# DNC email server most wanted evidence for Russia investigations


*The Democratic National Committee last year did not allow the FBI to physically inspect its machines, including servers. (Associated Press/File) The Democratic National Committee last year …* more >

It is perhaps the key piece of forensic evidence in Russia's suspected efforts to sway the November presidential election, but federal investigators have yet to get their hands on the hacked computer server that handled email from the Democratic National Committee.

Indeed, the only cybersecurity specialists who have taken a look at the server are from CrowdStrike, the Irvine, California-based private cybersecurity company that the DNC hired to investigate the hack — but which has come under fire itself for its work.

Some critics say CrowdStrike's evidence for blaming Russia for the hack is thin. Members of Congress say they still believe Russia was responsible but wonder why the DNC has never allowed federal investigators to get a look at the key piece of evidence: the server. Either way, a key "witness" in the political scandal consuming the Trump administration remains beyond the reach of investigators.

"I want to find out from the company [that] did the forensics what their full findings were," Sen. Lindsey Graham, a South Carolina Republican who is leading the Judiciary Committee's inquiry, told The Washington Times.

Scrutinizing the DNC server hack and CrowdStrike's analysis has not factored heavily in multiple probes exploring the Russia issue. But behind the scenes, discussions are growing louder, congressional sources say.

President Trump will hold an official bilateral meeting on Friday with Russian President Vladimir Putin on the sidelines of a Group of 20 summit in Germany, although it's unclear how big the Russian election hacking scandal will loom in their private talk.

**SPECIAL COVERAGE: Best of 2020: Top stories and columns from The Washington Times**

In recent days, questions about the server have taken on more importance as attention has focused on an email suggesting that the DNC and the Obama administration's Justice Department were trying to limit the scope of the FBI's investigation into Democratic presidential candidate Hillary Clinton's secret email account.

Mentioned in recent reporting and testimony from fired FBI Director James B. Comey, the correspondence reportedly shows Obama-era Attorney General Loretta E. Lynch privately assuring "someone in the Clinton campaign that the email investigation would not push too deeply into the matter."

Some observers have wondered whether the information is real or is Russian disinformation.

The hacked server was last photographed in the basement of the DNC's Washington headquarters near a file cabinet dating from the 1972 break-in of the DNC headquarters at the Watergate Hotel.

Both Republicans and Democrats say the DNC's reaction to the hacking is troubling.

Jeh Johnson, who served as homeland security secretary under President Obama, told the House Permanent Select Committee on Intelligence last month that his department offered to assist the DNC during the campaign to determine what was happening, but Mr. Johnson said he was rebuffed.

**SEE ALSO: House seeks contempt charges against CEO who maintained Hillary Clinton's secret email server**

"The DNC," Mr. Johnson said at the time, "did not feel it needed DHS' assistance at that time. I was anxious to know whether or not our folks were in there, and the response I got was the FBI had spoken to them, they don't want our help, they have CrowdStrike."

In January, Mr. Comey told the Senate Select Committee on Intelligence that the FBI issued "multiple requests at different levels" to assist the DNC with a cyberforensic analysis. Those requests were also denied.

DNC officials said the Russian hack had already been discovered and dealt with when the Homeland Security Department approached them last summer.

Sen. Kamala D. Harris, California Democrat and a member of the Senate intelligence committee, said more needs to be known about the interaction.

"As a general point, there is no question that we need to look into everything in terms of who did what, what was invasive about hacking, and what they gained from it and why," Ms. Harris told The Times. "Not only so we can establish what happened, but so it can teach us what is frankly inevitable about the next election cycle if we don't figure out what happened."

The White House has highlighted what it says is the DNC's reluctance to accept help dealing with the server hack. President Trump, in a May 7 tweet, wondered: "When will the Fake Media ask about the Dems dealings with Russia & why the DNC wouldn't allow the FBI to check their server or investigate?"

## Clouds over CrowdStrike

The DNC hack produced embarrassing internal emails that were posted to WikiLeaks and sparked a nasty internal battle just as the party was preparing for its convention and refereeing a spirited primary contest between front-runner Hillary Clinton and the insurgent campaign of Sen. Bernard Sanders.

Some emails suggested that the DNC leadership — including Chairwoman Debbie Wasserman Schultz — had plotted to undermine Mr. Sanders' ascent in the presidential race. The WikiLeaks revelations on July 22 eventually resulted in the departures of Ms. Wasserman Schultz and several other top DNC executives.

To explore the hack, the DNC called in CrowdStrike, a cybersecurity tech company launched in 2011 hoping to challenge better-known industry leaders such as Symantec and McAfee.

Co-founded by George Kurtz and Dmitri Alperovitch, both former McAfee employees, CrowdStrike quickly acquired a string of high-profile clients.

In 2014, it investigated the Sony Pictures leak, the disclosure of a trove of sensitive and embarrassing internal emails and executive salary data apparently orchestrated by hackers sympathetic to North Korea, and who objected to Sony's comic depiction of North Korean leader Kim Jong-un.

"We don't have a mission statement — we are on a mission to protect our customers from breaches," CrowdStrike's website declares.

The firm also has found success in generating venture capital support. Fortune magazine reported that it has raised $256 million and boasts a "valuation exceeding $1 billion."

Investors include Warburg Pincus, whose president, Timothy Geithner, worked for the Clinton and Obama administrations. The Clinton campaign's largest corporate contributor, Google, whose employees donated more than $1.3 million to Mrs. Clinton's campaign last year, also has funded CrowdStrike.

During the election cycle last year, the DNC paid CrowdStrike more than $410,000. This year, it has collected more than $121,000 from the party.

The DNC declined to answer questions about CrowdStrike. During a telephone call with The Times, DNC communications staff also refused to discuss the location of its infamous server.

