# Russian hackers hijack Ubiquiti routers to launch stealthy attacks

By Sergiu Gatlan

Published: 2024-02-27 · Archived: 2026-04-05 16:44:51 UTC

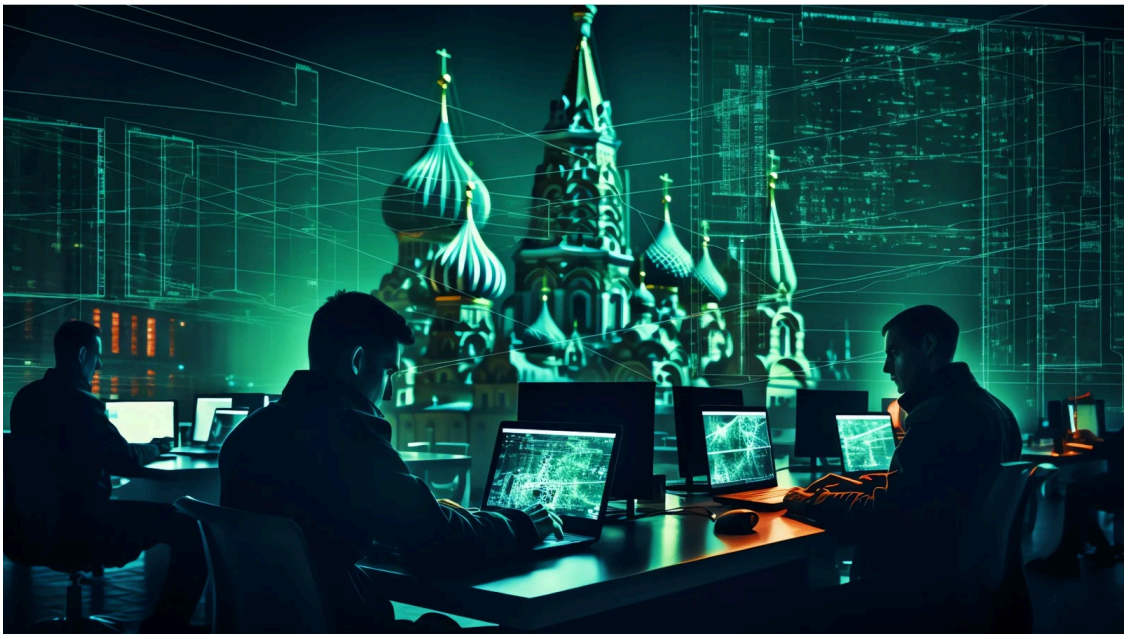
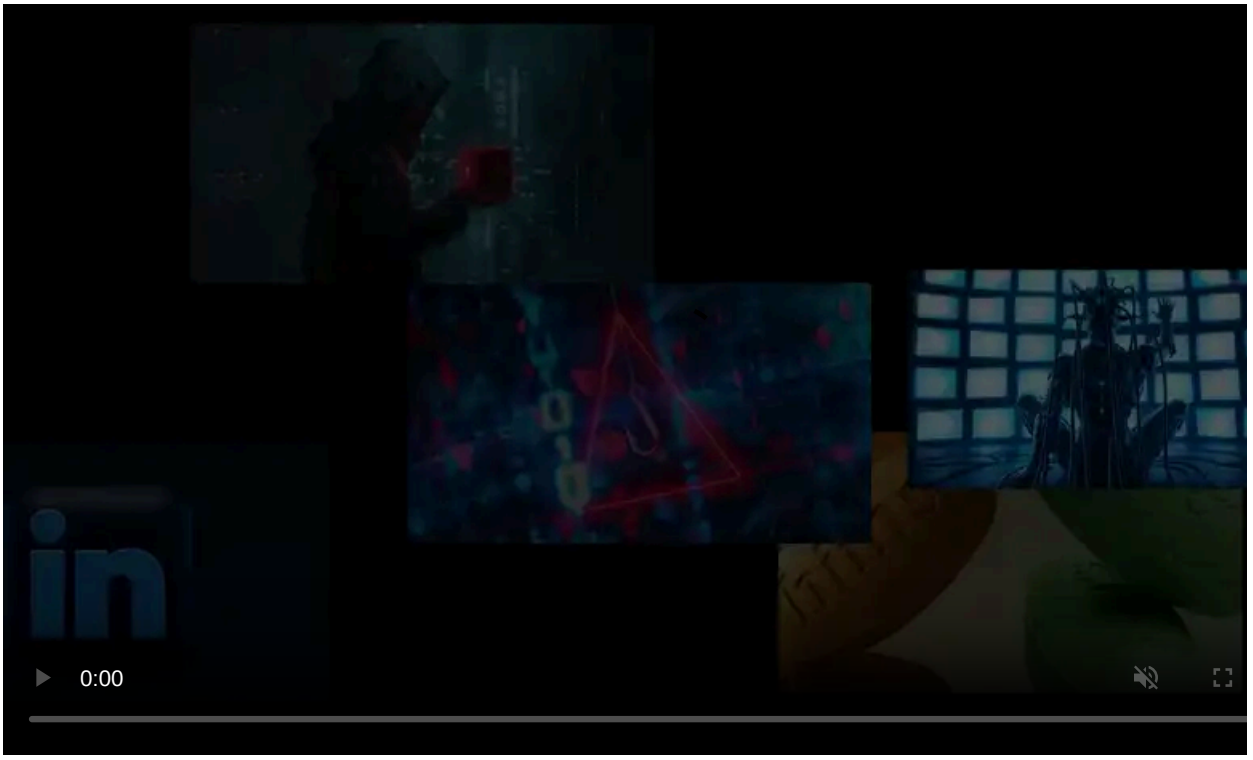
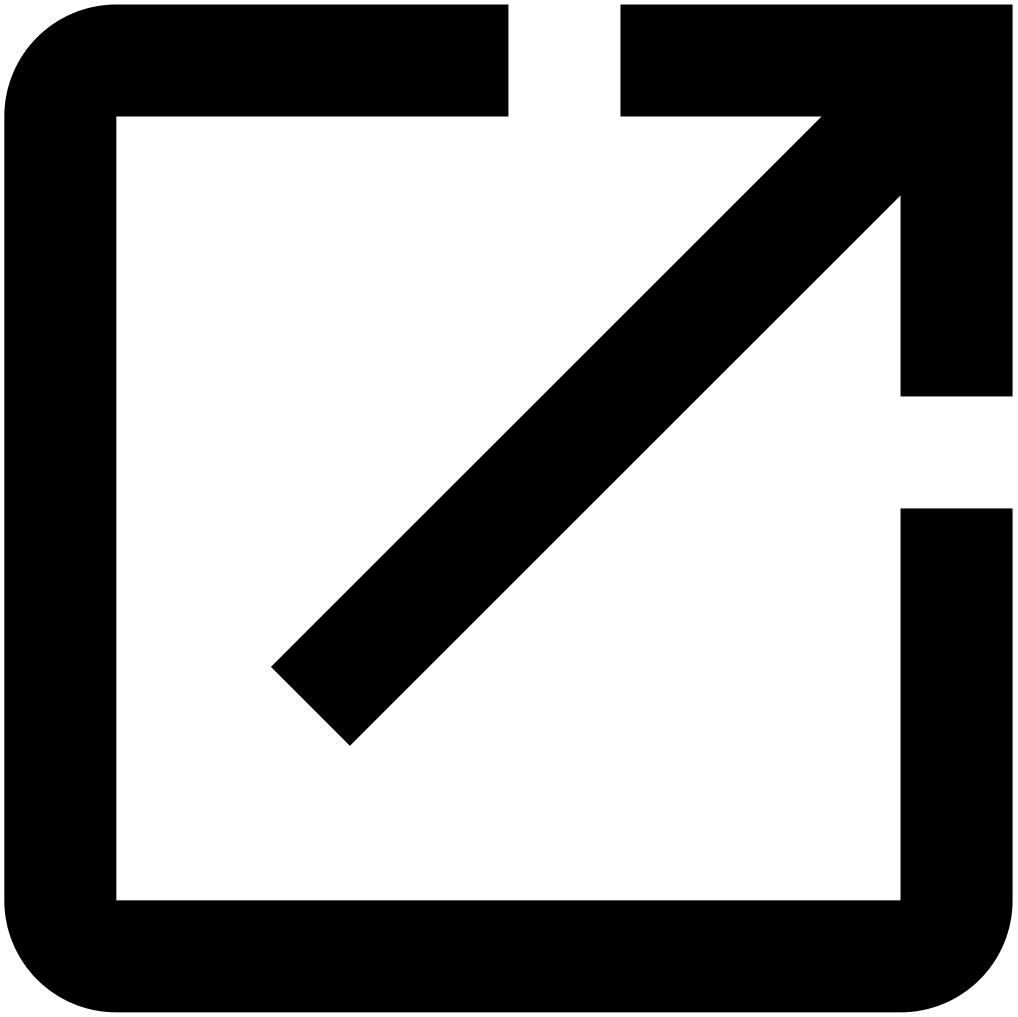


