Cybersecurity Bulletin Board: Revisiting Ransomware Threat Prevention and Mitigation

Antiy CERT

Draft completion date: September 1, 2022

Initial release date: September 3, 2022

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

1 Overview

In recent years, the increasing number of security vulnerabilities, new advanced persistent threat (APT) actors, and new ransomware families have fueled the continued prevalence and profitability of ransomware. Ransomware remains the greatest threat to global cybersecurity. Rapid vulnerability weaponization is a trend in ransomware attacks. Once a new vulnerability is released, attackers and defenders engage in a tug-of-war: will the attacker exploit the vulnerability first, or will the defender patch it? The attacker typically wins. Every minute of delay in patching the vulnerability becomes an opportunity window for attackers, who will spare no effort and rapidly develop exploit code. Looking back at the Microsoft Exchange vulnerability in March 2021 and the Log4J vulnerability in November, we can see how quickly vulnerable code can be transformed into effective exploits. Attackers can quickly "weaponize" vulnerabilities to attack target systems within a few hours. Amid the ongoing COVID-19 pandemic, the increasing exposure of vulnerable remote office terminals, the entry of various new families of ransomware, and the application of other new technologies, ransomware operators are attempting wider attack entrances. These changes will be accompanied by a series of serious and widespread vulnerabilities and large-scale supply chain attacks, exposing more government and enterprises to the risk of ransomware attacks.

Ransomware, a member of the Trojan family, has been around since 1989. In recent years, numerous ransomware families and the organizations behind them have been active worldwide, leading to frequent ransomware attacks. With the continuous advancement of network technology, ransomware attackers are constantly expanding their attack methods and extortion schemes, severely impacting individuals, society, and even critical national information infrastructure.

To strengthen defenses against ransomware attacks, the China Academy of Information and Communications Technology, under the guidance of the Cybersecurity Administration of the Ministry of Industry and Information Technology, collaborated with several other organizations to develop a ransomware protection manual. Antiy's ongoing threat analysis and assessment efforts have also enabled its full product line to gain the initiative in combating ransomware threats. Although ransomware attacks are increasing in number and their methods are becoming increasingly diverse, with some cybercrime organizations even achieving APT-level targeted ransomware attacks, individuals and government and enterprise users can still respond by raising awareness, implementing basic protections, and building a security system. Antiy's full product line can effectively support users' defenses.

2 Ransomware Threat Encyclopedia

2.1 Ransomware and Spread

Ransomware, a member of the Trojan family, has been discovered in recent years. It typically hijacks user files, encrypting documents, emails, databases, source code, images, compressed files, and other files, rendering them inoperable. The ransomware then demands payment in the form of real money, Bitcoin, or other virtual currencies. Typically, ransomware authors set a payment deadline. If the infected user doesn't pay within the specified timeframe, the ransom will increase over time. **Sometimes, even after paying the ransom, users still can't use their systems normally or restore encrypted files.**

