Analysis of Ransomware PLAY

Antiy CERT

Completion time of first draft: 18 October, 2023
Time of first release: 20 October, 2023

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

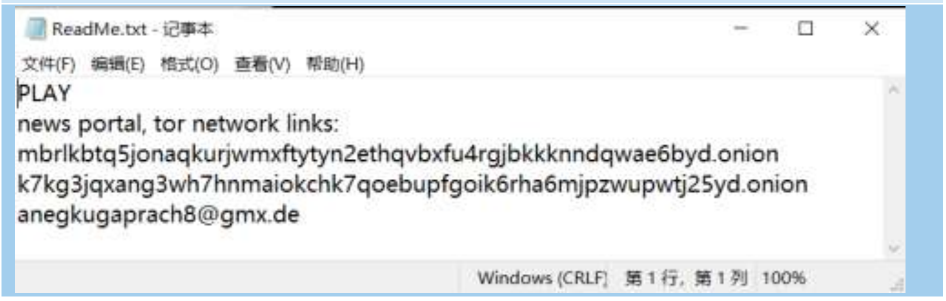
1 Overview

Recently, Antiy CERT monitors the PLAY blackmail event to present the active trend. Play ransomware, also known as PlayCrypt, was developed and operated by the Balloonfly organisation [1] and was first discovered in June 2022. The ransomware is spread mainly through phishing emails and exploit vulnerabilities, using a dual mode of "threatening exposure of corporate data + encrypted data." Since November 3, 2022, the Balloonfly attack group has successively released the victim information and stolen data which do not meet the attacker's needs in the dedicated data breach site (DLS) of Tor. As of October 16, 2023, the open source intelligence has disclosed information on 223 victims (including 196 published by the DLS). Attackers will remove victim information and stolen data when the demand is satisfied or for other reasons, and the actual number of victims far exceeds this number.

Ransomwar ePlay uses the "RSA + AES" algorithm to encrypt files, and no public decryption tools have been found. After the attack succeeds, the attacker will request the victim to contact through the dark network address or the mailbox.

Table 1-1 Overview of ransomware PLAY 1

Family name	Play (aka PlayCrypt)
Time of occurrence	June 2022
Mode of transmission	Phishing emails, exploit vulnerabilities, etc
Encryption suffix	.play
Encryption algorithm	"Rsa + AES"
Decryption tools	No public decryption tools were found

Method and amount of payment of ransom	Contact via a dark web address or mailbox
Encryption system	Windows
Double blackmail or not	Yes
Ransom note	 ReadMe.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) Windows (CRLF) 第 1 行，第 1 列 100%PLAY news portal, tor network links: mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion anegkugaprach8@gmx.de

2 Recommendations for protection

In response to ransomware attacks, Antiy recommends that individuals and businesses take the following precautions:

2.1 Personal protection

1. Enhance network security awareness: Maintain good habits of network use and actively learn relevant knowledge of network security;
2. Confirm the email content: Check the email address of the sender, verify the identity information, be cautious about the email requesting the account password, and avoid directly clicking the link or operation attachment in the suspicious email;
3. Install terminal protection: Install anti-virus software. It is suggested that Antiy IEP users open the ransomware defense tool module (open by default);
4. Strengthen password strength: Avoid using weak passwords, 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;
5. Change passwords on a regular basis: Change system passwords on a regular basis to avoid system intrusion due to password leakage;

6. Update patches in time: It is suggested to open automatic update and install system patches, and update system patches in time for vulnerable parts such as servers, databases and middleware;
7. Close high-risk ports: External services shall be minimized; if no use is needed, it is recommended to close high-risk ports such as 135, 139, 445 and 3389;
8. Close PowerShell: If PowerShell command line tools are not used, it is recommended to close them;
9. Regular data backup: Data backup of important files on a regular basis, and backup data shall be isolated from the host computer.

