

# Russian state hackers are targeting Biden and Trump campaigns, MSFT warns

Enlarge / Vladimir Putin.

## reader comments

1 with 1 posters participating

## Share this story

Fancy Bear—the Russian state hacking group that brought you the smash-and-leak attacks on the Democratic National Committee and World Anti-Doping Agency, the NotPetya worm that inflicted billions of dollars of damage worldwide, and the VPN Filter compromise of 500,000 routers—is targeting organizations involved in elections taking place in the US and UK, Microsoft has warned.

Over a two-week period last month, the group attempted attacks on more than 6,900 accounts belonging to 28 organizations, Microsoft said. Between September 2019 and last June, Fancy Bear targeted tens of thousands of accounts belonging to employees of more than 200 organizations. The hackers use two techniques—one known as “brute forcing” and the other called “password spraying”—in an attempt to obtain targets’ Office365 login credentials. So far, none of the attacks has succeeded.

Security researchers from a host of companies widely agree that Fancy Bear works on behalf of the GRU, Russia’s military intelligence agency. The GRU has been tied to more than a decade of advanced hacking campaigns, including several that

have inflicted serious damage to national security. Industry members use an assortment of colorful names to refer to the group. Besides Fancy Bear, there's also Pawn Storm, Sofacy, Sednit, and Tsar Team. Microsoft's name for the outfit is Strontium.

"Microsoft's Threat Intelligence Center (MSTIC) has observed a series of attacks conducted by Strontium between September 2019 and today," Microsoft Corporate Vice President Tom Burt wrote in a post published on Thursday. "Similar to what we observed in 2016, Strontium is launching campaigns to harvest people's log-in credentials or compromise their accounts, presumably to aid in intelligence gathering or disruption operations."

Strontium is one of three state-sponsored hacking groups that Microsoft said are targeting the 2020 elections. Zirconium—believed to work for the People's Republic of China—has been targeting "high-profile individuals associated with the election, including people associated with the Joe Biden for President campaign and prominent leaders in the international affairs community." Phosphorus, which researchers say works on behalf of the Islamic Republic of Iran, continues to target personal accounts of people associated with President Donald Trump's reelection campaign.

## **Big bad bear**

While campaigns from all three groups pose a risk, the one from Fancy Bear carries the biggest threat, given the group's advanced skill and techniques and its track record of brazen and dangerous hacks. An accompanying Microsoft post that provided technical details about the Fancy Bear hacking campaign said the group has streamlined and automated its operations significantly since 2016.

Four years ago, Fancy Bear leaned heavily on spear phishing, or the sending of convincing-looking emails that spoofed

personnel from Google or other well-known organizations. The emails, one that famously hooked Hillary Clinton's presidential campaign chairman, John Podesta, falsely reported to receivers that their accounts had been compromised. The spearphishes then instructed them to log in to what turned out to be a fake site and change their passwords.

Now, Fancy Bear is relying primarily on tools that perform password spraying and brute forcing. The change makes it easier to operate at scale and in a way that's more anonymized. The tools are distributed through a pool of roughly 1,100 IP addresses, with most of them belonging to the Tor anonymization service. In Thursday's technical post, Microsoft researchers wrote:

*This pool of infrastructure has evolved over time, with an average of approximately 20 IPs added and removed from it per day. STRONTIUM's tooling alternates its authentication attempts amongst this pool of IPs approximately once per second. Considering the breadth and speed of this technique, it seems likely that STRONTIUM has adapted its tooling to use an anonymizer service to obfuscate its activity, evade tracking, and avoid attribution.*

## Spreading the load

In the attacks between August 19 and September 3, Microsoft observed a daily average of 1,294 IP addresses from more than 500 address blocks and 250 autonomous system numbers. Some of the netblocks were used more often than others. The overutilization of the netblocks created an opportunity for researchers to ferret out Fancy Bear activity that used the anonymization service. Microsoft used this Azure Sentinel query to identify failed authentication attempts from the three most widely used address blocks and group them by the user agents attempting to log in.

The two techniques Fancy Bear is using are:

- Password spraying, which attempts to find valid username-password combinations. Typically, there are about four tries each hour over the course of days or weeks. Almost every attempt originates from a different IP address.
- Brute-forcing, which peppers a targeted account with about 300 login attempts per hour over the course of several hours or days.

## What, me worry?

Given the fallout from Fancy Bear's 2016 hacks, you might think that most high-value targets had since adopted multifactor authentication, which requires the person logging in to provide the correct password and to also prove possession of a device or present a fingerprint or other biometric. But according to Microsoft, you'd be wrong. Figures the company published last October show that less than 10 percent of large-organization accounts use any form of MFA. Turning multifactor authentication on thwarts most credential-harvesting attacks, Microsoft said.

Thursday's technical post also recommended high-value target organizations monitor logs for failed authentications.

"When monitoring login activity in your accounts, look for any type of discernible patterns in these failed authentications and track them over time," researchers advised. Password spray is an increasingly common tactic of nation-state actors."

<https://arstechnica.com/?p=1705249>