



A Review of Active Mining Trojans in 2024

Antiy CERT

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



First published at 17: 30, 06 February 2025

This version was updated at 17: 30 on 06 February 2025

Scan QR code for the latest
version of the report







Contents



1 General	1
2.The harm of mining Trojan	2
3.Trend of mining Trojan	2
3.1 BYOVD attacks into mining Trojan"new favorite" 2.....	2
3.2 The Rise of the Dark Net Pool Address II.....	3
3.3 Reasonable resource allocation makes it difficult for users to perceive 3.....	3
4.Introduction to active mining Trojan	4
4.1 "8220" 3.....	4
4.2outlaw4.....	5
4.3 TeamTNT5.....	7
4.4h2miner7	8
4.5libgcc _ a8	9
4.6 Perfct19	10
4.7 "hidden shovel" 10.....	12
4.8redtail11.....	13
Appendix I: Reference 12	14
Appendix II: About Antiy 13	错误!未定义书签。

1 Overview

The mining Trojanuses various means to implant the mining program into the victim's computer, and without the user's knowledge, uses the computing power of the victim's computer to mine the ore, thus obtaining illegal proceeds. In that prior art, a plurality of threat organization (for example, H2Miner, "8220," etc.) are known to propagate the mining Trojanhorse, so that the system resource of the user are occupied and consumed by malice, the life of the hardware is shortened, and the production and life of the user are seriously affected. Impairing national economic and social development. In 2024, Antiy CERT captured a number of Trojanattacks, and now the Trojan typical of 2024 is combed into an organization / family overview to share.

Table 1-1 Summary of TrojanOrganizations / Families for Active Mining in 2024 11

Mining Trojan organization / family	Time of occurrence	For platforms	An entry in the organization / family encyclopedia
"8220"	2017	Windows, Linux	
Outlaw	2018	Linux	
Teamtnt	October 2019	Linux	
H2miner	December 2019	Windows, Linux	
Libgcc_a	Aug-2021	Windows, Linux	
Perfctl	September 2023	Linux	

"Hidden shovel"	November 2023	Windows	
Redtail	Dec-2023	Linux	

2 The Harm of Mining Trojan

- Increase the resource consumption and operation risk of information system infrastructure:** Digging Trojans generally consume a large amount of resources of information system infrastructure, and slow operation of operating systems, services and application software. Even causing normal service collapse, resulting in a series of negative impacts such as interruption of bearer services and loss of business data;
- Harm the service life and operation performance of information system infrastructure:** Digging Trojan forces the information system infrastructure to run with high load for a long time, resulting in a shortened service life and a serious decline in operation performance;
- Retaining back door and deriving botnet:** Mining Trojans generally have malicious behaviors such as adding SSH password-free login back door, installing RPC back door, receiving remote IRC server instructions, and installing Rootkit back door. As a result, the network of victim organizations becomes a botnet;
- Used as a springboard to attack other targets:** Mining Trojans that allow an attacker to control a victim's server for DDoS attacks, use the server as a springboard to attack other computers, or release ransomware for ransom.

3 Mining Trojan Trends

3.1 Byovd Attacks "New Favor" of Mining Trojan.

In the emergency response to the mining Trojan event in 2024, Antiy CERT found an increase in cases of mining Trojan using a BYOVD (Bring Your Own Vulnerable Driver) attack to end the security software process. Byovd attack is a common attack technique in APT, and now mining attacks are beginning to make use of this technique. It

uses legitimate but vulnerable drivers to perform malicious operations, bypassing security safeguards. The driver runs in the kernel mode with high permission, and the attacker can realize many kinds of attack purposes through its vulnerability. In mining attacks, the attackers bypass the security mechanism of the operating system by abusing the drivers signed by the legitimate security manufacturers, and provide support for mining activities. This approach not only enhances the stealth of attacks, but also utilizes the high-authority execution capability of security software, and greatly enhances the efficiency of resources occupied by malicious mining. In the future, BYOVD attacks may be combined with zero-day exploit to further increase the complexity and destructiveness of attacks. This trend puts forward higher requirements for the security of government and enterprises, and the key points of protection should include the legitimacy detection of driver and the monitoring of running behavior.

