How US cybersleuths decided Russia hacked the DNC

Digital clues led security pros to agencies in Putin's government. It's as close as we'll ever get to proof that Russia did it.

BY

LAURA HAUTALA

MAY 3, 2017 9:13 AM PDT

It was a bombshell.

Operatives from two Russian spy agencies had infiltrated computers of the Democratic National Committee, months before the US national election.

One agency -- nicknamed Cozy Bear by cybersecurity company CrowdStrike -- used a tool that was "ingenious in its simplicity and power" to insert malicious code into the DNC's computers, CrowdStrike's Chief Technology Officer Dmitri Alperovitch wrote in a June blog post. The other group, nicknamed Fancy Bear, remotely grabbed control of the DNC's computers.

By October, the Department of Homeland Security and the Office of the Director of National Intelligence on Election Security agreed that Russia was behind the DNC hack. On Dec. 29, those agencies, together with the FBI, issued a joint statement reaffirming that conclusion.

And a week later, the Office of the Director of National Intelligence summarized its findings (PDF) in a declassified (read: scrubbed) report. Even President Donald Trump acknowledged, "It was Russia," a few days later -- although he told "Face the Nation" earlier this week it "could've been China."

On Tuesday, the House Intelligence Committee heard testimony from top intelligence officials, including FBI Director James Comey and NSA Director Mike Rogers. But the hearing was closed to the public, and new details on the hacking attacks haven't emerged from either the House or the Senate's investigations into Russia's alleged attempt to influence the election.

However, during the Senate Judiciary Committee's open hearing on Wednesday, Comey agreed that the Russian government was still influencing American politics.

"What we've done with DHS is share the tools, tactics and techniques we see hackers, especially from the 2016 election season, using to attack voter registration databases," Comey said.

We'll probably never really find out what the US intelligence community or CrowdStrike know or how they know it. This is what we do know:

CrowdStrike and other cyberdetectives had spotted tools and approaches they'd seen Cozy Bear and Fancy Bear use for years. Cozy Bear is believed to be either Russia's Federal Security Service, known as the FSB, or its Foreign Intelligence Service, the SVR. Fancy Bear is thought to be Russia's military intel agency, GRU.

It was the payoff of a long game of pattern recognition -- piecing together hacker groups' favorite modes of attack, sussing out the time of day they're most active (hinting at their locations) and finding signs of their native language and the internet addresses they use to send or receive files.

"You just start to weigh all these factors until you get near 100 percent certainty," says Dave DeWalt, former CEO of McAfee and FireEye, who now sits on the boards of five security companies. "It's like having enough fingerprints in the system."

Watching the cyberdetectives

CrowdStrike put that knowledge to use in April, when the DNC's leadership called in its digital forensics experts and custom software -- which spots when someone takes control of network accounts, installs malware or steals files -- to find out who was mucking around in their systems, and why.

"Within minutes, we were able to detect it," Alperovitch said in an interview the day the DNC revealed the break-in. CrowdStrike found other clues within 24 hours, he said.

One agency used a tool "ingenious in its simplicity and power" to hack the DNC.

Dimitri Alperovitch

Those clues included small fragments of code called PowerShell commands. A PowerShell command is like a Russian nesting doll in reverse. Start with the smallest doll, and that's the PowerShell code. It's only a single string of seemingly meaningless numbers and letters. Open it up, though, and out jumps a larger module that, in theory at least, "can do virtually anything on the victim system," Alperovitch wrote.

One of the PowerShell modules inside the DNC system connected to a remote server and downloaded more PowerShells, adding more nesting dolls to the DNC network. Another opened and installed MimiKatz, malicious code for stealing login information. That gave hackers a free pass to move from one part of the DNC's network to another by logging in with valid usernames and passwords. These were Cozy Bear's weapons of choice.

Fancy Bear used tools known as X-Agent and X-Tunnel to remotely access and control the DNC network, steal passwords and transfer files. Other tools let them wipe away their footprints from network logs.

CrowdStrike had seen this pattern many times before.

"You could never go into the DNC as a single event and come up with that [conclusion]," said Robert M. Lee, CEO of cybersecurity firm Dragos.

Pattern recognition

Alperovitch compares his work to that of Johnny Utah, the character Keanu Reeves played in the 1991 surfing-bank-heist flick "Point Break." In the movie, Utah identified the mastermind of a robbery by looking at habits and methods. "He's already analyzed 15 bank robbers. He can say, 'I know who this is,'" Alperovitch said in an interview in February.

"The same thing applies to cybersecurity," he said.

Pattern recognition is how Mandiant, owned by FireEye, figured out that North Korea broke into Sony Pictures' networks in 2014.

The government stole Social Security numbers from 47,000 employees and leaked embarrassing internal documents and emails. That's because the Sony attackers left behind a favorite hacking tool that wiped, and then wrote over, hard drives. The cybersecurity industry had previously traced that tool to North Korea, which had been using it for at least four years, including in a massive campaign against South Korean banks the year before.

It's also how researchers from McAfee figured out Chinese hackers were behind Operation Aurora in 2009, when hackers accessed the Gmail accounts of Chinese human rights activists and stole source code from more than 150 companies, according to DeWalt, who was CEO of McAfee at the time of the investigation. Investigators found malware written in Mandarin, code that had been compiled in a Chinese operating system and time-stamped in a Chinese time zone, and other clues investigators had previously seen in attacks originating from China, DeWalt said.

"You just start to weigh all these factors until you get near 100 percent certainty."

Dave DeWalt

One of the most common complaints about the evidence CrowdStrike presented is that the clues could have been faked: Hackers could have used Russian tools, worked during Russian business hours and left bits of Russian language behind in malware found on DNC computers.

It doesn't help that, almost as soon as the DNC revealed it had been hacked, someone calling himself Guccifer 2.0 and claiming to be Romanian took credit as the sole hacker penetrating the political party's network.

That set off a seemingly endless debate about who did what, even as additional hacks of former Hillary Clinton campaign chairman John Podesta and others led to more leaked emails.

Cybersecurity experts say it would be too difficult for hackers to consistently make it look like an attack was coming from a different group of hackers. One mistake could blow their cover.

Critics probably won't be getting definitive answers anytime soon, since neither CrowdStrike nor US intelligence agencies plan to provide more details to the public, "as the release of such information would reveal sensitive sources or methods and imperil the ability to collect critical foreign intelligence in the future," the Office of the Director of National Intelligence said in its report.

"The declassified report does not and cannot include the full supporting information, including specific intelligence and sources and methods."

The debate has taken Alperovitch by surprise.

"Our industry has been doing attribution for 30 years," although such work on focused on criminal activity, he said. "The minute it went out of cybercrime, it became controversial."

Tech Enabled: CNET chronicles tech's role in providing new kinds of accessibility.

Logging Out: Welcome to the crossroads of online line and the afterlife.

First published on May 2, 2017 at 5:30 a.m. PT.

Updated on May 3, at 9:13 a.m.: to include details from FBI Director James Comey's Senate judiciary hearing.