Analysis of the Active RansomHub Ransomware Attacking Group Situation

Antiy CERT

Time of first release: 12 September, 2024

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

1 Overview

The RansomHub ransomware attacking group was found in February 2024 and has continued to be active since its emergence, operating on a ransomware-as-a-service (RaaS) model to victimize victims through a "steal file + encrypt data" double blackmail strategy. Currently, no effective tool has been found that can successfully decrypt its encrypted data. The group uses specific means to disclose sensitive victim information and uses it as a blackmail to force victims to pay ransoms or meet other illegal demands in order to avoid further disclosure or sale of their data. As of September 12, 2024, the information distribution site used by the group had 227 victim information, and the actual number of victims would be higher because the attacker may choose not to make the information public or to delete it for some reason. For example, after negotiation and agreement with the victim, or the victim paid a ransom in exchange for the deletion of the information.

The attack techniques and tactics used by the RansomHub Group bear significant similarities to the Knight Group. In addition, it appears to have some connection with the BlackCat (aka ALPHV) group, which was once active in the world of ransomware attacks but has now withdrawn. In recent attacks, RansomHub has demonstrated the ability to use techniques and tactics commonly used by Advanced Persistent Threat (APT) organizations to execute blackmail attacks. As a result, the background of the RansomHub group is complex, whether it is "all evil in one" or "another," and it is not yet clear whether these theories point to a complex ecosystem of cybercrime. Among them, the lines between attackers may be far more blurred than they seem.

2 Background of the organization

In February 2024, ParanoidLab, a dark net monitoring cloud service, discovered that a user named "koley" had published a plan [1] on the RaaS of the RansomHub extortion attack organization in the Hacker Forum to attract

affiliated members. It includes the proportion of extortion and ransom, the characteristics of encryption tools and some rules.[1]