3.2 The Rise of the Address of the Dark Net Mine Pool

In 2024, in monitoring mining attacks, Antiy CERT found that individual mining Trojans used dark web addresses for mining, such as the use of TOR by Perfct1 malware for mining. The Outlaw mining botnet adds a dark web address to the configuration file, but has not yet developed a tor to connect to. The trend suggests that attackers are accelerating the transition to more secretive, harder-to-track mining methods to escape the onslaught of traditional security and law enforcement actions. Through the Tor network or other anonymous communication protocols, mine operators can effectively hide their real location and identity, which is difficult for law enforcement to locate and outlaw. The cryptocurrency is generally used as the payment method in the dark net mine pool, and the anonymous wallet technology is used to realize the complete anonymity of the attack proceeds. With the continuous maturity of the technology of dark net mine pool, the traditional method of mining threat detection based on internet will become invalid. Governments and enterprises need to adjust protective strategies, pay attention to the characteristics analysis of mining communication and abnormal detection of dark network traffic.

3.3 Reasonable allocation of resources makes it difficult for users to perceive

In 2024, the mining Trojan will be more intelligent in resource utilization, which will be reflected in a more reasonable resource allocation strategy. For example, the app Miner mining Trojan will check whether the system environment has tools such as curl, Python and Perl, and if not, it will download and adapt, and dynamically adjust the CPU power or resource use parameters on different systems. The Outlaw mining botnet will acquire the system architecture of the target host, and adjust the default thread count according to the system architecture. the number of arm architecture threads is set to 75, the number of i686 architecture threads is set to 325, and the number of other architectures is set

to 475. This trend not only increases mining efficiency, but also greatly increases the perceived risk of mining Trojans being found. Intelligent resource allocation dynamically adjusts the utilization rate of CPU and GPU according to the system load to avoid equipment abnormality or user's attention. The mining process is designed to be a low priority task, making full use of resources when the equipment is idle and reducing consumption when the user is active, thus extending the mining cycle. This trend of intelligent resource allocation makes mining Trojan more hidden and persistent, and becomes the difficult point of network threat protection.

4 Introduction of active mining Trojan

4.1 "8220"

"8220" is an organization that has long been active and adept at exploiting vulnerabilities and deploying mining programs, early on using Docker images to disseminate mining Trojan, and then gradually using multiple vulnerabilities to attack. Such as WebLogic vulnerability, Redis unauthorized access vulnerability, Hadoop Yarn unauthorized access vulnerability and Apache Struts vulnerability. In 2020 found that the group began using SSH brute force for horizontal attack propagation. Since the Apache Log4j 2 remote code execution vulnerability was exposed, the organization has used the vulnerability to create a vulnerability and use a script to spread it, with a wide range of impacts.

4.1.1 Organizational Overview

Table 4-1 Introduction to "8220" Mining Organization 4

Organization name	"8220"
Time of occurrence	2017
For platforms	Windows, Linux
Mode of transmission	Ssh brute force cracking, Docker mirroring and exploit
Exploited vulnerabilities	Apache Log4j 2 remote code execution vulnerability Oracle WebLogic vulnerability Atlassian Confluence vulnerability Redis unauthorized access vulnerability Hadoop Yarn unauthorized access vulnerability Apache Struts vulnerability

Excavation
currency

Menlo coins (XMR)

4.1.2 Typical Cases

- **Analysis of Attacks against Oracle WebLogic Vulnerabilities**

Water Sigbin (8220 Gang) is a threat actor focused on deploying cryptocurrency mining malware that aggressively targets Oracle WebLogic servers. The threat actor exploited vulnerabilities in Oracle WebLogic Server (specifically CVE-2017-3506 and CVE-2023-21839) to deploy cryptocurrency mining programs through PowerShell scripts. The researchers analyzed the multi-stage loading technique used to pass the PureCrypter loader and the XMRIG encryption miner. All payloads used during this activity are protected with .net Reactor, a .net code protection software, to prevent reverse engineering. This protection obfuscates the code, making it difficult for defenders to understand and copy. In addition, it employs anti-debug techniques. The payload is delivered by using CVE-2017-3506 [1].^[1]

