CyclopsBlink (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:32:14 UTC

CyclopsBlink

According to CISA, Cyclops Blink appears to be a replacement framework for the VPNFilter malware exposed in 2018, and which exploited network devices, primarily small office/home office (SOHO) routers and network attached storage (NAS) devices. Cyclops Blink has been deployed since at least June 2019, fourteen months after VPNFilter was disrupted. In common with VPNFilter, Cyclops Blink deployment also appears indiscriminate and widespread. The actor has so far primarily deployed Cyclops Blink to WatchGuard and ASUS devices, but it is likely that Sandworm would be capable of compiling the malware for other architectures and firmware.

References

2022-04-15 · splunk ·
STRT-TA03 CPE - Destructive Software
AcidRain CyclopsBlink

2022-04-11 · Bleeping Computer · Sergiu Gatlan
CISA warns orgs of WatchGuard bug exploited by Russian state hackers
CyclopsBlink

2022-04-07 · InQuest · Nick Chalard, Will MacArthur
Ukraine CyberWar Overview
CyclopsBlink Cobalt Strike GraphSteel GrimPlant HermeticWiper HermeticWizard MicroBackdoor PartyTicket Saint Bot Scieron WhisperGate

2022-04-06 · Bleeping Computer · Sergiu Gatlan
US disrupts Russian Cyclops Blink botnet before being used in attacks
CyclopsBlink

2022-04-06 · US Department of Justice · Department of Justice
Attorney General Merrick B. Garland Announces Enforcement Actions to Disrupt and Prosecute Russian Criminal Activity (video)
CyclopsBlink

2022-04-06 · US Department of Justice · Department of Justice
EDCA Search Warrant Package (CyclopsBlink)
CyclopsBlink

2022-04-06 · US Department of Justice · Department of Justice
Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)
CyclopsBlink

2022-03-21 · Github (trendmicro) · Trend Micro Research
Python script to check a Cyclops Blink C&C
CyclopsBlink

2022-03-18 · The Register · Jessica Lyons Hardcastle
Cyclops Blink malware sets up shop in ASUS routers
CyclopsBlink

2022-03-17 · Trendmicro · Feike Hacquebord, Fernando Mercês, Stephen Hilt
Cyclops Blink Sets Sights on Asus Routers
CyclopsBlink

2022-03-17 · Trendmicro · Feike Hacquebord, Fernando Mercês, Stephen Hilt
Cyclops Blink Sets Sights on Asus Routers (Appendix)
CyclopsBlink

2022-03-17 · Bleeping Computer · Bill Toulas
ASUS warns of Cyclops Blink malware attacks targeting routers
CyclopsBlink

2022-02-23 · CISA · CISA
Alert (AA22-054A) New Sandworm Malware Cyclops Blink Replaces VPNFilter
CyclopsBlink VPNFilter

2022-02-23 · The Shadowserver Foundation · Shadowserver Foundation
Shadowserver Special Reports – Cyclops Blink
CyclopsBlink

2017-05-31 · MITRE · MITRE ATT&CK
Sandworm Team
CyclopsBlink Exaramel BlackEnergy EternalPetya Exaramel GreyEnergy KillDisk MimiKatz Olympic Destroyer Sandworm

Yara Rules

▶ [TLP:WHITE] elf_cyclops_blink_w0 (20220316 | Detects notable strings identified within the Cyclops Blink executable)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/elf.cyclops_blink