Tunnel - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:53:18 UTC

Tool: X-Tunnel

Names	X-Tunnel XTunnel Shunnael Trojan.Shunnael XAPS
Category	Malware
Type	Tunneling
Description	X-Tunnel is a network proxy tool that implements a custom network protocol encapsulated in the TLS protocol. win.xtunnel_net is a rewrite of win.xtunnel using the .NET framework that surfaced late 2017.
Information	<https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/> <https://www.root9b.com/sites/default/files/whitepapers/R9b_FSOFACY_0.pdf> <https://www.root9b.com/sites/default/files/whitepapers/root9b_follow_up_report_apt28.pdf> <https://www.invincea.com/2016/07/tunnel-of-gov-dnc-hack-and-the-russian-xtunnel/> <http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf> <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> <http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf> <https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28>
MITRE ATT&CK	<https://attack.mitre.org/software/S0117/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.xtunnel> <https://malpedia.caad.fkie.fraunhofer.de/details/win.xtunnel_net>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool X-Tunnel

Changed	Name	Country	Observed

APT groups

	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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

↑
