2023 Active Mining Trojan Review

Antiy CERT

First draft completed: January 22, 2024
First published time: January 29, 2024

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

1 Overview

Mining Trojans use various means to implant mining programs into victims' computers, and use the computing power of victims' computers to mine without the knowledge of users, thereby obtaining illegal profits. Currently, multiple threat organizations (for example, H2Miner, "8220", etc.) are known to spread mining Trojans, causing users' system resources to be maliciously occupied and consumed, and hardware life to be shortened, seriously affecting users' production and life, and hindering national economic and social development. In 2023, Antiy CERT released several analysis reports on mining Trojans. Now we will sort out the typical mining Trojans in 2023 to form an organization/family overview for sharing.

Table 1Overview of active mining trojan organizations/families in 2023

Mining Trojan Organization/Family	Appearance time	Targeted Platform
"8220"	2017	Windows, Linux
Outlaw	2018	Linux
WatchDog	January 2019	Windows, Linux
TeamTNT	October 2019	Linux
H2Miner	December 2019	Windows, Linux
Sysry-hello	December 2020	Windows, Linux
libgcc_a/warmup	August 2 021	Windows, Linux
Kthmimu	March 2022	Windows, Linux
aminer	June 2022	Linux
Diicot/color1337/Mexals	October 2022	Linux

2 The Harm of Mining Trojans

1. **Increased resource consumption and operational risks of information system infrastructure**: Mining Trojans generally consume a large amount of resources of information system infrastructure, causing the operating system and its services and application software to run slowly, and even causing normal services to crash, resulting in a series of negative impacts such as business interruption and business data loss;
2. **Endangering the service life and operating performance of information system infrastructure**: Mining Trojans force information system infrastructure to run at high load for a long time, shortening its service life and seriously reducing its operating performance;
3. **Waste of energy and increase of carbon emissions**: Mining Trojans consume a lot of electricity, resulting in huge energy consumption. At present, the main source of electricity in China is coal-based fossil fuel combustion. Therefore, its mining operations increase carbon emissions pollution.
4. **Leaving backdoors and generating botnets**: Mining Trojans generally have malicious behaviors such as adding SSH password-free login backdoors, installing RPC backdoors, receiving remote IRC server instructions, and installing rootkit backdoors, causing the victim organization's network to become a botnet;
5. **As a springboard to attack other targets**: Mining Trojans allow attackers to control the victim's server to launch DDoS attacks, use this server as a springboard to attack other computers, or release ransomware to demand ransom, etc.

3 Mining Trojan Trends

3.1 The AI Era Drives a New Wave of Mining Trojans

In 2023, with the continuous maturity and popularization of large-model artificial intelligence technologies, led by ChatGPT, the use of large models to launch network attacks has made network security more severe. Especially in the field of mining Trojans, this type of malware that illegally uses computing resources to mine cryptocurrencies is undergoing a transformation driven by AI technology. Against this background, some attackers who mainly rely on open source tools or scripts have begun to rise. They use artificial intelligence to write and optimize attack scripts for them, making mining Trojan attacks a serious network security threat to the network environment. With the

powerful capabilities of AI, attackers can quickly generate a large number of variant malicious scripts, which are often used as leading files of mining Trojans to prepare the environment, evade detection, or perform actual mining operations. The intervention of AI has significantly reduced the technical threshold for writing advanced malicious scripts, and even attackers with relatively low technical capabilities can create a wide range of impacts in cyberspace.

3.2 Kernel-Level Tools Make Mining Trojans Harder to Detect

In the mining forensics in 2023, Antiy CERT found that mining Trojan attackers are increasingly inclined to use rootkit kernel-level tools, such as yayaya Miner, TeamTNT and "8220". This trend indicates that the popularity of such tools will rise further in the future. The reason why rootkit kernel-level tools are popular is mainly because they can lurk at the bottom of the system , providing deeper concealment and control. These tools can directly reach the core of the operating system and load malicious kernel modules to avoid being detected by traditional security software. They can effectively hide malicious processes and files. Due to the advanced control of these tools over the system, they can continue to run in the background even when the system is restarted, ensuring that the continuous mining activities are not disturbed. **As mining Trojan attackers continue to pursue profits, mining Trojans combined with rootkit technology will become more and more complex.** They are not only satisfied with using the victim's computing resources, but are also likely to conduct deeper network penetration, posing a potential threat to other terminals in the network.

