How to detect VPNFilter malware before it destroys the router

VPNFilter is a destructive malware for routers, IoT devices and even some network storage devices (NAS). How do you detect if your devices are infected with VPNFilter malware? And how can you remove it?

Malware on routers (routers), Internet devices and Internet of Things are increasingly popular. Most of them infect vulnerable devices and very powerful botnets. The router and Internet of Things (IoT) devices are always powered, always online and waiting for instructions. And the botnet takes advantage of that to attack these devices.

But not all malware (malware) is the same.

VPNFilter is a destructive malware for routers, IoT devices and even some network storage devices (NAS). How do you detect if your devices are infected with VPNFilter malware? And how can you remove it? Let's take a closer look at VPNFilter through the following article.

How to detect VPNFilter malware before it destroys the router

1. What is VPNFilter?
2. What can VPNFilter do?
    1. Extract server IP address
    2. Packet sniffing is targeted
3. Where does VPNFilter come from?
4. How do I know if my device is infected with VPNFilter?
5. If you are infected with VPNFilter, what should you do?

What is VPNFilter?

VPNFilter is a sophisticated modular malware variant, primarily targeting network devices from a variety of manufacturers, as well as NAS devices. VPNFilter was originally found on Linksys, MikroTik, NETGEAR and TP-Link network devices, as well as QNAP NAS devices, with about 500,000 infections in 54 countries.

The VPNFilter team, Cisco Talos, recently updated the details related to this malware, showing that network devices from manufacturers such as ASUS, D-Link, Huawei, Ubiquiti, UPVEL and ZTE is currently showing signs of VPNFilter infection. However, at the time of writing, no Cisco network device is affected.

This malware is unlike most malware that focuses on other IoT because it persists after restarting the system, making it more difficult to remove them. Devices that use their default login credentials or with zero-day vulnerabilities (computer software vulnerabilities are not known), in case they are not regularly updated, the firmware is particularly vulnerable. than.

What can VPNFilter do?

VPNFilter is a "multi-platform, multi-platform" platform that can damage and destroy devices. Moreover, it can also become a worrying threat, when collecting user data. VPNFilter works in several stages.

Stage 1 : VPNFilter at stage 1 establishes a landing position on the device, contact the command and control server (C&C) to download additional modules and wait for instructions. Phase 1 also has many contingency plans integrated to position phase 2 C&C, in case of infrastructure changes during deployment. VPNFilter malware in phase 1 can also exist when rebooted, making it a very dangerous threat.

Phase 2 : VPNFilter at stage 2 does not exist after rebooting, but it has a lot of possibilities at this stage. Phase 2 can collect personal data, execute orders and interfere with device management. In addition, there are different versions of stage 2 in practice. Some versions are equipped with a destruction module that overwrites a partition of the device firmware, then reboots to make the device unusable (basically, malware will be disabled Turn on router, IoT or NAS devices.

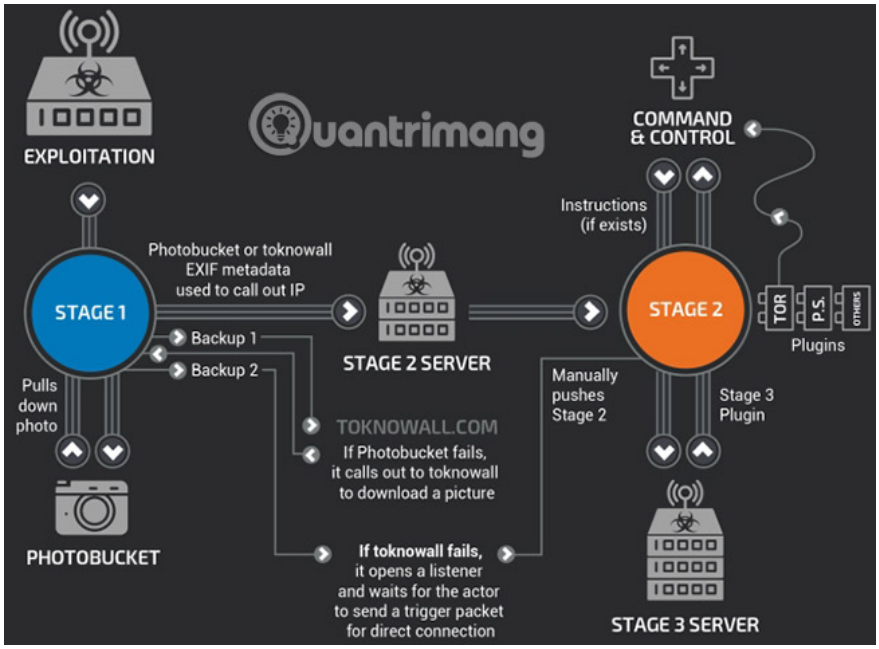
Stage 3 : The VPNFilter module in phase 3 works as the plugin for phase 2, extending the functionality of VPNFilter. A module acts as a packet sniffer, collecting traffic to the device and stealing login information. Another allows phase 2 malware to communicate securely with Tor. Cisco Talos also found a module that infects malicious content into traffic through the device, meaning hackers can exploit other connected devices via a router, IoT or NAS device.

In addition, VPNFilter 'modules allow for theft of site login information and monitoring of Modbus SCADA protocols'.

