Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:32:30 UTC

Tool: RotBot

Names	RotBot
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Credential stealer, Info stealer, Exfiltration, Tunneling
Description	(Talos) RotBot, the QuasarRAT client variant, in its initial execution phase, performs several detection evasion checks on the victim machine and conducts system reconnaissance. RotBot then connects to a host on a legitimate domain, likely controlled by the threat actor, and downloads the configuration file for the RotBot to connect to the C2. CoralRaider uses the Telegram bot as the C2 channel in this campaign.
Information	<https://blog.talosintelligence.com/coralraider-targets-socialmedia-accounts/>

Last change to this tool card: 18 June 2024

Download this tool card in JSON format

All groups using tool RotBot

Changed	Name	Country	Observed	
Other groups				
	CoralRaider		2023-Feb 2024	

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