Security warning: Hackers are using this new malware to target firewall appliances

www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/security-warning-hackers-are-using-this-new-malware-to-target-firewall-appliances/

Danny Palmer

- Home
- Innovation
- Security

NCSC, CISA, NSA and FBI issue warning over malware linked to Sandworm hacking group, which targets firewalls and provides remote access to networks.

Written by Danny Palmer, Senior Reporter
on February 23, 2022

Cybersecurity: Let's get tactical

Hackers linked to the Russian military are exploiting security vulnerabilities in firewalls to compromise networks and infect them with malware, allowing them to gain access remotely.

An alert by the UK National Cyber Security Centre (NCSC), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) has detailed the new malware, Cyclops Blink, attributing it to Sandworm, an offensive hacking operation they've previously linked to Russia's GRU.

Analysis by the NCSC describes Cyclops Blink as a "a highly sophisticated piece of malware" that has been "professionally developed".

SEE: Cybersecurity: Let's get tactical (ZDNet special report)

Cyclops Blink appears to be a replacement for VPNFilter, malware that was used by state-linked Russian hacking groups in widespread attacks used to compromise network devices, predominantly routers, in order to access networks.

According to the NCSC, CISA, FBI and NSA, Cyclops Blink has been active since at least June 2019, and like VPNFilter before it, the targeting is described as "indiscriminate and widespread" with the ability to gain persistent remote access to networks.

It can also upload and download files from infected machines and it is modular, allowing new functionality to be added to malware that is already running.

The cyberattacks are primarily focused on WatchGuard firewall devices, but the agencies warned that Sandworm is capable of repurposing the malware to spread it via other architectures and firmware.

Cyclops Blink persists on reboot and throughout the legitimate firmware update process. It targets WatchGuard devices that were reconfigured from the manufacturer default settings to open remote management interfaces to external access.

An infection doesn't mean the organisation is the primary target, but it's possible that infected machines could be used to conduct additional attacks.

The NCSC urges affected organisations to take steps to remove the malware, which have been detailed by WatchGuard.

"Working closely with the FBI, CISA, DOJ, and UK NCSC., WatchGuard has investigated and developed a remediation for Cyclops Blink, a sophisticated state-sponsored botnet, that may have affected a limited number of WatchGuard firewall appliances," said a WatchGuard statement.

"WatchGuard customers and partners can eliminate the potential threat posed by malicious activity from the botnet by immediately enacting WatchGuard's 4-Step Cyclops Blink Diagnosis and Remediation Plan," it added.

The NCSC warned that any passwords present on a device infected by Cyclops Blink should be assumed to be compromised and should be changed.

Other advice about protecting networks from cyberattacks includes avoiding the exposure of management interfaces of network devices to the internet, keeping devices up to date with the latest security patches, and using multi-factor authentication.

The NCSC notes that the advisory is not directly linked to the current situation in Ukraine.

MORE ON CYBERSECURITY