Analysis of the aminer Mining Trojan Activity

Antiy CERT

Draft completed: June 14, 2023
First published: September 21, 2023

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

1 aminer Mining Trojan

Recently, Antiy CERT captured a batch of active mining trojan samples through Attack Capture System[1]SSH and Redis weak password brute force. Because the name of the mining file downloaded in its initial script is "aminer.gz", Antiy CERT named this mining trojan "aminer".

Table 1-1 aminer mining overview

Active mining overview	Explanation
Mining trojan name	aminer
The main method of spreading mining trojans	SSH and Redis weak password brute force attacks
Appearance time	June 2022
Active time	May 2023
Mining currency	Monero
Targeting the system	Linux
Main technical features	Persistence; IRC backdoor; hidden behavior, etc.

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

2 Sample Function and Technology Review

The aminer mining trojan actually consists of a series of instructions, including writing the specified DNS server address, installing a series of tools and libraries using the yum package manager, downloading the install.tgz file and decompressing it before executing the install script, downloading the ns2.jpg file and executing it in memory, and downloading the aminer.gz file and decompressing it before executing the start script to mine.

The install.tgz file contains many malicious files with the same names as system files, such as "top". These files are called by the install script. Their main functions include adding SSH public keys, replacing system files such as "top", "netstat", and "crontab", executing an IRC client to establish a backdoor, and filtering network connections to ports 20 and 43.

ns2.jpg is actually a script file written in Perl language, used to implement Shell Boot functionality. When run, it connects to an IRC server on port 20. The aminer.gz compressed package contains mining programs for two operating system architectures. After executing the start script, it determines which mining program to use based on the victim's operating system architecture, creates a persistent service, and finally executes the mining program to mine.

2.1 oto (Initial Attack Script)

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

1. Enter the DNS server address, including "114.114.114.114", "114.114.115.115", "8.8.8.8", and "1.1.1.1".
2. Install a series of tools and libraries, including gcc, cmake, wget, curl, nano, etc.
3. The memory executes ns2.jpg , which is actually a script file written in Perl language Shell Boot. After running, it will connect to the IRC server (irc.tung-shu.cf), the port number is 20, and the channel is #ROOT.
4. Use the start script to execute the mining program for mining. The mining pool address is 3389.xiao.my.id:3389.

2.2 install.tgz (Persistence)

The install.tgz compressed package contains many files. The functions of each file are shown in the following table:

Table 2-1 Functions of each file in install.tgz

File name	Function

authorized_keys	SSH key storage file
cleaner.c	Cleaning tool
crond.c	IRC client
crontab	Determine whether it is root permission
decode.c	Read the contents of the file /usr/share/boot.sync
execute	Initialize and run the monitor sample, and enable and start the crond and cron services
flush	Configure access rules for the SSH service to only allow connections using the added public key
install	Persistence Operations
monitor.c	IRC client
netstat	Filters network connections with port numbers 20 and 43 , as well as network connections containing the strings "send", "dhcl", and "sendmail".
top	Execute the replaced flush and execute commands
where.c	IRC client
whereis	Run the whereos file and execute malicious commands in the background

3 Mining Trojan Detection and Removal Solution

3.1 Identification of Mining Trojans

1. Account name:

- more /etc/sudoers | grep -v "^#|^$" | grep "ALL=(ALL)"

Note: Use the command to check whether other accounts besides the root account have sudo permissions.

- daemon

Note: A malicious account that allows the daemon user to execute any command without entering a password.

