Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:34:26 UTC

Tool: CORESHELL

Names	CORESHELL SOURFACE Sofacy
Category	Malware
Type	Downloader
Description	CORESHELL is a downloader used by APT28. The older versions of this malware are known as SOURFACE and newer versions as CORESHELL.
Information	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> <https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html> <http://www.malware-reversing.com/2012/12/3-disclosure-of-another-0day-malware.html> <http://malware.prevenity.com/2014/08/malware-info.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0137/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.coreshell>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:coreshell>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool CORESHELL

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=d4ba1992-de1d-4c94-941d-454e3f3fd249