Illicit Cryptomining Threat Actor Rocke Changes Tactics, Now More Difficult to Detect

By Anomali Threat Research

Published: 2025-12-18 · Archived: 2026-04-05 22:46:18 UTC

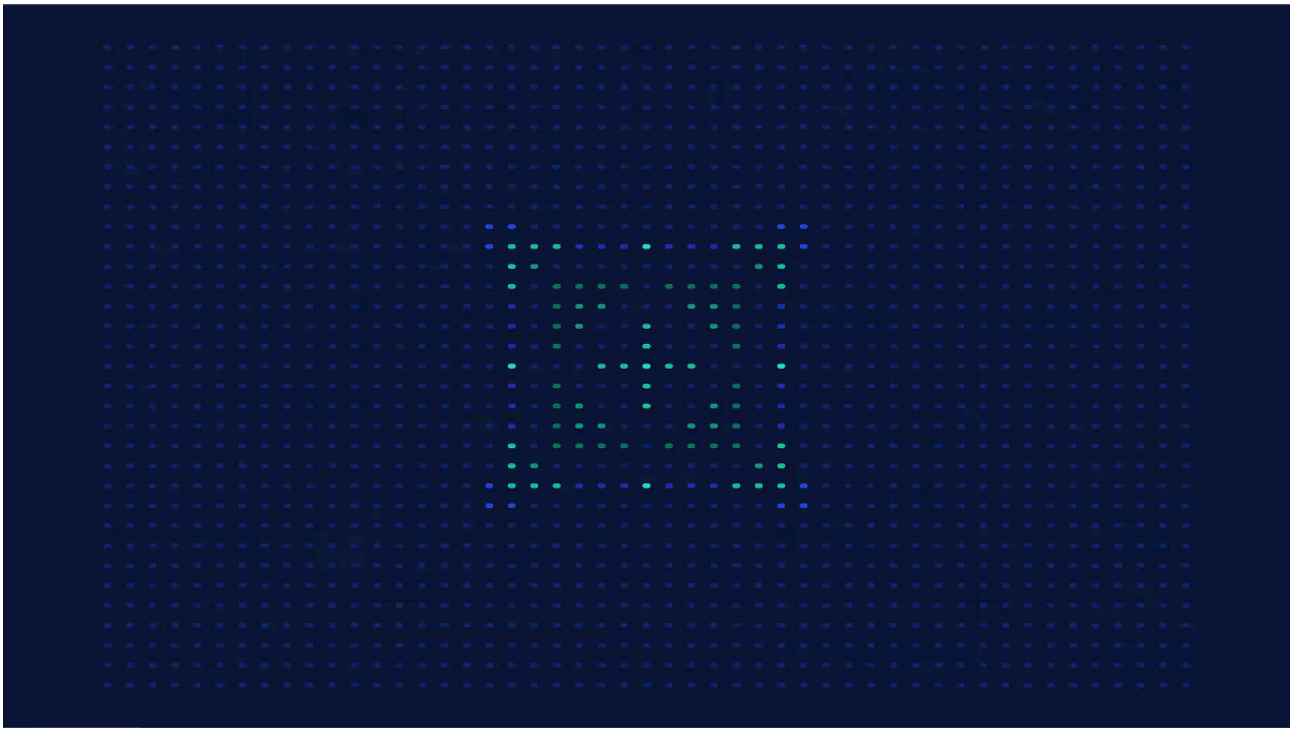
All Posts

1

min read

China-based cryptomining threat actor Rocke has changed its Command and Control (C2) infrastructure away from Pastebin to a self-hosted solution.

Published on



Summary

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. The setup scripts were hosted on the domains “lsd.systemten[.]org” and “update.systemten[.]org” as pastes. In September 2019, the actor moved away from hosting the scripts on dedicated servers and instead started to use Domain Name System (DNS) text records. These records are accessed via normal DNS queries or DNS-over-HTTPs (DoH) if the DNS query fails. In addition to the C2 change, functionality was also added to their LSD malware to exploit ActiveMQ servers vulnerable to CVE-2016-3088.

The change in technique observed by Rocke is a step forward in regards to the threat actor's overall sophistication. By moving from Pastebin to self-hosted and DNS records, the actor is better protected against potential takedowns, and its malicious operations may become more difficult to detect. As of this writing, Rocke is primarily known for cryptomining, however, it is possible for the actor to change payloads to something more damaging if Rocke wished to try to make illegal funds with a different technique. Therefore, it is paramount to take steps to mitigate the possibility of Rocke-styled campaigns.