- **New toy of 8220 mining gang: K4spreader**

On June 17, 2024, researchers found an ELF sample written in c language using VT 0 testing, this sample using anamorphic upx shelled, and after shelling, they got another anamorphic upx shelled elf file. Write in cgo mode. After analysis, it was found that this is a new tool from the "8220" mining gang to install other malware to execute, mainly building the Tsunami DDoS botnet and installing the PwnRig mining program. According to the name of the function in the sample, we named it as "k4spreader." After further analyzing the data of VT and honeypot, we find that k4spreader is still in the development stage, but there are three variants [2].^[2]

4.2 Outlaw

The Outlaw mining botnet was first discovered in 2018, with mining attacks mainly targeting cloud servers and continuing to be active. Suspected to be from Romania, it was first named Outlaw by Trend Technologies and translated as "Outlaw" in Chinese. When the mining botnet was first discovered, attackers built robots using a backdoor program in Perl scripting language, hence the name Shellbot. The main propagation path is SSH brute force attack target system and write SSH public key in order to achieve long-term control target system goal, and at the same time download the back door based on Perl script language and open-source Menlo coin mining Trojan.

4.2.1 Organizational Overview

Table 4-2 Introduction to Outlaw Mining Botnet 41

Organization name	Outlaw
Organization Introduction	A botnet that spreads Shellbot written based on Perl through exploit and SSH brute force cracking, and later starts to put mining Trojan to profit
Time of initial disclosure	November 1, 2018
First Disclosure of Manufacturer	Trend technology
Country of attribution	Suspected to be Romania
Reason for naming	Derived from the Romanian translation of Haiduc, the group's main hacking tool is Haiduc
Type of threat	Botnets, mining trojans
Targeting	Linux, IoT
Route of transmission	Shellshock (CVE-2014-7169) vulnerability, Drupalgeddon2 vulnerability (CVE-2018-7600) vulnerability and SSH brute cracking are mainly adopted, and vulnerability exploitation is only used in the initial stage
Organizational components	Hidden process tool (XHide), SSH brute force crack tool (Haiduc, ps, tsm), Shellbot program, mining Trojan(XMRig)
Version iteration	There are 5 iterations of the botnet sample, the main differences are the addition of functions, the replacement of cracking tools, and the changes in the functions of cracking tools

4.2.2 Typical Cases

- **Analysis of recent activity of outlaw mining botnet**

Antiy CERT monitored a number of Outlaw mining botnet attacks, which were discovered as early as in 2018, mainly engaged in mining activities for cloud servers, and remained active. In its analysis of recent attacks, Antiy CERT found that the mining botnet sample has been significantly updated from the third version, with more diverse functions, higher stealth and more difficult to remove. The main propagation path and function is still SSH brute force attack target system, embedding SSH public key to achieve the goal of long-term control target system, At the same time, download and execute the backdoor and open-source Menlo coin mining Trojan written based on Perl scripting language, and use scanning and brute force cracking tools to attack other hosts accordingly [3].^[3]

4.3 Teamtnt

The TeamTNT mining organization was first identified in 2019 and targeted attacks on Docker Remote API unauthorized access vulnerabilities, incorrectly configured Kubernetes clusters and Redis service brute force cracking. After the successful invasion, it will steal all kinds of login credentials and leave back doors, mainly using target system resources to dig mines and build a botnet. In recent years, the botnet controlled by the group has grown to a large scale and used attack components that are updated frequently, making it one of the main attack groups currently mining Linux servers. The group, which is suspected to be from Germany, was named after the group's original use of the name teamtnt .red.

4.3.1 Organizational Overview

Table 4-3 Introduction to excavation organization of TeamTNT 4

Organization name	Teamtnt
Time of initial disclosure	October 2019
Country of attribution	Germany
Reason for naming	First to use the domain name teamtnt. red
Type of threat	Mining Trojanhorse, back door
Targeting	Jupiter Lab, Docker, Kubernetes and Redis
Route of transmission	Incorrect configuration and SSH credentials, etc
Organizational armoury	Tsunami, Rathole, Ezuri, Punk.py, libprocessshider, tmate, masscan, pnsan, ZGrab, Tiny Shell, Mimipy, BotB, Diamorphine, Docker Escape Tool and others
The organization excels in technology	Scan LAN ports, add firewall rules, delete other competitor processes, create persistence schedule tasks, steal service credentials, collect machine information, Rootkit hide processes, deploy mining programs, and move sideways
Twitter account	Hildegard @ TeamTNT @ HildeTNT
Github account	Hilde @ TeamTNT Hildeteamtnt
Hosting website	Teamtnt.red

