Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:50:15 UTC

Tool: RokRAT

Names	RokRAT
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Credential stealer, Info stealer, Exfiltration, Downloader
Description	(Carbon Black) ROKRAT is a Remote Access Trojan (RAT). ROKRAT provides attackers with numerous capabilities to introduce additional tools and malware onto a network, exfiltrate data, harvest credentials, as well as capture screenshots of the victim system. The latest variants of ROKRAT use internet cloud solutions such as PCloud, Dropbox, and Yandex as a command and control (C2) channel.
Information	<https://www.carbonblack.com/2018/02/27/threat-analysis-rokrat-malware/> <http://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/002/191/original/Talos_RokRatWhitePaper.pdf> <http://blog.talosintelligence.com/2017/04/introducing-rokrat.html> <http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html> <https://www.intezer.com/apt37-final1stspy-reaping-the-freemilk/> <http://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html> <https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/rokrat-analysis/> <https://research.checkpoint.com/2023/chain-reaction-rokrats-missing-link/> <https://threatmon.io/reverse-engineering-rokrat-a-closer-look-at-apt37s-onedrive-based-attack-vector/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0240/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rokrat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ROKRAT>

Last change to this tool card: 21 June 2023

Download this tool card in JSON format

All groups using tool RokRAT

Changed	Name	Country	Observed	
APT groups				
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1339c5d9-ed14-42ef-b70d-58de896c5d42