2022 网络安全威胁的回顾与展望

Antiy Annual Security Report

Disclaimer: This document is an internal document of Antiy Labs and is the basic material for the official version of Antiy Cyber Threat Annual Report. It is not a mature annual report. It is only for internal discussion of Antiy and shared with industry experts and partners for supplementary comments. Any public release and disclosure of all or part of this document must be authorized by Antiy again.

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

First draft completed: December 31, 2022, 21:32

First published time: January, 2023

This version updated: January 9, 2023

This report is a machine-translated version.

Antiy Computer Emergency Response Team (Antiy CERT)

Introduction

Digital economy is the direction of future development. General Secretary Xi Jinping pointed out in the report of the 20th National Congress of the Communist Party of China that "we should accelerate the development of digital economy and promote the deep integration of digital economy and real economy". Against the backdrop of the accelerated evolution of the century-old changes, the continuous impact of the century-old epidemic, and the complex and turbulent international situation, the cybersecurity industry should establish a practical, systematic and normalized security barrier to ensure the development of the digital economy. Cybersecurity companies need to use their own security product system to solve the security problems of digital data.

It has been a tradition for Antiy to release a pre-release version of the annual report at the winter training camp every year and solicit opinions and suggestions from participating experts.

In this year's annual report, Antiy summarized its thoughts and opinions on advanced persistent threats (APT), ransomware attacks, mining Trojans, botnets, attack and defense confrontation, data leakage, industrial Internet security risks, and threat generalization:

Regarding advanced persistent threats (APT): Antiy sorted out the distribution and activity of global APT organizations and actions in 2022, and produced a "Global APT Attack Actions, Organizational Affiliation and Geographical Location Distribution (Activity) Map".

The "Russia-Ukraine conflict" has caused both sides to suffer varying degrees of losses in cyberspace. Cyber blitzkrieg has become Russia's vanguard in the "Russia-Ukraine conflict". Russia's operating habits and tactics are to first launch a cyber attack, successfully target network infrastructure and other targets through phishing, and finally launch a coordinated combat attack on the battlefield of traditional kinetic weapons. Russia's application of advanced attack technology in cyber warfare has had an impact on global geopolitical activities, prompting more intense geopolitical activities in countries and regions around the world, including Russia and Ukraine.

The ease of tampering with digital evidence has prompted foreign APT organizations to use cyber attacks to frame others. In February 2022, Antiy released a report revealing the hidden signs of an APT organization with an Indian background, finding that the organization mainly targeted social activists, social groups, and opposition parties in India, and also stole important intelligence on military and political targets in neighboring countries such as China

and Pakistan. The attackers reported the results to the local police, who raided the target's home and seized the illegal letters used as digital evidence for the purpose of framing.

APT attacks using IoT devices to conduct battlefield pre-installation are frequent. In early 2022, Antiy discovered that the OceanLotus organization, in its cyber attack activities against China, pre-captured public network routers, cameras and other IoT devices throughout many important provinces and cities in China through weak password blasting and vulnerability attacks, and installed traffic forwarding tools to forward the secret-stealing and control traffic of the Torii remote control Trojan through one or more layers of springboards to the real Torii remote control server.

About ransomware attacks: Ransomware is usually used as a criminal tool by attack organizations for economic purposes. Looking back at the ransomware attacks that occurred in 2022, it was found that some **ransomware was used by attack organizations with national backgrounds as a "politicized" criminal tool to carry out cyber attacks. During the** Russian-Ukrainian conflict, "politicized" ransomware attacks occurred frequently and were accompanied by the reappearance of "destructive" ransomware, disguised as ransomware attacks, but the actual goal was to destroy the operation of the system, thereby transforming cyberspace attacks into physical space impacts. With the continuous innovation of network security technology and the construction of solid border protection barriers by security equipment, threat actors cannot achieve intrusion by using common executor propagation methods, and hire victim target internal personnel to carry out cyber attacks as a new means. There has also been a new shift in ransomware strategies, from the traditional ransomware attack "stealing + encryption" to "stealing + deletion or destruction" attacks. Cross-platform ransomware executors help threat actors infiltrate increasingly complex network environments, and also bring new challenges to security workers in executor analysis.

About mining Trojans: With the continuous improvement of mining Trojan anti-technology, more and more mining Trojan gangs have mastered the ability to quickly integrate vulnerabilities. Their way of connecting to the mining pool is also more covert, and traditional intelligence mining pool blacklist detection will gradually become ineffective. The decline in virtual currency prices in 2022 has not only failed to reduce malicious mining, but has made it more active.

About botnets: The global political situation continues to change in 2022, and using botnets to launch politically motivated DDoS attacks has become the main means of confrontation between major powers; through statistics on

vulnerability exploits disclosed in 2022, it is found that botnets are actively using newly emerging vulnerabilities to spread; botnets using P2P propagation methods are widely spread among IoT devices.

Regarding attack and defense confrontation: In recent years, the inequality of attack and defense confrontation costs has become increasingly obvious. Government and enterprise users often need to pay a lot of network security construction and operation costs to fight against the rapidly increasing complexity of various attack surfaces, the difficult-to-control supply chain product security, and the new exposure and security risks brought by new infrastructure and information technology products. However, the widespread abuse of standardized cyberspace equipment with hidden payloads has undoubtedly made the cost of attack and defense confrontation even more unequal. At the same time, the shortage of professional security practitioners will continue to promote the development of automation in the field of security operations, and artificial intelligence (AI) will be effectively used in a series of products to provide enhanced security results at a faster rate.

About data leakage: In 2022, the COVID-19 pandemic is still raging around the world. All walks of life around the world have accelerated their digital transformation. While the value of data has been further highlighted, data leakage continues to occur frequently. Data leakage incidents continue to become news hotspots, involving fields including industrial manufacturing, government affairs, medical care, finance, transportation, etc., and the situation is still very severe. The more information-based an industry is, the more data leakage incidents there are, and the greater the harm caused by the leakage. The continued high-frequency data leakage incidents have seriously threatened the privacy and security of hundreds of millions of people around the world.

Regarding the security risks of the Industrial Internet: In recent years, China has actively laid out the Industrial Internet. Driven by national policies and market demand, China's Industrial Internet has flourished, many applications have been gradually implemented, and the market scale has continued to expand. In this year, the cybersecurity threats faced by the Industrial Internet also deserve our high attention, including but not limited to: the geopolitical situation has intensified , regional military conflicts represented by the Russia-Ukraine conflict, and territorial conflicts represented by the Arab-Israeli conflict have erupted, and their negative impact has affected the Industrial Internet to a certain extent; the number of vulnerability risks disclosed for Industrial Internet infrastructure worldwide has exceeded 100, and the serious negative impact that may be caused by the vulnerability risks cannot be ignored; in the face of new attack scenario risks such as "Evil PLC Attack", all parties involved in the Industrial Internet should promptly change their defense ideas and formulate effective targeted defense plans as soon as possible; for the emergence and development of the dark web market "Industrial Spy" that is related to the security of the

Industrial Internet and trades stolen data, all parties involved in the Industrial Internet should also pay necessary attention and strengthen corresponding defense measures.

Regarding the threat of generalization: The generalization of threats leads to an increase in the exposure of users' assets. Attackers can use the increased attack surface to create a wide range of security threats such as unauthorized access, springboard attacks, intrusion into "isolated networks", asset control, asset destruction, data leakage, etc.

1 Advanced Persistent Threat (APT)

The overall situation of global advanced persistent threat (APT) activities in 2022 remains very severe. Based on internal and external intelligence sources that Antiy continuously monitors, there are 521 global public security research reports in 2022, of which the disclosed security reports involve 134 APT threat organizations, 57 new APT threat organizations in 2022, and no less than 67 attacks against China in 2022. Antiy sorted out the distribution and activity of global APT organizations and actions in 2022 , and produced a "Global APT Attack Actions, Organizational Attribution Geographical Location Distribution (Activity) Map", of which there are 490 APT organizations (due to limited image space, only the main attack organizations are shown). According to the diagram, it can be found that they are mainly distributed in the United States, Russia, India, Iran, the Korean Peninsula, the Middle East and some countries and regions. Some organizations have failed to determine their belonging countries or regions due to insufficient intelligence.

Figure 1-1 Global APT attack operations, organization affiliation and geographical location distribution map in 2022

1.1 We Need to Be Vigilant Against More Unknown APT Organizations Lurking Deep in Cyberspace

In 2022, Antiy tracked more than 500 APT-related reports around the world, involving more than 130 APT organizations, including more than 50 new APT organizations. Through the study of historical reports, it is found that global cybersecurity agencies expose and disclose new APT organizations every year. After years of accumulation, compared with typical well-known APT organizations, on the one hand, the number of these organizations is already very large, which is several times that of typical well-known organizations; on the other hand , there are few reports on in-depth research and attribution of these attack organizations. Security agencies and researchers lack understanding of their techniques and tactics, infrastructure and behind-the-scenes background; therefore, these organizations are more complex, mysterious and hidden than typical well-known organizations. It is precisely because of this that these unknown organizations need our attention and vigilance. They may lurk for a long time without being discovered, causing greater harm than well-known organizations.

Figure 1-2APT organizations observed by Antiy in 2022

For unknown APT organizations that disclose very little information, although in most cases security research institutions can learn some information about the attackers, such as their native language or location information, the remaining missing clues may lead to embarrassing attribution errors or worse judgments. As a large number of tracing technology reports have been made public, attackers in the dark are also making every effort to use various means to ensure that they are not discovered, and even if they are captured, they will ensure that they are not attributed and leave as few traces as possible. They have implemented a variety of technologies to make analysis and research more difficult. For example, using commercial software, penetration testing tools, and fileless entity technologies to mislead security researchers by placing false marks. These anti-tracing and anti-forensic technologies will make organizational attribution a matter of luck. This is also why security researchers have often discovered attack activities of new organizations in recent years, but rarely have they dug out complete actions and background attribution. In the future of tracking and confronting APT organizations, it may be more important to deeply track and dig into these unknown organizations.

1.2 Cyber Blitzkrieg Becomes Russia's Vanguard in the "Russia-Ukraine Conflict"

Cyber blitzkrieg aims to explore the collaboration between cyber forces and traditional combat forces [1]. According to the security vendor ESET [2], on February 23, 2022, a destructive cyber attack using HermeticWiper against multiple Ukrainian organizations preceded its military operations by several hours. Based on the timeline of the malicious code, it can be judged that the cyber attack had been planned for several months. The attacker first obtained Active Directory server permissions, and then HermeticWiper is deployed through the default domain policy (GPO). In addition, in the intranet, the related custom worm HermeticWizard spreads HermeticWiper in the infected network through SMB and WMI. On February 24, 2022, the Russian-Ukrainian conflict broke out. The second destructive attack on the Ukrainian government network began, this time with the release of a new wiper IsaacWiper. According to the existing threat intelligence, IsaacWiper may have been spread through lateral movement after the previous successful intrusion, or remotely released through the remote access tool RemCom.

The "Russian-Ukrainian conflict" has caused both sides to suffer varying degrees of losses in cyberspace. GhostSec, a hacker group supporting Ukraine (which has long operated as part of Anonymous), has previously controlled printers of Russian state and military organizations. On July 20, 2022, GhostSec wrote a tool called KillBus for attacks against Modbus devices. As the name of the software suggests, by extracting information, overwriting data, and then using it as a slave device (communication in the Modbus protocol is based on the principle of passing

data messages between clients), it effectively destroyed the industrial control system server of the hydroelectric power plant, the intervention in the power plant system, and subsequently caused an explosion at the Gysinoozerskaya Hydropower Station in Russia, which led to the subsequent emergency shutdown of the power plan and caused power outages in large areas of Siberia. GhostSec claimed responsibility for the attack.

