Analysis of the Lilith Botnet and the Hacker Group Behind It

Antiy CERT

Completion time of first draft: 29 August, 2022

Time of first release: 2 September, 2022

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

1 Overview

Recently, Antiy CERT captured the Lilith botnet developed and sold by the Jester hacking gang. In addition to the functions of malicious codes such as secret Trojan, clipboard hijacker and mining Trojan developed and sold by the gang, the botnet also has the functions of persistence and remote control. It causes the threat of confidential data leakage, virtual property loss and system resource exhaustion to the users.

Antiy CERT published the "Analysis of the Active Jester Stealer Trojan and the Hacker Gang Behind it" in May 2022 [1]. The report analyzed in detail the Jester hacker gang development sale Jester Stealer Trojan, Merlynn Cliper clipboard hijacker and other malicious code. In combination with the Lilith botnet samples captured this time, it can be seen that the hacker gang is developing more types of malicious code to meet the needs of the attackers in pursuit of the maximization of interests. And the addition of new malicious features, subscription mode to achieve higher returns. In the environment of fierce competition of commercial malicious codes, the average cost and technical threshold for attackers to launch network attacks are further lowered, and it can be expected that the number of network attacks will continue to increase in the future. It brings more severe challenges to the network security industry.[1]

It has been proved that Antiy IEP can effectively detect and kill the botnet program, and Antiy PTD can accurately detect the C2 communication of the botnet.

2 ATT&CK Mapping Map of Samples

Technical characteristic distribution map corresponding to the sample:

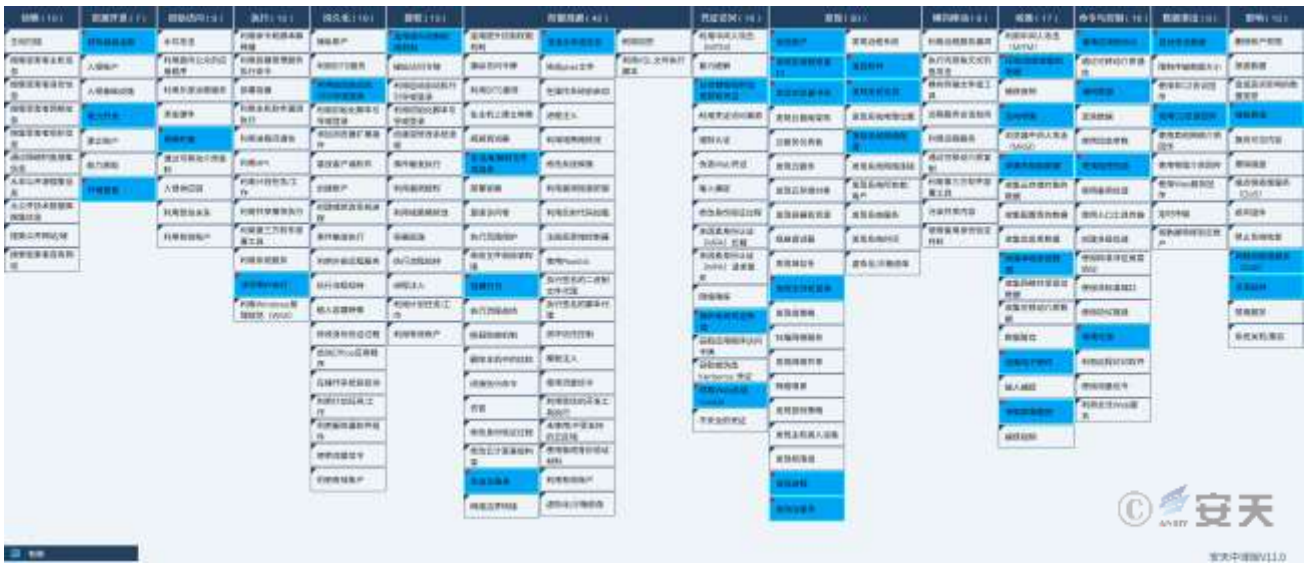

Figure 2-1 Mapping of Technical Features to ATT&CK 2-1

Specific ATT&CK technical behavior description table:

Table 2-1 ATT&CK Technical Behavior Description Table 2-1

ATT&CK stages / categories	Specific behavior	Notes
Resource development	Access to infrastructure	Build C2 server
	Capacity development	Developing malware
	Environmental preparation	Using Github to manage files
Initial access	Phishing	Spread by phishing on the Internet
Execution	Inducing the user to execute	Inducing the user to execute
Persistence	Use automatic startup to perform booting or logging	Copies itself to the startup directory
Right to Submission	Abuse of enhanced control authority mechanism	Bypass the UAC
Defensive evasion	Anti-obfuscate / decode files or information	Decrypt C2 Address Configuration
	Concealment	Concealment
	Modify the registry	Modify the registry
	Confusion of documents or information	Confusion of documents or information
Credential Access	Obtain credentials from the location where the password is stored	Obtain credentials from the location where the password is stored
	Operating system credential dump	Operating system credential dump
	Stealing Web Session Cookie	Stealing Web Session Cookie

Findings	Discovery of account	Discover the current user name
	Discover the application window	Discover the application window
	Discover browser bookmarks	Discover browser bookmarks
	Find files and directories	Find files and directories
	Discovery Process	Discovery Process
	Query the registry	Query the registry
	Discovery Software	Discovery Software
	Discovery of system information	Discovery of system information
	Discovery system network configuration	Discovery system network configuration
Collection	To compress / encrypt the collected data	The theft component packages the data as ZIP
	Automatic collection	Automatic data collection
	Collect clipboard data	Read the clipboard
	Collect local system data	Collect local system data
	Collect e-mail	Collect e-mail
	Get a screenshot	Get a screenshot
Command and control	The application layer protocol is used	Use the HTTP protocol
	Encoded data	Use Base64 to encode online packages
	Use an encrypted channel	Communication data is encrypted using aes
	Use of Agent	Using the Tor Agent
Data seeps out	Automatically seeps out data	Automatically seeps out data
	The C2 channel is used for backtransmission	The same channel as c2 is used for backtransmission
Impact	Manipulation of data	Modify the clipboard
	Network side Denial of Service (DoS)	Launching a DDoS attack
	Resource hijacking	Carry out the excavation procedure

3 Recommendations for protection

In order to effectively defend such malicious codes and improve the level of security protection, Antiy suggests the enterprise take the following protection measures:

3.1 Improve that security protection capability of the host machine

（1） Install the terminal protection system: Install the anti-virus software, and it is recommended to install the terminal protection system of Antiy IEP;

（2） Strengthen password strength: Avoid using weak passwords, recommend using 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid using the same password for multiple servers;

（3） Deployment of Intrusion Detection System (IDS): Deployment of traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of malicious codes. Taking network traffic as the detection and analysis object, the Antiy PTD can accurately detect a mass of known malicious codes and network attack activities, and effectively detect suspicious behaviors, assets and various unknown threats on the network;

3.2 Improve that consciousness of network security protection

（1） When receiving an email, confirm whether the sending source is reliable, and avoid opening the URL and attachment in the suspicious email;

（2） It is recommended to use the sandbox environment to execute suspicious files, and then use the host computer to execute the files with security. Based on the combination of deep static analysis and dynamic loading of sandbox, the PTA can effectively detect, analyze and identify all kinds of known and unknown threats.

3.3 Timely initiate emergency response in case of attack

（1） Contact the emergency response team: In case of malware attack, it is suggested to isolate the attacked host in time, protect the site and wait for the security engineer to check the computer; Antiy 7 * 24 service hotline: 400-840-9234.

It has been proved that Antiy IEP can effectively detect and kill the botnet.

