Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:08:31 UTC

Tool: GuLoader

Names	GuLoader vbdropper CloudEyE
Category	Malware
Type	Loader
Description	(Proofpoint) Proofpoint researchers have observed a new downloader in the wild that we and other researchers are calling “GuLoader.” Our researchers first observed GuLoader in late December 2019 being used to deliver Parallax RAT, which itself had recently been released. While we regularly observe new loaders, GuLoader has gained popularity quickly and is in active use by multiple threat actors. GuLoader is a downloader, written partly in VB6, which typically stores its encrypted payloads on Google Drive or Microsoft OneDrive (underscoring that threat actors continue to adopt the cloud just like legitimate businesses are). GuLoader is a portable executable (PE) file that is often observed embedded in a container file such as an .iso or .rar file. We have also observed it being downloaded directly from various cloud hosting platforms. GuLoader is used predominantly to download remote access Trojans (RATs) and information stealers such as Agent Tesla/Origin Logger, Formbook, NanoCore RAT, NetWire RC, RemcosRAT, Ave Maria/Warzone RAT and Parallax RAT.
Information	<https://www.proofpoint.com/us/threat-insight/post/guloader-popular-new-vb6-downloader-abuses-cloud-services> <https://blog.malwarebytes.com/threat-analysis/2020/07/malspam-campaign-caught-using-guloader-after-service-relaunch/> <https://www.deepinstinct.com/blog/-down-loaded-by-guloader-malware> <https://unit42.paloaltonetworks.com/guloader-variant-anti-analysis/> <https://www.crowdstrike.com/blog/guloader-dissection-reveals-new-anti-analysis-techniques-and-code-injection-redundancy/> <https://www.trellix.com/en-us/about/newsroom/stories/research/guloader-the-nsis-vantage-point.html>

	<https://www.esentire.com/blog/guloader-targeting-the-financial-sector-using-a-tax-themed-phishing-lure> <https://www.malwarebytes.com/blog/news/2023/04/guloader-returns-with-a-rotten-shipment> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/guloader-campaigns-a-deep-dive-analysis-of-a-highly-evasive-shellcode-based-loader/> <https://blog.morphisec.com/guloader-campaign-targets-law-firms-in-the-us> <https://asec.ahnlab.com/en/55978/> <https://www.elastic.co/security-labs/getting-gooey-with-guloader-downloader> <https://unit42.paloaltonetworks.com/malware-configuration-extraction-techniques-guloader-redline-stealer/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/guloader-unmasked-decrypting-the-threat-of-malicious-svg-files/> <https://www.cadosecurity.com/blog/guloader-targeting-european-industrial-companies>
MITRE ATT&CK	<https://attack.mitre.org/software/S0561/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye> <https://malpedia.caad.fkie.fraunhofer.de/details/win.guloader>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:guloader>

Last change to this tool card: 26 December 2024

Download this tool card in JSON format

All groups using tool GuLoader

Changed	Name	Country	Observed	
APT groups				
	DarkCasino	[Unknown]	2021	
	RATicate	[Unknown]	2019	

2 groups listed (2 APT, 0 other, 0 unknown)