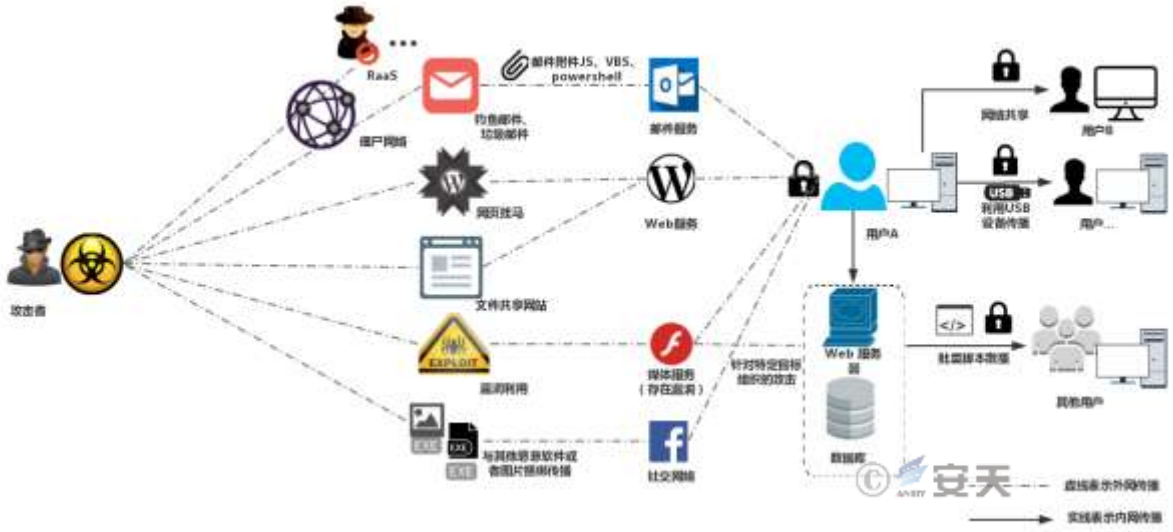

Figure 1Main means of spreading ransomware

Ransomware is a malicious program used by hackers to hijack user assets or extort resources. **It primarily spreads through phishing emails, web malware, exploits, remote login attacks, supply chain intrusions, and removable media.** As businesses accelerate their digital transformation and become increasingly reliant on IT and operational systems, the profits from cybercrime are rising, allowing attackers to employ more sophisticated tactics.

2.2 Can Ransomware Be Decrypted?

Ransomware typically uses a combination of symmetric and asymmetric encryption algorithms to encrypt data. Most ransomware first encrypts the victim's data using a symmetric algorithm, then uses an asymmetric algorithm to encrypt the symmetric key. The private key for an asymmetric algorithm is held only by the attacker. **Brute-forcing an asymmetric algorithm would theoretically take hundreds of years. Therefore, unless the ransomware is absolutely flawed, data recovery is generally impossible.**

2.3 Beware of Third-Party "Decryption Service" Scams

In recent years, with the proliferation of ransomware, various organizations, industries, and even government departments have suffered attacks. This has also led to the emergence of numerous third-party "decryption services". These services offer both paid and free services. They may obtain decryption tools from attackers privately at a price lower than the ransom, effectively profiting from the difference. However, more often, these so-called third-party "decryption services" defraud their victims. Not only are they unable to recover data, they also demand payment before providing "decryption services". Once the victim pays, the "decryption service" will block the victim, pocket the money, and abscond. **Paying third-party services to resolve ransomware attacks after files have been encrypted is often unreliable. Emergency response should be conducted under professional guidance.**

- **Don't pay the ransomDon't Pay the Ransom**

If a user encounters a ransomware attack, he or she should contact the security vendor or security team as soon as possible, conduct emergency response under professional guidance, **minimize losses, and try not to pay the ransom.**

In the emergency response to ransomware attacks, Antiy has encountered cases where victims paid the ransom but did not receive decryption; some attackers even sold the data or directly destroyed it, leaving the victims with nothing but money and goods, resulting in double losses.

For example, in the case of WannaCry, although the organizers behind it claimed that the decryption could be obtained by paying the ransom, the gang only had a payment channel and could not identify the targets who had paid the ransom. In other words, they had no idea who paid the money, and of course they had no way of providing decryption.

On the other hand, remaining uncompromising in the face of criminal activity is a sign of support for justice, while paying is a disguised encouragement of extortion. Attackers are essentially cybercriminals lacking a sense of technical justice and basic business ethics. They are untrustworthy and must be resolutely combated.

2.4 Main Ransomware Types

➢ Encryption

Encryption ransomware encrypts the target's important user data, including documents, audio and video files, pictures, and other files, as well as important system files, disk master boot records, volume boot records, etc. Once the victim's data is encrypted, except for a very small amount of data that may be decrypted due to factors such as logical errors in the encryption algorithm, in most cases, data recovery is only theoretically possible and is basically impossible to crack.

➢ Stealing and leaking secrets

This type of ransomware is primarily designed to increase the success rate of ransomware and counter the target's data backup solutions. It steals relevant data before encryption and filters important data in the background. Later, in addition to encrypting files for ransom, it also extorts the target by publicly exposing this data, imposing multiple extortion demands on the target to force the user to pay the ransom.

