Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:09:05 UTC

Tool: PINEGROVE

Names	PINEGROVE
Category	Malware
Type	Exfiltration
Description	(Mandiant) During the intrusion, Mandiant observed APT41 leveraging PINEGROVE for their data exfiltration. PINEGROVE is a command-line uploader written in Go with functionality to collect and upload a file to OneDrive via the OneDrive API. PINEGROVE expects an authentication JSON file including relevant OneDrive credentials and the target file to upload.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.pinegrove>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool PINEGROVE

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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