Case Analysis of High-Frequency Incidents in City-side Network Security

Antiy Cybersecurity Guard Team

2025/4/15

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

1 Overview

During major events in Heilongjiang Province, Antiy served as the overall technical support unit for the city's cybersecurity guarantee, supporting the provincial and municipal authorities. It deployed hundreds of sets of traffic and honeypot probes, as well as tens of thousands of sets of terminal and server security protection systems, and provided various services including vertical response, online threat analysis, and secure DNS.

Modern cities are digital cities, with a large number of government and enterprise institutions as well as individual citizens and families' devices connected to the metropolitan area network. The protection targets are complex and diverse, with a vast number of exposed assets and potential attack points. Undercurrents of attack activities are rampant. During the activity period alone, the Antiy Cybersecurity Guard Team detected a total of 50.76 million instances of various types of foreign cyber attacks on the city side. The main high-frequency events include network scanning and probing, brute-force cracking of login credentials, vulnerability exploitation attacks, remote control Trojan implantation, mining Trojan infections, and botnet control, etc. If these attack activities are not promptly discovered, blocked, and dealt with, they may have a significant impact on the operation of the city. This report analyzes one case each of the six types of high-frequency cyber attack events in the relevant work, with the aim of providing reference and guidance for security protection and operation work.

2 Typical Cases of Network Attack on City Side Security

2.1 Network scanning case

Network scanning refers to the behavior of an attacker to collect key information (such as open ports, running services and operating system versions) by actively probing the target network or system, in order to find the asset exposed surface of the scanned target. Search for available attack entry points to prepare for subsequent attacks, which are in the "reconnaissance" link of network attack activities.

At 2: 00 on February 13, 2025, Antiy monitored and blocked a port scanning attack with the attack source IP address located in the United States. For the threat intelligence inquiry of the attack IP, the Antiy Threat Intelligence Center shows that the geographical location of the attack IP is the United States, with a number of historical threat activity tags. Through tracing analysis, it is found that the network segment of CENSYS-ARIN-01 is owned by US-based censys, Inc., which is a network security company registered in the US and specializing in attack surface management and threat search solutions.

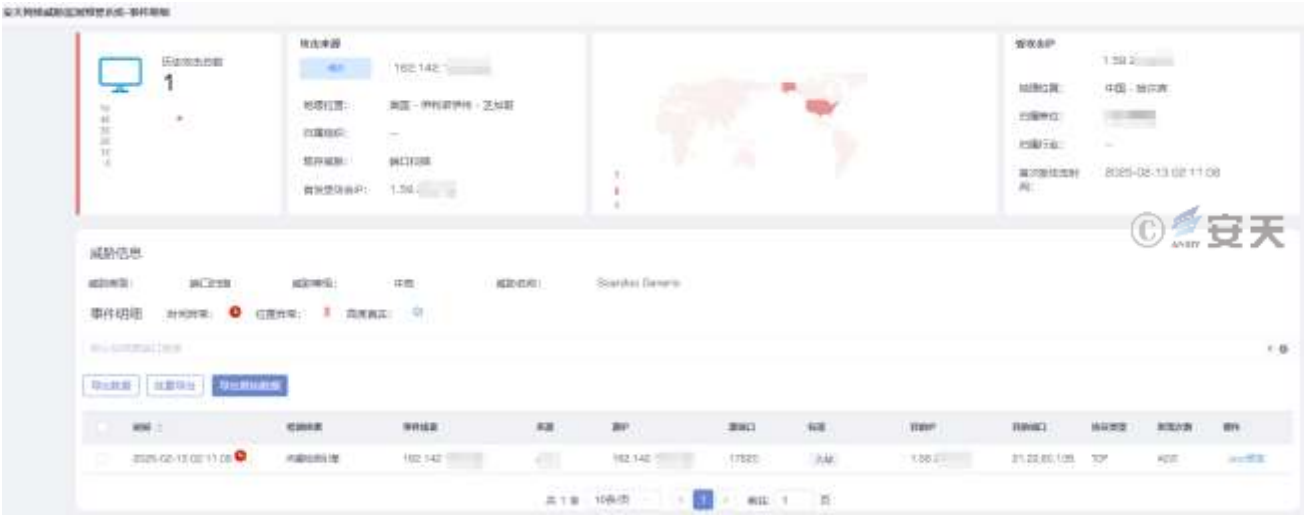

Figure 2-1 The Alarm Information of Antiy Network Threat Monitoring and Early Warning System1

According to the Threat Intelligence Center, the attack IP belongs to the United States, relying on historical behavior activities marked "malicious," "scanning," "demolition," "DDoS" and other activity tags.