➢ Locking

This type of ransomware primarily displays a prominent lock screen to demonstrate its ransomware intent. Its locking strategy primarily involves disguising the screen and blocking file or system access to achieve a certain degree of ransom. This type of ransomware generally does not encrypt user data, allowing for some data recovery potential. It is more prevalent on mobile devices.

➢ Destruction

The ultimate goal of this type of ransomware is to disrupt the availability of targeted systems and businesses, primarily through file rewriting, random string replacement, and malicious deletion of critical programs or files. Once a user's system is infected with this type of ransomware, recovery is virtually impossible.

2.5 The Development Trend of Ransomware Attacks

➢ **Ransomware attacks have become one of the major cyber threats facing the world**

In recent years, governments and enterprises have been vigorously promoting digital transformation. Individuals and organizations have become increasingly reliant on emerging technologies like the internet and cloud computing, and the importance of infrastructure assets and stable business operations has grown. Ransomware attacks target these very same government and enterprise entities. Ransomware platforms and services are constantly evolving, with new ransomware groups emerging. Ransomware attacks are becoming increasingly diverse, highly targeted, and multifaceted.

➢ **Multi-platform ransomware attacks are becoming more sophisticated**

Ransomware targeting Windows systems continues to emerge, while ransomware targeting Linux and macOS operating systems, such as DarkSide, Conti, MacRansom, and MacSpy, is also emerging. Ransomware targeting industrial control systems, such as EKANS and Cring, has even emerged. Furthermore, while large-scale ransomware attacks targeting mobile platforms have yet to occur, the sheer number of mobile users presents significant security risks.

➢ **The "multi-ransomware" model poses a greater threat**

With the emergence of mature solutions for user endpoint protection and data backup, single-file ransomware schemes, such as encrypted files, are no longer sufficient for attackers. Consequently, multiple ransomware schemes, such as stealing and encrypting, or stealing and encrypting, and leaking, have been adopted by many ransomware attackers. Once users fall victim to these ransomware attacks, even if their files are decrypted, the confidentiality of their data is no longer guaranteed.

➢ **Ransomware linked to APT attacks**

In order to implant ransomware into high-value target systems, it requires sophisticated attack techniques. In the cybersecurity space, users of sophisticated attack techniques are often associated with APT groups. Furthermore, after a ransomware attack, users often focus on the ransomware incident itself, demonstrating a strong ability to focus. This encourages ransomware attackers to continuously learn APT intrusion techniques, and APT groups often disguise targeted attacks as ransomware attacks.

- **The RaaS model is becoming more mature and stronger**

Driven by growing profits, the builders of Ransomware-as-a-Service continue to iterate RaaS functions and models, expand the scale of their ransomware, provide services to large ransomware gangs, and collect generous ransoms.

- **Ransomware and mining Trojans work hand in hand**

The successful insertion of ransomware relies on its intrusive capabilities. By the time the ransomware is delivered, it's already within the target system. Driven by profit, the ransomware attackers also deploy a mining trojan, which is equally profitable. This aligns with the nature of ransomware attackers, who continuously exploit their targets for surplus value. Furthermore, it's possible that the ransomware attackers will collaborate with mining gangs to maximize their profits.

- **Attacks targeting critical information infrastructure and industrial control systems emerge**

With the digital transformation of various industries, critical information infrastructure and industrial control systems are becoming increasingly important, with wider coverage and more functions. This has attracted the attention of attackers. For example, in May 2021, Antiy CERT detected an attack targeting industrial control systems with the Cring ransomware, which ultimately led to the temporary shutdown of industrial control systems in several European countries.

- **A mature third-party data leakage platform has emerged in the ransomware industry chain**

To exfiltrate stolen data for ransom, ransomware requires a relatively public and untampered platform. Therefore, attackers employing this ransomware model favor establishing such platforms on the dark web. According to statistics, since 2019, ransomware attack groups have collectively leaked data from over 2,100 companies via the dark web. At the same time, some groups are shifting gears to focus on data exfiltration for ransom, such as the Babuk group.

