VPNFilter malware has infected a million routers — here's what you need to know

Jerry Hildenbrand
Android Central, 11 Jun 2018

Malware linked to the Russian government can manipulate your internet traffic, harvest personal information, and serve as a launch point for a broad range of internet attacks.

A recent discovery that new router-based malware, known as VPNFilter, had infected well over 500,000 routers just became even worse news. In a report expected to be released June 13, Cisco states that over 200,000 additional routers have been infected and that the capabilities of VPNFilter are far worse than initially thought. Ars Technica has reported on what to expect from Cisco Wednesday.

VPNFilter is malware that is installed on a Wi-Fi router. It has already infected almost one million routers across 54 countries, and the list of devices known to be affected by VPNFilter contains many popular consumer models. It's important to note that VPNFilter is **not** a router exploit that an attacker can find and use to gain access —

it is software that is installed on a router unintentionally that is able to do some potentially terrible things.

VPNFilter is malware that somehow gets installed on your router, not a vulnerability that attackers can use to gain access.

VPNFilter's first attack consists using a man in the middle attack on incoming traffic. It then tries redirecting secure HTTPS encrypted traffic to a source that is unable to accept it, which causes that traffic to fall back to normal, unencrypted HTTP traffic. The software that does this, named ssler by researchers, makes special provisions for sites that have extra measures to prevent this from happening such as Twitter.com or any Google service.

Once traffic is unencrypted VPNFilter is then able to monitor all inbound and outbound traffic that goes through an infected router. Rather than harvest all traffic and redirect to a remote server to be looked at later, it specifically targets traffic that is known to contain sensitive material such as passwords or banking data. Intercepted data can then be sent back to a server controlled by hackers with known ties to the Russian government.

VPNFilter is also able to change incoming traffic to falsify responses from a server. This helps cover the tracks of the malware and allows it to operate longer before you can tell something is going wrong. An example of what VPNFilter is able to do to incoming traffic given to ARS Technica by Craig Williams, a senior technology leader and global outreach manager at Talos says:

But it appears [attackers] have completely evolved past that, and now not only does it allow them to do that, but they can manipulate everything going through the compromised device. They can modify your bank account balance so that it looks normal while at the same time they're siphoning off money and potentially PGP keys and things like that. They can manipulate everything going in and out of the device.

It's difficult or impossible (depending on your skill set and router model) to tell if you are infected. Researchers suggest anyone who uses a router known to be susceptible to VPNFilter assume they **are** infected and take the necessary steps to regain control of their network traffic.

Routers known to be vulnerable

This long list contains the consumer routers known to be susceptible to VPNFilter. If your model appears on this list it is suggested you follow the procedures in the next section of this article. Devices in the list marked as "new" are routers that were only recently found to be vulnerable.

Asus Devices:

- RT-AC66U (new)
- RT-N10 (new)
- RT-N10E (new)
- RT-N10U (new)
- RT-N56U (new)

D-Link Devices:

- DES-1210-08P (new)
- DIR-300 (new)
- DIR-300A (new)
- DSR-250N (new)
- DSR-500N (new)
- DSR-1000 (new)
- DSR-1000N (new)

Huawei Devices:

- HG8245 (new)

Linksys Devices:

- E1200
- E2500
- E3000 (new)
- E3200 (new)
- E4200 (new)
- RV082 (new)
- WRVS4400N

Mikrotik Devices:

- CCR1009 (new)
- CCR1016
- CCR1036
- CCR1072
- CRS109 (new)
- CRS112 (new)
- CRS125 (new)
- RB411 (new)
- RB450 (new)
- RB750 (new)
- RB911 (new)
- RB921 (new)

- RB941 (new)
- RB951 (new)
- RB952 (new)
- RB960 (new)
- RB962 (new)
- RB1100 (new)
- RB1200 (new)
- RB2011 (new)
- RB3011 (new)
- RB Groove (new)
- RB Omnitik (new)
- STX5 (new)

Netgear Devices:

- DG834 (new)
- DGN1000 (new)
- DGN2200
- DGN3500 (new)
- FVS318N (new)
- MBRN3000 (new)
- R6400
- R7000
- R8000
- WNR1000
- WNR2000
- WNR2200 (new)
- WNR4000 (new)
- WNDR3700 (new)
- WNDR4000 (new)
- WNDR4300 (new)
- WNDR4300-TN (new)
- UTM50 (new)

QNAP Devices:

- TS251
- TS439 Pro
- Other QNAP NAS devices running QTS software

TP-Link Devices:

- R600VPN
- TL-WR741ND (new)
- TL-WR841N (new)

Ubiquiti Devices:

- NSM2 (new)
- PBE M5 (new)

ZTE Devices:

- ZXHN H108N (new)

What you need to do

Right now, as soon as you're able, you should reboot your router. To do this simply unplug it from the power supply for 30 seconds then plug it back in. Many models of router flush installed apps when they are power cycled.

The next step is to factory reset your router. You'll find information about how to do this in the manual that came in the box or from the manufacturer's website. This usually involves inserting a pin into a recessed hole to press a microswitch. When you get your router back up and running, you need to ensure it is on the very latest version of its firmware. Again, consult the documentation that came with your router for details on how to update.

Next, perform a quick security audit of how you're using your router.

- **Never** use the default user name and password to administer it. All routers of the same model will use that default name and password and that makes for an easy way to alter settings or install malware.
- **Never** expose any internal devices to the internet without a strong firewall in place. This includes things like FTP servers, NAS servers, Plex Servers or any smart device. If you must expose any connected device outside your internal network you can likely use port filtering and forwarding software. If not, invest in a strong hardware or software firewall.
- **Never** leave remote administration enabled. It may be convenient if you're often away from your network but it's a potential attack point that every hacker knows to look for.
- **Always** stay up to date. This means check for new firmware regularly, and more importantly, be sure to **install it if it is available**.

Finally, if you're unable to update the firmware to prevent VPNFilter from becoming installed (your manufacturer's website will have details) just buy a new one. I know that spending money to replace a perfectly good and working router is a bit extreme, but you will have no idea if your router is infected unless you're a person who doesn't need to read these sort of tips.

We love the new mesh router systems that can be automatically updated whenever new firmware is available, such as Google Wifi, because things like VPNFilter can happen anytime and to anyone. It's worth having a look if you are in the market for a new router.

- Google Wifi review
- Google Home review
- Chromecast Ultra: all you need to know
- Which Chromecast should you buy?