Rocke, Iron Group - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:12:47 UTC

Other threat group: Rocke, Iron Group

Names	Rocke *(Talos)* Iron Group *(Intezer)* Aged Libra *(Palo Alto)* G0106 *(MITRE)*	
Country	China	
Motivation	Financial gain	
First seen	2018	
Description	(Talos) This threat actor initially came to our attention in April 2018, leveraging both Western and Chinese Git repositories to deliver malware to honeypot systems vulnerable to an Apache Struts vulnerability. In late July, we became aware that the same actor was engaged in another similar campaign. Through our investigation into this new campaign, we were able to uncover more details about the actor.	
Observed		
Tools used	Godlua, Kerberods, LSD, Pro-Ocean, Xbash and several 0-day vulnerabilities.	
Operations performed	Apr 2018	This threat actor initially came to our attention in April 2018, leveraging both Western and Chinese Git repositories to deliver malware to honeypot systems vulnerable to an Apache Struts vulnerability. <https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html>
	Dec 2018	By analyzing NetFlow data from December 2018 to June 16, 2019, we found that 28.1% of the cloud environments we surveyed had at least one fully established network connection with at least one known Rocke command-and-control (C2) domain. Several of

	those organizations maintained near daily connections. Meanwhile, 20% of the organizations maintained hourly heartbeats consistent with Rocke tactics, techniques, and procedures (TTPs). <https://unit42.paloaltonetworks.com/rockein-the-netflow/>
Jan 2019	Palo Alto Networks Unit 42 recently captured and investigated new samples of the Linux coin mining malware used by the Rocke group. The family was suspected to be developed by the Iron cybercrime group and it's also associated with the Xbash malware we reported on in September of 2018. The threat actor Rocke was originally revealed by Talos in August of 2018 and many remarkable behaviors were disclosed in their blog post. The samples described in this report were collected in October of 2018, and since that time the command and control servers they use have been shut down. <https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/>
May 2019	Pacha Group Competing against Rocke Group for Cryptocurrency Mining Foothold on the Cloud <https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/>
May 2019	Over the past month we have seen new features constantly being added to the malware. For instance, in their latest major update, they have added a function that exploits systems running the software development automation server Jenkins to increase their chance of infecting more systems, thereby generating more profits. In addition, they have also evolved their malware by adding new attack stages, as well as new redundancies in its multi-component execution to make it more dynamic and flexible. <https://www.fortinet.com/blog/threat-research/rocke-variant-ready-to-box-mining-challengers.html>
Summer 2019	Rocke, a China-based cryptomining threat actor, has changed its Command and Control (C2) infrastructure away from Pastebin to a self-hosted solution during the summer of 2019. <https://www.anomali.com/blog/illicit-cryptomining-threat-actor-rocke-changes-tactics-now-more-difficult-to-detect#When:14:00:00Z>
Jan 2021	Pro-Ocean: Rocke Group's New Cryptojacking Malware <https://unit42.paloaltonetworks.com/pro-ocean-rocke-groups-new-cryptojacking-malware/>

	Apr 2021	Rocke Group Actively Targeting the Cloud: Wants Your SSH Keys <https://www.intezer.com/blog/cloud-security/rocke-group-actively-targeting-the-cloud-wants-your-ssh-keys/>
Information	<https://redcanary.com/blog/rocke-cryptominer/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0106/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=agedlibra>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
