.91.42.3	westinlancanteraebrochure.com	https://whois.domaintools.com/westinlancanteraebrochure.com
198.91.42.56	westinproposal.com	https://whois.domaintools.com/westinproposal.com
198.91.42.3	westintysonsebrochure.com	https://whois.domaintools.com/westintysonsebrochure.com
198.91.42.26	westwardlookemenu.com	https://whois.domaintools.com/westwardlookemenu.com
198.91.42.3	wfortlauderdaleebrochure.com	https://whois.domaintools.com/wfortlauderdaleebrochure.com
198.91.42.30	whotelemenu.com	https://whois.domaintools.com/whotelemenu.com
198.91.42.56	whotelproposal.com	https://whois.domaintools.com/whotelproposal.com
198.91.42.1	wigwamebrochure.com	https://whois.domaintools.com/wigwamebrochure.com
198.91.42.25	windjammerexperience.com	https://whois.domaintools.com/windjammerexperience.com
198.91.42.144	winwestindetox.com	https://whois.domaintools.com/winwestindetox.com
198.91.42.24	wwiequesweddingsebrochure.com	https://whois.domaintools.com/wwiequesweddingsebrochure.com
198.91.42.43	wybostonlakesmail.com	https://whois.domaintools.com/wybostonlakesmail.com
198.91.42.26	wyndhammenu.com	https://whois.domaintools.com/wyndhammenu.com
198.91.42.24	wyndhamproposal.com	https://whois.domaintools.com/wyndhamproposal.com
198.91.42.24	wynnproposal.com	https://whois.domaintools.com/wynnproposal.com

198.91.42.5	yayagroves.com	https://whois.domaintools.com/yayagroves.com
-------------	----------------	---

DOMAINS HOSTED ON 63.251.151.0/24

IP Address	Domain	Whois Record URL
63.251.151.29	casaclaridgeconcierge.com	https://whois.domaintools.com/casaclaridgeconcierge.com
63.251.151.121	cendyn16.com	https://whois.domaintools.com/cendyn16.com
63.251.151.121	cendyn18.com	https://whois.domaintools.com/cendyn18.com
63.251.151.121	cendyn20.com	https://whois.domaintools.com/cendyn20.com
63.251.151.245	cendynproposal.com	https://whois.domaintools.com/cendynproposal.com
63.251.151.231	dolce-meetings.com	https://whois.domaintools.com/dolce-meetings.com
63.251.151.135	dolce-munich-ballhausforum.com	https://whois.domaintools.com/dolce-munich-ballhausforum.com
63.251.151.135	dolceballhausforum.com	https://whois.domaintools.com/dolceballhausforum.com
63.251.151.231	dolceconferencedestinations.com	https://whois.domaintools.com/dolceconferencedestinations.com
63.251.151.231	dolceconferencedestinations.net	https://whois.domaintools.com/dolceconferencedestinations.net
63.251.151.231	dolcegolf.es	https://whois.domaintools.com/dolcegolf.es
63.251.151.231	dolcehotel.de	https://whois.domaintools.com/dolcehotel.de
63.251.151.231	dolcehotel.es	https://whois.domaintools.com/dolcehotel.es
63.251.151.231	dolcehotelmanagement.com	https://whois.domaintools.com/dolcehotelmanagement.com
63.251.151.231	dolceinternational.net	https://whois.domaintools.com/dolceinternational.net
63.251.151.231	dolceinternationalonline.com	https://whois.domaintools.com/dolceinternationalonline.com
63.251.151.231	dolceinternationalonline.net	https://whois.domaintools.com/dolceinternationalonline.net
63.251.151.231	dolceintl.net	https://whois.domaintools.com/dolceintl.net
63.251.151.231	dolcemeeting.es	https://whois.domaintools.com/dolcemeeting.es
63.251.151.231	dolcemeetings.es	https://whois.domaintools.com/dolcemeetings.es
63.251.151.135	dolcemunich-unterschleissheim.com	https://whois.domaintools.com/dolcemunich-unterschleissheim.com
63.251.151.231	dolceonline.com	https://whois.domaintools.com/dolceonline.com
63.251.151.231	dolceonline.net	https://whois.domaintools.com/dolceonline.net
63.251.151.231	dolceresorts.es	https://whois.domaintools.com/dolceresorts.es
63.251.151.231	dolcespa.es	https://whois.domaintools.com/dolcespa.es
63.251.151.231	dolcevacation.es	https://whois.domaintools.com/dolcevacation.es
63.251.151.231	dolcevacation.it	https://whois.domaintools.com/dolcevacation.it
63.251.151.231	dolcevacations.es	https://whois.domaintools.com/dolcevacations.es
63.251.151.231	dolcewedding.es	https://whois.domaintools.com/dolcewedding.es
63.251.151.241	downtown-cc.com	https://whois.domaintools.com/downtown-cc.com

63.251.151.231	e-dolceconferencedestinations.com	https://whois.domaintools.com/e-dolceconferencedestinations.com
63.251.151.231	e-dolceconferencedestinations.net	https://whois.domaintools.com/e-dolceconferencedestinations.net
63.251.151.231	e-dolceinternational.com	https://whois.domaintools.com/e-dolceinternational.com
63.251.151.231	e-dolceinternational.net	https://whois.domaintools.com/e-dolceinternational.net
63.251.151.231	e-dolceintl.com	https://whois.domaintools.com/e-dolceintl.com
63.251.151.229	ecardemployee.com	https://whois.domaintools.com/ecardemployee.com
63.251.151.235	hotelcontessagroups.com	https://whois.domaintools.com/hotelcontessagroups.com
63.251.151.235	hotelcontessameetings.com	https://whois.domaintools.com/hotelcontessameetings.com
63.251.151.50	marriottmenus.com	https://whois.domaintools.com/marriottmenus.com
63.251.151.214	meetwithbedfordsprings.com	https://whois.domaintools.com/meetwithbedfordsprings.com
63.251.151.231	mydolceinternational.com	https://whois.domaintools.com/mydolceinternational.com
63.251.151.231	mydolceinternational.net	https://whois.domaintools.com/mydolceinternational.net
63.251.151.231	mydolceintl.com	https://whois.domaintools.com/mydolceintl.com
63.251.151.123	myproposal.com	https://whois.domaintools.com/myproposal.com
63.251.151.19	solvenhospitality.com	https://whois.domaintools.com/solvenhospitality.com
63.251.151.29	watercolorconciierge.com	https://whois.domaintools.com/watercolorconciierge.com

DOMAINS HOSTED ON 64.135.26.0/24

IP Address	Domain	Whois Record URL
64.135.26.49	acehotelreservations.com	https://whois.domaintools.com/acehotelreservations.com
64.135.26.65	amzak.com	https://whois.domaintools.com/amzak.com
64.135.26.5	arcanéo.com	https://whois.domaintools.com/arcanéo.com
64.135.26.46	bellemontfarm.com	https://whois.domaintools.com/bellemontfarm.com
64.135.26.48	c1awards.com	https://whois.domaintools.com/c1awards.com
64.135.26.3	cendyn-one.com	https://whois.domaintools.com/cendyn-one.com
64.135.26.49	cendyn17.com	https://whois.domaintools.com/cendyn17.com
64.135.26.5	cendynarcanéo.com	https://whois.domaintools.com/cendynarcanéo.com
64.135.26.49	cendynone.com	https://whois.domaintools.com/cendynone.com
64.135.26.5	cendynovations.org	https://whois.domaintools.com/cendynovations.org
64.135.26.15	client-qa.com	https://whois.domaintools.com/client-qa.com
64.135.26.3	clientqa.com	https://whois.domaintools.com/clientqa.com
64.135.26.49	contact-client.com	https://whois.domaintools.com/contact-client.com
64.135.26.49	contact-client2.com	https://whois.domaintools.com/contact-client2.com
64.135.26.56	embassysuiteslax.com	https://whois.domaintools.com/embassysuiteslax.com

64.135.26.49	esurvey-client.com	https://whois.domaintools.com/esurvey-client.com
64.135.26.3	halcyonhotelcherrycreek.com	https://whois.domaintools.com/halcyonhotelcherrycreek.com
64.135.26.14	hyattrsvp.com	https://whois.domaintools.com/hyattrsvp.com
64.135.26.50	kittitianhill.com	https://whois.domaintools.com/kittitianhill.com
64.135.26.52	laxembassy.com	https://whois.domaintools.com/laxembassy.com
64.135.26.56	laxresidenceinn.com	https://whois.domaintools.com/laxresidenceinn.com
64.135.26.56	losangelesresidenceinn.com	https://whois.domaintools.com/losangelesresidenceinn.com
64.135.26.38	lottenypalacemeetings.com	https://whois.domaintools.com/lottenypalacemeetings.com
64.135.26.56	marriottlax.com	https://whois.domaintools.com/marriottlax.com
64.135.26.59	muliabali.com	https://whois.domaintools.com/muliabali.com
64.135.26.59	muliaresort.com	https://whois.domaintools.com/muliaresort.com
64.135.26.59	muliaresortbali.com	https://whois.domaintools.com/muliaresortbali.com
64.135.26.59	muliavillabali.com	https://whois.domaintools.com/muliavillabali.com
64.135.26.59	muliavillasbali.com	https://whois.domaintools.com/muliavillasbali.com
64.135.26.5	ovationstechnologies.com	https://whois.domaintools.com/ovationstechnologies.com
64.135.26.66	paseocaribe.com	https://whois.domaintools.com/paseocaribe.com
64.135.26.49	reservations-client.com	https://whois.domaintools.com/reservations-client.com
64.135.26.56	residenceinnlax.com	https://whois.domaintools.com/residenceinnlax.com
64.135.26.57	saddlebrook.com	https://whois.domaintools.com/saddlebrook.com
64.135.26.58	saddlebrookprep.com	https://whois.domaintools.com/saddlebrookprep.com
64.135.26.59	themulia.com	https://whois.domaintools.com/themulia.com

DOMAINS HOSTED ON 64.95.241.0/34

IP Address	Domain	Whois Record URL
64.95.241.129	cendynhelp.com	https://whois.domaintools.com/cendynhelp.com
64.95.241.120	cendynhotelresort.com	https://whois.domaintools.com/cendynhotelresort.com
64.95.241.129	cendynresortqa.com	https://whois.domaintools.com/cendynresortqa.com
64.95.241.231	feeltheenergyathyatt.com	https://whois.domaintools.com/feeltheenergyathyatt.com
64.95.241.24	fourpointseplanner.com	https://whois.domaintools.com/fourpointseplanner.com
64.95.241.122	glbthyattthreeforfree.com	https://whois.domaintools.com/glbthyattthreeforfree.com
64.95.241.231	hssgrilling.com	https://whois.domaintools.com/hssgrilling.com
64.95.241.231	hyatt24hoursale.com	https://whois.domaintools.com/hyatt24hoursale.com
64.95.241.24	hyatteplanner.com	https://whois.domaintools.com/hyatteplanner.com
64.95.241.131	hyattfall08tv.com	https://whois.domaintools.com/hyattfall08tv.com
64.95.241.131	hyattfall2008.com	https://whois.domaintools.com/hyattfall2008.com
64.95.241.19	hyatthotdates.com	https://whois.domaintools.com/hyatthotdates.com

64.95.241.124	hyattsofsanantonio.com	https://whois.domaintools.com/hyattsofsanantonio.com
64.95.241.231	hybenefits.com	https://whois.domaintools.com/hybenefits.com
64.95.241.24	latorrettalakeresortepanner.com	https://whois.domaintools.com/latorrettalakeresortepanner.com
64.95.241.243	oceanahotelgroup.com	https://whois.domaintools.com/oceanahotelgroup.com
64.95.241.112	residenceinnfernandinabeach.com	https://whois.domaintools.com/residenceinnfernandinabeach.com
64.95.241.147	returntohyatt.com	https://whois.domaintools.com/returntohyatt.com
64.95.241.108	riverterraceinnebrochures.com	https://whois.domaintools.com/riverterraceinnebrochures.com
64.95.241.130	riviera-blackhawk.com	https://whois.domaintools.com/riviera-blackhawk.com
64.95.241.215	spalagunacliffs.com	https://whois.domaintools.com/spalagunacliffs.com

DOMAINS HOSTED ON 69.25.15.0/24

IP Address	Domain	Whois Record URL
69.25.15.114	1tierprocessing.com	https://whois.domaintools.com/1tierprocessing.com
69.25.15.101	4efi.com	https://whois.domaintools.com/4efi.com
69.25.15.100	4npa.com	https://whois.domaintools.com/4npa.com
69.25.15.104	aarmiami.com	https://whois.domaintools.com/aarmiami.com
69.25.15.112	affordableautorepairmiami.com	https://whois.domaintools.com/affordableautorepairmiami.com
69.25.15.113	eliteclient.capital	https://whois.domaintools.com/eliteclient.capital
69.25.15.117	eq.financial	https://whois.domaintools.com/eq.financial
69.25.15.107	equfi.com	https://whois.domaintools.com/equfi.com
69.25.15.20	fibercall.com	https://whois.domaintools.com/fibercall.com
69.25.15.20	i3adc.com	https://whois.domaintools.com/i3adc.com
69.25.15.20	i3computing.com	https://whois.domaintools.com/i3computing.com
69.25.15.20	i3medical.com	https://whois.domaintools.com/i3medical.com
69.25.15.20	i3servers.com	https://whois.domaintools.com/i3servers.com
69.25.15.20	i3soutions.com	https://whois.domaintools.com/i3soutions.com
69.25.15.20	innovativmed.com	https://whois.domaintools.com/innovativmed.com
69.25.15.13	kayecom munications.com	https://whois.domaintools.com/kayecom munications.com
69.25.15.111	nationalprocessingalliance.com	https://whois.domaintools.com/nationalprocessingalliance.com
69.25.15.166	palmbeachhistory.org	https://whois.domaintools.com/palmbeachhistory.org
69.25.15.166	pbhistory.com	https://whois.domaintools.com/pbhistory.com
69.25.15.166	pbhistory.org	https://whois.domaintools.com/pbhistory.org
69.25.15.102	sfeah.com	https://whois.domaintools.com/sfeah.com
69.25.15.122	stfrancisemergencyanimalhospital.com	https://whois.domaintools.com/stfrancisemergencyanimalhospital.com
69.25.15.103	wbaperformance.com	https://whois.domaintools.com/wbaperformance.com

69.25.15.123	wbapro.com	https://whois.domaintools.com/wbapro.com
--------------	------------	---

NOT A CERTIFIED COPY

APPENDIX B**DNS TESTING FOR EXTERNAL QUERY ACTIVITY (DNS FORGERY)**

Ankura conducted a test that explored the idea that an outside party could push a DNS request query to Alfa-Bank's DNS servers. Additionally, we wanted to capture the traffic being generated from a test DNS server, to validate the activity associated with the DIG command being executed.

To synthesize the network environment CTAPT set up a Virtual Private Server (VPS), purchased from Linode. Using best practice, that VPS was setup and configured as a Ubuntu DNS server. A single Virtual Machine (VM) running Kali Linux was also part of the testing process. The VPS was designed to simulate the Alfa's DNS server. While the VM was to simulate an outside third party attempting to push DIG request through the VPS. For testing purposes, Ankura.com was the intended target for all DIG request. Wireshark was also running on both VPS and VM in order to capture and further analyze all traffic data.

CTAPT used a common python module called Scapy. Scapy is frequently used by penetration testers to craft custom packets in order to bypass restrictive firewalls and other security measures to gain access to targeted networks. Using Scapy we forged packets to manipulate our test server (mimicking Alfa-Bank's DNS server) to conduct DNS DIG requests for "Ankura.com." To generate the request, we set the nameserver we're querying, "50.116.57.58", the name we're querying, "Ankura.com", and the type of query, 255 for ANY records or "A" for A records. Then the sr() function sends the request and waits for a response. The commands used:

```
>>> any_dns=IP(dst="50.116.57.58")/UDP()/DNS(rd=1, qdcount=1, qd=DNSQR(qname="ankura.com", qtype=255))
>>> A_dns=IP(dst="50.116.57.58")/UDP()/DNS(rd=1, qd=DNSQR(qname="ankura.com", qtype="A"))
>>> sr(any_dns)
>>> sr(A_dns)
```



```
116 30.532062052 195.181.168.201 → 50.116.57.58 QNS 70 Standard query 0x0000 A ankura.com
117 30.532777878 50.116.57.58 → 195.181.168.201 QNS 226 Standard query response 0x0000 A ankura.com A 216.14.91.98 NS
ns29.domaincontrol.com NS ns30.domaincontrol.com A 97.74.104.15 A 173.201.72.15 AAAA 2603:5:2181::f AAAA 2603:5:2281::f
118 31.225660582 195.181.168.201 → 50.116.57.58 QNS 70 Standard query 0x0000 ANY ankura.com
119 31.225867088 50.116.57.58 → 195.181.168.201 QNS 226 Standard query response 0x0000 ANY ankura.com A 216.14.91.98 NS
S ns30.domaincontrol.com NS ns29.domaincontrol.com A 97.74.104.15 A 173.201.72.15 AAAA 2603:5:2181::f AAAA 2603:5:2281::
f
120 31.749712771 195.181.168.201 → 50.116.57.58 QNS 70 Standard query 0x0000 ANY ankura.com
121 31.749957422 50.116.57.58 → 195.181.168.201 QNS 226 Standard query response 0x0000 ANY ankura.com A 216.14.91.98 NS
S ns30.domaincontrol.com NS ns29.domaincontrol.com A 97.74.104.15 A 173.201.72.15 AAAA 2603:5:2181::f AAAA 2603:5:2281::
f
```

NOT A CERTIFIED COPY

EXHIBIT 3

NOT A CERTIFIED COPY



ALFA-BANK

Investigation Report

November 04, 2016

NOT A CERTIFIED COPY

SECURITY
CONSULTING

CONTENTS

Management Summary	3
Intrusion Timeline	3
Findings	3
Investigation Details	5
Domain Name Service	5
Evidence Provided by <i>The New York Times</i>	5
Relevant Domains and Hosts	6
Investigated Evidence.....	10
Findings	10

NOT A CERTIFIED COPY

MANAGEMENT SUMMARY

Intrusion Timeline

Skadden, Arps, Slate, Meagher & Flom LLP retained Mandiant on behalf of Alfa-Bank to support an investigation into unexplained DNS requests. *The New York Times* approached Alfa-Bank and alleged that Alfa-Bank was maintaining contact with the Trump Organization via the server “mail1.trump-email.com” from their DNS (domain name service) servers. They indicated they had evidence to support that allegation.

The New York Times provided a scan of several pages of what appeared to be passive DNS logs showing DNS requests for the host “mail1.trump-email.com”. This domain was registered to an online marketing platform called “Cendyn”, who promotes hotels owned by the Trump Organization.

The New York Times alleges that these communications were not merely DNS requests, but some form of communication channel between Donald Trump and Alfa-Bank’s DMZ (demilitarized zone) DNS servers. According to Alfa-Bank, *The New York Times* further alleges that Alfa-Bank communicates trading information using the DNS connection mentioned above.

When Mandiant was engaged, a Russian security firm, Group IB, had already drafted a report that outlines the DNS environment in question and “whois” registrations (i.e., information to register a domain name including contact information such as name, email address, mailing address, and more).

Mandiant reviewed the report and initiated a detailed analysis of the DNS logs, email logs, Deep Discovery Inspector (DDI) logs, proxy logs, and email archives in coordination with the Alfa-Bank Team.

Log retention periods for DNS logs were set to 24 hours. Neither Alfa-Bank nor Mandiant could recover historical data beyond that period of time.

Tests were conducted that indicated using the domain in question would spark many DNS requests from different security appliances over the course of two days after mail entry. This was verified by sending a test email containing a test domain name to a specific internal account, and in parallel scanning the DNS and Deep Discovery Inspector logs for that domain name. However, there is no evidence indicating that scenario occurred for the requests between May and September 2016.

Findings

The evidence that *The New York Times* provided is consistent with passive DNS logs. These types of logs are generated when a sensor on the network path between the requestor and the resolving server generate a DNS request. In the case of “mail1.trump-email.com” and “trump1.contact-client.com”, the responsible DNS servers are “ns1.cdcservices.com”, “ns2.cdcservices.com”, and “ns3.cdcservices.com” as depicted in Figure 6. This means that when DNS requests from any computer on the Internet try to resolve the IP address for the domains above, the actual traffic goes to one of the three responsible DNS servers. The DNS servers belong to GoDaddy, a major network hosting provider.

Alfa-Bank has rules in place that only allow outbound traffic on port 25 (mail communication) to their mail servers. This indicated that direct communication on mail ports between Alfa-Bank DNS servers and “mail1.trump-email.com” and “trump1.contact-client.com” would have been blocked by the firewall.

In addition, on September 30, 2016, Alfa-Bank began blocking outgoing traffic to the two domains.

As GoDaddy hosts many more websites and domains, it is not possible for Alfa-Bank to block communication to the three mentioned DNS servers without interfering with normal usage of the Internet for their employees.

NOT A CERTIFIED COPY

INVESTIGATION DETAILS

Domain Name Service

The Domain Name Service (DNS) is defined in “Request for Comment” 1035 (RFC1035).

“The goal of domain names is to provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations.” (RFC1035)

Communication on the Internet is based on numerical IP addresses. As those are hard to remember for humans, the global Domain Name System acts like a phonebook and resolves textual domain names to IP addresses.

Thirteen logical root servers are the main authority for resolution. However, authority for actual domain names is typically delegated to so-called authoritative domain name servers responsible for a top-level domain. Examples of top-level domains (TLD) would include: .gov, .com or .mil.

Those authoritative domain name servers then point at a domain name server responsible for a certain domain, such as “trump-email.com”. The client that attempts to resolve the domain name contacts this domain name server to get the IP address currently assigned to the host delivering services under “trump-email.com”.

There are different types of requests. Two of those are important, in order to understand the technical details in this report:

- » **Type A requests:** Requests to resolve the IP address for a specific domain name
- » **Type MX requests:** Request domain name or IP address of the mail servers responsible to deliver email to all users with @<domain name> addresses.

At this point, the DNS resolution stage, there has not been any communication to the target host. The only communication that has occurred at this stage is communication to the responsible domain name server.

Evidence Provided by *The New York Times*

The New York Times provided Alfa-Bank with 61 pages of what appear to be passive DNS logs indicating requests from two servers in the Autonomous System zone (AS) AS15632 registered to “Alfa-Bank Moscow Russia” as shown in Figure 1.

Announced By		
Origin AS	Announcement	Description
AS15632	217.12.96.0/23	Alfa-Bank Moscow Russia

Figure 1: Details to AS15632

The files that *The New York Times* provided show events between May 4, 2016 and September 21, 2016. Figure 2 shows an example of the log entries provided by *The New York Times*. Every entry contains a timestamp, an IP address of one out of two Alfa-Bank servers, and the hostname mail1.trump-email.com.

There is no information showing the type or the content of the communication. However, “email look-ups” suggest only DNS MX lookups in technical terms.

```
2016-05-04T10:48:06.000Z|217.12.97.15|mail1.trump-email.com
2016-05-06T11:46:32.000Z|217.12.97.15|mail1.trump-email.com
2016-05-06T20:27:30.000Z|217.12.96.15|mail1.trump-email.com
2016-05-10T02:31:32.000Z|217.12.96.15|mail1.trump-email.com
```

Figure 2: Excerpt of Logs Provided by NYT

Relevant Domains and Hosts

This paragraph describes hosts, domain-names, and systems relevant to this investigation.

“trump-email.com”

This is the parent domain for “mail1.trump-email.com” and holds the registrar information. The domain was registered in the name of “Trump Organization” (sic). The administrative contact information is an organization called “Cendyn”, as shown in Figure 3. “Cendyn” is a company offering hospitality marketing. A 2007 news article indicates that “Cendyn has been selected as The Trump Organization’s exclusive interactive marketing agency” (<http://www.prnewswire.com/news-releases/cendyn-is-tapped-for-interactive-marketing-services-by-the-trump-organization-58251682.html>). It is not unusual for marketing companies to register domains in the name of their customers.

After September 22, 2016 the “whois” entry was changed, and reference to Cendyn no longer exists in the registration.

The domain name is still hosted by GoDaddy and was first registered in August 14, 2009, as depicted in Figure 4. The following DNS servers are responsible to resolve resources in the “trump-email” domain.

- » ns1.cdcservices.com
- » ns2.cdcservices.com
- » ns3.cdcservices.com

Those DNS servers host thousands of domain names for different customers.

Domain Name: TRUMP-EMAIL.COM
Registry Domain ID: 1565681481_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: <http://www.godaddy.com>
Update Date: 2016-06-29T14:27:44Z
Creation Date: 2009-08-14T20:06:37Z
Registrar Registration Expiration Date: 2017-07-01T03:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>
Domain Status: clientUpdateProhibited <http://www.icann.org/epp#clientUpdateProhibited>
Domain Status: clientRenewProhibited <http://www.icann.org/epp#clientRenewProhibited>
Domain Status: clientDeleteProhibited <http://www.icann.org/epp#clientDeleteProhibited>
Registry Registrant ID: Not Available From Registry
Registrant Name: Trump Orgainzation
Registrant Organization: Trump Orgainzation
Registrant Street: 725 Fifth Avenue
Registrant City: New York
Registrant State/Province: New York
Registrant Postal Code: 10022
Registrant Country: US
Registrant Phone: +1.2128322000
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: emcmullin@cendyn.com
Registry Admin ID: Not Available From Registry
Admin Name: Emily McMullin
Admin Organization: Cendyn
Admin Street: 1515 N Federal Highway
Admin Street: Suite 419
Admin City: Boca Raton

Figure 3: Whois Data for trump-email.com

Domain Name: TRUMP-EMAIL.COM
Registrar: GODADDY.COM, LLC
Sponsoring Registrar IANA ID: 146
Whois Server: whois.godaddy.com
Referral URL: http://www.godaddy.com
Name Server: NS1.CDCSERVICES.COM
Name Server: NS2.CDCSERVICES.COM
Name Server: NS3.CDCSERVICES.COM
Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>
Status: clientRenewProhibited <https://icann.org/epp#clientRenewProhibited>
Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>
Updated Date: 29-jun-2016
Creation Date: 14-aug-2009
Expiration Date: 01-jul-2017

Figure 4: DNS Servers for trump-email.com

“mail1.trump-email.com”

This is the server shown in the logs provided by *The New York Times*. At the time Mandiant initiated their investigation, none of the three responsible DNS server resolved the domain name “mail1.trump-email.com”. However, Alfa-Bank provided a report done by Group IB that indicated that the “mail1.trump-email.com” previously resolved to the IP address “66.216.133.29”.

“217.12.96.15” and “217.12.97.15”

These IP addresses belong to Linux DNS servers located in Alfa-Bank’s DMZ. At the time Mandiant initiated their investigation, Alfa-Bank’s log retention period was set to 24 hours. Alfa-Bank indicated this was due to normal operations generating a high volume of requests; therefore, physical space for log storage was not economically feasible.

“trump1.contact-client.com”

The FQDN (Fully Qualified Domain Name) “trump1.contact-client.com” was another domain that pointed to the IP 66.216.133.29, which was formerly used by “mail1.trump-email.com”.

Mandiant verified that “trump1.contact-client.com” still resolves to the IP address “66.216.133.29”, as shown in Figure 5.

```
# nslookup trump1.contact-client.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   trump1.contact-client.com
Address: 66.216.133.29
```

Figure 5: Nslookup for trump1.contact-client.com

“contact-client.com”

This is the parent domain for “trump1.contact-client.com”. According to “whois” information, the domain was registered to “Charles Deyo”. “Charles Deyo” was the name of the Cendyn CEO, as depicted in Figure 6. The webpage hosted at “contact-client.com” redirects to the “Cendyn” webpage.

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: CONTACT-CLIENT.COM
Registrar URL: http://www.godaddy.com
Registrant Name: Charles Deyo
Registrant Organization:
Name Server: NS3.CDCSERVICES.COM
Name Server: NS2.CDCSERVICES.COM
Name Server: NS1.CDCSERVICES.COM
DNSSEC: unsigned
```

Figure 6: whois information for contact-client.com

Investigated Evidence

Alfa-Bank provided access to the following evidence on site in Moscow. The files are too large to effectively transfer them electronically.

Type	Retention Period	Notes
DNS logs for 217.12.96.15 and 217.12.97.15	24 hours	DNS logs are now stored in ArcSight and available since October 7, 2016
Mail Server Logs	6 Months	timestamp, source, target, verdict
Proxy Server Logs	6 Months	timestamp, source, target, verdict
Deep Discovery Inspector	6 Months	
Mail archives	12 Months	

Table 1: Logs and Retention Periods

All logs have been analyzed. The analyst searched specifically for the general name “trump” and the IP addresses listed in the “Relevant domains and hosts” section. Furthermore, Mandiant conducted time based proximity analysis on randomly selected days where *The New York Times* logs show events.

Findings

Emails from “contact client.com”

Examining the mail logs indicated that emails from various hosts of the “contact-client.com” domain are incoming. Figure 7 shows an example of the incoming email request from “contact-client.com”. Queries for “trump1.contact-client.com” in the mail logs provided no results.

```
Jul [27/2016] 23:13:31 Spam;BLOKED;66f216f179f229fJ3BICIDUC119HR4T0T14BDJ5SDRH8BB1K1HD8E953eb;contact-client.com;ekaufman@alfabank.com;NoVirusFound
```

Figure 7: Example for Incoming contact-client.com email

Emails from trump-email.com

The mail logs did not show mails from or to trump-email.com addresses in the available timeframes (Figure 8).

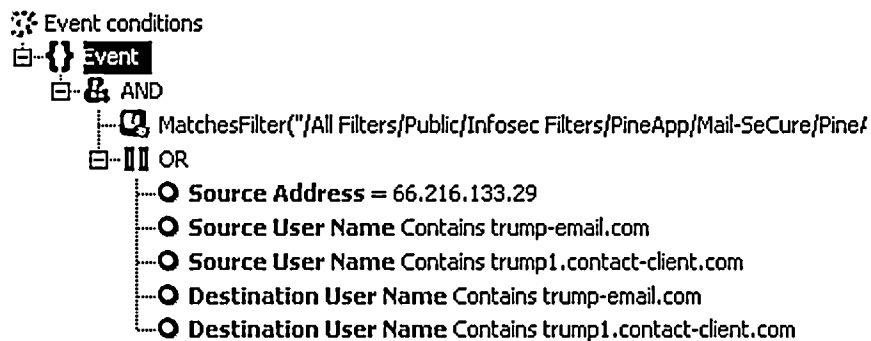


Figure 8: ArcSight Queries for Mail Log

DNS Lookup Peaks Caused by Deep Discovery Inspector

During the investigation, Mandiant, in conjunction with Alfa-Bank, observed that Trend Micro Deep Discovery Inspector resolves all domain names mentioned in email bodies multiple times. This is not only to determine if the domain name itself is flagged malicious, but also to determine if the currently assigned IP address shows up in a blacklist.

Further tests with other domain names indicated that Deep Discovery Inspector would try to resolve the domain name again, irregularly over the course of two days.

To test that, Alfa-Bank added the domain name "dns-servertrump-email.com" to an email message body. The domain "dns-servertrump-email.com" was fictitious. It was an attempt by Alfa-Bank to ensure, that any other source resolving that domain name did not exist on the Alfa-Bank network. This caused 11 automated DNS requests within the first 14 seconds of the mail coming in. In particular, the requests were A and AAAA requests, meaning simple DNS lookups for IPv4 and IPv6 addresses.

The investigation at Alfa-Bank generated mail traffic internally in Alfa-Bank, and between Alfa-bank and their security vendors containing the investigated domain names. These emails automatically lead to the generation of additional DNS requests for those domains originating from Deep Discovery Inspector.

Additional requests were generated by Alfa-Bank when they used "nslookup" to resolve the hosts' IP address for further log file investigations.

trump-email.com Used for Promotion

Mandiant also investigated how the "trump-email.com" domain was used in the past. Figure 9 shows that the domain formerly offered hotel promotion deals for a Trump hotel.

CHECK RATES



Trump International Hotel Las Vegas
 2000 Fashion Show Drive, Las Vegas, NV 89109
 ★★★★★
expired

Deal Analyzer™

from **\$234** **\$295/night - 21% off**

Call for even better deals!
 888-663-5671

GET THIS DEAL

how you save ▼

Details	Description
<p>book by: Aug 12, 2015 travel dates: Through Apr 30, 2011 minimum nights required: 1 source: trump-email.com</p>	<p>This offer includes accommodations plus</p> <ul style="list-style-type: none"> 40-minute muscle soothing massage 40-minute deep cleansing facial pedicure or blow out in the Trump Salon \$10 donation to the American Heart Association gift from the hotel's retail boutique <p><small>Editor's Note: This deal was found via an email promotion and may not be listed on the hotel's regular promotions page.</small></p> <p><small>tags: Casino Unadvertised Spa Charitable Donation This deal was published on trump-email.com with a starting price, which means that rates begin at the price listed but may be higher depending on your dates of travel.</small></p>

Figure 9: Hotel Promotion Using trump-email.com

Related Emails in Mail Archive

Analysis of the Alfa-Bank mail archives indicated three emails with hits for "mail1.trump-email.com domains". Two hits were the same promotion mail to two different users as shown in Figure 10. The third email was a different promotion email and is listed in Figure 11.

Two of the three emails were delivered via the "mail1.trump-email.com" server. The email sender, and links in the mail body, point to contact-client.com.

Inspirational Travel & Exciting Savings



Trump Hotel Collection <TrumpHotelCollection@contact-client.com>
Thursday 4 February 2016 at 17:23
An: smizenin@alfabank.ru

[View this email with images](#)

TRUMP HOTELS™

February 2016

LIVE THE LIFE.

ISSUE 76

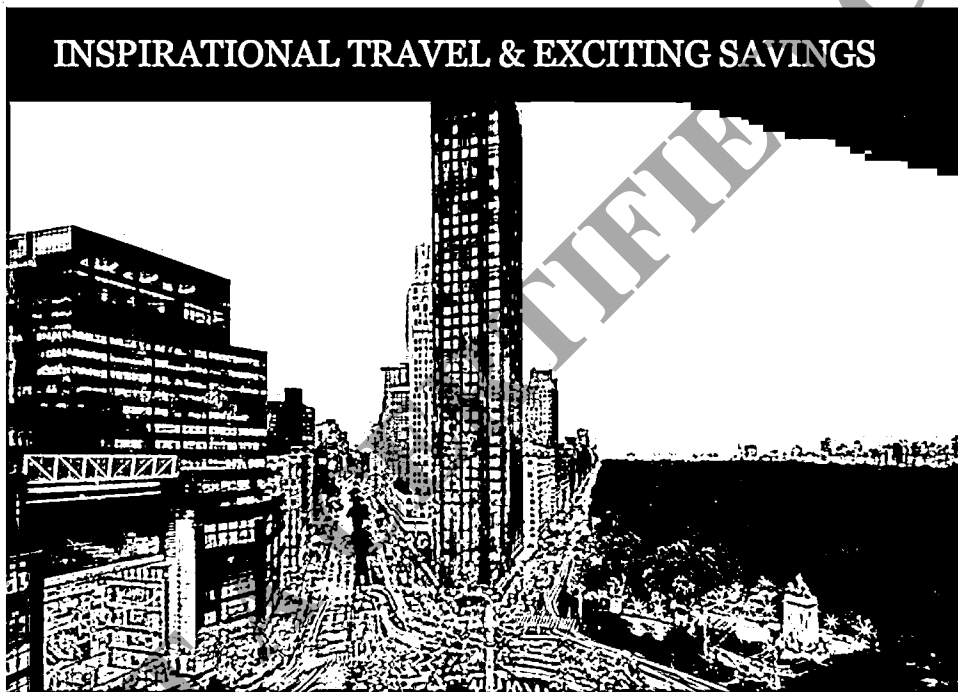


Figure 10: Promotion Mail in Feb. 2016



Trump Hotel Collection <TrumpHotelCollection@contact-client.com>
Thursday 3 December 2015 at 16:43
An: smizenin@alfabank.ru

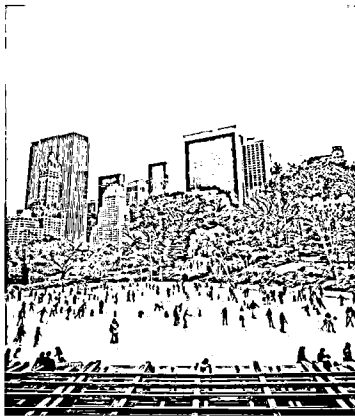
[View this email with Images](#)

**TRUMP
HOTEL
COLLECTION™**

December 2015

LIVE THE LIFE.

ISSUE 74



**YOUR INVITATION
FOR EXHILARATING
TRAVEL THIS WINTER**

This Winter, consider taking advantage of our endless options for an exciting trip. Our destinations in New York, Chicago, Las Vegas, Panama, Toronto, Waikiki, Miami and Ireland are each renowned for their locations, one-of-a-kind experiences, luxurious accommodations and unsurpassed service.



Trump Hotel Collection is proud to be nominated for Travel & Leisure 2016 World's Best Awards. Vote by February 29, 2016 and be entered to

Figure 11: Promotion Mail in Dec. 2015

EXHIBIT 4

NOT A CERTIFIED COPY

More[Create Blog](#) [Sign In](#)

Errata Security

Advanced persistent cybersecurity

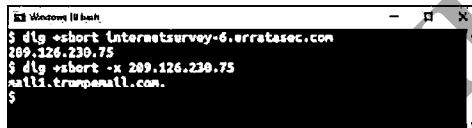
Sunday, March 19, 2017

Pranksters gonna prank

So Alfa Bank (the bank whose DNS traffic link it to trump-email.com) is back in the news with this press release about how in the last month, hackers have spoofed traffic trying to make it look like there's a tie with Trump. In other words, Alfa claims these packets are trying to frame them for a tie with Trump now, and thus (by extension) it must've been a frame last October.

There is no conspiracy here: it's just merry pranksters doing pranks (as this CNN article quotes me).

Indeed, among the people pranking has been me (not the pranks mentioned by Alfa, but different pranks). I ran a scan sending packets from IP address to almost everyone one the Internet, and set the reverse lookup to "mail1.trumpemail.com".



