Ransomware Attack Organizations Review In the First Half of 2024

Antiy CERT

First published: July 31, 2024

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

1 Overview

Ransomware is a highly destructive computer malware. In recent years, it has become one of the major cybersecurity threats to organizations around the world, and is used by attackers as a criminal tool to make illegal economic gains. In order to increase the probability of victims paying the ransom and to raise the ransom amount, attackers have evolved from maliciously encrypting data to a double extortion strategy of "stealing files + encrypting data". What's more, they have added DDoS attacks and harassment of third parties related to the victim on the basis of double extortion, evolving into "multiple extortion". Once attacked by ransomware, the normal operation of an organization will be seriously affected, which may lead to business interruption, data theft and malicious encryption. Attackers threaten victims with data recovery and exposure and demand ransom. The data includes documents, emails, databases, source code and other formats; the ransom can be paid in digital currencies such as Bitcoin, Monero and Ethereum. Attackers usually set a ransom payment deadline and increase the amount over time. Sometimes, even if the ransom is paid, the maliciously encrypted files cannot be fully restored.

Ransomware attack organizations use a variety of means to disclose the sensitive information of victims and use this as a threat to force victims to pay ransom or meet other illegal demands to avoid further leakage or sale of their data. According to incomplete statistics, as of the first half of 2024, **at least 62 organizations with different names have released victim information, of which 20 are new ransomware attack organizations that emerged in 2024. These attack organizations have released more than 2,700 victim information from different countries and regions, covering multiple key industries such as healthcare, public administration, social security, finance, energy, manufacturing and education.** The actual number of victims may be higher, because attackers may choose not to disclose or delete information for some reason, such as after negotiating and reaching an agreement with the victims, or the victims paid a ransom in exchange for the deletion of information. **For information about ransomware attack organizations, see the Computer Virus Encyclopedia [1].**

Although most victims have established corresponding network security protection systems, they are still not immune to ransomware attacks. The main reason is that current prevention measures are often still at the stage of fighting against traditional ransomware, without fully realizing that ransomware attacks have developed into a chain of infringements and formed a large-scale criminal industry.

2 Ransomware Attack Organizations Review

This article reviews the ransomware attacks that occurred in the first half of 2024 and takes stock of active ransomware attack organizations, including basic information about the organizations and related attack events, in alphabetical order. Following the inventory of active ransomware attack organizations in 2023[2]the [3]ransomware attack organization has fallen off the list after retiring in March.

Table 2-1 2of 2024

Organization name	Discovered time	How it works	Attack event
8Base	March 2022	Espionage + encryption, ransomware as a service, extortion and data trafficking	The German agricultural machinery manufacturer LEMKEN shut down its IT systems in many locations, stopped production, and had some data stolen. The Atlantic States Marine Fisheries Commission shut down some of its systems and had some of its data stolen.
Akira	March 2023	Espionage + encryption, ransomware as a service, two-part ransomware (decrypting files and deleting stolen data) and data trafficking	The data center of Finnish cloud service provider Tietoevry in Sweden was affected, causing business interruption for some customers. The Singapore law firm Shook Lin&Bok paid a ransom of about US$1.4 million to restore the system and prevent data leakage.
BianLian	June 2022	Espionage without encryption, ransomware as a service, extortion and data trafficking	Resulting in about 1TB of data being stolen from On Q Financial, a US financial institution, affecting more than 210,000 people. A large amount of data from Affiliated Dermatologists in the US medical institution was stolen, affecting more than 370,000 people.
Black Basta	April 2022	Espionage + encryption, ransomware as a service, extortion and data trafficking	As a result, about 140 hospitals and several nursing homes using the US healthcare system operator Ascension were affected.

