certTonga

Tonga National Computer
Emergency Response
Team

VPNFilter Malware

Dear Constituents,

Cisco's cyber intelligence unit and a few other vendors are warning that at least half a million routers and storage devices in 54 countries have been infected with a sophisticated malware program. Security researchers are calling this VPNFilter Malware. The malware can potentially be used to carry out network based attacks or extract information from network transactions. Additionally, it could also damage the infected appliance.

How the malware spreads

3 Stages of how VPN Filters operates and spread

- Stage 1 is focused on persistence and redundancy and can survive a reboot.
- Stage 2 contains data exfiltration, command execution, file collection, device management and in some versions, the self-destruct module.
- Stage 3 is comprised of modules that perform different tasks. Three modules have currently been identified, though there is a possibility that there are others. The known modules include:
    1. *A packet sniffer for traffic analysis and potential data exfiltration.*
    2. *The monitoring of MODBUS SCADA protocols.*
    3. *Communication with obfuscated addresses via TOR*

The malware spreads by exploiting weak credentials

VPNFilter is likely an advanced, state-sponsored modular malware system that has resulted in the widespread infection of primarily home and small business routers and network attached storage (NAS) devices. Activity from the campaign was initially seen in targeted, specific attacks in Ukraine, but data indicates that devices in over 100 countries are being scanned on ports 23, 80, 2000, and 8080, which are indicative of additional scanning for vulnerable Mikrotik and QNAP NAS devices.

List of affected devices:

Linksys E1200

Linksys E2500

Linksys WRVS4400N

Mikrotik RouterOS for Cloud Core Routers: Versions 1016, 1036, and 1072

Netgear DGN2200

Netgear R6400

Netgear R7000

Netgear R8000

Netgear WNR1000

Netgear WNR2000

QNAP TS251

QNAP TS439 Pro

Other QNAP NAS devices running QTS software

TP-Link R600VPN

(there may be others!)

source: https://www.bleepingcomputer.com/news/security/nation-state-group-hacked-500-000-routers-to-prepare-a-cyber-attack-on-ukraine/

What to do?

- Disable internet facing management interface (via web or other services). Make sure that the management interface can only be accessible from your local network.
- Ensure affected devices (and all devices) are up to date on all software / firmware taking precautions (e.g. backup of configuration) in case the update process goes wrong
- Ensure all your devices are password protected and are not using the default password

Reference

- Fortinet Blog: Defending Against the New VPNFilter Botnet
- Sophos Blog: VPNFilter – is a malware timebomb lurking on your router?
- Symantec Blog: VPNFilter: New Router Malware with Destructive Capabilities
- Palo Alto Networks Blog: Important information on VPNFilter Attacks
- Juniper Blog: VPNFilter: a nation-state campaign for surveillance and destructionMcAfee Blog: VPNFilter Botnet Targets Networking Devices
- *Source: https://www.cyberthreatalliance.org/cta-actions-around-vpnfilter/*

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: report@cert.to
web: www.cert.to

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services.