Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:23:16 UTC

Tool: MischiefTut

Names	MischiefTut
Category	Malware
Type	Backdoor, Reconnaissance, Info stealer
Description	(Microsoft) MischiefTut is a custom backdoor implemented in PowerShell with a set of basic capabilities. MischiefTut can run reconnaissance commands, write outputs to a text file and, ostensibly, send outputs back to adversary-controlled infrastructure. MischiefTut can also be used to download additional tools on a compromised system.
Information	<https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/>

Last change to this tool card: 06 March 2024

Download this tool card in JSON format

All groups using tool MischiefTut

Changed	Name	Country	Observed	
APT groups				
	Magic Hound, APT 35, Cobalt Illusion, Charming Kitten		2012-Jun 2025	

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