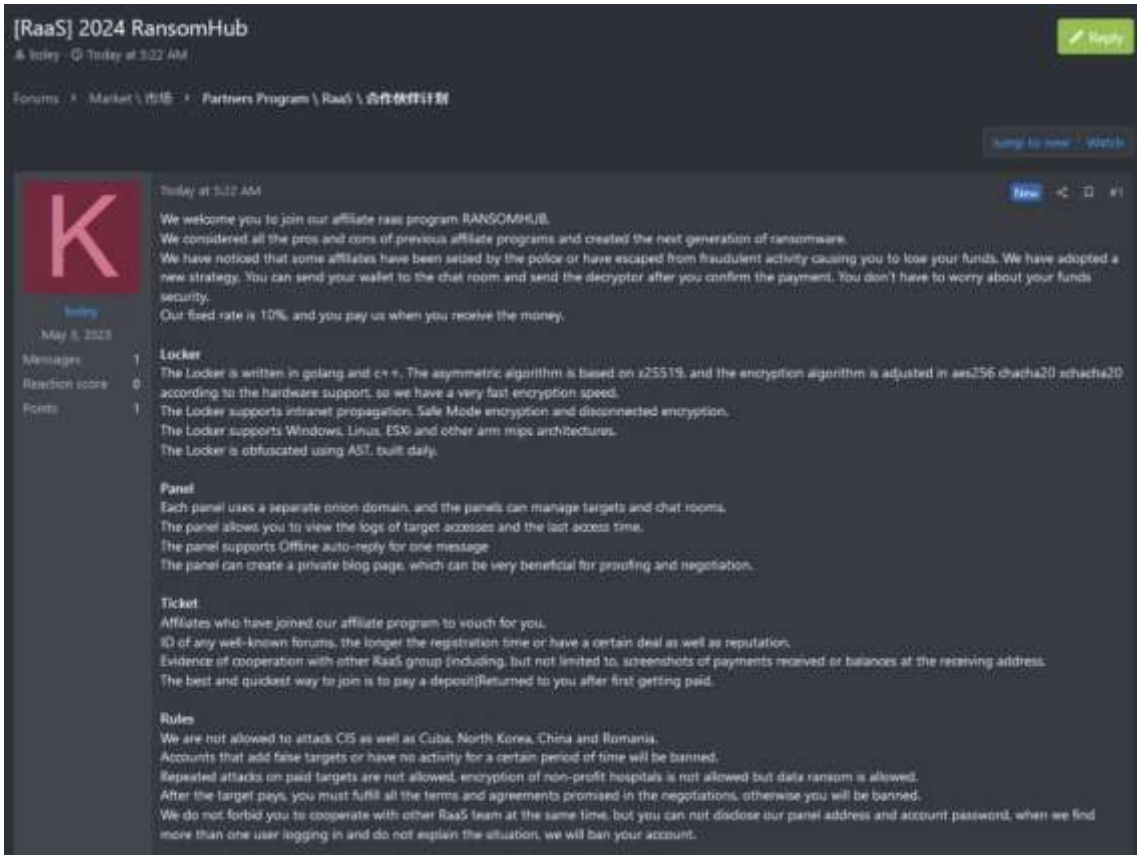

Figure 2-1 RansomHub organizing a RaaS plan 21

The Cyclops blackmail attack group first appeared in public in May 2023, and was renamed Knight in July that year. In February 2024, it was revealed that members of the group had publicly sold their core source code on hacking forums [2]. In that same month, meanwhile, the RansomHub group was found to use ransomware payload and techniques and tactics that bear significant similarity to Knight [3], In addition, the members of the two organizations registered in the forum at the same time point. This similarity is not difficult to speculate about, including the following possibilities: Ransomhub may have adopted Knight's source code; or, some of Knight's original members may have switched to RansomHub; or Knight may have undergone a rebranding exercise. Continuing its cybercrime with RansomHub's new identity.[2][3]