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

4 Lilith Botnet Network Analysis

4.1 Sample labels

Table 4-1 Binary executable file 4-1

Virus name	Trojan / Win32.Botnet
Original file name	Explorer.exe
Md5	1cae8559447370016ff20da8f717db53
Processor architecture	Advanced Micro Devices X86-64
File size	492.20 KB (504,008 bytes)
File format	Binexecute / Microsoft.EXE [: X64]
Time stamp	2089-09-02 08: 22: 23 UTC (forged)
Digital signature	Invalid
Shell type	None
Compiled Language	.net
Vt First Upload Time	2022-06-21 19: 16: 14 UTC
Vt test result	46 / 71

4.2 Detailed analysis

The GUID is generated as the user ID of the infected device and the mutex is created therefrom.

```
internal sealed class c_get_Help_ZKHJHA
{
    // Token: 0x0600055C RID: 1372 RVA: 0x00016EA0 File Offset: 0x000150A0
    public static string m_GetPermissions_6TW45K()
    {
        string text = string.Empty;
        if (c_get_StateMessage_77GN5R.m_Broadcast_UV41C2("Lilith:Guid"))
        {
            text = c_get_StateMessage_77GN5R.m_get_Headline_HCPLMS("Lilith:Guid");
        }
        else
        {
            text = Guid.NewGuid().ToString();
            c_get_StateMessage_77GN5R.m_RemovePlayerFromGroup_EIGJ6C("Lilith:Guid", text);
        }
        return text;
    }
```

Figure 4-1 Generation of User ID 4-1

Store the user ID encrypted in the registry.

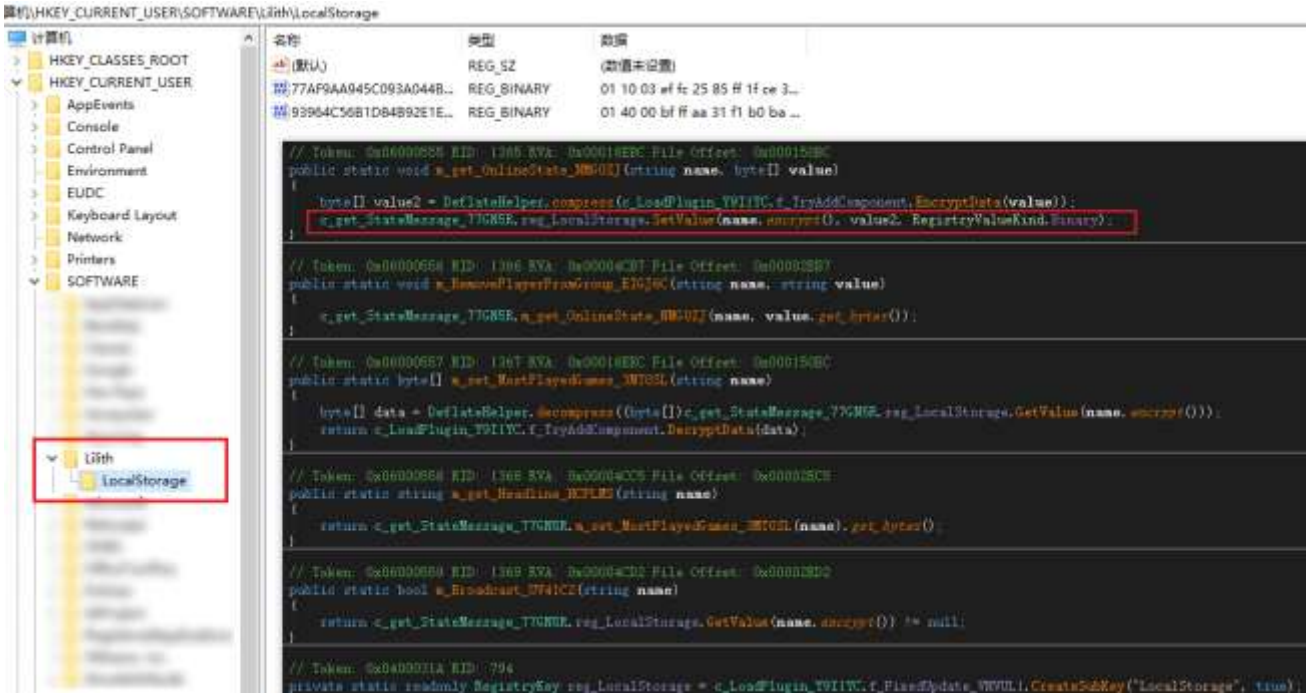

Figure 4-2 stores the user ID in the registry 4-2

Decrypt the configuration information, and obtain the C2 address, the communication key and the botnet code.