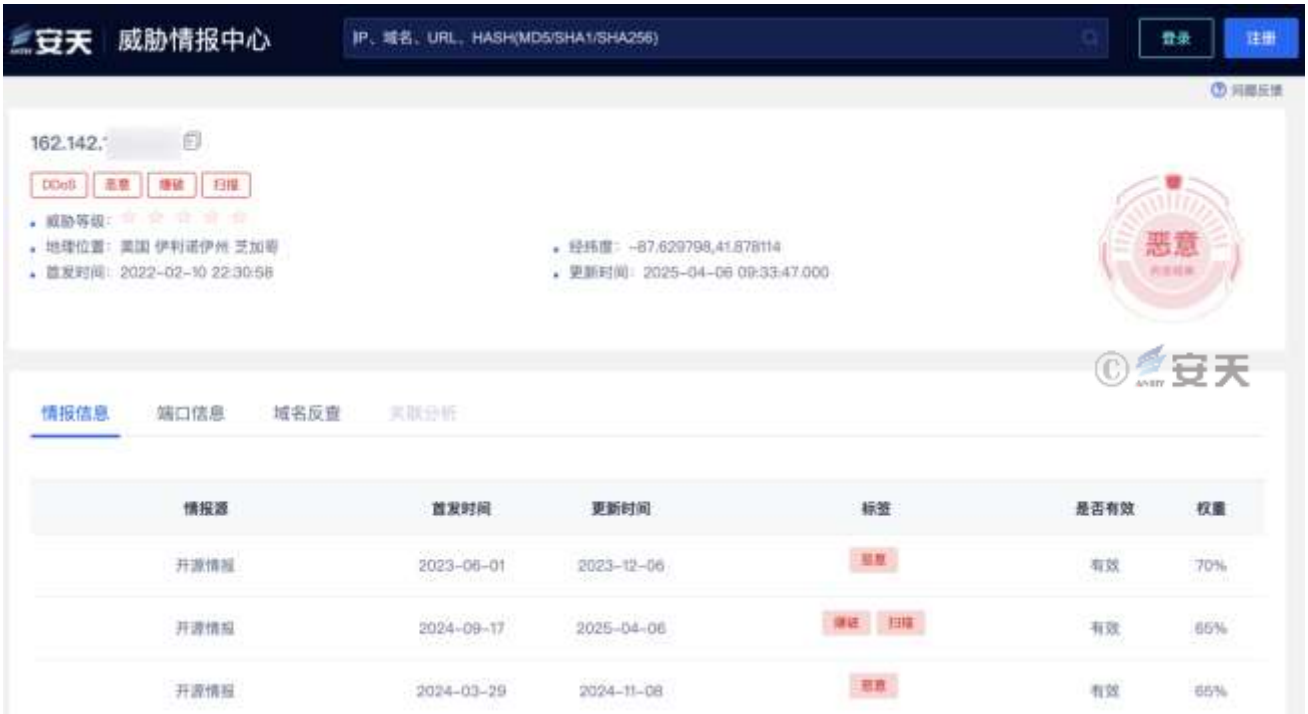

Figure 2-2 Antiy Threat Intelligence that the behavior tag of the attack IP is scanning.2

An ASN query is made to the attack IP and it is found that it belongs to AS 398324 (CENSYS-ARIN-01), and the CENSYS-ARIN-01 network segment is owned by US company Censys, Inc.

Figure 2-3 ASN Query shows that IP belongs to CENSYS 3

Of particular concern, in October 2024, the Center for Cyber Threat Intelligence Integration (CTIIC), a division of the Office of the Director of National Intelligence (ODNI), awarded Censys a multi-year contract, codenamed "Sentinel Horizon" (Sentinel Horizon). Under the contract, Censys will provide its Internet intelligence platform services to the agencies of the US intelligence community. Censys uses its global Internet continuous scanning and monitoring capabilities to provide US intelligence agencies with real-time coverage and access to all Internet-exposed assets around the world.

2.2 Case of brute force cracking

Brute force attack is to obtain the access right of the protected system through repeated attempts of system login without the attacker holding the login credentials of the target system. The basic principle is to try a null password, a weak password, a preset password for equipment exit or a password that has been historically cracked (leaked), or a combination based on user-related information and numbers or letters, etc. To repeatedly log in and find out the correct password, it is in the network attack activity in the "initial access," "credentials access" and other links.

At 22: 00 on February 8, 2025, Antiy monitored and blocked a violent attack incident in which the attack source IP address was located in Vietnam. The attacker uses the IP address 103.237. * * *. * * to initiate an SSH brute force attack attempt to the client server in an attempt to obtain the system access right. After in-depth analysis, Antiy

confirmed that the attack was not successful and immediately started the threat tracing process. Through multi-dimensional threat intelligence analysis, it shows that the geographic location of the attack IP is Vietnam, and the threat tag shows the related address associated scanning, brute force cracking and other malicious activities. The attack IP is linked to the business domain name (idtvieetnam [.] vn) of a library digitization company in Vietnam.

Figure 2-4 The Alarm Information of Antiy Network Threat Monitoring and Early Warning System 4

Antiy Threat Intelligence Center shows that the attack IP belongs to Vietnam, with "malicious," "demolition," "scanning" and other labels.