2. Unauthorized SSH public key:

- /root/.ssh/authorized_keys
- /usr/sbin/.ssh/authorized_keys
- /sbin/.ssh/authorized_keys

3. Files and directories:

- /root/.ssh
- /bin/crond
- /bin/where
- /bin/execute
- /bin/monitor
- /bin/netstat
- /bin/flush
- /bin/clean
- /sbin/.ssh

- /sbin/nologin
- /usr/sbin/.ssh
- /usr/sbin/nologin
- /usr/bin/netstatz
- /usr/bin/crontab
- /usr/bin/power
- /usr/bin/whereis
- /usr/bin/whereos
- /usr/bin/top
- /usr/sbin/top
- /usr/sbin/baca
- /etc/cron.d
- /etc/cron.daily
- /etc/cron.hourly
- /etc/cron.monthly
- /etc/cron.weekly
- /etc/sudoers
- /var/lib/dhclient/dhclient
- /var/lib/dhclient/config.json
- /usr/local/src/*

4. Service execution path:

```
[Unit]
Description=SDCard System Service
[Service]
User=sshd
ExecStart=/var/lib/dhclient/dhclient
Restart=always
Nice=10
[Install]
WantedBy=multi-user.target
```

5. Process name:

- CROND
- crond
- dhclient

6. Network

- 3389.xiao.my.id:3389
- irc.tung-shu.cf:20
- mircd.xiao.my.id.id

3.2 Removal Plan

1. Delete the SSH public key

- chattr -ia /root/.ssh/authorized_keys /usr/sbin/.ssh/authorized_keys /sbin/.ssh/authorized_keys
- rm /root/.ssh/authorized_keys /usr/sbin/.ssh/authorized_keys /sbin/.ssh/authorized_keys

2. Deleting a service
- rm /etc/systemd/system/sdcard.service

3. Deleting files and directories
- chattr -ia /root/.ssh /bin/crond /bin/where /bin/execute /bin/monitor /bin/netstat /bin/flush /bin/clean /sbin/.ssh /sbin/nologin /usr/sbin/.ssh /usr/sbin/nologin /usr/bin/netstatz /usr/bin/crontab /usr/bin/power /usr/bin/whereis /usr/bin/whereos /usr/bin/top /usr/sbin/top /usr/sbin/baca /etc/cron.d /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly /etc/cron.daily/cron.daily /etc/cron.hourly/cron.hourly /etc/sudoers
- rm -rf /root/.ssh /bin/crond /bin/where /bin/execute /bin/monitor /bin/netstat /bin/flush /bin/clean /sbin/.ssh /sbin/nologin /usr/sbin/.ssh /usr/sbin/nologin /usr/bin/netstatz /usr/bin/crontab /usr/bin/power /usr/bin/whereis /usr/bin/whereos /usr/bin/top /usr/sbin/top /usr/sbin/baca /etc/cron.d /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly /etc/cron.daily/cron.daily /etc/cron.hourly/cron.hourly /etc/sudoers

4. Delete mining program
- rm -rf /var/lib/dhclient/dhclient /var/lib/dhclient/config.json /usr/local/src/*

5. End a process
- dhclient
- crond
- CROND

6. Restart the operating system
- Because the malicious code is executed in memory and does not land on the ground, the operating system needs to be restarted.

7. Precautions
- Because the mining trojan replaces files such as top and netstat in the operating system, the removal solution will delete the maliciously replaced files. If you need to use these commands, you need to reinstall them.

4 Protective Recommendations

In response to mining attacks, Antiy recommends that companies take the following protective measures:

1. Windows/Linux version of Antiy Intelligent Endpoint Protection System;

2. Strengthen SSH passwords: Avoid using weak passwords. It is recommended to use passwords that are 16 characters or longer, including a combination of uppercase and lowercase letters, numbers, and symbols. Also, avoid using the same password on multiple servers.