Extract server IP address

Another interesting feature (but not newly discovered) of VPNFilter malware is the use of online photo sharing services to find the IP address for its C&C server. Talos analysis found that malware pointed to a series of URL Photobucket. Malware downloads the first image in the URL reference library and extracts the hidden IP address in the image metadata.

IP addresses are extracted from 6 integer values ??for latitude and longitude GPS in EXIF ??information. If that fails, phase 1 malware will return to the normal domain (toknowall.com - more information below) to download the image and try to do the same process.



Packet sniffing is targeted

Talos' update report shows some interesting details about packet module sniffing VPNFilter. Instead of interfering with everything, it has a set of strict rules that specifically target the types of traffic. Specifically, traffic from industrial control systems (SCADA), using VPN TP-Link R600, connects to a predefined list of IP addresses (denoting advanced knowledge about networks other and desired traffic), as well as 150 bytes or larger data packets.

Craig William, senior leader in global technology and array management at Talos, told Ars: 'VPNFilter is looking for very specific things. They do not try to collect as much traffic as possible. They just tried to get some very small things like login information and password. We don't have much information about it, other than knowing that it is very specific and extremely sophisticated. We are still trying to find out which object they are using this method with. '

Where does VPNFilter come from?

VPNFilter is said to be the work of a state-sponsored hacker group. The VPNFilter infection was originally discovered in Ukraine, and many sources believe that this is the product of the Fancy Bear attack group, backed by Russia.

However, no country or hacker group has claimed responsibility for the malware. With the detailed and targeted rules of malware for SCADA and other industrial system protocols, this software hypothesis is supported by a country that seems to be most likely.

However, the FBI believes that VPNFilter is the product of Fancy Bear. In May 2018, the FBI confiscated a domain - ToKnowAll.com - supposedly used to install and command VPNFilter malware in phase 2 and phase 3. The capture of this domain is likely Sure, it helped prevent the instantaneous spread of VPNFilter, but didn't solve the problem completely. The Ukrainian Security Agency (SBU) prevented a VPNFilter attack on a

chemical processing plant in July 2018.

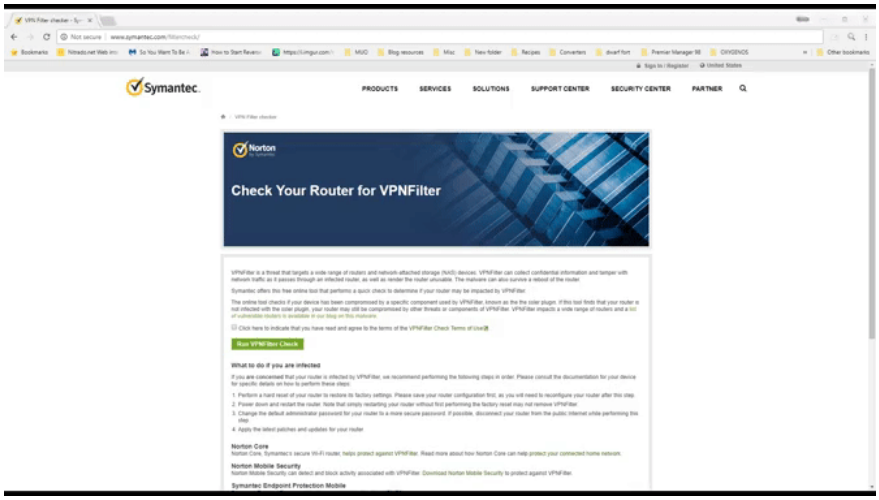
VPNFilter also bears similarities with BlackEnergy malware, an APT trojan used to counter a variety of goals in Ukraine. Once again, although there is no exact evidence, attacks targeted at Ukrainian systems are primarily derived from hacker groups with close ties to Russia.

How do I know if my device is infected with VPNFilter?

Very likely your router is not infected with VPNFilter malware. But it's still better if you're sure your device is safe:

Check your router with the link: **https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware.** If your device is not on the list, everything is fine.

You can visit the Symantec VPNFilter test page: **http://www.symantec.com/filtercheck/.** Check the terms and conditions box, then click the **Run VPNFilter Check** button in the middle. The test will be completed in seconds.



If you are infected with VPNFilter, what should you do?

If Symantec VPNFilter Check confirms that your router is infected with VPNFilter, you need to perform the following actions.

1. Reset your router, then run VPNFilter Check again.
2. Reset your router to the original settings.
3. Download the latest firmware for the router and complete the 'clean' firmware installation, preferably without the router making an online connection during the process.

Furthermore, you need to scan the entire system on each device connected to the VPNFilter-infected router.

You should always change the default login information of the router, as well as any IoT or NAS device (doing this task is not easy on IoT devices), if possible. In addition, although there is evidence that VPNFilter can bypass some firewalls, installing and configuring the firewall properly will help eliminate many other unpleasant

things from your network.

Malware on the router is increasingly popular. Malware and IoT vulnerabilities are everywhere and with the number of online devices increasing, the situation will get worse. Routers are the focus for data in your home. However, it does not receive as much security attention as other devices. Simply put, the router is not as secure as you think.

See more:

1. Steps to remove malware 9o0gle. com
2. How to identify computers infected with viruses with 10 characteristic signs