Russia's operating habits and tactics are to first launch a cyber attack, successfully target network infrastructure and other targets through phishing, and finally launch a coordinated combat attack on the battlefield of traditional kinetic weapons. At the same time, it is good at using the tactics and techniques of other APT organizations to launch cyber attacks. As shown in the figure below, it highlights the characteristics of Russia's coordinated cyber and traditional operations. Take the attack activities of the STRONTIUMN (APT28) organization with a Russian national background as an example. On March 4, 2022, STRONTIUMN moved horizontally on the computer network of the nuclear power company in the Ukrainian city of Vinnitsa. Subsequently, the Russian military attacked and occupied the company's largest nuclear power plant. In the same week, STRONTIUMN destroyed the computer network of the Vinnitsa government and launched eight cruise missiles at the airport in Vinnitsa two days later [3].

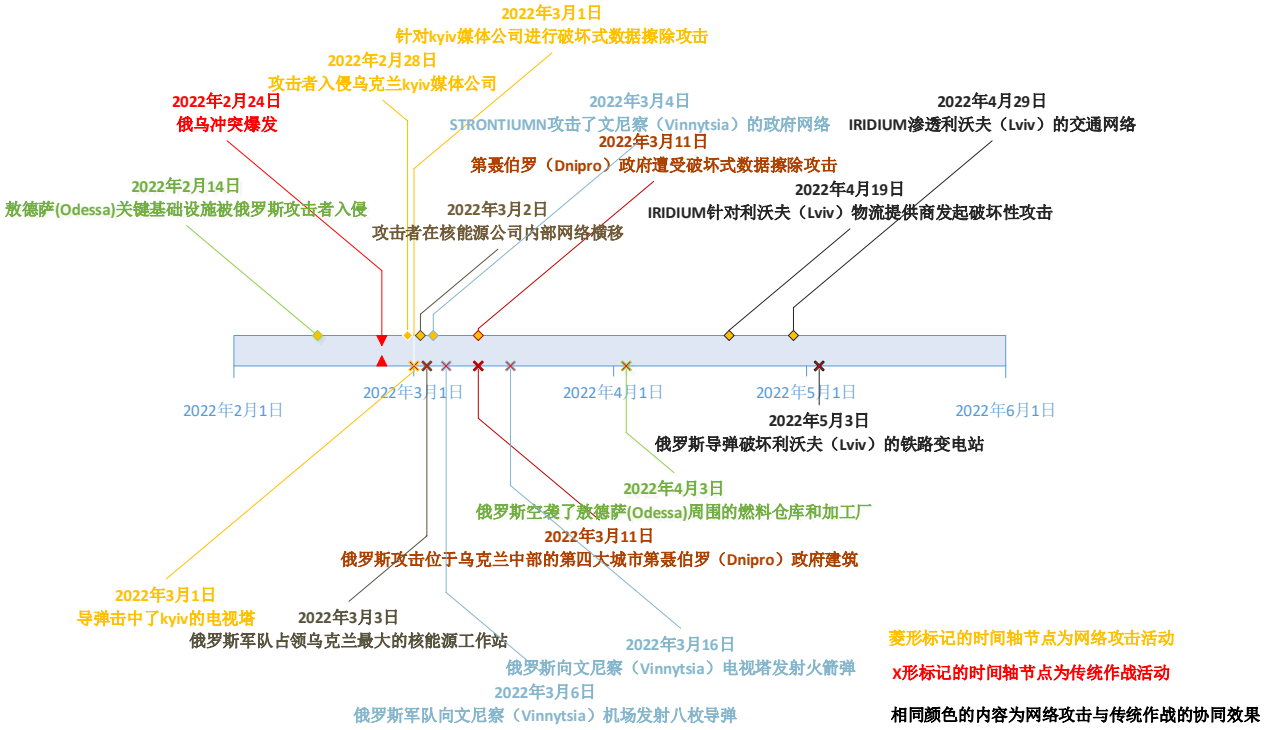

Figure 1-3Russian cyber and traditional coordinated operations [3]

1.3 Russia's Use of Advanced Attack Techniques in Cyber Warfare Has Had an Impact on Global Geopolitical Activities

The United States and the European Union claim that on February 24, 2022, Russia launched a cyberattack on a commercial satellite communications network called KA-SAT belonging to [4]. Viasat revealed that the cyberattack hit its KA-SAT network, rendering thousands of modems in Europe inaccessible. The cyberattack was intended to disrupt command and control operations in Ukraine and had significant spillover effects on other European countries, including Germany, Greece, Poland, Italy, and Hungary. It was not until a month later that European satellite broadband services recovered from the incident. Company experts noted that the malicious code issued destructive commands to overwrite critical data in the modem's flash memory, rendering the modem unable to access the network, but not permanently unusable. Security vendor SentinelLabs researchers attributed the malicious code that launched the cyberattack on KA-SAT's commercial satellite communications network to a new type of wiper malware called "AcidRain". AcidRain is designed to remotely wipe vulnerable modems and routers, and SentinelLabs has observed similarities between AcidRain and VPNFilter, a malware operation attributed to the Russian-backed "FancyBear" aka APT28 group. As the European and American alliances assert their unity in defending Ukraine, Russian intelligence agencies have stepped up cyber infiltration and espionage activities targeting allied governments outside Ukraine.

On the other hand, Russia used Konni infrastructure to launch attacks against high-value targets in Europe, including Poland, the Czech Republic, and other countries. The Securonix Threat Research (STR) team has been investigating a new Konni-based malware campaign called STIFF#BIZON [5]organizations with other national backgrounds. However, the STR team pointed out that there is a direct correlation between the IP addresses, hosting providers, and host names of this attack and historical data and APT28. Based on relevant threat intelligence, it is inferred that the STIFF#BIZON campaign may be APT28 imitating the tactics of the APT37 organization to launch attacks against European countries. Specific tactics include executing the second-stage malicious code through PowerShell after successful spear phishing, similar UAC bypassing techniques, stealing cookies with credential access, and similar install.bat installation methods. However, more advanced tactics were used in the STIFF#BIZON campaign, such as offline cracking of cookies to bypass MFA and using anti-debugging techniques leaked in WikiLeaks Vault 7 to escalate privileges and execute malicious code through the system file wusa.exe.

Whether it is self- developed advanced attack technology or learning and using the actual application of techniques and tactics of organizations with backgrounds in other countries, Russia has launched cyber attack

activities targeting target areas including Ukraine as the center and the Baltic Sea region, Europe and the United States as the radius, making the global phishing activities with the theme of the Russian-Ukrainian conflict more sensitive. For example, the Iranian APT organization Lyceum in the Middle East and the Indian Rattler organization in Asia used pictures of Russian attack activities in Ukraine to launch phishing attacks via email. The emergence of a new wiper malware Agrius in the supply chain attack activities against Israel means that advanced techniques and tactics such as "erasing malicious code" and "supply chain" are no longer unique to APT organizations with national backgrounds in Russia. This shows that **Russia's application of advanced attack technology in cyber warfare has had an impact on global geopolitical activities, prompting more intense geopolitical activities in countries and regions around the world, including Russia and Ukraine. As a result, the "Russian-Ukrainian conflict" has caused both sides to suffer varying degrees of losses in cyberspace.**

1.4 The Ease of Tampering with Digital Evidence Has Prompted Foreign Apt Organizations to Use Cyber Attacks to Frame Others

Digital evidence is widely present in computer system hardware and software, peripheral devices and related networks. Different from traditional physical evidence, digital evidence is easy to tamper with. Traditional physical evidence such as written materials will leave traces when they are destroyed or tampered with, which can usually be discovered through forensic identification of document examination through handwriting characteristics, ink type, printing format, etc. Digital evidence includes electronic documents, audio and video, which can be read, written and modified arbitrarily in terms of file content and metadata. Unless there is third-party encryption, overprinting and other storage methods for surveillance protection, it is often very difficult to re-examine the traces from electronic storage media that have been tampered with, deleted and destroyed.

In February 2022, Antiy released a report revealing the hidden signs of an APT organization with an Indian background [6], finding that the organization mainly targeted social activists, social groups, and opposition parties in India, and also stole important intelligence on military and political targets in neighboring countries such as China and Pakistan. When reviewing the Koregaon frame-up case, Antiy found that the Dark Elephant organization had been launching spear-phishing email attacks repeatedly against social movement individuals in India who were in a difficult situation and lacked awareness and means of network security prevention. After successfully implanting the NetWire remote control Trojan into the opponent's system , the attackers used the remote control Trojan to send carefully crafted documents and letters with contents that seriously violated

Indian laws, such as "purchasing arms" and "plotting to assassinate the Prime Minister", to the hidden file directories of the target's laptop and external mobile storage device many times. After that, **the attackers reported the results to the local police and went to the target's residence for a surprise inspection, and seized these illegal letters for the purpose of framing on the spot as digital evidence of guilt.**

In the process of digital evidence collection, in order to provide sufficient and reliable evidence to the judicial authorities, the on-site seizure of computers, mobile phones, tablets and other storage media devices related to the crime, the subsequent sealing and transfer, and the fixation, analysis and authentication of digital evidence in the devices all require rigorous process means and supervision. In the case involving Dark Image , after the network-level operation was achieved, the criminal's frame-up began from the stage of on-site seizure. From the subsequent secondary evidence collection process to provide evidence for overturning the case, the detailed information of the process, file and network in the computer system recorded by the antivirus software and the retention of the relationship between the three played a key role, especially the combination of the UsnJrnl record of the file system and the historical process information proved that the appearance of the illegal letter in the victim's computer came from the network transmission of the remote control Trojan.

1.5 APT Attacks Using IoT Devices Are Frequent

The Internet of Things is a network composed of intelligent devices with sensor systems that do not require human intervention. In today's human society, IoT exists in every corner of social applications, such as wearable devices, Internet of Vehicles, smart homes, smart cities, Industry 4.0, etc. IoT devices use a wide variety of network protocol technologies to make it possible for cyberspace to interact with information from the physical world. However, IoT itself has the following insecurity factors: First, most IoT devices themselves are not embedded with security mechanisms, and most of them are not within the traditional IT network, which means they are outside the security perception capability and cannot respond effectively once they encounter problems; second, most IoT devices are online 24 hours a day, which is a more "stable" attack source than desktop operating system hosts; third, IoT devices such as routers and cameras are used as agents to stably transmit traffic in the attack, distribution, theft and control stages. Due to the large network traffic itself, attack traffic can also be mixed into it to achieve the effect of hiding; fourth, in specific scenarios, most intranet devices can access routers, which can be used as a springboard to the intranet. At the same time, routers and cameras at the network boundary are sometimes exposed to the Internet,

and attackers can also access them directly from the Internet. The above characteristics make it a common practice for APT organizations to use IoT devices to build C2 infrastructure to gain relative attack advantages.

At the beginning of 2022, Antiy discovered that the OceanLotus organization, in its cyberattack activities against China [7], had previously used weak password blasting, vulnerability attacks and other means to compromise public network routers, cameras and other IoT devices in many important provinces and cities in China as springboards, install traffic forwarding tools, and forward the secret theft and control traffic of the Torii remote control Trojan through one or more layers of springboards to the real Torii remote control server. Through retrospective investigation, Antiy found that the earliest active time of the Torii remote control family can be traced back to 2017. It has rich functions and wide adaptability. It is designed to be a remote control weapon for various types of IoT system devices. It supports the generation of Trojan payloads of many types of CPU architectures such as ARM, x86, x64, MIPS, SPARC, PowerPC, SuperH , Motorola 68000, etc., and can conduct deep information theft and control of servers, IoT devices, office hosts, etc. running on the above architectures, and has more than 10 groups of command control capabilities.

In May 2022, Mandiant discovered that the attackers used a new backdoor based on the open source Dropbear SSH software while investigating the APT29 organization's eavesdropping activities to collect emails from victims' internal networks [8]have no endpoint-side detection and defense measures. It uses the Dropbear SSH function to enable SOCKS proxy forwarding traffic to establish a springboard. The attackers applied this method to old version conference room IP cameras in the target network. Since these devices are directly exposed to the Internet and are in a detection blind spot, the attackers mixed malicious behavior into normal traffic and remained undetected in the victim's network for a long time.