Introduction

Rocke is primarily focusing on illicit cryptomining that is conducted on compromised machines. The group was first reported by Cisco Talos[1] in August 2018, and Palo Alto's Unit 42 has produced numerous reports[2-4] on the group since then. Anomali's Threat Research Team has been tracking the actor's activity since March of 2019. Our report in March described how the actor started to use a malware written in Go (Golang) to set up and monitor the mining on the infected machine.[5] We have been observing the threat actor continuing to use the same malware throughout the year. In April 2019, Confluence users posted reports on Atlassian's support forum reporting infections of cryptominer.[6] Rocke utilized CVE-2019-3396, which was disclosed the month before, to install its malware on vulnerable Confluence servers. The activity of the group continued for a few months with only minor changes to their Tactics, Techniques, and Procedures (TTPs).

Summer 2019 activity

In June, Rocke shifted its technique from using "Pastebin" to self-hosting the initial setup script. This was performed by using subdomains on the domain "systemten[.]org", the domain name that is pointing to the mining pool/proxy used by the threat actor. Two of these subdomains are "lsd.systemten[.]org" and "update.systemten[.]org". On July 29, 2019, both of these subdomains saw a huge spike in requests, according to data from Cisco Umbrella. The "update" subdomain was still being requested until September 17, 2019, when it stopped abruptly. Figures 1 and 2 below are showing both of these events. The "lsd" subdomain is still being requested as of writing.

Data from Cisco Umbrella showing queries for "lsd.systemten[.]org" for a few days in July. A spike of over 20,000 queries per hour were recorded on July 29, 2019.
Figure 1 - Data from Cisco Umbrella showing queries for "lsd.systemten[.]org" for a few days in July. A spike of over 20,000 queries per hour were recorded on July 29, 2019.

Data from Cisco Umbrella showing how queries for "update.systemten[.]org" stopped on September 17, 2019.
Figure 2 - Data from Cisco Umbrella showing how queries for "update.systemten[.]org" stopped on September 17, 2019.

The two subdomains shown above were substituting the actor's use of Pastebin. The "update" subdomain returns the current version string. From it, the malware determines if it needs to download a newer version. The "lsd" subdomain serves the setup bash script, which is used to set up some persistence via cron jobs and download the latest version of the malware.

Changes to the LSD malware

The “LSD” malware has had some updates since it was first reported on by Anomali Threat Research team in March 2019. A reconstruction of the source code layout is shown below:

```
Package github.com/hippies/LSD/LSDB: /root/go/src/github.com/hippies/LSD/LSDB File:       init Line
```

One new functionality is the addition of the “StartHttpServer” function. The malware starts a web server that is listening on localhost and TCP port 65533. This serves as a mutex to ensure only one instance of the malware is running because only one application can bind to a specific port. In Figure 3 below it can be seen that the malware tries to connect to this port. If it succeeds, it knows another version is running and it exits. Otherwise, it continues with setting up the machine for mining.

Assembly snippet showing the malware connecting to localhost on port 65533 over TCP.
Figure 3 - Assembly snippet showing the malware connecting to localhost on port 65533 over TCP.

New Exploit Added

The first iteration of the malware, would try to gain access to other machines via SSH and Redis. This was performed by using weak credentials. Later during the spring, functionality for exploiting Jenkins servers was also added. In this phase, support for CVE-2016-3088 exploitation was the important addition. CVE-2016-3088 is a vulnerability in ActiveMQ that can allow uploading of an arbitrary file. In Figure 4 it can be seen that the malware tries to upload a cron job to the following locations: “/etc/cron.d/root”, “/var/spool/cron/root”, and “/var/spool/cron/crontabs/root”.

The LSD malware tries to add crontab files to “/etc/cron.d/root”, “/var/spool/cron/root”, and “/var/spool/cron/crontabs/root”.
Figure 4 - The LSD malware tries to add crontab files to “/etc/cron.d/root”, “/var/spool/cron/root”, and “/var/spool/cron/crontabs/root”.

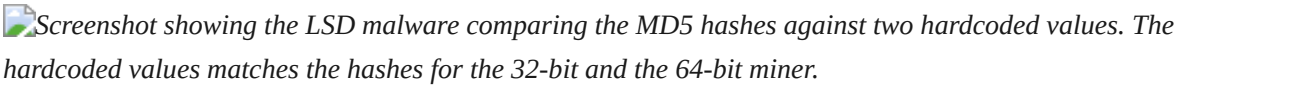
The exploit is performed by using two HTTP requests. First, the file is uploaded via a “PUT” request as can be seen in Figure 5. The file is then moved to the location for a crontab file via a “MOVE” request, shown in Figure 6.