			The incident caused the partial disruption of operations of Keytronic, a US printed circuit board manufacturer, and the suspension of its cross-border business. Approximately 530GB of data was stolen.
Hunters International	October 2023	Espionage + encryption, ransomware as a service, extortion and data trafficking	It caused the partial business system interruption of Hoya, a Japanese optical instrument manufacturer, and stole about 2TB of data, demanding a ransom of 10 million US dollars.
			Resulting in the theft of about 2TB (about 4.7 million files) of Chip Optoelectronics Co., Ltd. in Taiwan, involving product files of third-party companies.
INC	July 2023	Espionage + encryption, ransomware as a service, extortion and data trafficking	As a result, about 3TB of data was stolen from the UK National Health System Dumfries and Galloway, and some business systems were affected.
			Most of the business systems of the Richland City Government in the United States were shut down and a large amount of data was stolen.
LockBit	September 2019	Espionage + encryption, ransomware as a service, extortion and data trafficking	The website of Taiwan Jingding Precision Technology was tampered with, 5TB of data was stolen, and the stock price fell by about 3% due to this incident.
			33TB of data from Evolve, a US financial services company, was stolen, affecting more than 7.6 million people.
Medusa	June 2021	Espionage + encryption, ransomware as a service, extortion and data trafficking	The Kansas City Regional Transportation Authority shut down all its communication systems, some of its data was stolen, and a ransom of $2 million was demanded.
			The British defense service provider Chemring Group had about 187GB of data stolen and demanded a ransom of $3.5 million.
Play	June 2022	Espionage + encryption, claiming that they do not use ransomware as a service, based on ransom and data trafficking	A large amount of data was stolen from KC Scout, a traffic management system in Kansas, USA, affecting monitoring, traffic, weather and other service systems.
			The hack caused some production plants of Welch's, an American food company, to shut down and about 428GB of data was stolen.
RansomHub	February 2024	Espionage + encryption, ransomware as a service, extortion and data trafficking	The incident caused the shutdown of some business systems of Christie's auction house in the UK, and some data was stolen, affecting about 500,000 people.
			The US drugstore chain Rite Aid shut down some of its business systems and stores, and the stolen data affected about 2.2 million people.

According to incomplete statistics, in the first half of 2024, about 62 ransomware attack organizations with different names released victim information, and a total of more than 2,700 victims from different countries and regions were released.

Table 2-3 Ransomware attack groups that released victim information in the first half of 2024

Ransomware attack groups that released victim information in the first half of 2024 (in alphabetical order)				
0mega	8Base	Abyss	Akira	APT73/Erleig
Arcus Media	BianLian	Black Basta	BlackByte	BlackCat/ALPHV
Blackout	BlackSuit	Brain Cipher	Cactus	Cicada3301
Ciphbit	Cloak	Clop	Daixin	dAn0n
Dark Angel/Dunghill	Dark Vault	donex	donut	Dragon Force
Eldorado	Embargo	Everest	Fog	FSociety FLocker
Hunters International	INC	KillSecurity	LockBit	Lorenz
Mallox	Medusa	Meow	Money Message	Monti
Mydata/Alpha	Play	QiLin	Qiulong	RA World
RansomEXX	RansomHouse	RansomHub	Red	Rhysida
SenSayQ	SEXi（APT INC）	Slug	SpaceBears	Stormous
ThreeAM	Trigona	Trinity	Underground	UnSafe
Vanir Group	WereWolves			

According to incomplete statistics, 20 new attack groups with different names emerged in the first half of 2024, including APT73, Brain Cipher, SenSayQ and SEXi (APT INC) associated with LockBit[4]Embargo and Ransom Hub associated with BlackCat, and Space Bulls, which is suspected to be a Phobos ransomware attack group that has transformed into a double ransomware organization.

Table 2-4 New ransomware attack groups in the first half of 2024

New ransomware attack groups in the first half of 2024 (sorted by first letter)				
APT73/Erleig	Arcus Media	Blackout	Brain Cipher	Cicada3301
dAn0n	Donex	Eldorado	Embargo	FSociety FLocker
Fog	QiuLong	RansomHub	Red	SenSayQ
SEXi（APT INC）	Slug	SpaceBears	Trinity	Vanir Group

3 Ransomware Attacks

Ransomware attacks cause serious harm to individuals, businesses and critical infrastructure by encrypting and stealing data, including economic losses, social system paralysis, critical infrastructure risks, data leakage risks, industrial security threats, public service interruptions, corporate reputation damage, legal liability and personnel safety risks. With the continuous evolution of attack methods, ransomware attacks have become one of the main threats to global network security, requiring all parties to strengthen protection and response measures to ensure data security and stable system operation.