3. Update patches in a timely manner: It is recommended to enable the automatic update function to install system patches, and the server should update system patches in a timely manner;

4. Update third-party application patches in a timely manner: It is recommended to update third-party application patches such as Redis in a timely manner;

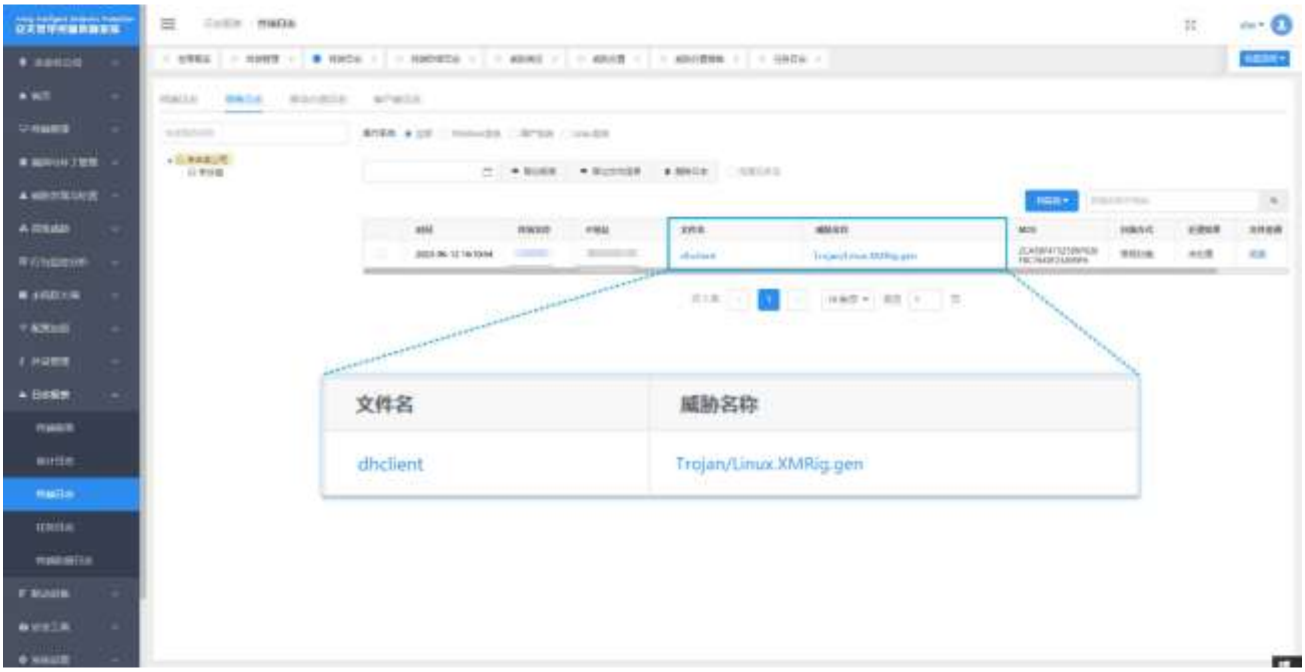
5. Enable logs: Enable key log collection functions (security logs, system logs, error logs, access logs, transmission logs, and cookie logs) to provide a basis for tracing security incidents.

6. Host reinforcement: perform penetration testing and security reinforcement on the system;

7. Deploy an Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracing of malicious code. Antiy Persistent Threat Detection System (PTD) uses network traffic as the detection and analysis object, and can accurately detect a large amount of known malicious code and network attack activities, effectively discovering suspicious network behavior, assets, and various unknown threats;

8. Antiy Service: If you are attacked by malware, it is recommended to isolate the attacked host in a timely manner and protect the site while waiting for security engineers to investigate the computer; Antiy 7*24 hour service hotline: 400-840-9234.

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



文件名	威胁名称
dhclient	Trojan/Linux.XMRig.gen

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 deploying the mining Trojan, Antiy sorted out the ATT&CK mapping map corresponding to this attack incident as shown in the figure below.

