VPNFilter: New Router Malware with Destructive Capabilities

symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware

Symantec Security ResponseSecurity Response Team

UPDATE: September 26, 2018:
This blog has been updated to include new information that was released by Cisco Talos on seven new Stage 3 modules. For further details see below.

UPDATE: June 6, 2018:
This blog has been updated to include new information that was released by Cisco Talos. This includes an expanded list of vulnerable devices and details on a newly discovered stage 3 module known as "ssler" which could permit the attackers to perform man-in-the-middle (MitM) attacks on traffic going through vulnerable routers and allow them to intercept web traffic and insert malicious code into it. For further details see below.

A new threat which targets a range of routers and network-attached storage (NAS) devices is capable of knocking out infected devices by rendering them unusable. The malware, known as VPNFilter, is unlike most other IoT threats because it is capable of maintaining a persistent presence on an infected device, even after a reboot. VPNFilter has a range of capabilities including spying on traffic being routed through the device. Its creators appear to have a particular interest in SCADA industrial control systems, creating a module which specifically intercepts Modbus SCADA communications.

According to new research from Cisco Talos, activity surrounding the malware has stepped up in recent weeks and the attackers appear to be particularly interested in targets in Ukraine. While VPNFilter has spread widely, data from Symantec's honeypots and sensors indicate that unlike other IoT threats such as Mirai, it does not appear to be scanning and indiscriminately attempting to infect every vulnerable device globally.

Q: What devices are known to be affected by VPNFilter?

A: To date, VPNFilter is known to be capable of infecting enterprise and small office/home office routers from Asus, D-Link, Huawei, Linksys, MikroTik, Netgear, TP-Link, Ubiquiti, Upvel, and ZTE, as well as QNAP network-attached storage (NAS) devices. These include:

- Asus RT-AC66U
- Asus RT-N10
- Asus RT-N10E
- Asus RT-N10U
- Asus RT-N56U
- Asus RT-N66U

- D-Link DES-1210-08P
- D-Link DIR-300
- D-Link DIR-300A
- D-Link DSR-250N
- D-Link DSR-500N
- D-Link DSR-1000
- D-Link DSR-1000N

Huawei HG8245

- Linksys E1200
- Linksys E2500
- Linksys E3000
- Linksys E3200
- Linksys E4200
- Linksys RV082

- Linksys WRVS4400N

- MikroTik CCR1009
- MikroTik CCR1016
- MikroTik CCR1036
- MikroTik CCR1072
- MikroTik CRS109
- MikroTik CRS112
- MikroTik CRS125
- MikroTik RB411
- MikroTik RB450
- MikroTik RB750
- MikroTik RB911
- MikroTik RB921
- MikroTik RB941
- MikroTik RB951
- MikroTik RB952
- MikroTik RB960
- MikroTik RB962
- MikroTik RB1100
- MikroTik RB1200
- MikroTik RB2011
- MikroTik RB3011
- MikroTik RB Groove
- MikroTik RB Omnitik
- MikroTik STX5

- Netgear DG834
- Netgear DGN1000
- Netgear DGN2200
- Netgear DGN3500
- Netgear FVS318N
- Netgear MBRN3000
- Netgear R6400
- Netgear R7000
- Netgear R8000
- Netgear WNR1000
- Netgear WNR2000
- Netgear WNR2200
- Netgear WNR4000
- Netgear WNDR3700
- Netgear WNDR4000
- Netgear WNDR4300

- Netgear WNDR4300-TN
- Netgear UTM50

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

- TP-Link R600VPN
- TP-Link TL-WR741ND
- TP-Link TL-WR841N

- Ubiquiti NSM2
- Ubiquiti PBE M5

Upvel Devices -unknown models

ZTE Devices ZXHN H108N

Q: How does VPNFilter infect affected devices?

A: 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.

Q: What does VPNFilter do to an infected device?

A: VPNFilter is a multi-staged piece of malware. Stage 1 is installed first and is used to maintain a persistent presence on the infected device and will contact a command and control (C&C) server to download further modules.