Table 3-12of 2024

Time	Victim	Ransomware attack group	Impact
January 17	Taiwan Province Jingding Precision Technology	LockBit	The website was tampered with, 5TB of data was stolen, and the stock price fell by about 3%
January 17	Schneider Electric France	Cactus	1.5TB of data stolen, some businesses interrupted
January 25	Claro, a Latin American telecom operator	Trigona	Telecommunications services are disrupted in some countries/regions
February 10	Romanian IT service provider RSC	Phobos	More than 100 hospitals affected
February 12	German battery manufacturer Varta	Not yet known	Five production plants were affected, and the stock price fell by about 3%
February 21	Change Healthcare, an American healthcare IT service provider	BlackCat	Hundreds of pharmacies and hospitals' online systems were affected; a large amount of data was stolen; it was not recovered after paying a ransom of $22 million; about $872 million was spent in the first quarter to deal with this incident
February 25	Hamilton, Canada	Cloak	Dozens of government agencies were affected, a large number of city service systems were interrupted, and about $5.7 million was spent to deal with the incident.
March 15	NHS Dumfries and Galloway	INC	3TB of data stolen, some business systems affected
April 3	Traffic Police, Delhi, India	KillSecurity	Stealing traffic violation data, about 250,000 traffic violation incidents
April 25	KC Scout, a traffic management system in Kansas, USA	Play	Large amounts of data were stolen, affecting monitoring, traffic, weather and other service systems
May 8	Ascension, an American healthcare system operator	Black Basta	About 140 hospitals and several nursing homes were affected
May 21	Kansas City Police Department, Kansas, USA	BlackSuit	Some police and fire service systems were affected

June 3	Synnovis, a UK pathology service provider	QiLin	Some data was stolen; operations, examinations, and blood matching at several hospitals were affected
June 8	Cleveland City Hall	Not yet known	Some public services in the city have been closed for more than a week
June 23	Evolve, an American financial services company	LockBit	About 33TB of data was stolen, affecting more than 7.6 million people

After Antiy conducted an in-depth analysis and review of the ransomware attack on Boeing [5], combined with similar incidents in the first half of the year, it is not difficult to find that ransomware attacks have caused a huge impact on victims and innocent third parties. These attacks not only pose a serious obstacle to the daily operations of enterprises, posing an unprecedented threat to the security of critical infrastructure, but also increase the risk of data leakage. They also disrupt the normal order of society and aggravate economic losses. With the continuous evolution of attack methods and the increasing frequency of attacks, ransomware attacks have become a cancer that poses a major threat to the normal operation of the country and society. They not only disrupt social order, but also have a profound impact on the peace of people's daily lives. The spread of such attacks, like an invisible plague, silently erodes every corner of society. Its wide range of harm and deep impact cannot be ignored.

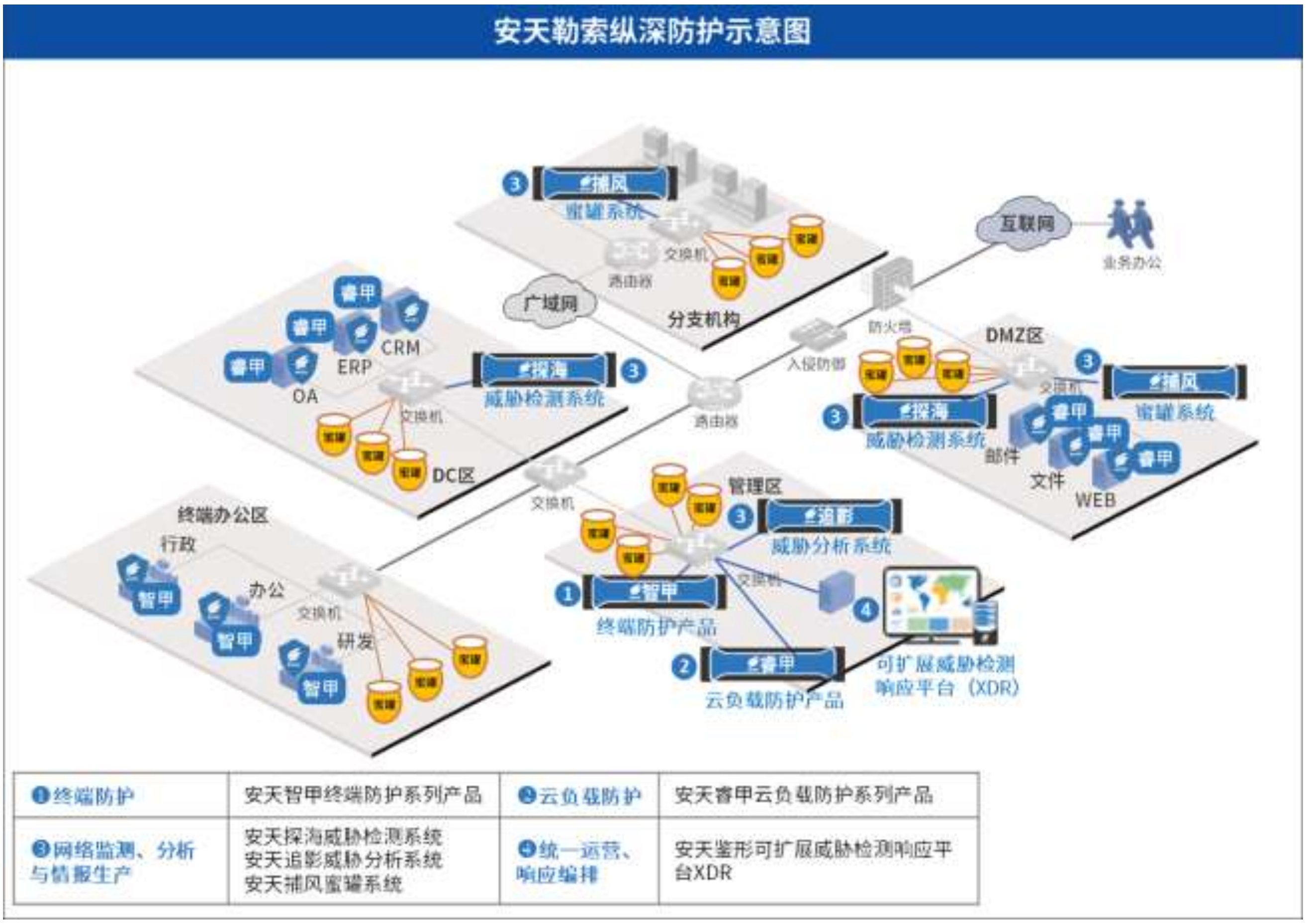
Most victims have not been spared even though they have established a basic network security protection system. The reason is that the current prevention of ransomware attacks is often still at the stage of the original ransomware, and many people do not realize that ransomware attacks are already a chain of infringements consisting of continuous targeted intrusions, stealing data, encrypting data to paralyze the system, extorting money, mining data for secondary use, selling data, reporting to regulatory agencies, and publicly stealing data, and have formed an extremely large criminal industry. In this context, the risk of encountering a ransomware attack is no longer a simple form of data loss and business suspension, but a series of chain risks such as all stolen data will be sold and made public.

