The Washington Post

National Security

Russian government hackers penetrated DNC, stole opposition research on Trump

By Ellen Nakashima
June 14, 2016

Russian government hackers penetrated the computer network of the Democratic National Committee and gained access to the entire database of opposition research on GOP presidential candidate Donald Trump, according to committee officials and security experts who responded to the breach.

The intruders so thoroughly compromised the DNC's system that they also were able to read all email and chat traffic, said DNC officials and the security experts.

The intrusion into the DNC was one of several targeting American political organizations. The networks of presidential candidates Hillary Clinton and Donald Trump were also targeted by Russian spies, as were the computers of some Republican political action committees, U.S. officials said. But details on those cases were not available.

"I completely rule out a possibility that the [Russian] government or the government bodies have been involved in this," Dmitry Peskov, the Kremlin's spokesman, told the Reuters news agency in Moscow.

Some of the hackers had access to the DNC network for about a year, but all were expelled over the past weekend in a major computer cleanup campaign, the committee officials and experts said.

The DNC said that no financial, donor or personal information appears to have been accessed or taken, suggesting that the breach was traditional espionage, not the work of criminal hackers.

The intrusions are an example of Russia's interest in the U.S. political system and its desire to understand the policies, strengths and weaknesses of a potential future president — much as American spies gather similar information on foreign candidates and leaders.

The depth of the penetration reflects the skill and determination of the United States' top cyber-adversary as Russia goes after strategic targets, from the White House and State Department to political campaign organizations.

"It's the job of every foreign intelligence service to collect intelligence against their adversaries," said Shawn Henry, president of CrowdStrike, the cyber firm called in to handle the DNC breach and a former head of the FBI's cyber division. He noted that it is extremely difficult for a civilian organization to protect itself from a skilled and determined state such as Russia.

"We're perceived as an adversary of Russia," he said. "Their job when they wake up every day is to gather intelligence against the policies, practices and strategies of the U.S. government. There are a variety of ways. [Hacking] is one of the more valuable because it gives you a treasure trove of information."

Russian President Vladimir Putin has spoken favorably about Trump, who has called for better relations with Russia and expressed skepticism about NATO. But unlike Clinton, whom the Russians probably have long had in their spy sights, Trump has not been a politician for very long, so foreign agencies are playing catch-up, analysts say.

"The purpose of such intelligence gathering is to understand the target's proclivities," said Robert Deitz, former senior councillor to the CIA director and
a former general counsel at
the National Security Agency. "Trump's foreign investments, for example, would be relevant to understanding how he would deal with countries where he has those investments" should he be elected, Deitz said. "They may provide tips for understanding his style of negotiating. In short, this sort of intelligence could be used by Russia, for example, to indicate where it can get away with foreign adventurism."

Other analysts noted that any dirt dug up in opposition research is likely to be made public anyway. Nonetheless, DNC leadership acted quickly after the intrusion's discovery to contain the damage.

"The security of our system is critical to our operation and to the confidence of the campaigns and state parties we work with," said Rep. Debbie Wasserman Schultz (Fla.), the DNC chairwoman. "When we discovered the intrusion, we treated this like the serious incident it is and reached out to CrowdStrike immediately. Our team moved as quickly as possible to kick out the intruders and secure our network."

Clinton called the intrusion "troubling" in an interview with Telemundo. She also said, "So far as we know, my campaign has not been hacked into," and added that cybersecurity is an issue that she "will be absolutely focused on" if she becomes president. "Because whether it's Russia, or China, Iran or North Korea, more and more countries are using hacking to steal our information, to use it to their advantage," she said.

A spokeswoman for the Trump campaign referred questions to the Secret Service.

DNC leaders were tipped to the hack in late April. Chief executive Amy Dacey got a call from her operations chief saying that their information technology team had noticed some unusual network activity.

"It's never a call any executive wants to get, but the IT team knew something was awry," Dacey said. And they knew it was serious enough that they wanted experts to investigate.

