Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:21:23 UTC

Tool: SkinnyBoy

Names	SkinnyBoy
Category	Malware
Type	Backdoor, Info stealer
Description	(Cluster25) The vector of the infection is a spear phishing email delivering a Word Office document with a significant name related to an International Conference. Both the vector and its naming are consistent with APT28 / FancyBear TTPs.As expected, the document triggers a MACRO function able to extract a Microsoft Dynamic Link Library (DLL) which then acts as downloader of a SkinnyBoy dropper (tdp1.exe) from a first dropurl.
Information	<https://cluster25.io/wp-content/uploads/2021/05/2021-05_FancyBear.pdf> <https://cybergeeks.tech/skinnyboy-apt28/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.skinnyboy>

Last change to this tool card: 28 December 2021

Download this tool card in JSON format

All groups using tool SkinnyBoy

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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