Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:23:01 UTC

Tool: Gamaredon

Names	Gamaredon
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader
Description	(Palo Alto) The custom-developed malware is fully featured an includes these capabilities: • A mechanism for downloading and executing additional payloads of their choice • The ability to scan system drives for specific file types • The ability to capture screenshots • The ability to remotely execute commands on the system in the user's security context
Information	<https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Gamaredon

Changed	Name	Country	Observed	
APT groups				
	Gamaredon Group		2013-Feb 2025	

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