Important Detection and Remediation Actions for Cyclops Blink State-Sponsored Botnet | WatchGuard Technologies

Published: 2022-02-23 · Archived: 2026-04-05 18:48:08 UTC

Working closely with the FBI, CISA, DOJ, and UK NCSC[1], 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. 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.

Scope of Potential Impact:

Based on our own investigation, an investigation conducted jointly with Mandiant, and information provided by the FBI, WatchGuard has concluded the following:

- Based on current estimates, Cyclops Blink may have affected approximately 1% of active WatchGuard firewall appliances; no other WatchGuard products are affected.
- Firewall appliances are not at risk if they were never configured to allow unrestricted management access from the internet. Restricted management access is the default setting for all WatchGuard's physical firewall appliances.
- There is no evidence of data exfiltration from WatchGuard or its customers.
- WatchGuard's own network has not been affected or breached.

WatchGuard's firewall appliances are primarily used by business customers. As such, we have no reason to believe that Cyclops Blink's activities affecting WatchGuard appliances impacted individual consumers.

Detecting, Remediating, and Preventing Cyclops Blink Infection:

In response to this sophisticated, state-sponsored botnet, WatchGuard has developed and released a set of simple and easy-to-use Cyclops Blink detection tools, as well as a 4-Step process to help customers diagnose, remediate if necessary, and prevent future infection. WatchGuard, supported by the FBI, CISA, NSA[2], and the UK NCSC, strongly recommends that all customers promptly take the actions outlined in the 4-Step Cyclops Blink Diagnosis and Remediation Plan. Please note that the remediation steps are only necessary if you have an infected appliance; however, the future protection steps are applicable to all customers.

The recommended 4-Step Cyclops Blink Diagnosis and Remediation Plan includes information to help customers select the detection tool most appropriate for their individual needs. It also enables customers to navigate directly to the most appropriate detection tool and remediation instructions in the event they detect an infection, as well as to the latest Fireware downloads which contain critical fixes and new mandatory security features for enhanced firmware protection.

Visit detection.watchguard.com to review and enact the 4-Step Cyclops Blink Diagnosis and Remediation Plan now.

Additional Resources

The team has been working proactively with government authorities, and leading forensic experts, including Mandiant, the FBI, CISA, DOJ, and UK NCSC, to investigate and respond to the attack. We are sharing information across several communications channels in the best interests of our customers, partners, and the greater security community. Additional resources are available here:

- WatchGuard's 4-Step Cyclops Blink Diagnosis and Remediation Plan
- Detailed Instructions for Enacting the 4-Step Cyclops Blink Diagnosis and Remediation Plan
- Cyclops Blink Frequently Asked Questions (FAQ)
- Joint Government Advisory Issued by the FBI, CISA, NSA, and the UK NCSC
- Security Best Practices Provided By FBI, CISA, NSA, and UK NCSC (see Further Guidance section)

As always, WatchGuard Support is available 24/7 to support customers and partners as they implement these fixes.

[1] Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, Department of Justice, and UK National Cyber Security Centre.
[2] National Security Agency
