VPNFilter, Software S1010 | MITRE ATT&CK®

Archived: 2026-04-05 18:39:21 UTC

VPNFilter is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and destructive cyber attack operations. VPNFilter modules such as its packet sniffer ('ps') can collect traffic that passes through an infected device, allowing the theft of website credentials and monitoring of Modbus SCADA protocols. [1] [2] VPNFilter was assessed to be replaced by Sandworm Team with Cyclops Blink starting in 2019. [3]

ⓘ

Platforms: Network Devices, Linux

Last Modified: 15 April 2025

Techniques Used

Domain	ID		Name	Use
Enterprise	T1561	.001	Disk Wipe: Disk Content Wipe	VPNFilter has the capability to wipe a portion of an infected device's firmware.[4]
ICS	T0830		Adversary-in-the-Middle	The VPNFilter's ssler module configures the device's iptables to redirect all traffic destined for port 80 to its local service listening on port 8888. Any outgoing web requests on port 80 are now intercepted by ssler and can be inspected by the ps module and manipulated before being sent to the legitimate HTTP service. [1] [2]

Domain	ID	Name	Use
ICS	T0842	Network Sniffing	The VPNFilter packet sniffer looks for basic authentication as well as monitors ICS traffic, and is specific to the TP-LINK R600-VPN. The malware uses a raw socket to look for connections to a pre-specified IP address, only looking at TCP packets that are 150 bytes or larger. Packets that are not on port 502, are scanned for BasicAuth, and that information is logged. This may have allowed credential harvesting from communications between devices accessing a modbus-enabled HMI. [1] [2]

Groups That Use This Software

References

1. William Largent 2018, June 06 VPNFilter Update - VPNFilter exploits endpoints, targets new devices Retrieved. 2019/03/28
2. Carl Hurd 2019, March 26 VPNFilter Deep Dive Retrieved. 2019/03/28
3. NCSC, CISA, FBI, NSA. (2022, February 23). New Sandworm malware Cyclops Blink replaces VPNFilter. Retrieved March 3, 2022.
4. Tung, Liam. (2018, May 29). FBI to all router users: Reboot now to neuter Russia's VPNFilter malware. Retrieved March 7, 2024.