2.2 Enterprise protection

1. Network security training and security drill: Regularly carry out network security training and security drill to improve employees "network security awareness;
2. Install terminal protection: Install anti-virus software, and recommend the installation of Antiy IEP for different platforms;
3. Update patches in time: It is suggested to open automatic update and install system patches, and update system patches in time for vulnerable parts such as servers, databases and middleware;
4. Enable log: Enable the key log collection function (security log, system log, PowerShell log, IIS log, error log, access log, transmission log and cookie log) to provide a foundation for security event tracing and tracing;
5. Set IP whitelist rules: Configure advanced secure Windows firewall, set the inbound rules for remote desktop connection, add the IP address or IP address range used to the rules, and prevent violent attack of non-rule IPs;
6. Host reinforcement: Conduct penetration test and safety reinforcement for the system;
7. Deploy Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of ransomware. Taking network traffic as the detection and analysis object, the Antiy PTD can accurately detect a mass of known malware and network attack activities, and effectively detect suspicious behaviors, assets and various unknown threats on the network;

8. Disaster backup plan: Establish a security disaster backup plan to ensure that the backup business system can be quickly enabled in case of a security event;

9. Safe service: In case of a ransomware attack, it is recommended to disconnect the network in time, and protect the site and wait for the security engineer to check the computer. Antiy 7 * 24 Service Hotline: 400-840-9234.

It has been proved that Antiy IEP, the cloud host security monitoring system and the container security detection system can effectively detect and kill ransomware PLAY .

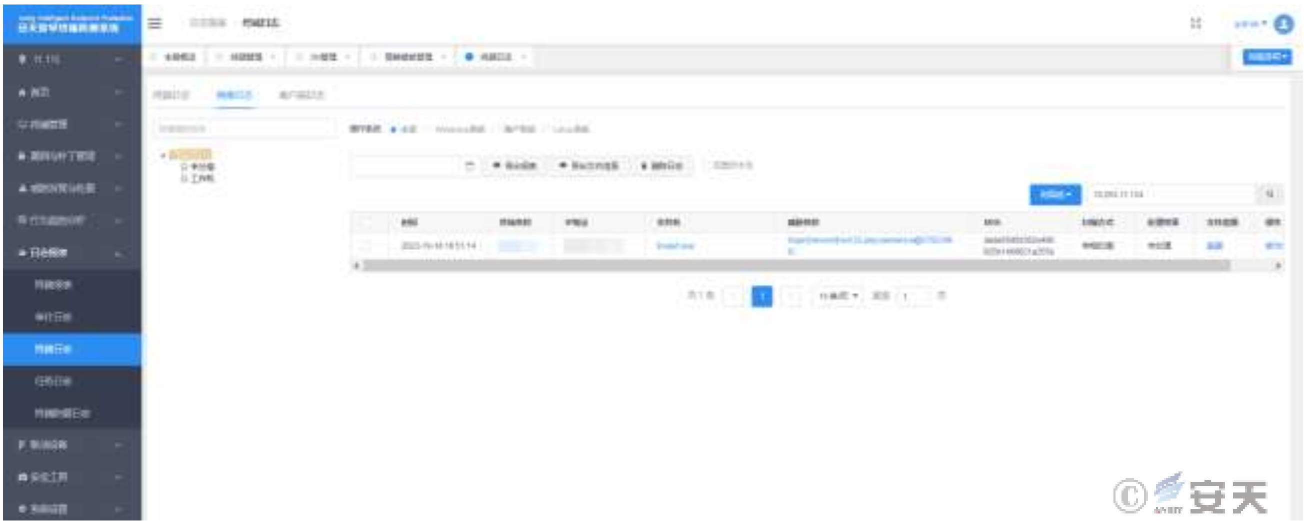


Figure 2-1 Antiy IEP can effectively kill ransomware PLAY

3 Disposal suggestions

When the machine is infected with the ransomware, do not panic, the following emergency work can be carried out immediately to reduce the harm caused by the ransomware: Isolation of the network, classified disposal, timely reporting, investigation and reinforcement, contact professional services.

1. The first thing to do is to disconnect the machines infected with the ransomware and prevent the ransomware from spreading sideways to infect other machines in the LAN.

2. Do not restart the machine, some ransomware writing has a logic problem, in the case of non-restart, there is the possibility of retrieving some of the encrypted files.

3. Do not rush to redo the system, or format the hard disk, such as the destruction of encrypted documents. First backup of the encrypted documents, encrypted with the suffix after the file is not infectious, can be copied to any computer for backup storage, but the possibility of recovery is extremely small. Depending on the situation, whether to wait for the decryption scheme or not, there are a small number of ransomware decryption tools that will be released for a variety of reasons.

4. Although the type of ransomware family can be determined from the information such as the suffix and the ransom letter, it is still impossible to determine the type of ransomware accurately due to the temporary absence of the specific process of how the ransomware is encrypted and transmitted in the user's network. Although virus samples with similar functions can be obtained from the threat intelligence database and confirmed by simulating the infection process, the location of the infection source needs to be refined during the infection process. It is suggested to locate and trace to the source in the form of on-site safety service.