4.3.2 Typical Cases

- **Teamtnt launched a new round of attacks**

Researchers found that TeamTNT was planning a new attack. In this attack, TeamTNT appears to be returning to its roots, preparing for a massive attack on the cloud environment. The group currently targets the exposed Docker daemon, deploying Sliver malware, web worms and encryption miners, using infected servers and Docker Hub as the infrastructure to spread the malware. At the event, TeamTNT used the Docker Hub to store and distribute malware by attaching infected instances of Docker to Docker Swarm. They also rent the victim's computing power to third parties, effectively making money indirectly through cryptocurrency mining without having to manage it themselves. In addition, they have adopted new hacking tools, replacing the traditional Tsunami backdoor with more covert Sliver malware [4].^[4]

- Dark clouds on the horizon: The recovery of TeamTNT?**

The researchers found clear evidence of TeamTNT's new activity affecting the CentOS operating system-based VPS cloud infrastructure. The investigation revealed that the initial access was through a secure shell (SSH) brute force attack on the victim's assets, during which the threat actor uploaded malicious scripts. Malicious scripts disable safety features, delete logs, and modify system files when searching for existing miners. It also terminates the cryptocurrency mining process, deletes the Docker container, and updates the DNS settings for Google's servers. Install the Diamorphine toolkit for hiding and root permissions, and use custom tools to maintain persistence and control. The system is locked by modifying file properties, creating a backdoor user with root access, and deleting command history to hide its activities [5].^[5]

4.4 H2miner

H2miner mining Trojan first appeared in December 2019, and in the early stage of the outbreak and the subsequent period, the Trojan was aimed at the Linux platform until after November 2020. Started to use WebLogic vulnerability against the Windows platform to invade and implant the corresponding mining program. In addition, that mine Trojan frequently exploits other common Web component vulnerability to invade related servers and implant mining programs. For example, in December 2021, attackers implemented the launch of the H2Miner mining Trojan using the Log4j vulnerability.

4.4.1 Organizational Overview

Table 4-4 Introduction to H2Miner Mining Organization 4-2

Organization	H2miner / Kinsing
---------------------	-------------------

name	
Time of occurrence	December 2019
For platforms	Windows, Linux
Mode of transmission	Exploit vulnerabilities
Exploited vulnerabilities	Looney Tunables privileged upgrade vulnerability Apache ActiveMQ RCE vulnerability (CVE-2023-46604) Apache Solr's DataImportHandler (CVE-2019-0193) Redis does not authorize RCE Confluence Not Authorised RCE (CVE-2019-3396) Weblogic RCE vulnerability (CVE-2020-14882 / 14883) Log4j vulnerability (CVE-2021-44228) .
Excavation currency	Menlo coins (XMR)

4.4.2 Typical Cases

- **The Kinding organization integrates newly disclosed vulnerabilities into a vulnerability exploitation library and expands its botnet**

The Kinding organization integrates newly disclosed vulnerabilities into a vulnerability exploitation library and expands its botnet. The group has actively planned illegal cryptocurrency mining activities since 2019. In recent year, Activities involving Golang-based malware have exploited various flaws in Apache ActiveMQ, Apache Log4j, Apache NiFi, Atlas Confluence, Citrix, Liferay Portal, Linux, Openfire, Oracle WebLogic Server and SaltStack to compromise vulnerable systems [6].^[6]

4.5 Libgcc _ a

Libgcc _ a mining Trojanis propagated by SSH brute force attack on Linux system, and by RDP brute force attack on Windows system. Mining Trojanin the affected host after infection, but also will carry on the horizontal transmission further infection network other host. Use a variety of defense methods for anti-detection, such as the open source rootkit tool r77-rootkit, which has ring 3 hiding capability, You 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, that attack uses the open-source Menlo coin mine program XMRig to mine, and uses the netpass tool to read the local plaintext RDP password on the Windows platform.

