GOVERNMENT EXHIBIT

0666

21-CR-582 CRC

From: Franklin Foer <flfoer@gmail.com>
Sent: Sunday, October 30, 2016 10:46 PM
To: Peter Fritsch <pfritsch@fusiongps.com>
Subject: Re: Reid

Here's the first 2500 words

The greatest miracle of the Internet is that it exists—the second greatest is that it persists. Every so often we're violently reminded that bad actors wield great skill and have little conscience about the harm they inflict on the world's digital nervous system. They feverishly invent viruses, botnets, and sundry species of malware. There's good money to be made deflecting these incursions, but profit motive alone isn't enough to sustain the relentless efforts required to fend off such creative adversaries. That's why a small, tightly-knit community of computer scientists—some at cyber-security firms, some in academia, some with close ties to three-letter federal agencies—wraps its work in 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 University of Indiana 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 cyber-security 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.

Protecting the Internet requires highly-specialized knowledge of the intricacies of the Domain Name System (DNS) —the protocol that allows us to type e-mail addresses and website names to initiate communication. DNS enables our words to set in motion a chain of connections between servers that delivers the results we desire. To create a usable, collective archive of malware, computer scientists have built a set of massive DNS databases, which provide fragmentary histories of communications flows. These databases give a useful, though far from comprehensive, snapshot of traffic across the Internet. The most trusted DNS specialists—an elite group of malware hunters, who work for private contractors—have access to a truly comprehensive logs of communication between servers. They work in close concert with Internet Service Providers, the systems most vulnerable to massive attacks. To extend the traffic metaphor, these are scientists with cameras posted on the Internet's stoplights and overpasses. They are entrusted with something close to the complete real-time record of all the servers of the world connecting with each other.

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. That 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 much larger 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 to colleagues in the cybersecurity world. Six of them began scrutinizing them for clues.

(I communicated extensively with Tea Leaves and two of his closest collobotators, who spoke with me on the condition of anonymity, since they also work for firms trusted by banks and law enforcement to analyze sensitive data. They persuasively demonstrated some of their analytical methods to me--and showed me academic-style white papers that track the evolution of their analysis. I also spoke with academics who vouched for Tea Leaves' integrity and his unusual access to information. "Without him, your inbox would be full of spam and the web would be shut down by malicious attack," according to Jean Camp.)

The researchers' quickly dismissed the initial fear of 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 the world's nastiest botnet attack . "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 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. But 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. "It's pretty clear that it's not an open mail server," Jean Camp told me. "These organizations are communicating in a way designed to block other people out.

(A small portion of the logs showed communication with a server belonging to Michigan-based Spectrum Health, a company owned by the Devos family, founders of Amway and long-time benefactors of the Republican party. Eighty-seven percent of DNS look up, however, were directed to the two Alfa servers.)

Earlier this month, the group 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. As they watched, their suspicions of collaboration were confirmed in the most unexpected ways.

DROP CAP

While the researchers went about their work, the conventional wisdom about Russian interference in the campaign began to shift. There were reports hat the Trump campaign had ordered the Republican Party to re-write its platform position on Ukraine, maneuvering the GOP towards a policy preferred by Russia. (At the time, the campaign was being run by Paul Manafort, who had done extensive work for the Kremlin-backed Ukrainian president Victor Yanukovych.) 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. These events changed the question that the researchers were asking about the DNS logs. Perhaps Russian hackers weren't just sniffing about for intelligence; perhaps they weren't indiscriminately sowing paranoia and chaos. Evidence mounted that Putin might actively be rooting for Trump to win—and there was a circumstantial, highly speculative case building that the campaign might even be coordinating with the Kremlin. (I wrote about this possibility in early July.)

In the face of these accusations, Trump 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. When the computer scientists poured over the logs, they couldn't believe that Trump would be so categorical in his descriptions. (The Cambridge University cybersecurity researcher Richard Clayton, who reviewed an analysis of the data circulated by Tea Leaves' colleagues, quipped, "If they say, then I have never heard of Russia, then that would be a bit thin.")