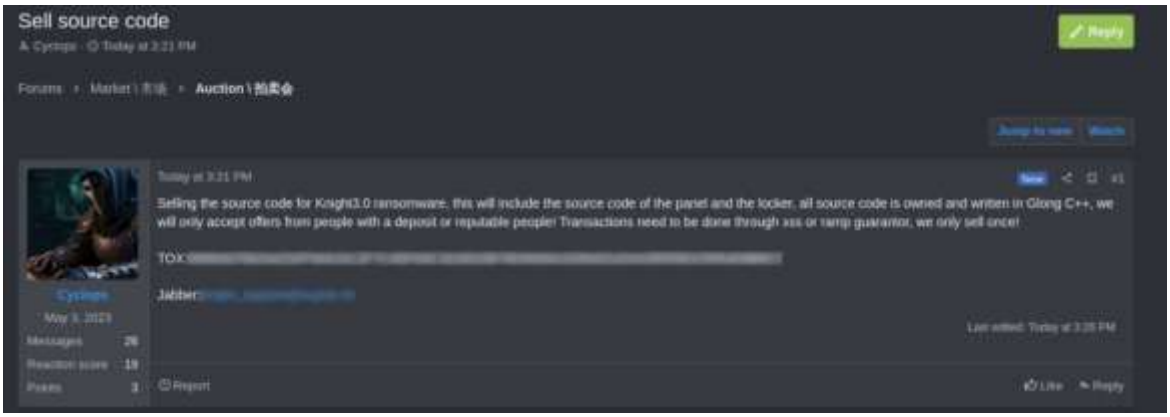

Figure 2-2 Knight selling code 22

In February 2024, Change Healthcare, a giant in the US healthcare industry, was unfortunately targeted by members of the BlackCat blackmail group, Notchy [4]. The attack resulted in encryption of parts of the company's business systems and the theft of terabytes of sensitive data. In the face of this, Change Healthcare made the decision in early March to pay the ransom, totaling about $22 million, to ensure the company's data can be recovered and to prevent the stolen data from being further leaked or sold on the black market. But member "Notchy" said the victim did not receive his share after paying the ransom, and the full amount of the ransom was held by BlackCat officials. Subsequently, BlackCat executives in the Hacker Forum said that the BlackCat brand out of the blackmail market error! Reference source not found. whose code was sold. In April, "Notchy" transferred the stolen data to the RansomHub group and went on to blackmail Change Healthcare. All these actions can't help but raise doubts about whether it is a play he has directed and acted in order to mislead the public into believing that BlackCat has really dropped out of the ransomware market, or that it has changed its name and continues to do evil.[4]**错误!未找到引用源。**

2.1 Part of the ransomware sample

The RansomHub ransomware samples are written in C + + and Go languages, and code snippets are obfuscated in a specific way to interfere with security personnel analysis. The ransomware sample must be read before a specific json file is executed. if the read fails, the sample cannot be executed. This technology is similar to BlackCat ransomware [6].[6]

When the ransomware load is executed, the pre - json file is read, and different functions are realized according to the preset field information in the json file.

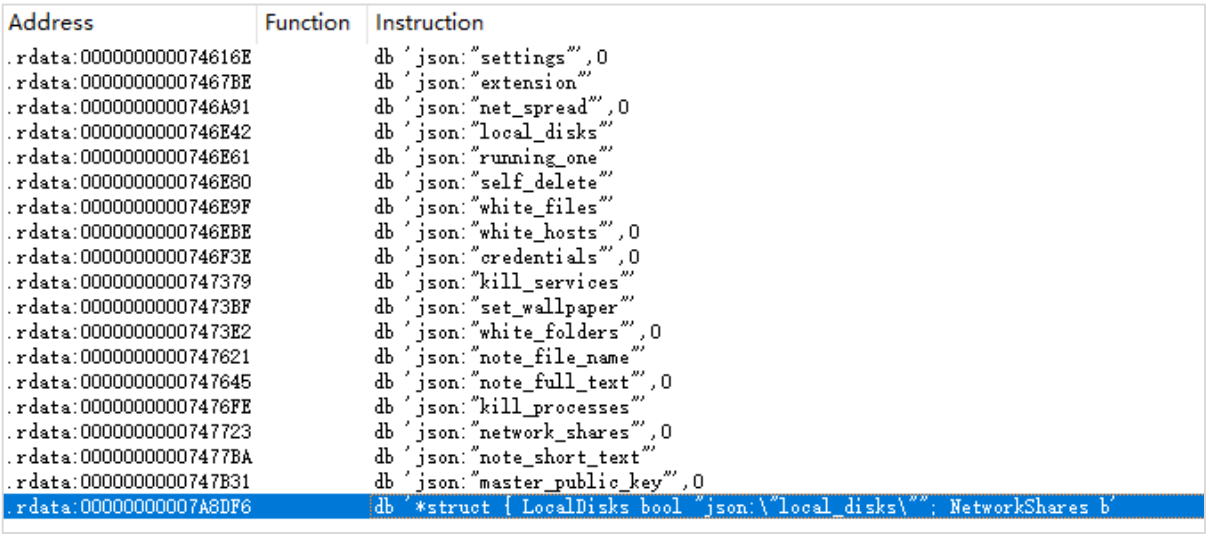

Figure 2-3 Function fields in the json file 23

According to the field settings in the json file and some features of the ransomware, the corresponding functions are predicted. see the table below for details:

Table 2-1 json fields and corresponding function information table 21

Field	Corresponding functions	Field	Corresponding functions
Extension	The suffix of the encrypted file	Net spread	Internet communication
Local disks	Local disk encryption	Running one	Only once
Self delete	From Delete	White files	Unencrypted files
White hosts	An unencrypted host	Credentials	The credential information used for access
Kill Services	End a specific service	Set wallpaper	Set the desktop background
White folders	Unencrypted directory	Note file name	Name of the ransom note
Note full text	Complete ransom note	Kill processes	End a particular process
Network shares	Network sharing encryption	Note short text	The contents of a short ransom note
Master public key	The master public key used for encryption		

In that part of the ransomhub feature, both RansomHub and Knight support different function by selecting different option through the command line mode, and some modes are the same as the corresponding fields.