4.5.1 Organizational Overview

Table 4-5 Libgcc _ a Mining Organization Introduction 4-3

Organization name	Libgcc _ a
Time of occurrence	2023
For platforms	Windows, Linux
Mode of transmission	Rdp brute force attack Ssh brute force attack
Exploited vulnerabilities	None
Excavation currency	Menlo coins (XMR)

4.5.2 Typical Cases

● Analysis and Disposal of Libgcc _ a Mining TrojanHorse

Recently, the safety service center of Antiy has received security service orders from multiple users, and the protection equipment deployed in the user network has generated a large number of violent attack alarms, and the user business system has run the Caton. According to the evidence collected by the emergency response team of Antiy Security Service Center, it was found that the Trojan was infected with Libgcc _ a mining trojan, which was specially designed for Linux system and could be horizontally infected and controlled by SSH weak password. Strong self-concealment capability. The actions after infection include downloading the mining program to mine, adding the back door of the system, scanning the intranet for further infection, removing the security software and competitors, etc. the Trojan has a modular function and a strong attack automation. It has been improved in the aspects of self-persistence, behavior hiding and anti-reconnaissance, and it is difficult to find the infection in the traditional way [7].^[7]

4.6 Perfctl

Perfctl is a type of Linux-side malware that has been infecting Linux servers and workstations without being widely detected for at least the past three years. The malware exploits vulnerabilities and misconfigurations to invade the system, and the main purpose is to mine Menlo coins through the server's CPU resources. Perfctl uses rootkit technology to evade detection and uses TOR to encrypt communications to hide its activities. After infection, the malware not only hides its processes, it also stops mining when users log in, making it difficult to detect.

4.6.1 Organizational Overview

Table 4-6 Introduction to mining organization of Perfctl 4-4

Organization name	Perfctl
Time of occurrence	September 2023
For platforms	Linux
Mode of transmission	Exposed Docker Remote API Services and Vulnerability Exploitation
Exploited vulnerabilities	Rocketmq vulnerability (CVE-2023-33246) Polkit vulnerability (CVE-2021-4034)
Excavation currency	Menlo coins (XMR)

4.6.2 Typical Cases

- **Behind the Linux malware "Perfctl" lies years of cryptocurrency mining**

The researchers found that Linux malware, called "Perfctl," has been infecting Linux servers and workstations without widespread detection for at least the past three years. The malware exploits vulnerabilities and misconfigurations to break into the system, with the main goal being to mine Monero through the server's CPU resources. Perfctl uses rootkit technology to evade detection and uses TOR to encrypt communications to hide its activities. After infection, the malware not only hides its processes, it also stops mining when users log in, making it difficult to detect. It is estimated that thousands of servers have been infected [8].^[8]

- **The attackers deployed the Perfctl malware using the exposed Docker API**

The researchers found that the attackers deployed the Perfctl malware through exposed Docker remote API servers. An attacker first probes the target server, then uses the Docker API to create a privileged container that executes a Base64-encoded malicious payload. The payload contains the steps of escaping the container, creating a malicious script, setting environment variables, and downloading a malicious binary masquerading as a PHP extension. In addition, that attack uses a variety of circumvent detection techniques, such as checking for duplicate processes, creating a camouflage directory, and circumventing the protection mechanism through custom download functionality. To achieve persistence, malware creates system services or scheduled tasks [9].^[9]

4.7 "Hidden shovel"

The "hidden shovel" mining Trojan has been around since November 2023, with several component upgrades during the process, currently version 3.0. The mining Trojan attacks continued to be active, and the infection volume was on the rise. The main features are strong concealment, anti-analysis, DLL backdoor hijacking and shellcode injection. In the discovered attack activity, the attacker utilized two relatively novel techniques to combat the anti-virus software, The first technique is to abuse functionality in an older version of the kernel driver of the antivirus software to end the antivirus software and the edr, This technique is done with a main PowerShell script, a standalone PowerShell script, and a controller (a small executable that is loaded in memory). The PowerShell script of the main body is used to download and install the kernel driver of the old version of the anti-virus software, the independent PowerShell script is used to decrypt and load the memory of the controller, and the controller is used to control the kernel driver. Although the old version of the kernel driver that was abused has long been updated, it can still be used illegally and effectively end most antivirus software. The second technique is to use MSDTC to load backdoor DLL to realize self-starting backdoor and achieve the goal of persistence. This technique utilizes the mechanism of the MTxOCI component in the MSDTC service. after the MSDTC service is turned on, the component will search for oci.dll. Windows system does not contain oci.dll. by default. The attacker will download the backdoor DLL, rename it oci.dll and put it in the specified directory, and create the MSDTC service through the command in the PowerShell script, so the service will load the oci.dll backdoor and form the persistence operation.

