yayaya Miner Mining Trojan Analysis

Antiy CERT

Draft completed: May 8, 2023
First published: May 11, 2023

The original report is in Chinese, and this version is an AI-translated edition.

1 Overview of the Active yayaya Mining Trojan

Recently, Antiy CERT captured a batch of active mining Trojan samples, which mainly used SSH weak password brute force to attack the Linux platform. Because the "yayaya" string appeared many times in its initial attack script, and all information containing the string would be hidden in the Linux kernel module, Antiy CERT named the mining Trojan "yayaya Miner".

Table 1-1 Active mining overview

Active mining overview	Illustrate
Mining trojan name	yayaya Miner
The main way mining trojan spread	Use weak SSH passwords to perform brute force attacks
Appearance time	End of November 2022
Active time	Active in April 2023
Mining coins	Monero
Target system	Linux
Main technical features	Encrypt the initial script; delete competitor mining ; delete system logs; use open source tools to hide kernel modules, etc.

It has been verified that the Linux version of Antiy Intelligent Endpoint Protection System (IEP for short) can effectively detect and kill the mining Trojan.

2 Sample Functions and Technical Analysis

yayaya Miner mining Trojan uses the shc tool to encrypt the initial attack script. The tool can be used to convert the Shell script into a binary executable file (ELF) and encrypt it using the RC4 encryption algorithm. The initial attack script file will delete system logs, create directories such as yayaya, delete network connections of specific IPs,

download the Monero mining program, and use the open source tool Diamorphine for hidden operations. The mining process is injected into the memory and then hidden, making it more difficult for anti-virus software to detect.

2.1 yayaya xxxxxxxx (Initial Attack Script, X Represents Random Characters)

The overall process and core technology of the sample's initial attack script are as follows:

1. The initial file is actually a script file. After the initial attack script is encrypted by the shc tool, the Shell script file can be converted into a binary executable file (E LF). The script will first delete other mining trojan configuration files and system logs.
2. Use the firewall command to find and delete the network connections created by other mining Trojans, and then download their own p.zip (mining program) after deletion.
3. Use the open source tool **Diamorphine to hide Linux kernel modules and processes.** Specifically, hide the specified directory prefix "yayaya". Any directory with the "yayaya" prefix will be invisible in the system. Mark the mining process as hidden, that is, it will not be displayed in the process list. Specify the kernel module name as "nonono".
4. IDs of the current process to 0 to obtain root privileges.
5. Compile the kernel module nonono.ko and load it. Use the kill command to send a signal-63 to the process with the process number 10000000 to trigger the module's hook function. Use the kill command to send a signal-31 to the specified process to suspend its execution. After successful execution, delete all files and subdirectories in the /tmp/a directory.

2.2 p.zip (Mining Program)

The p.zip compressed file contains a file named "dsm_sa_ip". It has been determined that the file is an open source Monero mining program XMR ig, which uses encrypted communication for interactive mining. The mining pool address is as follows.

Table 2-1 Mining pool address

Mining pool address	example.amax.fun:443	example.amax.fun:80	example.amax.fun:3333
	example.gengzi.site:443	example.gengzi.site:80	example.gengzi.site:3333
	example.inspur.gay:443	example.inspur.gay:80	example.inspur.gay:3333

	example.sugon.store:443	example.sugon.store:80	example.sugon.store:3333
	dasan.one:443	dasan.one:80	dasan.one:3333
	172.104.170.240:443	172.104.170.240:80	172.104.170.240:3333

3 Mining Trojan Detection and Removal Solution

3.1 yayaya Miner Recognition

1. File (x represents random characters)

File name and path:

/usr/lib/x86_64-linux-gnu/yayayaxxxxxxxx

/etc/sysconfig/yayaya/dsm_sa_ip

2. Network side troubleshooting

146.190.193.147:80 (file download)

157.245.16.79:443 (mining pool connection)

3. Service execution path

ExecStart=/usr/lib/x86_64-linux-gnu/yayayaxxxxxxxx

4. Process name

Eight random characters

5. Kernel module name

nonono

3.2 Removal Solution

1. Make hidden kernel modules visible

kill -63 0

2. View hidden kernel modules nonono

cat /proc/modules |head -n 10

3. Remove kernel modules

rmmod nonono

4. End the mining process

pid of the process that occupies the most system resources, and use the kill-9 pid command to end the process. The mining program process path is generally in the form of a string similar to "/112d9a3b".

