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

By Pamela Brown and Jose Pagliery, CNN


Updated 6:00 AM ET, Fri March 10, 2017

Source: CNN

Sources: FBI investigates 'odd' computer link

08:27

(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.

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."