Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:07:43 UTC

Tool: VPNFilter

Names	VPNFilter
Category	Malware
Type	Backdoor, Botnet, Worm
Description	(Talos) For several months, Talos has been working with public- and private-sector threat intelligence partners and law e in researching an advanced, likely state-sponsored or state-affiliated actor's widespread use of a sophisticated modular n system we call 'VPNFilter.' We have not completed our research, but recent events have convinced us that the correct wa to now share our findings so that affected parties can take the appropriate action to defend themselves.
Information	<https://blog.talosintelligence.com/2018/05/VPNFilter.html> <https://blog.talosintelligence.com/2018/06/vpnfilter-update.html> <https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html> <https://securelist.com/vpnfilter-exif-to-c2-mechanism-analysed/85721/> <https://blog.trendmicro.com/trendlabs-security-intelligence/vpnfilter-affected-devices-still-riddled-with-19-vulnerabili <https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-VPN-Filter-analysis-v2.pdf> <https://www.dropbox.com/s/9lkeenhveb3xbkq/Whitepaper%20VPNFilter%20IoT%20botnet%20seized%20by%20the' dl=0>
MITRE ATT&CK	<https://attack.mitre.org/software/S1010>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.vpnfilter>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:vpnfilter>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool VPNFilter

Changed	Name	Country	Observed	
APT groups				
	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

2 groups listed (2 APT, 0 other, 0 unknown)