2 Ransomware Attacks

Looking back at the ransomware attacks that occurred in 2022, some ransomware was used by attack organizations with national backgrounds as a "politicized" criminal tool to carry out cyber attacks. During the Russian-Ukrainian conflict, "politicized" ransomware attacks occurred frequently and were accompanied by the reappearance of "destructive" ransomware, disguised as ransomware attacks, but the actual goal was to disrupt system operation, thereby transforming cyberspace attacks into physical space impacts. With the continuous innovation of network security technology and the construction of a solid border protection barrier by security equipment, threat

actors are unable to achieve intrusion using common executor propagation methods, and employ victim target internal personnel to carry out cyber attacks as a new means. There has also been a new shift in ransomware strategies, from the traditional ransomware attack of "stealing + encryption" to "stealing + deleting or destroying" attacks. Cross-platform ransomware executors help threat actors infiltrate increasingly complex network environments, and also bring new challenges to security workers in executor analysis.

2.1 Politicized Ransomware Attacks

Ransomware is usually used as a criminal tool by attacking organizations for economic purposes. Looking back at the ransomware attacks that occurred in 2022, it was found that **some ransomware was used as a "politicized" criminal tool by attacking organizations with national backgrounds to carry out cyber attacks.**

"Politicalized" ransomware attacks can be roughly divided into two categories. One is actually sabotage activities disguised as ransomware attacks. Antiy paid attention to "Not Petya" sabotage activities against Ukraine in 2017 [9]. The Iranian Ministry of Intelligence and Security (MOIS), under the leadership of the Iranian Minister of Intelligence, launched a series of destructive attacks on the Albanian government system from July 2022, including multiple ransomware attacks. Among them, the Iranian APT organization Muddy Water used public vulnerabilities to invade the victim's system and deploy ransomware [10]. In October 2022, the Ukrainian Computer Emergency Response Team (CERT-UA) issued a warning about the Cuba ransomware attack against the country. The attackers sent phishing emails disguised as content from the Ukrainian Armed Forces to trick victims into viewing and downloading the ransomware attack payload [11]. The other type is ransomware attacks by attack organizations with a "politicized" background to help the country gain benefits. For example, the Microsoft Threat Intelligence Center (MSTIC) discovered that North Korean attackers developed the H0lyGh0st ransomware, and that the ransomware had a certain relationship with the APT organization Lazarus affiliated with North Korea. Microsoft analysts speculated that its motive might be to help the North Korean government relieve economic pressure [12]. The APT38 organization affiliated with North Korea used ransomware such as Beaf, PXJ, ZZZZ and ChiChi to carry out attacks [13].

The Russian-Ukrainian conflict , several ransomware groups declared their political positions. On February 25, Conti released a statement on its dark web data leak platform, saying, "If any organization decides to launch a cyber attack or any war activity against Russia, we will mobilize all possible resources to counterattack the enemy's critical infrastructure." Conti was the first ransomware group to express its political position during the Russian-Ukrainian

conflict, but this move was met with dissatisfaction among internal staff. A member who was allegedly Ukrainian made public the group's internal chat records and ransomware builders online. The Stormous ransomware group expressed support for Russia and released a statement on March 1 saying that it had attacked the Ukrainian Ministry of Foreign Affairs[14]. Some ransomware groups did not publicly express their political positions, but actually launched targeted ransomware attacks, including Freeud, Prestige, NB65, and Hermetic Ransom (GoRansom).

While threat actors are often vocal about their intentions and claim responsibility for attacks, mapping real-world identities is difficult, and distinguishing between threat actors with political or financial motives for crime is increasingly challenging.

2.2 "Destructive" Ransomware Executor

"Destructive" ransomware is different from common ransomware. It does not use encryption algorithms to encrypt files, but instead uses data overwriting or data erasure to destroy files on the victim's system.

The Russian-Ukrainian conflict, several "destructive" ransomware appeared. On January 13, Microsoft discovered a ransomware attack called MBR Locker targeting Ukraine. The attack was divided into two stages: ransom and data wiping. The executor dropped during the ransom stage was actually a feint. Hidden behind the ransom was the WhisperGate data wiper executor. The ransom credit released during the ransom stage was to confuse the victim. Its real purpose was to cover up the malicious behavior of the WhisperGate data wiper after it invaded the victim's system [15]. The ransomware executor of Hermetic Ransom (GoRansom) was discovered in a Ukrainian network facility on February 23. Its function was similar to that of the MBR Locker attack. After dropping the ransomware executor, the HermeticWiper data wiper executor was executed[16]. The Onyx ransomware that appeared in the public eye in April is different from previous ransomware. Its encryption strategy is to judge the size of the encrypted file. It encrypts files smaller than 2M with the normal encryption algorithm and overwrites files larger than 2M with junk data. Even if the victim pays the ransom, all files larger than [17].

We predicted the reappearance of "destructive" ransomware in 2021. Attacks aimed at destruction can also be disguised as targeted ransomware attacks. Since ransomware encryption of data and files can lead to system or business failure, there have been incidents disguised as ransomware attacks, but the actual goal is to disrupt system operations, thereby transforming cyberspace attacks into physical space impacts.

2.3 Shift in Ransomware Tactics

Common methods of spreading ransomware executables include phishing, RDP brute force cracking, and vulnerability exploitation. With the continuous innovation of network security technology and the solid boundary protection barriers built by security equipment, threat actors cannot achieve intrusion by using common executor propagation methods. However, it is found that when enterprises implement network security construction plans, internal security is usually ignored. Combined with the economic factors caused by the epidemic, accompanied by spending cuts and layoffs, hiring **internal personnel of the victim target to carry out network attacks has become a new means**. The Lapsus $ ransomware organization does not rely on common executor propagation methods, but looks for internal personnel who are willing to sell access rights within their organization. This may also be the reason why many large companies were attacked by the Lapsus $ organization in 2022, including Nvidia, Samsung, Ubisoft, Microsoft , and Uber [18].

The use of "double extortion" has become a mainstream trend in ransomware operations, that is, the method of "stealing data + encrypting files". Many ransomware use Exmatter (also known as Fendr) data penetration tools as a weapon to steal files from victim systems, including well-known ransomware such as Black Matter and Black Cat. Since there may be loopholes in the development of ransomware, researchers can develop corresponding decryption tools to help victim units, which will result in ransomware developers and affiliated members being unable to obtain ransom money. In order to solve this problem, the developers of Exmatter data penetration tools overwrite the original files in the system after obtaining valuable files and successfully exporting them from the victim's system, that is, they no longer use encryption algorithms to encrypt files, but instead damage the original files in the system after successful theft, which means that victims can only obtain their own files by contacting attackers and paying ransom.

This new data corruption capability could represent a shift **from the traditional "steal+encrypt" ransomware attack to a "steal+delete or destroy" attack**. Under this approach, affiliates can keep all revenue generated by the attack because they do not need to share a percentage of the revenue with the encryptor developer. [19]As international sanctions on ransomware payments and law enforcement agencies improve their ability to track Bitcoin flows, ransomware groups are gradually moving away from using Bitcoin as a ransom payment option and turning to other forms.

2.4 The Growing Number of Cross-Platform Ransomware Executors

Big Game Hunting (BGH) [20]Cyber Big Game Hunting is a cyber attack program that usually refers to ransomware attacks against large, high-value and well-known corporate entities. This program has enabled ransomware threat actors to infiltrate increasingly complex network environments. In order to cause as much damage as possible, threat actors try to encrypt as many systems as possible, which means that their ransomware executors can run on different architectures and operating systems. One way to achieve this plan is to write ransomware in a "cross-platform programming language" such as Rust or Golang. There are other reasons for using cross-platform languages. Some ransomware may currently only target one platform, but writing it in a cross-platform language can make it easier to port the executor to other platforms. Another reason is that cross-platform executors are more difficult to analyze. In 2022, several well-known cross-platform ransomware executors have been discovered, such as the Linux version of AvosLocker and LockBit ransomware executors targeting VMware ESXi servers, TellYouThePass ransomware made a comeback using the Golang language to develop a new version of the executor, and Hive ransomware used the Rust language to develop an executor for Linux system VMware ESXi servers.

3 Mining Trojans

3.1 More and More Mining Trojans Have Mastered the Ability to Quickly Integrate Vulnerabilities

As mining Trojans continue to improve their anti-mining technology, more and more mining Trojans have mastered the ability to quickly integrate vulnerabilities. Mining Trojans not only fight against security products, but also block competition from peers. Whoever can quickly integrate vulnerabilities first can get priority access to the public network computing power with vulnerabilities, and thus obtain corresponding profits. Whenever a vulnerability with a wide impact appears, it is difficult for the affected devices in the entire network to repair the vulnerability in a short period of time, which gives mining Trojans an opportunity to take advantage. For example, after the Log4j2 vulnerability broke out, mining groups such as H2Miner [21]quickly integrated the vulnerability and launched attacks. Since the detailed information of the Confluence OGNL (CVE-2022-26134) vulnerability was released, the "8220" [22]mining organization and the Hezb [23]mining Trojan began to use the vulnerability to spread widely. For enterprises, it is necessary to improve the ability to quickly repair vulnerabilities, prevent mining Trojans

from using vulnerabilities to control host permissions, and develop solutions to prevent the risk of mining Trojans spreading to enterprises after the vulnerability is exposed.

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

Mining Trojans usually use two methods to mine, one is to mine directly in the mining pool, and the other is to mine through the mining pool agent. Mining Trojans directly connected to the mining pool usually let the victim's host directly connect to the mining pool address to upload the computing power results. The mining pool platform will send the reward to the wallet of the mining Trojan gang according to the contributed computing power. The disadvantage of this method is that security analysts can obtain the wallet address of the mining Trojan gang by analyzing the attack script, etc., and can also find the direct public mining pool address. In this way, by entering the corresponding mining Trojan gang's wallet address through the public mining pool website, you can find out how many victims are passively mining, the current total hash of the contributed computing power, and how many Monero coins are produced, etc. The mining pool agent can easily solve the above disadvantages, that is, add a transfer link between the miner and the mining pool. The mining pool agent obtains the task from the public mining pool and transfers it to the miner for calculation. The miner transfers the calculation result to the mining pool agent and then forwards it to the public mining pool. In recent years, more and more mining Trojans have begun to use mining pool proxies to mine, such as Kthmimu [24], "8220" [22], Sysrv-hello, Outlaw [25], etc. The popularity of mining pool proxies can conceal the real public mining pools for mining, bypassing traditional intelligence mining pool blacklist detection, making traditional blacklist detection ineffective.

