Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:24:15 UTC

Tool: Zebrocy

Names	Zebrocy Zekapab
Category	Malware
Type	Backdoor, Info stealer, Exfiltration, Tunneling
Description	Zebrocy is a Trojan that has been used by APT28 since at least November 2015. The malware comes in several programming language variants, including C++, Delphi, AutoIt, C#, and VB.NET.
Information	<https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/> <https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware> <https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/> <https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/> <https://www.welivesecurity.com/2018/11/20/sednit-whats-going-zebrocy/> <https://securelist.com/greyenergys-overlap-with-zebrocy/89506/> <https://www.vkremez.com/2018/12/lets-learn-dissecting-apt28sofacy.html> <https://www.vkremez.com/2018/12/lets-learn-reviewing-sofacys-zebrocy-c.html> <https://securelist.com/a-zebrocy-go-downloader/89419/> <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303b> <https://labs.sentinelone.com/a-deep-dive-into-zebrocys-dropper-docs/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0251/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy> <https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy_au3>

Last change to this tool card: 21 April 2021

Download this tool card in JSON format

All groups using tool Zebrocy

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1be50485-7c9f-45dc-96b5-1cd8d2977a0e