- **Imitating and impersonating "well-known" ransomware families to extort ransoms**

Because some ransomware is open source, it has, to some extent, encouraged imitation by other attackers. Some attackers, possessing some attack techniques but generally low levels of skill, will, after controlling and locking a victim's device, display a ransom note identical to that of a well-known ransomware family, giving the victim the illusion of a powerful ransomware attack. However, these attacks may not even encrypt the victim's data.

3 How to Prevent and Treat Ransomware?

3.1 To Prevent Ransomware, You Must Do the Following "Nine Things"

Figure 2 Nine tips for preventing ransomware

3.2 To Prevent Ransomware, You Must Do the Following "Four Don'ts"

Figure 3 : Preventing ransomware – Four things not to do

3.3 How to Deal with the Unfortunate Situation of Being Infected by Ransomware?

When a machine is infected with ransomware, don't panic. You can immediately carry out the following emergency measures to reduce the harm caused by the ransomware: **isolate the network, classify and deal with it, report it in time, investigate and reinforce it, and provide professional services.**

- First, the machine infected with the ransomware must be disconnected from the network to prevent the ransomware from spreading laterally and continuing to infect other machines in the local area network.
- Do not restart the machine. Some ransomware has logic problems in its writing, and it is possible to recover some encrypted files without restarting the machine.
- Don't rush to reinstall your system, format your hard drive, or do anything else that might damage encrypted documents. Back up encrypted documents first. Encrypted files with a suffix are not contagious and can be copied to any computer for backup and preservation, but the likelihood of recovery is extremely low. Consider waiting for a decryption solution, as some ransomware decryption tools are released for various reasons.
- While the ransomware family type can be identified from information such as the extension and ransom note, the specific process of how the malicious code encrypts and propagates within the user's network remains unclear, making it impossible to accurately determine its type. Although similar virus samples are available from the Antiy virus database and we intend to confirm this by simulating the infection process, the infection process and the source of infection require further refinement. We recommend on-site security services to locate and trace the source.

4 Build a Solid Foundation for Security Baseline Defense

➢ Password Management

Analysis of multiple ransomware incidents reveals that remote delivery and execution based on weak system passwords and unified passwords are also important attack vectors. Even with basic security configuration requirements such as setting complex passwords and prohibiting the use of unified passwords at multiple locations, many information systems still fail to implement them.

In network security protection, it is imperative to strictly implement account password security management, focusing on troubleshooting weak passwords and establishing relevant information security groups to manage, supervise, and audit account password issues. All terminals and servers must be configured with passwords, and the phenomenon of no passwords is prohibited. When transmitting account numbers and passwords, encryption measures should be taken to prevent them from being intercepted during transmission. Passwords should be of sufficient length and complexity, using a combination of numbers, letters, and symbols to make them difficult to guess and crack.

Passwords should be modified regularly, and the password usage cycle should not exceed the specified period. Users must change their passwords when the administrator requests a password change. There should be no direct connection between the new password and the old password to ensure that the new password cannot be inferred from the old password. Passwords should not use combinations with specific meanings, such as the user's name, birthday, and other easily guessed information. Password repetition rate should be strictly checked to avoid password sharing to prevent attackers from using the same password to invade multiple hosts. Passwords must not be stored in the local system to prevent them from being stolen. Each account must enter a password when logging in, and default account logins are prohibited.

➢ Vulnerability Patches

An increasing number of ransomware attacks are exploiting outdated vulnerabilities and system configuration flaws. Timely patch updates and security hardening can prevent most attacks, especially those that are not targeted. While the "EternalBlue" vulnerability used by WannaCry is certainly a weapons-grade vulnerability, at the time of the ransomware attack, the patch for this vulnerability had already been released for two months. It also includes the 2021 Exchange vulnerability and Log4J vulnerability. The Conti ransomware uses the ProxyShell (CVE-2021-34473, CVE-2021-34523 and CVE-2021-31207) vulnerabilities to spread to Microsoft Exchange servers; AvosLocker, Conti, Khonsari and TellYouThePass ransomware have used the Log4J vulnerability to carry out ransom attacks. Recently, the TellYouThePass ransomware used the vulnerability of Chanjet T+ software to spread; REvil ransomware used the VSA software (CVE-2021-30116, CVE-2021-30119 and CVE-2021-30120) vulnerabilities under Kaseya to spread; Magniber ransomware used the printer PrintNightmare (CVE-2021-34527) vulnerability to spread.