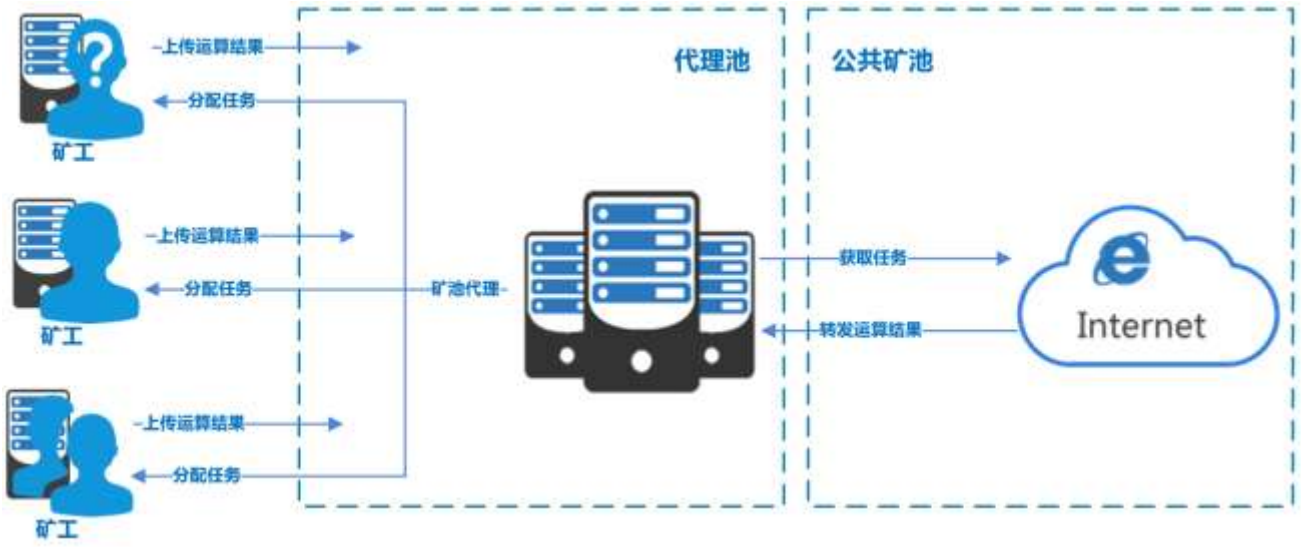

Figure 3-1 Mining pool proxy diagram

3.3 Due to the Stable Profits, More Threat Groups Are Engaging in Malicious Mining

In 2022, the entire virtual currency market suffered a huge impact, and the prices of almost all currencies fell. Take Bitcoin as an example. In January, the price of each Bitcoin was close to US$48,000, but by November, the price of each Bitcoin was only US$17,000, a drop of more than US$30,000. Despite this, malicious mining has not decreased, but has become more active. The most commonly used currency for malicious mining is Monero. Compared with other currencies, Monero is more stable, which is also favored by other ransomware organizations. For example, the AstraLocker [26]ransomware shut down its ransomware attack activities and turned its business to malicious mining activities. This shift is likely that the ransomware organization wants to earn virtual currency in a more low-key and covert way. After governments around the world strengthened their defense and law enforcement against ransomware, the profits of ransomware organizations have been greatly reduced. Unlike malicious mining, ransomware will affect the normal operation of the system after invading it. The way to earn ransom mainly depends on communicating with the victim. In serious cases, it may be suppressed by governments around the world. Malicious mining can earn virtual currency without the victim's knowledge, which is relatively low risk for ransomware organizations. Although there is no money to be made by extorting victims to pay ransom, malicious mining can earn virtual currency at almost zero cost, without worrying about the price of electricity or computing power, and can also earn generous rewards. Therefore, Antiy CERT believes that more threat organizations will engage in this low-risk, high-return malicious mining activity in the future.

4 Botnet

According to statistics from the Internet threat report released monthly by CNCERT [27], the active botnet families in 2022 include Mirai, Mozi, rapperbot, hybridmq, gafgyt and moobot. These active botnet families all have DDoS functions and have a large number of infections in China. Once an attack is launched, the damage and impact are huge. Antiy found that **the global political situation in 2022 is constantly changing, and using botnets to launch politically motivated DDoS attacks has become the main means of confrontation between major powers; after statistics on the vulnerability exploits disclosed in 2022, it was found that botnets are actively using newly emerging vulnerabilities to spread; botnets using P2P propagation methods are widely spread among IoT devices.**

4.1 DDoS Attacks Launched by Botnets Have Become a Powerful Weapon in the Fight Between Countries

A botnet is a group of computers centrally controlled by hackers. Its core feature is that hackers can manipulate hosts infected with Trojans or bots through a one-to-many command and control channel to perform the same malicious behavior, such as launching a DDoS attack on a target website at the same time, sending a large amount of spam, or conducting "mining". With the turbulence of the global political situation, **more and more state-backed APT attack organizations or individual organizations use botnets to launch politically motivated cyber attacks due to international relations.**

At the beginning of 2022, along with the Russia-Ukraine conflict, a cyber war without gunpowder broke out between the United States, Europe, Russia, and Ukraine . According to Ukrainian media reports, from January 14 to February 24 before the official outbreak of the (Russia-Ukraine conflict), more than 70 government websites of Ukraine, including the Ministry of Foreign Affairs, Ministry of Education, Ministry of Internal Affairs, and Ministry of Energy, were first shut down by DDoS network attacks from Russia. Subsequently, many information resources (websites and apps) such as the Ministry of Defense, Security Bureau, Armed Forces, and financial institutions were paralyzed and services were interrupted. Data on hundreds of machines was wiped. [28]According to the Russian Satellite News Agency, the "Anonymous" hacker group launched a large-scale DDoS attack, making multiple Russian government websites, including the Kremlin, Ministry of Defense, and Ministry of Foreign Affairs, completely inaccessible 错误!未找到引用源。

The China National Cyberspace Administration (CNCERT) released a monitoring report on March 11, 2022 [30], stating that since late February, China's Internet has continued to suffer from overseas cyber attacks. Foreign organizations have controlled computers in China through attacks and then launched cyber attacks on Russia, Ukraine, and Belarus. After analysis, these attack addresses mainly came from the United States, with more than 10 attack addresses from New York State alone. The peak attack traffic reached 36Gbps, and 87% of the attack targets were Russia. A small number of attack addresses also came from countries such as Germany and the Netherlands.

In 2022, the global political situation continues to change, and using botnets to launch politically motivated DDoS attacks has become the main means of confrontation between major powers. [31]

4.2 Botnet Exploits New Vulnerability to Spread

In 2022, Antiy Monitoring found that botnet operators expanded the size of their botnets by increasing the number of vulnerabilities and actively exploiting 1-day vulnerabilities. The following bar chart shows the types of IoT vulnerabilities that were captured in the wild between [27]:

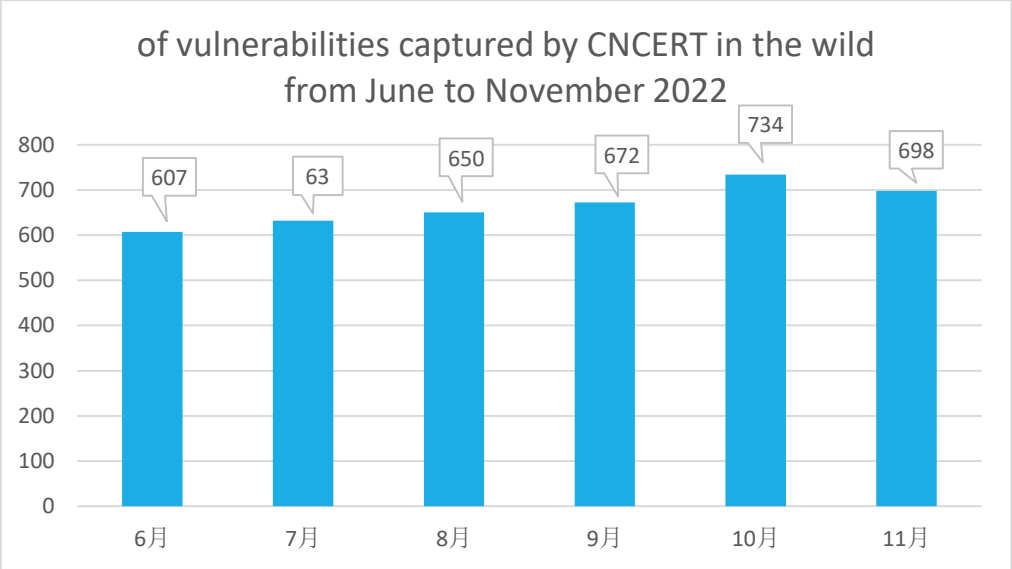

Figure 41wild vulnerability types captured by CNCERT/CC from June to November 2022

Take the CVE-2022-29591 vulnerability as an example, the vulnerability was first disclosed on May 10, 2022. Antiy captured the traffic exploiting the vulnerability on May 17. It can be seen that the operators of the Miori botnet are highly sensitive to new vulnerabilities and have certain vulnerability exploitation capabilities.

In November 2022, Antiy honeypot captured a DDoS-type botnet family named zero written in Go. Four different versions of this botnet appeared in a short period of time. Analysts found that it continued to update and add

vulnerabilities in version iterations. In 2022 alone, there were as many as 12 remote executor vulnerability exploits of various types.

By analyzing the vulnerability exploits disclosed in 2022, it was found that botnets are actively exploiting newly emerging vulnerabilities to spread.

4.3 Using P2P Propagation Are Widely Spread Among IoT Devices

With the rapid development of the information age and the concept of "Internet of Everything", IoT devices are increasing day by day, but most IoT devices include serious security issues, such as weak passwords, open access to management systems, default management credentials, or weak security configurations. IoT devices have become attractive targets for attackers. Attackers take advantage of the numerous vulnerabilities of IoT to control devices, which allows attackers to easily access them and cause disruptions to online services. And because the infection of IoT devices is usually not noticed by users, attackers can easily assemble hundreds of thousands of such devices into a powerful botnet, enabling large-scale attacks.

P2P propagation is one of the traditional propagation methods of some botnets. It has the characteristics of fast propagation speed, large infection scale, and difficulty in tracing the source. For example, botnet families such as Mirai and Mozi have been extremely active after using this propagation method. In 2022, the scale of botnet control between connected smart devices continued to increase [32]. Some large botnets control the controlled terminals by combining P2P propagation with centralized control. Infected devices can continue to maintain contact through P2P communication and infect other devices. As more IoT devices continue to be put into use, malicious programs that use P2P propagation may pose a greater threat to cyberspace.

5 Attack and Defense

At present, the network security confrontation mode has evolved into a comprehensive and systematic confrontation. The institutionalized attack organizations, supported by large-scale engineering systems, rely on standardized cyberspace equipment to complete the kill chain. Under the ongoing COVID-19 pandemic, government and enterprise departments have accelerated cloud and digital businesses. In particular, new infrastructure represented by new infrastructure and information innovation has introduced more attack surfaces and supply chain threats. The offensive and defensive confrontation has long been in an asymmetric situation of "easy to attack and difficult to defend".

5.1 Attack Surface Management (ASM) Becomes the First Window into Attack and Defense

Gartner first proposed the concept of attack surface management (ASM) in 2018, and then published attack surface management as the first in the cybersecurity risk management trend in February 2022. In recent years, security incidents caused by poor attack surface management have occurred frequently (such as the Log4j2 remote code execution vulnerability (CVE-2021-44228) exploited in the wild, and improper configuration of a city's health code AccessKey led to data leakage, etc.). In recent years, the concept of attack surface management has begun to be widely mentioned repeatedly in the field of attack and defense confrontation.

Affected by the repeated impact of the COVID-19 pandemic, government and enterprise departments have accelerated their digital transformation and cloud business work. The rapid implementation of 5G and IOT business has made the originally fragile attack surface management work more complicated. Relevant data show [33][34][35]that most companies believe that they should improve their attack surface monitoring capabilities, but when vulnerabilities appear, companies often need an average of more than 80 hours to update their attack surface range, while attackers can weaponize vulnerabilities in just 48 hours. Therefore, with the deepening of offensive and defensive combat exercises and the intensification of cyber confrontation between major countries, attack surface management has become the first window of offensive and defensive confrontation. Attackers can easily use the vulnerable attack surface to break through the original "monitoring-analysis-warning-disposal" security system, affecting the overall network security of enterprises.

5.2 Supply Chain Becomes One of the Biggest Breakthroughs in Attack and Defense

Supply chain security incidents occurred frequently in 2022. Security incidents such as the large-scale supply chain attack on the NPM repository and the Spring4Shell vulnerability attack proved that supply chain security cannot be ignored. According to statistics from the National Information Security Vulnerability Database (CNNVD), the total number of vulnerabilities in the first half of 2022 increased by 12% month-on-month, and ultra-high-risk vulnerabilities accounted for more than 50%. As the international community strengthens the management of vulnerability releases, the exploitation of vulnerabilities in the wild has a tendency to further increase.

In our observations, the proportion of popular vulnerabilities in attack and defense confrontations related to vulnerabilities in supply chain products such as office systems, project management systems, and email systems has exceeded 50%. In a large-scale attack and defense drill, the number of supply chain product vulnerabilities such as office systems, network equipment, and network security equipment that were exploited in the wild was as high as

20. The widespread use of attack chain vulnerability attacks has become one of the most common means in attack and defense confrontations. Since it is difficult for government and enterprise users to understand the network security level of suppliers, in attack and defense confrontations, the kill chain created by supply chain product vulnerabilities is often used to accurately attack and invade the target and control the target system facilities to achieve combat objectives. Attackers can also use common open source component vulnerabilities to carry out range attacks on combat targets, further increasing the difficulty of detection and response, and expanding the kill chain into a kill network to break through more combat targets. It can be seen that supply chain product vulnerabilities have become one of the biggest breakthroughs in attack and defense confrontations.

