Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:56:06 UTC

Tool: Graphite

Names	Graphite
Category	Malware
Type	Backdoor
Description	(Cluster25) Once obtained a new OAuth2 token, the Graphite malware will query the Microsoft GraphAPIs for new commands by enumerating the child files in the check OneDrive subdirectory. If a new file is found, the content is downloaded and decrypted through an AES-256-CBCdecryption algorithm. The monitoring of task executions and the uploading of their results is managed through a dedicated thread. Finally, the malware allows remote command execution by allocating a new region of memory and executing the received shellcode by calling a new dedicated thread.
Information	<https://blog.cluster25.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint-graphite/> <https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/prime-ministers-office-compromised.html> <https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/> <https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.graphite>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool Graphite

Changed	Name	Country	Observed
APT groups			

	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=54731956-6a9c-4fac-8622-2623eb886502