Threat Group Cards: A Threat Actor Encyclopedia

Tool: GraphicalProton

Names	GraphicalProton GraphDrop SPICYBEAT
Category	Malware
Type	Loader
Description	(Recorded Future) GraphicalProton acts as a loader and, much like previously described samples of GraphicalNeutrino, is staged within an ISO or ZIP file and relies on the newly identified compromised domains for delivery to targeted hosts. Unlike GraphicalNeutrino, which employed note-taking web application Notion for C2, the newly identified GraphicalProton sample uses Microsoft's OneDrive for C2 communication.
Information	<https://go.recordedfuture.com/hubfs/reports/cta-2023-0727-1.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.graphdrop>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool GraphicalProton

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

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