```

Windows [E] bash
$ dig +short Internetsurvey-6.erratasec.com
209.126.230.75
$ dig +short -x 209.126.230.75
mail1.trumpemail.com.
$
  
```

Sadly, my ISP doesn't allow me to put hyphens in the name, so it's not "trump-email.com" as it should be in order to prank well.

Geeks gonna geek and pranksters gonna prank. I can imagine all sorts of other fun pranks somebody might do in order to stir the pot. Since the original news reports of the AlfaBank/trump-email.com connection last year, we have to assume any further data is tainted by goofballs like me goofing off.

By the way, in my particular case, there's a good lesson to be had here about the arbitrariness of IP addresses and names. There is no server located at my IP address of 209.216.230.75. No such machine exists. Instead, I run my scans from a nearby machine on the same network, and "spoof" that address with *masscan*:

```
$ masscan 0.0.0.0/0 -p80 --banners --spoof-ip 209.216.230.75
```

This sends a web request to every machine on the Internet from that IP address, despite no machine anywhere being configured with that IP address.

I point this out because people are confused by the meaning of an "IP address", or a "server", "domain", and "domain name". I can imagine the FBI looking into this and getting a FISA warrant for the server located at my IP address, and my ISP coming back and telling them that no such server exists, nor has a server existed at that IP

Errata Security On Twitter

Robert Graham
(@ErrataRob)

David Maynor
(@Dave_Maynor)

Popular Posts

You are committing a crime right now
Are you reading this blog? If so, you are committing a crime under 18 USC 1030(a) (better known as the "Computer Fraud & ...



How The Intercept Outed Reality Winner

Today, The Intercept released documents on election tampering from an NSA leaker. Later, the arrest warrant request for an NSA contractor ...

SideJacking with Hamster

NOTE: you can download the program at <http://www.erratasec.com/sidejacking.zip> ; make sure to read the instructions. Others have done a be...



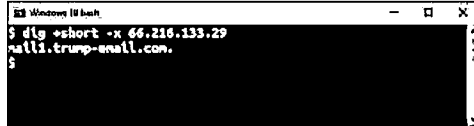
Extracting the SuperFish certificate

I extracted the certificate from the SuperFish adware and cracked the password ("komodia ") that encrypted it. I discuss how dow...

That NBC story 100% fraudulent
Yesterday (Feb 5 2014)
On February 4th, NBC News ran a story

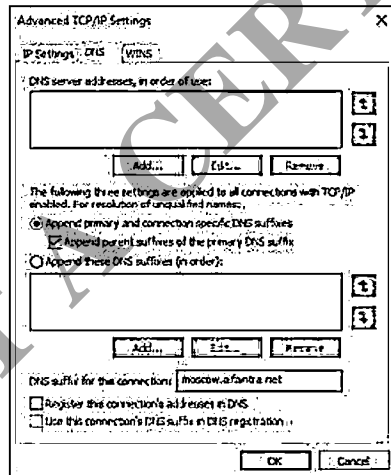
address for many years.

In the case of last years story, there's little reason to believe IP spoofing was happening, but the conspiracy theory still breaks down for the same reason: the association between these concepts is not what you think it is. Listrak, the owner of the server at the center of the conspiracy, still reverse resolves the IP address 66.216.133.29 as "mail1.trump-email.com", either because they are lazy, or because they enjoy the lulz.



It's absurd thinking anything sent by the server is related to the Trump Organization today, and it's equally plausible that nothing the server sent was related to Trump last year as well, especially since (as CNN reports), Trump had severed their ties with Cendyn (the marketing company that uses Listrak servers for email).

Also, as mentioned in a previous blog post, I set my home network's domain to be "moscow.alfaintra.net", which means that some of my DNS lookups at home are actually being sent to Alfa Bank. I should probably turn this off before the FBI comes knocking at my door.



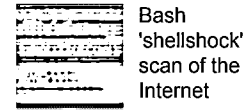
Tweet
Share26

By Robert Graham

Labels: Alfa Bank, Russia, Trump, Trump Organization

2 comments:

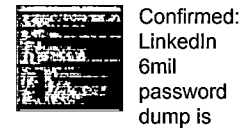
claiming that if you bring your mobile phone or laptop to the Sochi Olympics...



Bash 'shellshock' scan of the Internet
NOTE:
malware is now using this as their User-agent. I haven't run a scan now for over two days. I'm running a scan right now ...

Bash 'shellshock' bug is wormable
Early results from my scan: there's about 3000 systems vulnerable just on port 80, just on the root "/" URL, without Host fiel...

Some notes about HTTP/3
HTTP/3 is going to be standardized. As an old protocol guy, I thought I'd write up some comments. Google (pbuh) has both the most popu...



Confirmed: LinkedIn 6mil password dump is real
Today's news is that 6 million LinkedIn password hashes were dumped to the Internet. I can confirm this hack is real: the password I use...

Notes on the Ashley-Madison dump
Ashley-Madison is a massive dating site that claims 40 million users. The site is specifically for those who want to cheat on their spouse. ...

Blog Archive

March 2017 (9)

-

-

Anonymous said...

Two comments:

(1) EVAN MCMULLIN is the rogue CIA agent behind the Russian-Trump Towers mythology.

Emily McMullin was originally the trump-email.com Registrant with an email address emily@cendyn.com.

It has since been scrubbed, but here is someone's earlier screenshot that still shows cendyn but now shows removed@cendyn:
<http://emptylighthouse.com/who-tea-leaves-what-trump-emailcom-who-cedyn-528639029>

Now have a "way back" look at before any of it got scrubbed:
<https://web.archive.org/web/20170306183141/http://www.whois.com/whois/trump-email.com>

(2) How funny, my name is Robert David Graham too!

5:27 AM



Unknown said...

Great post. Check my website on hindi stories at [afsaana](#) . Thanks!

3:41 AM

Post a Comment

Links to this post

Create a Link

[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

EXHIBIT 5

NOT A CERTIFIED COPY

A REPORTER AT LARGE OCTOBER 15, 2018 ISSUE

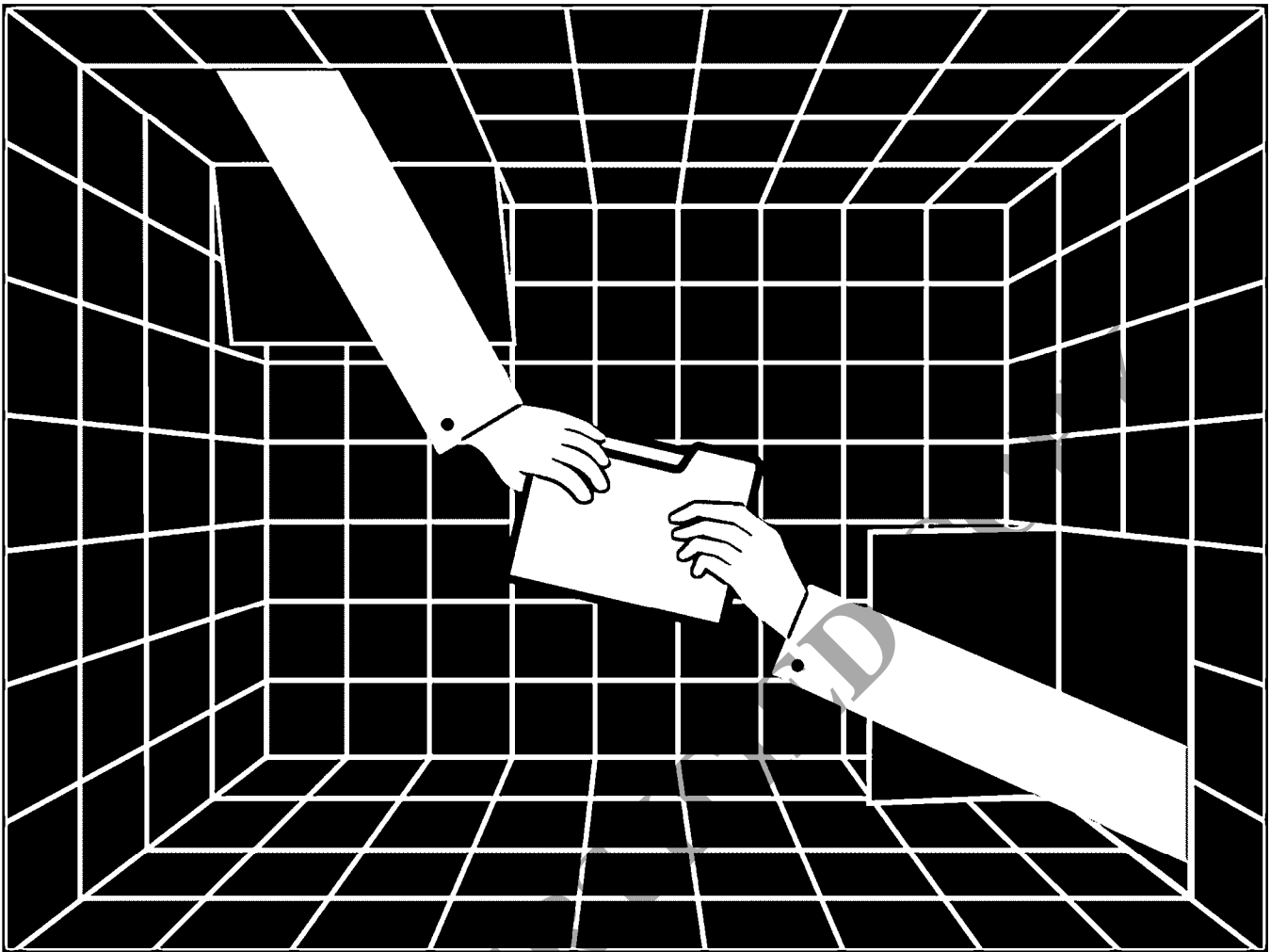
Was There a Connection Between a Russian Bank and the Trump Campaign?

A team of computer scientists sifted through records of unusual Web traffic in search of answers.

By Dexter Filkins

October 8, 2018

NOT A CERTIFIED COPY



A set of cryptic data has inspired a years-long argument over its meaning. Illustration by Jarek Waszul

In June, 2016, after news broke that the Democratic National Committee had been hacked, a group of prominent computer scientists went on alert. Reports said that the infiltrators were probably Russian, which suggested to most members of the group that one of the country's intelligence agencies had been involved. They speculated that if the Russians were hacking the Democrats they must be hacking the Republicans, too. "We

thought there was no way in the world the Russians would just attack the Democrats,” one of the computer scientists, who asked to be identified only as Max, told me.

The group was small—a handful of scientists, scattered across the country—and politically diverse. (Max described himself as “a John McCain Republican.”) Its members sometimes worked with law enforcement or for private clients, but mostly they acted as self-appointed guardians of the Internet, trying to thwart hackers and to keep the system clean of malware—software that hackers use to control a computer remotely, or to extract data. “People think the Internet runs on its own,” Max told me. “It doesn’t. We do this to keep the Internet safe.” The hack of the D.N.C. seemed like a pernicious attack on the integrity of the Web, as well as on the American political system. The scientists decided to investigate whether any Republicans had been hacked, too. “We were trying to protect them,” Max said.

Max’s group began combing the Domain Name System, a worldwide network that acts as a sort of phone book for the Internet, translating easy-to-remember domain names into I.P. addresses, the strings of numbers that computers use to identify one another. Whenever someone goes online—to send an e-mail, to visit a Web site—her device contacts the Domain Name System to locate the computer that it is trying to connect with. Each query, known as a D.N.S. lookup, can be logged, leaving records in a constellation of servers that extends through private companies, public institutions, and universities. Max and his group are part of a community that has unusual access to these records, which are especially useful to cybersecurity experts who work to protect clients from attacks.

Max and the other computer scientists asked me to withhold their names, out of concern for their privacy and their security. I met with Max and his lawyer repeatedly, and interviewed other prominent computer experts. (Among them were Jean Camp, of Indiana University; Steven Bellovin, of Columbia University; Daniel Kahn Gillmor, of the A.C.L.U.; Richard Clayton, of the University of Cambridge; Matt Blaze, of the University of Pennsylvania; and Paul Vixie, of Farsight Security.) Several of them independently

reviewed the records that Max's group had discovered and confirmed that they would be difficult to fake. A senior aide on Capitol Hill, who works in national security, said that Max's research is widely respected among experts in computer science and cybersecurity.

As Max and his colleagues searched D.N.S. logs for domains associated with Republican candidates, they were perplexed by what they encountered. "We went looking for fingerprints similar to what was on the D.N.C. computers, but we didn't find what we were looking for," Max told me. "We found something totally different—something unique." In the small town of Lititz, Pennsylvania, a domain linked to the Trump Organization (mail1.trump-email.com) seemed to be behaving in a peculiar way. The server that housed the domain belonged to a company called Listrak, which mostly helped deliver mass-marketing e-mails: blasts of messages advertising spa treatments, Las Vegas weekends, and other enticements. Some Trump Organization domains sent mass e-mail blasts, but the one that Max and his colleagues spotted appeared not to be sending anything. At the same time, though, a very small group of companies seemed to be trying to communicate with it.

Examining records for the Trump domain, Max's group discovered D.N.S. lookups from a pair of servers owned by Alfa Bank, one of the largest banks in Russia. Alfa Bank's computers were looking up the address of the Trump server nearly every day. There were dozens of lookups on some days and far fewer on others, but the total number was notable: between May and September, Alfa Bank looked up the Trump Organization's domain more than two thousand times. "We were watching this happen in real time—it was like watching an airplane fly by," Max said. "And we thought, Why the hell is a Russian bank communicating with a server that belongs to the Trump Organization, and at such a rate?"

Only one other entity seemed to be reaching out to the Trump Organization's domain with any frequency: Spectrum Health, of Grand Rapids, Michigan. Spectrum Health is closely linked to the DeVos family; Richard DeVos, Jr., is the chairman of the board, and one of its hospitals is named after his mother. His wife, Betsy DeVos, was appointed Secretary of Education by Donald Trump. Her brother, Erik Prince, is a Trump associate who has

attracted the scrutiny of Robert Mueller, the special counsel investigating Trump's ties to Russia. Mueller has been looking into Prince's meeting, following the election, with a Russian official in the Seychelles, at which he reportedly discussed setting up a back channel between Trump and the Russian President, Vladimir Putin. (Prince maintains that the meeting was "incidental.") In the summer of 2016, Max and the others weren't aware of any of this. "We didn't know who DeVos was," Max said.

The D.N.S. records raised vexing questions. Why was the Trump Organization's domain, set up to send mass-marketing e-mails, conducting such meagre activity? And why were computers at Alfa Bank and Spectrum Health trying to reach a server that didn't seem to be doing anything? After analyzing the data, Max said, "We decided this was a covert communication channel."

The Trump Organization, Alfa Bank, and Spectrum Health have repeatedly denied any contact. But the question of whether Max's conclusion was correct remains enormously consequential. Was this evidence of an illicit connection between Russia and the Trump campaign? Or was it merely a coincidence, cyber trash, that fed suspicions in a dark time?

In August, 2016, Max decided to reveal the data that he and his colleagues had assembled. "If the covert communications were real, this potential threat to our country needed to be known before the election," he said. After some discussion, he and his lawyer decided to hand over the findings to Eric Lichtblau, of the *Times*. Lichtblau met with Max, and began to look at the data.

Lichtblau had done breakthrough reporting on National Security Agency surveillance, and he knew that Max's findings would require sophisticated analysis. D.N.S. lookups are metadata—records that indicate computer interactions but don't necessarily demonstrate human communication. Lichtblau shared the data with three leading computer scientists, and, like Max, they were struck by the unusual traffic on the server. As Lichtblau talked to experts, he became increasingly convinced that the data suggested a substantive connection.

“Not only is there clearly something there but there’s clearly something that someone has gone to great lengths to conceal,” he told me. Jean Camp, of Indiana University, had also vetted some of the data. “These people who should not be communicating are clearly communicating,” she said. In order to encourage discussion among analysts, Camp posted a portion of the raw data on her Web site.

As Lichtblau wrote a draft of an article for the *Times*, Max’s lawyer contacted the F.B.I. to alert agents that a story about Trump would be running in a national publication, and to pass along the data. A few days later, an F.B.I. official called Lichtblau and asked him to come to the Bureau’s headquarters, in Washington, D.C.

At the meeting, in late September, 2016, a roomful of officials told Lichtblau that they were looking into potential Russian interference in the election. According to a source who was briefed on the investigation, the Bureau had intelligence from informants suggesting a possible connection between the Trump Organization and Russian banks, but no data. The information from Max’s group could be a significant advance. “The F.B.I. was looking for people in the United States who were helping Russia to influence the election,” the source said. “It was very important to the Bureau. It was urgent.”

The F.B.I. officials asked Lichtblau to delay publishing his story, saying that releasing the news could jeopardize their investigation. As the story sat, Dean Baquet, the *Times*’ executive editor, decided that it would not suffice to report the existence of computer contacts without knowing their purpose. Lichtblau disagreed, arguing that his story contained important news: that the F.B.I. had opened a counterintelligence investigation into Russian contacts with Trump’s aides. “It was a really tense debate,” Baquet told me. “If I were the reporter, I would have wanted to run it, too. It felt like there was something there.” But, with the election looming, Baquet thought that he could not publish the story without being more confident in its conclusions.

Over time, the F.B.I.'s interest in the possibility of an Alfa Bank connection seemed to wane. An agency official told Lichtblau that there could be an innocuous explanation for the computer traffic. Then, on October 30th, Senate Minority Leader Harry Reid wrote a letter to James Comey, the director of the F.B.I., charging that the Bureau was withholding information about "close ties and coordination" between the Trump campaign and Russia. "We had a window," Lichtblau said. His story about Alfa Bank ran the next day. But it bore only a modest resemblance to what he had filed. The headline— "INVESTIGATING DONALD TRUMP, F.B.I. SEES NO CLEAR LINK TO RUSSIA"—seemed to exonerate the Trump campaign. And, though the article mentioned the server, it omitted any reference to the computer scientists who had told Lichtblau that the Trump Organization and Alfa Bank might have been communicating. "We were saying that the investigation was basically over—and it was just beginning," Lichtblau told me.

That same day, Slate ran a story, by Franklin Foer, that made a detailed case for the possibility of a covert link between Alfa Bank and Trump. Foer's report was based largely on information from a colleague of Max's who called himself Tea Leaves. Foer quoted several outside experts; most said that there appeared to be no other plausible explanation for the data.

One remarkable aspect of Foer's story involved the way that the Trump domain had stopped working. On September 21st, he wrote, the *Times* had delivered potential evidence of communications to B.G.R., a Washington lobbying firm that worked for Alfa Bank. Two days later, the Trump domain vanished from the Internet. (Technically, its "A record," which translates the domain name to an I.P. address, was deleted. If the D.N.S. is a phone book, the domain name was effectively decoupled from its number.) For four days, the servers at Alfa Bank kept trying to look up the Trump domain. Then, ten minutes after the last attempt, one of them looked up another domain, which had been configured to lead to the same Trump Organization server.

Max's group was surprised. The Trump domain had been shut down after the *Times* contacted Alfa Bank's representatives—but before the newspaper contacted Trump. “That shows a human interaction,” Max concluded. “Certain actions leave fingerprints.” He reasoned that someone representing Alfa Bank had alerted the Trump Organization, which shut down the domain, set up another one, and then informed Alfa Bank of the new address.

A week after the *Times* story appeared, Trump won the election. On Inauguration Day, Liz Spayd, the *Times*' ombudsman, published a column criticizing the paper's handling of stories related to Trump and Russia, including the Alfa Bank connection. “The Times was too timid in its decisions not to publish the material it had,” she wrote. Spayd's article did not sit well with Baquet. “It was a bad column,” he told the *Washington Post*. Spayd argued that Slate had acted correctly by publishing a more aggressive story, which Baquet dismissed as a “fairly ridiculous conclusion.” That June, Spayd's job was eliminated, as the paper's publisher said that the position of ombudsman had become outdated in the digital age. When I talked to Baquet recently, he still felt that he had been right to resist discussing the server in greater depth, but he acknowledged that the *Times* had been too quick to disclaim the possibility of Trump's connections to Russia. “The story was written too knowingly,” he said. “The headline was flawed. We didn't know then what we know now.”

In April, 2017, Lichtblau left the *Times*, after fifteen years—in part, he said, because of the way that the Alfa Bank story was handled. He went to work for CNN, but resigned less than two months later, amid controversy over another story that he had worked on, about the Trump aide Anthony Scaramucci. This April, Lichtblau returned to the *Times* newsroom for a celebration: he had been part of a team of *Times* reporters that was awarded a Pulitzer Prize for its work on other aspects of the Trump campaign. “It was quite a year,” he said.

Meanwhile, the Trump-Alfa Bank story seemed to fade. The Trump campaign dismissed any connection, saying, “The only covert server is the one Hillary Clinton recklessly

established in her basement.” Bloggers and tech journalists assailed the Slate piece online. The cybersecurity researcher Robert Graham called the analysis “nonsense,” and complained, “This is why we can’t have nice things on the Internet.” He pointed out several problems. For instance, Foer’s sources had found that the Trump domain was blocking incoming e-mail, and argued that this was evidence that Trump and Alfa Bank were maintaining a private communications network; in fact, Listrak routinely configured its marketing servers to send e-mail but not to receive it. Graham also noted that the domain was administered not by Trump but by Cendyn, a company in Boca Raton that handled his company’s marketing e-mail.

Alfa Bank hired two cybersecurity firms, Mandiant and Stroz Friedberg, to review the data. Both firms reported that they had found no evidence of communications with the Trump Organization. The bank also began trying to uncover the anonymous sources in the Slate piece. Attorneys representing Alfa contacted Jean Camp, telling her that they were considering legal action and asking her to identify the researchers who had assembled the data. She declined to reveal their names. “This is what tenure is for,” she told me.

Alfa Bank was founded by Mikhail Fridman, in the last years of the Soviet Union. Fridman was born in western Ukraine and studied metallurgy in college. Like many others of his generation, he was introduced to the market economy through hustle. He sold theatre tickets, washed windows, and ran a student discothèque. After the Soviet Union collapsed, in 1991, Fridman joined the scramble to befriend members of the new government and amass a fortune with help from the state. Along with an economist named Petr Aven, who had previously served as the country’s minister for foreign economic relations, Fridman built Alfa Bank into one of the most successful businesses in the new Russia. Its parent company, Alfa Group, now controls the country’s largest private bank, along with financial institutions in several European nations.

Fridman and Aven acquired reputations as brilliant, relentless businessmen. Describing the lawless post-Soviet years to the journalist Chrystia Freeland, who is now the foreign

minister of Canada, Fridman said, “We were absolute savages.” In a notorious episode in 2008, a group of Russian companies, including Alfa Group, tried to gain control of a joint venture they’d formed with British Petroleum. The power struggle was so fierce that the C.E.O. of the joint venture, Robert Dudley, felt compelled to leave Russia. The oligarchs kept pushing for control of the BP venture until it was sold to a state-owned petroleum company, for fifty-five billion dollars; Alfa Group’s cut was almost fourteen billion.

Alfa Bank prospered during the Yeltsin years and has continued to do so under Putin.

Though Fridman and Aven are not part of Putin’s innermost circle, they have managed to avoid the fate of some other oligarchs, who have had assets seized and, in a few cases, been imprisoned, after falling out of favor. Michael McFaul, a former U.S. Ambassador to Russia, told me he was impressed that Fridman and Aven had “navigated the very difficult world of maintaining their private business interests and not crossing the Kremlin.”

One reason the server story alarmed Alfa Bank was that it threatened the bank’s standing in Washington. Members of Russia’s government and many of its businessmen have been under American economic sanctions since 2014, when Russia annexed Crimea, but Alfa’s principals and representatives have enjoyed access to U.S. politicians at the highest levels. Fridman and Aven met several times with officials at the Obama White House, discussing such issues as Russia’s effort to gain entrance to the World Trade Organization. (Alfa Bank maintains that it has “never advocated for political or trade issues on behalf of the Russian government.”) “Fridman and Aven were seen as people that Washington could talk to about U.S.-Russia, because they checked two boxes—they were ‘polite company’ oligarchs, and they could shed light on Putin’s intentions and perspective,” a senior official in the Obama Administration told me. “They got meetings at State and on the Hill and at the White House. And they were understood to be operating with the consent and guidance of Vladimir Putin.”

Alfa is still closely tied to the Russian system, but Fridman and Aven live much of the time in the United Kingdom. If there was a communications link with the Trump Organization,

it might have been created without their knowledge. According to experts I spoke to, large Russian companies typically have a member of the intelligence services, either active or retired, working at a senior level. If a company's services are required in some way, the officer—called a *kurator*—coördinates them. “A company couldn't say no,” a Washington-based Russia expert told me. (When asked about this, an Alfa Bank spokesperson said, “To our knowledge there are no senior intelligence officials at senior levels at Alfa Bank.”)

This past May, I saw Petr Aven in New York, at the Four Seasons Hotel. He had just come from a dinner in Washington, at which he had met a group of prominent Americans, including officials from the White House, to discuss Russia's economic situation. Aven seemed worried about surveillance; before we sat down, he brought his phone to the other side of the lobby and hid it behind a plant. He wouldn't say much for the record, but he told me that his bank didn't have “any connection at all with Trump—nothing.”

Aven and Fridman have visited Washington less often since Trump took office. But Trump's victory appeared to elevate Alfa Bank's connections there—at least by association. Don McGahn, the White House counsel, came from Jones Day, one of the law firms that represent Alfa Bank in the United States. McGahn brought five Jones Day lawyers with him into the White House; six more were appointed to senior posts in the Administration. Jones Day has done work for businesses belonging to a long list of Russian oligarchs, including Oleg Deripaska, Viktor Vekselberg, and Alexander Mashkevich. The firm has also represented the Trump campaign in its dealings with Robert Mueller. For this reason, McGahn secured an ethics waiver that allows him to talk to his old firm when its clients have business before the U.S. government.

In June, 2017, Trump nominated Brian Benczkowski, a lawyer who had overseen the Stroz Friedberg report for Alfa Bank, to lead the criminal division of the Justice Department. At his confirmation hearing, Benczkowski said emphatically that Stroz Friedberg, like Mandiant, had rejected the possibility of complicity. The investigation, he said, found that “there was no communications link between the Trump Organization and Alfa Bank.”

Democratic senators expressed concern that Benczkowski had taken on work for Alfa Bank; he had been a senior member of Trump's transition team and had good reason to expect that he would be appointed to a job in the Administration. "The client was a Russian bank that is under suspicion of having a direct connection with the Trump campaign," Senator Richard Durbin said, during the hearing.

He and the other Democratic senators were especially troubled that Benczkowski would not commit to recusing himself from dealing with Mueller's investigation, even though he had worked for two of Russia's leading oligarchs. "Why did you refuse to recuse yourself?" Senator Dianne Feinstein asked.

"I don't know what's in Special Prosecutor Mueller's investigation," Benczkowski said. "I'm a lawyer in private practice. I have no idea what he's up to, other than what I read in the papers."

Despite these questions, the Republican-led committee approved Benczkowski. This past July, the Senate confirmed him.

While Republicans in Congress have rejected the possibility of collusion, with some joining Trump in calling the Mueller inquiry a politically motivated "witch hunt," a few Democrats have continued to pursue the matter. After Trump's Inauguration, two Democratic senators who had reviewed the data assembled by Max's group—Mark Warner and a colleague who requested anonymity—asked the F.B.I. for an assessment of any potential contacts between Alfa Bank and the Trump Organization. The material was also brought to the attention of the C.I.A., which found it substantial enough to suggest that the F.B.I. investigate. In March, 2017, a Pennsylvania news outlet called Lancaster Online reported that F.B.I. agents had visited the offices of Listrak, the company that housed the Trump server. Ross Kramer, Listrak's C.E.O., told me, "I gave them everything they asked for."

Around the same time, the second Democratic senator approached a former Senate staffer named Daniel Jones and asked him to give the data a closer look. Jones had served as a counterterrorism investigator for the F.B.I. and then spent ten years working for the Senate Intelligence Committee, where he led the inquiry into the use of torture under the George W. Bush Administration. Now he was running an investigations firm, the Penn Quarter Group, and a nonprofit initiative called the Democracy Integrity Project, which was intended to help keep elections free from foreign interference.

To assess the Alfa Bank data, Jones assembled a team of computer scientists, divided into two groups, one on each coast. (They also consulted with Jean Camp, who agreed to cooperate despite the possibility that Alfa Bank might take legal action.) All these experts have national reputations in the field. Some have held senior cybersecurity jobs in the Pentagon, the White House, and the intelligence services, as well as in leading American technology companies. In order to encourage an unbiased outcome, Jones never introduced the East Coast group to the West Coast group.

I met several times with the two members of the East Coast group and spoke with them repeatedly. They used pseudonyms, Paul and Leto, in part because they had been alarmed by encounters with Russia while they were working at high levels of government. Leto said that, in 2016, as he was investigating cyber intrusions that seemed to originate in Russia, he became convinced that he was being followed. Both he and Paul believed that their phones had been hacked. These incursions coincided with a period of intense Russian activity in the U.S., including the hacking of the D.N.C., a pro-Trump social-media blitz, and the arrival of Maria Butina, who is accused of being a Russian agent sent to ingratiate herself with American conservative leaders. (Butina has denied the accusations.)

As Paul and Leto began working, they needed to verify that Max's data presented an accurate picture of the traffic. After the Slate story appeared, skeptics pointed out that no one has a comprehensive view of the Domain Name System. They speculated that other entities, besides Alfa Bank and Spectrum Health, had looked up the Trump domain, and

that Max had failed to see them. The D.N.S. company Dyn told a reporter that it had seen lookups from other computers around the world. But Dyn turned out to have registered only two additional lookups, both from the same address in the Netherlands.

Max and his colleagues maintain that they are able to see nearly all the D.N.S. lookups on a given domain; the senior Capitol Hill aide I spoke to affirmed that Max's group is widely understood to have this capability. Paul Vixie, one of the original architects of the D.N.S. network, examined the data and told me, "If this is a forgery, it's better than any forgery I've seen." Jones's team also ran analyses and real-time tests to check Max's access to D.N.S. records. "It's completely implausible that he could have fooled us," Paul said.

Max had provided the Jones team with thirty-seven million D.N.S. records, enough to fill thousands of screens with time stamps and I.P. addresses—long strings of numbers and letters in green type. Over the course of several months, Paul and Leto examined the data for patterns and anomalies. "We stared at a lot of green screens," Paul said. They regarded their inquiry as a statistical enterprise, capturing each Alfa Bank D.N.S. query from the ocean of data that they had been given and plotting it over a four-month period. Both said that they began their work as skeptics. "I started from an assumption that this is a bunch of nonsense," Leto told me.

Much of the information that was publicly available might well have supported that assumption. Foer's article in Slate had prompted online discussions, in which commentators offered explanations ranging from the benign to the sinister. The timing of the lookups, which came in the summer just before the election, invited speculation. Foer claimed that the biggest flurries of traffic coincided with major campaign events, including the party conventions. Paul and Leto were dubious. If anything, the traffic coincided with Paul Manafort's time as Trump's campaign manager—but the D.N.S. queries continued after Manafort stepped down. "A lot of people are seeing faces in clouds," Leto said.

The Trump Organization had done little to clarify the matter. In October, 2016, it released a statement denying interactions with Alfa Bank “or any Russian entity.” Instead, it offered a peculiar explanation for the D.N.S. traffic: it had been triggered when “an existing banking customer of Cendyn”—the marketing firm—had used the company’s systems to send communications to Alfa Bank. Such a scenario would be highly irregular; it was as if Gmail had allowed a user to send e-mail from another user’s account. “It makes no sense,” Paul told me.

Trump’s advocates claimed that the investigations sponsored by Alfa Bank had proved that Alfa and the Trump Organization were not communicating. In fact, they sidestepped the question. Mandiant, one of the cybersecurity firms, said that it was unable to inspect the bank’s D.N.S. logs from 2016, because Alfa retained such records for only twenty-four hours. The other firm, Stroz Friedberg, gave the same explanation for why it, too, was “unable to verify” the data.

As Jones’s team vetted the data, they examined various possible explanations. One was malware, which had played a role in the hack of the D.N.C.’s computers. Most malware has “distinctive patterns of behavior,” Camp told me. It is typically sent out in a blast, aimed simultaneously at multiple domains. There is a “payload”—a mechanism that activates the malicious activity—and a “recruitment mechanism,” which enables the malware to take over parts of a vulnerable computer. None of the experts whom Jones assembled found any evidence of this behavior on the Trump server. “Malware doesn’t keep banging on the door like that,” Paul said.

A second possibility was marketing e-mail. After the Slate article appeared, some commentators suggested that Trump’s server had innocently sent promotional e-mails to Alfa Bank, and that a computer there had responded with queries designed to verify the identity of the sender. This became a catchall answer for anyone who couldn’t explain what had happened. “Either this is something innocuous, like spam,” Rachel Cohen, a press secretary for Senator Warner, told me, “or it’s completely nefarious.”

Alfa Bank had received Trump marketing e-mails in the past. But Cendyn had told CNN that it stopped sending e-mails for the Trump Organization in March, 2016, before the peculiar activity began; Trump had transferred his online marketing to another company, called Serenata. Jones's team investigated, and found additional evidence that the server wasn't sending marketing e-mails at the time. One indicator was the unusually limited traffic. Kramer, of Listrak, told me that a typical client sends "tens of thousands of e-mails a day" to huge numbers of recipients. If the Trump server was following that pattern, it would have generated significant D.N.S. traffic. To establish a kind of control group, Jones's team asked Max to capture the D.N.S. logs for the Denihan Hospitality Group—a hotel chain, similar in size to Trump's, which was using Cendyn and Listrak to send marketing e-mails. In a sample spanning August and September, 2016, a Denihan domain received more than twenty thousand D.N.S. queries, from more than a thousand I.P. addresses. In the same period, the Trump domain had twenty-five hundred lookups, nearly all of them from Alfa Bank and Spectrum Health.

The timing and the frequency of the D.N.S. lookups also did not suggest spam, Paul and Leto believed. Mass-marketing e-mails are typically sent by an automated process, one after another, in an unbroken rhythm. The Alfa queries seemed to fall into two categories. Some came in a steady pulse, while others arrived irregularly—sometimes many in a day, sometimes a few. "The timing of the communication was not random, and it wasn't regular-periodic," Paul said. "It was a better match for human activity."

But, if the Trump server wasn't sending or receiving e-mail, what could explain the traffic? There was the possibility of "spoofing"—essentially, faking an identity. Did someone try to make it appear, falsely, that Alfa Bank was reaching out to the Trump Organization? Jones's team concluded that such an attack would have been unlikely to produce thousands of D.N.S. lookups, over such a long time. "Maybe for a few days, but not four months," Leto said. There was also a question of motive. In the spring of 2016, very few people knew that Max and his colleagues were able to monitor D.N.S. traffic so comprehensively, so any

spoofers would have been impersonating Alfa Bank with little expectation of being detected. News stories investigating the links between Trump and Russia were months away. “Why would someone do that?” Steven Bellovin, of Columbia, said. “And why would they pick those organizations?”

When I saw Petr Aven at the Four Seasons, he argued that the connections with the Trump Organization had been fabricated in order to frame his company. “This is a conspiracy against us,” he told me. “It is really much bigger than the computers.” Aven did not elaborate, but Jeffrey Birnbaum, a spokesperson for Alfa Bank, supplied more detail. The bank, he said, suspected that “we are victims of classic Russian *kompromat*—a well-known scam in which Russian competitors pay analysts to write false reports to damage reputations.” Birnbaum described the press inquiries into the matter as an extended affliction. “This has been a terrible ordeal for Alfa Bank, like living through a Kafka novel,” he said. (Max rejected the idea that his group had fabricated data. “If we were going to lie, then we would have made up a much better story than this!” he said.)

Because Alfa Bank did not retain its D.N.S. logs (many large companies don’t), its assessments of what produced the lookups in early 2016 are necessarily speculative. “We are as mystified as anybody about these false allegations,” Birnbaum told me this September. In a series of exchanges over three weeks, he offered a range of possibilities. He suggested that the data had been faked, but also that they had been stolen from the bank’s logs. He attributed the traffic to *kompromat*, but also expounded a scenario in which it had been caused by a technical glitch: Trump e-mails “hidden” in the system were intermittently processed by the bank’s security software, an application called Trend Micro Deep Discovery Inspector. In this explanation, Trump marketing e-mails from before March, 2016, had made it through the spam filter and been stored in a permanent archive, where the bank backs up all its e-mail. Periodically, the bank re-scanned that archive, as updates to the security software provided new information about which senders might be unsafe. During scans, the system performed D.N.S. lookups for every domain name contained in

every e-mail. In the course of several months, the bank said, this could account for the traffic.

The experts I spoke to confirmed that this was a technically plausible, if highly inefficient, way to configure security software. But the explanation raised questions of its own. Alfa Bank said that its scans ran for two days after each update. But Max's data don't show a consistent pattern of two-day spikes. Another concern lay in the chronology. The bank had received e-mails from the Trump domain in late 2015 and early 2016, which should have triggered lookups. But, according to the data, the lookups didn't begin until May, 2016. In response to a question about this discrepancy, Birnbaum said that the Trend Micro software had not been "fully integrated" until March—but that wouldn't account for the time between March and May.

A third problem was that, if Alfa Bank wasn't receiving new e-mails from the Trump Organization after March, 2016, then the number of Trump e-mails in the archive—and thus the number of lookups—should have remained steady through the summer. But Max's data showed a different pattern: no lookups in the spring, a small number in May, and then a slow increase starting in June, with spikes that lasted until the system went offline. When asked about the increase, Birnbaum offered another refinement of the explanation. The bank had previously said that the software had performed checks of old e-mails "multiple times over the six-month period." Now he said that a security update "around August" had caused old e-mails to be re-scanned.

In any case, for an explanation of this kind to work, it would require the servers at Spectrum Health to be simultaneously experiencing the same glitch, or another one with similar effects. (Spectrum declined to answer questions about its computer systems.) Trend Micro has thousands of users, most of them businesses, but in the sample that Max and his colleagues could see, only Alfa Bank and Spectrum Health exhibited this peculiar behavior.

For some, the most baffling part of the puzzle was the way that the lookups stopped. The Trump domain vanished from the Web on the morning of Friday, September 23rd, two days after the *Times* presented its data to B.G.R., Alfa Bank's lobbyists in Washington, but before it called Trump or Cendyn. In Max's view, this was evidence of direct contact between Alfa Bank and Trump. One researcher whom Foer interviewed put it vividly: "The knee was hit in Moscow, the leg kicked in New York." There is, however, at least one possibility that doesn't involve Moscow: the lobbyists in Washington could have passed along a warning to Trump, as a courtesy. But B.G.R. denies doing this, calling the idea "ridiculous on its face."

Whatever the reason that the Trump domain vanished, Alfa Bank's servers continued trying to look it up: Max's group observed fifteen failed attempts that Friday, twenty-eight on Saturday, none on Sunday, ninety on Monday, twenty on Tuesday. Spectrum Health's machine kept trying, too, in a weeklong spasm of activity that entailed thousands of seemingly automated lookups. Spectrum never succeeded in relocating the Trump server—but Alfa did. On the night of Tuesday, September 27th, ten minutes after the bank made its last failed attempt, it looked up the domain name trump1.contact-client.com—which was, it turned out, another route to the same Trump server.

The alternative domain name does not appear to have been previously active; no one has produced an e-mail sent from it. So how did Alfa find it? The easiest method would have been by consulting a PTR record, which shows what domain names are associated with a given I.P. address. But the PTR record for the Trump address did not include the alternative name.

Birnbaum said that Alfa Bank's researchers, investigating the traffic, found the new name in other public records and then performed a test lookup. Vixie said that such a lookup would be unusual, and questioned why the bank would feel that it was necessary: "Why did Alfa look up either name? And especially the second name?"

According to Max's data, Alfa Bank looked up the new domain name only once. In the following months, he and his group stopped collecting data on the Trump Organization domains. After the Slate story came out, curious readers looked up the address thousands of times, and the D.N.S. traffic devolved into statistical noise. The Trump Organization now controls the original domain; in March, 2017, Cendyn told CNN that it had been "transferred back." Records show that Cendyn handed over the domain only a few days before the CNN story ran—a year after the last e-mail was sent from it. Jones's team believed that Cendyn had continued its relationship with the Trump Organization in 2016. "There were thousands of e-mails between Trump and Cendyn through the entire period that Alfa Bank was looking up the Trump server," Max told me. Cendyn said that this was "regular business correspondence," related to transferring back the domain. When I called the company's C.E.O., Richard Deyo, to ask more broadly about the situation, he said, "This is old news—that's just Internet traffic," and then hung up. A spokesperson for Serenata, which took over Trump's hotel marketing, told me that the company had nothing to say. "Don't call again," she said.

As Jones's team sifted through explanations for the traffic, they began constructing their own theory. "What you have here is a minimally viable technical footprint of a small number of people who are using what I suspect is an ad-hoc system to communicate," Paul said. "Anytime the F.B.I. or anyone else pulls apart a cyber-crime organization, there is always some communication structure that's used for command and control. That's where the high-value communications happen." (Max and his colleagues did not see any D.N.S. evidence that the Trump Organization was attempting to access the server; they speculated that the organization was using a virtual private network, or V.P.N., a common security measure that obscures users' digital footprints.)

If this was a communications mechanism, it appeared to have been relatively simple, suggesting that it had been set up spontaneously and refined over time. Because the Trump Organization did not have administrative control of the server, Paul and Leto theorized that

any such system would have incorporated software that one of the parties was already using. “The likely scenario is not that the people using the server were incredibly sophisticated networking geniuses doing something obscure and special,” Max said. “The likely scenario is that they adapted a server and vender already available to them, which they felt was away from prying eyes.” Leto told me that he envisioned “something like a bulletin-board system.” Or it could have been an instant-messaging system that was part of software already in use on the server.

Kramer, of Listrak, insisted that his company’s servers were used exclusively for mass marketing. “We only do one thing here,” he told me. But Listrak’s services can be integrated with numerous Cendyn software packages, some of which allow instant messaging. One possibility is Metron, used to manage events at hotels. In fact, the Trump Organization’s October, 2016, statement, blaming the unusual traffic on a “banking customer” of Cendyn, suggested that the communications had gone through Metron, which supports both messaging and e-mail.

The parties might also have been using Webmail—e-mail that leaves few digital traces, other than D.N.S. lookups. Or, Paul and Leto said, they could have been communicating through software used to compose marketing e-mails. They might have used a method called foldering, in which messages are written but not sent; instead, they are saved in a drafts folder, where an accomplice who also has access to the account can read them. “This is a very common way for people to communicate with each other who don’t want to be detected,” Leto told me. David Petraeus, when he was the director of the C.I.A., used this method to exchange intimacies—and to share classified information—with his lover, Paula Broadwell. In June, an attorney for the Mueller investigation accused Paul Manafort of using foldering to facilitate secret communications.

Given the limitations of D.N.S. data, none of the independent experts I spoke to could be certain of what Alfa Bank and the Trump Organization were doing. Some of them cautioned that it was impossible even to guess at every way that an e-mail system might

malfunction. A senior analyst at a D.N.S.-service provider said, “Things can get messed up in unexpected ways.” But Paul and Leto maintained that they had considered and rejected every scenario that they had encountered in decades of cybersecurity work. “Is it possible there is an innocuous explanation for all this?” Paul said. “Yes, of course. And it’s also possible that space aliens did this. It’s possible—just not very likely.”

Paul and Leto periodically went back to Max in the course of their research, interrogating his assumptions and asking for more information. In one tranche of data that he gave them, they noticed that a third entity, in addition to Alfa Bank and Spectrum Health, had been looking up the Trump domain: Heartland Payment Systems, a payments processor based in Princeton. Of the thirty-five hundred D.N.S. queries seen for the Trump domain, Heartland made only seventy-six—but no other visible entity made more than two. Heartland had a link to Alfa Bank, but a tenuous one. It had recently been acquired by Global Payments, which, in 2009, had paid seventy-five million dollars for United Card Services, Russia’s leading credit-card-processing company; two years later, United Card Services bought Alfa Bank’s credit-card-processing unit. (A spokesperson for Global Payments said that her company had never had any relationship with the Trump Organization or with Alfa Bank, and that its U.S. and Russia operations functioned entirely independently.)

Spectrum Health has a similarly indirect business tie to Alfa Bank. Richard DeVos’ father co-founded Amway, and his brother, Doug, has served as the company’s president since 2002. In 2014, Amway joined with Alfa Bank to create an “Alfa-Amway” loyalty-card program in Russia. But such connections are circumstantial at best; the DeVos family seems far more clearly linked to Trump than to Russia.

If Trump and Alfa Bank—as well as Spectrum Health and Heartland Payment Systems—were communicating, what might they have been talking about? Max and some of the other scientists I spoke to theorized that they may have been using the system to