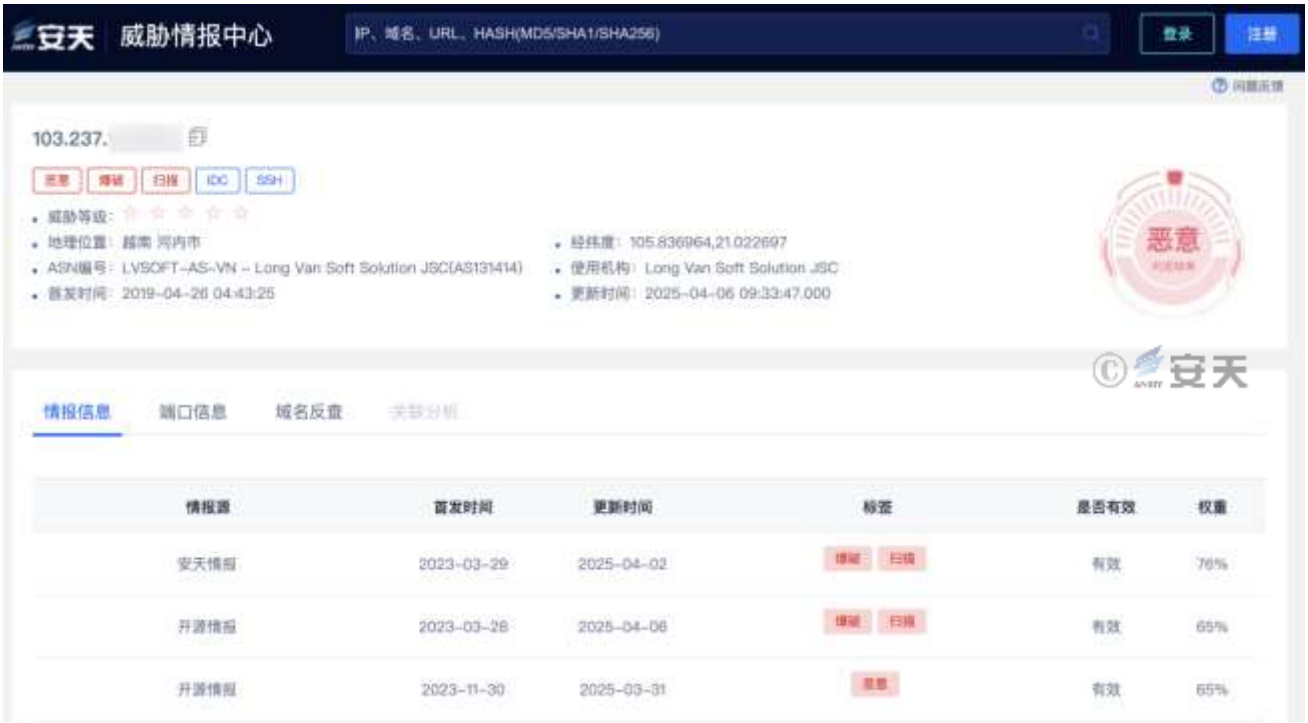

Figure 2-5 Antiy Threat Intelligence shows that the IP behavior label is explosion

Conduct domain name counter-searches on the attack IP, find the associated domain name (demo [] idtvietnam [.] vn), browse the content of idtvietnam [.] vn, a Vietnamese company specializing in library digitalization. It is preliminarily judged that the relevant host machine is invaded and controlled by the attacker, and becomes the attack broiler.

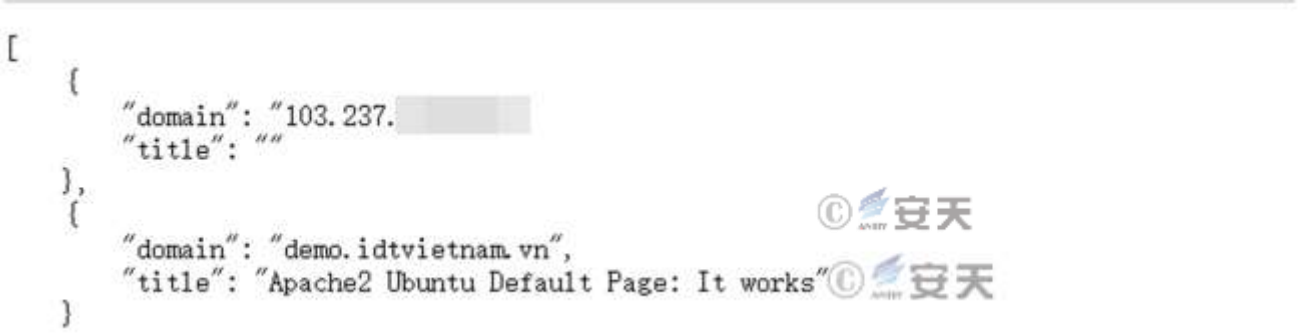

Figure 2-6 IP reverse domain name search result

2.3 Case of Vulnerability exploitation

Vulnerability exploitation refers to the behavior of an attacker who exploits security vulnerabilities in software, hardware or network protocols to perform unauthorized operations. It is in the network attack activity "initial access," "execution," "authority enhancement" and "defense bypass" and other links.

At 10: 00 on February 7, 2025, Antiy monitored and blocked a vulnerability exploitation attack in which the source IP address of the attack was located in the United States, and the attacker attempted to exploit the vulnerability to gain system control authority. The Antiy Cybersecurity Guard Team quickly responded and completed the study and judgment of the attack, confirmed that the attack did not cause actual harm, and immediately started to trace the source. Through such means as threat intelligence inquiry, domain name counter-search, historical asset mapping and Internet search, it is found that the IP is related to the domain name (binaryedge [.] ninja) of BinaryEdge, a Swiss network security company.

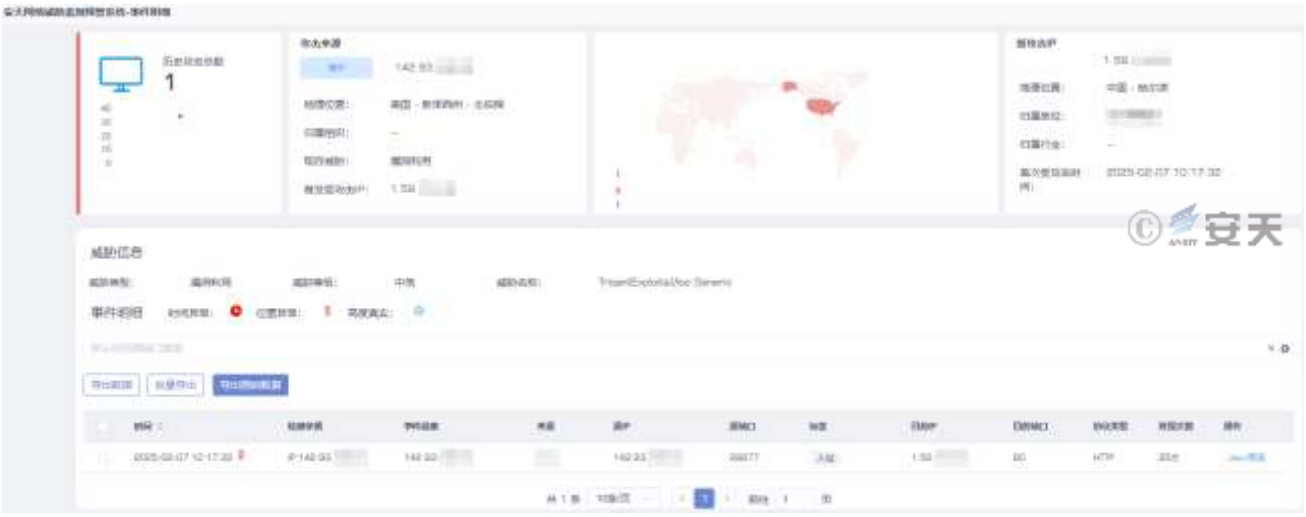

Figure 2-7 The Alarm Information of Antiy Network Threat Monitoring and Early Warning System 5

The Antiy Threat Intelligence Center shows that the attack IP belongs to the United States, with "malicious," "demolition," "scanning" and other labels.

