

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:29:33 UTC

Tool: RockLoader

Names	RockLoader
Category	Malware
Type	Downloader
Description	(Proofpoint) This actor is frequently using it as an intermediate “downloader”.
Information	< https://www.proofpoint.com/us/threat-insight/post/dridex-actors-get-in-ransomware-with-locky > < https://www.proofpoint.com/us/threat-insight/post/Locky-Ransomware-Cybercriminals-Introduce-New-RockLoader-Malware >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.rockloader >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:rockloader >

Last change to this tool card: 14 May 2020

Download this tool card in [JSON](#) format

All groups using tool RockLoader

Changed	Name	Country	Observed	
APT groups				
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

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

[1](#)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ab4af998-1f1e-410c-a6b9-728ecd492a6a>