3.3 SHC Encryption Script Makes Mining Trojans More Concealed

In 2023, Antiy CERT sorted out the mining Trojans it monitored and found that in order to evade security detection, mining Trojan attackers began to use various obfuscation and encryption techniques to hide their malicious code. Among them, **the practice of using Shell Script Compiler (SHC) to encrypt scripts has become increasingly popular, and SHC has become a new tool choice for attackers to enhance the concealment of their mining scripts.** SHC is a tool that encrypts Shell scripts into binary executable files. It can effectively hide the source code of the script, making it difficult for analysts to directly view the code content. This encryption not only prevents the script source code from being analyzed, but also bypasses the signature-based detection mechanism, because the binary files generated after each encryption have different signatures. In 2023, Antiy CERT successively analyzed mining Trojans such as Hoze, Yayaya Miner, and Diicot, all of which used SHC-encrypted scripts to launch initial attacks. This attack method facilitates the spread of mining Trojans and increases the risk of user systems being infected.

4 Introduction to Active Mining Trojan

4.1 "8220 "

"8220" is a long-term active organization that is good at using vulnerabilities to attack and deploy mining programs. In the early days, the organization used Docker images to spread mining Trojans, and later gradually used multiple vulnerabilities to attack, such as WebLogic vulnerabilities, Redis unauthorized access vulnerabilities, Hadoop Yarn unauthorized access vulnerabilities, and Apache Struts vulnerabilities. In 2020, it was discovered that the organization began to use SSH brute force to carry out lateral attacks and spread. Since the Apache Log4j 2 remote code execution vulnerability was exposed, the organization has used the vulnerability to create vulnerability exploit scripts for dissemination, which has a wide range of impact.

4.1.1 Organization Overview

Table 2"8220" mining organization

Organization name	"8220"
Appearance time	2017
Targeted platform	Windows, Linux
Propagation pathway	SSH Brute Force, Docker Images, and Vulnerability Exploitation
Vulnerability exploited	Apache Log4j 2 Remote Code Execution Vulnerability Oracle WebLogic Vulnerabilities Atlassian Confluence Vulnerability Redis Unauthorized Access Vulnerability Hadoop Yarn Unauthorized Access Vulnerability Apache Struts Vulnerability
Mining coins	Monero (XMR)

4.1.2 Typical Cases

- **"8220 " mining organization's activities**

In January 2022, Antiy CERT captured multiple batches of attack samples from the "8220" mining organization. The mining organization has been active since 2017, spreading malicious scripts to both Windows and Linux

platforms. The downloaded payloads are Monero mining programs and other botnet programs, port scanning and brute force cracking tools, etc. [1].

- **Analysis of the latest mining activities of the "8220 " mining organization**

Between January and February 2023, researchers observed an attack payload targeting Oracle WebLogic Server. The payload extracted ScrubCrypt, which obfuscated and encrypted the application, enabling it to evade security programs. In addition, an updated version has been available, and the seller's webpage promises to bypass Windows Defender and provide anti-debugging and some bypass capabilities. By analyzing the malware injected into the victim's system, researchers identified the attacker as the "8220" mining group and elaborated on the details of ScrubCrypt and other malware delivered by this encryptor in the past [2].

- **Analysis of attack activities targeting Oracle Weblogic vulnerabilities**

The "8220" mining group has been active since 2017 and continues to scan for vulnerable applications in cloud and container environments. They attacked Oracle WebLogic, Apache Log4j, Atlassian Confluence vulnerabilities, and misconfigured Docker containers with the goal of deploying cryptocurrency mining programs. The group has used tools such as Tsunami malware, XMRig cryptominer, masscan, and spirit. In recent attacks, researchers observed that they exploited the CVE-2017-3506 vulnerability to attack Oracle WebLogic. This vulnerability affects the WLS security component of Oracle WebLogic. Attackers can use specific XML documents to execute arbitrary commands through remote HTTP requests, thereby gaining unauthorized access to sensitive data or invading the entire system [3].