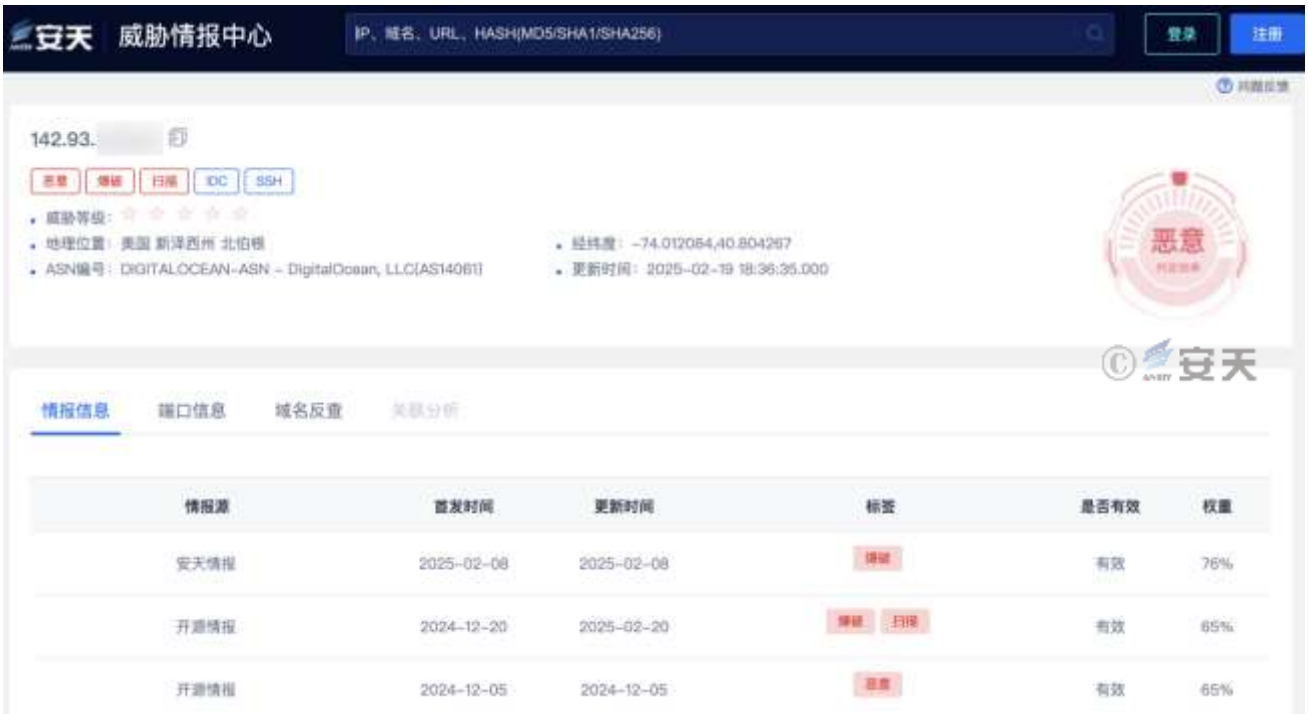

Figure 2-8 Antiy Threat Intelligence shows that the attack IP behavior label is scanning6

In the domain name counter-search on the attack IP, the related domain names binaryedge [.] ninja and binaryedge [.] io were found, and the domain name belonged to Swiss company BinaryEdge.

Binaryedge is a cyber security company that provides real-time threat intelligence on the inside of cyber attacks. Its platform collects information about open ports, services, potential vulnerabilities and poorly configured network sharing by scanning devices and services on the Internet. Through the above events, it is determined that the PoC

authentication is performed, not only the port service and the fingerprint detection are performed.

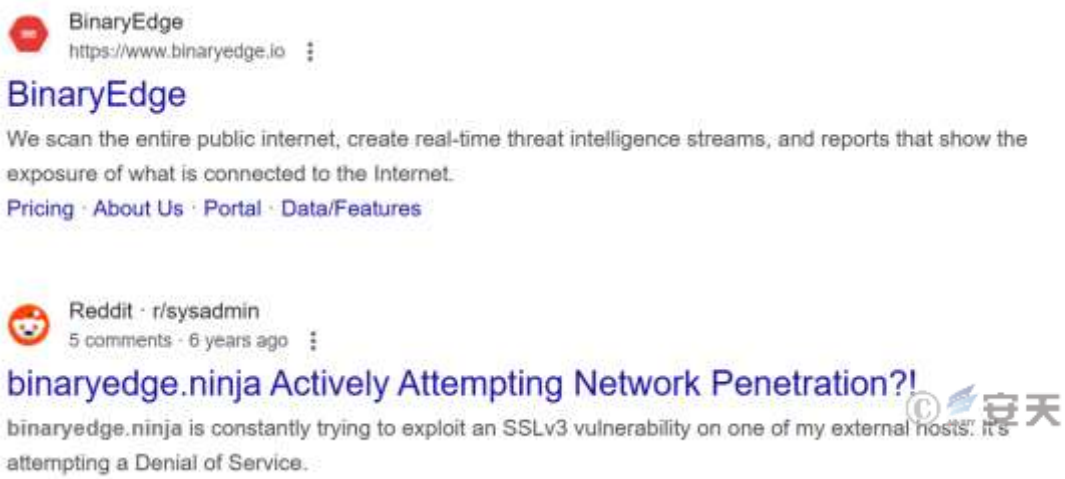

Figure 2-9 Counterfeit finds that the domain name belongs to BinaryEdge of Switzerland

2.4 Remote control attack case

Remote control attack means that an attacker implants a malicious program (Trojan, etc.) with remote control function or utilizes legitimate remote management tools (such as VNC, RDP, TeamViewer, etc.). And an open management service of the machine itself, such as a remote desktop, to enable behavior that can manipulate the target system, It is in the network attack activity "command and control," "persistent," "execution" and "defense bypass" and so on link.

