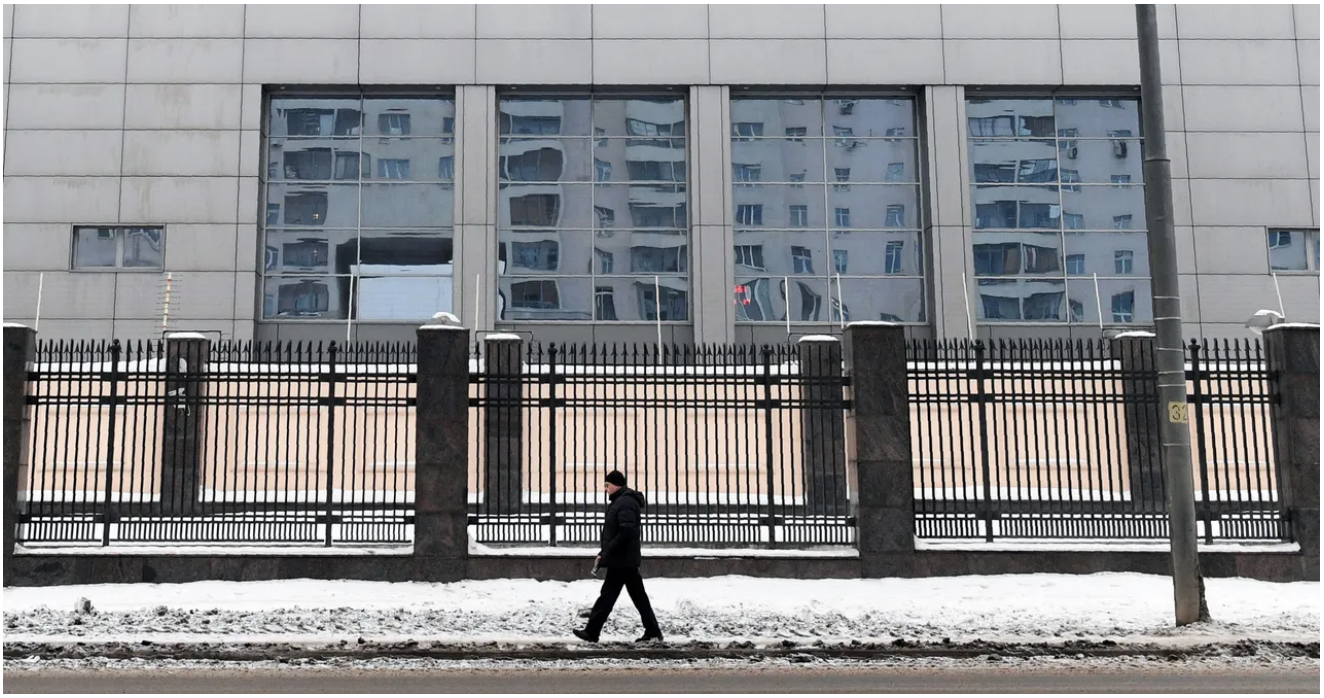
Russia's GRU Hackers Hit US Government and Energy Targets

wired.com/story/russia-fancy-bear-us-hacking-campaign-government-energy/

Andy Greenberg July 24, 2020



Russia's GRU military intelligence agency has carried out many of the most aggressive acts of hacking in history: destructive worms, blackouts, and—closest to home for Americans—a broad hacking-and-leaking operation designed to influence the outcome of the 2016 US presidential election. Now it appears the GRU has been hitting US networks again, in a series of previously unreported intrusions that targeted organizations ranging from government agencies to critical infrastructure.

From December 2018 until at least May of this year, the GRU hacker group known as APT28 or Fancy Bear carried out a broad hacking campaign against US targets, according to an FBI notification sent to victims of the breaches in May and obtained by WIRED. According to the FBI, the GRU hackers primarily attempted to break into victims' mail servers, Microsoft Office 365 and email accounts, and VPN servers. The targets included "a wide range of US-based organizations, state and federal government agencies, and educational institutions," the FBI notification states. And technical breadcrumbs included in that notice reveal that APT28 hackers have targeted the US energy sector, too, apparently as part of the same effort.

"The natural worry is, am I the next John Podesta?"

APT28 Victim

The revelation of a potentially ongoing US-targeted GRU hacking spree is especially troubling in light of the GRU's past operations, which have often gone beyond mere espionage to include embarrassing email leaks or even disruptive cyberattacks. APT28 hackers in particular have been the subject of US indictments alleging hack-and-leak operations targeting both the 2016 US election and the Worldwide Anti-doping Agency. The latter attack was in apparent retaliation for the International Olympic Committee banning Russia from the 2018 Olympics for performance-enhancing drug use.