signal one another about events or tasks that had to be performed: money to be transferred, for instance, or data to be copied. “My guess is that, whenever someone wanted to talk, they would do a D.N.S. lookup and then route the traffic somewhere else,” Richard Clayton, of the University of Cambridge, said. Camp also speculated that the system may have been used to coordinate the movement of data. She noted that Cambridge Analytica, which was working for the Trump campaign, took millions of personal records from Facebook. In Camp’s scenario, these could have been transferred to the Russian government, to help guide its targeting of American voters before the election.

The researchers I spoke with were careful to point out that the limits of D.N.S. data prevent them from going beyond speculation. If employees of the companies were talking, the traffic reveals nothing about who they were or what they were saying; it is difficult to rule out something as banal as a protracted game of video poker. “If I’m a cop, I’m not going to take this to the D.A. and say we’re ready to prosecute,” Leto said. “I’m going to say we have enough to ask for a search warrant.” More complete information could be difficult to obtain. This March, after Republicans on the House Intelligence Committee announced that it had found no evidence of collusion between the Trump campaign and Russia, the committee’s Democrats filed a dissent, arguing that there were many matters still to be investigated, including the Trump Organization’s connections to Alfa Bank. The Democrats implored the majority to force Cendyn to turn over computer data that would help determine what had happened. Those records could show who in the Trump Organization used the server. There would probably also be a record of who shut down the Trump domain after the *Times* contacted Alfa Bank. Cendyn might have records of any outgoing communications sent by the Trump Organization. But the request for further investigation is unlikely to proceed as long as Republicans hold the majority. “We’ve all looked at the data, and it doesn’t look right,” a congressional staffer told me. “But how do you get to the truth?”

The enigma, for now, remains an enigma. The only people likely to finally resolve the question of Alfa Bank and the Trump Organization are federal investigators. Max told me that no one in his group had been contacted. But, he said, it wasn't necessary for anyone in the F.B.I. to talk to him, if the agents gathered the right information from other sources, like Listrak and Cendyn. "I hope Mueller has all of it," he said. ♦

Published in the print edition of the October 15, 2018, issue, with the headline "Enigma Machines."

Dexter Filkins is a staff writer at The New Yorker and the author of "The Forever War," which won a National Book Critics Circle Award.

More: [Cybersecurity](#) [Hacking](#) [2016 Election](#) [Elections](#) [Democratic National Committee](#) [Russia](#)
[Pres. Donald Trump](#) [Trump Organization](#) [Collusion](#)

NOT A CERTIFIED COPY

EXHIBIT 6

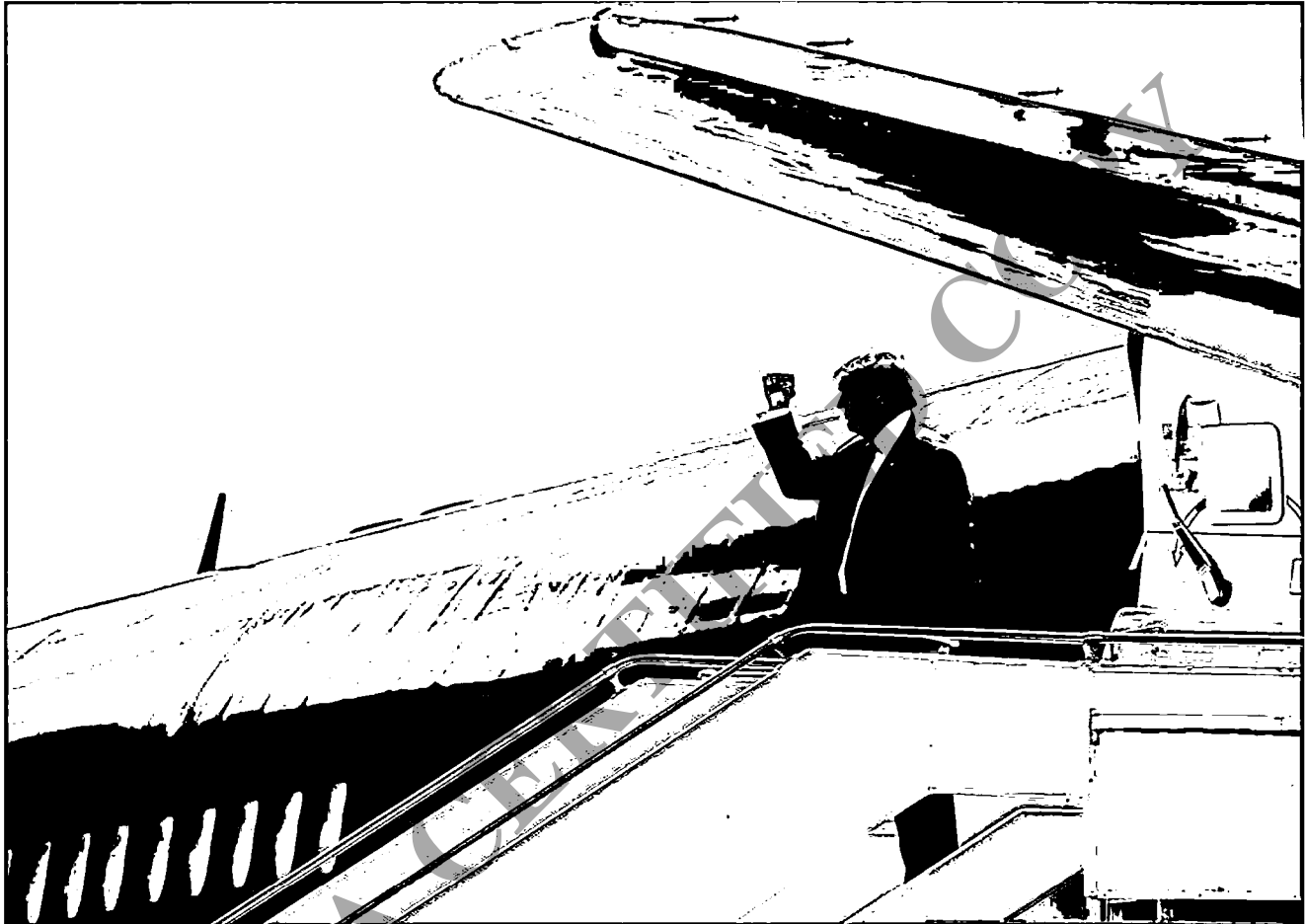
NOT A CERTIFIED COPY

Was a Trump Server Communicating With Russia?

SLATE

slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

Franklin Foer



Donald Trump gives a fist-pump to the ground crew as he arrives on his plane in St. Augustine, Florida, on Oct. 24.

Jonathan Ernst/Reuters

Read Franklin Foer's follow-up story for new statements from the Trump campaign and Alfa Bank and analysis of the competing theories about the server and its activity. [W3 x W3]

The greatest miracle of the internet is that it exists—the second greatest is that it persists. Every so often we're reminded that bad actors wield great skill and have little conscience about the harm they inflict on the world's digital nervous system. They invent viruses, botnets, and sundry species of malware. There's good money to be made deflecting these incursions. But a small, tightly knit community of computer scientists who pursue such work—some at cybersecurity firms, some in academia, some with close ties to three-letter federal agencies—is also spurred by a sense of shared idealism and considers itself the

benevolent posse that chases off the rogues and rogue states that try to purloin sensitive data and infect the internet with their bugs. “We’re the Union of Concerned Nerds,” in the wry formulation of the Indiana University computer scientist L. Jean Camp.

Advertisement

In late spring, this community of malware hunters placed itself in a high state of alarm. Word arrived that Russian hackers had infiltrated the servers of the Democratic National Committee, an attack persuasively detailed by the respected cybersecurity firm CrowdStrike. The computer scientists posited a logical hypothesis, which they set out to rigorously test: If the Russians were worming their way into the DNC, they might very well be attacking other entities central to the presidential campaign, including Donald Trump’s many servers. “We wanted to help defend both campaigns, because we wanted to preserve the integrity of the election,” says one of the academics, who works at a university that asked him not to speak with reporters because of the sensitive nature of his work.

Hunting for malware requires highly specialized knowledge of the intricacies of the domain name system—the protocol that allows us to type email addresses and website names to initiate communication. DNS enables our words to set in motion a chain of connections between servers, which in turn delivers the results we desire. Before a mail server can deliver a message to another mail server, it has to look up its IP address using the DNS. Computer scientists have built a set of massive DNS databases, which provide fragmentary histories of communications flows, in part to create an archive of malware: a kind of catalog of the tricks bad actors have tried to pull, which often involve masquerading as legitimate actors. These databases can give a useful, though far from comprehensive, snapshot of traffic across the internet. Some of the most trusted DNS specialists—an elite group of malware hunters, who work for private contractors—have access to nearly comprehensive logs of communication between servers. They work in close concert with internet service providers, the networks through which most of us connect to the internet, and the ones that are most vulnerable to massive attacks. To extend the traffic metaphor, these scientists have cameras posted on the internet’s stoplights and overpasses. They are entrusted with something close to a complete record of all the servers of the world connecting with one another.

In late July, one of these scientists—who asked to be referred to as Tea Leaves, a pseudonym that would protect his relationship with the networks and banks that employ him to sift their data—found what looked like malware emanating from Russia. The destination domain had Trump in its name, which of course attracted Tea Leaves’ attention. But his discovery of the data was pure happenstance—a surprising needle in a large haystack of DNS lookups on his screen. “I have an outlier here that connects to

Russia in a strange way,” he wrote in his notes. He couldn’t quite figure it out at first. But what he saw was a bank in Moscow that kept irregularly pinging a server registered to the Trump Organization on Fifth Avenue.

More data was needed, so he began carefully keeping logs of the Trump server’s DNS activity. As he collected the logs, he would circulate them in periodic batches to colleagues in the cybersecurity world. Six of them began scrutinizing them for clues.

Advertisement

(I communicated extensively with Tea Leaves and two of his closest collaborators, who also spoke with me on the condition of anonymity, since they work for firms trusted by corporations and law enforcement to analyze sensitive data. They persuasively demonstrated some of their analytical methods to me—and showed me two white papers, which they had circulated so that colleagues could check their analysis. I also spoke with academics who vouched for Tea Leaves’ integrity and his unusual access to information. “This is someone I know well and is very well-known in the networking community,” said Camp. “When they say something about DNS, you believe them. This person has technical authority and access to data.”)



Trump Tower.
Ullstein
Bild/Getty
Images

The researchers quickly dismissed their initial fear that the logs represented a malware attack. The communication wasn’t the work of bots. The irregular pattern of server lookups actually resembled the pattern of human conversation—conversations that began during office hours in New York and continued during office hours in Moscow. It dawned on the researchers that this wasn’t an attack, but a sustained relationship between a server registered to the Trump Organization and two servers registered to an entity called Alfa Bank.

The researchers had initially stumbled in their diagnosis because of the odd configuration of Trump’s server. “I’ve never seen a server set up like that,” says Christopher Davis, who runs the cybersecurity firm HYAS InfoSec Inc. and won a FBI Director Award for Excellence for his work tracking down the authors of one of the world’s nastiest botnet attacks. “It looked weird, and it didn’t pass the sniff test.” The server was first registered to Trump’s business in 2009 and was set up to run consumer marketing campaigns. It had a history of sending mass emails on behalf of Trump-branded properties and products. Researchers were ultimately convinced that the server indeed belonged to Trump. (Click [here](#) to see the server’s registration record.) But now this capacious server handled a strangely small load of traffic, such a small load that it would be hard for a company to justify the expense and trouble it would take to maintain it. “I get more mail in a day than the server handled,” Davis says.

“I’ve never seen a server set up like that.”

Christopher Davis of the cybersecurity firm HYAS InfoSec Inc.

That wasn't the only oddity. When the researchers pinged the server, they received error messages. They concluded that the server was set to accept only incoming communication from a very small handful of IP addresses. A small portion of the logs showed communication with a server belonging to Michigan-based Spectrum Health. (The company said in a statement: "Spectrum Health does not have a relationship with Alfa Bank or any of the Trump organizations. We have concluded a rigorous investigation with both our internal IT security specialists and expert cyber security firms. Our experts have conducted a detailed analysis of the alleged internet traffic and did not find any evidence that it included any actual communications (no emails, chat, text, etc.) between Spectrum Health and Alfa Bank or any of the Trump organizations. While we did find a small number of incoming spam marketing emails, they originated from a digital marketing company, Cendyn, advertising Trump Hotels.")

Advertisement

Spectrum accounted for a relatively trivial portion of the traffic. Eighty-seven percent of the DNS lookups involved the two Alfa Bank servers. "It's pretty clear that it's not an open mail server," Camp told me. "These organizations are communicating in a way designed to block other people out."

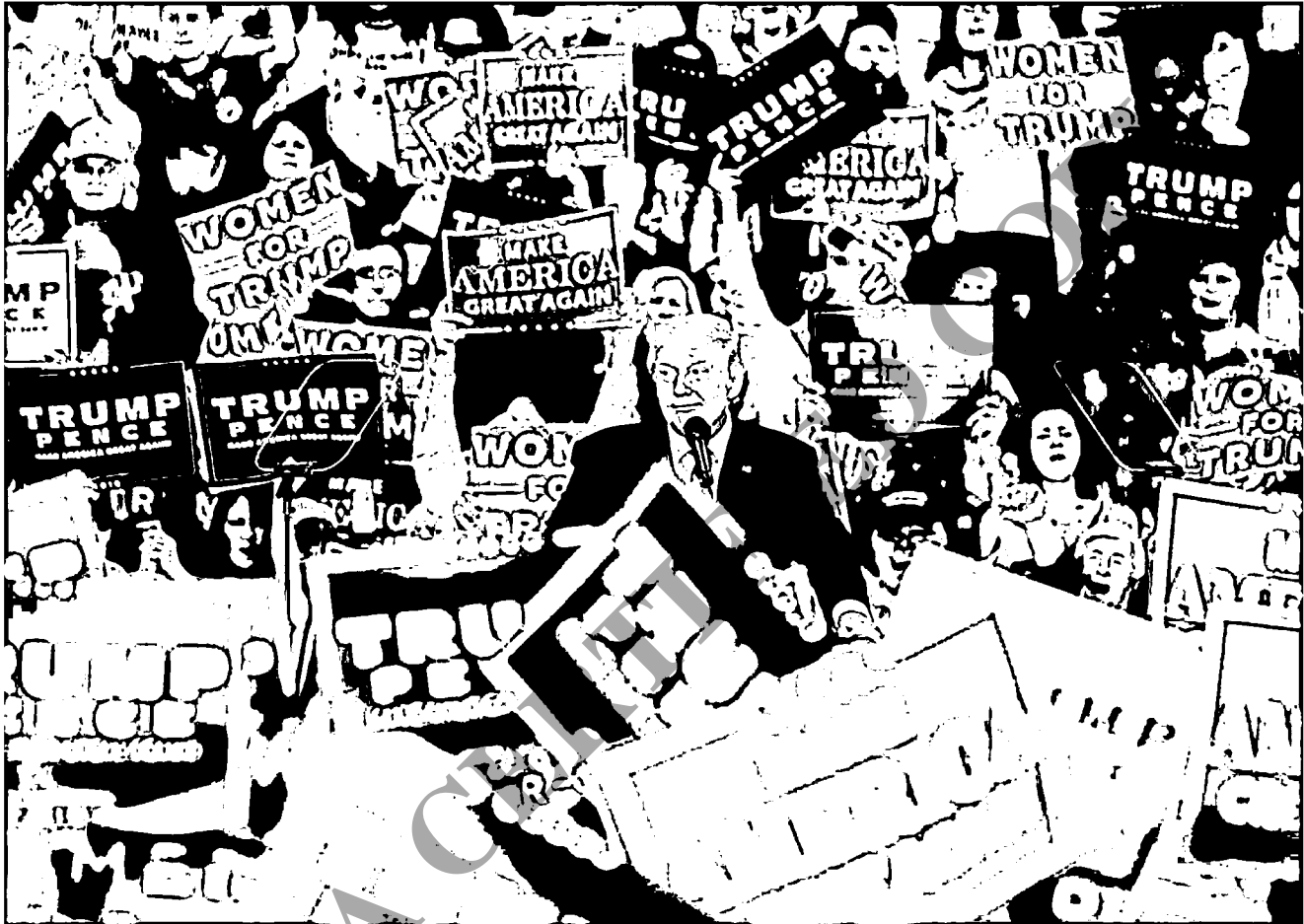
Earlier this month, the group of computer scientists passed the logs to Paul Vixie. In the world of DNS experts, there's no higher authority. Vixie wrote central strands of the DNS code that makes the internet work. After studying the logs, he concluded, "The parties were communicating in a secretive fashion. The operative word is *secretive*. This is more akin to what criminal syndicates do if they are putting together a project." Put differently, the logs suggested that Trump and Alfa had configured something like a digital hotline connecting the two entities, shutting out the rest of the world, and designed to obscure its own existence. Over the summer, the scientists observed the communications trail from a distance.

* * *

While the researchers went about their work, the conventional wisdom about Russian interference in the campaign began to shift. There were reports that the Trump campaign had ordered the Republican Party to rewrite its platform position on Ukraine, maneuvering the GOP toward a policy preferred by Russia, though the Trump campaign denied having a hand in the change. Then Trump announced in an interview with the *New York Times* his unwillingness to spring to the defense of NATO allies in the face of a Russian invasion. Trump even invited Russian hackers to go hunting for Clinton's emails, then passed the comment off as a joke. (I wrote about Trump's relationship with Russia in early July.)

Advertisement

In the face of accusations that he is somehow backed by Putin or in business with Russian investors, Trump has issued categorical statements. "I mean I have nothing to do with Russia," he told one reporter, a flat denial that he repeated over and over. Of course, it's possible that these statements are sincere and even correct. The sweeping nature of Trump's claim, however, prodded the scientists to dig deeper. They were increasingly confident that they were observing data that contradicted Trump's claims.



Donald Trump speaks at a rally at in Springfield, Ohio, on Thursday.
Paul Vernon/Getty Images

In the parlance that has become familiar since the Edward Snowden revelations, the DNS logs reside in the realm of metadata. We can see a trail of transmissions, but we can't see the actual substance of the communications. And we can't even say with complete certitude that the servers exchanged email. One scientist, who wasn't involved in the effort to compile and analyze the logs, ticked off a list of other possibilities: an errant piece of spam caroming between servers, a misdirected email that kept trying to reach its destination, which created the impression of sustained communication. "I'm seeing a preponderance of the evidence, but not a smoking gun," he said. Richard Clayton, a cybersecurity researcher at Cambridge University who was sent one of the white papers laying out the evidence, acknowledges those objections and the alternative theories but considers them improbable. "I think mail is more likely, because it's going to a machine

running a mail server and [the host] is called mail. Dr. Occam says you should rule out mail before pulling out the more exotic explanations.” After Tea Leaves posted his analysis on Reddit, a security blogger who goes by [Krypt3ia](#) expressed initial doubts—but his analysis was tarnished by several incorrect assumptions, and as he examined the matter, his skepticism of Tea Leaves softened somewhat.

I put the question of what kind of activity the logs recorded to the University of California’s Nicholas Weaver, another computer scientist not involved in compiling the logs. “I can’t attest to the logs themselves,” he told me, “but assuming they are legitimate they do indicate effectively human-level communication.”

Weaver’s statement raises another uncertainty: *Are the logs authentic?* Computer scientists are careful about vouching for evidence that emerges from unknown sources—especially since the logs were pasted in a text file, where they could conceivably have been edited. I asked nine computer scientists—some who agreed to speak on the record, some who asked for anonymity—if the DNS logs that Tea Leaves and his collaborators discovered could be forged or manipulated. They considered it nearly impossible. It would be easy enough to fake one or maybe even a dozen records of DNS lookups. But in the aggregate, the logs contained thousands of records, with nuances and patterns that not even the most skilled programmers would be able to recreate on this scale. “The data has got the right kind of fuzz growing on it,” Vixie told me. “It’s the interpacket gap, the spacing between the conversations, the total volume. If you look at those time stamps, they are not simulated. This bears every indication that it was collected from a live link.” I asked him if there was a chance that he was wrong about their authenticity. “This passes the reasonable person test,” he told me. “No reasonable person would come to the conclusion other than the one I’ve come to.” Others were equally emphatic. “It would be really, really hard to fake these,” Davis said. According to Camp, “When the technical community examined the data, the conclusion was pretty obvious.”

Advertisement

It’s possible to impute political motives to the computer scientists, some of whom have criticized Trump on social media. But many of the scientists who talked to me for this story are Republicans. And almost all have strong incentives for steering clear of controversy. Some work at public institutions, where they are vulnerable to political pressure. Others work for firms that rely on government contracts—a relationship that tends to squash positions that could be misinterpreted as outspoken.

* * *

The researchers were seeing patterns in the data—and the Trump Organization’s potential interlocutor was itself suggestive. Alfa Bank emerged in the messy post-Soviet scramble to create a private Russian economy. Its founder was a Ukrainian called [Mikhail Fridman](#). He

erected his empire in a frenetic rush—in a matter of years, he rose from operating a window washing company to the purchase of the Bolshevik Biscuit Factory to the co-founding of his bank with some friends from university. Fridman could be charmingly open when describing this era. In 2003, he told the Financial Times, “Of course we benefitted from events in the country over the past 10 years. Of course we understand that the distribution of state property was not very objective. ... I don’t want to lie and play this game. To say one can be completely clean and transparent is not realistic.”

To build out the bank, Fridman recruited a skilled economist and shrewd operator called Pyotr Aven. In the early '90s, Aven worked with Vladimir Putin in the St. Petersburg government—and according to several accounts, helped Putin wiggle out of accusations of corruption that might have derailed his ascent. (Karen Dawisha recounts this history in her book *Putin's Kleptocracy*.) Over time, Alfa built one of the world’s most lucrative enterprises. Fridman became the second richest man in Russia, valued by *Forbes* at \$15.3 billion.

Alfa’s oligarchs occupied an unusual position in Putin’s firmament. They were insiders but not in the closest ring of power. “It’s like they were his judo pals,” one former U.S. government official who knows Fridman told me. “They were always worried about where they stood in the pecking order and always feared expropriation.” Fridman and Aven, however, are adept at staying close to power. As the U.S. District Court for the District of Columbia once ruled, in the course of dismissing a libel suit the bankers filed, “Aven and Fridman have assumed an unforeseen level of prominence and influence in the economic and political affairs of their nation.”

Unlike other Russian firms, Alfa has operated smoothly and effortlessly in the West. It has never been slapped with sanctions. Fridman and Aven have cultivated a reputation as beneficent philanthropists. They endowed a prestigious fellowship. The Woodrow Wilson International Center for Scholars, the American-government funded think tank, gave Aven its award for “Corporate Citizenship” in 2015. To protect its interests in Washington, Alfa hired as its lobbyist former Reagan administration official Ed Rogers. Richard Burt, who helped Trump write the speech in which he first laid out his foreign policy, previously served on Alfa’s senior advisory board.* The branding campaign has worked well. During the first Obama term, Fridman and Aven met with officials in the White House on two occasions, according to visitor logs.

Fridman and Aven have significant business interests to promote in the West. One of their holding companies, LetterOne, has vowed to invest as much as \$3 billion in U.S. health care. This year, it sank \$200 million into Uber. This is, of course, money that might otherwise be invested in Russia. According to a former U.S. official, Putin tolerates this

condition because Alfa advances Russian interests. It promotes itself as an avatar of Russian prowess. “It’s our moral duty to become a global player, to prove a Russian can transform into an international businessman,” Fridman told the *Financial Times*.

* * *

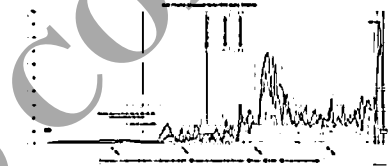
Tea Leaves and his colleagues plotted the data from the logs on a timeline. What it illustrated was suggestive: The conversation between the Trump and Alfa servers appeared to follow the contours of political happenings in the United States. “At election-related moments, the traffic peaked,” according to Camp. There were considerably more DNS lookups, for instance, during the two conventions.

In September, the scientists tried to get the public to pay attention to their data. One of them posted a link to the logs in a Reddit thread. Around the same time, the *New York Times*’ Eric Lichtblau and Steven Lee Myers began chasing the story.* (They are still pursuing it.) Lichtblau met with a Washington representative of Alfa Bank on Sept. 21, and the bank denied having any connection to Trump. (Lichtblau told me that *Times* policy prevents him from commenting on his reporting.)

The *Times* hadn’t yet been in touch with the Trump campaign —Lichtblau spoke with the campaign a week later—but shortly after it reached out to Alfa, the Trump domain name in question seemed to suddenly stop working. When the scientists looked up the host, the DNS server returned a fail message, evidence that it no longer functioned. Or as it is technically diagnosed, it had “SERVFAILED.” (On the timeline above, this is the moment at the end of the chronology when the traffic abruptly spikes, as servers frantically attempt to resend rejected messages.) The computer scientists believe there was one logical conclusion to be drawn: The Trump Organization shut down the server after Alfa was told that the *Times* might expose the connection. Weaver told me the Trump domain was “very sloppily removed.” Or as another of the researchers put it, it looked like “the knee was hit in Moscow, the leg kicked in New York.”

As one of the researchers put it, it looked like “the knee was hit in Moscow, the leg kicked in New York.”

Four days later, on Sept. 27, the Trump Organization created a new host name, trump1.contact-client.com, which enabled communication to the very same server via a different route. When a new host name is created, the first communication with it is never



Start: DNS lookup history start date. **RFC from Alfa-Bank:** Alfa-Bank rep provided with 2 ips, hostname, count. **Errors:** 4:11 a.m. UTC: DNS lookup errors Trump-Email.com. **Errors:** 1:12 a.m. UTC: DNS lookup errors Trump-Email.com. **Taken down:** 9:53 a.m. EST USA time: Trump-Email.com deleted from Trump authoritative name server zone.

random. To reach the server after the resetting of the host name, the sender of the first inbound mail has to first learn of the name somehow. It's simply impossible to randomly reach a renamed server. "That party had to have some kind of outbound message through SMS, phone, or some noninternet channel they used to communicate [the new configuration]," Paul Vixie told me. The first attempt to look up the revised host name came from Alfa Bank. "If this was a public server, we would have seen other traces," Vixie says. "The only look-ups came from this particular source."

According to Vixie and others, the new host name may have represented an attempt to establish a new channel of communication. But media inquiries into the nature of Trump's relationship with Alfa Bank, which suggested that their communications were being monitored, may have deterred the parties from using it. Soon after the *New York Times* began to ask questions, the traffic between the servers stopped cold.

* * *

Last week, I wrote to Alfa Bank asking if it could explain why its servers attempted to connect with the Trump Organization on such a regular basis. Its Washington representative, Jeffrey Birnbaum of the public relations firm BGR, provided me the following response:

Alfa hired Mandiant, one of the world's foremost cyber security experts, to investigate and it has found nothing to the allegations. I hope the below answers respond clearly to your questions. Neither Alfa Bank nor its principals, including Mikhail Fridman and Petr Aven, have or have had any contact with Mr. Trump or his organizations. Fridman and Aven have never met Mr. Trump nor have they or Alfa Bank had any business dealings with him. Neither Alfa nor its officers have sent Mr. Trump or his organizations any emails, information or money. Alfa Bank does not have and has never had any special or exclusive internet connection with Mr. Trump or his entities. The assertion of a special or private link is patently false.

I asked Birnbaum if he would connect me with Mandiant to elaborate on its findings. He told me:

Mandiant is still doing its deep dive into the Alfa Bank systems. Its leading theory is that Alfa Bank's servers may have been responding with common DNS look ups to spam sent to it by a marketing server. But it doesn't want to speak on the record until it's finished its investigation.

It's hard to evaluate the findings of an investigation that hasn't ended. And of course, even the most reputable firm in the world isn't likely to loudly broadcast an opinion that bites the hand of its client.

I posed the same basic questions to the Trump campaign. Trump spokeswoman Hope Hicks sent me this in response to my questions by email:

The email server, set up for marketing purposes and operated by a third-party, has not been used since 2010. The current traffic on the server from Alphabank's [sic] IP address is regular DNS server traffic—not email traffic. To be clear, The Trump Organization is not sending or receiving any communications from this email server. The Trump Organization has no communication or relationship with this entity or any Russian entity.

I asked Hicks to explain what caused the Trump Organization to rename its host after the *New York Times* called Alfa. I also asked how the Trump Organization arrived at its judgment that there was no email traffic. (Furthermore, there's no such thing as "regular" DNS server traffic, at least not according to the computer scientists I consulted. The very reason DNS exists is to enable email and other means of communication.) She never provided me with a response.

What the scientists amassed wasn't a smoking gun. It's a suggestive body of evidence that doesn't absolutely preclude alternative explanations. But this evidence arrives in the broader context of the campaign and everything else that has come to light: The efforts of Donald Trump's former campaign manager to bring Ukraine into Vladimir Putin's orbit; the other Trump adviser whose communications with senior Russian officials have worried intelligence officials; the Russian hacking of the DNC and John Podesta's email.

We don't yet know what this server was for, but it deserves further explanation.

Update, Oct. 31, 2016: *The article has been updated to make clear that the New York Times reporters learned of the logs independently, not from the Reddit thread. [Return.](#)*

Correction, Nov. 1, 2016: *The article originally stated that Richard Burt serves on Alfa's senior advisory board. He no longer sits on that board. [Return.](#)*

Read [Franklin Foer's follow-up story](#) for new statements from the Trump campaign and Alfa Bank and analysis of the competing theories about the server and its activity.

[See more of Slate's election coverage.](#)

EXHIBIT 7

NOT A CERTIFIED COPY

Summary of Cyber Incident Investigation

NOT A CERTIFIED COPY

Prepared for:

Kirkland & Ellis LLP & Alfa Bank JSC

Prepared by:

Stroz Friedberg, LLC

July 19, 2017

TABLE OF CONTENTS

I. Summary of Investigation..... 1

 A. Analysis of Log and Email Data..... 1

 B. Analysis of Data Posted by Professor Camp..... 3

 C. Conclusions..... 3

NOT A CERTIFIED COPY

I. SUMMARY OF INVESTIGATION

Kirkland & Ellis LLP, on behalf of its client Alfa Bank JSC (“Alfa-Bank”), engaged Stroz Friedberg, LLC (“Stroz Friedberg”) on March 14, 2017, to provide technical and digital forensics services in support of Alfa-Bank’s investigation of claims that the bank purportedly communicated with The Trump Organization. This document provides a high-level summary of Stroz Friedberg’s work on this matter.

In February 2017, Alfa-Bank observed suspicious entries in its DNS¹ logs showing that Alfa-Bank servers received 16 queries, such as “mail.trump-email.com.MOSCOW.ALFAINTRA.NET” (an invalid hostname), from external IP addresses.² These DNS requests were identical to the unverified DNS queries that were previously highlighted by security researcher Professor L. Jean Camp in 2016. Then, in March 2017, Alfa-Bank servers received more than 20,000 additional suspicious DNS queries for the same host name.

Kirkland & Ellis and Alfa-Bank asked Stroz Friedberg to conduct an independent investigation into the suspicious 2017 DNS queries to determine, to the extent possible, if they resulted from communications between Alfa-Bank and The Trump Organization. Kirkland & Ellis also informed Stroz Friedberg that Alfa-Bank received similar DNS queries in 2016, but those queries were outside our scope. Another incident response company, Mandiant, has already investigated and reported on the 2016 activity. The only aspect of the 2016 information Stroz Friedberg was asked to examine was the information posted online by Professor Camp. Stroz Friedberg was asked to determine, to the extent possible, whether the information might have originated from Alfa-Bank servers, and if so, whether there was any indication of how this information was obtained from Alfa-Bank systems.

A. ANALYSIS OF LOG AND EMAIL DATA

Stroz Friedberg searched Alfa-Bank’s available aggregated log data and email archives for information related to bank communications to determine, to the extent possible, whether any communications occurred between Alfa-Bank and The Trump Organization. Specifically, Stroz Friedberg searched, among other data sources:

- + DNS logs from all DNS servers in use at Alfa-Bank from February 18, 2017 to March 23, 2017
- + Firewall logs from all firewalls at Alfa-Bank from February 20, 2017 to March 23, 2017
- + The email archive containing all messages sent or received by email servers at Alfa-Bank from January 29, 2017 to April 6, 2017

¹ DNS, or the Domain Name System, is the system on the internet for converting easier to use alphanumeric names into numeric IP addresses computers need to connect to one another.

² IP addresses are the unique numbers assigned to computers to facilitate communication on the internet or across other computer networks.

These sets of information incorporated all available log and email data available at the time our searches were executed. We searched the available data using a broad set of search terms designed to return any communications between Alfa-Bank and The Trump Organization. For example, we searched the DNS logs for the word “trump” as well as any email message where the word “trump” appears in the sender, recipients, subject, or body of the email message. In total, we searched the available data using more than 20 broad keywords. Stroz Friedberg then analyzed the results of those searches to determine the nature of those search hits and to formulate follow-up searches.

From this data, Stroz Friedberg identified 321 unique IP addresses from across the world (many associated with Amazon Web Services) that sent the suspicious DNS queries containing the word “trump” to Alfa-Bank. We then searched the available log data to identify all other log entries containing those IP addresses to determine, to the extent possible, how those devices from those suspicious IP addresses interacted with Alfa-Bank systems. The combined efforts of the broad search, followed by specific follow-up searches, returned hundreds of thousands of DNS log entries, almost two million entries from the firewall logs, and several thousand email messages, all of which Stroz Friedberg analyzed and reviewed as part of its investigation.

Based on our analysis of the available 2017 email and log data, Stroz Friedberg found no evidence of any connections or communications between Alfa-Bank and The Trump Organization occurring in 2017. Nor did our analysis of the suspicious DNS requests made against the DNS servers at Alfa-Bank for “mail.trump-email.com.moscow.alfaintra.net” reveal any evidence to support claims that Alfa-Bank was exchanging email messages or other communications with The Trump Organization in 2017. Specifically, Stroz Friedberg observed:

- + All mentions of “Trump” in email messages were false-positive results, i.e., were not communications with President Trump or anyone in The Trump Organization. The vast majority of the email messages mentioning “Trump” were news alert emails or market research emails from web sites such as Bloomberg.net, Barclays.com, Factiva.com, The Wall Street Journal (wsj.com), and WashingtonPost.com.
- + None of the messages we reviewed contained any US government email addresses. Nor did they contain any Trump-related email addresses in the address fields of the messages.
- + We identified no DNS queries for any host at trump.com, which should have existed if there were actually any email or other type of communication with The Trump Organization.
- + All queries relating to trump-email.com were made by outside parties querying Alfa-Bank’s DNS servers. These queries appear to have originated from multiple outside parties from a variety of source IP addresses. Further, the high volume of queries requesting IP addresses for a wide variety of host names other than “mail.trump-email.com.moscow.alfaintra.net” is consistent with the type of traffic often seen coming from security researchers or attackers checking or testing a company’s security. While some of these queries appear random, the vast majority of the queries relate to actual systems at Alfa-Bank, which could have been uncovered by researching domain names with similar domain registration information.

B. ANALYSIS OF DATA POSTED BY PROFESSOR CAMP

Stroz Friedberg analyzed data posted to Professor Camp’s website that appears to originate from Alfa-Bank systems. That data included certain DNS requests dated September 2016 that are substantively identical to DNS requests identified in 2017. As seen in the chart below, the only difference between several 2016 requests and some of the 2017 requests is capitalization:

September 2016	mail.trump-email.com.moscow.alfaintra.net
February 2017	mail.trump-email.com.MOSCOW.ALFAintRa.nEt
March 2017	mail.trump-email.com.moscow.alfaintra.net

Multiple news articles and blog posts speculated that these 2016 and 2017 DNS queries are indicative of communication between Alfa-Bank and The Trump Organization. These articles and posts generally cited the invalid hostname “mail.trump-email.com.moscow.alfaintra.net,” which is a concatenation of two separate names (“mail.trump-email.com” and “moscow.alfaintra.net”), as evidence of communication. Our analysis of the available 2017 data, however, does not support the supposition that communication occurred in 2017. Rather, our analysis revealed that a broad group of people simply sent queries for the term “mail.trump-email.com.moscow.alfaintra.net” to Alfa-Bank DNS servers.

Further, we found no evidence of unauthorized access to the Alfa-Bank’s DNS servers in any of the 2017 data we reviewed. We examined the DNS logs, firewall logs, and network packet captures for any evidence of an outside party interacting with Alfa-Bank’s systems in a suspicious way beyond the DNS queries. None of the data we reviewed revealed any suspicious traffic or connections other than the already identified DNS queries.

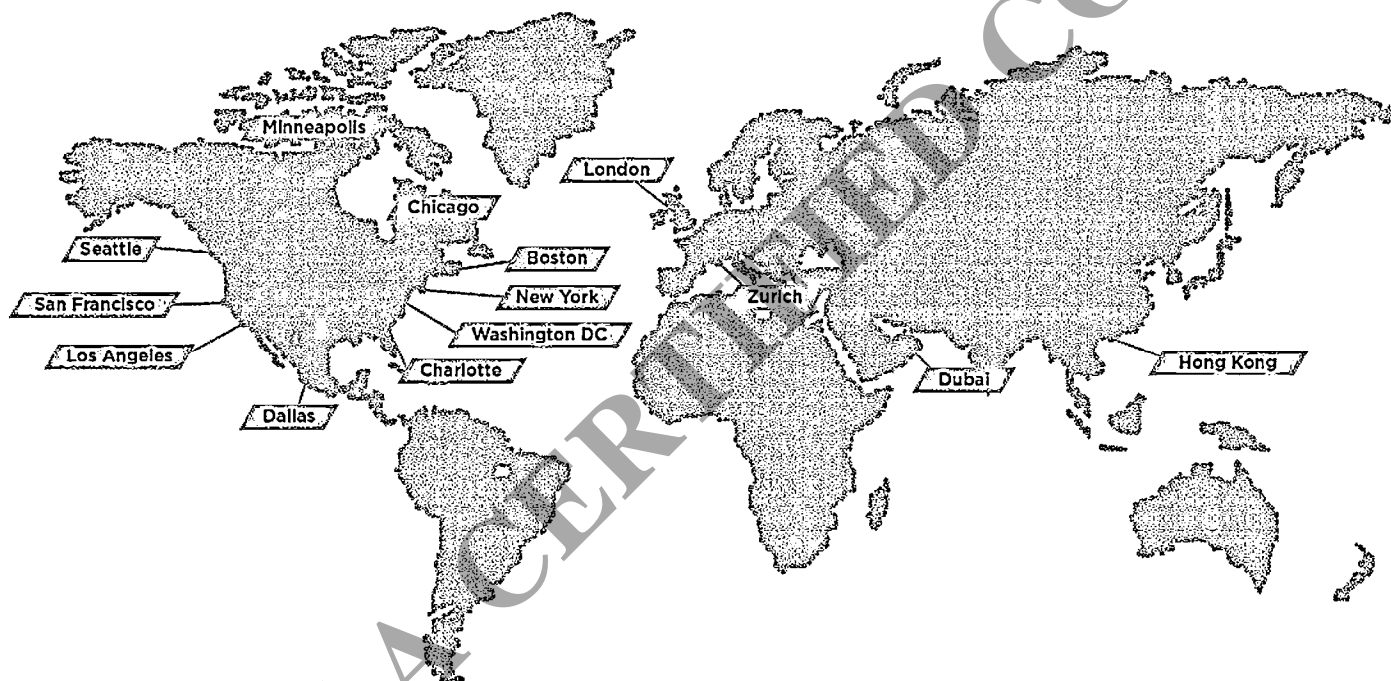
The information posted online by Professor Camp appears to include DNS log data from Alfa-Bank. However, because the information is from 2016 (when Alfa-Bank’s practice was to preserve DNS log data only for 24 hours), log data at the bank no longer exists for that timeframe. As such, we were unable to verify whether or not the information is valid. Additionally, the format of the data does not match the format of actual logs at Alfa-Bank. If the DNS log data posted by Professor Camp is actual DNS log data from Alfa-Bank, it has been edited and placed into a different format. It is unknown how or from whom Professor Camp obtained this unverified data, seemingly from Alfa-Bank systems.

C. CONCLUSIONS

Our investigation revealed no actual connections or communications between Alfa-Bank and President Trump or The Trump Organization in any of the 2017 data we analyzed and no evidence of a compromise of the Alfa-Bank DNS servers in 2017. Because the concatenated name “mail.trump-email.com.moscow.alfaintra.net” has been widely published, it is likely that the suspicious queries came from researchers and/or would-be attackers who learned of this name from online sources and then issued queries to Alfa-Bank’s DNS servers.

STROZ FRIEDBERG

an Aon company



About Stroz Friedberg

Stroz Friedberg, an Aon company, is a specialized risk management firm built to help clients solve the complex challenges prevalent in today's digital, connected, and regulated business world. Our focus is on cybersecurity, with leading experts in digital forensics, incident response, and security science; investigation; eDiscovery; intellectual property; and due diligence. Stroz Friedberg works to maximize the health of an organization, ensuring its longevity, protection, and resilience. Founded in 2000 and acquired by Aon in 2016, Stroz Friedberg has thirteen offices across nine U.S. cities, London, Zurich, Dubai, and Hong Kong. Stroz Friedberg serves Fortune 100 companies, 80% of the AmLaw 100, and the Top 20 UK law firms. Learn more at <https://www.strozfriedberg.com/>.

This document and/or its attachments may contain information that is confidential and/or protected by privilege from disclosure. If you have reason to believe you are not the intended recipient, please immediately notify the sender by reply e-mail or by telephone, then destroy this document, as well as all copies, including any printed copies. Thank you.

EXHIBIT 8

NOT A CERTIFIED COPY

Press Statement: Alfa Bank confirms it has sought help from U.S. authorities, and discloses new cyberattacks linked to Trump hoax

[Alfabank.com/news/press-statement-alfa-bank-confirms-it-has-sought-help-from-u-s-authorities-and-discloses-new-cyberattacks-linked-to-trump-hoax/](http://alfabank.com/news/press-statement-alfa-bank-confirms-it-has-sought-help-from-u-s-authorities-and-discloses-new-cyberattacks-linked-to-trump-hoax/)

Alfa Bank, a privately owned Russian bank, confirmed today that it has contacted U.S. law enforcement authorities for assistance and offered U.S. agencies its complete co-operation in finding the people behind attempted cyberattacks on its servers that have made it appear falsely that it has been communicating with the Trump Organization.

Alfa Bank confirmed a story in Circa News that it had been subjected to three new attempted domain name server (DNS) cyberattacks of increasing intensity over the last few weeks. In the attacks, multiple DNS requests were made by unidentified individuals, mostly using U.S. server providers, to a Trump Organization server. The DNS requests were made to appear as if they originated from Alfa Bank. The DNS responses from the Trump server were then erroneously returned to Alfa Bank, activating Alfa Bank's automated security systems on February 18 and again on March 11 and 13. Alfa Bank has engaged the U.S.-based cyber forensics firm Stroz Friedberg to investigate these new attacks.

Alfa Bank believes that these malicious attacks are designed to create the false impression that Alfa Bank has a secretive relationship with the Trump Organization. In fact, there is not and never has been such a relationship.

New February 2017 attack on Alfa Bank server

On February 18, 2017, Alfa Bank experienced suspicious cyber-activity from an unidentified third-party. Specifically, the unidentified third-party repeatedly sent suspicious DNS queries from servers in the U.S. to a Trump Organization server. The unidentified individuals made it look as though these queries originated from variants of MOSCOW.ALFAintRa.nET. As a result, the DNS responses from the Trump server were returned incorrectly to Alfa Bank's server, which triggered Alfa Bank's automated security system.

Alfa Bank believes that unknown individuals — using an identified U.S.-based service provider — are behind this recent attack, and that they are attempting to trigger verification signals between Alfa Bank and a server associated with the Trump Organization.

It believes that someone or some group manufactured this deceit by «spoofing» or falsifying DNS lookups to create the impression of communication between Alfa Bank and the Trump Organization. However, Alfa Bank's DNS servers neither send nor receive email. Instead, they react when contacted by unwanted and unsolicited messages by sending out DNS verification signals asking, in effect, who is the server contacting Alfa Bank.

An Alfa Bank spokesperson said:

"The cyberattacks are an attempt by unknown parties to manufacture the illusion of contact between Alfa Bank's DNS servers and 'Trump servers'.

«A simple analogy would be someone in the U.S. sending an empty envelope (in this case a DNS signal) to a Trump office (server) addressed to Trump, but on the back of the envelope the return address is Russia (Alfa Bank) instead of its own real address. The Trump office, recognizing there is nothing in the empty envelope to deal with, returns it as undelivered to Russia instead of to the U.S.-based sender. So, on cursory examination, Alfa Bank appears to have been receiving responses to queries it never actually sent.

«We have gone to the U.S. Justice Department and offered our complete co-operation to get to the bottom of this sham and fraud.»

Other indications of human intervention include the fact that the queries occurring in these logs included mixed uppercased and lowercased letters. The majority of DNS queries are machine based queries (for example, browsers and email clients), which would send lowercased queries to the DNS servers.

A few days after the February 18 DNS attack, Alfa Bank again started to receive inquiries from U.S. media outlets, including CNN, about allegations of cyber links with Donald Trump. No such link exists or, in fact, has ever existed between Alfa Bank and Mr. Trump or his organization.

An anonymous group has been trying for months to persuade news organizations to publish stories that such a link is real. Alfa Bank has asked reporters who have contacted it about the traffic to assist by letting the bank know if someone is trying to create the false impression that Alfa Bank has business or other dealings with Mr. Trump.

Two new confirmed March 2017 attacks on Alfa Bank server

On March 11 and 13, Alfa Bank was subjected to two new DNS attacks using similar methods. These attacks appear to have been orchestrated from multiple servers primarily in the U.S.

Between 02:00 and 07:00 (Moscow Time) on March 11 and at 21:00 on March 13, Alfa Bank experienced suspicious cyber activity from an unidentified third party or parties. The unidentified third parties or party repeatedly sent unusual DNS queries to a Trump server, the responses to which again ultimately triggered Alfa Bank's automated security system.

Over a five-hour period on Saturday — and again on Monday — Alfa Bank received more than 1,340 DNS responses containing mail.trump-email.com.moscow.alfaintra.net.

These malicious and seemingly co-ordinated DNS attacks are coming from unidentified users using a variety of predominantly U.S. servers, including Google and Amazon web services. These IP service providers are inadvertently allowing their infrastructure to be used to attack Alfa Bank.

Alfa Bank suspects the unidentified parties are attempting to cover their tracks by using cloud services from these providers.

Given the frequency of the attacks and the variety of Internet service providers used in the attacks, Alfa Bank's working hypothesis is that these new attacks are being launched from a botnet.

Possible third new attack In March 2017

Alfa Bank has now started to monitor all incoming messages to its servers containing the word «trump.» This monitoring has revealed that Alfa Bank also is receiving unsolicited marketing emails from «marketing@trumphotels.com.» These incoming spam marketing emails also trigger Alfa Bank's security system, which automatically sends multiple DNS verification requests back to the originating server — here, the Trump server — in order to ascertain the identity of the sender.

Alfa Bank does not know whether these marketing emails are legitimate, or whether a third-party is orchestrating the campaign in another attempt to create the false impression of inappropriate communications between Alfa Bank and the Trump Organization.

In response to media questions that started last September, Alfa Bank asked Mandiant, one of the world's leading cyber experts, to investigate allegations suggested by an anonymous cyber group of a link between Alfa Bank and Trump, based on unverified DNS logs.

Mandiant completed its independent investigation late last year. After examining Alfa Bank's system both remotely and on the ground in Moscow, and the unverified DNS data presented to the media by the anonymous cyber group, Mandiant concluded that there is no evidence of substantive contact, such as emails or financial links, between Alfa Bank and the Trump Campaign or the Trump Organization.

Mandiant investigated (1) the DNS data given to the media, which journalists had shared with independent DNS experts, and (2) Alfa Bank servers for any evidence of links.

Mandiant concluded:

DNS data — There is no information that indicates where the list (obtained by reporters) has come from. The list contains approximately 2,800 look ups of a Domain Name over a period of 90 days. The information is inconclusive and is not evidence of substantive contact or a direct email or financial link between Alfa Bank and the Trump Campaign or Organization.

Alfa Bank servers — Nothing we have or have found alters our view as described above that there is no evidence of substantive contact or a direct email or financial link between Alfa Bank and the Trump Campaign or Organization.

Mandiant's working hypothesis is that the activity the reporters' sources alleged last year was caused by an email marketing/spam campaign possibly targeted at Alfa Bank employees by a marketing server, which triggered security software.

Earlier this year, Alfa Bank launched another investigation to find out who was — and maybe still is — behind this elaborate hoax.

Access to other's DNS data is highly privileged and is usually independently examined for academic purposes and cyber security research. Therefore, the examination and sharing of DNS data by the people involved in these fraudulent activities brings into question whether these data were acquired lawfully and whether it was ethical to misuse privileged access in order to manufacture a deceit.

Alfa Bank's working hypothesis is that an individual — possibly well known in internet research circles — may have fed selected DNS data to an anonymous cyber group to ensure they reached a specific (and erroneous) conclusion. Alternatively, the cyber group may have been complicit in the deceit. In the most recent cases, unknown individuals demonstrably attempted to insert falsified records onto Alfa Bank's computer systems designed to create the same impression.

An Alfa Bank spokesperson said: «The anonymous cyber group, which is led according to news accounts by 'Tea Leaves,' cannot produce evidence of a link because there never has been one. Alfa Bank believes that it is under attack and has pledged its complete cooperation to U.S. authorities to find out who is behind these malicious attacks and false stories.»

EXHIBIT 9

NOT A CERTIFIED COPY

Intra Net DNS Leakage

An "intranet" is a company's internal network, intra or inside the boundaries of the company. Intranets are not intended to be accessible or visible from the outside except via special access. These private networks are for business; these are not public accessible. Even regular checking account holders of Alfa Bank don't get access. Such networks run off a green list or white list of approved parties. DNS leakage does occur occasionally between a company internal network and the Internet, especially during times of errors and configuration because of human factors.

Here we see clear indication that the Moscow division of the INTERNAL Alfa Bank network most definitely has purposeful communications with a hostname registered by the Trump Organization. The concatenation below is a DNS leak of an internal configuration.

If a machine were spamming a company, you would block it. You be would be highly unlikely to change your internal intranet records to make sure the connection continued.

Here we see a change to the Trump-Email.com zone from DNS by CenDyn. (CenDyn has stated that the host was indeed in use for "a bank" that wanted to have "meetings" with Alfa Bank - read those details [here](#)).

SCROLL DOWN TO CONTINUE READING

TIMESTAMP | HOSTNAME | QUERY ORIGINATOR IP

The QUERY ORIGINATOR IP is typically a recursive DNS resolver