In an ironic twist, CrowdStrike has added the National Republican Congressional Committee to its client list. The NRCC also declined to answer questions for this report.

In an email to The Times, CrowdStrike defended its record and said criticisms about its DNC work and interaction with U.S. law enforcement agencies are unfounded.

"In May 2016 CrowdStrike was brought to investigate the DNC network for signs of compromise, and under their direction we fully cooperated with every U.S. government request," a spokesman wrote. The cooperation included the "providing of the forensic images of the DNC systems to the FBI, along with our investigation report and findings. Those agencies reviewed and subsequently independently validated our analysis."

## Questions

Still, the company faces increasing scrutiny, including over the impartiality of co-founder Mr. Alperovitch.

Mr. Alperovitch is also a senior fellow at the Atlantic Council, a Washington-based think tank focused on international issues that is partially funded by Ukrainian billionaire Victor Pinchuk, who reportedly has donated at least $10 million to the Clinton Foundation.

Late last year, the International Institute for Strategic Studies, a respected British think tank, disputed CrowdStrike's analysis of a Russian hack during Ukraine's war with Russian-backed separatists. CrowdStrike later revised and retracted portions of its analysis.

CrowdStrike's most famous finding — that Russian-supported hackers penetrated the DNC server — has triggered the most questions.

Last year, that finding was wrapped into the assessment from the Office of the Director of National Intelligence, which first raised alarms about Russian meddling.

The DNI, which briefed Mr. Obama and Mr. Trump on the Russian meddling operation and issued classified and public assessments, concluded that "the Russian government directed the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations," meaning the DNC hack.

CrowdStrike said it found malware known as X-Agent on the DNC computers. Russia's Federal Security Service and its main military intelligence branch, the GRU, have used this malware to penetrate unclassified networks at the White House, the State Department and the Joint Chiefs of Staff.

CrowdStrike also said it had identified two teams of Russian hackers, with the code names "Fancy Bear" and "Cozy Bear," operating inside the DNC network.

"We've had lots of experience with both of these actors attempting to target our customers in the past and know them well," Mr. Alperovitch wrote on CrowdStrike's blog in June 2016.

But cybersecurity consultant Jeffrey Carr questioned whether CrowdStrike's evidence clinches the case.

"X-Agent has been around for ages and has always been attributed to the Russian government, but others use it," said Mr. Carr, who has supplied the U.S. intelligence community with analysis.

Mr. Carr said in an interview that the malware can be recovered, reverse-engineered and reused. Copies of X-Agent exist outside Russian hands, including one with an American cybersecurity company. He said it's possible CrowdStrike was duped — or simply sees Russia's handiwork everywhere.

WikiLeaks has consistently denied that it received the material from the Kremlin amid reports that a leaker within the DNC might have abetted the hack. WikiLeaks founder Julian Assange told Fox News in January: "We can say, we have said, repeatedly over the last two months that our source is not the Russian government and it is not a state party."

Atlanta-based hacker Robert David Graham, who runs a consultancy called Errata Security, said CrowdStrike's certainty about the Russian role can't be accepted uncritically.

"CrowdStrike is better than anything that the government has," he said. "But once you decide it is Russia, you will go looking for Russia."

Overall, he said, political factors distorted what needs to be a more scientific approach to who had access to the DNC servers.

"For good or bad, we make judgments based on our expertise and knowledge," he said. "Sometimes they are insightful and awesomely correct. Sometimes they fall flat on their face."

Mr. Graham, a libertarian like many others in the hacker community, said that from a privacy standpoint, he understands why the DNC would not want to hand over its server to the federal government. "What private company would?"

**Congressional inquiry?**

Whether CrowdStrike appears before a congressional inquiry anytime soon could depend on the momentum of the overall Russia investigations throughout Capitol Hill.

Late last month, after hearing Mr. Johnson say the DNC denied Homeland Security overtures to help secure its computers, Rep. Trey Gowdy, South Carolina Republican and the incoming chairman of the House Oversight and Government Reform Committee, said, "There may be something else on that server [that the DNC] didn't want law enforcement to see."

Mr. Graham has insisted he needs to know more about CrowdStrike.

"What did they find?" he asked.

Some on Capitol Hill have an even harsher take. Rep. Louie Gohmert, a conservative Texas Republican and a former prosecutor, said DNC and CrowdStrike are acting like defendants with something to hide in declining to allow government investigators access to the server.

"Why would they not invite them in?" Mr. Gohmert asked in a Fox News interview last month. "And I'm really interested in their excuse. But just from my own experience in all those years, usually the reason somebody didn't want to invite law enforcement in to investigate is because they knew they would find that they had committed crimes if they came in and started investigating."

The cybersecurity community also wants more answers.

"The only things that pay in the cybersecurity world are claims of attribution," Mr. Carr said. "Which foreign government attacked you? If you are critical of the attack, you make zero money. CrowdStrike is the poster child for companies that operate like this."

Last year, alongside one of the DNI assessments, the Obama administration released a spreadsheet containing part of CrowdStrike's cyberforensic work. The data included digital signatures and IP addresses, which trace computer-to-computer communications and help identify hackers. Mr. Graham, the hacker, said the only way to dispel all doubt would be to analyze independently everything CrowdStrike has seen. To do so would mean getting access to the DNC server.

As for CrowdStrike, when asked whether officials would be willing to testify before a congressional inquiry, a spokesman reiterated in an email that the company already "provided the forensic images and our analysis to the FBI." He said the company is "standing by the work it did for the DNC."

In May, less than a week after Mr. Comey was fired as FBI director, CrowdStrike announced it had raised $100 million in venture capital.

• *Dan Boylan can be reached at dboylan@washingtontimes.com.*