

# Russia's Fancy Bear Hackers Likely Penetrated a US Federal Agency

wired.com/story/russias-fancy-bear-hack-us-federal-agency/

Andy Greenberg

October 1, 2020



A warning that unidentified hackers broke into an agency of the US federal government and stole its data is troubling enough. But it becomes all the more disturbing when those unidentified intruders are identified—and appear likely to be part of a notorious team of cyberspies working in the service of Russia's military intelligence agency, the GRU.

Last week the Cybersecurity and Infrastructure Security Agency published an advisory that hackers had penetrated a US federal agency. It identified neither the attackers nor the agency, but did detail the hackers' methods and their use of a new and unique form of malware in an operation that successfully stole target data. Now, clues uncovered by a researcher at cybersecurity firm Dragos and an FBI notification to hacking victims obtained by WIRED in July suggest a likely answer to the mystery of who was behind the intrusion: They appear to be Fancy Bear, a team of hackers working for Russia's GRU. Also known as APT28, the group has been responsible for everything from hack-and-leak operations targeting the 2016 US presidential election to a broad campaign of attempted intrusions targeting political parties, consultancies, and campaigns this year.

"They're a formidable actor, and they're still capable of getting access to sensitive areas."

John Hultquist, FireEye

The clues pointing to APT28 are based in part on a notification the FBI sent to targets of a hacking campaign in May of this year, which WIRED obtained. The notification warned that APT28 was broadly targeting US networks, including government agencies and educational institutions, and listed several IP addresses they were using in their operations. Dragos researcher Joe Slowik noticed that one IP address identifying a server in Hungary used in that APT28 campaign matched an IP address listed in the CISA advisory. That would suggest that APT28 used the same Hungarian server in the intrusion described by CISA—and that at least one of the attempted intrusions described by the FBI was successful.

"Based on the infrastructure overlap, the series of behaviors associated with the event, and the general timing and targeting of the US government, this seems to be something very similar to—if not a part of—the campaign linked to APT28 earlier this year," says Slowik, the former head of Los Alamos National Labs' Computer Emergency Response Team.

Aside from that FBI notification, Slowik also found a second infrastructure connection. A report last year from the Department of Energy warned that APT28 had probed a US government organization's network from a server in Latvia, listing that server's IP address. And that Latvian IP address, too, reappeared in the hacking operation described in the CISA advisory. Together, those matching IPs create a web of shared infrastructure that ties the operations together. "There are one-to-one overlaps in the two cases," Slowik says.

Confusingly, some of the IP addresses listed in the FBI, DOE, and CISA documents also seem to overlap with known cybercriminal operations, Slowik notes, such as Russian fraud forums and servers used by banking trojans. But he suggests that means Russia's state-sponsored hackers are most likely reusing cybercriminal infrastructure, perhaps to create deniability. WIRED reached out to CISA, as well as the FBI and DOE, but none responded to our request for comment.

Although it doesn't name APT28, CISA's advisory does detail step-by-step how the hackers carried out their intrusion inside an unidentified federal agency. The hackers had somehow obtained working usernames and passwords for multiple employees, which they used to gain entry onto the network. CISA admits it doesn't know how those credentials were obtained, but the report speculates that the attackers may have used a known vulnerability in Pulse Secure VPNs that CISA says has been exploited widely across the federal government.

The intruders then used command line tools to move among the agency's machines, before downloading a piece of custom malware. They then used that malware to access the agency's file server and move collections of files to machines the hackers controlled, compressing them into .zip files they could more easily steal.

While CISA didn't make a sample of the hackers' custom trojan available to researchers, security researcher Costin Raiu says that the attributes of the malware matched another sample uploaded to the malware research repository VirusTotal from somewhere in the United Arab Emirates. By analyzing that sample, Raiu found that it appears to be a unique

creation built from a combination of the common hacking tools Meterpreter and Cobalt Strike, but with no obvious links to known hackers, and obfuscated with multiple layers of encryption. "That wrapping makes it kind of interesting," says Raiu, director of Kaspersky's global research and analysis team. "It is kind of unusual and rare in the sense that we couldn't find connections with anything else."

Even aside from their 2016 breaches of the Democratic National Committee and the Clinton campaign, Russia's APT28 hackers loom over the 2020 election. Earlier this month [Microsoft warned that the group has been carrying out mass-scale, relatively simple techniques to breach election-related organizations](#) and campaigns on both sides of the political aisle. According to Microsoft, the group has used a combination of password-spraying that tries common passwords across many users' accounts and password brute-forcing that tries many passwords against a single account.



But if APT28 is indeed the hacker group described in the CISA advisory, it's a reminder that they're also capable of more sophisticated and targeted spying operations, says John Hultquist, the director of intelligence at security firm FireEye, which didn't independently confirm Slowik's findings linking the CISA report to APT28. "They're a formidable actor, and they're still capable of getting access to sensitive areas," says Hultquist.

APT28, before its more recent hack-and-leak operations of the last few years, has a long history of espionage operations that have targeted US, NATO, and Eastern European government and military targets. The CISA advisory, along with the DOE and FBI findings that track related APT28 hacking campaigns, all suggest that those spying operations continue today.

"It's certainly not surprising that Russian intelligence would be trying to penetrate the US government. That's kind of what they do," says Slowik. "But it is worth identifying that not only is such activity continuing, it's been successful."

---

## More Great WIRED Stories

-  Want the latest on tech, science, and more? [Sign up for our newsletters!](#)
- The cheating scandal that [ripped the poker world apart](#)
- The 20-Year hunt for the man [behind the Love Bug virus](#)
- There's no better time [to be an amateur radio geek](#)
- The 15 TV shows you [need to binge this fall](#)
- Could a tree help find a [decaying corpse nearby?](#)
-  Things not sounding right? Check out our favorite [wireless headphones](#), [soundbars](#), and [Bluetooth speakers](#)