4.2 Outlaw

The Outlaw mining botnet was first discovered in 2018. It mainly carries out mining attacks on cloud servers and remains active. It is suspected to be from Romania and was first named Outlaw by Trend Micro, which means "dead man" in Chinese. When the mining botnet was first discovered, the attacker used a backdoor program in the Perl scripting language to build the robot, so it was named "Shellbot". Its main propagation method is to brute-force SSH to attack the target system and write the SSH public key to achieve the purpose of long-term control of the target system, while downloading a backdoor written in the Perl scripting language and an open source Monero mining Trojan.

4.2.1 Organization Overview

Table 3Outlaw mining botnet

Organization name	Outlaw
Organization introduction	Shellbot written in Perl language by exploiting vulnerabilities and SSH brute force, and later began to deploy mining Trojans for profit
First disclosure time	November 1 , 2018
First disclosure manufacturer	Trend Micro
Country	Suspected Romania
Reason for naming	Derived from the Romanian word haiduc, the hacking tool H aiduc used by the organization
Threat type	Botnet, mining Trojans
Target	Linux, IoT
Propagation pathway	Shellshock (CVE-2014-7169), Drupalgeddon2 (C VE-2018-7600) and SSH brute force attacks, mainly using the latter, which was only used in the early stages
Organization components	Hidden process tool (XHide), SSH brute force cracking tools (Haiduc, ps , tsm), Shellbot program, mining trojan (XMRig)
Version iteration	This botnet sample has 5 versions, the main differences are the addition of new functions, replacement of cracking tools, and changes in cracking tool functions.

4.2.2 Typical Cases

- **Analysis of typical mining families 1: Outlaw mining botnet**

Outlaw mining botnet was first discovered in November 2018. At the time, the attackers behind it were just an organization that used vulnerabilities to hack into IoT devices and Linux servers and implanted malicious programs to form a botnet. They mainly engaged in DDoS attacks and provided DDoS-for-hire services on the dark web. In the subsequent development process, affected by the appreciation of virtual currencies, they gradually began to implant mining Trojans in botnet nodes and use the botnet to infiltrate and expand externally, obtain larger-scale computing resources, and obtain more virtual currencies in the mining process [4].

- **Outlaw hacker group resurfaces**

In February 2022 , researchers discovered a server intrusion incident involving malicious scripts and malware. Through the identified attack features (SSH key comments, malicious tool and script names, directory structure), it can be determined that this attack is very similar to the attack by the Outlaw hacker group discovered by TrendMicro in 2018. The Outlaw hacker group initially targeted the automotive and financial industries in 2018, and the recent resurgence of activities proves that the group has never stopped its activities and has evolved compared to the past. Outlaw has carried out extensive attacks against Europe in the past, and the new activities may be the same. The investigation also found the attacker's persistent means and malicious tools used by the attacker in the past, which show a certain evolution in the Outlaw activity pattern [5].

- **Watch Dog**

The WatchDog mining organization has been discovered since January 2019. It is named after the Linux daemon process watchdogd. It mainly uses exposed Docker Engine API endpoints and Redis servers to launch attacks, and can quickly turn from a single infected machine to the entire network. The WatchDog mining program consists of three parts, a Go language binary set and a bash or PowerShell script file. These binaries perform specific functions, one of which is to simulate the Linux watchdogd daemon function to ensure that the mining process does not hang, overload, or terminate unexpectedly. The second Go binary downloads a configurable list of IP address segments after providing targeted targeted operation functions for Linux or Windows systems. Finally, the third Go binary script will use the custom configuration from the initialized bash or PowerShell script to start a mining operation on the Windows or Linux operating system. WatchDog uses Go binaries to perform operations on different operating systems, such as Windows and Linux , as long as the target system has the Go language platform installed.

