# Hacking groups compete for cryptojacking cloud-based infrastructure

Reference: Memo [190514-1] Date: 14/05/2019 - Version: 1.0
Keywords: Pacha, Rocke, cryptomining, cryptojacking, cloud-based infrastructure
Sources: publicly available information

## Key Points

- Two hacking groups associated with large-scale cryptomining campaigns wage war on one another.
- Pacha Group and Rocke Group compete to compromise as much cloud-based infrastructure as possible.
- One group is using techniques to kill any other cryptocurrency malware running on infected machines.
- Cloud infrastructure is quickly becoming a common target for threat actors, particularly on vulnerable Linux servers.

## Summary

Two cryptomining threat actor groups are competing with one another for cryptocurrency mining foothold on cloud-based infrastructures.

Cryptomining malware, also known as crypto jacking or cryptocurrency mining malware, refers to software developed to take over a server's or a computer's resources and use them for cryptocurrency mining without a user's explicit permission.

According to open sources, the first group, tracked as Pacha, has Chinese origins and was first detected in September 2018. It is known to deliver the Linux.GreedyAntd miner. The Pacha Group's attack chain starts by compromising vulnerable servers by launching brute-force attacks against services like WordPress or PhpMyAdmin, or in some cases leveraging a known exploit for an outdated version of similar services.

As early as April 2018, the second group known as Rocke Group also used cryptocurrency miners in campaigns that attempted to kill any other cryptocurrency malware running on infected machines, leveraging both Western and Chinese Git repositories to deliver malware to honeypot systems affected by an Apache Struts vulnerability. In response to agent-based Cloud Workload Protection Platforms from cloud service providers, the malware used by the Rocke Group gradually developed the capability to evade detection before exhibiting any malicious behaviours.

Both groups are actively targeting cloud infrastructure to run their cryptocurrency miners and have now started fighting each another. Pacha Group, to in order to oust the rivals, has added Rocke IP addresses to a hardcoded blacklist implemented by the Linux.GreedyAntd aimed at blocking Rocke's miners by routing their traffic back to the compromised machines.

The miners used by both groups are able to discover and disable cloud security and monitoring products from various vendors such as Alibaba Cloud and Tencent Cloud. Both malware also include a lightweight user-mode rootkit known as Libprocesshider and have abused the recently published Atlassian Confluence vulnerabilities.

## Comments

Cloud infrastructure is quickly becoming a common target for threat actors, particularly on vulnerable Linux servers. Unfortunately, the detection rates of Linux-based malware remain low and the security community needs more awareness in order to more effectively mitigate these threats.

Researchers were able to present evidence that the Pacha Group is targeting cloud-based environments and is especially aggressive towards the Rocke Group.

The main Pacha malware infrastructure appears to be identical to previous Pacha Group campaigns, although there is a distinguishable effort to detect and mitigate Rocke Group's implants. In the blacklist of Linux miners (Linux.GreedyAntd), several file names known to be used for Rocke Group were recognised. Furthermore, there are other strings detected within a file path blacklist which are used to search and disable cloud protection solutions, such as Alibaba Server Guard Agent. Another interesting update in the Pacha Group's infrastructure in comparison to previous campaigns is that it would only be possible to download further implants from Pacha Group's servers if the HTTP GET request was completed with a specific user-agent.

The variant of the malware used by the Rocke group is an example that demonstrates that an agent-based cloud security solution may not be enough to prevent evasive malware targeted at public cloud infrastructure.

The public cloud infrastructure is one of the main targets for these cybercrime groups. Realising that the existing cloud monitor and security products may detect the possible malware intrusion, malware authors continue to create new evasion technologies to avoid being detected by cloud security products.

Cryptojacking is not the only emerging threat to cloud-based infrastructure. Recently CERT-EU reported on other kinds of threats affecting cloud-based infrastructure, such as ransomware (see Memo 190103-1), supply chain compromise (see Memo 190319-1), targeted intrusion (see Memo 190312-1), remote desktop protocol (RDP) abuse (see Memo 190225-2), storing and trading of leaked credentials (see MEMO 190121-1).


Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.