Security patches are a security maintenance measure provided by the manufacturer, while security hardening strengthens the system's inherent security capabilities. These are both cost-effective and effective. A comprehensive security mechanism and security operation specifications are needed to uniformly manage asset vulnerabilities, patches and upgrades, and security configuration hardening. This includes establishing an asset vulnerability database, patch sources, patch reliability verification, customized patch upgrade plans, patch phased upgrades, a retention review mechanism, and security configuration hardening in accordance with STIG standards. These measures must be strictly implemented according to the roles, responsibilities, and processes defined in the security operation specifications to ensure the inherent security of the system.

➢ Permission Control

The significance of authority control is to ensure that employees perform their duties, each person is responsible for different content, and do not interfere with each other, thereby improving work efficiency; the scope of work that each person is responsible for is specific and clear, responsibilities are assigned to individuals, rights and responsibilities are clearly defined, and problems can be traced; the importance of the work that different people are responsible for varies, such as confidential or important decisions are only known to a few people, which can ensure privacy and avoid risks.

When employees' job responsibilities change and their existing responsibilities are no longer consistent with their existing account permissions, they should apply for a permissions change. If an administrator discovers that a user has permissions not required for their current job, they can notify the administrator and revoke the unnecessary permissions. Regularly check account status and contact the account manager to determine account closure and permission limits. Once an account is opened, permissions should be established according to the principle of providing services with minimal permissions and minimal resources. Any request for higher permissions requires review and approval based on actual circumstances. These methods can mitigate the wider impact of a single account compromise.

➢ Intranet Enhancement

Enterprises should establish necessary partitions based on the access scope of each system, logically isolating each system from another. Similarly, each system should also be partitioned to prevent widespread system downtime in the event of a security threat.

Based on security requirements and mitigation needs, a security barrier should be established between internal and external networks by integrating firewalls, one-way transmission gateways, intrusion detection, deep packet inspection, restoration, and caching. For similar threats, relying solely on network interception is insufficient; the last line of defense at the endpoint must be strengthened, emphasizing the effective return of endpoint defense. Deploy endpoint defense software focused on effective protection. Regularly review device event alerts daily to avoid situations where incidents have already occurred but remain unnoticed; strengthen system protection strategies; and review host-related security settings, promptly revising any issues.

Determine the importance of enterprise systems, data, and configuration files based on the company's own characteristics, adopt different backup strategies for different importance, and regularly confirm the validity of backup information.

5 Industry Joins Forces to Tackle Ransomware Threats

To strengthen defenses against ransomware attacks, the China Academy of Information and Communications Technology (CAICT), under the guidance of the Cybersecurity Administration of the Ministry of Industry and Information Technology (MIIT), collaborated with seven organizations—China Telecom, China Mobile, China Unicom, Antiy Technology Group, Hangzhou Anheng Information Technology, Qi'anxin Technology Group, and NSFOCUS—to develop the "Ransomware Security Protection Handbook", which was officially released by CAICT. Antiy contributed a significant amount of original material, including analytical reports, case studies, and protection recommendations, to the development of this handbook.

As the "national cybersecurity team" that has continuously engaged in real-world combat against cyber threats for two decades, Antiy has maintained ongoing tracking and analysis of ransomware attacks. In 2006, it captured China's earliest known Redplus ransomware Trojan. In August 2015, Antiy released a lengthy report, "Unveiling the True Face of Ransomware". In May 2017, during the response to the major WannaCry ransomware attack, Antiy pioneered the release of the network's first full-length analysis report. It quickly provided specialized anti-virus tools and a Monday boot guide, distributed thousands of emergency response CDs to government and enterprise organizations, and subsequently developed a decryption tool based on memory key retrieval, earning praise from multiple regulatory authorities. Antiy also conducted emergency response and conducted detailed analysis and assessment of major and prevalent ransomware strains, including GANDCRAB, GlobeImposter, Sodinokibi, Phobos, and WannaRen. The company has published over 40 reports, including analysis, warnings, and response recommendations, related to ransomware attacks.