4.2.3 Organization Overview

Table 4 Introduction to WatchDog Mining Organization

Organization name	WatchDog
Appearance time	January 2019
Targeted platform	Windows, Linux
Propagation pathway	Exposed Docker Engine API endpoints Redis Server
Vulnerability exploited	CVE-2014-3120 CVE-2015-1427 CVE-2018-1273

	...
Mining coins	Monero (XMR)

4.2.4 Typical Cases

- **WatchDog mining organization**

In 2023, Antiy CERT captured a batch of active WatchDog mining organization samples. The organization mainly uses exposed Docker Engine API endpoints and Redis servers to launch attacks, and can quickly switch from an infected machine to the entire network. The WatchDog mining organization has been discovered since January 2019 and is still active. The WatchDog mining organization mainly uses exposed Redis servers to launch attacks. On the Windows side, a PowerShell script named "init.ps1" will first be downloaded from the Ma server . The script will download the mining program for mining, the vulnerability scanner for scanning, the daemon process for the mining process, the script file returns the host name and IP address, and the exe file adds the administrator group. On the Linux side, a sh script named "init.sh" will be downloaded from the Ma server . The script will also download the mining program, vulnerability scanner and daemon process on the Linux side, and their functions are the same as those on the Windows side. In addition, the script also has the following functions: clearing firewall rules, clearing logs, creating scheduled tasks, terminating security products, adding SSH public keys , terminating competitive mining , lateral movement, and terminating specific network connections[6].

- **WatchDog evolves with new multi-stage mining attack**

The WatchDog mining group is launching a new mining campaign that uses advanced intrusion, worm-propagation, and security software evasion techniques. The mining group targets exposed Docker Engine API endpoints and Redis servers and can quickly move from a single infected machine to an entire network. WatchDog launches the attack by compromising a misconfigured Docker Engine API endpoint with an open port 2375, giving them access to the daemon under default settings [7].

4.3 TeamTNT

The TeamTNT mining organization was first discovered in 2019, mainly targeting Docker Remote API unauthorized access vulnerabilities, misconfigured Kubernetes clusters, and Redis service brute force attacks. After the successful invasion, various login credentials are stolen and backdoors are left. The target system resources are mainly used for mining and to form a botnet. After development in recent years, the botnet controlled by the

organization is large in scale, and the attack components used are frequently updated. It is currently one of the main attack organizations for mining Linux servers. The organization is suspected to be from Germany, and its naming method is based on the teamtnt.red domain name that the organization first used.

4.3.1 Organization Overview

Table 5 Introduction to TNT Mining Organization

Organization name	TeamTNT
First disclosure time	October 2019
Country	Germany
Reason for naming	The earliest use of the teamtnt.red domain name
Threat types	Mining Trojans and Backdoors
Target	JupyterLab, Docker, Kubernetes and Redis
Propagation pathway	Wrong configuration and SSH credentials, etc.
Organizational arsenal	Tsunami, Rathole, Ezuri, Punk.py, libprocesshider, tmate, masscan, pnscan, ZGrab, Tiny Shell, Mimipy, BotB, Diamorphine, Docker Escape Tool, etc.
Organizations excel in technology	Scan LAN ports, add firewall rules, delete other competitor processes, create persistent scheduled tasks, steal service credentials, collect machine information, rootkit hidden processes, deploy mining programs and lateral movement, etc.
Twitter account	HildeGard@TeamTNT@HildeTNT
GitHub account	hilde@TeamTNT HildeTeamTNT
Hosting website	teamtnt.red

4.3.2 Typical Cases

- **Mining attacks targeting cloud-native environments**

In July 2023, researchers discovered an attack campaign targeting cloud-native environments and discovered the infrastructure used to carry out the attack. The infrastructure was in the early stages of testing and deployment, and mainly targeted exposed JupyterLab and Docker APIs to spread Tsunami malware and conduct further attacks

such as cloud credential hijacking, resource hijacking, and worm infection. After investigating the relevant infrastructure, researchers said that the attack campaign may be related to the TeamTNT organization[8].

