Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:25:08 UTC

Tool: GraphicalNeutrino

Names	GraphicalNeutrino SNOWYAMBER
Category	Malware
Type	Loader
Description	(Recorded Future) GraphicalNeutrino acts as a loader with basic C2 functionality and implements numerous anti-analysis techniques including API unhooking, dynamically resolving APIs, string encryption, and sandbox evasion. It leverages Notion's API for C2 communications and uses Notion's database feature to store victim information and stage payloads for download.
Information	<https://go.recordedfuture.com/hubfs/reports/cta-2023-0127.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.graphical_neutrino>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool GraphicalNeutrino

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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