2022 Active Mining Trojan Review

Antiy CERT

First draft completed: January 17, 2023

First published time: February 8, 2023

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, "8220", H2Miner, 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 2022, Antiy CERT released several analysis reports on mining Trojans. Now we will sort out the typical mining Trojans in 2022 into a family overview for sharing.

Mining Trojan Family	Appearance Time	Targeted Platform
"8220"	2017	Windows, Linux
Outlaw	2018	Linux
TeamTNT	October 2019	Linux
H2Miner	December 2019	Windows, Linux
Sysrv-hello	December 2020	Windows, Linux
"1337"	December 2021	Linux
Kthmimu	March 2022	Windows, Linux
Hezb	May 2022	Windows, 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 More and More Mining Trojans Have Mastered the Ability to Quickly Integrate Vulnerabilities

As the means of combating mining trojans become more despicable, more and more mining trojan gangs have mastered the ability to quickly integrate vulnerabilities. Mining trojans not only attempt to fight security products, but also to block competition from peers. In other words, whoever can quickly integrate vulnerabilities first will have priority access to the public network computing power with vulnerabilities, and thus obtain corresponding profits. Whenever a vulnerability with a wide impact appears, it is difficult for all affected devices on the entire network to complete the vulnerability repair in a short period of time, which gives mining trojans an opportunity to take advantage.

3.2 Mining Trojans Are Becoming More Hidden, And Traditional Intelligence Detection Will Gradually Become Ineffective

Mining Trojans usually use two methods to mine, one is to mine directly in the mining pool, and the other is to mine through the mining pool agent. Mining Trojans directly connected to the mining pool usually let the victim's host directly connect to the mining pool address to upload the computing power results. The mining pool platform will send the reward to the wallet of the mining Trojan gang according to the contributed computing power. The disadvantage of this method is that security analysts can obtain the wallet address of the mining Trojan gang by analyzing the attack script, etc., and can find the direct public mining pool address. Then, by entering the corresponding mining Trojan gang's wallet address through the public mining pool website, you can find out how many victims are passively mining, the current total hash of the contributed computing power, and how many Monero coins are produced. The mining pool agent can easily solve the above disadvantages, that is, add a transfer link between the miner and the mining pool. The mining pool agent obtains the task from the public mining pool and transfers it to the miner for calculation. The miner transfers the calculation result to the mining pool agent, and then forwards it to the public mining pool. The popularity of mining pool proxies will conceal the actual public mining pools used for mining, which can bypass traditional intelligence mining pool blacklist detection and make traditional blacklist detection ineffective.

3.3 Driven by Relatively Stable Profits, More Threat Groups Are Starting to Carry out Mining Attacks

2022, the entire virtual currency market suffered a huge impact, and the prices of almost all currencies fell. Take Bitcoin as an example. In January, the price of each Bitcoin was close to US$ 48,000, but in November, the price of each Bitcoin was only US$ 17,000, a drop of 64.58 %. Despite this, mining attacks have not decreased, but have become more active. The most commonly mined currency in mining attacks is Monero. Compared with other currencies, Monero is more stable, which is also favored by other ransomware organizations. For example, AstraLocker ransomware shut down the ransomware attack and turned its business to mining attacks. This shift is likely that the ransomware organization wants to earn virtual currency in a more low-key and covert way. After governments have strengthened their defense and law enforcement against ransomware, the profits of ransomware organizations have been greatly reduced. The way to earn ransom mainly depends on communicating with victims. In serious cases, they may be suppressed by governments. Mining attacks can earn virtual currency without the

victim's knowledge, which is relatively low risk for ransomware organizations. Although it is not as profitable as forcing victims to pay ransom, mining attacks earn virtual currency at almost zero cost, without worrying about electricity prices or computing power , and can earn lucrative rewards. Therefore, Antiy CERT believes that more threat organizations will implement this low-risk, high-return mining attack in the future.

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 Family Overview

Table 4-1 Introduction to the "8220" mining organization

Mining Trojan Family	"8220"
Appearance Time	2017
Targeted Platform	Windows, Linux
Transmission Methods	SSH Brute Force, Docker Images, and Vulnerability Exploitation
Vulnerability Exploited	Apache Log4j 2 Remote Code Execution Vulnerability WebLogic Vulnerabilities Redis Unauthorized Access Vulnerability Hadoop Yarn Unauthorized Access Vulnerability Apache Struts Vulnerabilities
Mining Coins	Monero (XMR)

4.1.2 Typical Cases

1. "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. 错误!未找到引用源。.

2. An Analysis Report on the Recent Activities of the "8220" Hacker Attack Group

In May 2022, the National Computer Network Emergency Response Technical Coordination Center (CNCERT/CC) and Topsec jointly analyzed and excavated a cybercrime gang, which was identified as the "8220" mining gang after external intelligence comparison. According to CNCERT/CC data, the gang was relatively active on the Internet and continued to spread threats through the Tsunami botnet. The gang infiltrated about 4,000 devices and spread mining Trojans. The mining Trojans they controlled were also continuously iterating, constantly enhancing their adaptability to mining 错误!未找到引用源。.

