Cyclops Blink - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:10:58 UTC

Tool: Cyclops Blink

Names	Cyclops Blink CyclopsBlink
Category	Malware
Type	Reconnaissance, Backdoor, Downloader, Info stealer, Exfiltration, Botnet
Description	(CISA) The NCSC, CISA, the FBI, and NSA, along with industry partners, have now identified a large-scale modular malware framework (T1129) which is targeting network devices. The new malware is referred to here as Cyclops Blink and 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 devices, but it is likely that Sandworm would be capable of compiling the malware for other architectures and firmware.
Information	<https://www.cisa.gov/uscert/ncas/alerts/aa22-054a> <https://www.watchguard.com/wgrd-news/blog/important-detection-and-remediation-actions-cyclops-blink-state-sponsored-botnet> <http://blog.talosintelligence.com/2022/02/threat-advisory-cyclops-blink.html> <https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0687/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.cyclops_blink>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Cyclops Blink

Changed	Name	Country	Observed

APT groups

	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c097a8f7-313e-4d79-94b1-1f09d3013be7