The continuous emergence of various major security threat events easily leads to doubts such as whether to focus on preventing ransom attacks or APT attacks. From a technical perspective, the level of the leading attack part of a few ransom attacks is close to the level of APT attacks by ultra-high-capability cyber threat actors, and ransom attacks will bring more direct and rapid economic losses and obvious impact on the reputation of institutions than APT attacks. Targeted ransom attacks are indeed a combination of APT capabilities + ransom behavior. But from another perspective, since ransomware attack organizations must benefit in a relatively short period of time, they do not have the critical willpower that APT attackers must have to break through the central target. In terms of long-term lurking, persistence and covert operations, they will not show the strategic patience of APT attackers. Therefore, for every government and enterprise organization, the exposure of its assets and personnel must face multiple attack organizations at the same time, but the judgment of the highest intensity or level of attack it may encounter needs to be based on the assumption that the value of its comprehensive business assets is placed in the context of complex social security and geopolitical security.

However, it must be pointed out that for many organizations, the current problem is not the choice of whether to focus on APT attacks or ransomware attacks, but the problem of not completing the construction of the basic defense. For various complex combined attacks, it is necessary to deploy defense layers. There is no such thing as "one trick to conquer all". The premise of flexible adjustment of all resources, manpower, and strategic investment is that the basic actions of building basic defense capabilities have been completed, and a dynamic, comprehensive, and effective closed-loop defense system has been basically formed. Only in this way can targeted deployment be implemented in response to changes in threats. It can be said that if the defense system can effectively defend against APT attacks, it can also effectively defend against targeted ransomware attacks.

4 Building In-Depth Protection Capabilities Against Ransomware

In the face of targeted ransomware and even APT-level targeted attacks, in order to achieve the actual situation of the operation purpose on the host system side, it is necessary to build a multi-level and practical ransomware protection-in-depth solution for the end/cloud/network to minimize the risk of users being attacked by ransomware. By strengthening the cornerstone role of the entire host system protection, enhancing network-side monitoring, analysis and intelligence production, relying on the XDR platform for unified operation and response orchestration, the overall automated closed-loop operation capability for ransomware attack protection is improved, and the ransomware prevention and control capabilities are verified and improved with the help of drill services.



❶终端防护	安天智甲终端防护系列产品	❷云负载防护	安天睿甲云负载防护系列产品
❸网络监测、分析与情报生产	安天探海威胁检测系统 安天追影威胁分析系统 安天捕风蜜罐系统	❹统一运营、响应编排	安天鉴形可扩展威胁检测响应平台XDR

Figure 4-1Building a multi-layered, practical ransomware protection solution for end/cloud/network

- **Strengthening the cornerstone of full host system protection**

By protecting the three key links of ransomware attack landing, execution, and effectiveness on the entire host system side, the host system side executor governance capabilities are strengthened, the business scenarios on the host system side are integrated, and the risk of users being subjected to ransomware attacks is reduced.

