TLP:WHITE

NCCIC

Alert (TA18-145A)

Cyber Actors Target Home and Office Routers and Networked Devices Worldwide

Original release date: May 25, 2018

Systems Affected

- Small office/home office (SOHO) routers
- Networked devices
- Network-attached storage (NAS) devices

Overview

Cybersecurity researchers have identified that foreign cyber actors have compromised hundreds of thousands of home and office routers and other networked devices worldwide [1] [2]. The actors used VPNFilter malware to target small office/home office (SOHO) routers. VPNFilter malware uses modular functionality to collect intelligence, exploit local area network (LAN) devices, and block actor-configurable network traffic. Specific characteristics of VPNFilter have only been observed in the BlackEnergy malware, specifically BlackEnergy versions 2 and 3.

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) recommend that owners of SOHO routers power cycle (reboot) SOHO routers and networked devices to temporarily disrupt the malware.

DHS and FBI encourage SOHO router owners to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by email at CyWatch@fbi.gov. Each submitted report should include as much informaiton as possible, specifically the date, time, location, type of activity, number of people, the type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Description

The size and scope of this infrastructure impacted by VPNFilter malware is significant. The persistent VPNFilter malware linked to this infrastructure targets a variety of SOHO routers and network-attached storage devices. The initial exploit vector for this malware is currently unknown.

The malware uses a modular functionality on SOHO routers to collect intelligence, exploit LAN devices, and block actor-configurable network traffic. The malware can render a device inoperable, and has destructive functionality across routers, network-attached storage devices, and central processing unit (CPU) architectures running embedded Linux. The command and control mechanism implemented by the malware uses a combination of secure

TLP:WHITE

sockets layer (SSL) with client-side certificates for authentication and TOR protocols, complicating network traffic detection and analysis.

Impact

Negative consequences of VPNFilter malware infection include:

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Solution

DHS and FBI recommend that all SOHO router owners power cycle (reboot) their devices to temporarily disrupt the malware.

Network device management interfaces—such as Telnet, SSH, Winbox, and HTTP—should be turned off for wide-area network (WAN) interfaces, and, when enabled, secured with strong passwords and encryption. Network devices should be upgraded to the latest available versions of firmware, which often contain patches for vulnerabilities.

Rebooting affected devices will cause non-persistent portions of the malware to be removed from the system. Network defenders should ensure that first-stage malware is removed from the devices, and appropriate network-level blocking is in place prior to rebooting affected devices. This will ensure that second stage malware is not downloaded again after reboot.

While the paths at each stage of the malware can vary across device platforms, processes running with the name "vpnfilter" are almost certainly instances of the second stage malware. Terminating these processes and removing associated processes and persistent files that execute the second stage malware would likely remove this malware from targeted devices.

References

- [1] New VPNFilter malware targets at least 500K networking devices worldwide
- [2] Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage

Revisions

- May 25, 2018: Initial Version