Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:39:08 UTC

Tool: HIDEDRV

Names	HIDEDRV
Category	Malware
Type	Rootkit, Loader
Description	(ESET) The rootkit is configured to hide Downdelph and itself from the user, and also to inject Downdelph into explorer.exe. We are now going to describe how those two operations are implemented.
Information	<https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf> <https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html> <http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0135/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hidedrv>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool HIDEDRV

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=bc3d715a-2e5c-42ae-8450-f01e7f729af1