Stage 2 contains the main payload and is capable of file collection, command execution, data exfiltration, and device management. It also has a destructive capability and can effectively “brick” the device if it receives a command from the attackers. It does this by overwriting a section of the device’s firmware and rebooting, rendering it unusable.

There are several known Stage 3 modules, which act as plugins for Stage 2. These include a packet sniffer for spying on traffic that is routed through the device, including theft of website credentials and monitoring of Modbus SCADA protocols. Another Stage 3 module allows Stage 2 to communicate using Tor.

A newly discovered (disclosed on June 6) Stage 3 module known as “ssler” is capable of intercepting all traffic going through the device via port 80, meaning the attackers can snoop on web traffic and also tamper with it to perform man-in-the-middle (MitM) attacks. Among its features is the capability to change HTTPS requests to ordinary HTTP requests, meaning data that is meant to be encrypted is sent insecurely. This can be used to harvest credentials

and other sensitive information from the victim's network. The discovery of this module is significant since it provides the attackers with a means of moving beyond the router and on to the victim's network.

A fourth Stage 3 module known as "dstr" (disclosed on June 6) adds a kill command to any Stage 2 module which lacks this feature. If executed, dstr will remove all traces of VPNFilter before bricking the device.

Details on seven more Stage 3 modules were released on September 26, 2018. These include:

- **"htpx":** Similar to ssler, it redirects and inspects all HTTP traffic transmitted through the infected device to identify and log any Windows executables. This may be used to Trojanize executables as they pass through infected routers, providing attackers with a way of installing malware on computers connected to the same network.
- **"ndbr":** A multi-function SSH tool.
- **"nm":** A network mapping tool which can be used to scan and map the local subnet.
- **"netfilter":** A denial of service utility which may be used to block access to some encrypted applications.
- **"portforwarding":** Module which forwards network traffic to attacker-specified infrastructure.
- **"socks5proxy":** Module to enable establishment of a SOCKS5 proxy on compromised devices.

"tcpvpn": Allows establishment of a Reverse-TCP VPN on compromised devices, enabling remote attacker to access internal networks behind infected devices.

Q: What should I do if I'm concerned my router is infected?
Concerned users are advised to use Symantec's free online tool to help check if their router is impacted by VPNFilter. This also includes instructions on what to do if the router is infected.

Q: What do the attackers intend to do with VPNFilter's destructive capability?

A: This is currently unknown. One possibility is using it for disruptive purposes, by bricking a large number of infected devices. Another possibility is more selective use to cover up evidence of attacks.

Q: Do Symantec/Norton products (Win/Mac/NMS) protect against this threat?

A: Symantec and Norton products detect the threat as Linux.VPNFilter.

Acknowledgement: Symantec wishes to thank Cisco Talos and the Cyber Threat Alliance for sharing information on this threat in advance of publication.

UPDATE: Netgear is advising customers that, in addition to applying the latest firmware updates and changing default passwords, users should ensure that remote management is turned off on their router. Remote management is turned off by default and can only be turned on using the router's advanced settings. To turn it off, they should go to www.routerlogin.net in their browser and log in using their admin credentials. From there, they should click "Advanced" followed by "Remote Management". If the check box for "Turn Remote Management On" is selected, clear it and click "Apply" to save changes.

UPDATE May 24, 2018: The FBI has announced that it has taken immediate action to disrupt the VPNFilter, securing a court order, authorizing it to seize a domain that is part of the malware's C&C infrastructure.

Meanwhile, Linksys is advising customers to change administration passwords periodically and ensure software is regularly updated. If they believe they have been infected, a factory reset of their router is recommended. Full instructions can be found here.

MikroTik has said that it is highly certain that any of its devices infected by VPNFilter had the malware installed through a vulnerability in MikroTik RouterOS software, which was patched by MikroTik in March 2017. Upgrading RouterOS software deletes VPNFilter, any other third-party files and patches the vulnerability.
UPDATE May 25, 2018: QNAP has published a security advisory on VPNFilter. It contains guidance on how to use the company's malware removal tool to remove any infections.

About the Author

Symantec Security Response

Security Response Team

Symantec's Security Response organization develops and deploys new security content to Symantec customers. Our team of global threat analysts operate 24x7 to track developments on the threat landscape and protect Symantec customers.