- **Mining attacks targeting multiple cloud service platforms**

Researchers found that the attackers who previously stole Amazon Web Services (AWS) certificates expanded their tools to include modules targeting Azure and Google Cloud Platform in June 2023. Researchers believe that this attack activity is associated with the TeamTNT organization. Researchers found iconic shell scripts in this attack activity and malicious ELF files written in Golang. One point worth noting is that the attackers added new functions targeting Azure and Google Cloud Platform in their scripts. Although the function was not called, this shows that these functions are under active development and may be used in subsequent attack activities[8].

4.4 H2Miner

The H2Miner mining trojan first appeared in December 2019. In the early stages of the outbreak and for a period of time thereafter, the mining trojan targeted the Linux platform. It was not until November 2020 that it began to exploit the WebLogic vulnerability to invade the Windows platform and implant the corresponding mining program. In addition, the mining trojan frequently exploited other common Web component vulnerabilities to invade related servers and implant mining programs. For example, in December 2021, the attacker exploited the Log4j vulnerability to implement the H2Miner mining trojan.

4.4.1 Organization Overview

Table 6H2Miner mining organization introduction

Organization name	H2Miner/Kinsing
Appearance time	December 2019
Targeted platform	Windows, Linux
Propagation pathway	Exploits
Vulnerability exploited	Looney Tunables Privilege Escalation Vulnerability Apache ActiveMQ RCE Vulnerability (CVE-2023-46604) Apache Solr 's DataImportHandler (CVE-2019-0193) Redis Unauthorized RCE Confluence Unauthorized RCE (CVE-2019-3396) WebLogic RCE Vulnerability (CVE-2020-14882/14883) Log4j Vulnerability (CVE-2021-44228)

	...
Mining coins	Monero (XMR)

4.4.2 Typical Cases

- **Kinsing group exploits Looney Tunables vulnerability for attack activities**

Researchers have discovered that the Kinsing group is attempting to exploit a disclosed Linux privilege escalation vulnerability called Looney Tunables to compromise cloud environments. The Kinsing group will obtain and execute additional PHP exploits, which are deobfuscated and found to be JavaScript malicious code used to further attack activities. The JavaScript code is a web shell that allows attackers to gain backdoor access to the server, allowing them to perform file management, command execution, and collect more information about the machine running on it. Unlike the Kinsing group's previous attack mode of deploying malware and mining trojans, the ultimate goal of this attack appears to be to steal credential data [10].

- **Kinsing organization exploits CVE-2023-46604 vulnerability to conduct attack activities**

The Kinsing group is exploiting the Apache ActiveMQ RCE vulnerability (CVE-2023-46604) to conduct attacks, executing mining programs and malware on vulnerable systems. Before launching the mining program, Kinsing checks whether there are other Monero mining programs on the machine by terminating any related processes, crontabs, and network connections. After that, it establishes persistence through a cronjob, which is used to obtain the latest version of its infection script and add the rootkit to /etc/ld.so.preload[11].

4.5 Sysrv-hello

The Sysrv-hello mining trojan was first disclosed on December 31, 2020. It spreads through vulnerabilities, has no targeted targets, and has frequently updated worm samples. It is a dual-platform mining worm active on Windows and Linux. Based on its activities in the past two years, its development can be divided into three stages: early attempts to spread, mid-term expansion of spread, and late focus on defense avoidance and maintaining spread. From the analysis of samples in the three stages, it can be seen that the black industry organization behind it does not attach importance to maintaining access to the target host. It only adds the function of implanting SSH public keys in the target system in the mid-term and late Redis vulnerability exploitation; it pays more attention to revenue, expands and maintains its propagation capabilities as much as possible. Since its later mining pool connection method uses a

mining pool proxy , its comprehensive revenue situation cannot be obtained, but during March 2021, it earned an average of one Monero every two days, which is an average of US $ 100 per day at the market price at the time.

