COVER STORY | READ THIS FIRST. | OCT. 31 2016 5:36 PM

# Was a Trump Server Communicating With Russia?

This spring, a group of computer scientists set out to determine whether hackers were interfering with the Trump campaign. They found something they weren't expecting.

*By Franklin Foer*

GOVERNMENT EXHIBIT
**0054**
21-CR-582 CRC

http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

*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.*

Franklin Foer

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.

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.

http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

*Trump Tower.*

Ullstein Bild/Getty Images

(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.")

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.

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.")

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.)

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.”

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.”

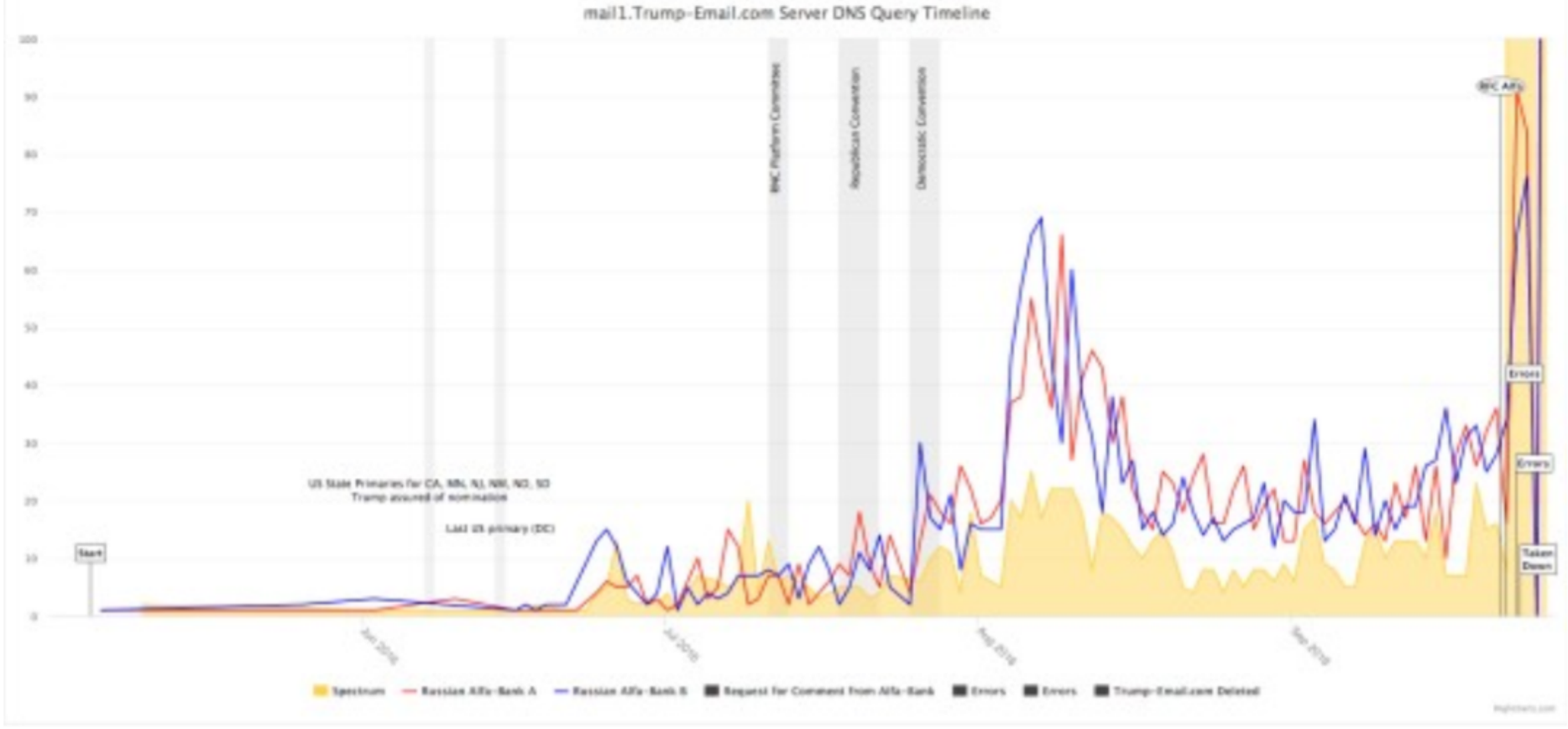
Unlike other Russian firms, Alfa has operated smoothly and effortlessly in the West. It has never been slapped with sanctions. Fridman and Aven have cultivated a reputation as beneficent philanthropists. They endowed a prestigious fellowship. The Woodrow Wilson International Center for Scholars, the 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.




***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.*

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."

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 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.*