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 Family Overview

Table 42Outlaw mining botnet

Organization Name	Outlaw
About the Organization	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 Vendor	Trend Micro
Country	Suspected Romania
Reason for Naming	Derived from the Romanian word haiduc, the hacking tool Haiduc used by the organization
Threat Types	Botnet, mining Trojans
Target	Linux, IoT
Transmission Methods	Shellshock (CVE-2014-7169) , Drupalgeddon2 (CVE -2018-7600) and SSH brute force attacks, mainly using the latter, which was only used in the early stages
Organizational 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

1. Analysis of Typical Mining Families 1: Outlaw Mining Botnet

The 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 [3].

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 Family Overview

Table 4-3 Introduction to TeamTNT mining organization

Organization Name	TeamTNT
First Disclosure Time	October 2019
Country	Germany
Reason	The earliest use of the teamtnt.red domain name
Threat Types	Mining Trojans and Backdoors
Target	Docker , Kubernetes , and Redis
Transmission Methods	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.
Technologies in Which the Organization Excels	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

1. Attacks on AWS and Alibaba Cloud

2022, researchers discovered modified versions of malicious shell scripts used by the TeamTNT mining group. The malware authors modified these tools after realizing that security researchers had disclosed previous versions of their scripts. These scripts are primarily designed to target Amazon Web Services (AWS) and Alibaba Cloud, but can also be run locally, in containers, or in other forms of Linux instances [4].

2. TeamTNT launches Kangaroo attack

In September 2022, researchers discovered that the TeamTNT mining organization launched the Kangaroo attack, hijacking a large number of servers as solver algorithms to crack Bitcoin and attempting to crack the keys and signatures of the secp256k1 elliptic curve. This attack was named the Kangaroo attack because it used Pollard's Kangaroo WIF solver. The attack scanned vulnerable Docker Daemons programs and launched Alpine OS images and eventually the solver from GitHub [5].

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 Family Overview

Table 4-4Introduction to H2Miner mining organization

Mining Trojan Family	H2Miner
Appearance Time	December 2019
Targeted Platform	Windows, Linux
Transmission Methods	Exploits
Vulnerability Exploited	SaltStack RCE (CVE-2020-11651) ThinkPHP5 RCE 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

1. H2Miner Mining Trojan Exploits the Rce Vulnerability to Launch Attacks

In March 2022, researchers captured a sample of a variant of the H2Miner mining trojan. The H2Miner organization was first active at the end of 2019. It is good at using the latest disclosed RCE vulnerabilities to carry out "tear-off" penetration attacks, implanting trojans into target servers, turning them into "mining machines", and ultimately carrying out illegal mining activities. It is reported that the organization has illegally mined Monero and made a profit of more than 3.7 million RMB [6].

4.5 Sysrv-hello

The Sysrv-hello mining worm 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 Family Overview

Table 4-5 Basic information of Sysrv-hello mining worm

Family Name	Sysrv-hello
First Disclosure Time	December 31, 2020
Reason	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
Transmission Methods	Vulnerability exploitation, brute force cracking, SSH private keys stored on the victim host

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

4.5.2 Typical Cases

1. Beware! Dual-Platform Mining Botnet Sysrv-hello Attacks Again with New Vulnerability

In April 2022, researchers captured the first new variant of the Sysrv-hello mining botnet in the wild that exploited the Spring Cloud Gateway Actuator RCE vulnerability (CVE-2022-22947) to attack user servers for mining. Since this vulnerability is a high-risk vulnerability, the exploitation method is relatively simple and has been made public (it can be achieved by constructing a malicious request packet), there is a risk of being widely exploited, and therefore it is very harmful 错误!未找到引用源。.

2. Beware of Malware Exploiting Confluence Remote Code Execution Vulnerability

In May 2022, researchers collected and analyzed a lot of attack traffic against Atlassian Confluence. Although this vulnerability has different attack vectors, the malware attacks discovered recently all target the parameter "queryString", including the Sysrv-hello mining Trojan, the Monero mining virus that uses WMI for persistence, and the mining virus that uses image format for disguise 错误!未找到引用源。.

4.6 "1337"

The "1337" organization determined the scope of the attack target by scanning the TCP 22 port exposed on the Internet, and used the SSH brute force tool to carry out brute force attacks on the information infrastructure that exposed the port. After the brute force attack was successful, the attacker would download the corresponding tools and scripts from the hosting website to scan and brute force the TCP 22 port of the victim's internal network. On this basis, the IP address of the victim's internal network was scanned and spied on, and the scan results were written into the specified text. Then, the brute force tool was used to carry out brute force attacks on the endpoint facilities corresponding to the surviving IP addresses, so as to achieve lateral movement in the victim's internal network. The mining program and the mining program execution script were downloaded to mine. It was determined that the mining program was the open source mining program Phoenix Miner, which mainly mines Ethereum.