5. Delete service

rm -rf /usr/lib/systemd/system/yayayaxxxxxxxx.service

6. Delete malicious files

m -rf /usr/lib/x86_64-linux-gnu/yayayaxxxxxxxx

rm -rf /etc/sysconfig/yayaya

4 Protective Recommendations

Antiy recommends that enterprises take the following protective measures against mining attacks:

1. Install terminal protection: Install anti-virus software. For different platforms, it is recommended to install the Windows/Linux version of Antiy Intelligent Endpoint Protection System;
2. Strengthen SSH passwords: Avoid using weak passwords. It is recommended to use passwords of 16 characters or longer, including a combination of uppercase and lowercase letters, numbers, and symbols. Avoid using the same password on multiple servers.
3. Update patches in time: It is recommended to enable the automatic update function to install system patches. The server should update system patches in time;
4. Update third-party application patches in a timely manner: It is recommended to update third-party application patches such as WebLogic in a timely manner;
5. Enable logs: Enable key log collection functions (security logs, system logs, error logs, access logs, transmission logs, and cookie logs) to provide a basis for tracing security incidents.
6. Host reinforcement: conduct penetration testing and security reinforcement on the system;
7. Deploy intrusion detection system (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracking of malicious code. Antiy Persistent Threat Detection System (PTD) uses network traffic as the detection and analysis object, and can accurately detect a large number of known malicious codes and network attack activities, and effectively discover suspicious network behaviors, assets and various unknown threats;
8. Antiy Service: If you are attacked by malware, it is recommended to isolate the attacked host in time and protect the site while waiting for security engineers to check the computer; Antiy 7*24 hours service hotline: 400-840-9234.

It has been verified that Antiy Intelligent Endpoint Protection System (IEP for short) can effectively detect and kill the mining Trojan.

Figure 4-1 Antiy IEP can effectively detect and kill the mining Trojan

5 ATT&CK Mapping Diagram Corresponding to the Incident

Regarding the complete process of the attacker launching the mining Trojan, Antiy sorted out the ATT&CK mapping map corresponding to this attack incident as shown in the figure below.

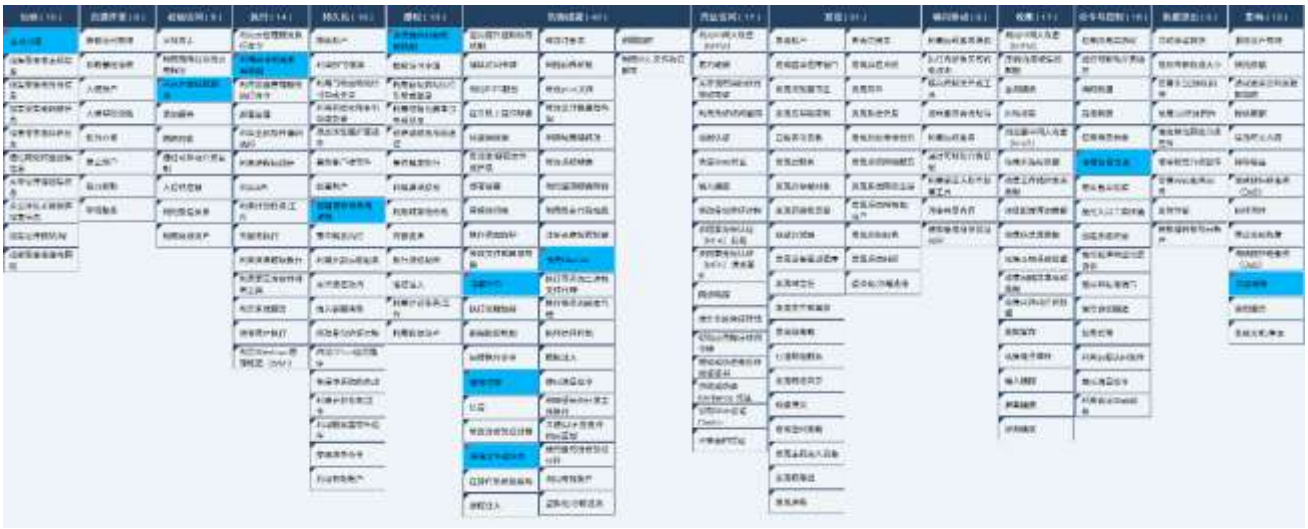

Figure 5-1 ATT&CK mapping diagram corresponding to the incident

The following table lists the techniques used by the attackers:

Table 5-1 ATT&CK technical behavior description table corresponding to the incident

ATT&CK Phase/Category	Specific Behavior	Notes

Reconnaissance	Active scan	Scan 22 ports
Initial visit	Leverage external remote services	Remote service access using SSH
Execute	Use command and script interpreters	Use shell script
Persistence	Create or modify system processes	Create service
Privilege escalation	Abuse of the control privilege escalation mechanism	Modify uid and gid to increase permissions
Defense evasion	Use rootkits	Use LKM rootkit
	Hidden behavior	Hidden process
	Delete beacon	Delete malicious file itself
	Obfuscate files or information	Use the shc tool to obfuscate files
Command and Control	Use encrypted channels	Use SSL encrypted channel
Influence	Resource hijacking	Occupy CPU resources

6 IoCs

IoCs
172.104.170.240
example.amax.fun
example.gengzi.site
example.inspur.gay
example.sugon.store
dasan.one
hxxp://example.established.site/p.zip
hxxp://w.amax.fun/p.zip
hxxp://172.104.170.240/p.zip

Appendix 1: References

[1]. Analysis of Typical Mining Families Series 2 | TeamTNT Mining Organization

https://www.antiy.cn/research/notice&report/research_report/20221207.html

[2]. Shc Linux Malware Installing CoinMiner

https://asec.ahnlab.com/en/45182/

Appendix 2: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft,

escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.