```

2016-09-01T19:45:53.000Z|Mail.alfaintra.net|217.12.96.15
2016-09-01T19:53:53.000Z|_ldap._tcp.dc._msdcs.WORKGROUP.alfaintra.net|217.12.96.15
2016-09-02T06:42:00.000Z|relay1.alfaintra.net|173.37.137.68
2016-09-02T07:40:12.000Z|_ldap._tcp.dc._msdcs.WORKGROUP.moscow.alfaintra.net|217.12.97.15
2016-09-02T07:56:07.000Z|Mail2.moscow.alfaintra.net|217.12.97.15
2016-09-02T07:56:24.000Z|Mail.moscow.alfaintra.net|217.12.97.15
2016-09-02T07:57:41.000Z|MailApp.moscow.alfaintra.net|217.12.97.15
2016-09-05T19:58:26.000Z|mail4.moscow.alfaintra.net|216.66.80.30
2016-09-06T11:27:33.000Z|_kerberos._tcp.Central-Office._sites.dc._msdcs.moscow.alfaintra.net|217.12.97.137
2016-09-06T19:26:27.000Z|_ldap._tcp.Central-Office._sites.moscow.alfaintra.net|217.12.97.137
2016-09-06T20:27:53.000Z|_ldap._tcp.Central-Office._sites.dc._msdcs.moscow.alfaintra.net|217.12.97.137
2016-09-09T20:53:29.000Z|mail.moscow.alfaintra.net|90.154.74.27
2016-09-18T18:57:12.000Z|vhipchatft.regions.alfaintra.net|95.143.192.211
2016-09-23T13:50:50.000Z|mail.trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-09-23T13:51:03.000Z|mail.trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-09-23T13:51:18.000Z|mail.trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-09-23T13:51:27.000Z|mail.trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-09-23T13:51:34.000Z|mail.trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-09-23T13:51:42.000Z|mail.trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-09-23T13:52:58.000Z|trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-09-23T13:52:59.000Z|mail.trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-09-23T13:53:07.000Z|trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-09-23T13:56:29.000Z|trump-email.com.moscow.alfaintra.net|217.12.97.137
2016-10-11T08:53:32.000Z|_ldap._tcp.Default-First-Site-Name._sites.alfaintra.net|62.140.253.2
2016-10-26T17:55:46.000Z|_ldap._tcp.gc._msdcs.alfaintra.net|62.140.253.2
2016-10-30T13:25:58.000Z|_kerberos._tcp.dc._msdcs.moscow.alfaintra.net|62.140.253.2
2016-10-30T21:20:37.000Z|_ldap._tcp.dc._msdcs.moscow.alfaintra.net|62.140.253.2
2016-10-30T21:27:53.000Z|_ldap._tcp.moscow.alfaintra.net|62.140.253.2

```

This query is unusual in that it merges two hostnames into one. It makes the most sense as a human error in inserting a new hostname in some dialog window, but neglected to hit the backspace to delete the old hostname.

Of course, this runon hostname doesn't exist; it's just two hostnames run together. Some 90 seconds later, the networks stopped talking about this host (at 2016-09-23T13:56:29.000Z), and further queries were not seen. But the brief minute life of the query associates the trump-email server to a new zone: the Alfa Bank intranet network.

The moscow.alfaintra.net is the internal LAN of AlfaBank. Like most careful organizations, the bank intranet is only resolved and reachable via a VPN (or by being inside the Bank's network of course). The internal LAN network contains ldap servers, a Microsoft Active Directory server, a HipChat server, a few Apple Caching Servers, some Microsoft Key Management Service (KMS) systems, etc.


The hybrid hostname suggests that Alfa was attempting to accommodate the Trump host in its network. After the 90-second "fat finger" event, the queries ceased as the record was corrected, and the targeted domain entered correctly.

NOT A CERTIFIED COPY

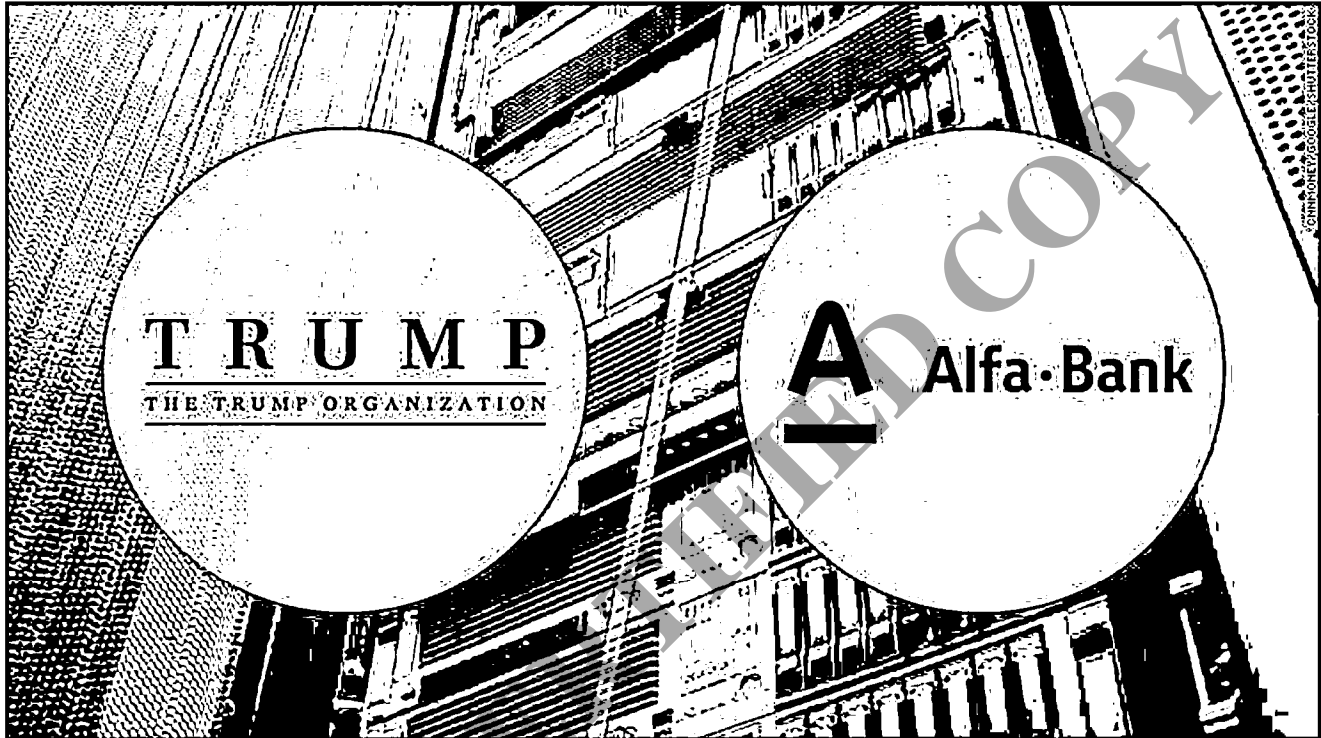
EXHIBIT 10

NOT A CERTIFIED COPY

Sources: FBI investigation continues into 'odd' computer link between Russian bank and Trump Organization

 cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/index.html

March 9, 2017



(CNN)Federal investigators and computer scientists continue to examine whether there was a computer server connection between the Trump Organization and a Russian bank, sources close to the investigation tell CNN.

Questions about the possible connection were widely dismissed four months ago. But the FBI's investigation remains open, the sources said, and is in the hands of the FBI's counterintelligence team -- the same one looking into Russia's suspected interference in the 2016 election.

One U.S. official said investigators find the server relationship "odd" and are not ignoring it. But the official said there is still more work for the FBI to do. Investigators have not yet determined whether a connection would be significant.

Read More

The server issue surfaced again this weekend, mentioned in a Breitbart article that, according to a White House official, sparked President Trump's series of tweets accusing investigators of tapping his phone.

CNN is told there was no Foreign Intelligence Surveillance Act warrant on the server. The FBI declined to comment. The White House did not respond to a request for

comment.

In addition, companies involved have provided CNN with new explanations that at times conflict with each other and still don't fully explain what happened.

The story -- of a possible connection between computer servers -- is a strange tale because there are no specific allegations of wrongdoing and only vague technical evidence.

Internet data shows that last summer, a computer server owned by Russia-based Alfa Bank repeatedly looked up the contact information for a computer server being used by the Trump Organization -- far more than other companies did, representing 80% of all lookups to the Trump server.

It's unclear if the Trump Organization server itself did anything in return. No one has produced evidence that the servers actually communicated.

Slate and The New York Times were first to report the unusual server activity.

The Times said the FBI had concluded there could be an "innocuous explanation." And cybersecurity experts told CNN this isn't how two entities would communicate if they wanted to keep things secret.

But for those who have studied the data, the activity could suggest an intent to communicate by email during a period of time when ties between the Trump Organization and Russia are being closely scrutinized because of Russia's alleged involvement in hacking the emails of the Democratic National Committee and Hillary Clinton campaign chief John Podesta.

This issue intrigued a dozen computer researchers at a recent business conference in Washington, D.C. that pulled together the world's top network operators, the ones who help run the internet. To them, it's a strange coincidence that merits further scrutiny.

Another computer researcher, Richard Clayton of Cambridge University, said it's just plain weird.

"It's not so much a smoking gun as a faint whiff of smoke a long way away. Maybe there's something else going on. It's hard to tell," said Clayton, who has independently examined the scant evidence available.

What is known:

Last year, a small group of computer scientists obtained internet traffic records from the complex system that serves as the internet's phone book. Access to these records is reserved for highly trusted cybersecurity firms and companies that provide this lookup service.

These signals were captured as they traveled along the internet's Domain Name System (DNS).

These leaked records show that Alfa Bank servers repeatedly looked up the unique internet address of a particular Trump Organization computer server in the United States. In the computer world, it's the equivalent of looking up someone's phone number -- over

and over again. While there isn't necessarily a phone call, it usually indicates an intention to communicate, according to several computer scientists.

What puzzled them was why a Russian bank was repeatedly looking up the contact information for mail1.trump-email.com.

Publicly available internet records show that address, which was registered to the Trump Organization, points to an IP address that lives on an otherwise dull machine operated by a company in the tiny rural town of Lititz, Pennsylvania.

From May 4 until September 23, the Russian bank looked up the address to this Trump corporate server 2,820 times -- more lookups than the Trump server received from any other source.

As noted, Alfa Bank alone represents 80% of the lookups, according to these leaked internet records.

Far back in second place, with 714 such lookups, was a company called Spectrum Health. Spectrum is a medical facility chain led by Dick DeVos, the husband of Betsy DeVos, who was appointed by Trump as U.S. education secretary.

Together, Alfa and Spectrum accounted for 99% of the lookups.

This server behavior alarmed one computer expert who had privileged access to this technical information last year. That person, who remains anonymous and goes by the moniker "Tea Leaves," obtained this information from internet traffic meant to remain private. It is unclear where Tea Leaves worked or how Tea Leaves obtained access to the information.

Tea Leaves gave that data to a small band of computer scientists who joined forces to examine it, several members of that group told CNN, which has also reviewed the data.

Possible explanations

The corporations involved have different theories to explain the server activity. But they haven't provided proof -- and they don't agree.

Alfa Bank has maintained that the most likely explanation is that the server communication was the result of spam marketing. Bank executives have stayed at Trump hotels, so it's possible they got subsequent spam marketing emails from the Trump Organization. Those emails might have set off defensive cybersecurity measures at the bank, whose servers would respond with a cautious DNS lookup. Alfa Bank said it used antispam software from Trend Micro, whose tools would do a DNS lookup to know the source of the spam.

Alfa Bank said it brought U.S. cybersecurity firm Mandiant to Moscow to investigate.

Mandiant had a "working hypothesis" that the activity was "caused by email marketing/spam" on the Trump server's end, according to representatives for Alfa Bank and Mandiant. The private investigation is now over, Alfa Bank said.

Computer scientists agree that such an explanation is possible in theory. But they want to see evidence.

Alfa Bank and Mandiant could not point to marketing emails from the time period in

question. "Mandiant has found evidence of an old marketing campaign, which... is too old to be relevant," Alfa Bank said in a statement.

CNN reached out to the Trump Organization with detailed technical questions but has not received answers.

Cendyn is the contractor that once operated marketing software on that Trump email domain. In February, it provided CNN a Trump Organization statement that called the internet records "incomplete" and stressed that they do not show any signs of "two-way email communication." That statement lends credibility to the spam marketing theory, because it says the Trump server was set up in 2010 to deliver promotional marketing emails for Trump Hotels. But Cendyn acknowledged that the last marketing email it delivered for Trump's corporation was sent in March 2016, "well before the date range in question."

Spectrum Health told CNN it "did find a small number of incoming spam marketing emails" from "Cendyn, advertising Trump Hotels." But it pointed to emails sent in 2015, long before the May-through-September 2016 time period examined by scientists. Spectrum Health said that it "has not been contacted by the FBI or any government agency on this matter." Having the Trump Organization server set up for marketing also doesn't explain why Alfa Bank and Spectrum would stand out so much.

"If it were spam, then a lot of other organizations would be doing DNS lookups. There would be evidence of widespread connectivity with devices," said L. Jean Camp, a computer scientist at Indiana University who has studied the data.

Cendyn has also provided another possible explanation, suggesting a highly technical case of mistaken identity.

Cendyn routinely repurposes computer servers -- like the one used by the Trump Organization.

Cendyn's software, like its event planning tool Metron, sends email and thus relies on the 20 different email servers rented by the company. After "a thorough network analysis," Cendyn has said that it found a bank client had used Metron to communicate with AlfaBank.com.

But Alfa Bank starkly denies "any dealings with Cendyn." And, it says, it's unlikely that it received any emails from that server. "Mandiant investigated 12 months of email archives and it found no emails to or from any of the IP addresses given to us by the media."

On Wednesday, Cendyn provided another explanation to CNN. Cendyn claims the Trump Hotel Collection ditched Cendyn and went with another email marketing company, the German firm Serenata, in March 2016. Cendyn said it "transferred back to" Trump's company the mail1.trump-email.com domain.

Serenata this week told CNN it was indeed hired by Trump Hotels, but it "never has operated or made use of" the domain in question: mail1.trump-email.com.

Upon hearing that Cendyn gave up control of the Trump email domain, Camp, said: "That does not make any sense to me at all. The more confusing this is, the more I think we need an investigation."

Other computer experts said there could be additional lookups that weren't captured by the original leak. That could mean that Alfa's presence isn't as dominant as it seems. But Dyn, which has a major presence on the internet's domain name system, spotted only two such lookups — from the Netherlands on August 15.

Alfa Bank insists that it has no connections to Trump. In a statement to CNN, Alfa Bank said neither it, bank cofounder Mikhail Fridman and bank president Petr Aven "have had any contact with Mr. Trump or his organizations. Fridman and Aven have never met Mr. Trump nor have they or Alfa Bank had any business dealings with him. Neither Alfa Bank nor its officers have sent Mr. Trump or his organization any emails, information or money. Alfa Bank does not have and has never had any special or exclusive internet connection with Mr. Trump or his entities."

Scientists now silent

The bank told CNN it is now trying to identify the person or entity who disseminated this internet traffic. "We believe that DNS traffic in mainland Europe was deliberately captured - in a manner that is unethical and possibly illegal -- in order to manufacture the deceit," it said.

Fear has now silenced several of the computer scientists who first analyzed the data. Tea Leaves refused to be interviewed by CNN and is now "hiding under a rock," according to an intermediary contact.

Paul Vixie, who helped design the very DNS system the internet uses today, was quoted in the Slate story saying that Alfa Bank and the Trump Organization "were communicating in a secretive fashion." Vixie declined to go on the record with CNN.

Even the skeptics have unanswered questions.

Robert Graham is a cybersecurity expert who wrote a widely circulated blog post in November that criticized computer scientists for premature conclusions connecting the Trump Organization and Alfa Bank.

But he's still wondering why Alfa Bank and Spectrum Health alone dominated links to this Trump server.

"It's indicative of communication between Trump, the health organization and the bank outside these servers," he told CNN. "There is some sort of connection I can't explain, and only they are doing it. It could be completely innocent."

EXHIBIT 11

NOT A CERTIFIED COPY

HERE'S THE PROBLEM WITH THE STORY CONNECTING RUSSIA TO DONALD TRUMP'S EMAIL SERVER

Sam Biddle, Lee Fang, Micah Lee, Morgan Marquis-Boire

November 1 2016, 3:51 p.m.



Photo: Vasily Fedosenko/Reuters/Newscom

On Monday night, Slate's Franklin Foer published a story that's been circulating through the dark web and various newsrooms since summertime, an enormous, eyebrow-raising claim that Donald Trump uses a secret server to communicate with Russia. That claim resulted in an explosive night of Twitter confusion and misinformation.

The gist of the Slate article is dramatic — incredible, even: Cybersecurity researchers found that the Trump Organization used a secret box configured to communicate exclusively with Alfa Bank, Russia's largest privately-held commercial bank. This is a story that any reporter in our election cycle would drool over, and drool Foer did:

The researchers quickly dismissed their initial fear that the logs represented a malware attack. The communication wasn't the work of bots. The irregular pattern of server look-ups actually

resembled the pattern of human conversation — conversations that began during office hours in New York and continued during office hours in Moscow. It dawned on the researchers that this wasn't an attack, but a sustained relationship between a server registered to the Trump Organization and two servers registered to an entity called Alfa Bank.

These claims are based entirely on “DNS logs,” digital records of when one server looks up how to contact another across the internet. The logs, first gathered by an anonymous researcher going by the moniker “Tea Leaves” (an irony that should be lost on no one) and shared with a small group of academics, were provided to The Intercept and a handful of other news organizations. The New York Times, the Washington Post, Reuters, the Daily Beast, and Vice all examined these materials to at least some extent and did not publish the claims.

You can think of DNS like a phone book that maps people's names to their phone numbers. For example, every time Alice wants to call Bob, she first looks up Bob's phone number in the phone book, and then she dials the number into her phone. However, it's possible that Alice might look up Bob's phone number and not call him on the phone. It's even possible that she might look up Bob's phone number over and over on a regular basis, over the course of months, without actually calling him. The DNS look-ups that The Intercept and others (including Slate) reviewed are similar to records of Alice looking up Bob's phone number in the phone book, but to call that evidence of sinister collusion between the two is, politely, a stretch. These DNS records alone simply cannot prove that any specific messages were sent at those times. In fact, they can't really prove anything at all, and certainly not “communication” between Trump and Alfa. This cannot be overstated: No one, not Tea Leaves, not his academic peers, and not Franklin Foer, can show that a single message was exchanged between Trump and Alfa.

Inconsistencies

Putting aside how little there actually is to read in these tea leaves, the information we reviewed was filled with inconsistencies and vagaries. The Intercept (and other outlets) were presented with three documents: an academia-style white paper about the server, an analysis of that white paper, and a sprawling dossier on Alfa Bank. The author of the analysis paper refused to comment on the record or allow his name to be published. Both Tea Leaves and the analysis author said they did not know who wrote the other documents, and would not say how they obtained them. Professor L. Jean Camp, an esteemed computer scientist quoted at length in the Slate piece and also interviewed by The Intercept,

said she knew the author of the Alfa Bank document — compiled with the exhaustive detail of a political oppo team, not a university researcher — but would not reveal who it was. Tea Leaves himself told The Intercept that he had to keep his identity and methods secret because “I run a cybersecurity company and I do not want DDOS and never have we been DDOS, nor do I want other attention.”

Looking at the documents themselves provided further oddities and errors. The white paper contends the following:

The Spectrum Health IP address is a TOR exit node used exclusively by Alfa Bank, i.e., Alfa Bank communications enter a Tor node somewhere in the world and those communications exit, presumably untraceable, at Spectrum Health. There is absolutely no reason why Spectrum would want a Tor exit node on its system.

This is simply untrue and easy to disprove using publicly available information: The Intercept confirmed that the IP address in question, and all other IP addresses on Spectrum Health's network, did not host a Tor node during the time period.

On Tea Leaves' WordPress site, he claimed that “only two networks resolved the mail1.trump-email.com host.” This is contradicted by the very works of analysis furnished by Tea Leaves' collaborators: The author of the white paper found that at least 19 IP addresses, all belonging to different networks except for the two that belong to Alfa Bank, had looked up Trump's server. And these are only the 19 the author was able to observe in a short time period — it can't be ruled out that there were many more, which quickly deflates the portrait of a shady Russian backchannel.

The white paper included DNS look-up data, but not nearly enough to reproduce the results. Rather than the 19 IP addresses we expected to see, the data only included three, and the DNS look-ups were not for the same time period that the paper described. Tea Leaves published a different set of data on the dark web, which we also looked at, but this set of data only included a total of four IP addresses. When we pressed Tea Leaves for the complete set of data so we could attempt to reproduce the analysis, he gave us a new, more comprehensive set of data, but still that included a total of only eight IP addresses, and it was missing an IP address belonging to a VPN service in Utah that accounted for a significant portion of the DNS look-ups described in the paper.

What percentage of DNS look-ups for Trump's email server could Tea Leaves and his colleagues observe, out of all DNS look-ups for that server on the whole internet? How can they be sure that the majority of DNS look-ups for Trump's email server originated from Alfa Bank, when

much of the data they collected didn't even include DNS look-ups from IPs described in their own paper? What's their margin of error? None of the analysis that we (and other journalists) obtained answered these questions.

The Simplest Explanation

Although the Slate article mentions Occam's Razor, Foer never actually takes seriously the simplest plausible explanation for all of this: The Trump Organization owns a bunch of expensive, obnoxious spam servers that churn out marketing emails for its expensive, obnoxious hotels. Spectrum Health, an entity in this story whose presence never made any sense, provided the following statement:

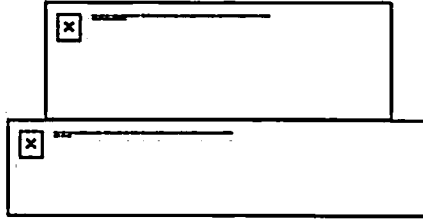
Our experts have conducted a detailed analysis of the alleged internet traffic and did not find any evidence that it included any actual communications (no emails, chat, text, etc.) between Spectrum Health and Alfa Bank or any of the Trump organizations. While we did find a small number of incoming spam marketing emails, they originated from a digital marketing company, Cendyn, advertising Trump Hotels.

Spectrum also provided us with something not even Tea Leaves could: a copy of an email sent from the mail1.trump-email.com server. Did it contain a Cyrillic cipher? Not quite:

NOT A CERTIFIED COPY

From: Trump Hotels <TrumpHotelCollection@contact-client.com>
Sent: Wednesday, November 25, 2015 11:49 AM
To:
Subject: Black Friday through Cyber Tuesday Suite Savings

[View this email in your inbox](#)



We invite you to experience signature
Trump luxury at a substantial savings.



Enjoy a 30% savings on all suite accommodations booked
November 27th through December 1st only, for all Trump Hotels
destinations.

In addition, for every reservation made during this time, Trump

Spectrum was kind enough to include the email's header data, which
shows its origin:

Received: from bl-mail2.spectrumhealth.org (167.73.114.24) by
 DVMSHTS03.Spectrum-Health.org (10.200.26.36) with Microsoft SMTP Server (TLS)
 id 14.3.266.1; Wed, 25 Nov 2015 12:01:00 -0500

Received: from s12p02m073.mxlogic.net (unknown [208.65.145.246]) by
 bl-na-mail-dc-3.spectrum-health.org with smtp (TLS:
 TLSv1/SSLv3,256bits,DHE-RSA-AES256-GCM-SHA384) id
 091a_f27c_24aee326_2e91_463c_a716_6052ff08b7fe; Wed, 25 Nov 2015 12:00:58
 -0500

Authentication-Results: s12p02m073.mxlogic.net; spf=pass

Received: from unknown [66.216.133.29] (EHLO mail.trump-email.com) by
 s12p02m073.mxlogic.net(mxlm_mta-8.5.0-3) with ESMTP id:
 949e5565.0.5617971.00-2266.11108474.s12p02m073.mxlogic.net (envelope-from
 <2oq0np1u8535af2t0b59cko4s3bdicb5ve1r30qv0jooocfo8q0ov52gnltk02ld@b.contact-client.com>);
 Wed, 25 Nov 2015 10:00:57 -0700 (MST)

DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=key1; d=contact-client.com;
 h=List-Unsubscribe:MIME-Version:From:To:Date:Subject:Content-Type:Content-Transfer-Encoding:Message-ID;

i=TrumpHotelCollection@contact-client.com;

bh=HA1FqVes2qzZ5anIKZbcwlHRtZk=;

b=hKd1pZgUhGXA2uyEXrh3+5uExsKpKdpHYFauGAVnsoox819sJKOZZ/Of2/f3tpHujAguW3jogw65
 8ElnWmTR1ZdJrdHUfcXfBKfpBlkQSOyPshh4idGQLgYtGQeQyj54YkJoCs82RfOu4HMnuDpN3DqR
 yOfeoT6gPw7Dqmal9TM=

Received: by mail.trump-email.com id hanl161n70kr for
 ; Wed, 25 Nov 2015 11:52:12 -0500
 (envelope-from

Alfa Bank provided the same:

Inspirational Travel & Exciting Savings



Trump Hotel Collection <TrumpHotelCollection@contact-client.com>
Thursday 4 February 2016 at 17:23
An: [REDACTED]@alfabank.ru

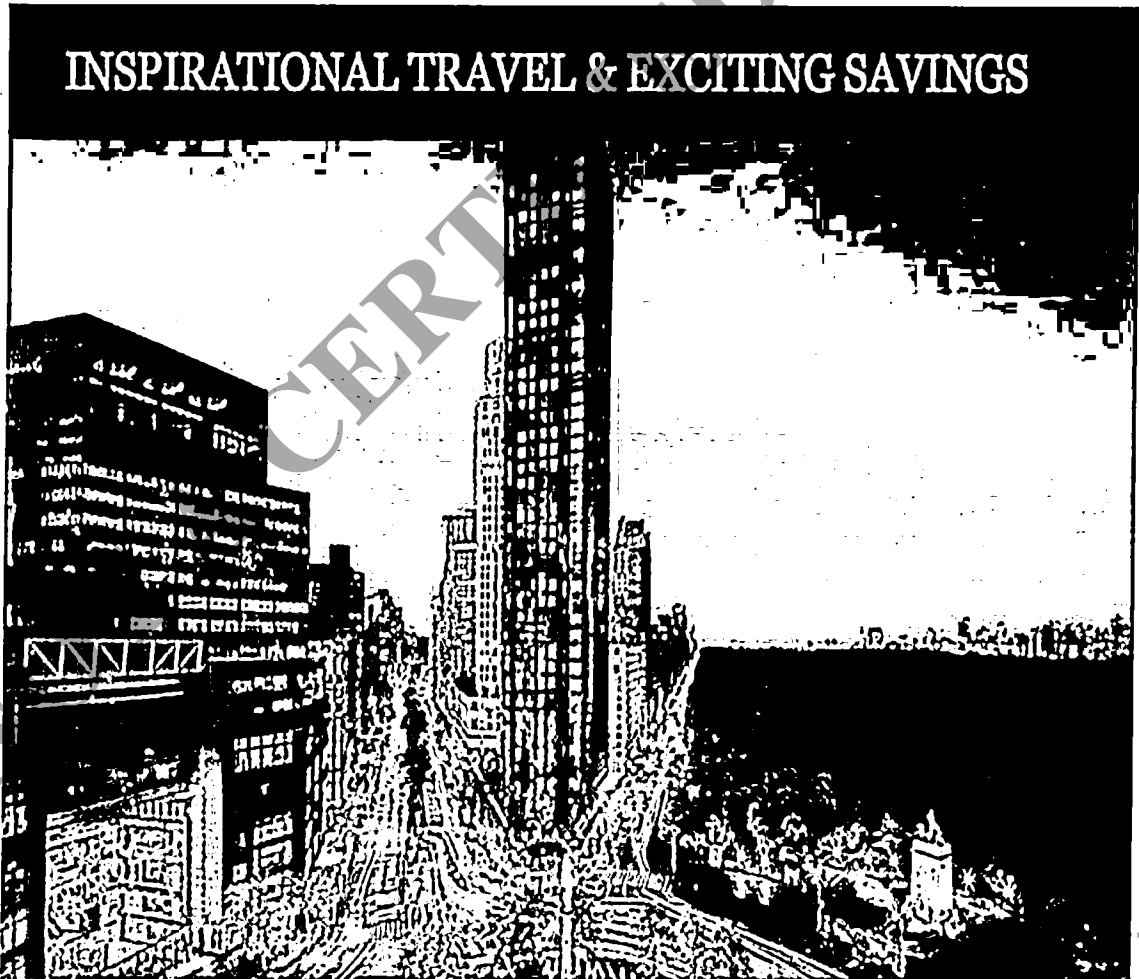
[View this email with images](#)

TRUMP HOTELS™

February 2016

LIVE THE LIFE.

ISSUE 76



Now, these emails are from outside the time period observed by Tea Leaves et al. and only represents one data point. On the other hand, we

now have one checkmark in the “this is just some dumb spam server” column, and zero in the “this is a hotline to Putin’s bedroom” column. Mandiant, a cybersecurity firm Alfa Bank hired to investigate the DNS logs once reporters came knocking, provided another deeply plausible explanation: All of the look-ups were the result of Alfa’s mail servers trying to figure out who was spamming them so much.

The information presented is inconclusive and is not evidence of substantive contact or a direct email or financial link between Alfa Bank and the Trump Campaign or Organization. The list presented does not contain enough information to show that there has been any actual activity opposed to simple DNS look-ups which can come from a variety of sources including anti-spam and other security software.

Security researcher Rob Graham points out that it’s a stretch to even claim that this server is truly “Trump’s”:

The evidence available on the internet is that Trump neither (directly) controls the domain “*trump-email.com*,” nor has access to the server. Instead, the domain was setup and controlled by Cendyn, a company that does marketing/promotions for hotels, including many of Trump’s hotels. Cendyn outsources the email portions of its campaigns to a company called Listrak, which actually owns/operates the physical server in a data center in Philadelphia. ...

... When you view this “secret” server in context, surrounded by the other email servers operated by Listrak on behalf of Cendyn, it becomes more obvious what’s going on. In the same internet address range of Trump’s servers you see a bunch of similar servers, many named [*client*]-*email.com*. In other words, *trump-email.com* is not intended as a normal email server you and I are familiar with, but as a server used for marketing/promotional campaigns.

Paul Vixie, quoted throughout the Slate story, is a legendary figure in the history of the internet whose expertise is near unparalleled when it comes to DNS. But even Vixie conceded to The Intercept that Tea Leaves’ evidence was conclusive of nothing: “It’s a perfect he-said, she-said situation. ... Mandiant is guessing no. I am guessing yes. Neither of us has direct evidence.”

There are other, non-technical issues with the Foer piece. For one, the political connections between Trump and Alfa Bank are presented to the reader by highlighting the relationship between Trump and Richard Burt, a consultant who drafted a Trump campaign speech. Burt, Foer charges, “serves on Alfa’s senior advisory board.” Burt has indeed

worked for years as an adviser to Alfa Bank and its founder, Mikhail Fridman. But he no longer serves on the board of Alfa Capital Partners, the Moscow-based fund associated with Alfa Bank. That company closed shop over a year ago. Foer made the same allegation in another piece published by Slate in July.

Could it be that Donald Trump used one of his shoddy empire's spam marketing machines, one with his last name built right into the domain name, to secretly collaborate with a Moscow bank? Sure. At this moment, there's literally no way to disprove that. But there's also literally no way to prove it, and such a grand claim carries a high burden of proof.

Without more evidence it would be safer (and saner) to assume that this is exactly what it looks like: A company that Trump has used since 2007 to outsource his hotel spam is doing exactly that. Otherwise, we're all making the exact same speculation about the unknown that's caused untold millions of voters to believe Hillary's deleted emails *might have contained* Benghazi cover-up PDFs.

Given equal evidence for both, go with the less wacky story.

Top photo: The logo of Alfa Bank is visible on a building in Minsk, Belarus, on June 19, 2016.

Update: November 1, 2016 This article has been updated to clarify Alfa Bank's status as the largest private commercial bank.

NOT A CERTIFIED COPY

EXHIBIT 12

NOT A CERTIFIED COPY

Trump's Russian Bank Account

gdd53.wordpress.com/2016/10/05/first-blog-post/

leavestea

October 5, 2016

Trump and Russia's largest private bank communicated via a hidden server since at least 2016 May. The RData for this host were served by the Central Dynamics (CC-801) authority resolvers ns{1,2,3}.cdcservices.com:

```
$ORIGIN trump-email.com.
```

```
$TTL 3600
```

```
trump-email.com. IN TXT "Internet Solution from Cendyn.com."
```

```
trump-email.com. IN TXT "v=spf1 ip4:198.91.42.0/23  
ip4:64.135.26.0/24 ip4:64.95.241.0/24 ip4:206.191.130.0/24  
ip4:63.251.151.0/24 ip4:69.25.15.0/24 mx ~all"
```

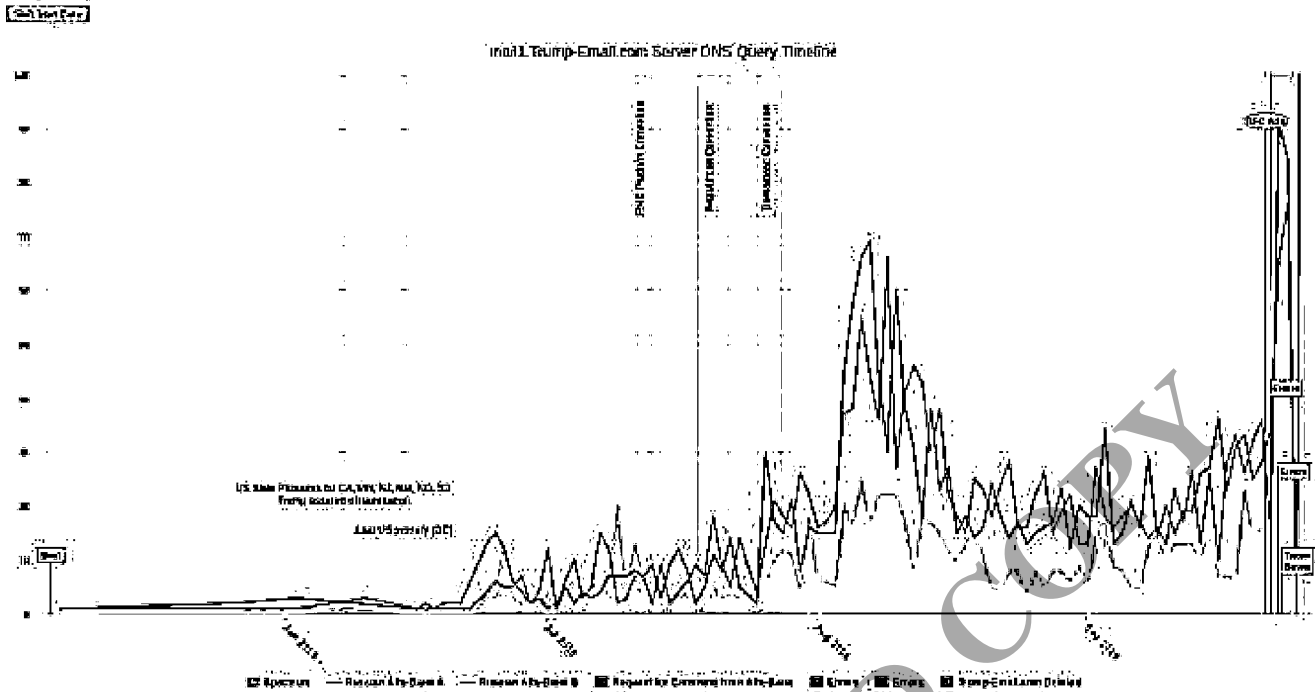
```
trump-email.com. IN SOA ns1.cdcservices.com.  
postmaster.centraiservices.local. (2012062509 1200 120 1209600  
3600);
```