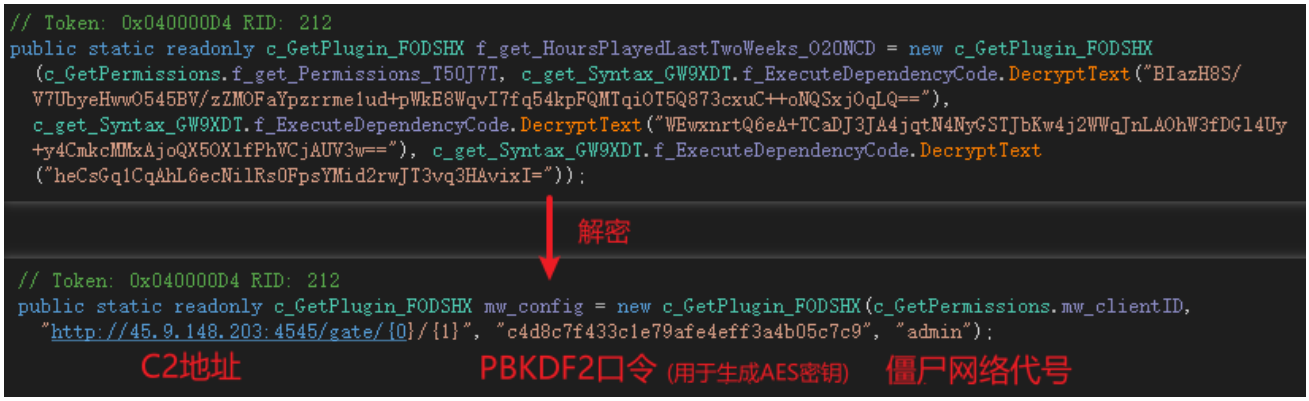

Figure 4-3 Decrypt the configuration information 4-3

Copy itself to the boot directory for persistence.

```
// Token: 0x17000103 RID: 259
// (get) Token: 0x0600053F RID: 1343 RVA: 0x000169E8 File Offset: 0x00014BE8
public static string StartupFileName
{
    get
    {
        string text = c_LoadPlugin_Y9I1YC.f_ParseUInt32.ToLower();
        return Path.Combine(c_Translate_4B3CNR.mw_startup, (text.EndsWith(".exe") || text.EndsWith(".com") || text.EndsWith
          (".scr")) ? c_LoadPlugin_Y9I1YC.f_ParseUInt32 : (c_LoadPlugin_Y9I1YC.f_ParseUInt32 + ".exe"));
    }
}

// Token: 0x06000540 RID: 1344 RVA: 0x00004C3A File Offset: 0x00002E3A
public static bool m_GetPermissions_QUB8OH()
{
    return File.Exists(c_Translate_4B3CNR.StartupFileName);
}

// Token: 0x06000541 RID: 1345 RVA: 0x00016A48 File Offset: 0x00014C48
public static bool m_Unload_7WED5B()
{
    bool result;
    try
    {
        File.Copy(c_Translate_4B3CNR.f_set_Name_VDLRQF, c_Translate_4B3CNR.StartupFileName, true);
        return true;
    }
    catch
    {
        result = false;
    }
    return result;
}
```