4.5.1 Organization Overview

Table 7 Sysrv-hello mining organization introduction

Organization name	Sysrv-hello	
First disclosure time	December 31, 2020	
Reason for naming	The original file names of a large number of captured samples are mainly "sysrv" strings, and the function or module paths used in the samples all contain the "hello" string.	
Threat types	Mining, worms	
Target	No special target, worm propagation targets are randomized, including cloud hosts	
Propagation pathway	Vulnerability exploitation, brute force cracking, SSH private keys stored on the victim host	
Propagation Components	Laravel Debug mode RCE (CVE-2021-3129)	XXL-JOB executor unauthorized access vulnerability
	Jenkins RCE Vulnerability (CVE-2018-1000861)	Jupyter Unauthorized Access Vulnerability
	Nexus Repository Manager 3 RCE Vulnerability (CVE-2019-7238)	ThinkPHP5 RCE Vulnerability
	WebLogic RCE Vulnerability (CVE-2020-14882)	Hadoop YARN REST API Unauthorized Vulnerability
	Supervisord RCE Vulnerability (CVE-2017-11610)	Wordpress - XMLRPC Brute Force
	JBOOS Deserialization Vulnerability (CVE-2017-12149)	SSH weak password brute force cracking
	PostgreSQL RCE Vulnerability (CVE-2019-9193)	Tomcat weak password brute force cracking
	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396)	Brute force cracking of Redis weak password
	Apache Struts2 RCE Vulnerability (CVE-2017-5638)	Nexus weak password brute force cracking
	PHPUnit RCE Vulnerability (CVE-2017-9841)	Jupyter weak password brute force cracking
	Spring Cloud Gateway Actuator RCE vulnerability	Jenkins weak password brute force

	(CVE-2022-22947)	cracking
	GitLab CE/EE RCE Vulnerability (CVE-2021-22205)	MySQL weak password brute force cracking

4.5.2 Typical Cases

- **Analysis of a typical mining family series 3 | Sysrv-Hello mining worm**

Sysrv-hello is a mining worm that exploits multiple vulnerabilities to spread on both Windows and Linux platforms. Its main purpose is to spread the mining worm and then realize mining profits. The mining worm was first disclosed on December 31, 2020. Since the original file names of a large number of captured samples are mainly "sysrv" strings, and the function or module paths used in the samples all contain the "hello" string, researchers named it Sysrv-hello. The files spread by the Sysrv-hello mining worm mainly include core scripts, worm mothers, and mining programs. The core script file types include Shell and PowerShell, which are mainly responsible for downloading and executing worms. The Linux script functions include ending competing products, defense evasion, persistence, and lateral spread. The PowerShell script focuses more on defense evasion and persistence. The worm matrix is written in Golang and uses various vulnerabilities to spread the core script, thereby achieving indirect propagation. The mining program is responsible for hijacking the computing resources of the target host to implement mining. The program is mainly released and executed by the worm matrix, but there is a period of time when the core script is responsible for downloading and executing it[12].

4.6 libgcc_a

2023, Antiy CERT received multiple mining Trojan emergency response incidents. After investigation, it was found that many emergency response incidents were related to the libgcc mining Trojan, which was mainly spread by SSH brute force cracking on Linux systems and by RDP brute force cracking on Windows systems. After infecting the victim host, the mining Trojan will also spread horizontally to further infect other hosts in the network. Use a variety of defense methods for anti-detection, such as the open source rootkit tool r77- rootkit, which has a ring 3 hiding function that can hide files, directories, processes and CPU usage, registry keys and values, services, TCP and UDP connections, connection points, named pipes and scheduled tasks. In addition, attackers use the open source Monero mining program XMRig for mining, and use the netpass tool on the Windows platform to read local plaintext RDP passwords.

4.6.1 Organization Overview

Table 8 Libgcc_a mining organization introduction

Organization name	libgcc_a /Warmup
Appearance time	2023
Targeted platform	Windows, Linux
Propagation pathway	RDP brute force cracking SSH Brute Force
Vulnerability exploited	none
Mining coins	Monero (XMR)

4.6.2 Typical Cases

- **Revealing r77 Rootkit and XMRig mining program joint deployment**

Researchers have discovered a malicious cryptominer that has been deployed in multiple countries across Asia. The attackers exploited an open source user-mode rootkit called r77. The main purpose of r77 is to hide the presence of other software on the system by hooking important Windows APIs, making it an ideal tool for stealthy attacks. By leveraging the r77 rootkit, the authors of the malicious cryptominer were able to evade detection and continue their attack campaigns [13].

