Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:18:32 UTC

Tool: RCLONE

Names	RCLONE Rclone
Category	Tools
Type	Downloader, Exfiltration
Description	Rclone is a command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA. Rclone has been used in a number of ransomware campaigns, including those associated with the Conti and DarkSide Ransomware-as-a-Service operations.
Information	<https://rclone.org> <https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html> <https://redcanary.com/blog/rclone-mega-extortion/> <https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/> <https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/> <https://unit42.paloaltonetworks.com/darkside-ransomware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1040/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool RCLONE

Changed	Name	Country	Observed	
APT groups				
	UNC2447	[Unknown]	2020	

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