May 31, 2018

Is your home router hacked?

CYBERSECURITY
BY STEPHEN BISH

At Schneider Downs, we understand that cybersecurity threats to our clients will sometimes extend to devices and systems outside their IT purview. As the acceptance and utilization of remote employees increases, so does the risk associated with remote offices. This article outlines the dangers posed by the presence of VPNFilter, the most recent and widespread threat to these environments and our recommendations on how to defend against it.

What is VPNFilter?

VPNFilter is an advanced, persistent, modular malware system that has infected over 500,000 networking devices in more than 50 countries around the world. Cisco's TALOS Intelligence Group had been researching the malware for months with the assistance of public- and private-sector threat intelligence partners and law enforcement, but after observing a dramatic spike of infection rates, they decided to publish their unfinished work so that affected parties and the cybersecurity community can better defend themselves.

What Devices Are Being Targeted?

Unpatched personal networking devices like small office/home office (SOHO) routers are rarely updated and, hence, often susceptible to well-known, public vulnerabilities. If we think of these devices as one large network of internet-facing systems with minimal security, it's easy to see how an advanced malware like VPNFilter can leverage pre-existing vulnerabilities and propagation capabilities to gain a large footprint. So far, the following devices are known to be affected, but other personal networking devices are likely affected as well:

LINKSYS DEVICES:	MIKROTIK ROUTEROS VERSIONS FOR CLOUD CORE ROUTERS:	NETGEAR DEVICES:	QNAP DEVICES:
E1200	1016	DGN2200	TS251

E2500	1036	R6400/R7000/R8000	TS439 Pro
WRVS4400N	1072	WNR1000	-
-	-	WNR2000	-

What Is The Impact?

Data Collection – Networking devices provide a natural capability to collect data. Components of the VPNFilter malware allow for theft of website credentials and general monitoring of network traffic.

Cyber Obfuscation – Threat actors can leverage infected devices to cover their digital footprint and true point of origin. Devices infected with VPNFilter could easily be used as hop points before connecting to the intended victim device.

Botnet – Large-scale threat actors can leverage infected devices to remotely serve multiple operational needs, including distributed denial of service (DDoS) attacks. Devices infected with VPNFilter have been observed conducting TCP scans on ports 23, 80, 2000 and 8080, which were likely to identify additional devices to infect. These scans targeted devices in over 100 countries.

Self-Destruction – VPNFilter has a destructive capability that can render an infected device unusable. This can be triggered on individual victim machines or multiple infected machines at once, which has the potential of cutting off internet access for hundreds of thousands of victims worldwide.

Our Recommendations:

Owners of personal networking devices should reset them to factory defaults to remove the persistence module of the malware, then reboot the device to flush out any non-persistent modules and lastly, ensure your device is up to date with the latest patch versions, as VPNFilter initially exploits devices by utilizing well-known vulnerabilities that have available patches.

Due to the relatively low cost of personal networking devices and the direct relationship between the age of a device and its known vulnerabilities, it’s likely that upgrading to a newer networking device with additional security features could be the best course of action. This could also be the preferred solution for users unable to reset their devices to factory defaults.

Organizations utilizing remote employees should ensure that all confidential resources can only be accessed through a secured virtual private network (VPN). Schneider Downs also highly recommends that two-factor authentication be enforced on all VPNs. In our experience providing penetration testing services, we frequently identify single-factor authentication and are able to bypass it through Password Spraying, Phishing and other techniques.

References:

Cisco's TALOS Intelligence Group:
https://blog.talosintelligence.com/2018/05/VPNFilter.html

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.