4.7 Kthmimu

The Kthmimu mining trojan is mainly spread through the Log4j 2 vulnerability. Since the Log4j 2 vulnerability was exposed, the trojan's mining activities have been relatively active, spreading malicious scripts to both Windows and Linux platforms, downloading Monero mining programs for mining. The mining trojan uses PowerShell scripts on the Windows platform to download and execute the open source Monero mining program XMRig. In addition, the script also has the functions of creating persistent scheduled tasks, judging whether the system user contains key strings, and creating scheduled tasks. On the Linux platform, the trojan uses Shell scripts to download mining programs, and the script also has the functions of clearing other competing mining programs, downloading other scripts, and creating scheduled tasks.

4.7.1 Organization Overview

Table 9 Introduction to Kthmimu Mining Organization

Organization name	Kthmimu
Appearance time	March 2022
Targeted platform	Windows, Linux
Propagation pathway	Exploits
Vulnerability exploited	Apache Log4j 2 Remote Code Execution Vulnerability
Mining coins	Monero (XMR)

4.7.2 Typical Cases

- **Active Kthmimu mining trojan**

Since March 2022, Antiy CERT has captured a number of Kthmimu mining Trojan attack samples, which are mainly spread through the Log4j 2 vulnerability. Since the Log4j 2 vulnerability was exposed, the Trojan's mining activities have been relatively active, spreading malicious scripts to both Windows and Linux platforms, downloading Monero mining programs for mining [14].

4.8 aminer

In June 2023, Antiy CERT captured a batch of active mining Trojan samples through the wind-catching honeypot system. The mining Trojan mainly used SSH and Redis weak password brute force to attack the Linux platform. Since the name of the mining file downloaded in its initial script is "aminer.gz", Antiy CERT named the mining Trojan "aminer".

4.8.1 Overview of Mining Trojans

Table 10 Introduction to aminer mining Trojan

Mining trojan name	aminer
Appearance time	June 2022
Active time	May 2023
Targeted platform	Linux
Propagation pathway	SSH and Redis weak passwords

Main technical features	Persistence; IRC backdoor; hidden behavior, etc.
Mining coins	Monero (XMR)

4.8.2 Typical Cases

- **aminer mining trojan activity**

The aminer mining trojan actually consists of a series of instructions, including writing the specified DNS server address, using the yum package manager to install a series of tools and libraries, downloading the install.tgz file and decompressing it to execute the install script, downloading the ns2.jpg file and decompressing it to execute the start script to mine. The install.tgz file contains many malicious files with the same name as system files, such as top. These files are all called by the install script. Their main functions include adding SSH public keys , replacing system files such as top, netstat, crontab, etc., executing the irc client to establish a backdoor, filtering network connections with port numbers 20 and 43, etc. ns2.jpg is actually a script file written in Perl language, which is used to implement ShellBot functions. After running, it will connect to the irc server with port number 20. The aminer.gz compressed package contains mining programs for two operating system architectures. After the start script is executed, it will decide which mining program to use based on the current victim's operating system architecture, create a service for persistence, and finally execute the mining program to mine [15].

4.9 Diicot

The Diicot mining organization (also known as color1337 and Mexals) targets devices that expose port 22 on the Internet and uses SSH brute force tools to invade. After success, it uses the hosting website to send different payloads based on the device's CPU performance. When the device performance is weak, it downloads the corresponding tools and scripts from the hosting website, performs scanning and brute force cracking to spread; when the device performance is strong, it downloads the mining program to mine.