Strengthen terminal protection. Antiy IEP terminal protection series products are equipped with Antiy's next-generation threat detection engine to accurately detect and kill ransomware viruses. Based on kernel-level active defense capabilities, a fine-grained and multi-level ransomware protection boundary is built, namely system reinforcement, (host) boundary defense, scanning and filtering, active defense, and document security. Based on ransomware attack behavior monitoring, ransomware attacks can be detected and blocked in the first place.

Strengthen cloud load protection. Based on a probe, the Antiy UWP cloud load protection series of products flexibly combines multiple security capabilities, provides business-oriented zero-trust construction, and detects and blocks ransomware attacks in the first place based on automated correlation of intrusion detection events and ransomware attack behavior monitoring. Application-level micro-isolation based on identity ID allows for refined control and curbs on the lateral movement of ransomware attacks, reducing the risk of falling victim to ransomware attacks.

- **Enhance network-side monitoring, analysis, and intelligence production**

Through the Antiy Attack Capture System, a deceptive defense environment is created to effectively perceive ransomware attacks, quickly discover ransomware incidents and generate intelligence, and link other systems to respond to ransomware attacks.

Based on Antiy Persistent Threat Detection System, network traffic monitoring and response are enhanced, integrating multi-dimensional detection capabilities such as malicious code detection engine, network behavior detection engine, command and control channel detection engine, etc., to perceive ransomware attack behavior, combine bypass blocking and intelligence production, and work with other systems to complete disposal.

Antiy Persistent Threat Analysis System is triggered based on fine-grained ransomware behavior, generates detection rules for Antiy Persistent Threat Detection System and produces intelligence locally. At the same time, other business or security systems in the network can deliver files to Shadow Chaser to achieve security judgment and reveal ransomware behavior.

- **Unify operations and response orchestration to improve automated closed-loop operations**

With Antiy's extensible threat detection and response platform XDR as the core, we strengthen unified operations and response orchestration. By configuring the automatic connection of heterogeneous logs of Antiy products and third-party security products, we integrate terminal/cloud/network/business/identity data analysis to form high-confidence and high-value alarms. Based on automatic analysis and correlation of high-value event chains, we provide risk detection and kill chain restoration for ransomware attack scenarios. For business scenarios, security operators can use preset scripts and custom plan configurations to achieve refined control and response to ransomware attack entrances and execution behaviors. With the continuous operation mode of "people in the closed loop", we will improve the automated closed-loop operation capabilities for ransomware attacks.

- **Conduct ransomware prevention drills to test and improve ransomware prevention capabilities**

On the premise of ensuring stable business operation, we conduct ransomware prevention and control drills by adopting the method of "simulating ransomware attacks + selecting real ransomware samples + combining typical ransomware techniques and tactics". We complete verification design, sample selection (extracting the top 10 families of mainstream ransomware viruses to form a sample set), environment construction, verification and evaluation, emergency response, forensic analysis, and environmental cleanup in combination with business scenarios. We comprehensively verify the prevention and control capabilities for actual ransomware attacks, help managers and security operations personnel to form an intuitive understanding of ransomware attack methods, attack paths, and used resources, discover the exposed and attackable surfaces in business scenarios, and put forward optimization suggestions around the construction of ransomware prevention and control capabilities and management systems, enhance the emergency response capabilities for ransomware attacks, and reduce potential economic and reputation losses.

Appendix 1: References

[1]. Antiy. Computer Virus Encyclopedia

https://www.virusview.net/

[2]. Antiy. 2023 Active Ransomware Attack Organizations Review[R/OL].(2024-01-25)

https://mp.weixin.qq.com/s/C33dR8D_EIot6TqFzDGyPQ

[3]. Antiy. Beware of Data Leaks Caused by BlackCat Ransomware[R/OL].(2023-07-03)

https://mp.weixin.qq.com/s/4sPVG-nCFx1ba_3KMA49vw

[4]. Antiy. Analysis of LockBit Ransomware Samples and Defense Thinking Against Targeted Ransomware[R/OL].(2023-11-17)

https://mp.weixin.qq.com/s/Ncefpps86iVgesMmHSRaLg

[5]. Antiy. Analysis and Review of the Ransomware Attack on Boeing - Threat Trend Analysis and Defense Thinking of Targeted Ransomware [R/OL]. (2023-12-30)

https://mp.weixin.qq.com/s/K1tb86Gy6V9GlrIb__ZM_g

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.