That evening, she spoke with Michael Sussmann, a DNC lawyer who is a partner with Perkins Coie in Washington. Soon after, Sussmann, a former federal prosecutor who handled computer crime cases, called Henry, whom he has known for many years.

Within 24 hours, CrowdStrike had installed software on the DNC's computers so that it could analyze data that could indicate who had gained access, when and how.

The firm identified two separate hacker groups, both working for the Russian government, that had infiltrated the network, said Dmitri Alperovitch, CrowdStrike co-founder and chief technology officer. The firm had analyzed other breaches by both groups over the past two years.

One group, which CrowdStrike had dubbed Cozy Bear, had gained access last summer and was monitoring the DNC's email and chat communications, Alperovitch said.

The other, which the firm had named Fancy Bear, broke into the network in late April and targeted the opposition research files. It was this breach that set off the alarm. The hackers stole two files, Henry said. And they had access to the computers of the entire research staff — an average of about several dozen on any given day.

The computers contained research going back years on Trump. "It's a huge job" to dig into the dealings of somebody who has never run for office before, Dacey said.

CrowdStrike is not sure how the hackers got in. The firm suspects they may have targeted DNC employees with "spearphishing" emails. These are communications that appear legitimate — often made to look like they came from a colleague or someone trusted — but that contain links or attachments that when clicked on deploy malicious software that enables a hacker to gain access to a computer. "But we don't have hard evidence," Alperovitch said.

The two groups did not appear to be working together, Alperovitch said. Fancy Bear is believed to work for the GRU, or Russia's military intelligence service, he said. CrowdStrike is less sure of whom Cozy Bear works for but thinks it might be the Federal Security Service, or FSB, the country's powerful security agency, which was once headed by Putin.

The lack of coordination is not unusual, he said. "There's an amazing adversarial relationship" among the Russian intelligence agencies, Alperovitch said. "We have seen them steal assets from one another, refuse to collaborate. They're all vying for power, to sell Putin on how good they are."

The two crews have "superb operational tradecraft," he said. They often use previously unknown software bugs — known as "zero-day" vulnerabilities — to compromise applications. In the DNC's case, the hackers constantly switched tactics to maintain a stealthy presence inside the network and used built-in Windows tools so that they didn't have to resort to malicious code that might trigger alerts. "They flew under the radar," Alperovitch said.

The two groups have hacked government agencies, tech companies, defense contractors, energy and manufacturing firms, and universities in the United States, Canada and Europe as well as in Asia, he said.

Cozy Bear, for instance, compromised the unclassified email systems of the White House, State Department and Joint Chiefs of Staff in 2014, Alperovitch said.

"This is a sophisticated foreign intelligence service with a lot of time, a lot of resources, and is interested in targeting the U.S. political system," Henry said. He said the DNC was not engaged in a fair fight. "You've got ordinary citizens who are doing hand-to-hand combat with trained military officers," he said. "And that's an untenable situation."

Russia has always been a formidable foe in cyberspace, but in the past two years, "there's been a thousand-fold increase in its espionage campaign against the West," said Alperovitch, who is also a senior fellow at the Atlantic Council. "They feel under siege."

Western sanctions, imposed after Russia's annexation of Crimea in Ukraine, have hurt the economy and led the government to increase its theft of intellectual property to limit the impact of import restrictions, he said. And Russia's growing isolation has increased the need for intelligence to understand and influence political decisions in other countries, he added.

CrowdStrike is continuing the forensic investigation, said Sussmann, the DNC lawyer. "But at this time, it appears that no financial information or sensitive employee, donor or voter information was accessed by the Russian attackers," he said.

The firm has installed special software on every computer and server in the network to detect any efforts by the Russian cyberspies to break in again. "When they get kicked out of the system," Henry predicted, "they're going to try to come back in."

Tom Hamburger contributed to this report.

Ellen Nakashima
Ellen Nakashima is a national security reporter with The Washington Post. She was a member of two Pulitzer Prize-winning teams, in 2018 for coverage of Russia's interference in the 2016 election, and in 2014 and for reporting on the hidden scope of government surveillance. Follow