4.7.1 Organizational Overview

Table 4-7 Introduction to "hidden shovel" mining organization 4-5

Organization name	"Hidden shovel" / GHOSTENGINE
Time of occurrence	November 2023
For platforms	Windows
Mode of transmission	Disguised as a legitimate program
Exploited vulnerabilities	None
Excavation currency	Menlo coins (XMR)

4.7.2 Typical Cases

- Analysis of "hidden shovel" mining Trojanactivity

The "hidden shovel" mining Trojan will first download the PowerShell script named "get .png" from the horse release server, and perform operations such as hash verification, creating scheduled tasks, disabling the system's anti-virus software and creating services after decoding. After that, the script "kill .png" and the compressed files "delete .png" and "kill (1) .png" will be downloaded, and the script will decode the shellcode. The shellcode code is decrypted to get the controller (an executable file) and injected into the process of powershell. exe, After the two compressed files are decompressed, the old versions of kernel drivers "aswArPots. sys" and "IObitUnlockers. sys" of anti-virus manufacturers are obtained, which are called by the controller to terminate the anti-virus software and the EDR program. According to the system model of the victim host, the corresponding "86 / 64.png" compressed file will be downloaded, and after decompression, the oci.dll file will be obtained, and DLL hijacking backdoor will be realized through MSDTC service call. In the "get .png" script, I also see the address of downloading the "backup .png" script, but the download function has not been implemented, and it may be added in a later version, and the main function of this script is to send heartbeat receive command. Finally, the "get .png" script will download the "smartscreen.exe" program, which will download the mining program and its components for mining [10].^[10]

- **Invisible miner: Revealing the secret of GHOSTENGINE's cryptocurrency mining operation**

Researchers have discovered a set of intrusions that contain multiple malicious modules and exploit vulnerable drivers to disable known security solutions (EDRs) for cryptographic mining. In addition, the team discovered the ability to build persistence, install previously unrecorded backdoors, and execute encryption mining programs. The researchers call this intrusion set REF4578 and the main payload GHOSTENGINE [11].^[11]

4.8 Redtail

The RedTail mining Trojan is a type of malware that uses system vulnerabilities to spread and implement cryptocurrency mining. It intrudes into the target system through a variety of high-risk vulnerabilities (such as Palo Alto Networks firewall vulnerability, TP-Link router vulnerability), and embeds a variant of XMRig mining program to mine Menlo coins. The Trojan is highly concealed and adopts encryption configuration, anti-debugging technology and dynamic adjustment of mining parameters to avoid easy detection and ensure mining efficiency. It also supports multi-platform architectures and can optimize its operation based on system resources. Not only will RedTail take up a large amount of system resources, resulting in slow operation of the device and increased electricity bills, but it may also become a portal for further intrusions by attackers, bringing serious security risks.

4.8.1 Organizational Overview

Table 4-8 Introduction to RedTail Mining Organization 4-6

Organization name	Redtail
Time of occurrence	Dec-2023
For platforms	IoT, Linux
Mode of transmission	Exploit vulnerabilities
Exploited vulnerabilities	Pan-OS (CVE-2024-3400) vulnerability Ivanti Connect Secure SSL-VPN (CVE-2023-46805, CVE-2024-21887) vulnerability Tp-Link Router (CVE-2023-1389) Vulnerability Vmware Workspace ONE Access and Identity Manager (CVE-2022-22954) vulnerability Thinkphp remote code execution (CVE-2018-20062) vulnerability
Excavation currency	Menlo coins (XMR)

