VPNFilter: the more you know

What is VPNFilter?

VPNFilter is the modular, multi-stage malware that infects Internet connected devices. (Primarily targeting SOHO routers & NAS devices)

*** 9/26/18 Update Description of modules used in VPNFilter attack

https://threatpost.com/vpnfilters-arsenal-expands-with-newly-discovered-modules/137715/

How does VPNFilter Work?

Stage 1: device is infected

For a thorough description:

Cisco Talos article May 23 2018:

https://blog.talosintelligence.com/2018/05/VPNFilter.html

Cisco Talos article June 6 2018:

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

To keep it simplified:

How are devices infected?

This is the unclear part. It is theorized that a vulnerability on the device is exploited and the device is infected.

Quite possibly the devices that are infected are due to using the default username/password combo, have outdated firmware, an existing vulnerability due to a poor configuration or a combination.

What devices could potentially be infected?

LIST UPDATE 6-14-18

ASUS DEVICES:

RT-AC66U (new)

RT-N10 (new)

RT-N10E (new)

RT-N10U (new)

RT-N56U (new)

RT-N66U (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)

UPVEL DEVICES:

Unknown Models* (new)

ZTE DEVICES:

ZXHN H108N (new)

* Malware targeting Upvel as a vendor has been discovered, but we are unable to determine which specific device it is targeting.

Stage 2:

C2 & Tor Communication

To keep it simplified:

Once infected what does it do?

Router creates a working environment for VPNFilter, establishes a connection to Command and Control servers and executes commands it receives. Then the router installs a Tor module so it can connect to onion domains and redirect traffic for further analysis.

Stage 3:

Data exfiltration / manipulation / device bricking

To keep it simplified:

Stage 3 module known as “ssler” is capable of intercepting all traffic going through the device via port 80, meaning the attackers can sniff 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.

Note: To ensure that these rules do not get removed, ssler deletes them and then adds them back approximately every four minutes.

How do I know I am infected?

It is difficult to determine infection without monitoring client/router traffic.

How do I protect against VPNFilter or clean up my router/clients?

Newer routers should be factory reset and the latest firmware should be applied.

Change the default username/password, disabled unneeded services on your router, disable external remote management, and monitor endpoints attached to your network.

Devices older than 3+ years might need to be replaced if the manufacturer hasn't updated the firmware or no longer supports the device.

Endpoints need updated endpoint protection/anti-virus software.

NAS Devices should have firmware updated or if the device is no longer supported to replace the device.

Sources:

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

https://www.fortinet.com/blog/threat-research/defending-against-the-new-vpnfilter-botnet.html

https://www.infosecurity-magazine.com/news/vpnfilter-malware-infected-500k/

https://www.theregister.co.uk/2018/06/07/vpnfilter_is_much_worse_than_everyone_thought/

https://blog.talosintelligence.com/2018/05/VPNFilter.html

https://forums.juniper.net/t5/Threat-Research/VPNFilter-a-nation-state-campaign-for-surveillance-and/ba-p/327038

https://github.com/socprime/VPNFilter-Malware-Detector

https://www.qnap.com/en/news/2018/response-to-claims-of-vpnfilter-malware-infections-security-concerns-were-addressed-in-2017

https://arstechnica.com/information-technology/2018/06/vpnfilter-malware-infecting-50000-devices-is-worse-than-we-thought/

https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware

https://thehackernews.com/2018/05/vpnfilter-botnet-malware.html

https://threatpost.com/vpnfilters-arsenal-expands-with-newly-discovered-modules/137715/