Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:36:31 UTC

Tool: GraphSteel

Names	GraphSteel Elephant Client
Category	Malware
Type	Reconnaissance, Backdoor, Credential stealer
Description	(SOC Investigation) GraphSteel features: • Gather hostname, username, and IP address information • Execute commands • Steal account credentials • Use WebSocket and GraphQL to communicate with C2 using AES and base64 encryption
Information	<https://www.socinvestigation.com/ukraines-cert-warns-russian-threat-actors-for-fake-av-updates/> <https://blog.malwarebytes.com/threat-intelligence/2022/04/new-uac-0056-activity-theres-a-go-elephant-in-the-room/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.graphsteel>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool GraphSteel

Changed	Name	Country	Observed	
APT groups				
	SaintBear, Lorec53		2021-Oct 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a332e2dd-65f4-46e9-8138-de9ae3ed7e50