4.6.1 Family Overview

Table 4-6 Introduction to the "1337" mining organization

Mining Trojan Family	"1337"
Appearance Time	December 2021
Targeted Platform	Linux
Transmission Methods	SSH Brute Force
Vulnerability Exploited	None
Mining Coins	Ethereum (ETH)

4.6.2 Typical Cases

1. "1337" Mining Organization's Activities

In early February 2022, Antiy and CERT Laboratory of Harbin Institute of Technology discovered during network security monitoring that a certain cyber attack organization was actively using SSH brute force to launch mining programs. After correlation analysis , it was found that the organization first appeared at the end of 2021. The hosting domain name used by the attacker was monitored as david1337.dev. The samples in this domain name

consisted of open source tools and mining programs. Later, it was successively associated with multiple domain names and IP addresses that were related to the "1337" string. Therefore, Antiy CERT named the mining organization the "1337" organization [9].

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 Family Overview

Table 4-7 Introduction to Kthmimu mining trojan

Mining Trojan Family	Kthmimu
Appearance Time	March 2022
Targeted Platform	Windows, Linux
Transmission Methods	Exploitation
Vulnerability Exploited	Apache Log4j 2 Remote Code Execution Vulnerability
Mining Coins	Monero (XMR)

4.7.2 Typical Cases

1. The 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 错误!未找到引用源。.

4.8 Hezb

The Hezb mining trojan uses a bat script named "kill.bat" on the Windows platform to perform its main functions, including terminating other competing mining processes, executing Monero mining, and downloading a script named "mad.bat", which is the configuration file of the Monero mining program. On the Linux platform, it uses a Shell script named "ap.sh" to perform its main functions, including downloading the curl tool to facilitate downloading subsequent malicious scripts, terminating other competing mining programs, moving horizontally, uninstalling security software, executing a script named "ap.txt", downloading kik malicious samples, and executing mining programs.

4.8.1 Family Overview

Table 4-8Introduction to Hezb mining trojan

Mining Trojan Family	Hezb
Appearance Time	May 2022
Targeted Platform	Windows, Linux
Transmission Methods	Exploits
Vulnerability Exploited	WSO2 RCE (CVE-2022-29464) Vulnerability Confluence OGNL (CVE-2022-26134) Vulnerability
Mining Coins	Monero (XMR)

4.8.2 Typical Cases

1. Analysis of Active Hezb Mining Trojans

In May 2022, Antiy CERT captured Hezb mining Trojan attack samples. In May, the Trojan mainly used the WSO2 RCE (CVE-2022-29464) vulnerability to spread. This vulnerability is an arbitrary file upload vulnerability that does not require authentication. It allows unauthenticated attackers to obtain RCE on the WSO2 server by uploading malicious JSP files. Since the detailed information of the Confluence OGNL (CVE-2022-26134)

vulnerability was released, the Hezb mining Trojan began to spread by using this vulnerability. This vulnerability allows remote attackers to construct OGNL expressions for injection without authentication, and execute arbitrary code on the Confluence Server or Data Center 错误!未找到引用源。.

Appendix 1 : References

[1]. Analysis of the "8220" Mining Organization's Activities
https://www.antiy.cn/research/notice&report/research_report/20220428.html

[2]. An Analysis Report on the Recent Activities of the "8220" Hacker Attack Group
https://www.cert.org.cn/publish/main/upload/File/8220%20APT.pdf

[3]. Analysis of Typical Mining Families Series 1 | Outlaw Mining Botnet
https://www.antiy.cn/research/notice&report/research_report/20221103.html

[4]. TeamTNT Targeting AWS, Alibaba
https://blog.talosintelligence.com/teamtnt-targeting-aws-alibaba-2/

[5]. Threat Alert: New Malware in the Cloud By TeamTNT
https://blog.aquasec.com/new-malware-in-the-cloud-by-teamtnt

[6]. Be Careful, Your Server May Become a " Mining Machine " ! Topsec Captures a Mutated H2Miner Mining Trojan
https://zhuanlan.zhihu.com/p/485155482

[7]. Beware! Dual-Platform Mining Botnet Sysrv-hello Attacks Again with New Vulnerability
https://mp.weixin.qq.com/s/PUwVvIGjon0ok8kmojksJw

[8]. Beware of Malware Exploiting the Confluence Remote Code Execution Vulnerability to Launch Attacks
https://mp.weixin.qq.com/s/XiZeonkI1AdwpX6EXC0f3g

[9]. "1337" Mining Organization's Activities
https://www.antiy.cn/research/notice&report/research_report/20220321.html

[10]. The Active Kthmimu Mining Trojan
https://www.antiy.cn/research/notice&report/research_report/20220527.html

[11]. The Active Hezb Mining Trojans
https://www.antiy.cn/research/notice&report/research_report/20220705.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.