5.3 Abuse of Payload Hiding Is One of the Major Challenges in Attack and Defense Confrontation

In the past, APT organizations often used a variety of payload hiding techniques to evade detection and achieve long-term concealment. With the deepening of actual combat attack and defense drills, in order to achieve the effect of the drills, payload hiding technology has also been widely discussed and studied. From the initial anti-killing confrontation and tunnel hiding to more advanced payload hiding methods such as non-physical file landing and signature anti-killing. In a large-scale attack and defense drill alone, we observed more than 7 payload hiding methods, which greatly tested the response capabilities of the security team.

- Use CDN domain pre-positioning and cloud function forwarding to disguise traffic, hide C2 addresses, and counter threat intelligence;
- Use code hosting platforms to host attack payloads, interfere with sandboxes, and confuse victims and analysts;
- Use signatures to create samples to avoid detection and resist multi-engine comparison results;
- Use memory horse technology to control and fight against terminal anti-virus software;
- Use fragmented transmission to send data packets to counter traffic detection features;
- Use secondary development of commercial weapons tools to counter traffic detection features;
- Use protocols such as DNS and ICMP to send payloads to resist traffic protocol detection.

These technologies are not only widely used in the field of attack and defense, but also widely discussed on social platforms, forums, and blogs, which greatly reduces the original threshold for use. We also found that some weaponized tools developed by attackers now support a variety of payload hiding methods and high-speed iteration, which brings great challenges to analysis, monitoring, and disposal. It can be seen that the abuse of payload hiding has become one of the major challenges in attack and defense.

5.4 AI Empowerment Will Bring More Challenges to Offensive and Defensive Confrontations

ChatGPT [36]is an artificial intelligence chatbot program developed by OpenAI. It was launched in November 2022 and has attracted widespread attention from all over the world. Security researchers soon discovered that ChatGPT can be trained to analyze code defects, write vulnerability detection rules, generate malicious code, generate vulnerability POCs, and even generate phishing emails.

The addition of AI has further reduced the cost of attack for attackers. On the one hand, AI can be used to generate hacker weapons to fight against security products, and can even be combined with public opinion warfare, network warfare, and information warfare to achieve greater combat objectives. It can also automate and scale combat tasks to increase the difficulty of attack and defense confrontation. On the other hand, AI can be used to drive network defense, improve business code quality, optimize network security equipment detection capabilities, automatically block cyber threats, significantly shorten threat discovery and response time, and effectively improve defense capabilities. It is undeniable that with the increase in AI computing power, the increasing accuracy of training models, and the continuous reduction of usage barriers, AI empowerment will bring more challenges to attack and defense confrontation.

5.5 The Offensive and Defensive Battle Against New Infrastructure Will Become the Main Battlefield of the Offensive and Defensive Confrontation

The current international order is facing profound adjustments, and the global technology competition landscape is accelerating its reconstruction. As the infrastructure of digital infrastructure, the new infrastructure has further expanded the attack surface and increased the difficulty of network security construction and management; on the other hand, the new infrastructure, especially the information and innovation products, due to the extensive use of open source products, will inevitably attract the attention of attackers, especially ultra-high- capability cyber threat actors, and will be targeted as a key attack. Therefore, with the accelerated implementation of new infrastructure,

especially information and innovation products, the future attack and defense of new infrastructure scenarios will become an important position for attack and defense confrontation.

5.6 Regular Security Operations Will Effectively Enhance the Offensive and Defensive Capabilities of Government and Enterprise Organizations

With the deepening development of digital construction of government and enterprise organizations, the extensive application of new technologies, and the continuous enrichment of online scenarios, network security faces new risks and challenges. At present, some government and enterprise users have deployed a large number of security devices, but the massive alarms generated by this have brought great pressure to daily security operation and maintenance, affecting the efficiency and effectiveness of security operations, and it is difficult to reflect the value of security construction.

Through regular security operations, we can continuously explore and analyze the key characteristics of cyber threat actors, and through the combination of security products and security services, we can discover, prevent and deal with threats, and assist customers in establishing an effective security protection system. Regular security operations are divided into the following four levels, which can fully consider the characteristics of business organizations and IT environments, as well as actual security needs, effectively reduce security operation and maintenance pressure, keep abreast of security trends at all times, continuously fight against threats, help government and enterprise organizations avoid security risks, and effectively improve offensive and defensive capabilities.

- Construction of security operation system: Improve the security operation management system and emergency plan system, strengthen the security operation coordination mechanism of key links, and ensure that the network security work of government and enterprise institutions can be carried out in an orderly manner under the leadership of the security operation organization.
- Pre-security assessment: Look at the asset security operation of government and enterprise institutions from a full life cycle perspective, sort out the asset attack surface, and discover security risks. Assist customers to make a good starting point for security operations and control risks before the system goes online.
- Incident emergency response: assist customers to locate the source of the incident, promptly block the lateral spread of the incident, analyze the cause and process of the incident, restore on-site losses, and strengthen related vulnerabilities to prevent the incident from happening again.

- Normal security operations: Based on the five levels of assets and systems, applications and execution bodies, networks and topology, identities and accounts, and data and business, we assist customers in building the basic operation layer, provide suggestions for realizing the system, topology, business, and data flow, assist government and enterprise organizations in realizing data classification and grading, and continuously carry out data security governance. Based on the operational results of security products, we continuously explore new attack surfaces, vulnerabilities, and threat events. We jointly conduct threat analysis to determine whether it is necessary to trigger a major incident response and disposal process.

6 Data Breach

In 2022, the COVID-19 pandemic is still raging around the world. All walks of life around the world have accelerated their digital transformation. While the value of data has been further highlighted, data leaks continue to occur frequently. Data leakage incidents have continued to become news hotspots, involving various information ranging from medical information, account credentials, personal information, corporate emails, and sensitive internal corporate data. The fields involved include industrial manufacturing, government affairs, medical care, finance, transportation, and so on. The situation we face is still very serious.

6.1 Leakage Incidents Continue to Occur Frequently in 2022

In 2022, data leakage incidents continued to occur frequently, and the number of data leakage incidents continued to increase. The amount of personal information and file data leakage was huge, which had a serious impact on individuals and corporate organizations.

In 2022, the most influential data leakage incidents mainly occurred in the Internet and various types of enterprises. File data leakage incidents mainly involved energy, medical care, manufacturing, government agencies, etc., and personal information data leakage incidents mainly involved the Internet, telecom operators, medical care, transportation and other fields. Among them, the data leakage suffered by Rosneft Deutschland GmbH, a branch of Russian Oil Company in Germany, and Travis CI, an open source software construction project on the Linux platform, were the most serious, resulting in the leakage of 20TB file data and 770 million user log records, respectively. **The higher the degree of informatization in an industry, the more data leakage incidents there are, and the greater the harm caused by the leakage. The main causes of data leakage incidents in 2022 are hacker theft, ransomware attacks, and improper configuration of databases or cloud storage of enterprises and institutions.**

The continuous and high-frequency data leakage incidents have seriously threatened the privacy and security of hundreds of millions of people around the world.