Antiy's continuous threat analysis and assessment work has also enabled Antiy's full range of products to gain the initiative in combating ransomware threats.

6 Antiy IEP Comprehensively Builds a Security Line of Defense on the Endpoint System Side

The vast majority of ransomware attacks target the host system and the data on it. At the same time, as encryption protocols are increasingly weakening security perimeters like firewalls, the focus of network security is shifting back to the host system. For government and enterprise endpoint scenarios, Antiy has developed the IEP terminal defense product family. Developed based on the UES (Unified Endpoint Security) concept, IEP integrates modules such as virus detection, configuration hardening, trusted environment verification, active defense, distributed firewalls, media control, and web server protection. These modules effectively cover the security needs of traditional desktops, workstations, servers, virtualization, and containers, and provide kernel-level defense for Windows, Linux, Android, and domestic operating systems such as Euler, Kylin, and Tongxin.

IEP has built a 5+2 defense system against ransomware attacks, offering a "five-layer defense, two-closed-loop" solution. The five layers of defense encompass system hardening, (host) perimeter defense, scanning and filtering, active defense, and document security. The two closed-loop systems include EPP (endpoint protection) for real-time defense and EDR (endpoint detection and response) for near-real-time/asynchronous defense.

Table 1 The mechanism of Antiy Intelligent Endpoint Protection System in protecting against ransomware

Protection level	Technical principle
System hardening	Through the baseline and patch checking functions, it is possible to check and patch system configuration vulnerabilities, strengthen patches, and adjust the system's own security policies, thereby reducing the exposure to ransomware attacks including open ports, weak passwords, unnecessary services, and reducing the success rate of vulnerability exploitation.
(Host) perimeter defense	Through the distributed host firewall and media control functions, scanning and intrusion data packets are intercepted, the transmission of attack payloads is blocked, and the automatic operation of USB flash drives, CDs, etc. is blocked, making it difficult for ransomware attacks to gain access to the host.
Scan filtering	Based on the Antiy AVL SDK anti-virus engine, it scans file objects, sector objects, memory objects, registry data objects, etc. to determine whether the detected object is a known virus or a suspected virus, thereby achieving accurate judgment and killing.

Active defense	Based on the kernel driver, it continuously monitors the operation behaviors of memory objects such as processes, and determines whether there are attacks such as persistence, privilege escalation, and information theft. It also determines whether there are operations such as batch reading, writing, deletion, and moving files or sectors. It enables the file credit (signature verification) mechanism and filters normal application operations to reduce false positives.
Document security	By deploying multiple decoy files and monitoring them in real time, we can trick ransomware into prioritizing their destruction, achieving a deceptive defense. A multi-point real-time backup mechanism ensures rapid recovery even if legitimate files are encrypted.

With such a mechanism design, supplemented by 10 local virus database upgrades per day, real-time cloud database upgrades, and regular threat intelligence push, Antiy IEP can effectively prevent viruses from landing, block malicious behaviors, protect important documents, and comprehensively and effectively protect users from the threat of ransomware attacks.

Figure 4 Schematic diagram of the protection principle of Intelligent Endpoint Protection System against ransomware

Figure 5 IEP (desktop edition) ransomware attack interception and document protection interface example