Figure 4-4 Set persistent startup 4-4

The information returned by the C2 server is encrypted by AES-256-CBC, and its AES encryption key is generated by PBKDF2 (Password-Based Key Derivation Function 2). Specifically, the security hash algorithm used in the algorithm is SHA-512. Password (Passphrase) is the hard-coded "c4d8c7f433c1e79afe4eff3a4b05c7c9" in the sample, salt value (Salt) is the user ID, and iteration rounds (Iterations) are 1000 rounds.

```
byte[] array = new byte[this.Salt.Length + 4];
Buffer.BlockCopy(this.Salt, 0, array, 0, this.Salt.Length);
Buffer.BlockCopy(c_checkCommandMappings.m_SaveGroup_N803YB(this.BlockIndex), 0, array, this.Salt.Length, 4);
byte[] array2 = this.Algorithm.ComputeHash(array);
byte[] array3 = array2;
for (int i = 2; i <= this.IterationCount; i++)
{
    array2 = this.Algorithm.ComputeHash(array2, 0, array2.Length);
    for (int j = 0; j < this.BlockSize; j++)
    {
        array3[j] ^= array2[j];
    }
}
if (this.BlockIndex == 4294967295U)
{
    throw new InvalidOperationException("Derived key too long.");
}
this.BlockIndex += 1U;
return array3;
```

SHA-512

迭代轮数

Figure 4-5 Generate a Communication Key 4-5

Check the network connection in a revolving manner, and send the online package to the C2 server at http://45.9.148.203:4545/gate/<用户 ID>/registerBot to obtain the configuration information after networking. The format of the requested User Agent is "Lilith-Bot / Version (Windows Version)" (for example: Lilith-Bot / 3.0 (Microsoft Windows NT 6.1.7601 Service Pack 1)), The request content includes information such as device IP address, user name, computer name, operating system and so on encoded by base64.