At 4: 00 on February 14, 2025, Antiy monitored and blocked a remote control attack in the Netherlands where the attack source IP address was located. The Antiy Cybersecurity Guard Team tracing analysis found that this IP had spread the remote control Trojan family NanoCore. Nanocore is a well-known remote control Trojan that was originally developed as a legitimate remote management tool, but is widely used for malicious purposes. It has functions such as remote control, keylogger, screen monitoring, data theft and camera control, and is often spread through phishing emails or vulnerabilities. Infection can result in privacy breaches, data theft and devices being fully controlled.

Figure 2-10 The Alarm Information of 2Antiy Network Threat Monitoring and Early Warning System7

According to the Threat Intelligence Center, the attack IP belongs to the Netherlands, with "malicious," "remote control," "NanoCore" and other tags.

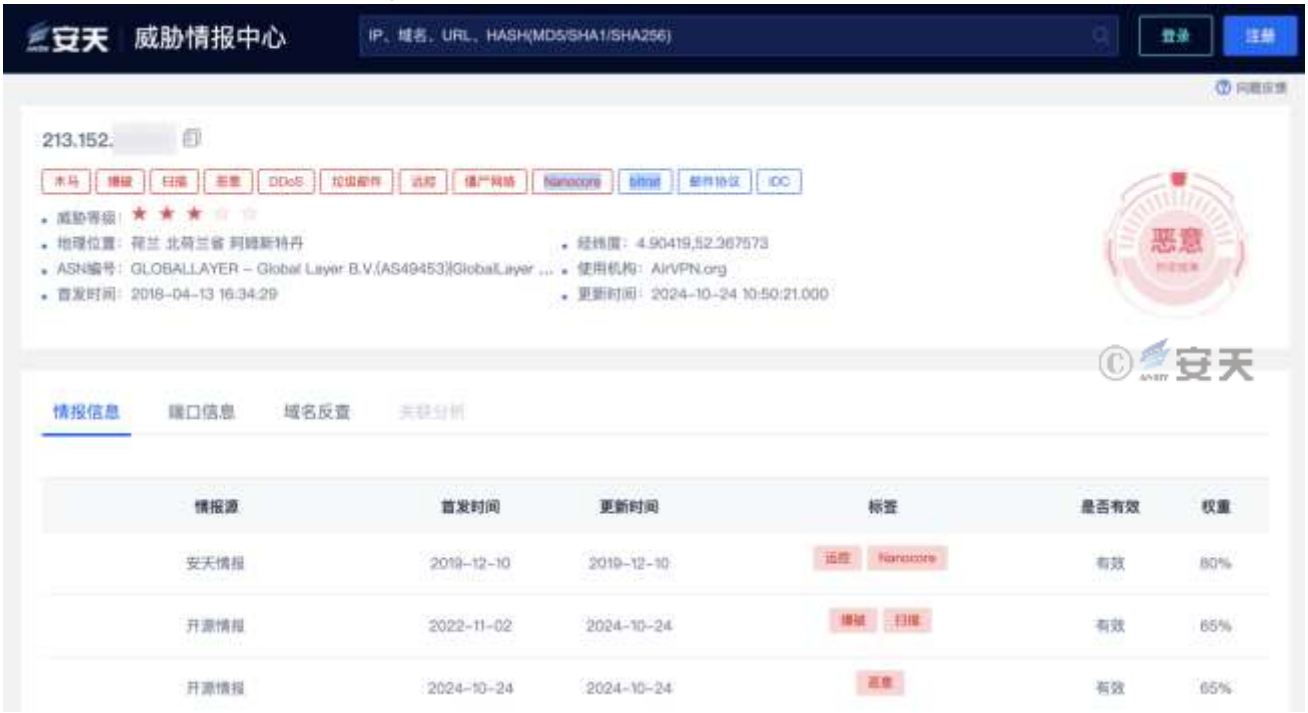

Figure 2-11 Antiy Threat Intelligence shows the attack IP uploads NanoCore (remote control Trojan)8

2.5 Mining attack case

Mining attack refers to the behavior that an attacker uses the computing resources (such as CPU and GPU) of the victim to mine cryptocurrencies (such as Bitcoin and Monroe coins) without authorization, for the purpose of profiting by stealing resources. It is in the network attack activity "execution," "persistent" and "defense bypass" and so on link.

During major activities, the Antiy Cybersecurity Guard Team responded to a number of server mining attacks. Based on the fact that the network side perceives the connection of the relevant server to the address of the mine pool, since the server is not installed with the protection software, the security team guides the user to handle the tool. Sample of Trojan discovered (sample hash: B4a802912838add056fb0aca7ee3a835, virus name: Trojan/Win64.CoinMiner). After executing, the Trojan first copies itself to the directory C:\ProgramData\WinMngr\, and names it as winmngrsa. exe, and creates a driver file named yoygdjmdclhw. sys under C:\Windows\TEMP\. The Trojan hides its behavior through a series of well-designed service operations, including deleting the original "WinMngr" service, re-creating the namesake service and setting it to self-start, and stopping the syslog service to evade detection. After the mining Trojan is started, it will connect the malicious IP address 185.215. * * *. * * * through the dwm.exe process. According to traffic analysis, these connections are all mining communication traffic, and the wallet address is 47fEQ5mTN8MCL91SaD6ooigyfKdGfTchFTudQLoyZ4Kps7jG19n1UA8eSwuzomEtjQqKkZr6NmcUWa3HtuA2dEe6e. The Trojan will consume a lot of computing resources of the system, which will result in the serious performance degradation of the server, affect the normal operation of business, and cause the waste of power resources and shorten the life of hardware equipment.