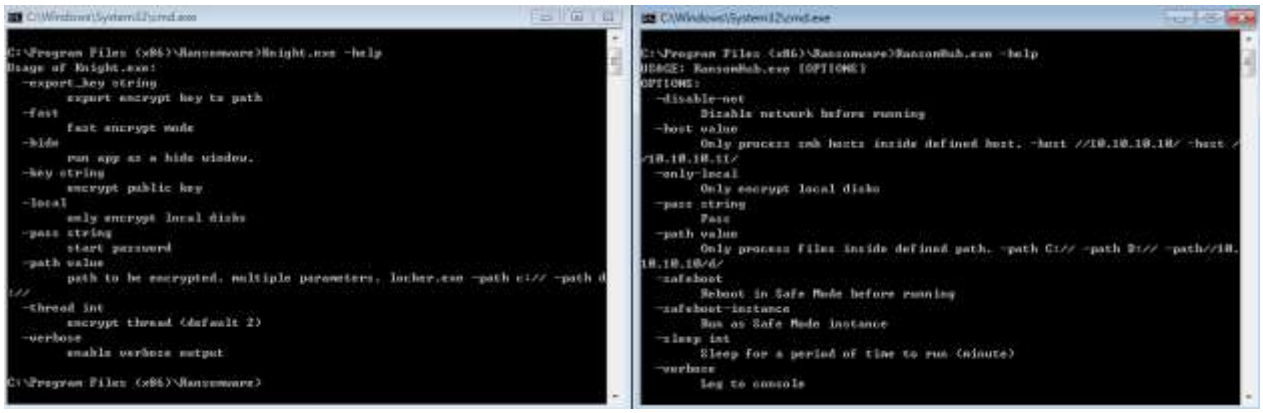

Figure 2-4 Functional comparison between RansomHub and Knight 24

Ransomhub Racketeers have recently used Bring Your Own Vulnerable Driver (BYOVD) technology to carry out extortion attacks. An attacker uses such technology to implant legitimate drivers with security vulnerabilities into a target system, and these drivers can often evade the review of security software because they have a legitimate digital signature. In order not to be marked or bloc. Once these drivers, especially kernel-mode drivers, are successfully used, they can provide a means for attackers to achieve kernel-level permissions on target systems. This permission enhancement not only gives attackers full access to system resources, but also enables them to disable or evade detection of endpoint security software so that they can carry out various malicious activities in the target system.

It is worth noting that this strategy is not original for RansomHub, and some APT groups, including Lazarus and Lamberts, have used similar techniques to carry out attacks. In addition, extortion attack groups such as BlackCat, Cuba and LockBit [7] have followed suit, using this technique to carry out extortion attacks. As mentioned in ATHAN's "Review and Outlook on Cybersecurity Threats" [8] released in 2021, part of the blackmail attack capability has reached the "APT" level.[7][8]

3 Information release platform for victims

The RansomHub group posts information about its victims on specific Tor network addresses. Each victim has its own separate information display area. The group classifies the status of victims into two categories based on whether the stolen data has been made public: "Undeclared" (countdown status) and "publicised." Under the status information of each victim, Key information including the number of Visits, the total amount of data stolen (Data Size), the last update time (Last View) and the time when the victim information was first published are also detailed.

