

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:02:56 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool CaddyWiper



Tool: CaddyWiper

Names	CaddyWiper KillDisk.NCX
Category	Malware
Type	Wiper
Description	<p>(ESET) ESET researchers have uncovered yet another destructive data wiper that was used in attacks against organizations in Ukraine.</p> <p>Dubbed CaddyWiper by ESET analysts, the malware was first detected at 11.38 a.m. local time (9.38 a.m. UTC) on Monday. The wiper, which destroys user data and partition information from attached drives, was spotted on several dozen systems in a limited number of organizations. It is detected by ESET products as Win32/KillDisk.NCX.</p> <p>CaddyWiper bears no major code similarities to either HermeticWiper or IsaacWiper, the other two new data wipers that have struck organizations in Ukraine since February 23rd.</p> <p>Much like with HermeticWiper, however, there's evidence to suggest that the bad actors behind CaddyWiper infiltrated the target's network before unleashing the wiper.</p>
Information	<p><https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/></p> <p><https://blog.talosintelligence.com/2022/03/threat-advisory-caddywiper.html></p> <p><https://blog.malwarebytes.com/threat-intelligence/2022/03/double-header-isaacwiper-and-caddywiper/></p> <p><https://blog.morphisec.com/caddywiper-analysis-new-malware-attacking-ukraine></p> <p><https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/></p> <p><https://therecord.media/a-deeper-look-at-the-malware-being-used-on-ukrainian-targets/></p> <p><https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works></p>
MITRE ATT&CK	< https://attack.mitre.org/software/S0693/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.caddywiper >

Last change to this tool card: 30 December 2022

Download this tool card in [JSON](#) format

All groups using tool CaddyWiper

Changed	Name	Country	Observed	
APT groups				
	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ed300463-d915-45b0-b79f-0a31acfe6bb0>