But in the parlance that has become familiar since the Edward Snowden revelations, we're in the realm of metadata. We can see the trail of the transmissions on the logs, 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 scientists who spoke to me on background 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 sustain communication. He noted that certain key pieces of data—namely a set of mail exchanger records—were missing, which prevented him for reaching a conclusive judgement. "I'm seeing a preponderance of the evidence, but not a smoking gun." Richard Clayton acknowledges those theoretical objections, 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."

When I put the question to the University of California's Nicholas Weaver, he told me, "I can't attest to the logs themselves, but assuming they are legitimate they do indicate effectively human-level communication limited to just between the Russian Bank, the health-care company, and trump-email.com." Are the logs authentic, the implicit uncertainty embedded in the hedging of Weaver's statement? Computer scientist 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. (Unfortunately, there's no other way to copy the data other than to stick them in a text file.)

Still, I asked nine computer scientists--some of whom agreed to speak on the record, some who asked for anonymity--if the DNS logs could be forged or manipulated. They considered it nearly impossible. Of course, it would be easy enough to fake one or maybe even a dozen records of DNS lookups. But in the aggregate the thousands of records contained nuances and patterns that not even the most skilled programmers would be able to recreate, especially not on this scale. Paul Vixie told me, "The data has got the right kind of fuzz growing on it. It's the inter packet 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 they was any chance that he was wrong about their authenticity. He told me. "This passes the reasonable person test. 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," Christopher Davis said. According to Jean Camp, "When the technical community examined the data, the conclusion was pretty obvious."

DROP CAP

The researchers were seeing clear patterns in the data—and the Trump organization's potential interlocutor itself was suggestive . Alfa Bank emerged in the messy post-Soviet scramble to create a private economy. Its founder was a Ukrainian called Mikhail Fridman. He erected his empire in a frenetic rush—in a matter of TK years, he rose from washing windows 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 Pytor Aven. In the early nineties, 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 US 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 geostrategic intelligence firm Stratfor has described Fridman, "His friends (few) and enemies (many) describe him as slick, nimble, evolving, patient, calculating, combative, vindictive, and above all, underestimated. Fridman has repeatedly outmaneuvered far more politically and economically powerful rivals to end up on top, crushing his foes in the process. His skilled allies, impeccable business acumen, lack of a temper and utter absence of emotional attachment to his business holdings has made him rich, and will keep him so for a long time to come."

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 fellowship program that sponsors internships at the State Department. The Woodrow Wilson Center, the American-government funded think tank, gave Aven its award for "Corporate Citizenship" in 2015. To protect its interests in Washington, Alfa hired top Republican lobbyists, including Richard Burt , who helped Trump write the speech laying out his foreign policy and former Reagan administration official Ed Rogers. The branding campaign has worked wonders. During the first Obama term, Fridman and Aven met with officials in the White House on two occasions, according to visitor logs.

Alfa has significant business interests to promote in the West. One of its holding companies, LetterOne, has vowed to invest $3 billion in US health care. Last year, it sank $200 million into Uber. This is, of course, money that might otherwise be invested in Russia. According to a former US official. Putin tolerates this condition because Alfa does his bidding. It presses western governments to roll bank sanctions on Russian business --and 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 *FT* last year.

American officials who have dealt with Fridman and Aven describe a maddening dynamic. Nearly as soon as the conversations finished, American intelligence would report that the contents of the conversations had been instantly relayed to the Kremlin. "This is how they and everyone else in their position stays in the good graces of the Kremlin," a former official told me. "They must act as an agent of the state."

On Oct 30, 2016, at 6:31 PM, Peter Fritsch <ptritsch@fusiongps.com> wrote:

Time to hurry

Sent from my iPhone

Begin forwarded message:

From: Thomas Catan <tcatan@fusiongps.com>
Date: October 30, 2016 at 6:24:08 PM EDT
To: Peter Fritsch <pfritsch@fusiongps.com>, Glenn Simpson <gsimpson@fusiongps.com>
Subject: Reid

Sam Stein (@samsteinhp)
10/30/16, 5:48 PM
Reid says he's talked w/ top NatSec officials who say that Comey "possesses explosive information" about Trump's ties to Russia

Download the Twitter app

Sent from my iPhone