



May 31, 2018

Cyber: District Residents Should Reboot Internet Routers

In response to recently discovered Russian malware—VPNFilter—US authorities are advising residents to reset home and office routers. VPNFilter has infected an estimated 500,000 routers in 54 countries; it blocks web traffic, collects information, and can disable routers.

- The Sofacy Group, which is linked to Russian military intelligence, is responsible for the attack and controls the network of infected routers, according to US authorities. The group, which targets foreign governments, military, and security agencies, also hacked the Democratic National Committee in 2016.
- FBI encourages residents to either turn off power to their routers and then turn it back on, or to unplug the device for at least ten seconds before restoring power; these steps will disrupt the malware and aid in the identification of infected devices. Authorities also recommend installing software updates, disabling the ability to login remotely, and creating strong, original passwords.

Key Definitions

Malware: software intended to damage or disable computers

Reboot: restart a device; turn it off and on

Router: a device that transmits data between computer networks



Commonly targeted router manufacturers are Linksys, MikroTik, Netgear, and TP-Link.

DC Homeland Security and Emergency Management Agency suggests the following steps to protect against cyber intrusions:

- Enable encryption and do not share passwords;
- Update devices to the latest versions of antivirus software;
- Avoid using public WiFi networks and turn off Bluetooth when not in use;
- Avoid public charging stations, such as those in airports or public computers;
- Do not click on any emails, attachments, or links from unknown senders; and
- Avoid emails that contain various grammatical errors and typos.

Resources:

- [Ready DC: Before, During and After a Cyber Attack](#)
- [FBI Public Service Announcement](#)
- [Justice Department Announcement](#)
- [DHS: Protect Myself from Cyber Attacks](#)