```
mail1 IN A 66.216.133.29 ;
```

Trump's host mail1.trump-email.com operated a Listrak virtual mail transfer agent outside the SPF sending range, configured for outbound delivery. Hosts receiving mail from Trump's host would validate the forward and reverse, causing DNS lookups.

Since May of 2016 only two networks resolved the mail1.trump-email.com host, AS15632 (JSC Alfa-Bank) and AS30710 (Spectrum Health).

Alfa Bank is Russia's largest bank and Spectrum Health is a integrated, managed care health care organization in Michigan.



These forward lookups come from Tea's eepsite <http://gdd.i2p> and match the reverse resolutions.

яркий

When a reporter called Alfa Bank for comment on September 21, the zone for mail1.trump-email.com was removed from ns1 and ns3.cdcservices.com causing RCODE=2 (Server Failure), and ns2 returned empty referrals. Since mail1 was unresolvable, Trump renamed the host to trump1.contact-client.com on October 27. The first host iterating for this domain was Alfa Bank on 2016-09-27 at 19:48 hours:

```
"ts": "1475005735",
"src_ip": "217.12.97.15",
"qname": "trump1.contact-client.com",
"node_id": "ams-ix23",
"qdcount": 1,
"qtype": 1,
"rd": 0
```

But the hostname trump1.contact-client.com appeared in the first passive DNS database three days later, and still has not appeared in some passive collections.

RRset results for **trump1.contact-client.com./ANY**

Returned 1 RRsets in 0.07 seconds.	
baillwick	contact-client.com.
count	2
first seen	2016-09-30 11:24:34 -0000
last seen	2016-09-30 11:24:34 -0000
trump1.contact-client.com.	A 66.216.133.29

В тихом омуте черти водятся

Alfa Bank knew that Trump renamed his host through ongoing email delivery and HELO/EHLO resolutions, or another channel. Trump and Alfa Bank have since coordinated their move to an office communications channel.

- Only Trump, Spectrum and Alfa Bank used the mail server.
- All other Trump messages went through normal delivery.
- When Alfa Bank was asked, Trump immediately changed his server name...
- ... and Alfa Bank knew the new hostname immediately, before anyone.

Trump has active business with a Russian bank. More on Tea's site.

NATO fought the Cold War and kept Europe free. Does this account explain why the US now debates whether to surrender a war it has already won?



EXHIBIT 13

NOT A CERTIFIED COPY

Menu ☰

✱ THINKING ABOUT THE HORIZON

POLITICS

Trump's Server, Revisited

Sorting through the new evidence, and competing theories, about the Trump server that appeared to be communicating with a Russian bank.

By FRANKLIN FOER
NOV 02, 2016 • 8:36 PM

TWEET

SHARE

COMMENT





Republican presidential nominee Donald Trump at a campaign rally at Macomb Community College South Campus in Warren, Michigan, on Monday.

Chip Somodevilla/Getty Images

On Monday, I published a reported piece that raised questions about a server owned by the Trump Organization. The server appeared to be unusually configured, and to communicate almost exclusively with two servers registered to Alfa Bank in Moscow. The piece followed a group of computer scientists who had stumbled upon the Trump server in July, and it told the story of how they deployed their expertise to make sense of their discovery.

The story required voyaging deep into the arcana of the internet. The key piece of evidence for the server's strange behavior was a set of logs of Domain Name Server, or DNS, look-ups. These are the communications between servers that enable an email to reach its destination. The computer scientists had no actual examples of email exchanged between Trump and Alfa—only inferences about that prospect, based on their close reading of the logs. I spoke with many DNS experts. They found the evidence strongly suggestive of a relationship between the Trump Organization and the bank but not conclusive. It was a subject that I believed deserved public airing and further exploration.

Publication of my article was quickly followed by responses from the Trump campaign and Alfa Bank, both of which offered more detailed accounts of the server activity than they had provided when I'd asked them for comment. My piece also elicited a series of valuable objections

and credible alternate theories from technology reporters and other computer scientists. I take these seriously and believe they also deserve public airing and exploration. Several of the critiques of the hypothesis offered by the experts in my piece offer simpler, more benign explanations for the server activity. I'll describe them here.

1) Does Trump control the server in question?

In a detailed post critiquing my piece, cybersecurity expert Rob Graham wrote, "The evidence available on the Internet is that Trump neither (directly) controls the domain trump-email.com, nor has access to the server." This echoes the point raised by Vox, the Intercept, and others that the server was not operated by the Trump Organization directly. Rather, it was run and managed by Cendyn, a vendor that organizes email marketing campaigns for hotels and resorts. This suggests that most of the emails that emanated from this address were mass emails, related to loyalty programs, discount offers, and the like. At first, Trump spokeswoman Hope Hicks told me the server "has not been used since 2010." She continued, "To be clear, The Trump Organization is not sending or receiving any communications from this email server." The Intercept has since turned up at least two examples of a Trump email, promoting hotels, being sent from that server in 2015 and 2016.

NOT A CERTIFIED COPY

Critics were right to focus on the relationship with Cendyn as a weak point in the theory. None of the computer scientists in my original story has an evidence-based explanation for why anyone at the Trump Organization would have used *this* server for the purposes of communicating with Alfa. The contention was that Cendyn is an organization trusted by the Trump Organization to host email. But clearly there would be easier ways to go about maintaining a quiet channel of communications than to work through a server operated by a vendor.

One of the intriguing facts in my original piece was that the Trump server was shut down on Sept. 23, two days after the *New York Times* made inquiries to Alfa Bank (and a week before the *Times* reached out to Trump). Was Cendyn acting on Trump's behalf when it shut down mail1.trump-email.com? I can't say for sure. (Cendyn didn't reply to my request for comment.) This may all be pure coincidence. Perhaps Cendyn shut down the server for bureaucratic reasons, such as Trump's failure to renew it, or perhaps Cendyn shut down the domain for very good technical reasons. "They may have shut it down to do a forensic analysis. Or they may have thought, in response to the inquiry, that the server was infected. It may actually have been infected," Cornell University's Emin Gun Sirer told me on Wednesday. Neither the Trump campaign nor Cendyn has offered an explanation for the shutting down of mail1.trump-email.com.

NOT A CENEDYN COPY

2) Could the communication with Alfa have been spam or marketing email?

In the statements they released after the publication of my piece, the Trump campaign and Alfa Bank provide different explanations for the DNS look-ups. According to Alfa, they were likely the result of its security systems furiously swatting away spam being sent by the Trump server. According to Trump, another Cendyn client, a bank, was using its servers to operate a “meeting management” application that allowed it to coordinate meetings with Alfa. The Trump campaign statement doesn’t name the bank. It’s strange that Cendyn would allow another client to use the Trump-owned servers, though it’s certainly possible. It’s also strange that investigators from Mandiant, the cybersecurity firm hired by Alfa to investigate, wouldn’t have easily found evidence of the meeting application and declared the case closed.

Was the server sending spam—unsolicited mail—as opposed to legitimate commercial marketing? There are databases that assiduously and comprehensively catalog spam. I entered the internet protocol address for mail1.trump-email.com to check if it ever showed up in Spamhaus and DNSBL.info. There were no traces of the IP address ever delivering spam. Perhaps the spam went uncataloged because it was being sent to a single bank in Russia, but L. Jean Camp, an Indiana University computer scientist and a source in my original story, thought that possibility unlikely. “It’s highly implausible that spam would continue for so many months, that it would never be reported to spam blocker, or that nobody else in the world would see the spam during that time frame,” she told me.

More likely, the Trump server was sending marketing material, like the emails the *Intercept* found from 2015 and 2016. Again, Hope Hicks says the Trump Organization no longer uses that server—and she denied the existence of any email sent to Alfa. It's certainly possible that the campaign isn't fully aware of every piece of internet marketing being dispersed by the Trump Organization. Or perhaps Cendyn sent mail on Trump's behalf by mistake.

Still, the marketing email theory has a few holes. A typical marketing campaign would involve the wide distribution of emails, spreading word of discounted prices and hotel openings far and wide. It seems unlikely that a campaign would so exclusively focus its efforts on a bank in Russia and a health care company in Michigan (which received a small batch of DNS look-ups), even if, as one critic has claimed, executives from Alfa Bank had a penchant for staying in Trump hotels. Again, there may be some perfectly innocuous explanation for this strange behavior. Naadir Jeewa, a consultant who works with systems similar to the ones discussed in the piece, has suggested, "One of the main reasons I discounted malfeasance is that email systems are terrible. ... [T]he fact that it still works is because of decades of workarounds and hacks to make it marginally secure. And they go wrong, all the time."

3) Was it a closed server?

Another reason the computer scientists in my piece found the server unusual is that it appeared to be configured in such a way to restrict access to all but a few communicants. Several reporters and news outlets have countered by saying, in essence, that the server was “not quite as shut off from the rest of the web as it seems.” But we know of only three parties that received messages from the server, the vast bulk going to Alfa Bank. (The *Intercept* correctly notes that 19 IP addresses had looked up the Trump address. This is an unusually small number, and most of the look-ups consisted of IP addresses registered as purveyors of malware. The *Intercept* also contends that the 19 look-ups might not be a complete list; more on that below.) The scientists theorized that the Trump and Alfa Bank servers had a secretive relationship after testing the behavior of mail1.trump-email.com using sites like Pingability. When they attempted to ping the site, they received the message “521 lvpmta14.lstrk.net does not accept mail from you.” It’s possible to impose restrictions—or, in the case of Cendyn’s system, create an access control list—to carefully regulate the number of communicants. We can’t be sure that any of these restrictions were deployed.

ADVERTISEMENT

You May Like

Sponsored Links by Taboola

New Portable AC Takes United States by Storm

WearableAC

She Made A Fortune From Commercials Alone

BrainSharper

Premium Masks with 3 Nanotech Layers. Free Same Day Shipping....

Space Masks

And as the Verge's Russell Brandom pointed out, this approach to communication would hardly remain secret forever: "If the servers were only meant to talk to each other, why not connect directly, storing the IP-domain link locally and skipping public domain registration entirely? Failing that, why not use a shared email account or any of dozens of private messaging services that leave less of a metadata trail? There are plenty of hard problems in building untraceable chat systems, but avoiding incriminating DNS records isn't one of them."

4) Does the conversation spike around political events?

Vox's Timothy Lee and others have questioned the contention of the computer scientists that traffic between the servers correlated with political happenings in the U.S. "There's a much smaller spike during the Democratic convention and no apparent increase before or during the Republican convention," he noted. "In short, this chart seems to be totally unrelated to the political calendar." He wonders why the largest spike occurs in August, after the party conventions. This happened to be a moment of potential interest in Russia, since those weeks were the denouement of the Paul Manafort era in the Trump campaign, with the exposure of logs showing he received \$12.7 million in off-the-book payments from the Putin-backed Party of Regions. But Lee's fundamental response is understandable: The chart shows possible correlations, not proven causation.

5) Are the DNS logs complete?

The Intercept also looked into this story and decided not to pursue it. One reason was that it doubted my source possessed an unabridged set of DNS logs: “What percentage of DNS look-ups for Trump’s email server could Tea Leaves and his colleagues observe, out of all DNS look-ups for that server on the whole internet? How can they be sure that the majority of DNS look-ups for Trump’s email server originated from Alfa Bank, when much of the data they collected didn’t even include DNS look-ups from IPs described in their own paper? What’s their margin of error? None of the analysis that we (and other journalists) obtained answered these questions.” As I noted in my piece, there’s no foolproof way to verify that these logs are complete and unedited. I believe in their authenticity, because of the credibility of the academics and programmers who vouched for them by name—specifically, Paul Vixie and Jean Camp. They took a meaningful risk in attaching their names to the data. Jean Camp has posted the full set of logs. Now that they are easily available, others can form their own opinion as to their validity and what they demonstrate about the servers.

NOT A

I pursued this story because I was impressed by the emphatic belief of the experts I consulted, my suspicions were raised by the evidence they presented, and I thought I would be remiss if I sat on data that I believed deserves to be evaluated and understood before we elect the next president. The underlying context for the piece is that Donald Trump has cultivated a troubling relationship with Russia, and the U.S. government has identified Russia as trying to meddle in this election. Not every nexus between the candidate and Russia is nefarious. This one might well be entirely innocent or even accidental. As the *New York Times* reported on Tuesday, after my story published, the FBI looked into the server activity but “ultimately concluded that there could be an innocuous explanation, like a marketing email or spam, for the computer contacts.” Or maybe it’s less than innocent, as the computer scientists suggested and still believe. (I’ve checked back with eight of the nine computer scientists and engineers I consulted for my original story, and they all stood by their fundamental analysis. One of them couldn’t be reached.) I concluded my account of these scientists’ search for answers by arguing that the servers and their activity deserved further explanation. Hopefully my story and the debate that has followed will move us closer to a fuller understanding.

[Tweet](#)[Share](#)[Comment](#)

2016 Campaign

Donald Trump

NOT A CERTIFIED COPY

YOU MAY LIKE

New Portable AC Takes United States by Storm

WEARABLEAC |

Sponsored

.....

She Made A Fortune From Commercials Alone

BRAINSHARPER |

Sponsored

.....

Premium Masks with 3 Nanotech Layers. Free Same Day Shipping. Get Yours

SPACE MASKS |

Sponsored

If You Drink Wine More Than Twice a Week You Need This S...

Firstleaf |

Sponsored

The Most Beautiful Sideline Reporters Ever

Sportinal |

Sponsored

See Who's on eharmony in New York

eharmony |

Sponsored

New York : Launches New Policy For Cars Used Less Than 59 Miles/Day

Bill Cruncher |

Sponsored

New Wearable AC is Selling Out Fast in United States

Blaux Wearable AC |



Sponsored

KN95 Masks Restocked. Guaranteed 7 Days Shipping

Stratton Medical Supply |

Sponsored

Internet Taking Forever To Load? Try This WiFi Hack!

SuperBoost |

Sponsored

Most Windows Users Don't Know This (Do It Today)

Total AV |

Sponsored

Most Computer Owners Don't Know This (Do It Today)

Security Savers Online |

Sponsored

Parker Schnabel's Net Worth Left His Family In Tears

Travel Patriot |

Sponsored

50 Disposable Masks \$26.95, 100 Gloves \$8.95

Online Stores LLC |

Sponsored

Man Turns Old Airplane Into His Home; Look When He Opens The Door And Reveals The Inside

Crowdy Fan |

Sponsored

Are you over 12? Then you must absolutely try this game

Plarium - Raid Shadow Legends |

Sponsored

Innovative Mask Is Flying Off The Shelf- Get Yours Now

Sponsored

New Senior Living Apartments Near New York Are A Dream ...

Senior Living/Assisted Living |

Sponsored

Yrump News de las 24 horas en español en línea y en vídeo en español Miami Herald: Hot Breaks Own Twitter...

Remember When Shawn Johnson Won Three Silvers At The Oly...

Sportinal |

Sponsored

Buy 2 Boxes Get 1 Free: Disposable Face Masks

Stratton Medical Supply |

Sponsored

The App That's Teaching Millennials Spanish in Just 3 ...

Babbel |

Sponsored

NOT A CERTIFIED COPY



Reprints	Work with us	FOLLOW US
Advertise: Site / Podcasts	Send us tips	Facebook
Commenting	User agreement	Twitter
Podcast FAQs	Privacy policy	Instagram
Contact / Feedback	AdChoices	RSS Feed
Pitch guidelines	Slate Shop	
Corrections	Do Not Sell My Personal	
About us	Information	

Slate is published by The Slate Group, a Graham Holdings Company.
All contents © 2020 The Slate Group LLC. All rights reserved.

NOT A CERTIFIED COPY

EXHIBIT 14

NOT A CERTIFIED COPY

Some Network Data

The first round of letters

[Alfa Bank Threat Letter](#)

[Jean Response](#)

The second round of letters

[Alfa Bank Second Letter](#)

[Second Legal Response](#)

After these letters Alfa Bank sent a [third letter](#), which asked, "...we should be most grateful if you would provide specific answers to the following questions:". The only answer would have been an unequivocal refusal. As we did not answer privately, I did not post publicly until now. I thought this might be the end of the matter. In case there is confusion, my answer is, "No".

However, at the same time Alfa Bank was sending the letter above, they also were pursuing a public records request with Indiana University. Please note that Indiana University does not have access to all the email accounts they request. The other parties in this letter come not from any investigations or factual requests, but rather from unsubstantiated assertions by people with zero knowledge of matter. As far as I can tell, Alfa Bank selected these names from random stangers on Twitter and Reddit. Here is the [Alfa FOIA request](#)

This is an ongoing investigation within Alfa Bank according to Alfa Bank. They are requested data and assistance. It is true that there was inconsistent self-contradictory documentation of a facile investigation. The letters above clearly state that the Alfa Bank investigation is continuing.

Here for a special engagement is data that consists of DNS look-ups and public information about Trump email server and Alfa bank. I believe it indicates a nexus of communication worthy of further investigation. It also appears to be human interaction, based on timing.

Initial Text Files

Text Files

Here are data files for you to examine. [DNS Lookups For mail1.trump_email.com](#)

[Log Of DNS Lookups For mail1.trump_email](#)

[PTR Contains Trump](#)

[Trump And Mail MTA Relay Etc](#)

[Trump Domains Registered](#)

[Trump Owned And Mail System](#)

[Trump Owned And Mail Systems WHOIS](#)

Five Months of Text Files

[README.txt](#)

[ns1_cdcservices_com.log](#)

[ns2_cdcservices_com.log](#)

[ns3_cdcservices_com.log](#)

[167.73.110.8.whois](#)

[198.91.42.242.whois](#)

[217.12.96.15.whois](#)

[217.12.97.137.whois](#)

[217.12.97.15.whois](#)

[66.216.133.29.whois](#)

[contact-client.com.whois](#)

[trump-email.com.whois](#)

Secret Connection?

Here is an [explanation of the use of the word secret](#).

Here is an [explanation of the use of the word connection](#).

I hope these prove clarifying.

This sentence is my warrant canary.

Graph

Here is a [partial graph of the data](#).

Ethical Considerations

It is almost always reasonable to demand that someone who has made a decision that affects another explain their underlying decision process. Since an article by Sam Biddle, and comments by Chris on twitter, I decided that being closed about the data but disclosing opinions is the worst possible outcome. So I posted the data after the first discussions in October. There has since then been no reason to remove it.

In this case, the first task was to look for anomalies. Given the reports of Russian engagement in the election looking at the interaction between campaign sites and Russia is unquestionably ethical. (The decision by the majority of journalists to refuse to report on this connection until after the election should also be evaluated and explained by those journalists.)

However, once these data are found, what then? I am generally a fan of risk-based disclosure. What is the potential harm of the data? What is the value of transparency? If the servers were infected in any way, then the disclosure (one that inherently includes the vendor) resolved the issue. If not, and this was purposeful communication, then the ethical challenge becomes difficult. In general, researchers are responsible NOT to identify criminal activity unless a person is at risk (e.g., child abuse must be reported, substance abuse cannot). In contrast, network operators are responsible specifically TO identify criminal and malicious activity. In security, disclosure is the default. In medicine, disclosure is the anomaly. The law is clear. Decisions are primarily driven by contractual considerations. Individual responsibility is less clear.

The release by Trump of either server data or financial/tax data could mitigate any concerns and be very much in line with democratic processes. When I initially saw this, it was September, and there was not the October surprise issue there was at initial publication. Since the election there has been a consistent concern.

In summary, this release is ethical based on these standards: 1) The data were collected during normal network operations, this was not a targeted hostile search nor research. 2) Any people I brought in this discussion were given full context and all the data in my possession. 3) Any harm by the release could be easily mitigated by the party at potential risk. 4) None of the data were in any way classified nor secret. And, finally, 5) there is a value to openness and to the disclosure. In this case, not disclosing would be to self-censor.

Since that time I have been under non-trivial pressure to self-censor. Thus, it is critical that these data remain available.

EXHIBIT 15

NOT A CERTIFIED COPY

EXECUTIVE SESSION

COMMITTEE ON THE JUDICIARY,

JOINT WITH THE

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT,

U.S. HOUSE OF REPRESENTATIVES,

WASHINGTON, D.C.

INTERVIEW OF: JAMES A. BAKER (DAY 2)

Thursday, October 18, 2018

Washington, D.C.

The interview in the above matter was held in Room 2141, Rayburn House Office Building, commencing at 10:01 a.m.

Present: Representatives Meadows, Jordan, Ratcliffe, and Gaetz.

did I -- oh, right here they are.

This is a footnote from the House Intelligence Committee's report. I just want to walk you through it.

Mr. Baker. Could I get one?

Thank you.

Mr. Jordan. I'm looking at footnote 43.

Mr. Baker. Okay. I've read through it.

Mr. Jordan. Okay. So in September 2016, redacted, shared similar information, whatever's above the large block of redacted information -- shared similar information in a one-on-one meeting with FBI General Counsel James Baker.

Is the redacted name there, is that Mr. Sussmann?

Mr. Baker. I don't know what's behind the redactions. I'm sorry.

Oh, in this? I would -- I'm sorry. In that September 2016?

Mr. Jordan. Yeah.

Mr. Baker. Yeah. I was talking about all the blackout above that.

Mr. Jordan. Yeah. No, I'm not asking about that.

Mr. Baker. I would guess, from -- my assumption is, from the context, that that's Sussmann.

Mr. Jordan. Yeah. That's what I think too.

And then as conveyed in an executive session December 18 of, blank, around the same time as the meeting with the FBI, blank shared the information with journalists, including a name at Slate Magazine.

COMMITTEE SENSITIVE

Follow all that? And, again, this is -- the redaction is Mr. Sussmann -- the two smaller redactions.

Mr. Baker. It seems like that, yes.

Mr. Jordan. Okay. First of all, why was it redacted? Did you -- the FBI do this?

Mr. Baker. You have to ask the Bureau. I don't know. I didn't participate in that process, to my recollection.

Mr. Jordan. Yeah, I don't know why that would be redacted.

Okay. And then it says Slate, who published at a Trump service communication with Russia, published an article that was titled, Was a Trump Service Communicating with Russia, on Slate Magazine October 31st, 2016.

I'm just curious, did you happen to read that article?

Mr. Baker. No, I did not.

Mr. Jordan. Okay. Do you know anything about what the article said? Have you read it since then?

Mr. Baker. I have not read the Slate article, no.

Mr. Jordan. It talks about some bank in Russia, Alfa-Bank, communicating with some Trump financial institutions in the server there.

None of that kind of conversation was related to you by Mr. Sussmann when you met?

Mr. Baker. Oh, yes. I mean, that is what he told me about. Yeah, absolutely.

Mr. Jordan. Okay. So -- well, tell me more about that.

COMMITTEE SENSITIVE

COMMITTEE SENSITIVE

Mr. Baker. I didn't read the Slate article, but Sussmann told me that that's, in essence, what this was all about.

Mr. Jordan. Okay. We'll go into more detail about that, because I think the last time we talked, you just said it was something about some hacking. We didn't get into what it was hacking about.

So what did Mr. Sussmann tell you?

Mr. Baker. So now I'm nervous that maybe the last time the FBI interposed an objection, so --

Mr. [REDACTED] May we consult very quickly?

I know you're on a tight clock.

Mr. Jordan. Yep.

[Discussion off the record.]

Mr. Baker. So if the question is what did Sussmann tell me?

Mr. Jordan. Yeah.

Mr. Baker. Okay. And given the guidance I just got from the FBI, so I'll answer this at a somewhat high level.

So he was describing a -- what appeared to be a surreptitious channel of communications -- communication between some part of President Trump's, I'll say organization but it could be his businesses. I don't mean like The Trump Organization, per se. I mean his enterprises with which he was associated. Some part of that and a -- an organization associated with -- a Russian organization associated with the Russian Government -- a private organization associated with the Russian --

Mr. Jordan. Private organization in Russia associated with the

COMMITTEE SENSITIVE

government had some kind of electronic communication with some organization, some business associated with the Trump family or the Trump organization?

Mr. Baker. Yes, sir. And there was some effort -- there was some belief that this was a -- being conducted in a way so as to make it a covert communications channel.

Mr. Jordan. Okay. And my first question would be how'd you get this? Did you ask that question?

Mr. Baker. I did ask that question at a high level, yes. And he explained that he had obtained it from, again, cyber experts who had -- who had obtained the information, and he said that the details of it would explain themselves. That's my recollection.

Mr. Jordan. And was he representing a client when he brought this information to you? Or just out of the goodness of his heart, someone gave it to him and he brought it to you?

Mr. Baker. In that first interaction, I don't remember him specifically saying that he was acting on behalf of a particular client.

Mr. Jordan. Did you know at the time that he was representing the DNC in the Clinton campaign?

Mr. Baker. I can't remember. I have learned that at some point. I don't -- as I think I said last time, I don't specifically remember when I learned that. So I don't know that I had that in my head when he showed up in my office. I just can't remember.

Mr. Jordan. Did you learn that shortly thereafter if you didn't know it at the time?

Mr. Baker. I wish I could give you a better answer. I just don't remember.

Mr. Jordan. I mean, I just find that unbelievable that the guy representing the Clinton campaign, the Democrat National Committee, shows up with information that says we got this, and you don't ask where he got it, you didn't know how he got it. But he got it from some, you know, quote, expert.

Mr. Baker. Well, if I could respond to that.

Mr. Jordan. Sure.

Mr. Baker. I mean, so I was uncomfortable with being in the position of having too much factual information conveyed to me, because I'm not an agent. And so I wanted to get this -- get the information into the hands of the agents as quickly as possible and let them deal with it. If they wanted to go interview Sussmann and ask him all those kind of questions, fine with me.

Mr. Jordan. Did that happen?

Mr. Baker. I don't know that. But I -- I mean, I -- well, A, I did hand it off to the -- to the investigators.

Mr. Jordan. I think you told us you handed it off to Mr. Strzok and Mr. Priestap?

Mr. Baker. My recollection is Mr. Priestap.

Mr. Jordan. Okay. And you don't know if they followed up or not?

Mr. Baker. Bill Priestap told me that they did follow up extensively.

Mr. Jordan. And back to a question I asked earlier. This was

EXHIBIT 16

NOT A CERTIFIED COPY

EXECUTIVE SESSION
PERMANENT SELECT COMMITTEE ON INTELLIGENCE,
U.S. HOUSE OF REPRESENTATIVES,
WASHINGTON, D.C.

INTERVIEW OF: MICHAEL SUSSMANN

Monday, December 18, 2017

Washington, D.C.

The interview in the above matter was held in Room HVC-304, the Capitol, commencing at 10:06 a.m.

Present: Representatives Conaway, Schiff, and Heck.

different clients, and since we've just spoken --

MS. RUEMLER: As long as you don't reveal identity of them, which you're not permitted to do under the rules, or any content.

MR. SUSSMANN: Can we step outside and talk about how to deal with the range of clients?

MS. RUEMLER: Yes.

[Discussion off the record.]

MR. SUSSMANN: Thank you.

██████████ No problem.

[The reporter read the record as requested.]

MR. SUSSMANN: So I'm not clear as to the scope of what you're asking your question, but I'm going to be sort of more expansive in my answer, because there's nothing -- you said in relation to the things that we discussed today, and this is not something we've discussed today.

But I did have -- I don't believe I had -- so two things. I don't believe I had -- I didn't have direct contact with [], but I can relate to you some indirect contacts with []. And I had a meeting [] as well.

BY ██████████

Q Okay.

A The [] contact related to specifically my representation of the DNC, and my contact [] did not relate to my specific representation of the DNC, or the Clinton campaign, or the Democratic Party. And I also -- I'm not -- I will do the best that I can with you. I think there are limits to what I can discuss in an unclassified setting.

Q Okay, fair enough. What was your contact [] about?

A So the contact [] was about reporting to them information that was reported to me about possible contacts, covert or at least nonpublic, between Russian entities and various entities in the United States associated with the -- or potentially associated with the Trump Organization.

Q And when did that contact [] occur, month and year?

A February 2017.

Q Where did you get that information from to relay to []?

A From a client of mine.

Q Why did you go to []?

A I initially reached out to [] --

MS. RUEMLER: Just to be very careful here to make sure that you don't disclose any attorney-client or work product privilege information. I think you can talk generally about your general purpose in seeking the meeting, but just be careful not to disclose any communications between you and your client.

A Okay. I'm sorry, so was the question why?

BY []

Q Yes.

A Well, so the purpose of the meeting was to share -- you may need to repeat your last question. I feel like I'm repeating myself. The purpose was to share information that --

Q Right.

A -- we had that might be --

Q You did say, right, that you had -- you'd received information from a client -- I'm not asking who -- that may be germane to the 2016 election and associates of the Trump campaign or people affiliated with the Trump campaign.

So my follow-up question was, why did you go to [] with this information?

A Oh, I'm sorry. And I apologize. I remember what I was going to say. It was -- it was, in large part, in response to President Obama's post-election IC review of potential Russian involvement in the election. And in that regard, I had made outreach prior to the change in administration in 2016. And for reasons known and unknown to me, it took a long time to -- or it took -- you know, it took a while to have a meeting, and so it ended up being after the change in administration. But --

Q When did you first reach out to [] in this regard?

A Probably early December, or sometime in December.

Q 2016?

A 2016.

[] Our time is up. We'll pick up there when we get off.

Mr. Ranking Member.

MR. SUSSMANN: Okay, thank you.

Congressman Schiff, I apologize that for the length of the questioning, I was showing you my ear and my shoulder --

MR. SCHIFF: No worries.

MR. SUSSMANN: -- and wasn't paying attention to you. Thank you, Mr.

Conaway.

MR. MCQUAID: It's his better side, so you're well positioned.

MR. SCHIFF: Mr. Sussmann, I want to go back over the timeline a bit. So you're first brought into this by a partner at the very end of April of 2016.

MR. SUSSMANN: Yes, sir.

A Well, I remember --

Q Do you remember the specific names of the agents you spoke with?

A No. I might be able to find that, but I reached out to [REDACTED] which was the -- I mentioned earlier, was the WFO cyber crime guy who the DNC -- sort of the DNC's main contact. And he would be my main contact.

Earlier this morning, I talked about threats. I was a central point for physical threats, and all sorts of threats would come in. I would sort of feed things through him. And I remember reaching out to him and saying There's a report, can you connect me with someone. He said, Oh, yeah, I know the Russia guys at WFO who've been doing this. I'll put you in touch.

I think one of the gentleman, his last name was [REDACTED] But I may be able to find a record of my communications and send that, if that would be helpful.

[REDACTED] Okay. Mr. Schiff, I'm -- we're almost done with our 15 minutes. I've got some more questions, so I'll just defer to you for the next 15. The next question I'm going to ask is going to probably have a lengthy response and follow up.

MR. SCHIFF: Why don't you continue.

[REDACTED] Okay. Yes, sir.

BY [REDACTED]

Q I want to now shift to [REDACTED]. So you also now had a conversation with representatives of [REDACTED].

A Uh-huh.

Q Can you explain when that conversation occurred exactly? What was the timeframe?

A So I had a conversation with the [REDACTED] current general counsel in

December 2016. And then in February, I believe, I had a meeting at [REDACTED]

Q Do you remember what time in February? Was it early or mid or late February?

A I think it was early.

Q Early February. And the -- let's go back to the conversation that you had with [REDACTED] OGC -- or general counsel, I guess. You had a meeting with the general counsel?

A Just a phone call.

Q Phone call. And what was the phone call about?

A I initiated the phone call. And I said, in some manner, I understand that the President has ordered a review of all intelligence relating to the election, and I have some information that may be germane to the subject matter of the investigation, and offered to come meet with her or, I don't know, you know, someone at [REDACTED], if they were interested, to hear about this information. And that was really the -- that was the nature of the call.

Q What was the response from the general counsel?

A Well, it was an expression of interest, but in fairness, this was a cold call. So I wasn't expecting any, like, thank you for calling, something along the lines of thank you for calling, and I'll speak to some people here and someone will get back to you.

Q And she -- did she indicate that she would get back to you in another point regarding your offer?

A Uh-huh.

Q And what was the information that you had in December of '16 that prompted the phone call? What was it that you wanted to share with [REDACTED]

UNCLASSIFIED, COMMITTEE SENSITIVE

A I wanted to share information showing possible contacts between, you know, people unknown to me in Russia and the Trump Organization -- I know that's a broad statement -- the Trump Organization and others in the United States.

Q And where did this information come from?

A It came from a client.

Q Can you mention who that client is?

MS. RUEMLER: I'm going to instruct you not to answer.

MR. SUSSMANN: I cannot.

BY [REDACTED]

Q Was that a client that you had represented prior to representing the DNC?

MS. RUEMLER: I think you can answer that question.

MR. SUSSMANN: Prior to representing the DNC on this matter?

BY [REDACTED]

Q Yes.

A Yes.

Q Did the information that you received from this client come into your possession or knowledge after the election, after the presidential election in November 2016?

A No.

Q So the information that you had that you discussed with the general counsel of [REDACTED] in December was information you knew about prior to the election, presidential election in 2016?

A Yes.

UNCLASSIFIED, COMMITTEE SENSITIVE

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

Q And when did you know -- when did your client, without giving me obviously the name of the client, when did your client tell you about this new information or information that you had known about, that prompted your call in December?

MS. RUEMLER: I'm going to instruct him not to answer that. I think that calls for information that's covered by privilege.

██████████ Well, I'm not asking -- and I understand your point. I'm not asking -- I'm only trying to get an understanding of when the information was conveyed to your client.

He's indicated that he had a phone call with the general counsel at So I'm just trying to understand when he became aware of this specific information that he then notified the GC about.

Can you just give me a timeframe as to --

MS. RUEMLER: Can you give the general timeframe?

MR. SUSSMANN: How general?

MS. RUEMLER: Season.

MR. MCQUAID: Season.

MR. SUSSMANN: Sure. Probably the summer of 2016.

BY ██████████

Q Okay. This information that you had that prompted -- and I guess, what prompted -- so I guess I should ask, what prompted you to make a call to in December if you had known about this information for, say, 6 months or longer?

A Because the -- as I -- I apologize, because I can't clearly recall which information I only departed to your colleague -- or not.

UNCLASSIFIED, COMMITTEE SENSITIVE

Q Yeah. And --

A So I apologize if I'm repeating something or I haven't said it before, but the President was -- President Obama had ordered a review of all intelligence regarding -- I don't remember specifically what the executive order said, but anything involving Russian interference or activity regarding the election.

And this information seemed to fall roughly within that, and so I thought that might be -- or my client thought that that might be something that was relevant for those that were gathering information regarding foreign-based actors.

Q Okay. I mean, so just for the record, you were not part of the administration. You were a private attorney at the time?

A Yes, sir.

Q And you'd heard about the -- this call?

A Yes, sir.

Q Okay. So why didn't you then -- if you felt that it was necessary to convey the information you had been aware of to appropriate sources, if you will, appropriate entities, in this case you'd thought was appropriate, why didn't you convey this information earlier to the FBI, or had you?

A I had.

Q So you had had a private -- you had had a separate conversation with a representative of the FBI regarding this same information?

A Yes.

Q And who in the FBI did you speak with?

A It's general counsel.

Q Okay. And that would be?

A Jim Baker.

UNCLASSIFIED, COMMITTEE SENSITIVE

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

A I don't think -- I'm not going to say anything about my clients.

MS. RUEMLER: I think you can answer the question if -- I think you can answer that question. Do you want to confer about this just to make sure you don't trip any wires?

And not to be difficult, it's just that we only have authorization from two specific clients from the Clinton campaign and from the DNC, and he doesn't have authorization from any other client.

So should we -- do you want to step outside for a second?

MR. SUSSMANN: I feel like you're worried about me, so we should.

MS. RUEMLER: No, I just want to make sure you're clear.

MR. SUSSMANN: I don't want to say anything I shouldn't, so --

MS. RUEMLER: This will just be 30 seconds.

[Discussion off the record.]

██████████ We can go ahead and go back on the record.

MR. SUSSMANN: Yes, sir. To answer your question, I have never represented Glenn Simpson.

BY ██████████

Q Okay. So the information that was conveyed to you was not from Glenn Simpson?

A Yes.

Q Was it from Peter Fritsch (ph)?

MS. RUEMLER: You can answer that.

MR. SUSSMANN: No, it was not.

BY ██████████

Q Or Thomas Kattan (ph)?

UNCLASSIFIED, COMMITTEE SENSITIVE

A I don't know who that person is.

Q Okay. The information, and you mentioned it just before we broke, you said it was communications between persons -- can you just describe it again, what the information was that you conveyed to the two principals? It was communications between U.S. persons and unknown folks in Russia?

A It was information that could demonstrate contacts or communications between unknown persons in Russia and unknown persons associated, or potentially associated with the Trump Organization.

Q I want to go back to . So you had -- after you had the phone call with the general counsel, you then had a meeting in early February?

A Yes.

Q And who was in the meeting?

A A representative from the Office of General Counsel.

Q And who was that individual?

A I don't know.

Q Okay.

A And another -- .

Q Okay. Where was the meeting located?

A

Q Okay. Was it in the Office of General Counsel or just -- do you remember where you had the meeting?

A I don't think it was in OGC, but, you know, I followed someone upstairs and we walk around, walk around, walk around, go in a conference room, so --

Q So the -- and the other person who was not a lawyer was -- did they identify where they work?

UNCLASSIFIED, COMMITTEE SENSITIVE

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

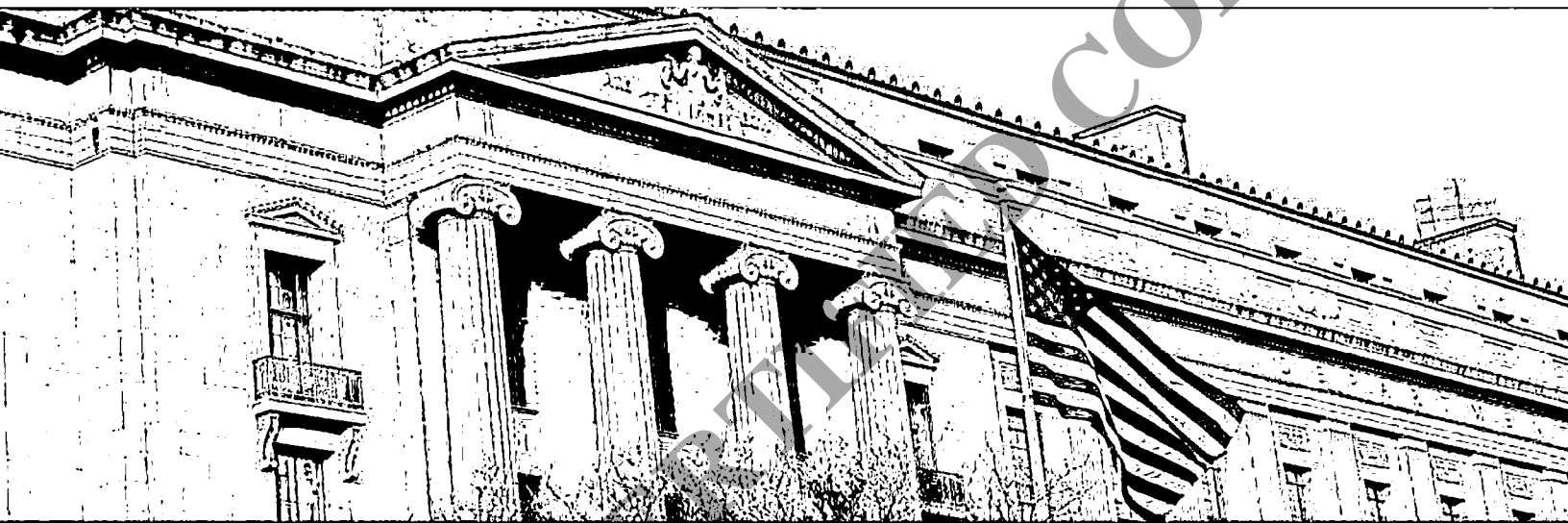
EXHIBIT 17

NOT A CERTIFIED COPY



Office of the Inspector General
U.S. Department of Justice

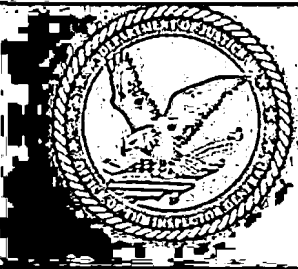
OVERSIGHT ★ INTEGRITY ★ GUIDANCE



**Review of Four FISA Applications and
Other Aspects of the FBI's Crossfire
Hurricane Investigation**

Oversight and Review Division 20-012

December 2019 (Revised)



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

Background

The Department of Justice (Department) Office of the Inspector General (OIG) undertook this review to examine certain actions by the Federal Bureau of Investigation (FBI) and the Department during an FBI investigation opened on July 31, 2016, known as "Crossfire Hurricane," into whether individuals associated with the Donald J. Trump for President Campaign were coordinating, wittingly or unwittingly, with the Russian government's efforts to interfere in the 2016 U.S. presidential election. Our review included examining:

- The decision to open Crossfire Hurricane and four individual cases on current and former members of the Trump campaign, George Papadopoulos, Carter Page, Paul Manafort, and Michael Flynn; the early investigative steps taken; and whether the openings and early steps complied with Department and FBI policies;
- The FBI's relationship with Christopher Steele, whom the FBI considered to be a confidential human source (CHS); its receipt, use, and evaluation of election reports from Steele; and its decision to close Steele as an FBI CHS;
- Four FBI applications filed with the Foreign Intelligence Surveillance Court (FISC) in 2016 and 2017 to conduct Foreign Intelligence Surveillance Act (FISA) surveillance targeting Carter Page; and whether these applications complied with Department and FBI policies and satisfied the government's obligations to the FISC;
- The interactions of Department attorney Bruce Ohr with Steele, the FBI, Glenn Simpson of Fusion GPS, and the State Department; whether work Ohr's spouse performed for Fusion GPS implicated ethical rules applicable to Ohr; and Ohr's interactions with Department attorneys regarding the Manafort criminal case; and
- The FBI's use of Undercover Employees (UCEs) and CHSs other than Steele in the Crossfire Hurricane investigation; whether the FBI placed any CHSs within the Trump campaign or tasked any CHSs to report on the Trump campaign; whether the use of CHSs and UCEs complied with Department and FBI policies; and the attendance of a Crossfire Hurricane supervisory agent at counterintelligence briefings given to the 2016 presidential candidates and certain campaign advisors.

OIG Methodology

The OIG examined more than one million documents that were in the Department's and FBI's possession and conducted over 170 interviews involving more than 100 witnesses. These witnesses included former FBI Director Comey, former Attorney General (AG) Loretta Lynch, former Deputy Attorney General (DAG) Sally Yates, former DAG Rod Rosenstein, former Acting AG and Acting DAG and current FBI General Counsel Dana Boente, former FBI Deputy Director Andrew McCabe, former FBI General Counsel James Baker, and Department attorney Bruce Ohr and his wife. The OIG also interviewed Christopher Steele and current and former employees of other U.S. government agencies. Two witnesses, Glenn Simpson and Jonathan Winer (a former Department of State official), declined our requests for voluntary interviews, and we were unable to compel their testimony.

We were given broad access to relevant materials by the Department and the FBI. In addition, we reviewed relevant information that other U.S. government agencies provided the FBI in the course of the Crossfire Hurricane investigation. However, because the activities of other agencies are outside our jurisdiction, we did not seek to obtain records from them that the FBI never received or reviewed, except for a limited amount of State Department records relating to Steele; we also did not seek to assess any actions other agencies may have taken. Additionally, our review did not independently seek to determine whether corroboration existed for the Steele election reporting; rather, our review was focused on information that was available to the FBI concerning Steele's reports prior to and during the pendency of the Carter Page FISA authority.

Our role in this review was not to second-guess discretionary judgments by Department personnel about whether to open an investigation, or specific judgment calls made during the course of an investigation, where those decisions complied with or were authorized by Department rules, policies, or procedures. We do not criticize particular decisions merely because we might have recommended a different investigative strategy or tactic based on the facts learned during our investigation. The question we considered was not whether a particular investigative decision was ideal or could have been handled more effectively, but rather whether the Department and the FBI complied with applicable legal requirements, policies, and procedures in taking the actions we reviewed or, alternatively, whether the circumstances surrounding the decision indicated that it was based on



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

inaccurate or incomplete information, or considerations other than the merits of the investigation. If the explanations we were given for a particular decision were consistent with legal requirements, policies, procedures, and not unreasonable, we did not conclude that the decision was based on improper considerations in the absence of documentary or testimonial evidence to the contrary.

The Opening of Crossfire Hurricane and Four Related Investigations, and Early Investigative Steps

The Opening of Crossfire Hurricane and Four Individual Cases

As we describe in Chapter Three, the FBI opened Crossfire Hurricane on July 31, 2016, just days after its receipt of information from a Friendly Foreign Government (FFG) reporting that, in May 2016, during a meeting with the FFG, then Trump campaign foreign policy advisor George Papadopoulos "suggested the Trump team had received some kind of suggestion from Russia that it could assist this process with the anonymous release of information during the campaign that would be damaging to Mrs. Clinton (and President Obama)." The FBI Electronic Communication (EC) opening the Crossfire Hurricane investigation stated that, based on the FFG information, "this investigation is being opened to determine whether individual(s) associated with the Trump campaign are witting of and/or coordinating activities with the Government of Russia." We did not find information in FBI or Department ECs, emails, or other documents, or through witness testimony, indicating that any information other than the FFG information was relied upon to predicate the opening of the Crossfire Hurricane investigation. Although not mentioned in the EC, at the time, FBI officials involved in opening the investigation had reason to believe that Russia may have been connected to the WikiLeaks disclosures that occurred earlier in July 2016, and were aware of information regarding Russia's efforts to interfere with the 2016 U.S. elections. These officials, though, did not become aware of Steele's election reporting until weeks later and we therefore determined that Steele's reports played no role in the Crossfire Hurricane opening.

