Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:28:31 UTC

Tool: WINELOADER

Names	WINELOADER
Category	Malware
Type	Backdoor
Description	(Mandiant) WINELOADER is likely a variant of the non-public historic BURNTBATTER and MUSKYBEAT code families which Mandiant uniquely associates with APT29. It shares a similar design and pattern, specifically around the invocation of the malware and the anti-analysis techniques used. However, the code family itself is considerably more customized than the previous variants, as it no longer uses publicly available loaders like DONUT or DAVESHELL and implements a unique C2 mechanism.
Information	<https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties> <https://www.zscaler.com/blogs/security-research/european-diplomats-targeted-spikedwine-wineloader>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.wineloader>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool WINELOADER

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c4851564-852e-49a5-b733-a8a4013dd06b