LSD malware constructing a “PUT” request to upload the crontab file to “/fileserver/go.txt” on the ActiveMQ host.
Figure 5 - LSD malware constructing a “PUT” request to upload the crontab file to “/fileserver/go.txt” on the ActiveMQ host.

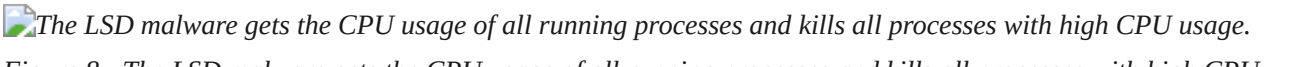
The malware constructs a “MOVE” request to move the crontab file from “/fileserver/go.txt” to one of the three crontab locations.
Figure 6 - The malware constructs a “MOVE” request to move the crontab file from “/fileserver/go.txt” to one of the three crontab locations.

King of the Hill

The malware tries to ensure only the threat actor's miner is running on the infected machine. It does so by killing any other processes with high CPU usage. The LSD malware identifies its miner via the MD5 hash of the file to make sure it doesn't kill its miner. In Figure 7 below it can be seen that the malware compares the MD5 hash to two hardcoded values. These hashes match the hashes of the 32-bit and the 64-bit version of the miner dropped by the malware.


Screenshot showing the LSD malware comparing the MD5 hashes against two hardcoded values. The hardcoded values matches the hashes for the 32-bit and the 64-bit miner.
Figure 7 - Screenshot showing the LSD malware comparing the MD5 hashes against two hardcoded values. The hardcoded values matches the hashes for the 32-bit and the 64-bit miner.

After the malware knows which process to ignore, it will iterate through all the running processes and capture the CPU usage. If it's above the threshold, the process is killed as can be seen in Figure 8.


The LSD malware gets the CPU usage of all running processes and kills all processes with high CPU usage.
Figure 8 - The LSD malware gets the CPU usage of all running processes and kills all processes with high CPU usage.

September and DoH

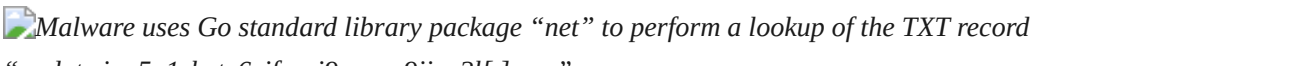
In September 2019, Rocke pushed a new version of the LSD malware. The malware maintains the functionality from the samples seen during the summer of 2019. A reconstruction of the source code layout is shown below:

```
Package github.com/hippies/LSD/LSDB: /root/go/src/github.com/hippies/LSD/LSDB File:      init Lines
```

The primary change is in the C2 functionality. Instead of using the domain "systemten[.]org" the threat actor has moved over to the domain "iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com". According to Cisco Umbrella data, the "update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com" subdomain, shown in Figure 9, started to be queried on September 17. This is the same day as when "update.systemten[.]org" stopped being queried.


DNS queries for "update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com" in September 2019. The requests are around 75 requests per hour.
Figure 9 - DNS queries for "update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com" in September 2019. The requests are around 75 requests per hour.

Instead of hosting the setup script and update version on a dedicated host, the threat actor is using TXT records. In Figure 10 it can be seen that the malware tries to lookup the TXT record for "update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com". The response is encrypted with AES-128.


Malware uses Go standard library package "net" to perform a lookup of the TXT record "update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com".
Figure 10 - Malware uses Go standard library package "net" to perform a lookup of the TXT record "update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com".

If the lookup fails, the malware tries to perform the same lookup via a DoH request, shown in Figure 11. The server queried for the DoH request is “cloudflare-dns.com”.


LSD malware creating a DoH request for TXT records.
Figure 11 - LSD malware creating a DoH request for TXT records.

The TXT record values are encrypted with 128-bit AES in cipher-block-chaining (CBC) mode and base64 encoded. The key is derived from the TXT record. Figure 12 shows a summary of the function used to derive the decryption key. The record, for example, “update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com” is hashed with two rounds of MD5. The 128-bit hash digest is passed to the Go standard library function for generating a new AES cipher. The key and block are added to the “LSDC.AesCipher128” struct, shown in Figure 13.


Summary of the function used to generate the AES key to decrypt the TXT request answer.
Figure 12 - Summary of the function used to generate the AES key to decrypt the TXT request answer.


Data structure used to hold decryption information.
Figure 13 - Data structure used to hold decryption information.