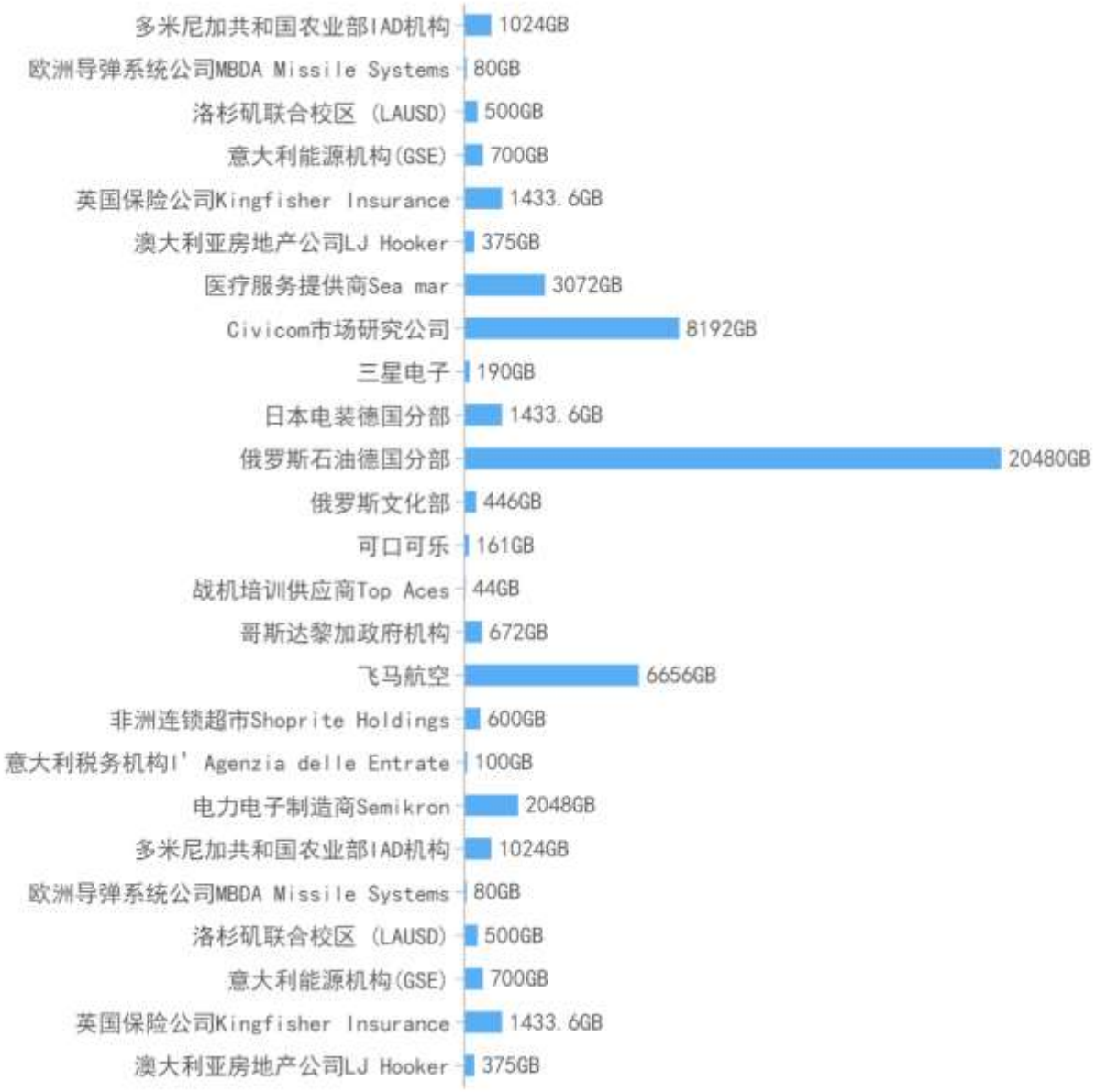

Figure 6-1 2

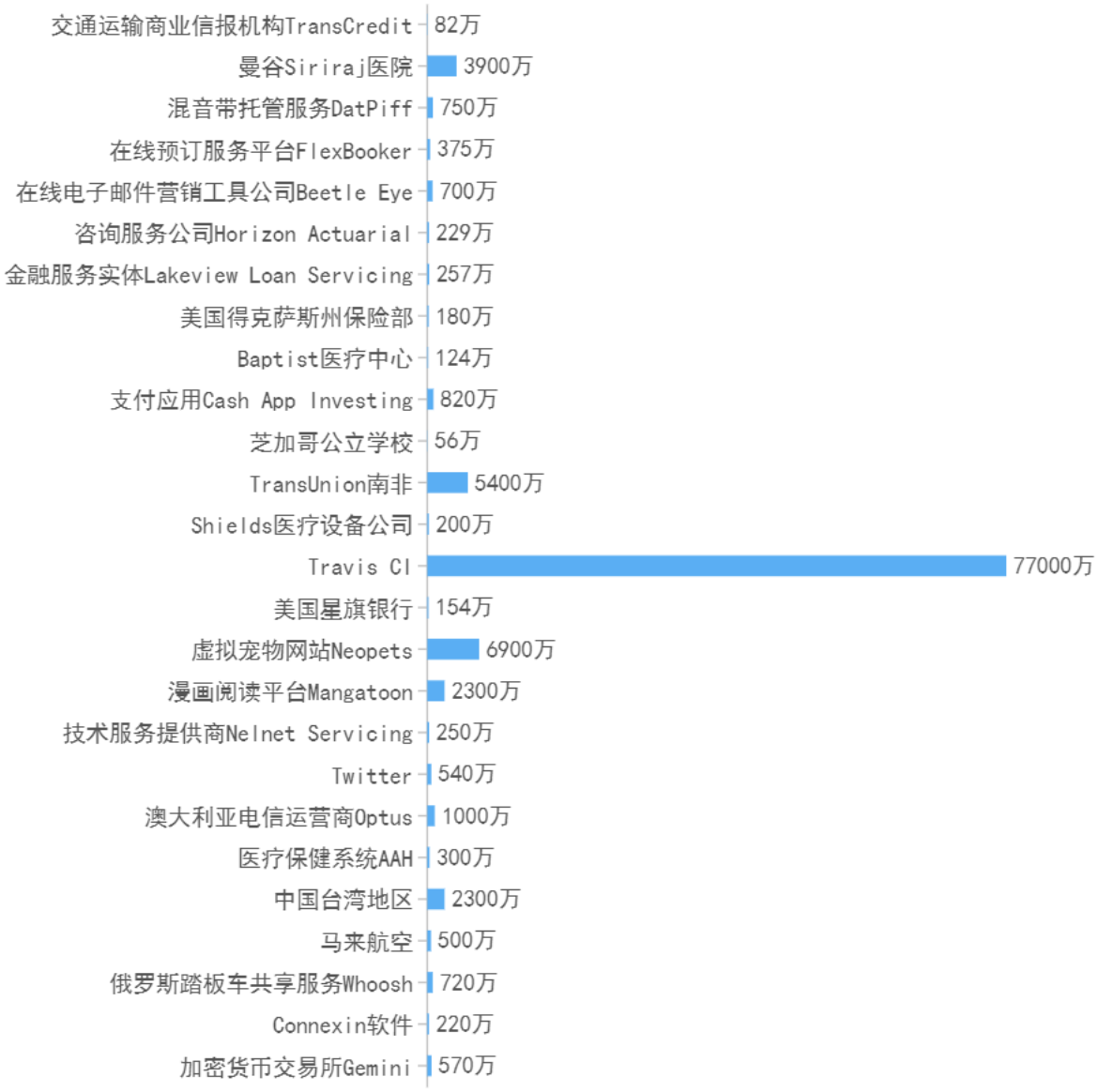

Figure 6-3 4

6.2 Hacker Forums Are Used as Platforms for Cybercrime Activities

In the digital age, data leakage is the biggest driving force behind the scale and industrialization of cybercrime, and hacker forums have become a platform for cybercriminals to resell data for profit. On July 21, a user posted on the BreachForums hacker forum to sell data of 5.4 million accounts claiming to belong to Twitter. The poster claimed that he exploited a vulnerability in December 2021 to collect the data. Although Twitter fixed the vulnerability in January 2022, it still exposed the private phone numbers and email addresses of millions of users; on November 11, a user of the BreachForums hacker forum released a database containing detailed information of approximately 7.2 million customers of the Russian scooter sharing service Whoosh. The seller also claimed that the

stolen data included 3 million promotional codes that people could use to rent Whoosh scooters for free; on November 16, a user of the BreachForums hacker forum posted a post to sell information data of more than 487 million users of the communication software WhatsApp. The data allegedly involved 84 countries and regions, of which about 32 million were from the United States, 45 million from Egypt, 35 million from Italy, and 20 million from France.

6.3 DiDi Was Fined for Data Leakage, Sounding the Alarm for User Information Data Security

On June 30, 2021, DiDi was officially listed on the New York Stock Exchange. On July 4, 2022, the Cyberspace Administration of China issued a message saying: "According to reports, after testing and verification, the 'DiDi' APP has serious problems in illegally collecting personal information. The Cyberspace Administration of China notified the app store to remove the 'DiDi' APP in accordance with the relevant provisions of the "Cybersecurity Law of the People's Republic of China."

On July 21, 2022, according to a document issued by the Cyberspace Administration of China [37], "The Cyberspace Administration of China has filed a case to investigate DiDi Global Co., Ltd.'s suspected illegal activities in accordance with the law." "After investigation, it was found that DiDi Global Co., Ltd.'s illegal and irregular activities in violation of the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law were clear in facts, with solid evidence, serious circumstances, and bad nature. On July 21, the Cyberspace Administration of China imposed a fine of RMB 8.026 billion on DiDi Global Co., Ltd. and a fine of RMB 1 million each on Cheng Wei, Chairman and CEO of DiDi Global Co., Ltd., and Jean Liu, President, in accordance with the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Administrative Penalty Law and other laws and regulations." At the press conference, the Cyberspace Administration of China stated that after investigation, DiDi Company had committed 16 illegal acts, which can be summarized into eight main aspects.

Digital transformation of industries around the world has become a major trend, but the continuous accumulation of sensitive data has also brought security issues such as data leakage, tampering, and abuse. With the promulgation and implementation of laws and regulations such as the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and the Measures for the Security Assessment of Data Export, China's data supervision legal system has been increasingly improved. **This data leakage incident is also a wake-up call for all domestic Internet companies. National information security is no small matter, and everyone is responsible for protecting information security.**

6.4 Cut off the "Black Hands" Of Stealing Secrets and Build a Firewall to Protect Personal Information

In the Internet age, citizens' personal information has become a commercial resource with extremely high "gold content" and a key target coveted by thieves. According to a report by Security Insider on November 21 [38], police officers from the Cyber Security Brigade of the Nangang Branch of the Harbin Public Security Bureau discovered during their work that a user on a hacker forum posted a post in October 2022 to sell citizens' personal information data, claiming that he held about 20GB of data and sold it for 0.2 bitcoins. The user also published 29 data samples, which also included citizens' names, contact numbers, home addresses and other personal information. After 96 hours of hard work by the special task force, on October 22, police officers from the Nangang Public Security Bureau arrested Ma, a criminal suspect suspected of illegally obtaining computer information system data, in Pingfang District, Harbin, and seized more than 100,000 pieces of illegally obtained citizens' personal information from his computer. After interrogation, the suspect Ma was an IT industry practitioner. He took advantage of a system loophole in a medical institution's WeChat public account and illegally obtained more than 100,000 pieces of computer system data through technical means between April and October 2022. He then posted the data on a hacker forum abroad for sale. Before he was arrested, he had made an illegal profit of $1,500. **The leakage of personal information will cause a series of chain threats. Sensitive information is directly related to the personal and property safety of citizens. If illegally obtained, it is very easy to cause related crimes, such as financial fraud, credit fraud, extortion, etc. The leaked data will also form an accurate user portrait.**

As the era of big data has developed, the leakage of personal information has become a hidden danger to social development. Protecting personal privacy is imperative, and protecting citizens' personal information from infringement has also become an inevitable requirement under the conditions of the rapid development of network information technology. Not only should citizens themselves improve their security awareness, but Internet platforms should also consciously assume the responsibility of protecting users' sensitive information. Key industries should also take corresponding preventive measures as soon as possible, strengthen technical management strategies and preventive measures, so as to minimize the risks brought by data leakage.

7 Industrial Internet

According to the Guiding Opinions of the State Council on Deepening the Development of Industrial Internet through "Internet + Advanced Manufacturing" [39], the Industrial Internet, as a product of the deep integration of new-generation information technology and manufacturing, is increasingly becoming a key support for the new industrial revolution and an important cornerstone for deepening "Internet + advanced manufacturing", and will have an all-round, profound and revolutionary impact on future industrial development. The Industrial Internet builds a new network infrastructure that fully connects people, machines and things by systematically constructing the three functional systems of network, platform and security, forming new business forms and application models for intelligent development, and is an important foundation for promoting the construction of a strong manufacturing country and a strong network country, and a strong support for building a moderately prosperous society in all respects and building a socialist modern power.

In recent years, China has actively deployed the industrial Internet. Driven by a series of policies and market demands, such as the "Industrial Internet Development Action Plan (2018-2020)" (MIIT Information Management Letter [2018] No. 188) [40]Management [2020] No. 8) [41], and the "Industrial Internet Innovation and Development Action Plan (2021-2023)" (MIIT Information Management [2020] No. 197) [42], China's industrial Internet has flourished, many applications have been gradually implemented, and the market scale has continued to expand; at the same time, the cybersecurity threats faced by the industrial Internet also deserve our high attention.

7.1 Geopolitical and Military Conflicts Affect the Industrial Internet

In 2022, geopolitical tensions intensified, regional military conflicts, territorial disputes and bloody conflicts broke out, and their negative impacts affected the industrial Internet to a certain extent.

On February 24, 2022, the Russian-Ukrainian conflict broke out. From the eve of the official outbreak of the conflict to the present, APT28, APT29, Turla, Sandworm, Dragonfly, Gamaredon, UNC1151, the Ukrainian Military Intelligence Agency (GURMO), IT Army of Ukraine, Anonymous, GhostSec, AgainstTheWest and other cyberspace threat actors have been involved, and their negative impact has been extended from the "fifth territory" (cyberspace) to the real physical world, affecting the industrial network security of relevant countries.

1) the Russian-Ukrainian conflict, the Ukrainian Computer Emergency Response Team (CERT-UA) and the Slovak cybersecurity company ESET issued an announcement stating that the Sandworm organization under the Russian Federation General Staff Intelligence Directorate (GRU) launched an attack on Ukraine's high-voltage substations. The attackers used a new malware variant Industroyer2; in addition, the attack organization also used several other destructive malware, including CaddyWiper, ORCSHRED, SOLOSHRED and AWFULSHRED.

2) On July 20, during the Russian-Ukrainian conflict, an explosion occurred at the Gysinoozerskaya Hydropower Station in Russia, causing the emergency shutdown of the power system and power outages in large areas of Siberia. The GhostSec organization claimed responsibility for the attack and said that its cyberattack was a response to the Russian side in the Russian-Ukrainian conflict; the organization's "leader" Sebastian Dante Alexander (Sebastian Dante Alexander) said through public channels such as " The Tech Outlook " that the attack was carefully designed by the organization. They wrote a tool called " KillBus " to attack Modbus devices. The tool rewrites data by extracting information and uses it as a slave device, which then destroys the industrial control system of the hydroelectric power plant and its servers. GhostSec 's malicious intervention in the power plant system led to the final explosion.

Since late March 2022, the Conflict between Arabian countries and Israel has intensified again, and its negative impact has also affected the industrial Internet.

1) In early June, Microsoft said it had blocked a Lebanese hacker group called Polonium from using the OneDrive cloud storage platform to attack Israeli organizations. Microsoft also suspended more than 20 malicious OneDrive applications used in the Polonium attack and updated tools to isolate attackers through security intelligence. According to analysis, in the attacks that have mainly targeted Israel's key manufacturing, IT, and defense industry sectors since February 2022, the Polonium hacker group may also coordinate their attacks with multiple attackers linked to Iran.

2) In early September, the GhostSec group claimed that they had hacked into 55 Berghof PLCs (programmable logic controllers) used by Israeli organizations. GhostSec shared a video on its Telegram channel that showed a successful login to the PLC's management panel, as well as an image of the HMI screen showing its current status and PLC process control. At the same time, GhostSec also released more screenshots, claiming to have gained access to another control panel that can be used to change the chlorine and pH

levels in the water. Researchers said that because the PLC is accessible over the Internet and has weak passwords, it can be compromised.

7.2 The Number of Disclosures of Vulnerabilities in Industrial Internet Infrastructure Exceeds 100

In 2022, the number of disclosures of vulnerability risks of industrial Internet infrastructure worldwide exceeded 100, and the serious negative impact that such vulnerability risks may cause cannot be ignored.

