# FBI to all router users: Reboot now to neuter Russia's VPNFilter malware

By Written by

Archived: 2026-04-05 15:05:15 UTC

**Security**

- 
- 
- 
- 

The FBI is urging small businesses and households to immediately reboot routers following Cisco's report that 500,000 infected devices could be destroyed with a single command.

The malware, dubbed VPNFilter, was developed by the Russian state-sponsored hacking group Sofacy, also known as Fancy Bear and APT28, according to the FBI, which last week obtained a warrant to seize a domain used to control the infected routers.

Cisco's Talos Intelligence researchers revealed in a report last week that 500,000 routers made by Linksys, MikroTik, Netgear, and TP-Link had been infected with VPNFilter.

The malware is capable of collecting traffic sent through infected routers, such as website credentials.

However, the most worrying capability is that malware allows its controllers to wipe a portion of an infected device's firmware, rendering it useless. The attackers can selectively destroy a single device or wipe all infected devices at once.

**See:** Special report: Cybersecurity in an IoT and mobile world (free PDF)

Cisco released the report on Wednesday after observing a spike this month in infections in the Ukraine, which accused Russia of planning an attack to coincide with Saturday's Champions Cup final in Kiev.

The country also blamed Russia for last June's NotPetya attacks that mostly affected Ukraine organizations but also spread within multinational corporations with offices in Ukraine.

Users with infected routers can remove the dangerous Stage 2 and Stage 3 components of VPNFilter by rebooting the device. However, Stage 1 of VPNFilter will persist after a reboot, potentially allowing the attackers to reinfect the compromised routers.

The web address the FBI seized on Wednesday, ToKnowAll[.]com, could have been used to reinstall Stage 2 and Stage 3 malware, but all traffic to this address is now being directed to a server under the FBI's control.

The FBI nonetheless is urging all small office and home router owners to reboot devices even if they were not made by one of the affected vendors. This will help neuter the threat and help the FBI identify infected devices.

"The FBI recommends any owner of small office and home office routers reboot the devices to temporarily disrupt the malware and aid the potential identification of infected devices," the FBI said in a public-service announcement.

"Owners are advised to consider disabling remote-management settings on devices and secure with strong passwords and encryption when enabled. Network devices should be upgraded to the latest available versions of firmware."

Cisco and the Justice Department have also urged all home and small office users to reboot routers.

**See:** What is phishing? How to protect yourself from scam emails and more

The Justice Department said the FBI-controlled server to which infected devices are now communicating with will collect the IP addresses of each device.

The addresses are being shared with the non-profit cyber security group, The Shadowserver Foundation, which will disseminate the addresses to foreign CERTs and ISPs. The FBI and US DHS CERT has also notified some ISPs.

It's not known how the attackers initially infected the routers, but Symantec noted in its report on VPNFilter that many of them have known vulnerabilities.

"Most of the devices targeted are known to use default credentials and/or have known exploits, particularly for older versions. There is no indication at present that the exploit of zero-day vulnerabilities is involved in spreading the threat," wrote Symantec researchers.

Known infected devices include:

- Linksys E1200
- Linksys E2500
- Linksys WRVS4400N
- MikroTik RouterOS for Cloud Core Routers: Versions 1016, 1036, and 1072
- Netgear DGN2200
- Netgear R6400
- Netgear R7000
- Netgear R8000
- Netgear WNR1000
- Netgear WNR2000
- QNAP TS251
- QNAP TS439 Pro
- Other QNAP NAS devices running QTS software
- TP-Link R600VPN

## Previous and related coverage

**Talos finds new VPNFilter malware hitting 500K IoT devices, mostly in Ukraine**

Cisco's Talos has published preliminary findings of the VPNFilter malware, which is targeting mostly consumer internet routers from a range of vendors, with some consumer NAS devices also hit.

**Russians suspected of new German attack may 'have been inside system for a year'**

German intelligence services and federal specialists are investigating "an IT security incident".

**Hackers are using a Flash flaw in fake document in this new spying campaign**

The payload is delivered via phishing emails about a real defence conference -- but nothing happens until the target scrolls down to the third page...

---