*Image: Midjourney*

Russian military hackers are using compromised Ubiquiti EdgeRouters to evade detection, the FBI says in a joint advisory issued with the NSA, the U.S. Cyber Command, and international partners.

Military Unit 26165 cyberspies, part of Russia's Main Intelligence Directorate of the General Staff (GRU) and tracked as APT28 and Fancy Bear, are using these hijacked and very popular routers to build extensive botnets that help them steal credentials, collect NTLMv2 digests, and proxy malicious traffic.


0:00



They're also used to host custom tools and phishing landing pages throughout covert cyber operations targeting militaries, governments, and other organizations worldwide.

"EdgeRouters are often shipped with default credentials and limited to no firewall protections to accommodate wireless internet service providers (WISPs). Additionally, EdgeRouters do not automatically update firmware unless a consumer configures them to do so," the FBI warns.

"In summary, with root access to compromised Ubiquiti EdgeRouters, APT28 actors have unfettered access to Linux-based operating systems to install tooling and to obfuscate their identity while conducting malicious campaigns."

Earlier this month, the FBI disrupted a botnet of Ubiquiti EdgeRouters infected with the Moobot malware by cybercriminals not linked with APT28 that the Russian hacking group later repurposed to build a cyber espionage tool with global reach.

While investigating the hacked routers, the FBI discovered various APT28 tools and artifacts, including Python scripts for stealing webmail credentials, programs designed to harvest NTLMv2 digests, and custom routing rules that automatically redirected phishing traffic to dedicated attack infrastructure.

APT28 is a notorious Russian hacking group found to be responsible for several high-profile cyber attacks since they first began operating

They breached the German Federal Parliament (Deutscher Bundestag) and were behind attacks on the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) ahead of the U.S. Presidential Election in 2016.

Two years later, APT28 members were charged in the U.S. for their involvement in the DNC and DCCC attacks. The Council of the European Union also sanctioned APT28 members in October 2020 for their involvement in the German Federal Parliament hack.

## How to 'revive' hijacked Ubiquiti EdgeRouters

The FBI and partner agencies behind today's advisory recommend the following measures to get rid of the malware infection and block APT28's access to compromised routers:

1. Perform a hardware factory reset to flush file systems of malicious files
2. Upgrade to the latest firmware version
3. Change any default usernames and passwords, and
4. Implement strategic firewall rules on WAN-side interfaces to prevent unwanted exposure to remote management services.

The FBI is seeking information on APT28 activity on hacked EdgeRouters to prevent further use of these techniques and hold those responsible accountable.

You should report any suspicious or criminal activities related to these attacks to your local FBI field office or the FBI's Internet Crime Complaint Center (IC3).

A joint alert issued by U.S. and U.K. authorities also warned six years ago, in April 2018, that Russian state-backed attackers were actively targeting and hacking home and enterprise routers.

As the April 2018 advisory cautioned, Russian hackers have historically targeted Internet routing equipment to use in man-in-the-middle attacks in support of espionage campaigns, maintain persistent access to victims' networks, and lay a foundation for other offensive operations.

---

Source: https://www.bleepingcomputer.com/news/security/russian-hackers-hijack-ubiquiti-routers-to-launch-stealthy-attacks/