4 Recent data leakage cases of ransomware PLAY

Since November 3, 2022, the Balloonfly attack group behind PLAY's ransomware has been publishing victim information and stolen data at the Tor dedicated data breach site (DLS) as of October 16, 2023. Its DLS releases information on a total of 196 affected units. Some data stolen will be released after the payment of ransom time, with a size of about 5G, involving sensitive information such as personal data, customer files, contracts, recruitment information, tax and financial information.

The following are recent cases of victimized units released by organizations behind the PLAY ransomware attack.

4.1 Hughes Gill Cochrane, an American information services company

On October 10, 2023, the attacker updated information about Hughes Gill Cochrane, an American information service company, on his DLS. Some of the documents released and stolen include personal data, customer documents, contracts, recruitment information, tax information, financial information and a total of 5G data.

4.2 Australian Finance Company NachtExpress Austria GmbH

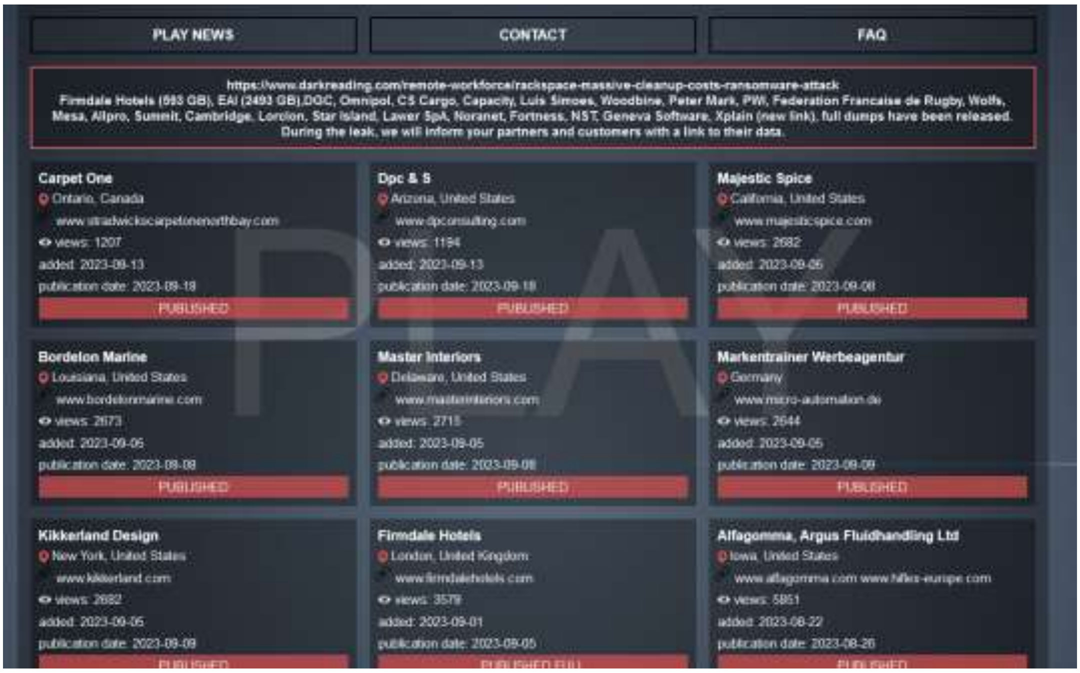
On October 9, 2023, the attacker updated information about Australian finance company NachtExpress Austria GmbH on his DLS, Some of the documents released and stolen include customer documents, contracts, recruitment information, ID cards, passports, payroll, tax, financial information and a total of 5G data.

4.3 Uk logistics company WCM Europe

On 9 October 2023, the attackers updated information relating to WCM Europe, the UK logistics company that was placed on their DLS, Some of the documents released and stolen include customer documents, contracts, recruitment information, ID cards, payroll, tax and financial information, and a total of 5G data.

5 Data statistics

Play ransomware has been active since June 2022 and has successfully attacked a total of 223 times, with the remaining 27 times being data monitored by Antiy CERT in addition to 196 times published by the dark network address. At present, the main target of the extortion group for Europe and the United States.



https://www.darkreading.com/remote-workforce/rackspace-massive-cleanup-costs-ransomware-attack
Firmdale Hotels (593 GB), EAI (2493 GB),DGC, Omnipol, CS Cargo, Capacity, Luis Simoes, Woodbine, Peter Mark, PWI, Federation Francaise de Rugby, Wolfs, Mesa, Allpro, Summit, Cambridge, Lorclon, Star Island, Lawer SpA, Noranet, Fortness, NST, Geneva Software, Xplain (new link). full dumps have been released.
During the leak, we will inform your partners and customers with a link to their data.