Table 2-1 Sample labels 1

Virus name	Trojan / Win64.CoinMiner
Original file name	Winmngrsa.exe
Md5	B4a802912838add056fb0aca7ee3a835
Processor architecture	Intel 386 or later processors and compatible processors
File size	2.50 MB (2,620,416 bytes)
File format	Binexecute / Microsoft.EXE [: X86]
Time stamp	2024-12-26 17: 17: 10
Digital signature	None
Shell type	None
Compiled Language	Microsoft Visual C + +

After running, the Trojan will copy itself to the directory C:\ProgramData\WinMngr\, name it winmngrsa.exe, and reside in the system with the process name winmngrsa. exe.

Figure 2-12 Copy itself to the current directory 9

The Trojan uses the driver technology and ATool (a security kernel analysis tool for security system), to discover the Trojan and create a driver file named yoygdjmdclhw.sys under C:\Windows\ TEMP\, and open the cloud search function of ATool. The driver file is tagged with both malicious content and malicious behavior by ATool's reputation analysis, but with a legitimate digital signature.

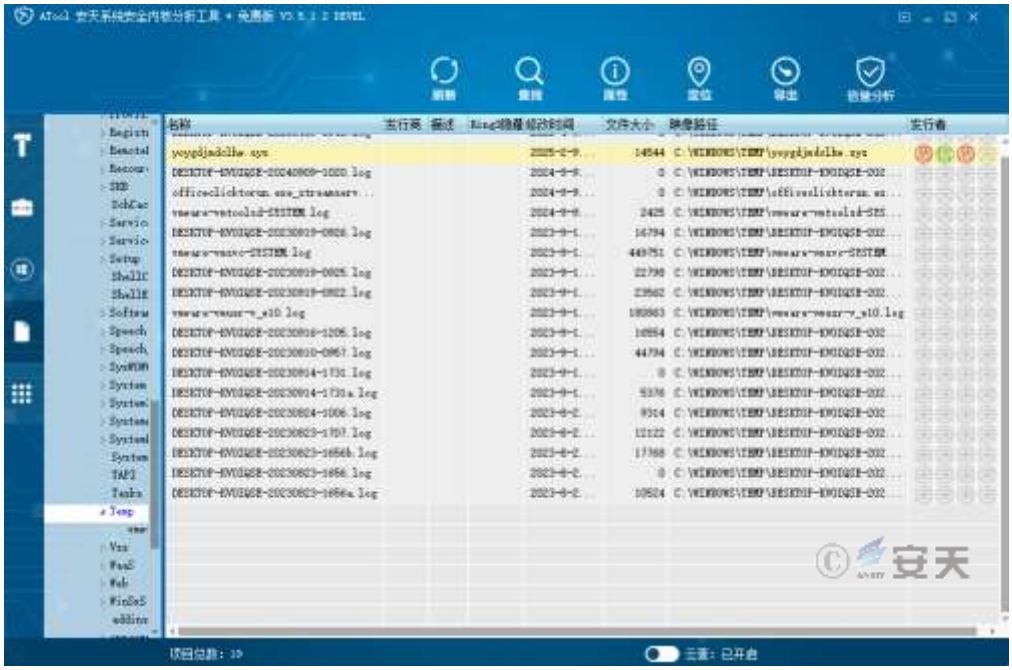

Figure 2-13 Create a driver file named yoygdjmdclhw. sys under the TEMP directory

Delete the original "WinMngr" service in the system, re-create the service with the same name and set it as self-startup, so as to facilitate the victim machine to execute again after restart. The following figure shows the service created by using ATool's cloud search function to find the virus, and orange means malicious.

Figure 2-14 Creating a "WinMngr" service10

After the mining virus is started, it will connect the malicious IP address 185.215. * * *. * * * through the dwm.exe process.

