National Security

Cybersecurity firm finds evidence that Russian military unit was behind DNC hack

A picture taken on Oct. 17, 2016, shows an employee walking behind a glass wall with machine coding symbols at the headquarters of Internet security giant Kaspersky in Moscow. (KIRILL KUDRYAVTSEV/AFP via Getty Images)

By Ellen Nakashima

December 22, 2016

A cybersecurity firm has uncovered strong proof of the tie between the group that hacked the Democratic National Committee and Russia’s military intelligence arm — the primary agency behind the Kremlin’s interference in the 2016 election.

The firm CrowdStrike linked malware used in the DNC intrusion to malware used to hack and track an Android phone app used by the Ukrainian army in its battle against pro-Russia separatists in eastern Ukraine from late 2014 through 2016.

While CrowdStrike, which was hired by the DNC to investigate the intrusions and whose findings are described in a new report, had always suspected that one of the two hacker groups that struck the DNC was the GRU, Russia's military intelligence agency, it had only medium confidence.

Now, said CrowdStrike co-founder Dmitri Alperovitch, "we have high confidence" it was a unit of the GRU. CrowdStrike had dubbed that unit "Fancy Bear."

The FBI, which has been investigating Russia's hacks of political, government, academic and other organizations for several years, privately has concluded the same. But the bureau has not publicly drawn the link to the GRU.

(Jhaan Elker/The Washington Post)

CrowdStrike's fingering of the GRU helps to deepen the public's understanding of how different arms of the Russian government are carrying out malicious and deeply troubling cyber acts in the United States. The director of national intelligence and the homeland security secretary in October publicly blamed the Russian government for interfering in the U.S. election, including through hacks of political organizations and targeting of state election systems.

After the election, the CIA and other intelligence agencies concluded that one of Russia's aims was to help President-elect Donald Trump win the election through a campaign of "active measures" or influence operations that included the hacking and dumping of emails onto public websites.

[FBI in agreement with CIA that Russia aimed to help Trump win White House]

The GRU, evidently, was key to this operation.

"The GRU is used for both tactical intelligence collection in the battlefield in support of Russian military operations and also strategic active measures or psychological warfare overseas," said Alperovitch, who is an expert on Russia and a senior fellow at the Atlantic Council. "The fact that they would be tracking and helping the Russian military kill Ukrainian army personnel in eastern Ukraine and also intervening in the U.S. election is quite chilling."

CrowdStrike found that a variant of the Fancy Bear malware that was used to penetrate the DNC's network in April 2016 was also used to hack an Android app developed by the Ukrainian army to help artillery troops more efficiently train their antiquated howitzers on targets.

The Ukrainian army's D-30 towed howitzers, which date to the Soviet era, typically take a number of minutes to position based on hand-drawn targeting data. With the Android app, positioning takes 15 seconds, CrowdStrike found.

The Fancy Bear crew evidently hacked the app, allowing the GRU to use the phone's GPS coordinates to track the Ukrainian troops' position. In that way, the Russian military could then target the Ukrainian army with artillery and other weaponry.

Ukrainian brigades operating in eastern Ukraine were on the front lines of the conflict with Russian-backed separatist forces during the early stages of the conflict in late 2014, CrowdStrike noted. By late 2014, Russian forces in the region numbered about 10,000. The Android app was useful in helping the Russian troops locate Ukrainian artillery positions.

According to the International Institute for Strategic Studies, Ukrainian artillery forces lost more than 50 percent of their weapons in the two years of conflict and more than 80 percent of their D-30 howitzers, the highest percentage of loss of any artillery piece in their arsenal, the report stated.

The app was not available in the Android app store and was distributed only through the social media page of its developer, who is a Ukrainian artillery officer, Yaroslav Sherstuk, according to CrowdStrike. It could be activated only after the developer was contacted and a code was sent to the individual downloading the application.

The other group that hacked the DNC also works for Russian intelligence, CrowdStrike reported earlier this year. But the firm is not sure if it is the more internally focused FSB, or the foreign intelligence arm, the SVR. Both grew out of the KGB.

That group, which CrowdStrike has called Cozy Bear, has not apparently been deployed in the influence operation, Alperovitch said. Rather, it is focused on traditional espionage. It is the group that is believed to have hacked unclassified networks of the State Department, White House and the Joint Chiefs of Staff.

More from National Security:

U.S. intelligence officials say Russian hacks ‘prioritized’ Democrats

The attorney general could have ordered FBI Director James Comey not to send his bombshell letter on Clinton emails. Here’s why she didn’t.

Hackers can now report bugs in Defense Dept. websites without fear of prosecution