4.9.1 Organization Overview

Table 11 Introduction to Diicot mining organization

Organization name	Diicot
Appearance time	October 2022
Targeted platform	Linux
Propagation pathway	SSH Brute Force

Mining coins	Monero (XMR)
Technical features	Actively scan 22 ports; SHC encryption; clear and create scheduled tasks; change root account password; end competing programs ; execute mining programs; SSH brute force cracking;

4.9.2 Typical Cases

- **Analysis of recent attack activities of Diicot mining organization**

2023, the National Computer Network Emergency Response Technical Coordination Center (CNCERT/CC) and Antiy jointly discovered that the Diicot mining organization (also known as color1337 and Mexals) frequently launched attacks, with more than 600 servers in China being victimized. By analyzing the C2 resources used by the attackers, it was found that the attackers continuously updated the attack payloads from October 13, 2022 to May 27, 2023, adding shc encryption and other techniques to achieve the purpose of avoiding killing. Tracking and monitoring found that from March 1, 2023 to the present, the number of victim servers in China (calculated by IP number) has accumulated to more than 600 [16].

References

[1] Antiy. Analysis of the "8220" Mining Organization Activities[R/OL].(2022-04-28)
https://www.antiy.cn/research/notice&report/research_report/20220428.html

[2] FortiGuard.Old Cyber Gang Uses New Crypter – ScrubCrypt[R/OL].(2023-03-08)
https://www.fortinet.com/blog/threat-research/old-cyber-gang-uses-new-crypter-scrubcrypt

[3] TREND.8220 Gang Evolves With New Strategies[R/OL].(2023-05-16)
https://www.trendmicro.com/en_za/research/23/e/8220-gang-evolution-new-strategies-adapted.html

[4] Antiy. Analysis of Typical Mining Families Series 1: Outlaw Mining Botnet[R/OL].(2022-11-03)
https://www.antiy.cn/research/notice&report/research_report/20221103.html

[5] CYE.'Outlaw Hacking Group' Resurfaces[R/OL].(2022-05-31)
https://hackernoon.com/outlaw-hacking-group-resurfaces

[6] Antiy. Analysis of Recent Activities of WatchDog Mining Organization[R/OL].(2023-10-13)
https://www.antiy.cn/research/notice&report/research_report/WatchDogTrojans_Analysis.html

[7] CADO.Tales From the Honeypot: WatchDog Evolves With a New Multi-Stage Cryptojacking Attack[R/OL].(2022-07-02)
https://www.cadosecurity.com/tales-from-the-honeypot-watchdog-evolves-with-a-new-multi-stage-cryptojacking-attack/

[8] Aqua.Threat Alert: Anatomy of Silentbob's Cloud Attack[R/OL].(2023-07-05)
https://blog.aquasec.com/threat-alert-anatomy-of-silentbobs-cloud-attack

[9] Sentinel.Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure, GCP.[R/OL].(2023-07-13)

https://www.sentinelone.com/labs/cloudy-with-a-chance-of-credentials-aws-targeting-cred-stealer-expands-to-azure-gcp/

[10] Aqua. Looney Tunables Vulnerability Exploited by Kinsing[R/OL].(2023-11-03)
https://blog.aquasec.com/loony-tunables-vulnerability-exploited-by-kinsing

[11] TREND. CVE-2023-46604 (Apache ActiveMQ) Exploited to Infect Systems With Cryptominers and Rootkits[R/OL].(2023-11-20)
https://www.trendmicro.com/en_nz/research/23/k/cve-2023-46604-exploited-by-kinsing.html

[12] Antiy. Analysis of Typical Mining Families Series 3 | Sysrv-Hello Mining Worm[R/OL].(2023-01-12)
https://www.antiy.cn/research/notice&report/research_report/20230112.html

[13] elastic.Elastic Security Labs Steps Through the R77 Rootkit[R/OL].(2023-05-22)
https://www.elastic.co/security-labs/elastic-security-labs-steps-through-the-r77-rootkit

[14] Antiy. Analysis of the Active Kthmimu Mining Trojan[R/OL].(2022-05-27)
https://www.antiy.cn/research/notice&report/research_report/20220527.html

[15] Antiy. Analysis of the Activity of the Aminer Mining Trojan[R/OL].(2023-06-21)
https://www.antiy.cn/research/notice&report/research_report/aminer_Analysis.html

[16] CNCERT/Antiy. Analysis of Recent Attack Activities of Diicot Mining Organization[R/OL].(2023-06-28)
https://www.cert.org.cn/publish/main/11/2023/20230628101118112966101/20230628101118112966101_.html

Appendix: 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.