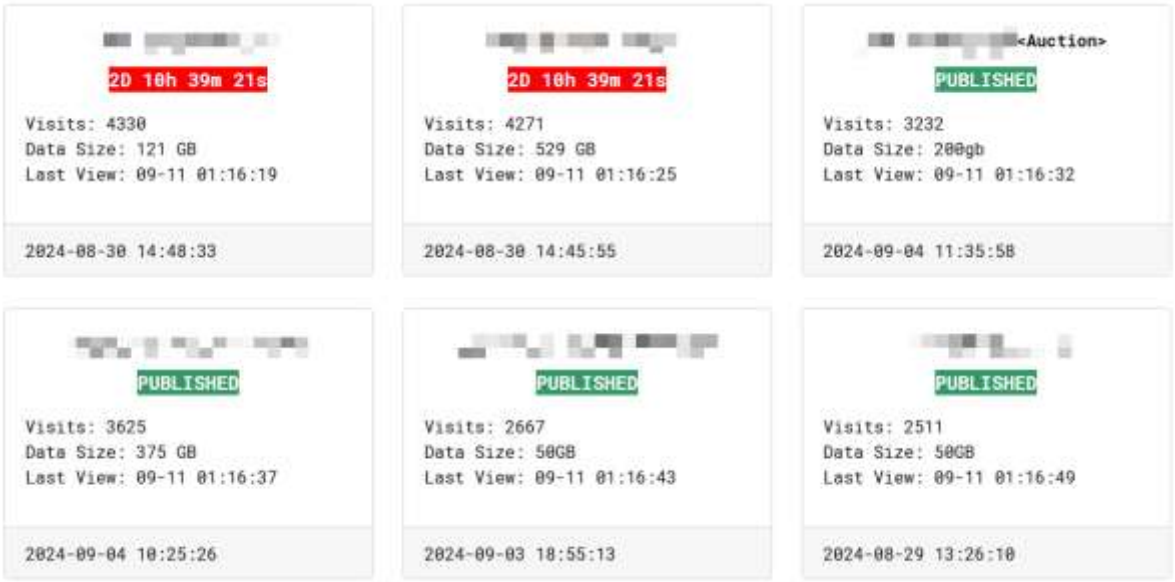

Figure 3-1 Tor page for posting victim information 31

As shown in the figure below, the victim information column indicates that the data stolen from the victim has been made public, has been viewed 2,585 times, 50 GB of data stolen, and last updated at 03: 30: 27 UTC, August 26. Originally published as 21 August 12: 03: 03 UTC.

Figure 3-2 Victim Information Status 32

Enter the information column to see a brief description of the victim, some examples of data stolen and the address used to download the published data.

Figure 3-3 Victim information and data download address 33

The group also sells stolen data by auction.

Figure 3-4 Selling data in the form of an auction 34

About the content of the page for the group related introduction and some regulations.