Carpet One
Ontario, Canada
www.stradwickscarpetonenorthbay.com
views: 1207
added: 2023-09-13
publication date: 2023-09-18
PUBLISHED

Dpc & S
Arizona, United States
www.dpconsulting.com
views: 1194
added: 2023-09-13
publication date: 2023-09-18
PUBLISHED

Majestic Spice
California, United States
www.majesticspice.com
views: 2682
added: 2023-09-05
publication date: 2023-09-08
PUBLISHED

Bordelon Marine
Louisiana, United States
www.bordelonmarine.com
views: 2673
added: 2023-09-05
publication date: 2023-08-08
PUBLISHED

Master Interiors
Delaware, United States
www.masterinteriors.com
views: 2715
added: 2023-09-05
publication date: 2023-09-08
PUBLISHED

Markentrainer Werbeagentur
Germany
www.micro-automation.de
views: 2644
added: 2023-09-05
publication date: 2023-09-09
PUBLISHED

Kikkerland Design
New York, United States
www.kikkerland.com
views: 2682
added: 2023-09-05
publication date: 2023-09-09
PUBLISHED

Firmdale Hotels
London, United Kingdom
www.firmdalehotels.com
views: 3579
added: 2023-09-01
publication date: 2023-09-05
PUBLISHED FULL

Alfagomma, Argus Fluidhandling Ltd
Iowa, United States
www.alfagomma.com www.hflex-europe.com
views: 5851
added: 2023-08-22
publication date: 2023-08-26
PUBLISHED

Figure 5-1 The attacker publishes part of the victim's information at the dark network address1

Based on the information collected, Antiy CERT collated the PLAY ransomware attacks between January and September 2023 and found that the ransomware group began carrying out frequent attacks since May. And the number of successful attacks each month is more than 20.

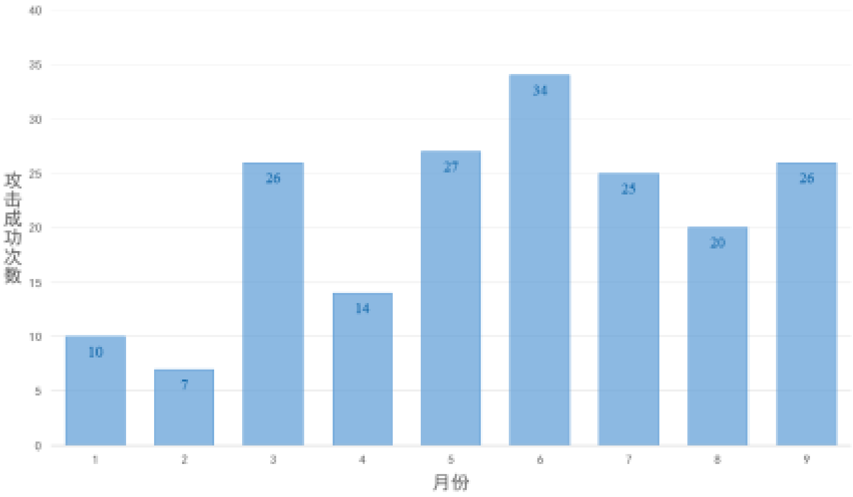


Figure 5-2 Number of successful attacks in the month 2

6 Sample analysis

The ransomware uses "RSA + AES" algorithm to encrypt files and keys in < original file name > + < suffix of original file > + <. Play >.