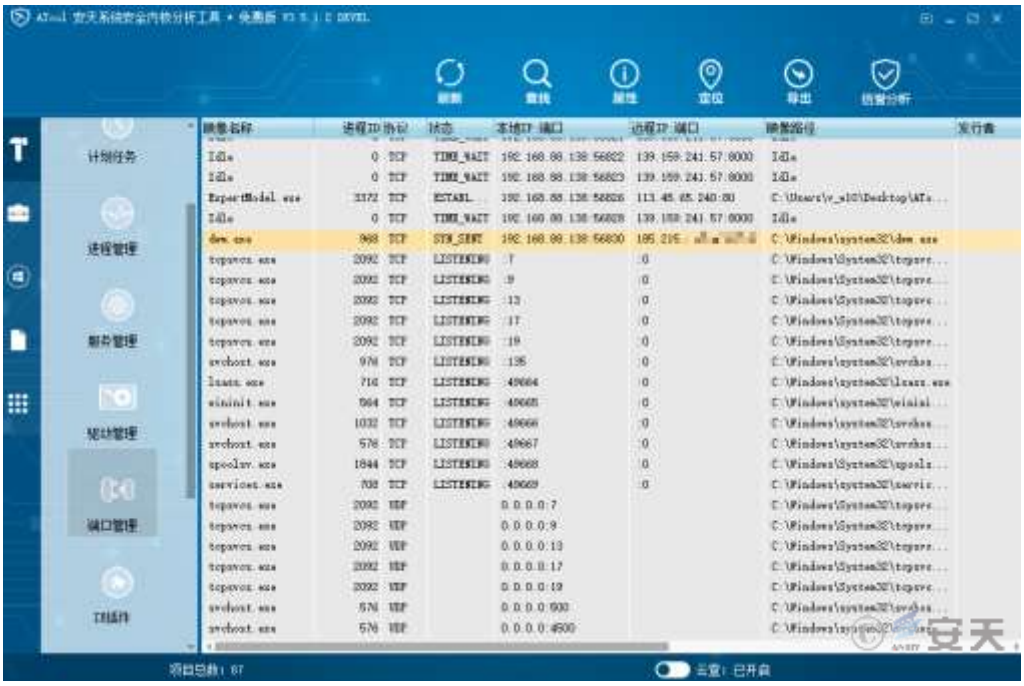

Figure 2-15 Connecting the malicious IP address 2-11

Virus built-in XMRig mining program for mining, version 6.21.3, wallet address 47fEQ5mTN8MCL91SaDm6ooigyfKddGchFTudHDQLoyZ4Kps7jG19n1UA8eSwuzomEKqKkKkZr6NmcbUWa3HtuA2deE6e.

{"id":1,"jsonrpc":"2.0","method":"login","params":
{"login":"47fEQ5mTN8MCL91SaDm6oo1gyfKddGfTchFTudHDQLoyZ4Kps7jG19n1UABeSwuzomEtjQqKkkZr6MacbUNa3HtuA2dEe6e","pass":"x","agent":"XMRig/6.21.3 (Windows NT
10.0; Win64; x64) libuv/1.38.0 msvc/2022","rigid":"","algo":["rx/0","cn/2","cn/r","cn/fast","cn/half","cn/xao","cn/rto","cn/rwz","cn/zls","cn/double","cn/
ccx","cn-lite/1","cn-heavy/0","cn-heavy/tube","cn-heavy/xhv","cn-pico","cn-pico/tlo","cn/upx2","cn/1","rx/wow","rx/arq","rx/graft","rx/sfx","rx/
keva","argon2/chukwa","argon2/chukwav2","argon2/ninja","ghostrider"]}}
{"jsonrpc":"2.0","id":1,"error":null,"result":{"id":"89d5574a99dedceb","job":
{"blob":"101093e3a1bd061841a5276679306142fd539fd5e2570ea3de2193ac201c36d7961cb963d1de00000000a0950212734e9a304a016e62e7f2eeece1ba2780db2fc6237441c1f8573b5ad
2c687","job_id":"20954","target":"f3220000","algo":"rx/0","height":
3343734,"seed_hash":"ddd4126b15ec91d5133dd5686f45a6dd52c129a16338fe5dce6f40ac7e4451ed"},"extensions":
["algo","nicehash","connect","tls","keepalive"],"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"1010a5e3a1bd061841a5276679306142fd539fd5e2570ea3de2193ac201c36d7961cb963d1de00000000a09a5e0c0943fecb28019e772293cb95d3d4868ff42c93c6d2450b719a3944c
ed208","job_id":"20955","target":"f3220000","algo":"rx/0","height":3343734,"seed_hash":"ddd4126b15ec91d5133dd5686f45a6dd52c129a16338fe5dce6f40ac7e4451ed"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"1010afe3a1bd061841a5276679306142fd539fd5e2570ea3de2193ac201c36d7961cb963d1de00000000a0bb77560f55dd9bc41ac5be4ffef164c1103c5af722dbc962edf12b5f39de5
ed90b","job_id":"20956","target":"f3220000","algo":"rx/0","height":3343734,"seed_hash":"ddd4126b15ec91d5133dd5686f45a6dd52c129a16338fe5dce6f40ac7e4451ed"}}

Figure 2-16 Excavation Flow12

For details of the mining Trojan, see the Virus Encyclopedia of Antiy.

Figure 2-17 Long pressing the identification QR code to view details of CoinMiner mining Trojan13

2.6 Botnet case

Botnet refers to a network system composed of a large number of devices (such as PC, server and IoT devices) infected by malicious software, which can be controlled in batch. The attacker remotely manipulates the command and control server (C & C server) to execute network attack activities (such as DDoS attack, stealing sensitive information, sending spam, etc.). And these infected computers are often referred to as "zombie hosts" or "broilers," It is in the "initial access," "execution," "persistence," "command and control" and "influence" of network attack activities.

Before the start of major activities, several government and enterprise units urgently deployed Antiy IEP (Network Security Responsibility Action Version) to cover tens of thousands of host terminals, and several zombie network infection events were discovered after the installation. To achieve a thorough clean-up. Killed a number of botnet viruses, including the "Phorpiex" botnet malware. The "Phorpiex" botnet has infected at least one million computers worldwide, and malware (MD5: A775d164cf76e9afd7eb1e3ab2e, virus name Trojan / Win32.Phorpiex) is the core component of the "Phorpiex" botnet. The virus first creates a hidden directory of random numbers on the

system disk, disguises itself as a dllhost. exe system file, and persists through registry startup keys and firewall exceptions. This sample has the ability to compromise system safety protection. By modifying the registry, viruses can simultaneously disable Windows Defender, turn off real-time protection, and mask security notifications and other critical security settings. In addition, that virus continuously monitor the contents of the clipboard and automatically replace the wallet address for theft when a cryptocurrency transaction is detect. In terms of propagation mechanism, the botnet exhibits a strong diffusion capability. Its built-in VNC worm module will scan random IP address and use hard-coded dictionary to brute-force crack port 5900; NetBIOS worm module will propagate through port 139 and use hard-coded password to attack. Once the defense line is broken, the virus will immediately download XMRig mining program, consuming host resources for the attackers profit.