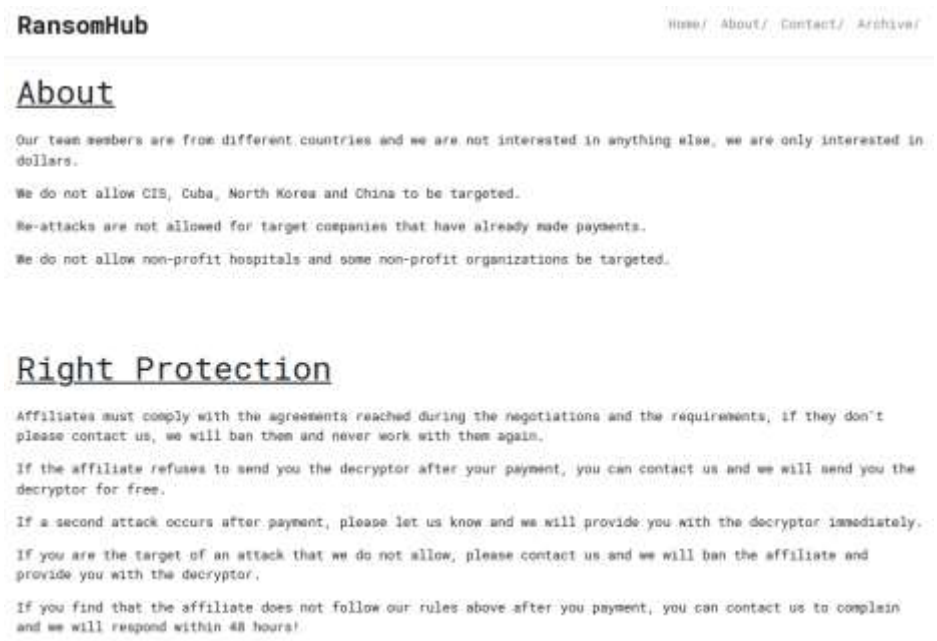

Figure 3-5 Introduction to the group in the Tor website 3-5

The content of the contact page is reserved for victims and members of the group who want to be affiliated.

Figure 3-6 Contact information in the Tor website 36

4 Recommendations for protection

It is suggested that enterprise users deploy professional terminal security protection products, conduct real-time detection of local new and start-up files, and perform periodic virus scanning in the network. Antiy IEP (hereinafter referred to as "IEP"), relying on Antiy's self-research threat detection engine and core-level active defense capability, can effectively check and kill the virus samples found this time.

With core-level protection capability, IEP judges whether there are attack actions such as persistence, power raising and information theft based on the operation behaviors of memory objects such as continuous monitoring of processes by the core driver. Combined with the detection of blackmail behavior characteristic database, we can analyze whether the process behavior is suspected of blackmail attack, and can block the discovered blackmail attack at the first time.

Figure 4-1 When a virus is found, IEP intercepts and sends an alarm at the first time 41

IEP also provides a unified management platform for users, through which administrators can view details of threats within the network in a centralized manner and handle them in batches, thus improving the efficiency of terminal security operation and maintenance.

Figure 4-2 Viewing and completing the handling of threat events through IEP Management Center2

5 Reference

[1] Paranoidlab.paranoidlab spotted RansomHub, a new Ransomware as a Service (RaaS) on the Dark Web. (2024-02-02)

Https: / / www.linkedin.com / feed / update / urn: Li: Activity: 7159288343535484928 /

[2] Bleepingcomputer.knight ransomware source code for sale after leak site shuts down [R/OL]. (2024-02-20)

Https: / / www.bleepingcomputer.com / news / security / knight-ransomware-source-code-for-sale-after-leak-site-cuts-down /

[3] Symantec.ransomhub: New Ransomware has Origins in Older Knight [R/OL]. (2024-06-05)

Https: / / symantec-enterprise-blogs.security.com / secret-intelligence / ransomhub-knight-ransomware

[4] Foresout.analysis: A new ransomware group reports from the Change Healthcare cyber attack [R/OL]. (2024-05-09)

Https: / / www.forescout.com / blog / analysis-a-new-ransomware-group-emergent-from-the-change-healthcare-cyber-attack /

[5] Bleepingcomputer.blackcat ransomware shuts down in exit scam, blades the "feds" [R/OL]. (2024-03-05)

Https: / / www.bleepingcomputer.com / news / security / blackcat-ransomware-shuts-down-in-exit-scam-blazes-the-feds /

[6] Antiy.Watch out for data breaches due to BlackCat ransomware [R/OL]. (2023-07-03)

Https: / / www.antiy.cn / research / notice & report / research _ report / BlackCat _ Analysis.html

[7] Antiy.Boeing Encountered with Blackmail Attack Analysis and Resuming - Threat Trend Analysis and Defense Thinking of Targeted Blackmail [R/OL]. (2023-12-30)

Https: / / www.antiy.cn / research / notice & report / research _ report / BoeingReport.html

[8] Antiy.Review and Outlook of Cybersecurity Threats in 2021 [R/OL]. (2022-01-28)

Https: / / www.antiy.cn / research / notice & report / research _ report / 2021 _ annualreport.html

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.