Threat Group Cards: A Threat Actor Encyclopedia

Tool: STEELHOOK

Names	STEELHOOK
Category	Malware
Type	Info stealer, Credential stealer
Description	(BleepingComputer) The Ukrainian CERT says APT28 also uses a set of PowerShell scripts named 'STEELHOOK' to steal data from Chrome-based web browsers, likely to extract sensitive information like passwords, authentication cookies, and browsing history.
Information	<https://www.bleepingcomputer.com/news/security/russian-military-hackers-target-ukraine-with-new-masepie-malware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.steelhook>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool STEELHOOK

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

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