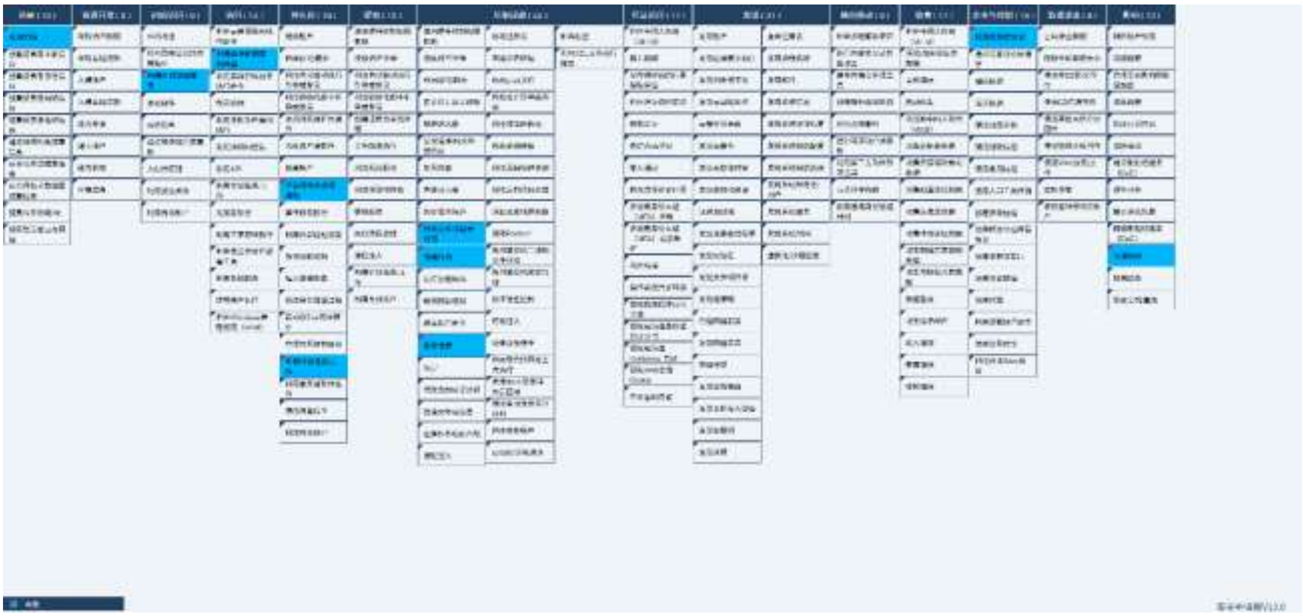


Figure 5-1 ATT&CK mapping diagram corresponding to the incident

The following table lists the techniques used by attackers.

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

ATT&CK Stage/Category	Specific behavior	Notes
Reconnaissance	Active scan	Scan ports 22 and 3306
Initial access	Leverage external remote services	Remote service access using SSH
Execute	Utilize command and script interpreters	Use shell scripts
Persistence	Create or modify system processes	Create a Service
	Work with scheduled tasks	Create a scheduled task
Defense Evasion	Modify file and directory permissions	Modify file and directory permissions
	Hidden behavior	Hidden process
	Deleting a beacon	Delete the malicious file itself
Command and Control	Use application layer protocols	Use the IRC protocol
Influence	Resource hijacking	Occupies CPU resources

6 IoCs

IoCs
124.70.7.7
hxxp://124.70.7.7/install.tgz
hxxp://124.70.7.7/ns1.jpg
hxxp://124.70.7.7/ns2.jpg
hxxp://124.70.7.7/ns3.jpg
hxxp://124.70.7.7/aminer.gz
3389.xiao.my.id:3389
irc.tung-shu.cf:20
mircd.xiao.my.id.id
mircd.hokkien.my.id
6AFD902FCBACBAFE7375E3C885741139
AB1D9528DAC5A2B42CCFC737DE5D0E8A
C4983A3AFD6E9C09B1E4C6CB59EEDE81
311A7ED77DEFEB0BB99CAA5E46A1CB0B
3D55920BABFB2B880D83282CF6B30E5D

Appendix 1: References

[1]. Antiy Product Tour (Series 5) - Attack Capture System

https://www.antiy.cn/About/news/20200312.html

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.