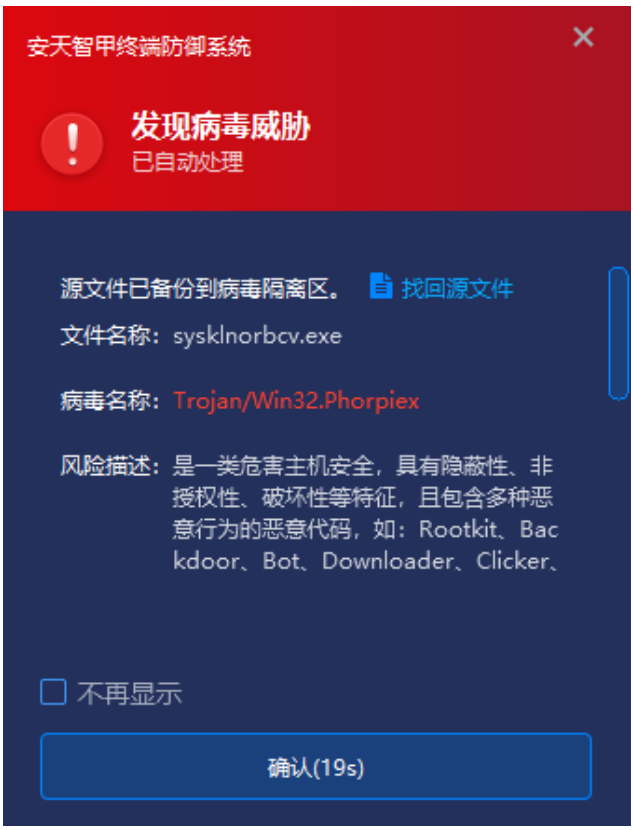

Figure 2-18 Interception of Phorpiex botnet malware14

According to the alarm log display of Antiy IEP, a total of 3 Phorpiex botnet malware attacks were checked and killed.

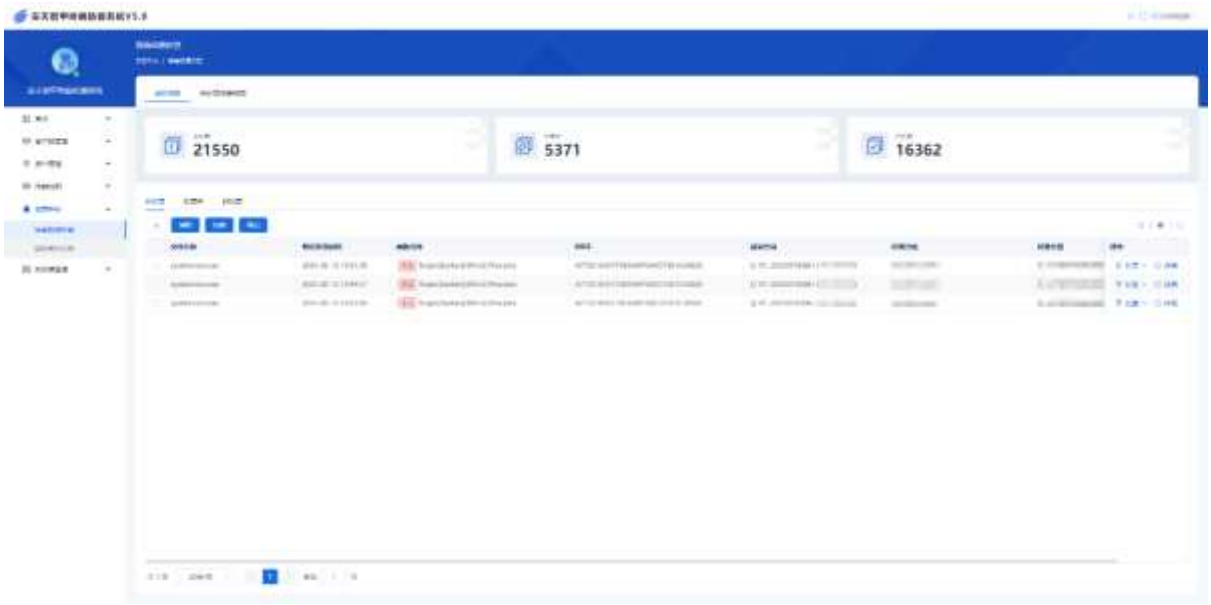

Figure 2-19 Management log for IEP killing of Phorpiex botnet malware15

Table 2-2 Sample labels2

Virus name	Trojan / Win32.Phorpiex
Original file name	Sysklnorbcv.exe
Md5	A775d164cf76e9a9ff6afd7eb1e3ab2e
Processor architecture	Intel 386 or later processors and compatible processors
File size	84.50 KB (86,528 bytes)
File format	Binexecute / Microsoft.EXE [: X86]
Time stamp	2024-09-21 20: 10: 13
Digital signature	None
Shell type	None
Compiled Language	Microsoft Visual C + +

Details of the botnet can be found at Antiy Virus Encyclopedia.

Figure 2-20 Long pressing the identification QR code to view details of the "Phorpiex" botnet 16

3 Summary

Network scanning, brute force cracking, vulnerability exploitation, remote control, mining and botnet attacks are all common and frequent attack events. The six typical events we disclose this time are typical cases among the massive events perceived and responded to during the security guarantee of this major event. The background of these events includes not only black and gray industry criminal gangs but also the shadow of certain national security enterprises and institutions, confirming the diversity and complexity of technological confrontation and interest games in cyberspace.

Facing complex, severe and persistent threats and challenges also reminds us that we cannot merely enhance security guarantee capabilities during major events. Instead, we need to summarize and distill the experience and achievements of cybersecurity guarantee for major events, and transform them into regular security guarantee capabilities. We should build a "bottom-line" mechanism for urban cybersecurity protection. Urban management institutions need to attach importance to the construction of common cybersecurity capabilities and infrastructure, form security management and regular cybersecurity operation capabilities, and ensure the operation of modern cities by establishing a long-term operation mechanism.

Reference:

Antiy. Major Activities: Experience Summary and Work Prospect of City-side Network Security [R/OL]. (2025-04-07)

https://mp.weixin.qq.com/s/KP7GDaY7lvxHwNTfaOqHpQ