Cyclops Blink malware sets up shop in ASUS routers

By Jessica Lyons

Published: 2022-03-18 · Archived: 2026-04-02 11:38:22 UTC

Cyclops Blink malware has infected ASUS routers in what Trend Micro says looks like an attempt to turn these compromised devices into command-and-control servers for future attacks.

ASUS says it's working on a remediation for Cyclops Blink and will post software updates if necessary. The hardware maker recommends users reset their gateways to factory settings to flush away any configurations added by an intruder, change the login password, make sure remote management access from the WAN is disabled, and ensure the latest firmware is installed to be safe.

Cyclops Blink has ties to Kremlin-backed Sandworm, the criminal gang behind the nasty VPNFilter malware that in 2018 targeted routers and storage devices. The crew also carried out several high-profile attacks including the 2015 and 2016 cyber-assaults on Ukraine's electrical grid, NotPetya in 2017, and the French presidential campaign email leak that same year.

A Trend Micro warning about the router hijackings follows a joint advisory last month from the FBI, CISA, the US Department of Justice, and the UK National Cyber Security Centre about Cyclops Blink, which the agencies said looked to be Sandworm's replacement for VPNFilter. At the time, the botnet had its sights set on WatchGuard firewall appliances.

"Our data also shows that although Cyclops Blink is a state-sponsored botnet, its C&C servers and bots affect WatchGuard Firebox and Asus devices that do not belong to critical organizations, or those that have an evident value on economic, political, or military espionage," Trend Micro said. "Hence, we believe that it is possible that the Cyclops Blink botnet's main purpose is to build an infrastructure for further attacks on high-value targets."

And while Cyclops Blink has infected routers from these two hardware providers, "we have evidence that the routers of at least one vendor other than Asus and WatchGuard are connecting to Cyclops Blink C&Cs as well, but so far we have been unable to collect malware samples for this router brand," the security shop said.

- Ukraine hit by DDoS attacks, Russia deploys malware
- France's cyber-agency says Centreon IT management software sabotaged by Russian Sandworm
- Ukraine invasion: This may be the quiet before the cyber-storm, IT staff warned
- Where are the (serious) Russian cyberattacks?

It's not clear exactly right now how the malware gets onto a device, though it probably involves exploiting a default admin password to gain access via an enabled remote management service. According to Trend Micro's Cyclops Blink technical analysis, once the modular malware, written in C, has been injected into the gateway and is running, it sets itself up and renames its process to "[ktest]" presumably to appear as a Linux kernel thread.

Next, it waits for 37 seconds and decides on the hard-coded command-and-control (C2) server to talk to along with the rate at which it communicates with the box. Then it begins communicating with its C2 server using an OpenSSL-encrypted channel to join the Cyclops Blink botnet. Among the commands it can receive, the compromised router can be given more malware to run, allowing the botnet's controllers to do whatever they like on the hijacked gateways. ®