Conclusion

Rocke keeps evolving its TTPs in attempts to remain undetected. By moving away from hosting scripts on Pastebin to self-hosted and DNS records, the threat actor is more protected against potential take-downs that could prevent ongoing malicious activity. It is expected that the group will continue to exploit more vulnerabilities to mine additional cryptocurrencies in the near future. Enterprises with internet-facing services should ensure all the software is always up-to-date and that no weak passwords are used. While illicit cryptocurrency mining can be seen as a minor issue, it could lead to increased resource drain and earlier hardware failure. In addition, it is possible that Rocke, or other cryptomining threat actors could change the payload from a cryptominer to something more dangerous, such as ransomware or a Remote Access Trojan (RAT). Therefore, it is paramount to take steps to mitigate the possibility of Rocke-styled campaigns.

Enterprise Threatstream users can access more information here, which includes password lists used by the actor for brute force attacks.

IOCs

- systemten[.]org
- lsd.systemten[.]org
- update.systemten[.]org
- 1x32.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
- 2x32.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
- 3x32.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
- 1x64.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
- 2x64.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
- 3x64.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
- shell.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com

- update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
- cron.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com

MITRE ATT&CK™ Techniques

Tactic	ID	Name	Description
Initial Access	T1190	Exploit Public-Facing Application	Rocke is using exploit known vulnerabilities in public facing services.
	T1078	Valid Accounts	The LSD malware uses stored ssh keys on the infected host to gain access to other machines.
Execution	T1168	Local Job Scheduling	The exploits are used to install cron jobs that will download the LSD malware.
	T1064	Scripting	The cron job will download a shell script that in turn downloads the LSD malware.
Persistence	T1156	.bash_profile and .bashrc	Entries to ".bashrc" is added to for persistence.
	T1168	Local Job Scheduling	Cron job entries are created to ensure a new version of the LSD malware is installed in the case it is removed.
	T1501	Systemd Service	The LSD malware creates a systemd service to ensure it is restarted when the machine reboots.
Defense Evasion	T1036	Masquerading	The LSD malware use filenames similar to common Linux services. For example, sshd and kerberods.
	T1099	Timestomp	Files created have their timestamp altered to appear older.
Credential Access	T1110	Brute Force	The LSD malware tries to compromise Redis and ssh servers via credential brute forcing.
Discovery	T1046	Network Service Scanning	The LSD malware scans for other machines that are running vulnerable services of ActiveMQ, Jenkins, ssh, and Redis.
	T1057	Process Discovery	The LSD malware enumerates all the running processes to find any other potential miners installed on the machine. If others are found, they are killed.

	T1018	Remote System Discovery	The setup script used by the threat actor uses the known_hosts file to find other machines it can access over ssh.
Lateral Movement	T1021	Remote Services	The setup script uses known ssh hosts and stored ssh keys to infect other machines.
Command and Control	T1043	Commonly Used Port	The LSD uses HTTP/HTTPs and DNS TXT records for C2.
	T1132	Data Encoding	The data retrieved from the DNS TXT records are encrypted and base64 encoded.
	T1079	Multilayer Encryption	The LSD malware uses DoH to retrieve encrypted instructions.
	T1071	Standard Application Layer Protocol	The LSD uses HTTP/HTTPs and DNS TXT records for C2.
Impact	T1496	Resource Hijacking	The LSD malware installs a Monero miner.

Endnotes

1. David Liedenberg, "Rocke: The Champion of Monero Miners," Talos Blog, accessed March 14, 2019, published August 30, 2018.
2. Nathaniel Quist, "Rocke'in the NetFlow", Palo Alto Networks Unit 42 Blog, accessed October 8, 2019, published August 1, 2019.
3. Claud Xiao, Cong Zheng and Xingyu Jin, "Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows", Palo Alto Networks Unit 42 Blog, accessed October 8, 2019, published September 17, 2018.
4. Xingyu Jin and Claud Xiao, "Malware Used by "Rocke" Group Evolves to Evade Detection by Cloud Security Products", Palo Alto Networks Unit 42 Blog, accessed October 8, 2019, published January 17, 2019.
5. Anomali Labs, "Rocke Evolves Its Arsenal With a New Malware Family Written in Golang", Anomali Blog, accessed October 8, 2019, published March 15, 2019.
6. "How come my Confluence installation was hacked by Kerberods malware?", Atlassian Community, accessed October 8, 2019, published Apr 10, 2019.

April 3, 2026

Anomali Cyber Watch

Read More

April 3, 2026

Public Sector

Anomali Cyber Watch

Read More

April 2, 2026

Anomali Cyber Watch

Read More

Explore All