"Although not all motives are clear, we can make judgments based on the nature of the target as seen through past indictments," an FBI spokesperson wrote in a statement responding to WIRED's request for further comment on the notification sent to APT28 hacking victims. The FBI also says that the GRU hacking campaign has likely continued into recent months. "An Advanced Persistent Threat is just that," the spokesperson added, referring to the APT acronym from which APT28 takes its name. "There is an expectation of continued activity."

According to the FBI's victim notification, the APT28 hackers have gained access to networks via spear-phishing emails sent to both personal and work email accounts. They've also used password-spraying attacks, in which hackers try common passwords across many accounts, as well as brute force attacks that guess a long list of passwords against one or a small number of accounts.

Within days of the FBI's notification being sent to victims in early May, the NSA issued a public advisory that Sandworm, a separate but closely linked GRU hacker group, was exploiting a vulnerability in Exim mail servers to target victims. The FBI told WIRED it knew of no connection between that Exim exploitation and the APT28 campaign.

One staff member at an affected organization told WIRED that the IT staff had seen no sign of a successful phishing attack—but nonetheless found that the hackers had accessed their email server. "Once they were on the server they stole entire mailboxes," says the staffer, who asked that WIRED not reveal either their identity or the organization they work for.

The organization was eventually notified by the FBI that they had in fact been breached by APT28. "The natural worry is, am I the next John Podesta?" the staffer says, referring to the Hillary Clinton campaign director whose emails were stolen and leaked by APT28 ahead of the 2016 election. "Reading the victim notification and realizing how many different organizations were probably targeted, it just underscores that exactly what we worried about in 2016 is something that Russia is literally still doing as we speak."

The FBI declined to comment on how many victims the APT28 campaign may have targeted, or how many of those attempts were successful. But security firm FireEye says it has learned of a "handful" of victim organizations that were compromised by hackers using the same IP addresses listed as used by APT28 in the FBI victim notification. In those cases, the hackers

appear not to have infected systems with malware, says Ben Read, a cyberespionage analyst at FireEye, instead using stolen credentials to move around the corporate network as employees would. "It was a pretty light touch," Read says.

While neither FireEye nor the FBI would reveal the identities of APT28's victims, at least one of the group's targets appears to have been in the US energy industry. A Department of Energy advisory issued in January warned that on Christmas Eve of last year, someone probed the login pages of a "US energy entity" from an IP address that had previously been used by APT28. That same IP address was also listed by the FBI among those used by APT28's hackers through May, confirming that APT28 was very likely behind that incident.

Energy sector intrusions would represent a shift in targeting for APT28, says Joe Slowik, the security researcher at industrial-control-system security firm Dragos who spotted the connection between the DOE advisory and the FBI victim notification. "Just given what we understand about how APT28 operates and its typical victimology, identifying that group interacting with the US energy sector would be substantially different from how this group has behaved previously," he says.

While apparently a new venture for APT28, the GRU as a whole does have a history of hacking critical infrastructure. The GRU hacker group Sandworm planted malware on the networks of US electric utilities in 2014, then carried out the first-ever cyberattack-induced blackouts in Ukraine in 2015 and 2016. The notion that APT28 may now be sniffing around US energy industry targets too—or that Sandworm is, given that the two groups have teamed up in the past—is disturbing, argues Slowik. "This is a concerning data point," Slowik says. "It's the first time in a while that this group has targeted US critical infrastructure."

A new GRU hacking campaign targeting US organizations in 2020 also raises the specter of another round of election meddling, given the GRU's notorious campaign of electoral interference in 2016. US intelligence officials have been warning since early this year that Russia has sought to interfere in US electoral politics again to help reelect President Trump. But the FBI and FireEye both say they saw no signs that this particular string of intrusions by APT28 were related to the upcoming presidential election.

Instead, says FireEye's Read, the campaign shows that the GRU's general interest in US targets hasn't ended, even as its endgame remain unclear. "The US continues to be the chief antagonist for Russia in their mind. It's an important reminder that this is still going on," says Read. "It's hard to say if it's a significant escalation. But it's obviously not good."

More Great WIRED Stories

- Behind bars, but still posting on TikTok
- My friend was struck by ALS. To fight back, he built a movement
- Deepfakes are becoming the hot new corporate training tool
- America has a sick obsession with Covid-19 polls

- Who discovered the first vaccine?
- 👁️ Prepare for AI to produce less wizardry. Plus: Get the latest AI news
- 🎙️ Listen to Get WIRED, our new podcast about how the future is realized. Catch the latest episodes and subscribe to the 📩 newsletter to keep up with all our shows
- 📱 Torn between the latest phones? Never fear—check out our iPhone buying guide and favorite Android phones