4.8.2 Typical Cases

- The RedTail mining group used the PAN-OS (CVE-2024-3400) vulnerability to launch an attack

In May 2024, researchers revealed that the RedTail Mining Organization had included Palo Alto's PAN-OS CVE-2024-3400 vulnerability in its attack kit. The vulnerability allows an attacker to create arbitrary files on the victim system by manipulating the SESSID cookie and using the path traversal technology to execute commands. Targets of the attack include IoT devices such as TP-Link routers, the ThinkPHP content management system, and security devices such as Ivanti Connect Secure and Palo Alto GlobalProtect. The attackers spread the malware through multiple vulnerabilities with the ultimate aim of cryptographically mining the Monero (XMR) digital currency [12].^[12]

Appendix I: Reference Materials

- [1] Trend.examining Water Sigbin's Infecting Routine Leading to an XMRig Cryptominer [R / OL]. (2024-06-28)
https://www.trendmicro.com/en_us/research/24/f/water-sigbin-xmag.html
- [2] Qianxin. 8220 New Toy of the Mining Gang: K4spreader [R / OL]. (2024-06-25)
<https://blog.xlab.qianxin.com/8220-k4spreader-new-tool-cn/>

- [3] Antiy.outlaw Mining Botnet Recent Activity Analysis [R / OL]. (2025-01-10)
[https://www.antiy.cn/research/notice & report/research _ report/Outlaw _ Analysis.html](https://www.antiy.cn/research/notice%20&%20report/research_report/Outlaw_Analysis.html)
- [4] Aqua.teamtnt's Docker Gatling Gun Campaign [R / OL]. (2024-10-25)
<https://www.aquasec.com/blog/treat-alert-teamtnts-docker-gating-gun-campaign/>
- [5] Group-IB.Storm contacts on the horizon: Recovery of TeamTNT? [R / OL]. (2024-09-18)
<https://www.group-ib.com/blog/teamtnt/>
- [6] Aqua.kinsing Demystified [R / OL] (2024-05-21)
[https://1665891.fs1.hubspotusercontent-na1.net/hubfs/1665891/Threat% 20reports/AquaSecurit
y_Kinning_Demystified_Technical_Guide.pdf](https://1665891.fs1.hubspotusercontent-na1.net/hubfs/1665891/Threat%20reports/AquaSecurity_Kinning_Demystified_Technical_Guide.pdf)
- [7] Antiy.dry Goods Sharing a Libgcc _ a Mining TrojanAnalysis and Disposal [R / OL] (2024-03-13)
<https://mp.weixin.qq.com/s/2UhXr3up-5cW3BrP6njxw>
- [8] Aqua.perftcl: A Stealthy Malware Targeting Millions of Linux Servers [R / OL] (2024-10-03)
<https://www.aquasec.com/blog/perftcl-a-stealthy-malware-targeting-millions-of-linux-servers/>
- [9] Trend.attackers Target Exposed Docker Remote API Servers With perftcl Malware [R / OL] (2024-10-21)
[https://www.trendmicro.com/en _ hk/research/24/j/attackers-target-exposed-doc-remote-api-servers-
with-perftcl.html](https://www.trendmicro.com/en_hk/research/24/j/attackers-target-exposed-doc-remote-api-servers-with-perftcl.html)
- [10] Antiy. "Hidden shovel" mining Trojanactivity analysis [R / OL] (2024-05-10)
[https://www.antiy.cn/research/notice & report/research _ report/HideShoveling.html](https://www.antiy.cn/research/notice%20&%20report/research_report/HideShoveling.html)
- [11] Elastic.invisible miners: Unchecked GHOSTENGINE's crypto mining operations [R / OL] (2024-05-22)
[https://www.elastic.co.uk/security-labs/invisible-miners-unveiling-ghost engine](https://www.elastic.co.uk/security-labs/invisible-miners-unveiling-ghost-engine)
- [12] Akamai.redtail Cryptominer Threat Actors Adopt PAN-OS CVE-2024-3400 Exploit [R / OL] (2024-05-30)
<https://www.akamai.com/blog/security-research/2024-redtail-crypto-pan-os-cve-exploit>

Appendix II: 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 cyberspace 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.