Agent - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:27:25 UTC

Tool: X-Agent

Names	X-Agent Xagent Popr-d30 SPLM CHOPSTICK fysbis Backdoor.SofacyX webhp
Category	Malware
Type	Backdoor, Keylogger, Info stealer, Tunneling
Description	CHOPSTICK is a malware family of modular backdoors used by APT28. It has been used since at least 2012 and is usually dropped on victims as second-stage malware, though it has been used as first-stage malware in several cases. It has both Windows and Linux variants. It is tracked separately from the X-Agent for Android.
Information	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> <http://blog.crysys.hu/2017/01/technical-details-on-the-fancy-bear-android-malware-poprd30-apk/> <http://blog.crysys.hu/2017/03/update-on-the-fancy-bear-android-malware-poprd30-apk/> <https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html> <https://download.bitdefender.com/resources/files/News/CaseStudies/study/143/Bitdefender-Whitepaper-APT-Mac-A4-en-EN-web.pdf> <http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf> <https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/> <https://www.thecssc.com/wp-content/uploads/2018/10/4OctoberIOC-APT28-malware-advisory.pdf> <http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf> <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> <http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0023/> <https://attack.mitre.org/software/S0410/>

	<https://attack.mitre.org/software/S0161/> <https://attack.mitre.org/software/S0314/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.popr-d30> <https://malpedia.caad.fkie.fraunhofer.de/details/elf.xagent> <https://malpedia.caad.fkie.fraunhofer.de/details/osx.xagent> <https://malpedia.caad.fkie.fraunhofer.de/details/win.xagent>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:X-Agent>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool X-Agent

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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

↑