The FBI assembled a Headquarters-based investigative team of special agents, analysts, and supervisory special agents (referred to throughout this report as "the Crossfire Hurricane team") who conducted an initial analysis of links between Trump campaign members and Russia. Based upon this

analysis, the Crossfire Hurricane team opened individual cases in August 2016 on four U.S. persons—Papadopoulos, Carter Page, Paul Manafort, and Michael Flynn—all of whom were affiliated with the Trump campaign at the time the cases were opened.

As detailed in Chapter Two, the Attorney General's Guidelines for Domestic Operations (AG Guidelines) and the FBI's Domestic Investigations Operations Guide (DIOG) both require that FBI investigations be undertaken for an "authorized purpose"—that is, "to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence." Additionally, both the AG Guidelines and the DIOG permit the FBI to conduct an investigation, even if it might impact First Amendment or other constitutionally protected activity, so long as there is some legitimate law enforcement purpose associated with the investigation.

In addition to requiring an authorized purpose, FBI investigations must have adequate factual predication before being initiated. The predication requirement is not a legal requirement but rather a prudential one imposed by Department and FBI policy. The DIOG provides for two types of investigations, Preliminary Investigations and Full Investigations. A Preliminary Investigation may be opened based upon "any allegation or information" indicative of possible criminal activity or threats to the national security. A Full Investigation may be opened based upon an "articulable factual basis" that "reasonably indicates" any one of three defined circumstances exists, including:

An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity.

In Full Investigations such as Crossfire Hurricane, all lawful investigative methods are allowed. In Preliminary Investigations, all lawful investigative methods (including the use of CHSs and UCEs) are permitted except for mail opening, physical searches requiring a search warrant, electronic surveillance requiring a judicial order or warrant (Title III wiretap or a FISA order), or requests under Title VII of FISA. An investigation opened as a Preliminary Investigation may be converted subsequently to a Full Investigation if



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

information becomes available that meets the predication standard. As we describe in the report, all of the investigative actions taken by the Crossfire Hurricane team, from the date the case was opened on July 31 until October 21 (the date of the first FISA order) would have been permitted whether the case was opened as a Preliminary or Full Investigation.

The AG Guidelines and the DIOG do not provide heightened predication standards for sensitive matters, or allegations potentially impacting constitutionally protected activity, such as First Amendment rights. Rather, the approval and notification requirements contained in the AG Guidelines and the DIOG are, in part, intended to provide the means by which such concerns can be considered by senior officials. However, we were concerned to find that neither the AG Guidelines nor the DIOG contain a provision requiring Department consultation before opening an investigation such as the one here involving the alleged conduct of individuals associated with a major party presidential campaign.

Crossfire Hurricane was opened as a Full Investigation and all of the senior FBI officials who participated in discussions about whether to open a case told us the information warranted opening it. For example, then Counterintelligence Division (CD) Assistant Director (AD) E.W. "Bill" Priestap, who approved the case opening, told us that the combination of the FFG information and the FBI's ongoing cyber intrusion investigation of the July 2016 hacks of the Democratic National Committee's (DNC) emails, created a counterintelligence concern that the FBI was "obligated" to investigate. Priestap stated that he considered whether the FBI should conduct defensive briefings for the Trump campaign but ultimately decided that providing such briefings created the risk that "if someone on the campaign was engaged with the Russians, he/she would very likely change his/her tactics and/or otherwise seek to cover-up his/her activities, thereby preventing us from finding the truth." We did not identify any Department or FBI policy that applied to this decision and therefore determined that the decision was a judgment call that Department and FBI policy leaves to the discretion of FBI officials. We also concluded that, under the AG Guidelines and the DIOG, the FBI had an authorized purpose when it opened Crossfire Hurricane to obtain information about, or protect against, a national security threat or federal crime, even though the investigation also had the potential to impact constitutionally protected activity.

Additionally, given the low threshold for predication in the AG Guidelines and the DIOG, we concluded that the FFG information, provided by a government the United States Intelligence Community (USIC) deems trustworthy, and describing a first-hand account from an FFG employee of a conversation with Papadopoulos, was sufficient to predicate the investigation. This information provided the FBI with an articulable factual basis that, if true, reasonably indicated activity constituting either a federal crime or a threat to national security, or both, may have occurred or may be occurring. For similar reasons, as we detail in Chapter Three, we concluded that the quantum of information articulated by the FBI to open the individual investigations on Papadopoulos, Page, Flynn, and Manafort in August 2016 was sufficient to satisfy the low threshold established by the Department and the FBI.

As part of our review, we also sought to determine whether there was evidence that political bias or other improper considerations affected decision making in Crossfire Hurricane, including the decision to open the investigation. We discussed the issue of political bias in a prior OIG report, *Review of Various Actions in Advance of the 2016 Election*, where we described text and instant messages between then Special Counsel to the Deputy Director Lisa Page and then Section Chief Peter Strzok, among others, that included statements of hostility toward then candidate Trump and statements of support for then candidate Hillary Clinton. In this review, we found that, while Lisa Page attended some of the discussions regarding the opening of the investigations, she did not play a role in the decision to open Crossfire Hurricane or the four individual cases. We further found that while Strzok was directly involved in the decisions to open Crossfire Hurricane and the four individual cases, he was not the sole, or even the highest-level, decision maker as to any of those matters. As noted above, then CD AD Priestap, Strzok's supervisor, was the official who ultimately made the decision to open the investigation, and evidence reflected that this decision by Priestap was reached by consensus after multiple days of discussions and meetings that included Strzok and other leadership in CD, the FBI Deputy Director, the FBI General Counsel, and a FBI Deputy General Counsel. We concluded that Priestap's exercise of discretion in opening the investigation was in compliance with Department and FBI policies, and we did not find documentary or testimonial evidence that political bias or improper motivation influenced his decision. We similarly found that, while the formal documentation opening each of the four individual investigations was approved by Strzok (as required by the DIOG), the



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

decisions to do so were reached by a consensus among the Crossfire Hurricane agents and analysts who identified individuals associated with the Trump campaign who had recently traveled to Russia or had other alleged ties to Russia. Priestap was involved in these decisions. We did not find documentary or testimonial evidence that political bias or improper motivation influenced the decisions to open the four individual investigations.

Sensitive Investigative Matter Designation

The Crossfire Hurricane investigation was properly designated as a "sensitive investigative matter," or SIM, by the FBI because it involved the activities of a domestic political organization or individuals prominent in such an organization. The DIOG requires that SIMs be reviewed in advance by the FBI Office of the General Counsel (OGC) and approved by the appropriate FBI Headquarters operational section chief, and that an "appropriate [National Security Division] official" receive notification after the case has been opened.

We concluded that the FBI satisfied the DIOG's approval and notification requirements for SIMs. As we describe in Chapter Three, the Crossfire Hurricane opening was reviewed by an OGC Unit Chief and approved by AD Priestap (two levels above Section Chief). The team also orally briefed National Security Division (NSD) officials within the first few days of the investigations being initiated. We were concerned, however, that Department and FBI policies do not require that a senior Department official be notified prior to the opening of a particularly sensitive case such as this one, nor do they place any additional requirements for SIMs beyond the approval and notification requirements at the time of opening, and therefore we include a recommendation to address this issue.

Early Investigative Steps and Adherence to the Least Intrusive Method

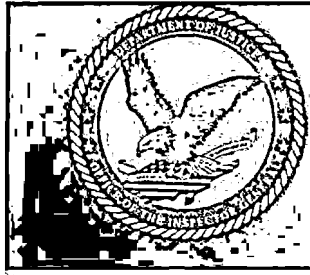
The AG Guidelines and the DIOG require that the "least intrusive" means or method be "considered" when selecting investigative techniques and, "if reasonable based upon the circumstances of the investigation," be used to obtain information instead of a more intrusive method. The DIOG states that the degree of procedural protection the law and Department and FBI policy provide for the use of a particular investigative method helps to determine its intrusiveness. As described in Chapter Three, immediately after opening the investigation, the

Crossfire Hurricane team submitted name trace requests to other U.S. government agencies and a foreign intelligence agency, and conducted law enforcement database and open source searches, to identify individuals associated with the Trump campaign in a position to have received the alleged offer of assistance from Russia. The FBI also sent Strzok and a Supervisory Special Agent (SSA) abroad to interview the source of the information the FBI received from the FFG, and also searched the FBI's database of CHSSs to identify sources who potentially could provide information about connections between individuals associated with the Trump campaign and Russia. Each of these steps is authorized under the DIOG and was a less intrusive investigative technique.

Thereafter, the Crossfire Hurricane team used more intrusive techniques, including CHSSs to interact and consensually record multiple conversations with Page and Papadopoulos, both during and after the time they were working for the Trump campaign, as well as on one occasion with a high-level Trump campaign official who was not a subject of the investigation. We found that, under Department and FBI policy, although this CHS activity implicated First Amendment protected activity, the operations were permitted because their use was not for the sole purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. Additionally, we found that under FBI policy, the use of a CHS to conduct consensual monitoring is a matter of investigative judgment that, absent certain circumstances, can be authorized by a first-line supervisor (an SSA). We determined that the CHS operations conducted during Crossfire Hurricane received the necessary FBI approvals and that, while AD Priestap knew about and approved of all of the operations, review beyond a first-level FBI supervisor was not required by Department or FBI policy.

We found it concerning that Department and FBI policy did not require the FBI to consult with any Department official in advance of conducting CHS operations involving advisors to a major party candidate's presidential campaign, and we found no evidence that the FBI consulted with any Department officials before conducting these CHS operations. As we describe in Chapter Two, consultation, at a minimum, is required by Department and FBI policies in numerous other sensitive circumstances, and we include a recommendation to address this issue.

Shortly after opening the Carter Page investigation in August 2016, the Crossfire Hurricane team discussed the possible use of FISA-authorized



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

electronic surveillance targeting Page, which is among the most sensitive and intrusive investigative techniques. As we describe in Chapter Five, the FBI ultimately did not seek a FISA order at that time because OGC, NSD's Office of Intelligence (OI), or both determined that more information was needed to support probable cause that Page was an agent of a foreign power. However, immediately after the Crossfire Hurricane team received Steele's election reporting on September 19, the team reinitiated their discussions with OI and their efforts to obtain FISA surveillance authority for Page, which they received from the FISC on October 21.

The decision to seek to use this highly intrusive investigative technique was known and approved at multiple levels of the Department, including by then DAG Yates for the initial FISA application and first renewal, and by then Acting Attorney General Boente and then DAG Rosenstein for the second and third renewals, respectively. However, as we explain later, the Crossfire Hurricane team failed to inform Department officials of significant information that was available to the team at the time that the FISA applications were drafted and filed. Much of that information was inconsistent with, or undercut, the assertions contained in the FISA applications that were used to support probable cause and, in some instances, resulted in inaccurate information being included in the applications. While we do not speculate whether Department officials would have authorized the FBI to seek to use FISA authority had they been made aware of all relevant information, it was clearly the responsibility of Crossfire Hurricane team members to advise them of such critical information so that they could make a fully informed decision.

The FBI's Relationship with Christopher Steele, and Its Receipt and Evaluation of His Election Reporting before the First FISA Application

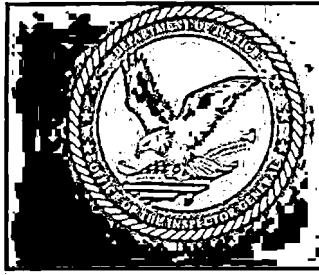
As we describe in Chapter Four, Steele is a former intelligence officer [REDACTED] who, in 2009, formed a consulting firm specializing in corporate intelligence and investigative services. In 2010, Steele was introduced by Ohr to an FBI agent, and for several years provided information to the FBI about various matters, such as corruption in the International Federation of Association Football (FIFA). Steele also provided the FBI agent with reporting about Russian oligarchs.

In 2013, the FBI completed the paperwork allowing the FBI to designate Steele as a CHS. However, as described in Chapter Four, we found that the FBI and Steele held significantly differing views about the nature of their relationship. Steele's handling agent viewed Steele as a former intelligence officer colleague and FBI CHS, with obligations to the FBI. Steele, on the other hand, told us that he was a businessperson whose firm (not Steele) had a contractual agreement with the FBI and whose obligations were to his paying clients, not the FBI. We concluded that this disagreement affected the FBI's control over Steele during the Crossfire Hurricane investigation, led to divergent expectations about Steele's conduct in connection with his election reporting, and ultimately resulted in the FBI formally closing Steele as a CHS in November 2016 (although, as discussed below, the FBI continued its relationship with Steele through Ohr).

In June 2016, Steele and his consulting firm were hired by Fusion GPS, a Washington, D.C., investigative firm, to obtain information about whether Russia was trying to achieve a particular outcome in the 2016 U.S. elections, what personal and business ties then candidate Trump had in Russia, and whether there were any ties between the Russian government and Trump or his campaign. Steele's work for Fusion GPS resulted in his producing numerous election-related reports, which have been referred to collectively as the "Steele Dossier." Steele himself was not the originating source of any of the factual information in his reporting. Steele instead relied on a Primary Sub-source for information, who used his/her network of sub-sources to gather information that was then passed to Steele. With Fusion GPS's authorization, Steele directly provided more than a dozen of his reports to the FBI between July and October 2016, and several others to the FBI through Ohr and other third parties. The Crossfire Hurricane team received the first six election reports on September 19, 2016—more than two months after Steele first gave his handling agent two of the six reports. We describe the reasons it took two months for the reports to reach the team in Chapter Four.

FBI's Efforts to Evaluate the Steele Reporting

Steele's handling agent told us that when Steele provided him with the first election reports in July 2016 and described his engagement with Fusion GPS, it was obvious to him that the request for the research was politically motivated. The supervisory intelligence analyst who supervised the analytical efforts for the Crossfire Hurricane team (Supervisory Intel Analyst)



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

explained that he also was aware of the potential for political influences on the Steele reporting.

The fact that the FBI believed Steele had been retained to conduct political opposition research did not require the FBI, under either DOJ or FBI policy, to ignore his reporting. The FBI regularly receives information from individuals with potentially significant biases and motivations, including drug traffickers, convicted felons, and even terrorists. The FBI is not required to set aside such information; rather, FBI policy requires that it critically assess the information. We found that after receiving Steele's reporting, the Crossfire Hurricane team began those efforts in earnest.

We determined that the FBI's decision to receive Steele's information for Crossfire Hurricane was based on multiple factors, including: (1) Steele's prior work as an intelligence professional for [REDACTED]; (2) his expertise on Russia; (3) his record as an FBI CHS; (4) the assessment of Steele's handling agent that Steele was reliable and had provided helpful information to the FBI in the past; and (5) the themes of Steele's reporting were consistent with the FBI's knowledge at the time of Russian efforts to interfere in the 2016 U.S. elections.

However, as we describe later, as the FBI obtained additional information raising significant questions about the reliability of the Steele election reporting, the FBI failed to reassess the Steele reporting relied upon in the FISA applications, and did not fully advise NSD or OI officials. We also found that the FBI did not aggressively seek to obtain certain potentially important information from Steele. For example, the FBI did not press Steele for information about the actual funding source for his election reporting work. Agents also did not question Steele about his role in a September 23, 2016 *Yahoo News* article entitled, "U.S. intel officials probe ties between Trump advisor and Kremlin," that described efforts by U.S. intelligence to determine whether Carter Page had opened communication channels with Kremlin officials. As we discuss in Chapters Five and Eight, the FBI assessed in the Carter Page FISA applications, without any support, that Steele had not "directly provided" the information to *Yahoo News*.

The First Application for FISA Authority on Carter Page

At the request of the FBI, the Department filed four applications with the FISC seeking FISA authority

targeting Carter Page: the first application on October 21, 2016, and three renewal applications on January 12, April 7, and June 29, 2017. A different FISC judge considered each application and issued the requested orders, collectively resulting in approximately 11 months of FISA coverage targeting Carter Page from October 21, 2016, to September 22, 2017. We discuss the first FISA application in this section and in Chapter Five.

Decision to Seek FISA Authority

We determined that the Crossfire Hurricane team's receipt of Steele's election reporting on September 19, 2016 played a central and essential role in the FBI's and Department's decision to seek the FISA order. As noted above, when the team first sought to pursue a FISA order for Page in August 2016, a decision was made by OGC, OI, or both that more information was needed to support a probable cause finding that Page was an agent of a foreign power. As a result, FBI OGC ceased discussions with OI about a Page FISA order at that time.

On September 19, 2016, the same day that the Crossfire Hurricane team first received Steele's election reporting, the team contacted FBI OGC again about seeking a FISA order for Page and specifically focused on Steele's reporting in drafting the FISA request. Two days later, on September 21, the FBI OGC Unit Chief contacted the NSD OI Unit Chief to advise him that the FBI believed it was ready to submit a formal FISA request to OI relating to Page. Almost immediately thereafter, OI assigned an attorney (OI Attorney) to begin preparation of the application.

Although the team also was interested in seeking FISA surveillance targeting Papadopoulos, the FBI OGC attorneys were not supportive. FBI and NSD officials told us that the Crossfire Hurricane team ultimately did not seek FISA surveillance of Papadopoulos, and we are aware of no information indicating that the team requested or seriously considered FISA surveillance of Manafort or Flynn.

We did not find documentary or testimonial evidence that political bias or improper motivation influenced the FBI's decision to seek FISA authority on Carter Page.

Preparation and Review Process

As we detail in Chapter Two, the FISC Rules of Procedure and FBI policy required that the Carter Page FISA applications contain all material facts. Although



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

the FISC Rules do not define or otherwise explain what constitutes a “material” fact, FBI policy guidance states that a fact is “material” if it is relevant to the court’s probable cause determination. Additionally, FBI policy mandates that the case agent ensure that all factual statements in a FISA application are “scrupulously accurate.”

On or about September 23, the OI Attorney began work on the FISA application. Over the next several weeks, the OI Attorney prepared and edited a draft application using information principally provided by the FBI case agent assigned to the Carter Page investigation at the time and, in a few instances, by an OGC attorney (OGC Attorney) or other Crossfire Hurricane team members. The drafting process culminated in an application that asserted that the Russian government was attempting to undermine and influence the upcoming U.S. presidential election, and that the FBI believed Carter Page was acting in conjunction with the Russians in those efforts. The application’s statement of facts supporting probable cause to believe that Page was an agent of Russia was broken down into five main elements:

- The efforts of Russian Intelligence Services (RIS) to influence the upcoming U.S. presidential election;
- The Russian government’s attempted coordination with members of the Trump campaign, based on the FFG information reporting the suggestion of assistance from the Russians to someone associated with the Trump campaign;
- Page’s historical connections to Russia and RIS;
- Page’s alleged coordination with the Russian government on 2016 U.S. presidential election activities, based on Steele’s reporting; and
- Page’s statements to an FBI CHS in October 2016 that that he had an “open checkbook” from certain Russians to fund a think tank project.

In addition, the statement of facts described Page’s denials of coordination with the Russian government, as reported in two news articles and asserted by Page in a September 25 letter to then FBI Director Comey.

The application received the necessary Department approvals and certifications as required by law. As we fully describe in Chapter Five, this application received more attention and scrutiny than a typical FISA application in terms of the additional layers

of review and number of high-level officials who read the application before it was signed. These officials included NSD’s Acting Assistant Attorney General, NSD’s Deputy Assistant Attorney General with oversight over OI, OI’s Operations Section Chief and Deputy Section Chief, the DAG, Principal Associate Deputy Attorney General, and the Associate Deputy Attorney General responsible for ODAG’s national security portfolio. However, as we explain below, the Department decision makers who supported and approved the application were not given all relevant information.

Role of Steele Election Reporting in the First Application

In support of the fourth element in the FISA application—Carter Page’s alleged coordination with the Russian government on 2016 U.S. presidential election activities—the application relied entirely on the following information from Steele Reports 80, 94, 95, and 102:

- Compromising information about Hillary Clinton had been compiled for many years, was controlled by the Kremlin, and had been fed by the Kremlin to the Trump campaign for an extended period of time (Report 80);
- During a July 2016 trip to Moscow, Page met secretly with Igor Sechin, Chairman of Russian energy conglomerate Rosneft and close associate of Putin, to discuss future cooperation and the lifting of Ukraine-related sanctions against Russia; and with Igor Divyevkin, a highly-placed Russian official, to discuss sharing with the Trump campaign derogatory information about Clinton (Report 94);
- Page was an intermediary between Russia and the Trump campaign’s then manager (Manafort) in a “well-developed conspiracy” of cooperation, which led to Russia’s disclosure of hacked DNC emails to WikiLeaks in exchange for the Trump campaign’s agreement to sideline Russian intervention in Ukraine as a campaign issue (Report 95); and
- Russia released the DNC emails to WikiLeaks in an attempt to swing voters to Trump, an objective conceived and promoted by Page and others (Report 102).

We determined that the FBI’s decision to rely upon Steele’s election reporting to help establish probable cause that Page was an agent of Russia was a judgment reached initially by the case agents on the



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

Crossfire Hurricane team. We further determined that FBI officials at every level concurred with this judgment, from the OGC attorneys assigned to the investigation to senior CD officials, then General Counsel James Baker, then Deputy Director Andrew McCabe, and then Director James Comey. FBI leadership supported relying on Steele's reporting to seek a FISA order on Page after being advised of, and giving consideration to, concerns expressed by Stuart Evans, then NSD's Deputy Assistant Attorney General with oversight responsibility over OI, that Steele may have been hired by someone associated with presidential candidate Clinton or the DNC, and that the foreign intelligence to be collected through the FISA order would probably not be worth the "risk" of being criticized later for collecting communications of someone (Carter Page) who was "politically sensitive." According to McCabe, the FBI "felt strongly" that the FISA application should move forward because the team believed they had to get to the bottom of what they considered to be a potentially serious threat to national security, even if the FBI would later be criticized for taking such action. McCabe and others discussed the FBI's position with NSD and ODAG officials, and these officials accepted the FBI's decision to move forward with the application, based substantially on the Steele information.

We found that the FBI did not have information corroborating the specific allegations against Carter Page in Steele's reporting when it relied upon his reports in the first FISA application or subsequent renewal applications. OGC and NSD attorneys told us that, while the FBI's "Woods Procedures" (described in Chapter Two) require that every factual assertion in a FISA application be "verified," when information is attributed to a FBI CHS, the Woods Procedures require only that the agent verify, with supporting documentation, that the application accurately reflects what the CHS told the FBI. The procedures do not require that the agent corroborate, through a second, independent source, that what the CHS told the FBI is true. We did not identify anything in the Woods Procedures that is inconsistent with these officials' description of the procedures.

However, absent corroboration for the factual assertions in the election reporting, it was particularly important for the FISA applications to articulate the FBI's knowledge of Steele's background and its assessment of his reliability. On these points, the applications advised the court that Steele was believed to be a reliable source for three reasons: his professional background; his history of work as an FBI CHS since 2013; and his prior non-election reporting,

which the FBI described as "corroborated and used in criminal proceedings." As discussed below, the representations about Steele's prior reporting were overstated and had not been approved by Steele's handling agent, as required by the Woods Procedures.

Due to Evans's persistent inquiries, the FISA application also included a footnote, developed by OI based on information provided by the Crossfire Hurricane team, to address Evans's concern about the potential political bias of Steele's research. The footnote stated that Steele was hired by an identified U.S. person (Glenn Simpson) to conduct research regarding "Candidate #1's" (Donald Trump) ties to Russia and that the FBI "speculates" that this U.S. person was likely looking for information that could be used to discredit the Trump campaign.

Relevant Information Inaccurately Stated, Omitted, or Undocumented in the First Application

Our review found that FBI personnel fell far short of the requirement in FBI policy that they ensure that all factual statements in a FISA application are "scrupulously accurate." We identified multiple instances in which factual assertions relied upon in the first FISA application were inaccurate, incomplete, or unsupported by appropriate documentation, based upon information the FBI had in its possession at the time the application was filed. We found that the problems we identified were primarily caused by the Crossfire Hurricane team failing to share all relevant information with OI and, consequently, the information was not considered by the Department decision makers who ultimately decided to support the applications.

As more fully described in Chapter Five, based upon the information known to the FBI in October 2016, the first application contained the following seven significant inaccuracies and omissions:

1. Omitted information the FBI had obtained from another U.S. government agency detailing its prior relationship with Page, including that Page had been approved as an "operational contact" for the other agency from 2008 to 2013, and that Page had provided information to the other agency concerning his prior contacts with certain Russian intelligence officers, one of which overlapped with facts asserted in the FISA application;
2. Included a source characterization statement asserting that Steele's prior reporting had been "corroborated and used in criminal proceedings,"



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

which overstated the significance of Steele's past reporting and was not approved by Steele's handling agent, as required by the Woods Procedures;

3. Omitted information relevant to the reliability of Person 1, a key Steele sub-source (who was attributed with providing the information in Report 95 and some of the information in Reports 80 and 102 relied upon in the application), namely that (1) Steele himself told members of the Crossfire Hurricane team that Person 1 was a "boaster" and an "egotist" and "may engage in some embellishment" and (2) the FBI had opened a counterintelligence investigation on Person 1 a few days before the FISA application was filed;
4. Asserted that the FBI had assessed that Steele did not directly provide to the press information in the September 23 *Yahoo News* article based on the premise that Steele had told the FBI that he only shared his election-related research with the FBI and Fusion GPS, his client; this premise was incorrect and contradicted by documentation in the Woods File—Steele had told the FBI that he also gave his information to the State Department;
5. Omitted Papadopoulos's consensually monitored statements to an FBI CHS in September 2016 denying that anyone associated with the Trump campaign was collaborating with Russia or with outside groups like WikiLeaks in the release of emails;
6. Omitted Page's consensually monitored statements to an FBI CHS in August 2016 that Page had "literally never met" or "said one word to" Paul Manafort and that Manafort had not responded to any of Page's emails; if true, those statements were in tension with claims in Report 95 that Page was participating in a conspiracy with Russia by acting as an intermediary for Manafort on behalf of the Trump campaign; and
7. Included Page's consensually monitored statements to an FBI CHS in October 2016 that the FBI believed supported its theory that Page was an agent of Russia but omitted other statements Page made that were inconsistent with its theory, including denying having met with Sechin and Divyekin, or even knowing who Divyekin was; if true, those statements contradicted the claims in Report 94 that Page

had met secretly with Sechin and Divyekin about future cooperation with Russia and shared derogatory information about candidate Clinton.

None of these inaccuracies and omissions were brought to the attention of OI before the last FISA application was filed in June 2017. Consequently, these failures were repeated in all three renewal applications. Further, as we discuss later, we identified 10 additional significant errors in the renewal applications.

The failure to provide accurate and complete information to the OI Attorney concerning Page's prior relationship with another U.S. government agency (item 1 above) was particularly concerning because the OI Attorney had specifically asked the case agent in late September 2016 whether Carter Page had a current or prior relationship with the other agency. In response to that inquiry, the case agent advised the OI Attorney that Page's relationship was "dated" (claiming it was when Page lived in Moscow in 2004-2007) and "outside scope." This representation, however, was contrary to information that the other agency had provided to the FBI in August 2016, which stated that Page was approved as an "operational contact" of the other agency from 2008 to 2013 (after Page had left Moscow). Moreover, rather than being "outside scope," Page's status with the other agency overlapped in time with some of the interactions between Page and known Russian intelligence officers that were relied upon in the FISA applications to establish probable cause. Indeed, Page had provided information to the other agency about his past contacts with a Russian Intelligence Officer (Intelligence Officer 1), which were among the historical connections to Russian intelligence officers that the FBI relied upon in the first FISA application (and subsequent renewal applications). According to the information from the other agency, an employee of the other agency had assessed that Page "candidly described his contact with" Intelligence Officer 1 to the other agency. Thus, the FBI relied upon Page's contacts with Intelligence Officer 1, among others, in support of its probable cause statement in the FISA application, while failing to disclose to OI or the FISC that (1) Page had been approved as an operational contact by the other agency during a five-year period that overlapped with allegations in the FISA application, (2) Page had disclosed to the other agency contacts that he had with Intelligence Officer 1 and certain other individuals, and (3) the other agency's employee had given a positive assessment of Page's candor.

Further, we were concerned by the FBI's inaccurate assertion in the application that Steele's prior reporting had been "corroborated and used in criminal



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

proceedings," which we were told was primarily a reference to Steele's role in the FIFA corruption investigation. We found that the team had speculated that Steele's prior reporting had been corroborated and used in criminal proceedings without clearing the representation with Steele's handling agent, as required by the Woods Procedures. According to the handling agent, he would not have approved the representation in the application because only "some" of Steele's prior reporting had been corroborated—most of it had not—and because Steele's information was never used in a criminal proceeding. We concluded that these failures created the inaccurate impression in the applications that at least some of Steele's past reporting had been deemed sufficiently reliable by prosecutors to use in court, and that more of his information had been corroborated than was actually the case.

We found no evidence that the OI Attorney, NSD supervisors, ODAG officials, or Yates were made aware of these issues before the first application was submitted to the court. Although we also found no evidence that Comey had been made aware of these issues at the time he certified the application, as discussed in our analysis in Chapter Eleven, multiple factors made it difficult for us to precisely determine the extent of FBI leadership's knowledge as to each fact that was not shared with OI and not included, or inaccurately stated, in the FISA applications. These factors included, among other things, limited recollections, the inability to question Comey or refresh his recollection with relevant, classified documentation because of his lack of a security clearance, and the absence of meeting minutes that would show the specific details shared with Comey and McCabe during briefings they received, beyond the more general investigative updates that we know they were provided.

FBI Activities After the First FISA Application and FBI Efforts to Assess Steele's Election Reporting

On October 31, 2016, shortly after the first FISA application was signed, an article entitled "A Veteran Spy Has Given the FBI Information Alleging a Russian Operation to Cultivate Donald Trump," was published by *Mother Jones*. Steele admitted to the FBI that he was a source for the article, and the FBI closed him as a CHS for cause in November 2016. However, as we describe below, despite having been closed for cause, the Crossfire Hurricane team continued to obtain information from Steele through Ohr, who met with the FBI on 13 occasions to pass along information he had been provided by Steele.

In Chapter Six, we describe the events that followed Steele's closing as a CHS, including the FBI's receipt of information from several third parties who had acquired copies of the Steele election reports, use of information from the Steele reports in an interagency assessment of Russian interference in the U.S. 2016 elections, and continuing efforts to learn about Steele and his source network and to verify information from the reports following Steele's closure.

Starting in December 2016, FBI staff participated in an interagency effort to assess the Russian government's intentions and actions concerning the 2016 U.S. elections. We learned that whether and how to present Steele's reporting in the Intelligence Community Assessment (ICA) was a topic of significant discussion between the FBI and the other agencies participating in it. According to FBI staff, as the interagency editing process for the ICA progressed, the Central Intelligence Agency (CIA) expressed concern about the lack of vetting for the Steele election reporting and asserted it did not merit inclusion in the body of the report. An FBI Intel Section Chief told us the CIA viewed it as "internet rumor." In contrast, as we describe in Chapter Six, the FBI, including Comey and McCabe, sought to include the reporting in the ICA. Limited information from the Steele reporting ultimately was presented in an appendix to the ICA.

FBI efforts to verify information in the Steele election reports, and to learn about Steele and his source network continued after Steele's closure as a CHS. In November and December 2016, FBI officials travelled abroad and met with persons who previously had professional contacts with Steele or had knowledge of his work. Information these FBI officials obtained about Steele was both positive and negative. We found, however, that the information about Steele was not placed in his FBI CHS file.

We further learned that the FBI's Validation Management Unit (VMU) completed a human source validation review of Steele in early 2017. The VMU review found that Steele's past criminal reporting was "minimally corroborated," and included this finding in its report that was provided to the Crossfire Hurricane team. This determination by the VMU was in tension with the source characterization statement included in the initial FISA application, which represented that Steele's prior reporting had been "corroborated and used in criminal proceedings." The VMU review also did not identify any corroboration for Steele's election reporting among the information that the Crossfire Hurricane team had collected. However, the VMU did not include this finding in its written validation report



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

and therefore members of the Crossfire Hurricane team and FBI executives were unaware of it.

We also found that the FBI's interviews of Steele, his Primary Sub-source, a second sub-source, and other investigative activity, revealed potentially serious problems with Steele's descriptions of information in his reports. For example, as detailed in Chapters Six and Eight, the Primary Sub-source made statements during his/her January 2017 FBI interview that were inconsistent with multiple sections of the Steele reports, including some that were relied upon in the FISA applications. Among other things, regarding the allegations attributed to Person 1, the Primary Sub-source's account of these communications, if true, was not consistent with and, in fact, contradicted the allegations of a "well-developed conspiracy" in Reports 95 and 102 attributed to Person 1.

We further determined that the Crossfire Hurricane team was unable to corroborate any of the specific substantive allegations regarding Carter Page contained in Steele's election reporting which the FBI relied on in the FISA applications. We were told by the Supervisory Intel Analyst that, as of September 2017, the FBI had corroborated limited information in the Steele election reporting, and much of that was publicly available information. Most relevant to the Carter Page FISA applications, the allegations contained in Reports 80, 94, 95, and 102, which were relied upon in all four applications, remained uncorroborated and, in several instances, were inconsistent with information gathered by the Crossfire Hurricane team.

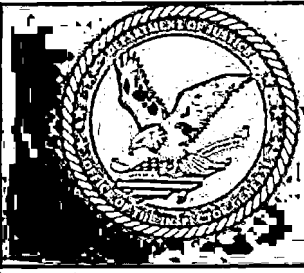


The Three Renewal Applications for Continued FISA Authority on Carter Page

As noted above, the FBI filed three renewal applications with the FISC, on January 12, April 7, and June 29, 2017. In addition to repeating the seven significant errors contained in the first FISA application and outlined above, we identified 10 additional

significant errors in the three renewal applications, based upon information known to the FBI after the first application and before one or more of the renewals. We describe the circumstances surrounding these 10 errors in Chapter Eight, and provide a chart listing additional errors in Appendix One. As more fully described in Chapter Eight, the renewal applications:

8. Omitted the fact that Steele's Primary Sub-source, who the FBI found credible, had made statements in January 2017 raising significant questions about the reliability of allegations included in the FISA applications, including, for example, that he/she did not recall any discussion with Person 1 concerning WikiLeaks and there was "nothing bad" about the communications between the Kremlin and the Trump team, and that he/she did not report to Steele in July 2016 that Page had met with Sechin;
9. Omitted Page's prior relationship with another U.S. government agency, despite being reminded by the other agency in June 2017, prior to the filing of the final renewal application, about Page's past status with that other agency; instead of including this information in the final renewal application, the OGC Attorney altered an email from the other agency so that the email stated that Page was "not a source" for the other agency, which the FBI affiant relied upon in signing the final renewal application;
10. Omitted information from persons who previously had professional contacts with Steele or had direct knowledge of his work-related performance, including statements that Steele had no history of reporting in bad faith but "[d]emonstrates lack of self-awareness, poor judgment," "pursued people with political risk but no intelligence value," "didn't always exercise great judgment," and it was "not clear what he would have done to validate" his reporting;
11. Omitted information obtained from Ohr about Steele and his election reporting, including that (1) Steele's reporting was going to Clinton's presidential campaign and others, (2) Simpson was paying Steele to discuss his reporting with the media, and (3) Steele was "desperate that Donald Trump not get elected and was passionate about him not being the U.S. President";



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

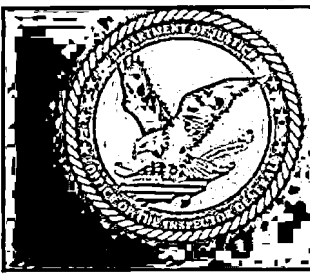
12. Failed to update the description of Steele after information became known to the Crossfire Hurricane team, from Ohr and others, that provided greater clarity on the political origins and connections of Steele's reporting, including that Simpson was hired by someone associated with the Democratic Party and/or the DNC;
13. Failed to correct the assertion in the first FISA application that the FBI did not believe that Steele directly provided information to the reporter who wrote the September 23 *Yahoo News* article, even though there was no information in the Woods File to support this claim and even after certain Crossfire Hurricane officials learned in 2017, before the third renewal application, of an admission that Steele made in a court filing about his interactions with the news media in the late summer and early fall of 2016;
14. Omitted the finding from a FBI source validation report that Steele was suitable for continued operation but that his past contributions to the FBI's criminal program had been "minimally corroborated," and instead continued to assert in the source characterization statement that Steele's prior reporting had been "corroborated and used in criminal proceedings";
15. Omitted Papadopoulos's statements to an FBI CHS in late October 2016 denying that the Trump campaign was involved in the circumstances of the DNC email hack;
16. Omitted Joseph Mifsud's denials to the FBI that he supplied Papadopoulos with the information Papadopoulos shared with the FFG (suggesting that the campaign received an offer or suggestion of assistance from Russia); and
17. Omitted information indicating that Page played no role in the Republican platform change on Russia's annexation of Ukraine as alleged in the Report 95, which was inconsistent with a factual assertion relied upon to support probable cause in all four FISA applications.

Among the most serious of the 10 additional errors we found in the renewal applications was the FBI's failure to advise OI or the court of the inconsistencies, described in detail in Chapter Six, between Steele and his Primary Sub-source on the reporting relied upon in the FISA applications. Although the Primary Sub-source's account of these communications, if true, was not consistent with and, in fact, contradicted the allegations of a "well-developed