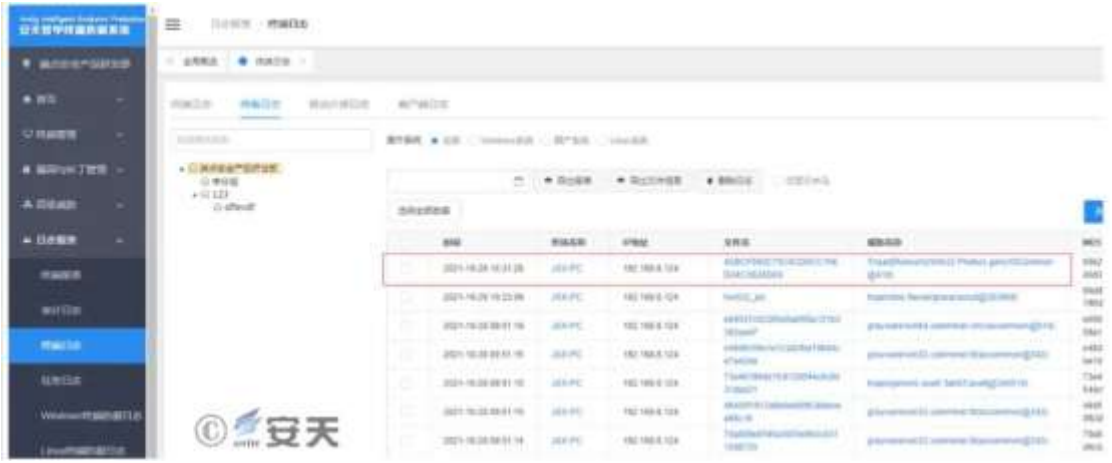

Figure 6 Threat alert and handling interface of IEP Management Center

7 Antiy's Full Range of Products Supports Users in Building a Comprehensive Protection System

Currently, the targeted ransomware attacks launched by some cybercrime organizations have reached the level of APT (Advanced Persistent Threat) targeted attacks. Users need a more dynamic and comprehensive ransomware attack security protection system. Antiy's full range of products can effectively support the construction of user defense positions.

Table 2 An introduction to the security protection value of Antiy's full range of products against ransomware attacks

Product brand	Product positioning	Deployment method	The value of ransomware attack protection

Intelligent Endpoint Protection System	UES (Unified Endpoint Defense, covering EPP\EDR\CWPP)	Installed (or prefabricated) on the system host.	The host hardening mechanism reduces attack surface exposure, while the perimeter defense mechanism intercepts network connections and media operations. Driver-level monitoring provides real-time awareness of newly added local files and their actions, invoking the Antiy AVL SDK anti-virus engine for precise detection and removal. Active defense mechanisms identify and terminate suspicious behavior, and combined with decoy file protection and process behavior profiling, programs with ransomware behavior can be discovered and intercepted. Furthermore, IEP can identify document write behavior and, if suspected malicious encryption activity is detected, automatically backs up the document before it is destroyed. File recovery can then minimize user losses.
Persistent Threat Detection System	NDR (Network Detection Response)	It can be deployed in bypass mode at government and enterprise network exits, key network segments, and other locations, and can be deployed as a cloud resource pool.	PTD senses and detects ransomware attacks based on network traffic, including scanning, probing, phishing email delivery, remote Trojan implantation, lateral movement, and C2 connection. It also captures attack payloads based on traffic-side protocol parsing and restoration, and calls the Antiy AVL SDK anti-virus engine for more accurate detection, enabling it to detect network-side activities of ransomware attacks in advance, and coordinate responses and disposal.
Attack Capture System	Threat Deception Capture	Supports deployment scenarios such as enterprise intranet, isolated network, private cloud, and public cloud.	ACS supports capturing threat attacks through simulated deception of systems and applications. It can be combined with diversion equipment to effectively perceive scanning detection, brute force cracking, vulnerability attacks, lateral spread of the intranet and payload delivery, thereby attracting ransomware attacks into the honeypot, quickly discovering ransomware incidents and intelligence, and coordinating responses and disposal to provide users with timely defense and block the spread of ransomware threats.

