Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:36:44 UTC

Tool: Sedreco

Names	Sedreco AZZY EVILTOSS ADVSTORESHELL NETUI
Category	Malware
Type	Backdoor, Info stealer, Loader
Description	(ESET) Sedreco serves as a spying backdoor; its functionalities can be extended with dynamically loaded plugins. It is made up of two distinct components: a dropper and the persistent payload installed by this dropper. We have not seen this component since April 2016.
Information	<https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/> <http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf> <http://www.malware-reversing.com/2012/12/3-disclosure-of-another-0day-malware_15.html> <https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/> <https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0045/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sedreco>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Sedreco

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=629e994e-7ff1-4a18-9f31-7ad8400139ca