In November 2022, the China Industrial Internet Research Institute released the Global Industrial Internet Innovation and Development Report [43], which stated that countries around the world currently attach importance to and continue to upgrade the industrial Internet security defense system, but the threat of attacks on the industrial Internet continues to intensify, and the global industrial Internet security development still faces huge challenges, including increasingly frequent network attacks on industrial control equipment and the general lack of security design in industrial control systems. For example, in March 2022, two zero-day vulnerabilities were exposed in the PLC and engineering workstation software of Rockwell Automation in the United States. Attackers can use these vulnerabilities to inject malicious code into industrial control systems and secretly modify automation processes.

In addition to this incident, what is the vulnerability risk situation of the industrial Internet infrastructure in 2022? As a capability -based security company selected as the "2023 Industrial Information Security Monitoring Emergency Support Unit" by the National Industrial Information Security Development Research Center [44], Antiy has always paid great attention to the security protection and operation in the field of industrial information security, strengthening the implementation of capability-based security products, and strengthening the implementation of security value for the Internet of Things and industrial scenarios; for some of the disclosures of vulnerability risks of the industrial Internet infrastructure this year [45], a brief summary is shown in the following table:

Table 1 Disclosure of vulnerability risks in industrial internet infrastructure in 2022 (partial)

Number	Time	Industrial Internet Infrastructure Objects Involved	Information Related to the Vulnerability Risk of the Object
1	March 2022	Siemens RUGGEDCOM ROX and ROS devices	Siemens has published 15 new advisories, informing customers of more than 100 vulnerabilities affecting its products, including more than 90 security vulnerabilities caused by the use of third-party components. The three advisories describing third-party component vulnerabilities are related to RUGGEDCOM ROX and ROS devices. The affected components include NSS and ISC DHCP.

			Exploitation of the vulnerability can lead to code execution, denial of service (DoS), or disclosure of sensitive information. Although Siemens has released patches for many of these vulnerabilities, for some of them, the German industrial giant has only provided mitigation measures.
2	April 2022	ABB Symphony Plus SPIET800 and PNI800 network interface modules	ABB, a Swiss industrial technology company, has developed patches for three serious vulnerabilities found by researchers in some network interface modules of its products. Due to defects in the way these products handle certain data packets, attackers with local access to the control network or remote access to the system server can exploit these vulnerabilities to launch a denial of service attack, which users can only solve by manually restarting. ABB said that exploiting these vulnerabilities could cause disruptions in industrial environments. In addition to directly affecting SPIET800 and PNI800 devices, systems connected to these devices will also be affected.
3	April 2022	Elcomplus SmartPTT SCADA	Automation company Elcomplus 'SmartPTT SCADA was disclosed to have nine vulnerabilities. The product combines the functionality of a SCADA/ IIoT system with dispatch software for professional radio systems. The list of security vulnerabilities includes path traversal, cross-site scripting (XSS), arbitrary file upload, authorization bypass, cross-site request forgery (CSRF), and information disclosure vulnerabilities. Exploiting these vulnerabilities, an attacker can upload files, read or write arbitrary files on the system, obtain credentials stored in plain text, perform various actions on behalf of the user, execute arbitrary code, and increase privileges to access management functions.
4	June 2022	Korenix JetPort Industrial Serial Device Servers	Korenix JetPort industrial serial device server was revealed to have a backdoor account. Korenix The JetPort Industrial Serial Device Server has a backdoor account that can be exploited by an attacker on the network to access the device's operating system and gain full control. The attacker can reconfigure the device and potentially gain access to other systems connected to the server.
5	June 2022	Carrier LenelS2 Mercury Access Control Panel	Eight zero-day vulnerabilities have been discovered in Carrier's LenelS2 Mercury access control panel. The vulnerabilities affect the LenelS2 Mercury access control panel, which is used to grant physical access to facilities and integrate with more complex building automation deployments. Some of these issues require mitigation, while most can be resolved in firmware updates.
6	June 2022	Siemens SINEMA Remote Connection Server Schneider Electric IGSS SCADA Product Data Server Module, C-Bus Home Automation Products	Siemens and Schneider Electric released the June 2022 patch bulletin, announcing that a total of more than 80 vulnerabilities affecting their products have been fixed. Thirty of these vulnerabilities affect the SINEMA remote connection server. These security vulnerabilities, many of which affect third-party components, can lead to remote code execution, authentication bypass, privilege escalation, command injection, and information leakage; Schneider Electric issued recommendations to address seven serious vulnerabilities that could be used for remote code execution in the data server module of the IGSS SCADA product, and two critical authentication-related vulnerabilities in the C-Bus home automation product.

7	June 2022	Multiple OT equipment manufacturers (Siemens, Motorola, Honeywell, Yokogawa, ProConOS , Emerson, Bentley Nevada, Omron, and JTEKT)	Multiple OT device manufacturers disclosed to be affected by 56 'ICEFALL' vulnerabilities. Security researchers have discovered 56 new vulnerabilities, collectively dubbed 'ICEFALL', that affect several of the largest OT device manufacturers serving critical infrastructure organizations. The vulnerabilities are grouped into four main categories: insecure engineering protocols, weak cryptography or broken authentication schemes, insecure firmware updates, and remote code execution via local functionality.
8	June 2022	AutomationDirect PLC and HMI Products	AutomationDirect has announced that it has fixed several vulnerabilities in its PLC and HMI products. AutomationDirect has patched several serious vulnerabilities in some of its programmable logic controller (PLC) and human-machine interface (HMI) products. These vulnerabilities can allow attackers to cause damage and make unauthorized changes to the targeted devices. These security holes have been fixed in firmware version 6.73. Two other advisories from CISA describe vulnerabilities in DirectLOGIC PLCs, one for serial communications and one for Ethernet communications.
9	August 2022	NetModule Router Software (NRSW)	Two critical vulnerabilities in NetModule router software could be exploited by remote attackers to bypass authentication and access management features.
10	August 2022	OPC UA Protocol	Researchers disclose details of OPC UA protocol vulnerabilities. Software development and security solutions provider JFrog has disclosed details of several vulnerabilities affecting the OPC UA protocol, including a vulnerability that its employees exploited in an earlier hacking contest. OPC UA (Open Platform Communications Federation Architecture) is a machine-to-machine communication protocol that many industrial solution providers use to ensure interoperability between various types of industrial control systems (ICS).
11	September 2022	Dataprobe iBoot - PDU Power Distribution Unit	The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued an Industrial Control Systems (ICS) alert, noting seven security vulnerabilities in Dataprobe 's iBoot -PDU power distribution unit product, which is mainly used in industrial environments and data centers. Successful exploitation of these vulnerabilities could lead to the destruction of Dataprobe's iBoot-PDU power distribution unit product. Unauthenticated remote code execution on iBoot -PDU devices. iBoot -PDU is a power distribution unit (PDU) that provides users with real-time monitoring capabilities and sophisticated alert mechanisms through a web interface to control the power supply to devices and other equipment in OT environments.

12	November 2022	ABB Oil and Gas Flow Computers	A security vulnerability exists in oil and gas flow computers manufactured by Swiss industrial technology company ABB that could allow attackers to cause disruptions and prevent utility companies from billing their customers. The entire vulnerability exploit chain allows an unauthenticated attacker to execute arbitrary code with root privileges, which could give the attacker full control of the device and disrupt its ability to measure oil and gas flow, thereby preventing the victim company from billing its customers.

As can be seen from the table above, the vulnerability issues of industrial Internet infrastructure this year involve risks in protocols, software, hardware, etc. Although some of these vulnerability issues have been fixed by relevant companies, there are still a large number of vulnerability risks that may continue to increase and are in a dangerous situation that can be exploited by attackers. All relevant parties are urgently required to pay enough attention and take effective risk reduction measures. **At the same time, the vulnerability risks exposed by relevant foreign organizations also provide important warnings and references for similar manufacturing companies and industrial Internet security-related companies in China.**

7.3 Industrial Internet Infrastructure Faces New Attack Scenarios

In August 2022, Team 82, a research team at industrial cybersecurity company Claroty, revealed a new attack scenario, "Evil PLC Attack" [46][47]DefCon presentation: After the attacker invades the programmable logic controller (PLC), instead of using it as the endpoint or final target of the attack, the attacker uses it as a springboard to weaponize the invaded PLC and infect any engineering workstation and other PLCs that communicate with the PLC.

The researchers designed three attack scenarios for the Evil PLC attack: Weaponizing PLCs to Achieve Initial Access, Attacking Traveling Integrators, and Weaponizing PLCs as a Honeypot. In the first attack scenario, the PLC is the only vehicle to enter the secure facility. After the attacker invades and weaponizes the PLC, he can wait for the engineer to connect to the PLC and infect the engineer's workstation/operation terminal, or deliberately cause the PLC to fail. The engineer responsible for PLC operation and maintenance troubleshooting will be lured to the PLC and use his engineering workstation to connect to the PLC to troubleshoot the fault, and then the engineer's workstation/operation terminal will be infected.

In the second attack scenario, attackers can use the current situation of third-party system integrators or contractor engineers who usually interact with many different organizational networks and PLCs as a ferry carrier to continuously invade different organizations and sites around the world. An engineer workstation/operation terminal

infected by a hacked PLC may spread malicious code to multiple other companies. Attackers can further invade new PLCs and engineering workstations in more other organizations, thereby continuously expanding the impact of Evil PLC.

Faced with the risks of new attack scenarios faced by the above-mentioned industrial Internet infrastructure, all relevant parties should promptly adapt their defense ideas and formulate effective targeted defense plans as soon as possible.

7.4 New Market for Stolen Data from the Industrial Internet Emerges

Dark web market called "Industrial Spy" emerged. The cyber threat actor behind it set up a website on the surface network to promote and guide visits to its dark web address , and declared on the website: "There, you can buy or download competitors' private and confidential data for free. We make public plans, drawings, technologies, political and military secrets, accounting reports and customer databases. All of this is collected from the world's largest companies, conglomerates and every activity. We exploit vulnerabilities in their IT infrastructure to collect data." And judging from the Industrial Spy malicious code samples captured by cybersecurity defenders, the cyber threat actor behind it launched its own ransomware in May 2022 [48], trying to create a criminal "one-stop service" from encryption to sales.

All relevant parties in the Industrial Internet should pay necessary attention to the emergence and development of the dark web market, which is relevant to the security of the Industrial Internet and involves the trading of stolen data, and strengthen corresponding defense measures.

8 Threat Generalization

In 2013, Antiy used the term "malware/other" to indicate the evolution of security threats to new areas such as smart devices and the Internet of Things. Since then, "generalization" has been an important threat trend studied by Antiy. Threat generalization leads to an increase in the exposure of users' assets. Attackers can use the increased attack surface to generate a wide range of security threats such as unauthorized access, springboard attacks, intrusion into "isolated networks", asset control, asset destruction, and data leakage.

The report of the 20th CPC National Congress pointed out that "we should accelerate the development of the Internet of Things, build an efficient and smooth circulation system, and reduce logistics costs. We should accelerate

the development of the digital economy, promote the deep integration of the digital economy and the real economy, and build a digital industry cluster with international competitiveness." The development of science and technology such as the Internet of Things is of great significance to building a cyber power and realizing a socialist modern power. In 2022, the number of IoT devices worldwide is expected to reach 35 billion, and IoT technology will be widely used in manufacturing, agriculture, transportation, energy, logistics, infrastructure, medical care and other fields.

However, the openness, multi-source heterogeneity, diversity and complexity of terminal devices and applications of the Internet of Things have made the security issues of the Internet of Things increasingly prominent. In the process of interaction, the entire life cycle of the Internet of Things may be attacked, including physical attacks, authentication attacks, protocol attacks, communication attacks, etc. The intelligent functions of smart cars provide many conveniences, but security issues in the vehicle system and wireless keys can allow attackers to gain control. For example, in October 2022, Europol smashed a hacker gang that specialized in invading the keyless unlocking system of cars, arrested 31 suspects and confiscated more than US$1 million (about RMB 7.75 million) in criminal assets. For example, in the field of smart homes, smart cameras are the hardest hit areas in smart homes. Smart doorbells and smart cameras have become channels for attackers to eavesdrop and peek, and people's home privacy is threatened. AI technology is being actively applied to all walks of life. However, research reports warn that this emerging technology can easily be exploited by cyber criminals and illegal hackers. For example, attackers will target leaders, use AI to simulate speech synthesis, bypass identity authentication through face recognition vulnerabilities, etc., in order to deceive GPS to mislead ships, mislead self-driving vehicles, modify AI-driven missile targets, etc. The vulnerabilities of complex and diverse IoT devices also give cyber attackers more options. In December 2022, Antiy revealed in the article "Analysis of Torii Remote Control Cyber Attack Activities of Ocean Lotus Organization" [7]that the Ocean Lotus Organization launched an attack on IoT devices of important government and enterprise units in China.