conspiracy" in Reports 95 and 102 attributed to Person 1, the FBI did not share this information with OI. The FBI also failed to share other inconsistencies with OI, including the Primary Sub-source's account of the alleged meeting between Page and Sechin in Steele's Report 94 and his/her descriptions of the source network. The fact that the Primary Sub-source's account contradicted key assertions attributed to his/her own sub-sources in Steele's Reports 94, 95, and 102 should have generated significant discussions between the Crossfire Hurricane team and OI prior to submitting the next FISA renewal application. According to Evans, had OI been made aware of the information, such discussions might have included the possibility of foregoing the renewal request altogether, at least until the FBI reconciled the differences between Steele's account and the Primary Sub-source's account to the satisfaction of OI. However, we found no evidence that the Crossfire Hurricane team ever considered whether any of the inconsistencies warranted reconsideration of the FBI's assessment of the reliability of the Steele reports or notice to OI before the subsequent renewal applications were filed.

Instead, the second and third renewal applications provided no substantive information concerning the Primary Sub-source's interview, and offered only a brief conclusory statement that the FBI met with the Primary Sub-source "[i]n an effort to further corroborate Steele's reporting" and found the Primary Sub-source to be "truthful and cooperative." We believe that including this statement, without also informing OI and the court that the Primary Sub-source's account of events contradicted key assertions in Steele's reporting, left a misimpression that the Primary Sub-source had corroborated the Steele reporting. Indeed, in a letter to the FISC in July 2018, before learning of these inconsistencies from us during this review, the Department defended the reliability of Steele's reporting and the FISA applications by citing, in part, to the Primary Sub-source's interview as "additional information corroborating [Steele's] reporting" and noting the FBI's determination that he/she was "truthful and cooperative."

The renewal applications also continued to fail to include information regarding Carter Page's past relationship with another U.S. government agency, even though both OI and members of the Crossfire Hurricane expressed concern about the possibility of a prior relationship following interviews that Page gave to news outlets in April and May 2017 stating that he had assisted other U.S. government agencies in the past. As we describe in Chapter Eight, in June 2017, SSA 2, who was to be the affiant for Renewal Application No. 3



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

and had been the affiant for the first two renewals, told us that he wanted a definitive answer to whether Page had ever been a source for another U.S. government agency before he signed the final renewal application. This led to interactions between the OGC Attorney assigned to Crossfire Hurricane and a liaison from the other U.S. government agency. In an email from the liaison to the OGC Attorney, the liaison provided written guidance, including that it was the liaison's recollection that Page had or continued to have a relationship with the other agency, and directed the OGC Attorney to review the information that the other agency had provided to the FBI in August 2016. As noted above, that August 2016 information stated that Page did, in fact, have a prior relationship with that other agency. The next morning, immediately following a 28 minute telephone call between the OGC Attorney and the OI Attorney, the OGC Attorney forwarded to the OI Attorney the liaison's email (but not the original email from the OGC Attorney to the liaison setting out the questions he was asking). The OI Attorney responded to the OGC Attorney, "thanks I think we are good and no need to carry it any further." However, when the OGC Attorney subsequently sent the liaison's email to SSA 2, the OGC Attorney altered the liaison's email by inserting the words "not a source" into it, thus making it appear that the liaison had said that Page was "not a source" for the other agency. Relying upon this altered email, SSA 2 signed the third renewal application that again failed to disclose Page's past relationship with the other agency. Consistent with the Inspector General Act of 1978, following the OIG's discovery that the OGC Attorney had altered and sent the email to SSA 2, who thereafter relied on it to swear out the third FISA application, the OIG promptly informed the Attorney General and the FBI Director and provided them with the relevant information about the OGC Attorney's actions.

None of the inaccuracies and omissions that we identified in the renewal applications were brought to the attention of OI before the applications were filed. As a result, similar to the first application, the Department officials who reviewed one or more of the renewal applications, including Yates, Boente, and Rosenstein, did not have accurate and complete information at the time they approved them.

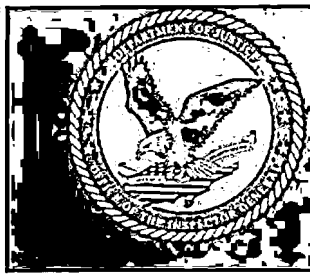
We do not speculate whether or how having accurate and complete information might have influenced the decisions of senior Department leaders who supported the four FISA applications, or the court, if they had known all of the relevant information. Nevertheless, it was the obligation of the FBI agents and supervisors who were aware of the information to

ensure that the FISA applications were "scrupulously accurate" and that OI, the Department's decision makers, and ultimately, the court had the opportunity to consider the additional information and the information omitted from the first application. The individuals involved did not meet this obligation.

Conclusions Concerning All Four FISA Applications

We concluded that the failures described above and in this report represent serious performance failures by the supervisory and non-supervisory agents with responsibility over the FISA applications. These failures prevented OI from fully performing its gatekeeper function and deprived the decision makers the opportunity to make fully informed decisions. Although some of the factual misstatements and omissions we found in this review were arguably more significant than others, we believe that all of them taken together resulted in FISA applications that made it appear that the information supporting probable cause was stronger than was actually the case.

We identified at least 17 significant errors or omissions in the Carter Page FISA applications, and many additional errors in the Woods Procedures. These errors and omissions resulted from case agents providing wrong or incomplete information to OI and failing to flag important issues for discussion. While we did not find documentary or testimonial evidence of intentional misconduct on the part of the case agents who assisted OI in preparing the applications, or the agents and supervisors who performed the Woods Procedures, we also did not receive satisfactory explanations for the errors or problems we identified. In most instances, the agents and supervisors told us that they either did not know or recall why the information was not shared with OI, that the failure to do so may have been an oversight, that they did not recognize at the time the relevance of the information to the FISA application, or that they did not believe the missing information to be significant. On this last point, we believe that case agents may have improperly substituted their own judgments in place of the judgment of OI, or in place of the court, to weigh the probative value of the information. Further, the failure to update OI on all significant case developments relevant to the FISA applications led us to conclude that the agents and supervisors did not give appropriate attention or treatment to the facts that cut against probable cause, or reassess the information supporting probable cause as the investigation progressed. The agents and SSAs also did not follow, or appear to even



Executive Summary

- Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

know, the requirements in the Woods Procedures to re-verify the factual assertions from previous applications that are repeated in renewal applications and verify source characterization statements with the CHS handling agent and document the verification in the Woods File.

That so many basic and fundamental errors were made by three separate, hand-picked teams on one of the most sensitive FBI investigations that was briefed to the highest levels within the FBI, and that FBI officials expected would eventually be subjected to close scrutiny, raised significant questions regarding the FBI chain of command's management and supervision of the FISA process. FBI Headquarters established a chain of command for Crossfire Hurricane that included close supervision by senior CD managers, who then briefed FBI leadership throughout the investigation. Although we do not expect managers and supervisors to know every fact about an investigation, or senior officials to know all the details of cases about which they are briefed, in a sensitive, high-priority matter like this one, it is reasonable to expect that they will take the necessary steps to ensure that they are sufficiently familiar with the facts and circumstances supporting and potentially undermining a FISA application in order to provide effective oversight, consistent with their level of supervisory responsibility. We concluded that the information that was known to the managers, supervisors, and senior officials should have resulted in questions being raised regarding the reliability of the Steele reporting and the probable cause supporting the FISA applications, but did not.

In our view, this was a failure of not only the operational team, but also of the managers and supervisors, including senior officials, in the chain of command. For these reasons, we recommend that the FBI review the performance of the employees who had responsibility for the preparation, Woods review, or approval of the FISA applications, as well as the managers and supervisors in the chain of command of the Carter Page investigation, including senior officials, and take any action deemed appropriate. In addition, given the extensive compliance failures we identified in this review, we believe that additional OIG oversight work is required to assess the FBI's compliance with Department and FBI FISA-related policies that seek to protect the civil liberties of U.S. persons. Accordingly, we have today initiated an OIG audit that will further examine the FBI's compliance with the Woods Procedures in FISA applications that target U.S. persons in both counterintelligence and counterterrorism investigations. This audit will be informed by the findings in this review, as well as by our prior work over

the past 15 years on the Department's and FBI's use of national security and surveillance authorities, including authorities under FISA, as detailed in Chapter One.

Issues Relating to Department Attorney Bruce Ohr

In Chapter Nine, we describe the interactions Department attorney Bruce Ohr had with Christopher Steele, the FBI, Glenn Simpson (the owner of Fusion GPS), and the State Department during the Crossfire Hurricane investigation. At the time of these interactions, which took place from about July 2016 to May 2017, Ohr was an Associate Deputy Attorney General in the Office of the Deputy Attorney General (ODAG) and the Director of the Organized Crime and Drug Enforcement Task Force (OCDEF).

Ohr's Interactions with Steele, the FBI, Simpson, and the State Department

Beginning in July 2016, at about the same time that Steele was engaging with the FBI on his election reporting, Steele contacted Ohr, who he had known since at least 2007, to discuss information from Steele's election reports. At Steele's suggestion, Ohr also met in August 2016 with Simpson to discuss Steele's reports. At the time, Ohr's wife, Nellie Ohr, worked at Fusion GPS as an independent contractor. Ohr also met with Simpson in December 2016, at which time Simpson gave Ohr a thumb drive containing numerous Steele election reports that Ohr thereafter provided to the FBI.

On October 18, 2016, after speaking with Steele that morning, Ohr met with McCabe to share Steele's and Simpson's information with him. Thereafter, Ohr met with members of the Crossfire Hurricane team 13 times between November 21, 2016, and May 15, 2017, concerning his contacts with Steele and Simpson. All 13 meetings occurred after the FBI had closed Steele as a CHS and, except for the November 21 meeting, each meeting was initiated at Ohr's request. Ohr told us that he did not recall the FBI asking him to take any action regarding Steele or Simpson, but Ohr also stated that "the general instruction was to let [the FBI] know...when I got information from Steele." The Crossfire Hurricane team memorialized each of the meetings with Ohr as an "interview" using an FBI FD-302 form. Separately, in November 2016, Ohr met with senior State Department officials regarding Steele's election reporting.



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

Department leadership, including Ohr's supervisors in ODAG and the ODAG officials who reviewed and approved the Carter Page FISA applications, were unaware of Ohr's meetings with FBI officials, Steele, Simpson, and the State Department until after Congress requested information from the Department regarding Ohr's activities in late November 2017.

We did not identify a specific Department policy prohibiting Ohr from meeting with Steele, Simpson, or the State Department and providing the information he learned from those meetings to the FBI. However, Ohr was clearly cognizant of his responsibility to inform his supervisors of these interactions, and acknowledged to the OIG that the possibility that he would have been told by his supervisors to stop having such contact may have factored into his decision not to tell them about it.

We concluded that Ohr committed consequential errors in judgment by (1) failing to advise his direct supervisors or the DAG that he was communicating with Steele and Simpson and then requesting meetings with the FBI's Deputy Director and Crossfire Hurricane team on matters that were outside of his areas of responsibility, and (2) making himself a witness in the investigation by meeting with Steele and providing Steele's information to the FBI. As we describe in Chapter Eight, the late discovery of Ohr's meetings with the FBI prompted NSD to notify the FISC in July 2018, over a year after the final FISA renewal order was issued, of information that Ohr had provided to the FBI but that the FBI had failed to inform NSD and OI about (and therefore was not included in the FISA applications), including that Steele was "desperate that Donald Trump not get elected and was passionate about him not being the U.S. President."

FBI Compliance with Policies

The FBI's CHS Policy Guide (CHSPG) provides guidance to agents concerning contacts with CHSs after they have been closed for cause, as was the case with Steele as of November 2016. According to the CHSPG, a handling agent must not initiate contact with or respond to contacts from a former CHS who has been closed for cause absent exceptional circumstances that are approved by an SSA. The CHSPG also requires reopening of the CHS if the relationship between the FBI and a closed CHS is expected to continue beyond the initial contact or debriefing. Reopening requires high levels of supervisory approval, including a finding that the benefits of reopening the CHS outweigh the risks.

We found that, while the Crossfire Hurricane team did not initiate direct contact with Steele after his closure, it responded to numerous contacts made by Steele through Ohr. Ohr himself was not a direct witness in the Crossfire Hurricane investigation; rather, his purpose in communicating with the FBI was to pass along information from Steele. While the FBI's CHS policy does not explicitly address indirect contact between an FBI agent and a closed CHS, we concluded that the repeated contacts with Steele should have triggered the CHS policy requiring that such contacts occur only after an SSA determines that exceptional circumstances exist. While an SSA was present for the meetings with Ohr, we found no evidence that the SSAs made considered judgments that exceptional circumstances existed for the repeated contacts. We also found that, given that there were 13 different meetings with Ohr over a period of months, the use of Ohr as a conduit between the FBI and Steele created a relationship by proxy that should have triggered, pursuant to FBI policy, a supervisory decision about whether to reopen Steele as a CHS or discontinue accepting information indirectly from him through Ohr.

Ethics Issues Raised by Nellie Ohr's Former Employment with Fusion GPS

Fusion GPS employed Nellie Ohr as an independent contractor from October 2015 to September 2016. On his annual financial disclosure forms covering calendar years 2015 and 2016, Ohr listed Nellie Ohr as an "independent contractor" and reported her income from that work on the form. We determined that financial disclosure rules, 5 C.F.R. Part 2634, did not require Ohr to list on the form the specific organizations, such as Fusion GPS, that paid Nellie Ohr as an independent contractor during the reporting period.

In addition, for reasons we explain in Chapter Eleven, we concluded that the federal ethics rules did not require Ohr to obtain Department ethics counsel approval before engaging with the FBI in connection with the Crossfire Hurricane matter because of Nellie Ohr's prior work for Fusion GPS. However, we found that, given the factual circumstances that existed, and the appearance that they created, Ohr displayed a lapse in judgment by not availing himself of the process described in the ethics rules to consult with the Department ethics official about his involvement in the investigation.

Meetings Involving Ohr, CRM officials, and the FBI Regarding the MLARS Investigation



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

Ohr's supervisors in ODAG also were unaware that Ohr, shortly after the U.S. elections in November 2016, and again in early 2017, participated in discussions about a money laundering investigation of Manafort that was then being led by prosecutors from the Money Laundering and Asset Recovery Section (MLARS), which is located in the Criminal Division (CRM) at the Department's headquarters.

As described in more detail in Chapter Nine, in November 2016, Ohr told CRM Deputy Assistant Attorney General Bruce Swartz and Counsel to the CRM Assistant Attorney General Zainab Ahmad about information he was getting from Steele and Simpson about Manafort. Between November 16, 2016 and December 15, 2016, Ohr participated in several meetings that were attended, at various times, by some or all of the following individuals: Swartz, Ahmad, Andrew Weissmann (then Section Chief of CRM's Fraud Section), Strzok, and Lisa Page. The meetings involving Ohr, Swartz, Ahmad, and Weissmann focused on their shared concern that MLARS was not moving quickly enough on the Manafort criminal investigation and whether there were steps they could take to move the investigation forward. The meetings with Strzok and Page focused primarily on whether the FBI could assess the case's relevance, if any, to the FBI's Russian interference investigation. MLARS was not represented at any of these meetings or told about them, and none of attendees had supervisory responsibility over the MLARS investigation.

There were no meetings about the Manafort case involving Ohr, Swartz, Ahmad, and Weissmann from December 16, 2016 to January 30, 2017. On January 31, 2017, one day after Yates was removed as DAG, Ahmad, by then an Acting CRM Deputy Assistant Attorney General, after consulting with Swartz and Weissmann, sent an email to Lisa Page, copying Weissmann, Swartz, and Ohr, requesting a meeting the next day to discuss "a few Criminal Division related developments." The next day, February 1, Swartz, Ohr, Ahmad, and Weissmann met with Strzok, Lisa Page, and an FBI Acting Section Chief. None of the attendees at the meeting could explain to us what the "Criminal Division related developments" were, and we did not find any. Meeting notes reflect, among other things, that the group discussed the Manafort criminal investigation and efforts that the Department could undertake to investigate attempts by Russia to influence the 2016 elections. MLARS was not represented at, or told about, the meeting.

We are not aware of information indicating that any of the discussions involving Ohr, Swartz,

Weissmann, Ahmad, Strzok, and Lisa Page resulted in any actions taken or not taken in the MLARS investigation, and ultimately the investigation remained with MLARS until it was transferred to the Office of the Special Counsel in May 2017. We also did not identify any Department policies prohibiting internal discussions about a pending investigation among officials not assigned to the matter, or between those officials and senior officials from the FBI. However, as described in Chapter Nine, we were told that there was a decision not to inform the leadership of CRM, both before and after the change in presidential administrations, of these discussions in order to insulate the MLARS investigation from becoming "politicized." We concluded that this decision, made in the absence of concerns of potential wrongdoing or misconduct, and for the purpose of avoiding the appearance that an investigation is "politicized," fundamentally misconstrued who is ultimately responsible and accountable for the Department's work. We agree with the concerns expressed to us by then DAG Yates and then CRM Assistant Attorney General Leslie Caldwell. Department leaders cannot fulfill their management responsibilities, and be held accountable for the Department's actions, if subordinates intentionally withhold information from them in such circumstances.

The Use of Confidential Sources (Other Than Steele) and Undercover Employees

As discussed in Chapter Ten, we determined that, during the 2016 presidential campaign, the Crossfire Hurricane team tasked several CHSs, which resulted in multiple interactions with Carter Page and George Papadopoulos, both during and after the time they were affiliated with the Trump campaign, and one with a high-level Trump campaign official who was not a subject of the investigation. All of these CHS interactions were consensually monitored and recorded by the FBI. As noted above, under Department and FBI policy, the use of a CHS to conduct consensual monitoring is a matter of investigative judgment that, absent certain circumstances, can be authorized by a first-line supervisor (a supervisory special agent). We determined that the CHS operations conducted during Crossfire Hurricane received the necessary FBI approvals, and that AD Priestap knew about, and approved of, all of the Crossfire Hurricane CHS operations, even in circumstances where a first-level supervisory special agent could have approved the operations. We found no evidence that the FBI used CHSs or UCEs to interact with members of the Trump campaign prior to the opening of the Crossfire Hurricane investigation. After the opening of the investigation, we



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

found no evidence that the FBI placed any CHSs or UCEs within the Trump campaign or tasked any CHSs or UCEs to report on the Trump campaign. Finally, we also found no documentary or testimonial evidence that political bias or improper motivations influenced the FBI's decision to use CHSs or UCEs to interact with Trump campaign officials in the Crossfire Hurricane investigation.

Although the Crossfire Hurricane team's use of CHSs and UCEs complied with applicable policies, we are concerned that, under these policies, it was sufficient for a first-level FBI supervisor to authorize the domestic CHS operations that were undertaken in Crossfire Hurricane, and that there was no applicable Department or FBI policy requiring the FBI to notify Department officials of the investigative team's decision to task CHSs to consensually monitor conversations with members of a presidential campaign. We found no evidence that the FBI consulted with any Department officials before conducting these CHS operations. We believe that current Department and FBI policies are not sufficient to ensure appropriate oversight and accountability when such operations potentially implicate sensitive, constitutionally protected activity, and that they should require, at minimum, Department consultation. As noted above, we include a recommendation in this report to address this issue.

Consistent with current Department and FBI policy, we learned that decisions about the use of CHSs and UCEs were made by the case agents and the supervisory special agents assigned to Crossfire Hurricane. These agents told the OIG that they focused the CHS operations on the FFG information and the four investigative subjects, and that they viewed CHS operations as one of the best methods available to quickly obtain information about the predicated allegations, while preventing information about the nature and existence of the investigation from becoming public, and potentially impacting the presidential election.

During the meeting between a CHS and the high-level Trump campaign official who was not a subject of the investigation, the CHS asked about the role of three Crossfire Hurricane subjects—Page, Papadopoulos, and Manafort—in the Trump campaign. The CHS also asked about allegations in public reports concerning Russian interference in the 2016 elections, the campaign's response to ideas featured in Page's Moscow speech, and the possibility of an "October Surprise." In response, the campaign official made no comments of note about those topics. The CHS and the high-level campaign official also discussed [REDACTED]

[REDACTED] We found that the Crossfire Hurricane team made no use of any information collected from the high-level Trump campaign official, because the team determined that none of the information gathered was "germane" to the allegations under investigation. However, we were concerned that the Crossfire Hurricane team did not recall having in place a plan, prior to the operation involving the high-level campaign official, to address the possible collection of politically sensitive information.

As discussed in Chapter Ten, through the use of CHSs, the investigative team obtained statements from Carter Page and Papadopoulos that raised questions about the validity of allegations under investigation. For example, when questioned in August 2016 about other individuals who were subjects in the investigation, Page told a CHS that he had "literally never met" or "said one word to" Manafort and that Manafort had not responded to any of Page's emails. As another example, Papadopoulos denied to a CHS that anyone associated with the Trump campaign was collaborating with Russia or with outside groups like WikiLeaks in the release of emails. Papadopoulos stated that the "campaign, of course, [does not] advocate for this type of activity because at the end of the day it's...illegal" and that "our campaign is not...engag[ing] or reaching out to WikiLeaks or to the whoever it is to tell them please work with us, collaborate because we don't, no one does that...." Papadopoulos also said that "as far as I understand...no one's collaborating, there's been no collusion and it's going to remain that way." In another interaction, Papadopoulos told a CHS that he knew "for a fact" that no one from the Trump campaign had anything to do with releasing emails from the DNC, as a result of Papadopoulos's involvement in the Trump campaign. Despite the relevance of this material, as described in Chapters Five and Seven, none of Papadopoulos's statements were provided by the Crossfire Hurricane team to the OI Attorney and Page's statements were not provided to the OI attorney until June 2017, approximately ten months after the initial Carter Page FISA application was granted by the FISC.

Through our review, we also determined that there were other CHSs tasked by the FBI to attempt to contact Papadopoulos, but that those attempted contacts did not lead to any operational activity. We also identified several individuals who had either a connection to candidate Trump or a role in the Trump



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

campaign, and were also FBI CHSs, but who were not tasked as part of the Crossfire Hurricane investigation. One such CHS did provide the Crossfire Hurricane team with general information about Crossfire Hurricane subjects Page and Manafort, but we found that this CHS had no further involvement in the investigation.

We identified another CHS that the Crossfire Hurricane team first learned about in 2017, after the CHS voluntarily provided his/her handling agent with an

—and the handling agent forwarded the material, through his supervisor and FBI Headquarters, to the Crossfire Hurricane team.

The handling agent told us that, when he subsequently informed the Crossfire Hurricane team that the CHS had access to [REDACTED], a Crossfire Hurricane team intelligence analyst asked the handling agent to collect [REDACTED] from the CHS, which the handling agent did. We found that the Crossfire Hurricane team determined that there was not “anything significant” in this [REDACTED] collection, and did not seek to task the CHS. While we found that no action was taken by the Crossfire Hurricane team in response to receiving [REDACTED], we nevertheless were concerned to learn that the handling agent for the CHS placed [REDACTED] into the FBI’s files, and we promptly notified the FBI upon learning that they were still being maintained in the FBI’s files. We further concluded that, because the CHS’s handling agent did not understand the CHS’s political involvement, no assessment was performed by the source’s handling agent or his supervisors (none of whom were members of the Crossfire Hurricane team) to determine whether the CHS required re-designation as a “sensitive source” or should have been closed during the pendency of the campaign.

While we concluded that the investigative activities undertaken by the Crossfire Hurricane team involving CHSs and UCEs complied with applicable Department and FBI policies, we believe that in certain circumstances Department and FBI policies do not provide sufficient oversight and accountability for investigative activities that have the potential to gather sensitive information involving protected First Amendment activity, and therefore include recommendations to address these issues.

Finally, as we also describe in Chapter Ten, we learned during the course of our review that in August

2016, the supervisor of the Crossfire Hurricane investigation, SSA 1, participated on behalf of the FBI in a strategic intelligence briefing given by Office of the Director of National Intelligence (ODNI) to candidate Trump and his national security advisors, including Michael Flynn, and in a separate strategic intelligence briefing given to candidate Clinton and her national security advisors. The stated purpose of the FBI portion of the briefing was to provide the recipients “a baseline on the presence and threat posed by foreign intelligence services to the National Security of the U.S.” However, we found that SSA 1 was selected to provide the FBI briefings, in part, because Flynn, who was a subject in the ongoing Crossfire Hurricane investigation, would be attending the Trump campaign briefing.

Following his participation in the briefing of candidate Trump, Flynn, and another Trump advisor, SSA 1 drafted an EC documenting his participation in the briefing, and added the EC to the Crossfire Hurricane investigative file. We were told that the decision to select SSA 1 to participate in the ODNI briefing was reached by consensus among a group of senior FBI officials, including McCabe and Baker. We noted that no one at the Department or ODNI was informed that the FBI was using the ODNI briefing of a presidential candidate for investigative purposes, and found no applicable FBI or Department policies addressing this issue. We concluded that the FBI’s use of this briefing for investigative reasons could potentially interfere with the expectation of trust and good faith among participants in strategic intelligence briefings, thereby frustrating their purpose. We therefore include a recommendation to address this issue.

Recommendations

Our report makes nine recommendations to the FBI and the Department to assist them in addressing the issues that we identified in this review:

- The Department and the FBI should ensure that adequate procedures are in place for OI to obtain all relevant and accurate information needed to prepare FISA applications and renewal applications, including CHS information. In Chapter Twelve, we identify a few specific steps to assist in this effort.



Executive Summary

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

- The Department and FBI should evaluate which types of SIMs require advance notification to a senior Department official, such as the DAG, in addition to the notifications currently required for SIMs, especially for case openings that implicate core First Amendment activity and raise policy considerations or heighten enterprise risk, and establish implementing policies and guidance, as necessary.
- The FBI should develop protocols and guidelines for staffing and administrating any future sensitive investigative matters from FBI Headquarters.
- The FBI should address the problems with the administration and assessment of CHSs identified in this report, including, at a minimum, revising the FBI's standard CHS admonishments, improving the documentation of CHS information, revising FBI policy to address the acceptance of information from a closed CHS indirectly through a third party, and taking other steps we identify in Chapter Twelve.
- The Department and FBI should clarify the terms (1) "sensitive monitoring circumstance" in the AG Guidelines and the DIOG to determine whether to expand its scope to include consensual monitoring of a domestic political candidate or an individual prominent within a domestic political organization, or a subset of these persons, so that consensual monitoring of such individuals would require consultation with or advance notification to a senior Department official, such as the DAG, and (2) "prominent in a domestic political organization" so that agents understand which campaign officials fall within that definition as it relates to "sensitive investigative matters," "sensitive UDP," the designation of "sensitive sources," and "sensitive monitoring circumstance."
- The FBI should ensure that appropriate training on DIOG § 4 is provided to emphasize the constitutional implications of certain monitoring situations and to ensure that agents account for these concerns, both in the tasking of CHSs and in the way they document interactions with and tasking of CHSs.
- The FBI should establish a policy regarding the use of defensive and transition briefings for investigative purposes, including the factors to be considered and approval by senior leaders at the FBI with notice to a senior Department official, such as the DAG.
- The Department's Office of Professional Responsibility should review our findings related to the conduct of Department attorney Bruce Ohr for any action it deems appropriate. Ohr's current supervisors in CRM should also review our findings related to Ohr's performance for any action they deem appropriate.
- The FBI should review the performance of all employees who had responsibility for the preparation, Woods review, or approval of the FISA applications, as well as the managers, supervisors, and senior officials in the chain of command of the Carter Page investigation for any action it deems appropriate.

Trump and was an "open secret" in Putin's government; (2) sex videos existed of Trump; and (3) the FSB funneled payments to Trump through an Azerbaijani family. According to Steele's notation to the report, Steele did not have a way to verify the source(s) or the information but noted that, even though the reporting originated from a different source network, some of it was "remarkably similar" to Steele's reporting, especially with regard to the alleged 2013 Ritz Carlton incident involving Trump and prostitutes, Trump's compromise by the FSB, and the Kremlin's funding of the Trump campaign by way of the Azerbaijani family. The Supervisory Intel Analyst characterized the report as "yet another report that would need to be evaluated."

In addition to continuing to provide reporting to the FBI, Steele also was, unbeknownst to the FBI at the time, continuing his outreach to the media concerning alleged contacts between the Trump campaign and the Russian government. According to information from the foreign litigation noted above, Steele returned to Washington, D.C., in mid-October and provided additional briefings to *The New York Times*, *The Washington Post*, and *Yahoo News*. We asked Steele why he did not advise the FBI of his engagements with the media. He stated that he did not alert the FBI because the media briefings were part of his contract with Fusion GPS and were set up and attended by Simpson. As noted above, Steele did not believe that the FBI had raised the issue of media contacts with him at the early October meeting, and his contemporaneous notes from that meeting do not mention the issue.

Further, Steele met on October 11 at the State Department with Winer and Deputy Assistant Secretary Kathleen Kavalec, who was a deputy to then Assistant Secretary Victoria Nuland. Steele told us that Winer had originally contacted him to request that he meet with Nuland, who ultimately did not attend.²⁵⁵ Notes of the meeting taken by State Department staff reflect that Steele addressed a wide array of topics during the meeting, including:

- Derogatory information on Trump;
- Manafort's role as a "go-between" with the campaign and Kremlin;
- The role of Alfa Bank, one of Russia's largest privately owned banks, as a conduit for secret communications between Manafort and the Kremlin;
- Manafort's debts to the Russians;
- Carter Page's meeting with Sechin;
- The Russian Embassy's management of a network of Russian émigrés in the United States who carry out hacking and recruiting operations; and

²⁵⁵ Steele told us that he was delayed from the airport and arrived late for the meeting, by which time Nuland had departed.

- The Russian cyber penetration of the DNC.²⁵⁶

The notes also indicate that Steele explained that the information his firm collected on the connection between Trump and Russia came from [REDACTED], [REDACTED]

[REDACTED] According to the notes, Steele stated that [REDACTED]

[REDACTED] The notes also state that Steele's firm had [REDACTED]

We asked Kavalec about the meeting with Steele. She stated that Nuland did not ask to meet with Steele and that Nuland requested she attend the meeting because Nuland did not want to devote time to it. It was Kavalec's understanding that Steele sought the meeting with Nuland as part of a wider effort to disseminate his election report findings to persons in Washington, D.C. She stated that during the meeting Steele expressed frustration that the FBI had not acted on his reporting and explained that when he first offered information to the FBI he found a lack of interest.

Kavalec told us that shortly after the meeting with Steele, she encountered the FBI's liaison to the State Department and mentioned the meeting to him. According to Kavalec, she explained to the liaison that she was willing to be interviewed by the FBI regarding her meeting with Steele, though Steele had informed her that he had already been in contact with the FBI to share his reporting. The FBI liaison told us that Kavalec also informed him that a particular piece of information in Steele's reporting appeared to be incorrect. She explained to the FBI liaison that Russia did not have a consulate in Miami as indicated by Steele's reporting, which claimed that a cyber-hacking operation was being run, in part, out of the Russian consulate in Miami.²⁵⁷ The FBI liaison informed SSA 1 and Case Agent 1 via email on November 18 that Kavalec had met with Steele, she had taken notes of their meeting, the liaison could obtain information from Kavalec about the meeting, and, according to Kavalec, the information from Steele's reporting about a Russian consulate being located in Miami was inaccurate.²⁵⁸ The

²⁵⁶ Much of the information presented by Steele at the State Department briefing can be found in Reports 130 and 132, both of which Steele provided to the FBI in October.

²⁵⁷ Kavalec's typed notes from Steele's October 11, 2016 briefing stated that Steele told her that a Russian cyber hacking operation targeting the 2016 U.S. elections was making payments to involved persons from "the Russian [c]onsulate in Miami." Steele's election Report 95 contained similar, but not fully consistent, information. Report 95 did not explicitly state that there was a Russian consulate in Miami. Instead, Report 95 stated that Russian consular officials and diplomatic staff in Miami were making payments in order to facilitate a secret exchange of intelligence between persons affiliated with Trump and the Russian government.

²⁵⁸ After reviewing a portion of our draft report and his November 18, 2016 email to SSA 1 and Case Agent 1, the FBI liaison told us that he believes that he first learned about Kavalec's meeting with Steele on or about November 18, 2016.

FBI liaison told us that he received no directives from the Crossfire Hurricane team to gather information from Kavalec regarding her contact with Steele.

In anticipation of an FBI interview, Kavalec said she prepared a typewritten summary of the meeting within 1 to 2 weeks after talking with the liaison. The typed summary began by noting that Steele said at the meeting that he had undertaken the investigation "at the behest of an institution he declined to identify that had been hacked." The summary also noted that Steele told the attendees that the "institution...is keen to see this information come to light prior to November 8." However, the FBI did not interview Kavalec nor did they seek her notes.

Two days after the meeting with Steele, Kavalec emailed an FBI CD Section Chief a document that Kavalec received from Winer discussing allegations about a linkage between Alfa Bank and the Trump campaign, a topic that was discussed at the October 11 meeting.²⁵⁹ Kavalec advised the FBI Section Chief in the email that the information related to an investigation that Steele's firm had been conducting. The Section Chief forwarded the document to SSA 1 the same day.

We asked Steele why he did not inform the FBI of the meeting at the State Department and why he did not abide by the FBI's request for exclusivity. He said he did not think it was appropriate to turn down a meeting request from an Assistant Secretary of State, which he said he received on short notice. He also stated that, at the time he received the meeting request, the meeting agenda was unclear, and he was uncertain what topics he would be asked to discuss. He said it was his understanding that the FBI did not object to his discussing general themes with other agencies as opposed to "details" about his intelligence and source network.

Handling Agent 1 told us that he believed Steele should have alerted him to both his media contacts in September and October and his meeting with State Department staff in October. As noted above, the Crossfire Hurricane team first learned of Steele's October meeting with the State Department from the FBI liaison on November 18, by which date the FBI had already closed Steele as a CHS because of his *Mother Jones* disclosure, which we discuss in Chapter Six. Handling Agent 1 explained that Steele should have recognized the need to provide this notice to the FBI, especially given the discussions that took place with the Crossfire Hurricane team in early October.

²⁵⁹ Steele separately wrote in Report 112, dated September 14, 2016, that Alfa Bank allegedly had close ties to Putin. The Crossfire Hurricane team received Report 112 on or about November 6, 2016, from a *Mother Jones* journalist through then FBI General Counsel James Baker. Additionally, Ohr advised the FBI on November 21, 2016, according to an FBI FD-302, that Steele had told Ohr that the Alfa Bank server was a link to the Trump campaign and that Person 1's Russia/American organization in the U.S. had used the Alfa Bank server two weeks prior. Steele told us that the information about Alfa Bank was not generated by Orbis. The FBI investigated whether there were cyber links between the Trump Organization and Alfa Bank, but had concluded by early February 2017 that there were no such links. The Supervisory Intel Analyst told us that he factored the Alfa Bank/Trump server allegations into his assessment of Steele's reporting.

2. Ohr's August 22, 2016 Meeting with Simpson

On August 22, 2016, Simpson emailed Ohr requesting that Ohr call him. Later that same day, at Simpson's request, Ohr met with Simpson, and Simpson provided Ohr with the names of three individuals who Simpson thought were potential intermediaries between Russia and the Trump campaign.⁴¹⁴ The three names are included in notes that Ohr told us he wrote on the same day as his meeting with Simpson. According to these notes, one of the three names provided by Simpson was one of the sub-sources in Steele's election reports, who we reference as Person 1 in previous chapters. Another of the names was Carter Page's "[b]usiness partner" who was an "[a]lleged" Russian intelligence officer and "the 'brains' behind [Carter] Page's company—Global Energy Capital." Ohr stated that he was uncomfortable receiving this information from Simpson and did not recall Simpson asking him to do anything with it.

Ohr told the OIG that he was troubled by Simpson's information. He stated that he could not remember when or how he provided Simpson's information to the FBI, but would have likely contacted Handling Agent 1 or the FBI's Transnational Organized Crime-East (TOC-East) Section Chief. Emails indicate that Ohr and Handling Agent 1 spoke on August 24, 2016, but neither of them could recall what they discussed.⁴¹⁵

On September 12, 2016, Ohr and Handling Agent 1 exchanged emails referencing Steele. In one email, Handling Agent 1 informed Ohr that an FBI team was looking into Steele's information. In response, Ohr asked Handling Agent 1 to let him know who to contact with additional information. Handling Agent 1 told us that he did not reply to Ohr's question, and we did not find a response.

3. Ohr's September 23, 2016 Meeting with Steele

On September 23, 2016, at Steele's request, Steele met with Ohr in Washington, D.C. Ohr told us they spoke about various topics related to Russia, including information regarding Russian Oligarch 1's willingness to talk with the U.S. government about Manafort. Ohr said that Steele identified the person who was funding Fusion GPS's opposition research; however, according to Ohr, he did not recognize the name and could not remember it long enough to write it down after the meeting. Ohr also said that he and Steele also discussed allegations that an Alfa Bank server in the United States was a link between Russia and the Trump campaign; that Person 1's Russian/American organization in the United States had

⁴¹⁴ On November 14, 2017, Simpson testified before the House Permanent Select Committee on Intelligence. During his testimony, Simpson told the Committee that he did not meet with Ohr prior to the November 2016 presidential election. He stated further that he met with Ohr one time after Thanksgiving 2016. See *Interview of Glenn Simpson Before the Executive Session of the H. Perm. Select Comm. On Intelligence, 115th Cong. 78 (November 14, 2017) (hereinafter HPSCI Interview of Glenn Simpson)*.

⁴¹⁵ Department emails indicate that Ohr first spoke with the TOC-East Section Chief regarding Steele and Simpson's information in October 2016, which we discuss below.

used the Alfa Bank server earlier in September; and that an individual working with Carter Page was a Russian intelligence officer.

According to Steele, he and Ohr also discussed Steele's concerns that if Trump won the election, Steele's source network may be in jeopardy. Steele said that a new FBI Director and new agency heads appointed by Trump would have a higher degree of loyalty to the new President, and could decide to take action against Steele and his source network. Steele told us that Ohr explained that the FBI Director had a 10-year term and could not be removed from the position by the President, so information about Steele's source network should be protected.⁴¹⁶ According to Steele, he also asked Ohr about why it appeared from the news that the U.S. government was not addressing his election reporting. Steele said that Ohr told him that the Hatch Act made it a criminal offense for a federal official to make a public statement to the detriment or benefit of a candidate within 90 days of an election.⁴¹⁷ When we asked Ohr about this, he told us he did not recall talking to Steele about either of these concerns.

Ohr did not recall whether he provided anyone with the information he received from Steele at this meeting, but stated that he might have spoken to Swartz and Handling Agent 1 about it. Swartz told us that Ohr provided him with specific information at the time regarding Steele's reporting, but he could not recall the specific information when interviewed by the OIG. Handling Agent 1 told us he did not recall discussing these topics with Ohr.

4. Ohr's Early October 2016 Activities Regarding Steele's Information

Sometime prior to October 13, 2016, Ohr talked to the FBI's TOC-East Section Chief about Steele's information, but Ohr could not recall what he told him. The TOC-East Section Chief recalled Ohr mentioning Steele to him starting in mid-2016, but stated that he could not specifically recall the information Ohr relayed concerning Steele's election reporting.⁴¹⁸