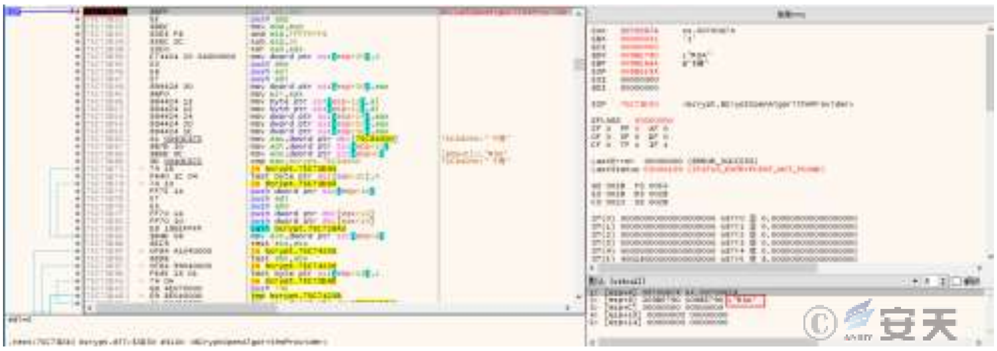
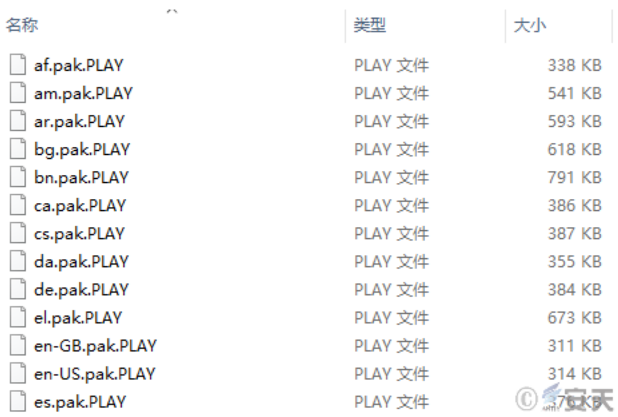


Figure 6-1 RSA algorithm 1

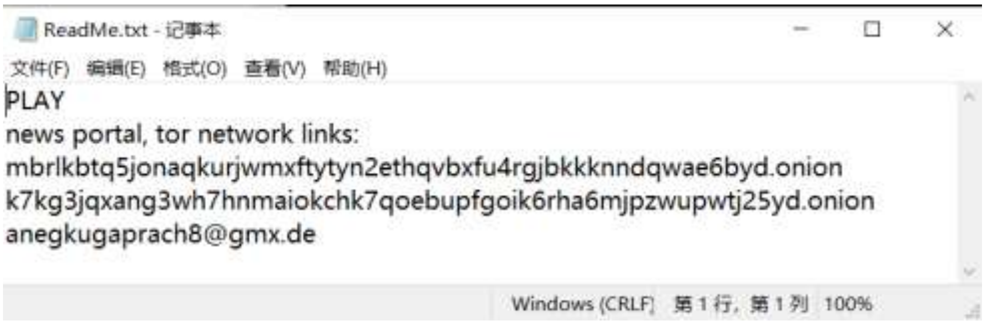


名称	类型	大小
af.pak.PLAY	PLAY 文件	338 KB
am.pak.PLAY	PLAY 文件	541 KB
ar.pak.PLAY	PLAY 文件	593 KB
bg.pak.PLAY	PLAY 文件	618 KB
bn.pak.PLAY	PLAY 文件	791 KB
ca.pak.PLAY	PLAY 文件	386 KB
cs.pak.PLAY	PLAY 文件	387 KB
da.pak.PLAY	PLAY 文件	355 KB
de.pak.PLAY	PLAY 文件	384 KB
el.pak.PLAY	PLAY 文件	673 KB
en-GB.pak.PLAY	PLAY 文件	311 KB
en-US.pak.PLAY	PLAY 文件	314 KB
es.pak.PLAY	PLAY 文件	

Figure 6-2 Encrypted file 2

The ransomware does not encrypt RAM and CD-ROM type memories, does not encrypt files named ReadMe.txt and bootmgr, does not encrypt files with PLAY, exe, msi, dll, lnk, sys as suffixes, and deletes disk shadow backups.

In encryption, a ransom note named "ReadMe.txt" is released under the root directory of each disk, in which the address of the dark network and the email address of the attacker are given, and the details are as follows:


ReadMe.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Windows (CRLF) 第 1 行，第 1 列 100%

PLAY
news portal, tor network links:
mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion
anegkugaprach8@gmx.de

Figure 6-3 Contents of a ransom letter

3

7 IoCs

IoCs
5ea71206b0701fdfcef38dc1080bea3b
8b7e28ab198c36e6cc75f95a9c513399
Ffdbf029182d045c20d694e794755694
7b14f0cf56a38c8123f6ff9041159f0a
Deee1b66ad2797868edc4c5c7bb1a4603
Mbrlkbtq5jonaqkurjwmxftytyn2ethqbxfu4rgjbkknndqwae6byd.onion

K7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwuptj25yd.onion
Anegkugaprach8 @ gmx.de

Appendix I: Reference

[1]. Play Ransomware Group Using New Custom Data - Gathering Tools

Https: / / symantec-enterprise-blogs.security.com / blogs / secret-intelligence / play-Ransomware-volume-shadow-copy

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 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.