The deep integration of cloud computing technology and the Internet of Things has made security scenarios more complex and decentralized. Enterprises and the cloud will inevitably have to manage a wider attack surface. The risk of security intrusion is increasing. Cloud hosts and IoT devices have become the preferred targets of botnets and mining Trojans. Most IoT devices include serious security issues such as weak passwords, open access to management systems, default management credentials, or weak security configurations. Botnet attacks seize the opportunity of IoT vulnerabilities to control devices and cause online service interruptions, achieving a large amount

of DDoS attack traffic. Among them, Mirai is the number one killer of botnets. Mining Trojans have been rampant in the past two years, and the rise of cloud services has become a new battlefield for mining gangs. Currently, active mining hacker groups include Outlaw, TeamTNT, etc., which are active organizations that mine cloud hosts. For enterprises, an effective security strategy is to make predictions and preparations as much as possible in advance: where are the valuable cloud assets? Which cloud application defects may affect business operations? On this basis, security personnel need to solve necessary cloud security issues as soon as possible.

In addition, attacks on critical infrastructure are becoming increasingly serious. On the one hand, cyber warfare has become an important part of modern warfare. In the "Russia-Ukraine conflict", the attack and defense of critical infrastructure by both sides has become the key to cyber warfare. Large-scale attacks have directly led to the paralysis of transportation, medical care, communications, electricity and infrastructure. On the other hand, cybercrime organizations have also launched a series of complex cyber attacks on critical infrastructure, among which attacks on medical institutions are particularly prominent. Many organizations ignore the security of equipment, and critical infrastructure equipment often involves hardware and firmware security issues, resulting in the inability to update IoT devices in a timely manner. Many devices still have known vulnerabilities, leaving security risks. Financial, power, medical and other facilities face many challenges. One by one, technical loopholes and product backdoors are deeply buried "time bombs" that may be actively or passively detonated at any time, bringing a catastrophic blow to the interests of the country and the people.

At present, the generalization of security threats has become the norm. Antiy still uses the same method as in previous years to publish "Generalization and Distribution of Cybersecurity Threats" in the annual report, using a new chart to illustrate the situation of generalization of threats in 2022.

2022网络安全威胁泛化与分布

征求意见稿

本图引自《安天实验室2022网络安全年报》

Appendix 1 : References

[1] Tsinghua University Institute for International Governance of Artificial Intelligence. [AIIG Observation No. 107] Former Chairman of the U.S. National Intelligence Council: Urgent need to redefine Internet governance and protect the Internet's non-political status and openness

https://www.d-arts.cn/article/article_info/key/MTIwMzU3OTAwNDOD33mrsIa0cw.html

[2] ESET.HermeticWiper: New data-wiping malware hits Ukraine

https://www.eset.com/sg/about/newsroom/press-releases1/products/hermeticwiper-new-data-wiping-malware-hits-ukraine/

[3] Microsoft.Defending Ukraine: Early Lessons from the Cyber War

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[4] Juan Andres Guerrero- Saade and Max van Amerongen.AcidRain | A Modem Wiper Rains Down on Europe

https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/#:~:text=AcidRain%20is%20the%207th%20wiper%20malware%20associated%20with,in%20the%20February%2024th%20attack%20against%20their%20modems.

[5] Securonix Threat Labs, Threat Research: D. Iuzvyk , T. Peck, O. Kolesnikov. Securonix Threat Labs Initial Coverage Advisory: STIFF#BIZON Detection Using Securonix – New Attack Campaign Observed Possibly Linked to Konni/APT37 (North Korea)

https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/

[6] Antiy. "Dark Elephant" Organization: A Decade of Hidden Cyber Attacks

https://www.antiy.com/response/20220617.html

[7] Antiy. Remote Control Network Attack Activities Organized by OceanLotus

https://www.antiy.cn/research/notice&report/research_report/20221202.html

[8] Mandiant.UNC3524: Eye Spy on Your Email

https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

[9] Antiy's Analysis and Response to the "PETYA" Virus That Attacks Ukraine and Other Countries

https://www.antiy.com/response/petya/petya.pdf

[10] US DEPARTMENT OF THE TREASURY.Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities

https://home.treasury.gov/news/press-releases/jy0941

[11] CERT- UA.Kaiberata na Derezhavnī Oregano України з використанням skhidlivo Programma RomCom . Mozhliva причетність Cuba Ransomware aka Tropical Scorpius aka UNC2596 (CERT-UA#5509)

https://cert.gov.ua/article/2394117

[12] Microsoft Threat Intelligence Center (MSTIC),Microsoft Digital Security Unit (DSU). North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware

https://www.microsoft.com/en-us/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

[13] Sergiu Gatlan.New ransomware strains linked to North Korean govt hackers

https://www.bleepingcomputer.com/news/security/new-ransomware-strains-linked-to-north-korean-govt-hackers/

[14] Trend Micro Research.Cyberattacks are Prominent in the Russia-Ukraine Conflict

https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

[15] Microsoft Threat Intelligence Center (MSTIC),Microsoft Digital Security Unit (DSU),Microsoft Defender Threat Intelligence,Microsoft Detection and Response Team (DART).Destructive malware targeting Ukrainian organizations

https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[16] kaspersky daily. Ransomware as a distraction

https://www.kaspersky.com/blog/hermeticransom-hermeticwiper-attacks-2022/43825/

[17] Lawrence Abrams.Beware : Onyx ransomware destroys files instead of encrypting them

https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/

[18] Lawrence Abrams.Microsoft confirms they were hacked by Lapsus $extortion group

https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/

[19] Sergiu Gatlan.Ransomware data theft tool may show a shift in extortion tactics

https://www.bleepingcomputer.com/news/security/ransomware-data-theft-tool-may-show-a-shift-in-extortion-tactics/

[20] CrowdStrike.CYBER BIG GAME HUNTING

https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/#:~:text=Cyber%20big%20game%20hunting%20is,organizations%20or%20high%2Dprofile%20entities.

[21] Antiy. Dual-Platform Communication - Analysis of Active H2Miner Mining Organization

https://www.antiy.cn/research/notice&report/research_report/20211117.html

[22] Antiy. Analysis of the "8220" Mining Organization Activities

https://www.antiy.cn/research/notice&report/research_report/20220428.html

[23] Antiy. Analysis of the Active Hezb Mining Trojan

https://www.antiy.cn/research/notice&report/research_report/20220705.html

[24] Antiy. Analysis of the Active Kthmimu Mining Trojan

https://www.antiy.cn/research/notice&report/research_report/20220527.html

[25] Antiy. Analysis of Typical Mining Families Series 1 | Outlaw Mining Botnet

https://www.antiy.cn/research/notice&report/research_report/20221103.html

[26] Sergiu Gatlan.AstraLocker ransomware shuts down and releases decryptors

https://www.bleepingcomputer.com/news/security/astralocker-ransomware-shuts-down-and-releases-decryptors/

[27] National Internet Emergency Response Center. CNCERT / CC Internet Security Threat Report

https://www.cert.org.cn/publish/main/45/index.html

[28] BBC.Ukraine cyber-attack: Russia to blame for hack, says Kyiv

https://www.bbc.com/news/world-europe-59992531

[29] China News Network. Russian Media: "Anonymous" Hacker Group Announced the Launch of a "Cyber War" Against Russia

https://www.chinanews.com.cn/gj/2022/02-25/9685853.shtml

[30] National Internet Emergency Response Center. China's Internet Suffers Cyber Attacks from Abroad

https://www.cert.org.cn/publish/main/8/2022/20220311172614196863695/20220311172614196863695_.html

[31] Hebei Network Security (Official account of Information Security Evaluation Center of Hebei Provincial Cyberspace Administration). IoT Botnets Have Become the Soil That Fuels DDoS Attacks.

https://baijiahao.baidu.com/s?id=1741489828389779000&wfr=spider&for=pc

[32] CNCERT National Engineering Research Center. IoT Security Threat Intelligence

https://mp.weixin.qq.com/s/t7gMWthB6W3vF_SA7gk_QA

[33] Randori.The State of Attack Surface Management 2022

https://www.randori.com/reports/the-state-of-attack-surface-management-2022/

[34] ISC 2022, Zero Zero Security CEO Wang Yu. External Attack Surface Management (EASM) Technology Development and Practice

http://vd3.bdstatic.com/mda-nerbmg8n8fsead78/360p/h264/1653553480461981126/mda-nerbmg8n8fsead78.mp4

[35] China Information Security Evaluation Center. "Observation on Cybersecurity Vulnerability Situation in the First Half of 2022"

http://www.itsec.gov.cn/zxxw/202209/t20220902_112723.html

[36] Security Insider. Application Prospects of ChatGPT in Information Security Field

https://www.secrss.com/articles/49912

[37] China Cyberspace Administration of China: Decision of the Cyberspace Administration of China to impose administrative penalties on DiDi Global Co., Ltd. in accordance with the law for cybersecurity review

https://mp.weixin.qq.com/s/JvME41TaNixTLQXC2mYMqg

[38] Security Insider. A loophole in the public account system of a medical institution was exploited, and the attacker stole more than 100,000 citizen data and sold them overseas and was arrested

https://www.secrss.com/articles/49228

[39] State Council. Guiding Opinions of the State Council on Deepening the Development of Industrial Internet through "Internet + Advanced Manufacturing"

http://www.gov.cn/zhengce/content/2017-11/27/content_5242582.htm

[40] Ministry of Industry and Information Technology. Notice on Issuing the "Industrial Internet Development Action Plan (2018-2020)" and the "Industrial Internet Special Working Group 2018 Work Plan"

https://www.miit.gov.cn/zwgk/zcwj/wjfb/zh/art/2020/art_3feeff24ae854421b06134a9efd73753.html

[41] Notice of the General Office of the Ministry of Industry and Information Technology on Promoting the Accelerated Development of the Industrial Internet

https://www.miit.gov.cn/jgsj/xgj/wjfb/art/2020/art_56f2702b081743bfa6be118b6d2e336e.html

[42] Ministry of Industry and Information Technology. Notice on Issuing the Action Plan for the Innovation and Development of Industrial Internet (2021-2023)

https://www.miit.gov.cn/jgsj/xgj/gzdt/art/2021/art_ecb6ec1ddbf748eebe05ac69c086339d.html

[43] China Industrial Internet Research Institute. Global Industrial Internet Innovation and Development Report

https://www.china-aii.com/achievements?id=754ae9ca-9f42-46f4-9f1d-2a7bc7b28936&ty=2

[44] Antiy. Antiy was selected as the 2023 Industrial Information Security Monitoring Emergency Support Unit

https://mp.weixin.qq.com/s/exhZeF8oNsyDkcKyGvYqaQ

[45] Antiy. Threat Analysis and Research - Threat Information - Daily Security Information

https://www.antiy.cn/research/respond/safe_info/index.html#

[46] Team82, Claroty Research Team.EVIL PLC ATTACK: WEAPONIZING PLCS https://claroty-statamic-assets.nyc3.digitaloceanspaces.com/resource-downloads/team82-evil-plc-attack-research-paper.pdf

[47] CNCERT National Engineering Research Center. PLC becomes an attack springboard - evil PLC attack: weaponizing PLC https://mp.weixin.qq.com/s?__biz=MzUzNDYxOTA1NA==&mid=2247530557&idx=2&sn=1b7fead602769b072c6318fb7e0e600b&scene=21#wechat_redirect

[48] Atinderpal Singh.Technical Analysis of Industrial Spy Ransomware https://www.zscaler.com/blogs/security-research/technical-analysis-industrial-spy-ransomware