In an October 13, 2016 email, the TOC-East Section Chief told Ohr that counterintelligence agents had traveled to a European city and spoken with Handling Agent 1. Ohr responded that he had additional information to share,

⁴¹⁶ This statement concerning the FBI Director's term is incorrect. The President has the authority to remove the FBI Director prior to the expiration of the 10-year term. See Pub. L. No. 94-503, § 203, 90 Stat. 2407 (1976); 5 U.S.C. § 532 notes.

⁴¹⁷ The Hatch Act does not address this issue. Rather, among other things, it prohibits federal employees from participating in certain political activities on and off duty. Section 7323(a)(1) provides that "an employee may not use his official authority or influence for the purpose of interfering with or affecting the result of an election." 5 U.S.C. § 7323(a)(1); 5 C.F.R. §§ 734, 734.401(a)(2), 734.407, 734.411.

⁴¹⁸ The TOC-East Section Chief noted that while it was odd to have a high-level Department official in contact with Russian oligarchs, it did not surprise him that Ohr would be approached by individuals, such as Steele, who wanted to talk to the U.S. government. The TOC-East Section Chief said that it would be "outside [of Ohr's] lane" to continue the relationship with these potential sources after their introduction to the FBI.

EXHIBIT 18

NOT A CERTIFIED COPY

Washington, DC

Page 1

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

SENATE JUDICIARY COMMITTEE
U.S. SENATE
WASHINGTON, D.C.

INTERVIEW OF: GLENN SIMPSON

TUESDAY, AUGUST 22, 2017
WASHINGTON, D.C.

The interview in this matter was held at the
Hart Senate Office Building, commencing at 9:34 a.m.

1 but you're saying whatever information you had was
2 not generated by Fusion GPS?

3 A. That's right. I know they're a big player
4 and they have long, deep ties to Vladimir Putin.
5 One of the founders, Pyotr Aven, P-Y-O-T-R, second
6 word Aven, A-V-E-N, was an associate of Vladimir
7 Putin when he was in the mayor's office in Saint
8 Petersburg around the time same that Bill Browder
9 was doing business with the mayor's office.
10 They're very powerful politically and economically
11 in Russia and they have -- in the tens of billions
12 are the assets of the founders and they have all
13 sorts of interests. They have epic disputes with
14 western corporations, including BP. So people in
15 my business tend to just have a lot of
16 institutional knowledge about them and, you know, I
17 shared my institutional knowledge about them.

18 Q. You mentioned other founders. Are those
19 other founders Mikhail Fridman and German Khan?

20 A. Yes.

21 Q. Do you have any information there have
22 been reports about potential communications between
23 a server at Alpha Bank and potentially servers that
24 belong to the Trump organization or Trump -- some
25 entity associated with Donald Trump? Do you have

1 any information about those particular reports?

2 A. That's kind of an open-ended question. I
3 think what I said is we were asked about that and
4 it wasn't -- that information wasn't generated by
5 us and I'm happy to say it's beyond our competence
6 to have generated, but in the course of being asked
7 about it, you know, people gave us information. I
8 don't know what else to say.

9 Q. And what information were you given?

10 A. A bunch of data. I mean, we were shown
11 like do you know what this would mean, does this
12 mean, and it's beyond -- it's really -- it's
13 certainly beyond my competence.

14 Q. So the data that you were shown, you could
15 not draw any conclusions from it?

16 A. I did not draw any conclusions from the
17 data.

18 Q. Another individual that there's been a lot
19 of press reporting on is Sergei Millian. Other
20 than what -- what, if anything, can you tell us
21 about did you conduct any research into
22 Mr. Millian? And, if so, what conclusions did you
23 reach with regard to Russian interference in the
24 2016 election?

25 A. We learned from sources that he had

EXHIBIT 19

NOT A CERTIFIED COPY



Dossier author Christopher Steele breaks silence with IG report rebuttal



*Christopher Steele, former British intelligence officer, said the law firm Perkin Coie wanted to be in a position to contest the 2016 election results. (Associated Press) ** FILE ** more >*

By Rowan Scarborough - *The Washington Times* - Monday, December 16, 2019

Christopher Steele has released his first on-the-record statement on how he investigated Donald Trump, but he does not specifically defend his dossier's list of disproved felony allegations against the then-candidate.

Mr. Steele, a former British intelligence officer financed by Democrats, issued his statement through Washington attorneys and focused much of his ire at the Justice Department inspector general's Dec. 9 report.

With the release of special counsel Robert Mueller's report in March and the IG's findings, Mr. Steele's dossier and its central allegation of a huge Trump-Russia election conspiracy have been largely discredited.

TOP STORIES

Bill de Blasio flips, now vows to defund New York police

Lincoln Memorial, WWII Memorial defaced by vandals in rioting

'Bigger than life': George Floyd known for big heart, good works, struggles with drugs, crime

Inspector General Michael E. Horowitz found that the Steele dossier was "essential" for the FBI to obtain wiretaps on Trump campaign volunteer Carter Page under the Foreign Intelligence Surveillance Act (FISA).

The IG drew a negative profile of Mr. Steele's main contact, identified as "Primary Sub-Source." Based in Moscow, the sub-source told the FBI that his information flow was "just talk" and hearsay and that he never imagined that Mr. Steele would put it into a report sent to America to influence the 2016 election.



Here are Mr. Steele's observations about the FBI and Mr. Horowitz:

- Mr. Steele, a former MI6 officer once posted to Moscow, objected to the label of "confidential human source," or CHS, as listed by the FBI and the Horowitz report. He previously had been paid \$94,000 for other investigative projects, including a FIFA soccer scandal.

"Orbis and Christopher Steele repeatedly told the FBI that he could not be a CHS because his obligations to his former government employer [M16] prohibited his acting in such a capacity," the statement says.

He told the FBI that the relationship could only be a contract between the bureau and his business, Orbis Business Intelligence in London.

- Mr. Steele was never given a chance to respond to the primary sub-source's allegations that the dossier relied on gossip.

“Had Orbis been given the opportunity to respond in a private session, the statements by the ‘Primary Sub-Source’ would be put in a very different light,” the statement says. “The ‘Primary Sub-Source’s’ debriefings by Orbis were meticulously documented and recorded.”

- The FBI never admonished Mr. Steele not to provide information to the news media. The IG report said that agents warned him during a huddle in Rome in October 2016 as the FBI was preparing to ask a federal judge to approve the first electronic surveillance on Mr. Page.

Mr. Steele’s paymaster, the Washington investigative firm Fusion GPS, required him to brief reporters on his anti-Trump package so news stories would appear during the election.

“The Report shows that the FBI agents who attended the meeting have very different recollections of what was and was not discussed at the meeting,” Mr. Steele said.

He said the IG reviewed his meetings notes and they confirm that he told the FBI he could not fire Fusion in favor of the bureau.

Later in October 2016, the FBI closed its CHS relationship with Mr. Steele after he leaked an anti-Trump story to Mother Jones magazine. But, in 2017 the FBI continued to receive his Trump packages as the candidate became the president.

Concerning the FISA warrant, the FBI attested to judges that Mr. Steele told agents that a September 2016 Yahoo News story didn’t come from the dossier writer. The implication was that it corroborated Mr. Steele’s reporting that Mr. Page met with Kremlin figures in Moscow in July and discussed bribes. (The Mueller report found no such wrongdoing.)

“Christopher Steele would have had no reason to deny these media contacts if asked about them by the FBI, as they related to intellectual property that belonged to Fusion,” the statement said.

- Mr. Steele denied he pushed the oft-repeated conspiracy theory that the Trump Organization in New York maintained a secret direct computer server hook-up with Alfa, Russia’s largest commercial bank whose owners are close to President Vladimir Putin.

“In fact, Orbis did not investigate or report on that issue,” Mr. Steele said, adding that he merely passed along public information.

The IG report said he did. It also said the FBI debunked the theory in early 2017.

Mr. Steele’s denial is contradicted by notes taken by Kathleen Kavalec, a deputy assistance secretary of state with whom he met in Washington in October 2016.

She memorialized the meeting: “Peter [sic] Aven of Alfa Bank has been the conduit for secret communications between the Kremlin and Manafort; messages are encrypted via TOR software and run between a hidden server managed by Alfa Bank.”

There was no evidence of this in the Mueller report.

Ms. Kavalec said Mr. Steele told her he wrote an Alfa server report.

Fusion GPS co-founder Glenn Simpson pushed the Alfa story to reporters and also to Bruce Ohr, then the No. 4 ranking official at the Justice Department.

Mr. Ohr met with Mr. Simpson in December 2016. His notes from the meeting: “The New York Times story on Oct. 31 downplaying the connection between Alfa servers and the Trump campaign was incorrect. There was communication and it wasn’t spam.”

“Alfa server in US is link to campaign,” Mr. Ohr quoted Mr. Simpson as saying.

Mr. Steele didn’t push the server conspiracy in the dossier, but he did link Alfa’s partners to Russian election interference. They are suing him for defamation in London, as is another Russian businessman whom Mr. Steele said actually did the computer hacking into Democratic Party computers.

- Mr. Steele did address his own work — the dossier — on a single issue.

In the dossier, Mr. Steele alleges that Mr. Page, while in Moscow to deliver a public university commencement address, met with Igor Sechin, head of the giant energy firm Rosneft. The two discussed a bribe in exchange for ending economic sanctions. Mr. Page has always denied ever meeting Mr. Sechin, a close Putin adviser.

Mr. Steele argued that Mr. Page confirmed this in his 2017 testimony before the House Permanent Select Committee on Intelligence.

Here is what Mr. Page, an energy investor who worked in Moscow from 2004 to 2007 with Merrill Lynch, said: An “old friend” from his Moscow days, Andrey Baranov, and he met at a bank-sponsored event to watch a soccer match at a bar. Since Mr. Page left Moscow, Mr. Baranov had become director of investor relations at Rosneft.

Mr. Page testified that they may have talked about sanctions since the issue was in the news. He recalled no discussion of a private sale of a 19% stake in Rosneft, which had been announced in mid-July.

"I can tell you for sure is I have never had any discussions with him about changing any sanctions policy or things I could even conceivably do in that regard," he testified.

After the election, Mr. Page returned to Moscow in December and had lunch with Mr. Baranov. He said they may have discussed the Rosneft private sale since it was in the news. He said he had no financial interest.

Mr. Page was exonerated by the Muller report.

It does not appear Mr. Steele has given any on-the-record news media interviews since his identity was revealed in January 2017. But his views on certain events have come through in generally sympathetic books and articles.

Before Mr. Steele's Dec. 10 press statement, his only on-the-record remarks came in libel lawsuits filed in Florida and London.

Sen. Lindsey Graham, South Carolina Republican, unleashed scathing criticism of Mr. Steele during the Senate Judiciary Committee's hearing on the IG report on Dec. 12.


"If you had spent 30 minutes looking at Christopher Steele, you would understand this guy is biased. He's got an ax to grind. He's on the payroll of the opposing party. Take anything he says with a grain of salt," Mr. Graham said.

SIGN UP FOR DAILY NEWSLETTERS

Submit [Manage Newsletters](#)

Please read our comment policy before commenting.

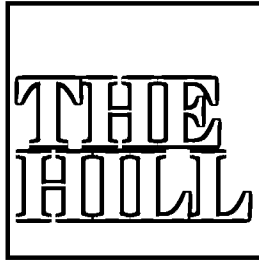
LEARN MORE

 Fisher Investments
Read our latest Stock Market Outlook to

NOT A CERTIFIED COPY

EXHIBIT 20

NOT A CERTIFIED COPY



Christopher Steele's nugget of gold was easily disproven — but FBI didn't blink an eye

BY JOHN SOLOMON — 05/21/19 06:30 PM EDT
THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

Just In...

Trump's Hollywood Walk of Fame star spray painted with Black Lives Matter

IN THE KNOW — 5M 57S AGO

Bezos says he's 'happy to lose' customers over his Black Lives Matter support

MEDIA — 11M 10S AGO

Biden wins Virgin Islands caucuses

CAMPAIGN — 15M 41S AGO

COVID-19 and the cost of health care: What happens when the pandemic ends?

OPINION — 27M 38S AGO

Oil giant BP cuts 10,000 employees

ENERGY & ENVIRONMENT — 32M 6S AGO

Dunkin' hiring 25,000 workers amid coronavirus recovery

FINANCE — 32M 55S AGO

Biden launches program to turn out LGBTQ vote

CAMPAIGN — 37M 37S AGO

Miami-Dade County officials call for civilian police review board

STATE WATCH — 39M 18S AGO

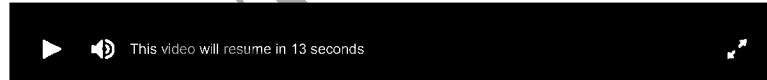
[VIEW ALL](#)

[View Latest Opinions >>](#)

7,313 SHARES

SHARE

TWE



Of all the wild tales that Christopher Steele spun about Russia-Trump collusion during a visit to the State Department shortly before the 2016 election, only one was deemed worth forwarding to his FBI handlers.

Long hidden, the now-disclosed email speaks volumes about both the quality of Steele's so-called intelligence gathering and the FBI's willingness to vet an informant who was openly biased against Donald Trump, paid by Trump's Democratic opponent, and motivated by an Election Day deadline.

Multiple sources confirm to me that the attachment that Deputy Assistant Secretary of State Kathleen Kavalec sent to then-FBI section chief Stephen Laycock on Oct. 13, 2016, was a summary from Steele's company alleging Trump and Russia might be communicating through a computer server at Russia's Alfa Bank.

This long-debunked allegation has floated around Washington since the summer of 2016, compliments of Hillary Clinton backers ranging from a university computer science professor who spread it across the internet to a lawyer for Clinton's campaign who delivered it to the FBI in summer 2016.

The theory — worthy of a spy novel — was that a series of data pings between a computer in Trump Tower and Alfa Bank in Moscow actually was a secret beacon alerting the Putin and Trump teams that it was time to talk about colluding on hijacking the American presidential election.

The story eventually made its way to mainstream media such as The New York Times, Slate, CNN and, just last fall, The New Yorker. It has been debunked by the FBI, and it was not mentioned as a reliable allegation in special counsel [Robert Mueller's report](#).

Steele's version of the allegation was uploaded to a private internet storage service, then downloaded by Kavalec and sent on Oct. 13, 2016, to Laycock, who immediately forwarded it to the FBI team investigating Trump-Russia collusion, according to people who have seen it.

The email arrived eight days before the FBI choose to use allegations in Steele's so-called dossier to secure an extraordinary Foreign Intelligence Surveillance Act (FISA) [warrant to spy](#) on the Trump campaign in the final days of the 2016 election.

In other words, it was a clear signal for the FBI to check Steele's credibility before offering him to the judges as a reliable informant. The reason? It was clear, convincing evidence that the FBI informant had broken protocol and was leaking to entities outside his chain of command, experts say.

Had the FBI done due diligence — and there's no evidence it did — then its agents would have followed up with Kavalec to see what else Steele had blabbed to State. And they would have learned that he admitted he had an Election Day deadline to get his information public, was leaking to the news media and had provided demonstrably false information to State officials, according to [Kavalec's own notes](#).

All of that, FBI intelligence experts tell me, would be enough to question Steele's credibility and reliability as an informant and to push a "pause" button on the FISA request.

But even absent checking with State, the very piece of Steele intelligence that Kavalec transmitted to FBI — the alleged back-door computer channel at Alfa Bank — already was deemed unreliable by the bureau.

The FBI received similar information in summer of 2016 from the Democratic Party's and Clinton campaign's lawyer, who forwarded it to then-FBI chief counsel James Baker.

I first heard about the allegation in late September 2016 and, by the first week of October, I reached multiple U.S. officials — including one inside the FBI — who told me the [allegation had been investigated](#) and the pings were determined to be "innocuous" contacts, most likely related to errant spam emails. Alfa Bank hired two experts who reached similar conclusions.

Every time the story surfaced over the next two years, I [got the same answer](#) from U.S. officials. And I wasn't alone. The New York Times [published a similar answer](#) before the 2016 election: "The F.B.I. ultimately concluded that there could be an innocuous explanation, like a marketing email or spam, for the computer contacts," it reported on Oct. 31, 2016.

In the end, Kavalec's email to the bureau about Steele was a perfect test of Steele's credibility and of the FBI's willingness to question the credibility of its star informant in one of the most controversial FISA applications in American history.

Both failed. Steele passed along easily debunked intelligence, and the FBI failed to ask hard questions about his credibility or to alert FISA judges to the concerns that Steele's behavior raised before the warrant was secured.

Related News by |



Obama officials owe the nation an apology for

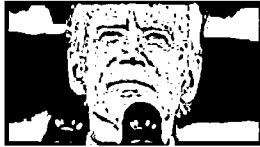


Live Poll: Are You Voting for Joe Biden?

Sponsored | [share.joebiden.com](#)



From tragedy to opportunity: We could



Biden's 'allies' gearing up to sink his campaign

NOT A CONFIDENTIAL COPY

In other words, before the FBI and its then-director, James Comey, swore to the FISA court on Oct. 21, 2016, that they had verified the FISA warrant application and deemed Steele a credible informant with no known derogatory information, the government knew:

- Steele had told senior Justice official Bruce Ohr he was “desperate” to defeat Trump and was working in some capacity for the Clinton campaign;
- he leaked his dossier to the news media;
- he offered demonstrably false intelligence, such as the Alfa pings and an allegation given to Kavalec that Russian hackers were being paid by a nonexistent Russian Consulate in Miami.

Rep. Mark Meadows (R-N.C.), a leader of the FISA abuse investigation, said the discovery two weeks ago of the State documents further heightens his concerns about the “problematic genesis” of the FBI’s probe of Trump. “Each day we receive additional confirmation that those at the highest levels of the FBI were fully aware of the bias and lack of credibility that the whole investigation was initiated upon,” he told me. Far worse revelations for the FBI likely lie ahead.

Most Americans now support an investigation into whether the FBI abused FISA to smear Trump.

Man arrested, charged with threatening to attack Muslims in Germany
Markets continue upward trend with eye to recovery

President Trump is preparing to declassify the first tranche of documents in the Russia case, and they are expected to show the FBI possessed — but did not alert the court to — damning evidence of the Trump campaign’s innocence, including recorded conversations of targeted campaign aides denying wrongdoing.

But even before that happens, the State Department email that was kept from the American public and Congress for 2 1/2 years should be appreciated for what it signifies: It was a missed opportunity to assess Steele’s research for what it was — political fool’s gold.

John Solomon is an award-winning investigative journalist whose work over the years has exposed U.S. and FBI intelligence failures before the Sept. 11 attacks, federal scientists’ misuse of foster children and veterans in drug experiments, and numerous cases of political corruption. He serves as an investigative columnist and executive vice president for video at The Hill. Follow him on Twitter [@jsolomonReports](#).

TAGS HILLARY CLINTON MARK MEADOWS DONALD TRUMP JAMES COMEY
TRUMP-RUSSIA INVESTIGATION FBI BIAS 2016 ELECTION

SHARE

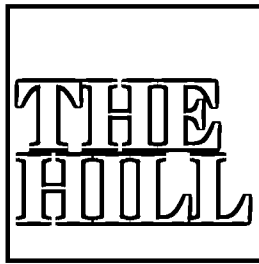
TWEET



NOT A CERTIFIED COPY

EXHIBIT 21

NOT A CERTIFIED COPY



Move over 'grassy knoll,' the Trump-Russia bank tale joins unproven conspiracies list

BY JOHN SOLOMON, OPINION CONTRIBUTOR — 10/14/18 09:00 AM EDT
THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

Just In...

Reported US troop drawdown could hurt NATO security, German official says

DEFENSE — 1M 47S AGO

A national testing strategy to safely reopen America

OPINION — 2M 38S AGO

Trump's Hollywood Walk of Fame star spray painted with Black Lives Matter

IN THE KNOW — 10M 57S AGO

Bezos says he's 'happy to lose' customers over his Black Lives Matter support

MEDIA — 16M 10S AGO

Biden wins Virgin Islands caucuses

CAMPAIGN — 20M 41S AGO

COVID-19 and the cost of health care: What happens when the pandemic ends?

OPINION — 32M 38S AGO

Oil giant BP cuts 10,000 employees

ENERGY & ENVIRONMENT — 37M 6S AGO

Dunkin' hiring 25,000 workers amid coronavirus recovery

FINANCE — 37M 55S AGO

[VIEW ALL](#)

1,337 SHARES

SHARE

TWE



© Getty Images

If Democrats and their media accomplices keep recycling it, the unproven Donald Trump-Alfa Bank conspiracy may one day live right up there with the extra JFK gunman at Dallas' grassy knoll, the missing Oak Island treasure, or the Lost City of Atlantis.

After all, the best unsolved mysteries — especially in politics — are those that can be neither proven nor disproven.

And therein lies the travesty of the unrelenting, yet uncorroborated, allegation that Trump's campaign set up a covert communication system with Russia during the 2016 election, using a computer server in the United States and another owned by a Russian bank.

This allegation first surfaced with a Hillary Clinton-loving computer nerd in the fall of 2016, who claimed her group obtained domain name server (DNS) logs showing frequent "pings," or contacts, between a server owned by Russia's Alfa Bank and one in the name of the Trump Organization.

It turns out, though, that the server wasn't actually in the Trump Organization in New York. It was in a tiny Pennsylvania town. And it actually wasn't controlled by the Trump Organization but, rather, by an independent email marketing firm once hired by the president's company.

[View Latest Opinions >>](#)

But, for now, we won't let those facts get in the way a good yarn. Plus, there are some interesting characters to follow.

Christopher Steele — the Trump-hating former British spy hired by opposition research firm Fusion GPS, which was hired by Clinton's campaign and the Democratic Party to dig up Trump dirt in Russia — was next to pick up the allegation. Eventually, allegations of connections between Alfa Bank's parent-company Alfa Group, Russia and Trump made it into the dossier that Steele gave the FBI, although his grasp of the information was so shoddy that he misspelled the bank's name.

Next, the allegation surfaced in [a Slate](#) and [a New York Times article](#) just a few days before Trump was elected. (Perhaps appropriately, the stories ran on Halloween.) The Times's story, however, conceded the FBI was dubious of the whole matter.

Not to be outdone, private attorney Michael Sussman walked in similar allegations to then-FBI General Counsel James Baker in September 2016, according to four congressional sources familiar with testimony and documents gathered in the Russia case. The evidence of the connections to the Alfa Bank allegations also are in a footnote in the House Intelligence Committee report, where Sussman's name was redacted by the FBI. Congressional investigators are investigating whether someone in Sussman's firm, Perkins Coie, also provided Russia-related information to the CIA in early 2017.

That's significant because Perkins Coie's clients included the Democratic National Committee and Hillary Clinton's campaign, and that firm paid Fusion GPS for Steele's dirt-digging. Sussman declined to say, through a spokesman, if he met with a CIA contact but insisted any contact the firm may have had with the CIA wasn't done at the behest of the DNC or Clinton. Still, it is hard to ignore his political connections.

And if that wasn't enough to pressure the FBI to look at the allegation, Fusion GPS founder Glenn Simpson — Steele's boss on the Trump research project — brought the Alfa allegations directly to the No. 4 Justice Department official in December 2016. Assistant Deputy Attorney General Bruce Ohr's notes from the meeting have a nifty notation. "The New York Times story on Oct. 31 downplaying the connection between Alfa servers and the Trump campaign was incorrect," Ohr wrote in quoting Simpson. "There was communication and it wasn't spam."

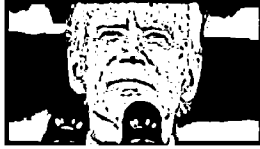
Though the FBI repeatedly and publicly cast doubt on the allegations, some media outlets, such as CNN, continued to fan the flames of this tale, like Santa Ana winds on a California wildfire.

The latest to do so was New Yorker magazine, which just this month ran a long opus under the banner: "Was There a Connection Between a Russian Bank and the Trump Campaign?" No "new" news in that story, really. Just recycled fragments woven into a long, magazine-style story with an implicit plea for Democrats to resurrect the issue if they win control of Congress in November.

The relentless campaign to keep the allegations alive is remarkable not only for its political origins, but for what often has been omitted from the public narrative.

First off, the FBI has, on repeated occasions in 2016 and 2017, told me emphatically that it looked at the allegations and could find no conspiracy and, instead, believed the server communications were simply explained by normal internet traffic activities.

Related News by |



Biden's 'allies' gearing up to sink his campaign



The sad spectacle of Trump's enablers



Quick Poll: Will You Vote for Biden

Sponsored | Democratic Governors Association



Juan Williams: Bush could strike blow for

NOT A REPRODUCED COPY

Secondly, Alfa Bank's law firm traveled to meet an FBI cyber team in Chicago in 2017 and opened up its data vaults to assist the investigation. There was no follow-up, Alfa Bank says.

The private lawyer who supervised the review for Alfa Bank was Brian Benzckowski. He later was confirmed to be the chief of the U.S. Justice Department's criminal division, one of the most sensitive and important jobs in law enforcement; Democrats asked him about the Alfa review during his confirmation. And neither the FBI nor the intelligence community offered any information to the Senate during his confirmation to contradict his conclusions that there was no conspiracy involving the Alfa-Trump servers.

Furthermore, not once in the 17 months of the Robert Mueller special counsel investigation has a member of Mueller's staff reached out to Alfa Bank to raise questions about collusion or the servers, the bank says.

Another common omission from the news stories on this subject involves the political leanings of a key researcher who has pushed the Alfa-Trump narrative. Indiana University professor L. Jean Camp, who is well respected in computer science circles, was an unabashed supporter of and donor to Hillary Clinton in 2016. After the 2016 election, Camp accused the FBI in a tweet of ignoring the Trump server allegations and instead focusing on the reopening of Clinton's email case. "The data are there and worth investigation. Why did FBI, #NYTimes kill this story before election to focus on Her Emails?" she tweeted in March 2017.

Camp acknowledged her political leanings to me last year, but insisted they had no bearing on her decision to raise questions about the data.

There's one final omission worth noting. Most of the stories include a passing reference that Alfa commissioned one or two reports concluding there was no nefarious communications between Trump and Alfa servers. But nearly all ignore one of the most important findings in the reports: The DNS data released by researchers such as Camp to make their case of a possible conspiracy between Trump and Alfa were formatted differently than the bank server's DNS logs.

"The format of the data does not match the format of actual logs at Alfa Bank," the respected firm Stroz Friedberg wrote in a 2017 report. "If the DNS log data posted by Professor Camp is actual DNS log data from Alfa Bank, it has been edited and placed into a different format."

That's a pretty big deal for a jury in the court of public opinion. And it is has been consistently omitted from stories on the subject, including the most recent New Yorker article.

The computer researchers, the DNC lawyer, Steele, Ohr and Simpson all may have had the best of intentions in reporting information to the FBI despite their political leanings.

That's not why the Alfa-Trump story lives on. It survives and festers because those who continue to recycle it omit essential facts that are germane to judging it.

News consumers and policymakers should demand that future iterations of this tale be more complete and balanced, and only told anew if new, substantial facts emerge from a place like the Mueller investigation.

Anything less is simply conspiratorial myth-making.

John Solomon is an award-winning investigative journalist whose work over the years has exposed U.S. and FBI intelligence failures before the Sept. 11 attacks, federal scientists' misuse of foster children and veterans in drug experiments, and numerous cases of political corruption. He is The Hill's executive vice president for video.

TAGS HILLARY CLINTON ROBERT MUELLER DONALD TRUMP
RUSSIAN INTERFERENCE IN THE 2016 UNITED STATES ELECTIONS SPECIAL COUNSEL INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE BRUCE OHR FUSION GPS CHRISTOPHER STEELE

SHARE

TWEET



THE HILL 1625 K STREET, NW SUITE 900 WASHINGTON DC 20006 | 202-628-8500 TEL | 202-628-8503 FAX
THE CONTENTS OF THIS SITE ARE ©2020 CAPITOL HILL PUBLISHING CORP., A SUBSIDIARY OF NEWS COMMUNICATIONS, INC.

NOT A CERTIFIED COPY

EXHIBIT 22

NOT A CERTIFIED COPY

archive.today
webpage capture

Saved from <https://heatst.com/world/exclusive-fbi-granted-fisa-warrant-covering-trump-camps-tie> search

12 Apr 2017 02:58:39 UTC

All snapshots from host heatst.com

Linked from conservapedia.com » 2016 Hillary Clinton presidential campaign
conservapedia.com » Barack Obama Controversies
[16 more](#)

Webpage

Screenshot

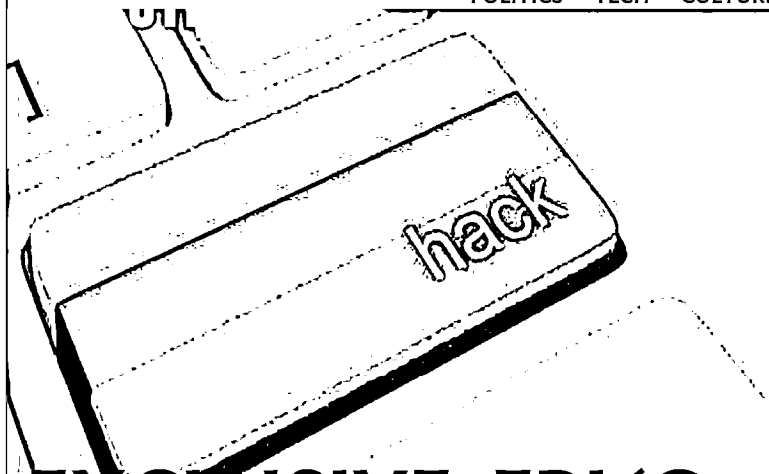
share

download .zip

report bug or abuse

donate

POLITICS TECH CULTURE WARS BIZ ENTERTAINMENT LIFE



EXCLUSIVE: FBI 'Granted FISA Warrant' Covering Trump Camp's Ties To Russia

Home > World

By Louise Mensch | 10:18 pm, November 7, 2016

Like



Two separate sources with links to the counter-intelligence community have confirmed to Heat Street that the FBI sought, and was granted, a FISA court warrant in October, giving counter-intelligence permission to examine the activities of 'U.S. persons' in Donald Trump's campaign with ties to Russia.

Contrary to earlier reporting in the New York Times, which cited FBI sources as saying that the agency did not believe that the private server in Donald Trump's Trump Tower which was connected to a Russian bank had any nefarious purpose, the FBI's counter-intelligence arm, sources say, re-drew an earlier FISA court request around possible financial and banking offenses related to the server. The first request, which, sources say, named Trump, was denied back in June, but the second was drawn more narrowly and was granted in October after evidence was presented of a server, possibly related to the Trump campaign, and its alleged links to two banks; SVB Bank and Russia's Alfa Bank. While the *Times* story speaks of metadata, sources suggest that a FISA warrant was granted to look at the full content of emails and other related documents that may concern US persons.

Get Our Exclusive Newsletter—The Best of Heat Street Every Day!

Email Address

Subscribe

ADVERTISEMENT

The FBI agents who talked to the New York Times, and rubbished the ground-breaking stories of Slate (Franklin Foer) and Mother Jones (David Corn) may not have known about the FISA warrant, sources say, because the counter-intelligence and criminal sides of the FBI often work independently of each other employing the principle of 'compartmentalization'.

The FISA warrant was granted in connection with the investigation of suspected activity between the server and two banks, SVB Bank and Alfa Bank. However, it is thought in the intelligence community that the warrant covers any 'US person' connected to this investigation, and thus covers Donald Trump and at least three further men who have either formed part of his campaign or acted as his media surrogates. The warrant was sought, they say, because actionable intelligence on the matter provided by friendly foreign agencies could not properly be examined without a warrant by US intelligence as it involves 'US Persons' who come under the remit of the FBI and not the CIA. Should a counter-intelligence investigation lead to criminal prosecutions, sources say, the Justice Department is concerned that the chain of evidence have a basis in a clear warrant.

In June, when the first FISA warrant was denied, the FBI was reportedly alarmed at Carter Page's trip to Moscow and meetings with Russian officials, one week before the DNC was hacked. Counter intelligence agencies later reported to both Presidential candidates that Russia had carried out this hack; Donald Trump said publicly in the third debate that 'our country has no idea' if Russia did the hacking. The discovery of the Trump Tower private Russian server, however, communicating with Alfa Bank, changed matters, sources report.

To further complicate the story, the FISA warrant was allegedly granted in part because of the involvement of Vladimir Putin's own daughters. One is married to a senior official at Gazprom, where Carter Page and Paul Manafort reportedly have holdings; another to Kirill Shamalov, a banking official.

The fact that the alleged warrant was a FISA warrant is itself significant. The court exists to grant warrants to examine cases concerned with Foreign Intelligence.

Pursuant to FISA, the Court entertains applications submitted by the United States Government for **approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes.** Most of the Court's work is conducted *ex parte* as required by statute, and due to the need to protect classified national security information.

Bradley P. Moss is a national security lawyer. He told us:

If a FISA warrant was issued, it does not necessarily mean that the court considered any U.S. persons as literal 'spies.' I can imagine an argument having been made that there was probable cause to believe they were "agents of influence" who were unwittingly being influenced by a foreign power.

If the operation concerns suspected money laundering involving a foreign government, the FISA warrant could theoretically encompass U.S. persons in that limited context. A FISA warrant is authorization to collect evidence, not to arrest.

Elsewhere



Female Air Force Mechanic, 26, Becomes World Famous Instagram Supermodel

HEATSTREET



On October 9th, the Trump campaign released a large number of documents pointing out what they alleged were Hillary Clinton's ties to Russia. On October 12th, rumors of a FISA warrant started to surface online. Donald Trump's campaign had not answered requests for comment on the matter at time of going to press.

<https://twitter.com/robertcaruso/status/786382771128107008>

@1CheekyLilMe1 @MrDane1982 There was ex FBI Counter Intelligence agent on @amjoyshow he said; don't be surprised FISA court warrant fr Trump

— Tim (@russelltim151) November 6, 2016

MORE

1. **Russian Intel Bots Are Boosting Infowars Alt-Right Twitter Accounts For Trump**
2. **Evan McMullin: Massive Surge in Final Utah Poll, Momentum To Overtake Trump**
3. **Wonder Woman Is 'Downright Offensive and Simplistic,' Says Woke Feminist**

Hey guest, welcome to Heat Street! Sign up and become a member.

- Facebook
- Google
- Twitter
- Email

Popular Teacher Suspended for Posting 'Sultry and Provocative' Facebook Selfies

HEATSTREET



'Sex Mad' Mom Jailed for Wild Sex Romps With Underage Boys

HEATSTREET



Woman charged with raping taxi driver

NEW YORK POST

Trending



'Centerfold' Guitarist J. Geils Has Been Found Dead in His Massachu...

The famed musician and namesake of The J. Geils Band was 71 years old



Genetically-modified mice could spot next potential flu pandemic be...

Scientists in Germany have developed a transgenic mouse that mimics the human...



Apocalypse Now: Scientists Predict the Earth is About to Swap Magne...

The consequences are not certain, but they might be lethal for the humanity



Amazon Just Scored a Touchdown With Thursday Night Football

Amazon.com (NASDAQ: AMZN) just won the streaming rights to 10 of the NFL's Th...



China Threatens To Bomb North Korea's Nuclear Facilities If It Cros...

With everyone putting down new and/or revised "red lines", be it on Syria or ...

NOT A CERTIFIED COPY

ADVERTISEMENT

ALSO ...

Evan McMullin Crushing Clinton And Closing on

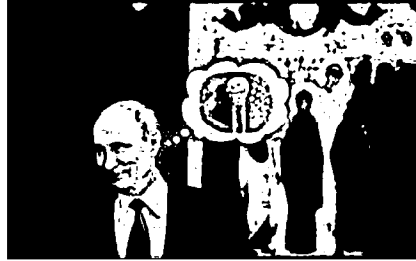


Final Deseret News poll: young families push Evan McMullin barely behind Trump - with 24% undecided

Louise Mensch



How Russia's BotNet Uses the AltRight For Trump



We asked a data scientist to take a look at how the altright works with Putin's 'Eggs For Trump' Russian bot-net

Louise Mensch



[Privacy Policy](#) | [Cookie Policy](#) | [Copyright Policy](#) | [Data Policy](#) | [Terms of Use](#) | [Your Ad Choices](#) | [Contact Us](#)

Copyright ©2017 Dow Jones & Company, Inc. All Rights Reserved. Powered by WordPress.com VIP

NOT A CERTIFIED COPY

EXHIBIT 23

NOT A CERTIFIED COPY

https://lancasteronline.com/news/local/fbi-gets-lititz-firm-s-help-in-probe-of-russian-bank-s-odd-interest-in/article_ef5d5ed0-05ae-11e7-a003-471e5543b26a.html

FBI gets Lititz firm's help in probe of Russian bank's 'odd' interest in Trump Hotels marketing emails



TIM MEKEEL | Staff Writer

Mar 10, 2017

Listrak is a Lititz company that gets hired to send emails on behalf of stores, hotels and other businesses.

The rapidly growing company sends more than two billion of those marketing emails a month — generating interest in its clients, not Listrak.

But marketing emails that Listrak sent last year for Trump Hotels have led to Listrak inadvertently drawing curiosity about itself.

From the FBI.

Why? The computer server of a Russian bank repeatedly looked up the unique internet address of the server sending out the Trump Hotel emails — Listrak's server.

The ongoing investigation is being handled by the FBI counterintelligence team, the same team that's probing Russia's suspected interference in the 2016 presidential election, CNN reported Friday.

There are no allegations of wrongdoing, said CNN. Rather, the FBI is checking out a situation it considers "odd."

Listrak Chief Executive Officer Ross Kramer said that the FBI came to the Listrak office before the November election, when Donald Trump defeated Hillary Clinton.

While declining to provide details on the FBI visit, he did say, "It was very cordial, and we've given them everything they need."

Kramer said that Listrak was retained by a Florida company, Cendyn, that specializes in marketing for the hospitality industry. Cendyn hired Listrak to send emails on behalf of Trump Hotels.

Listrak sent them from a domain name that incorporates the name of the business being marketed, as is standard practice. In this case, the domain name was trump-email.com, said Kramer.

"If you look back at the election, with all of the allegations swirling around emails ... the domain name trump-email.com is going to get some attention. It's a mystery to me how the (Russian bank) people got involved with it," said Kramer.

CNN's story also comes as the Trump administration's ties to Russia are drawing intense scrutiny.

The news channel's story didn't name the company who had the server that the Russian bank's server was looking up.

CNN just said the internet address "lives on an otherwise dull machine operated by a company in the tiny rural town of Lititz, Pennsylvania."

But news website BuzzFeed and cybersecurity website Errata Security reported in November that Listrak produces email marketing for Trump Hotels.

Listrak's role in sending emails on behalf of Trump businesses also was mentioned in The Washington Post on Sunday.

In its Friday story, CNN said the server at Alfa Bank in Moscow looked up the unique internet address of a Trump server nearly 3,000 times.

CNN described the actions of the Alfa Bank server this way:

“In the computer world, it's the equivalent of looking up someone's phone number — over and over again. While there isn't necessarily a phone call, it usually indicates an intention to communicate, according to several computer scientists.”

Yet investigators have not yet determined whether a connection, if it had occurred, would be significant, the news channel said.

Alfa Bank denied having any ties to the Trump Organization — the name for the various holdings with ties to Trump or his family — or trying to contact the organization through email or other means.

The bank told CNN it believes the server activity was generated by someone posing as the bank in an attempt to “manufacture the deceit.”

The writer of the November article for Errata Security said that Alfa Bank “executives like to stay at Trump hotels all the time (like in Vegas and New York), and there was a company function one of Trump's golf courses. In other words, there's good reason for the company to get spam from, and need to communicate with, Trump hotels to coordinate events.”

— *LNP Staff Writer Tim Stuhldreher contributed to this story.*

EXHIBIT 24

NOT A CERTIFIED COPY

FBI refuses to say if it has received Daniel Jones' anti-Trump research

[washingtontimes.com/news/2019/may/8/fbi-refuses-reveal-if-daniel-jones-alfa-bank-serve](https://www.washingtontimes.com/news/2019/may/8/fbi-refuses-reveal-if-daniel-jones-alfa-bank-serve)

By Rowan Scarborough

The FBI has turned down a request from The Washington Times to disclose whether it has received any opposition research from Daniel J. Jones, the former Senate Democratic staffer who raised \$50 million to investigate President Trump.

Mr. Jones has spread the discredited Alfa Bank server conspiracy, which says Russia's largest commercial bank supposedly had a direct link to the Trump campaign via a computer network.

The FBI said The Times' request under the Freedom of Information Act has been closed. The action should not be construed as acknowledging that the material does or doesn't exist, the bureau said in an April 25 letter.

TOP STORIES

[Democrats know their time grows short](#)

['Bigger than life': George Floyd known for big heart, good works, struggles with drugs, crime](#)

[Bill de Blasio flips, now vows to defund New York police](#)

Mr. Jones, a former FBI investigator and once an intelligence aide to Sen. Dianne Feinstein of California, met with bureau agents in March 2017, according to an FBI memo obtained by the then-Republican majority on the House Permanent Select Committee on Intelligence.

Sources said the meeting appeared to involve a transfer of information. Mr. Jones told the FBI about his fundraising from seven to 10 Democratic Party donors. He said he had hired two prominent operators in the Trump-Russia affair: the opposition research firm Fusion GPS and former British intelligence officer Christopher Steele.

Mr. Jones said he planned to continue investigating Russia's interference in the 2016 election and give the research to the news media and Capitol Hill.

Mr. Steele was paid \$160,000 in Democratic Party funds to write a 35-page anti-Trump dossier. It alleged an "extensive conspiracy" between the Trump campaign and the Kremlin to interfere in the 2016 election.

Special counsel Robert Mueller's final report delivered March 22 said no such conspiracy was established during his 22-month investigation.

The FBI letter to The Times stated: "Please be advised the FBI will neither confirm nor deny the existence of such records pursuant to FOIA exemptions. ... The mere acknowledgment of the existence of FBI records on third party individuals could reasonably be expected to constitute an unwarranted invasion of personal privacy. ... As a result, your request has been closed."

What Mr. Jones, head of the secretive Penn Quarter Group investigative firm, has produced for the news media or any other recipient in the past two years is unclear.

There is one known media story: The New Yorker magazine last year used Mr. Jones' research to further an allegation pushed by Fusion GPS co-founder Glenn R. Simpson and by the Democratic Party's private law firm. It said Moscow's Alfa Bank, controlled by oligarchs close to Russian President Vladimir Putin, operated a computer server with a direct line to a server at Trump Tower in New York City.

The FBI investigated. There is no mention of such a server in Mr. Mueller's 448-page report.

The Mueller team interviewed Petr Aven, Alfa's controlling partner. He testified to the grand jury that he was so disconnected from Trump people that when Mr. Putin asked him to reach out to the presidential transition, he had no contacts.

"According to Aven, at his Q4 2016 one-on-one meeting with Putin, Putin raised the prospect that the United States would impose additional sanctions on Russian interests, including sanctions against Aven and/or Alfa-Bank. Putin suggested that Aven needed to take steps to protect himself and Alfa-Bank. Aven also testified that Putin spoke of the difficulty faced by the Russian government in getting in touch with the incoming Trump Administration. According to Aven, Putin indicated that he did not know with whom formally to speak and generally did not know the people around the President-Elect," the Mueller report says.

Mr. Aven instead turned to former U.S. Ambassador to Germany Richard Burt to find out whether he could make contact to discuss U.S. sanctions. Mr. Burt sits on the board of another company controlled by Mr. Aven.

Mr. Burt contacted Russia-born Dimitri Simes, who runs the Center for the National Interest, which promotes Moscow-Washington ties. Mr. Simes told him it was not a good idea to establish a back channel, given the intense scrutiny on the Kremlin's hacking of Democratic Party computers.

The Mueller report summed up the episode: “In the first quarter of 2017, Aven met again with Putin and other Russian officials. At that meeting, Putin asked about Aven’s attempt to build relations with the Trump Administration and Aven recounted his lack of success.”

The Trump Organization has told The Washington Times that the server suspected of being a direct link to [Alfa](#) by liberals on social media was actually a third-party server housed at a spam marketing center in Pennsylvania.

Sign up for Daily Newsletters

[Manage Newsletters](#)

Copyright © 2020 The Washington Times, LLC. [Click here for reprint permission.](#)

Please read our [comment policy](#) before commenting.

NOT A CERTIFIED COPY

EXHIBIT 25

NOT A CERTIFIED COPY

RPTR FORADORI

EDTR SECKMAN

FORMER SPECIAL COUNSEL ROBERT S. MUELLER III ON THE INVESTIGATION INTO
RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION

Wednesday, July 24, 2019

U.S. House of Representatives,

Permanent Select Committee on Intelligence,

Washington, D.C.

The committee met, pursuant to call, at 12:50 p.m., in Room HVC-304, Capitol Visitor Center, the Honorable Adam Schiff (chairman of the committee) presiding.

Present: Representatives Schiff, Himes, Sewell, Carson, Speier, Quigley, Swalwell, Castro, Heck, Welch, Maloney, Demings, Krishnamoorthi, Nunes, Conaway, Turner, Wenstrup, Stewart, Crawford, Stefanik, Hurd, and Ratcliffe.

Director Mueller, you've been asked many times this afternoon about collusion, obstruction of justice, and impeachment, and the Steele dossier. And I don't think your answers are going to change if I ask you about those questions.

So I'm going to ask about a couple of press stories, because a lot of what the American people have received about this have been on press stories, and some of that has been wrong, and some of those press stories have been accurate.

On April 13, 2018, McClatchy reported that you had evidence Michael Cohen made a secret trip to Prague during the 2016 Presidential election. I think he told one of the committees here in Congress that that was incorrect. Is that story true?

Mr. Mueller. I can't -- well, I can't go into it.

Mr. Hurd. Gotcha.

On October 31, 2016, Slate published a report suggesting that a server at Trump Tower was secretly communicating with Russia's Alfa Bank, and then I quote, "akin to what criminal syndicates do."

Do you know if that story is true?

Mr. Mueller. Do not. Do not --

Mr. Hurd. You do not?

Mr. Mueller. -- know whether it's true.

Mr. Hurd. So did you not investigate these allegations which are suggestive of a potential Trump-Russia --

Mr. Mueller. Because I believe it not true doesn't mean it would not be investigated. It may well have been investigated. Although my belief at this point, it's not true.

Mr. Hurd. Good copy. Thank you.

As a former CIA officer, I want to focus on something I think both sides of the