Persistent Threat Analysis System	FA (Document Analysis)	In bypass deployment, the linkage device and the query result terminal must be reachable.	PTA can be used in conjunction with Antiy's full range of products, including IEP and PTD, or manually interacted with by security engineers. It uses a dual mechanism to analyze file objects based on deep static analysis and a highly simulated sandbox environment. For ransomware attack file payloads, it can effectively analyze and identify vulnerability exploitation, privilege escalation, defense confrontation, file encryption, and backup disabling behaviors, assisting users in generating threat intelligence and coordinating threat response and disposal.
Antiy Emergency Handling Toolbox	Emergency Response	Based on U disk, CD, portable device and scene connection.	Based on threat detection and analysis of terminal systems, including the extraction and analysis of all elements of objects such as processes, services, kernels, and boot sectors, Tophen uses the Antiy AVL SDK anti-virus engine for more accurate detection, detecting and retaining attack payloads, and extracting suspicious objects. This effectively discovers ransomware attacks on endpoints and, through underlying disposal capabilities, eliminates ransomware entities and their boot chains, completing a closed-loop threat discovery, analysis, evidence collection, and disposal service.

8 Antiy's User-Facing Products and Services

➢ Vertical Response Service Platform

"Antiy Vertical Response Service Platform" is a one-stop service platform under Antiy that focuses on meeting the security needs of small and medium-sized enterprises and individual (family) users. The Antiy Vertical Response Service Platform has launched a lightweight ransomware risk assessment for Windows hosts and provides dedicated response tools to help customers quickly identify process risks.

Detailed address: https://vs.antiy.cn/endpoint/rdt

➢ Antiy Antivirus Software

For personal and home users, it is recommended to install and use Antiy Antivirus (Windows version) for effective security protection. Detailed address: https://vs.antiy.cn/endpoint/anti-virus

➢ Antiy Emergency Response Service

Antiy continues to empower users to build effective ransomware attack security protection systems and achieve effective security value.

National service hotline: 400-840-9234

Service support email: support@antiy.cn

Appendix 1: References

[1]. Analysis of Cring Ransomware Samples Targeting Industrial Control Systems

https://www.antiy.cn/research/notice&report/research_report/20210528.html

[2]. Conti Ransomware Analysis Report

https://www.antiy.cn/research/notice&report/research_report/20211220.html

[3]. Chanjet 0day ransomware attack incident correlation attribution and product solutions

https://www.antiy.cn/research/notice&report/research_report/20220830.html

[4]. China Academy of Information and Communications Technology releases the Ransomware Security Protection Manual

http://www.caict.ac.cn/kxyj/qwfb/ztbg/202109/t20210908_389515.htm

[5]. Antiy Ransomware Attack Series Report

https://www.antiy.cn/research/notice&report/research_report/index.html

[6]. Antiy CERT: Unveiling the True Face of Ransomware

https://www.antiy.com/response/ransomware.html

[7]. Analysis of WannaCry Ransomware Worm Variants

https://www.antiy.com/response/Antiy_Wannacry_Explanation.html

[8]. Antiy products help users effectively protect against ransomware attacks

https://www.antiy.cn/About/news/20211101.html

[9]. Understanding Ransomware Attacks and Their Dangers from Eight Aspects, Part 1: Four Roles in Ransomware Attacks

https://www.antiy.cn/About/news/20211102.html

[10]. Understanding Ransomware Attacks and Their Dangers from Eight Aspects, Part 2: Two Typical Patterns of Ransomware Attacks

https://www.antiy.cn/About/news/20211103.html

[11]. Understanding Ransomware Attacks and Their Dangers from Eight Perspectives, Part 3: Common Spreading Methods and Intrusion Routes

https://www.antiy.cn/About/news/20211104.html

[12]. Understanding Ransomware Attacks and Their Dangers from Eight Perspectives, Part 4: Analysis of the Ransomware Kill Chain

https://www.antiy.cn/About/news/20211105.html

[13]. Understanding Ransomware Attacks and Dangers from Eight Aspects Part 5: Four Main Types of Ransomware

https://www.antiy.cn/About/news/20211108.html

[14]. Understanding Ransomware Attacks and Their Dangers from Eight Aspects Part 6: Important Attack Characteristics

https://www.antiy.cn/About/news/20211109.html

[15]. Understanding Ransomware Attacks and Their Dangers from Eight Aspects Part 7: Ten Typical Families

https://www.antiy.cn/About/news/20211110.html

[16]. Understanding Ransomware Attacks and Their Dangers from Eight Aspects Part 8: The Development Trend of Ransomware Attacks

https://www.antiy.cn/About/news/20211111.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.