Rocke Group Actively Targeting the Cloud: Wants Your SSH Keys

By Nicole Fishbein

Published: 2021-04-06 · Archived: 2026-04-05 19:50:30 UTC

New Malware Variant Exploits Production Environment

Rocke Group is a Chinese-based threat actor most known for running cryptojacking malware on Linux machines. The group has been active since 2018 and continues to evolve by modifying its tools and techniques to stay evasive. In 2019, we reported that Rocke Group was competing with Pacha Group for cryptomining positioning on Linux-based servers in the cloud.

We have found a new malware variant developed by Rocke Group, that infects other machines in the network using saved SSH keys and weak passwords. It also exploits vulnerabilities in popular platforms and services such as Jenkins, Redis and ActiveMQ. Once the victim is infected a Monero cryptominer is executed. Below we present our findings with instructions on how to check if your system has been compromised, as well as how to protect your cloud environments against future Rocke Group attacks.

Capabilities and Findings on Rocke Group Malware

The malware that is initially delivered to the victim's server is packed with a modified UPX which can make it harder for some Endpoint Detection and Response (EDR) products to detect the malicious code. This threat contains a number of modules that are stored in a compressed form inside the malware, and during the execution the payloads are extracted and executed.

Rocke Group uses a new script that downloads malware from a hosting server and executes it. The malware then uses public SSH keys, which are saved in a file called "known_hosts" on the victim's Linux machine, to infect other machines on the network.

The malware archives persistence using a scheduled task in crontab and bashrc files. It creates a service that controls the execution of the malware and configures it to be executed on startup. The payload of the service is extracted from within the Rocke Group sample.

Next, the malware attempts to spread in the network by brute forcing SSH, Redis and Jenkins with weak passwords. Then, it exploits vulnerabilities. For Jenkins it uses two vulnerabilities for executing code (**CVE-2018-1000861**, **CVE-2019-1003000**) and for ActiveMQ it tries to do an arbitrary file writing (**CVE-2016-3088**).

To hide the activity of the malware, it implements an evasion technique that uses library hijacking. This way the information retrieved by system commands is altered in a way that hides resources used by the malware and its components. For instance, running the 'top' command will not show the high CPU usage caused by the cryptomining malware.

One of the compressed modules is an XMRig Miner. Before the miner is executed the dropper kills any other process that uses more than 30% of the cloud server's CPU, this way the cryptominer will have all of the CPU for itself.

Detection and Response

Detect if a machine in your system has been compromised by following all of these steps:

1. 1. The malware creates files in the following directories:
    - /usr/local/sbin
    - /usr/local/bin
    - /usr/bin
    - /usr/libexec
    - /tmp

Check if there are suspicious files in these locations. This campaign is known for using similar names to valid Linux services and file names such as "kerberods", so pay attention to the files you see in these directories. In other cases, it uses file names like: 6ff4ba5d0de4498. In addition, the malware changes the timestamps of files created during the attack so that they appear older. You should not rely on the creation/modification time of the files. **Response:** Remove the malicious files **MITRE Technique:** Masquerading (T1036)

1. 1. Check if there is a service that listens on port 61131 for incoming connections. Use the command: *netstat -tupln*

Response: Find the PID of the process and kill it. Run the following command to get the PID: *netstat -ltnp | grep -w ':61131'* and then: *sudo kill -9 <PID>* to kill the process.

1. 1. Check if you have a service called **sshservice.service**. You can do this by running: *systemctl status sshservice.service*

Response: Stop and remove the service by running these commands:

systemctl stop [servicename] systemctl disable [servicename] rm /etc/systemd/system/[servicename] rm /etc/systemd/system/[servicename] rm /usr/lib/systemd/system/[servicename] rm /usr/lib/systemd/system/[servicename] systemctl daemon-reload systemctl reset-failed

MITRE Technique: Create System Process (T1543) and Masquerading (T1036)

1. 1. Check if the cron jobs include commands in the following format: **/15 * * * * (curl -fsSL -m180 ||wget -q -T180 -O-)|sh*Check the following location of scheduled jobs:
    - /var/spool/cron/root
    - /var/spool/cron/crontabs/root
    - /etc/cron.d/root

    Response: Delete these commands from the crontab **MITRE Technique:** Scheduled Task/Job (T1053)
2. Check that */etc/bashrc* contains commands in the same format as the crontab files

Response: Delete the commands from the file **MITRE Technique:** Event Triggered Execution using .bashrc file (T1546)

1. 1. This campaign uses DNS over HTTPs (DoH) to obtain the address of the C2 server using hard-coded domains that send back an encrypted DNS record. Inspect your network traffic for anomalies in HTTPs packages. Check if your machine tried to access one (or more) of the following domains:
    - Update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
    - cloudflare-dns[.]com

MITRE Technique: Protocol Tunneling (T1572) and Encrypted Channel (T1573)

1. 1. The malware tries to infect other machines in the network by brute forcing weak passwords and exploiting vulnerabilities in Jenkins, Redis, SSH and ActiveMQ. Follow all of the steps above for machines that have these services.

MITRE Technique: Network Service Scanning (T1046)

TTPs now available in Intezer. Speed up malware analysis with relevant insights to understand how malware behaves.

Be Proactive

- Use strong passwords for SSH, Jenkins and Redis services. It is also highly recommended to use TLS authentication.
- Use different passwords and authentication keys for each machine in the network.
- Make sure that your Jenkins and ActiveMQ services have the latest updates.
- Restrict access to services and machines, and give only the required permissions for each user.
- Filter network traffic to untrusted or known bad domains.
- Apply detection of anomalies in the networks to detect suspicious communication that digresses from the usual traffic.

Runtime Protection is a Must

This attack is sophisticated in that it implements evasion techniques making detection much harder. It also spreads to other services and machines on the network making it harder to respond to. Runtime protection gives you immediate visibility over all code running in your systems and alerts you whenever unauthorized code is executed. So, if Rocke Group attacks an environment with runtime protection, the user would immediately get an alert on all infected machines with the ability to terminate the malicious processes. While there are dozens of cloud attack vectors that threat actors can utilize, such as software vulnerabilities and misconfigurations, eventually all attackers must run code or commands in the production environment to conduct any damage. Consider that it’s not realistic to be able to close all attack vectors. Not only does it take time to fix vulnerabilities, but there are always attack vectors that are practically impossible to prevent such as supply chain or unknown vulnerabilities. Recent attacks have shown that Linux cryptominers and other threats will find their way into the production environment no matter how hard you work to reduce the attack surface. Runtime protection is a necessary last line of defense as actors like Rocke Group remain active.

IoCs

Dropper Script

F947e69f9f8d113fb9fba3e795827110ee17feb310b54a7f7b6672a5386a3de2

Malware

Fe27d4a8a5f299b0b25d10816e98cef2852af6dc3541bf25a77960b1573ca61d

Mining Pool

minexmr[.]com pool

XMRig Miner

398e3608455dbea2cba8e9944d9b43cbb0982b48b2882fe54adf937a7a62d9e2

Domains Used to Download the Malware

img[.]sobot.com cdn[.]xiaoduoai.com https://user-images[.]githubusercontent.com

Domains Used for Resolving the C2 Address

Update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com cloudflare-dns[.]com

Thanks to Joakim Kennedy for contributing to this post.