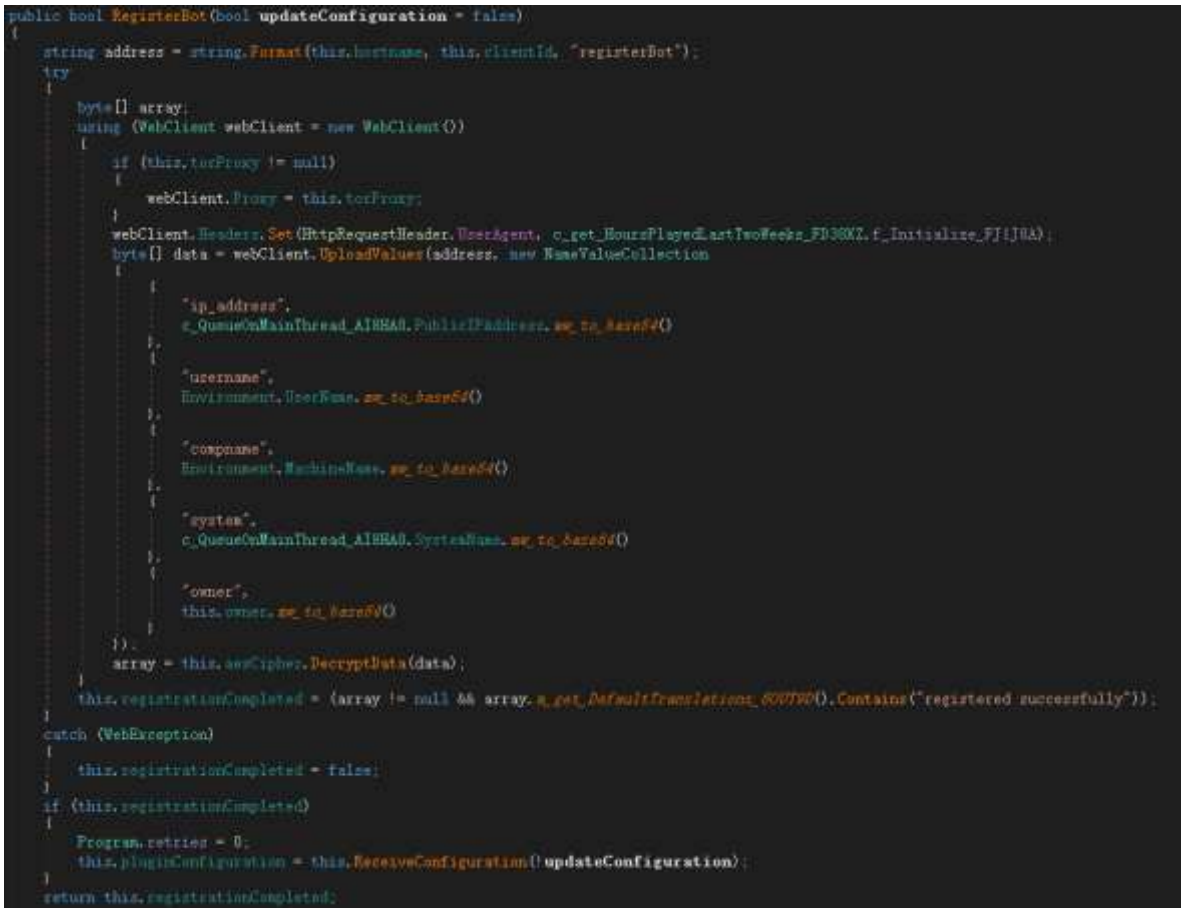

Figure 4-6 Sending the online package 4-6

Connect http://45.9.148.203:4545/gate/<用户 ID>/getFile?name=<僵尸网络代号>_plugin_settings.json to obtain the configuration information. the decrypted contents and meanings are shown in the figure below.

```
{
    "Lilith": {
        "CommandsCheckInterval": 10  获取指令间隔时间（秒）
    },
    "BotKiller": {
        "Enabled": false  执行自删除
    },
    "Stealer": {
        "Enabled": true  启用窃密功能
    },
    "Clipper": {
        "Enabled": true, 启用剪贴板劫持功能
        "Addresses": { 劫持后的钱包地址
            "XMR":
            "49CsHzjLmHTNgrhqnfSdpjL4ZyzyTTZPiYlulnwWgZo2NSk5RdvAcKTMkXpZbE6YD8f
            B2oG27RqgpTnWJ6EpUJSo5kDSvjK",
            "BTC": "1KEHVRrzYTLRwvYjoNh7BVEuaSzzuwnUK",
            "ETH": "0xe298e33f927adefd0bd287f7B028e93062b77a3a"
        }
    },
    "Miner": {
        "Enabled": true,  启用挖矿
        "Pool": "pool.minexmr.com:4444", 矿池地址
        "Wallet":
        "49CsHzjLmHTNgrhqnfSdpjL4ZyzyTTZPiYlulnwWgZo2NSk5RdvAcKTMkXpZbE6YD8fB2oG
        27RqgpTnWJ6EpUJSo5kDSvjK", 钱包地址
        "Password": "x", 密码
        "MaxCPU": "40" 最大CPU资源占用（%）
    }
}
```

Figure 4-7 Acquired configuration information 4-7

According to the configuration information, connecthttp://45.9.148.203:4545/gate/<用户 ID>/getCommands to obtain the remote control instruction at an interval, and the instruction is composed of multiple strings separated by ":" The first two paragraphs are instruction classification and instruction name, and the remaining part is the parameter list, if the parameter contains ":" Use "\:" Escape, if the beginning of the parameter is "< B64 >," the parameter content is encoded in base64. The relevant codes for analyzing remote control instructions are as follows.

```
// Token: 0x060001E3 RID: 483 RVA: 0x0000AB00 File Offset: 0x00008D00
public c_add_OnRockedInitialized_MIWD3B(string Command)
{
    string[] array = Regex.Split(Command, "(?<!\\\\):"); 匹配非转义的 ":"
    this.LibraryName = Path.GetFileNameWithoutExtension(array[0]); 指令分类
    this.FunctionName = array[1]; 指令名称
    this.FunctionPath = string.Join(":", new string[]
    {
        this.LibraryName,
        this.FunctionName
    });
    this.Args = array.Skip(2).Select(delegate(string s)
    {
        if (!s.StartsWith("<B64>")) base64编码的参数
        {
            return s;
        }
        return s.Remove(0, 5).m_RegisterFromAssembly().mw_byte2str();
    }).ToArray<string>();
    this.Args = (from s in this.Args
    select s.Replace("\\:", ":")).ToArray<string>(); 转义 "\:"
}
```

Figure 4-8 Analysis of relevant codes of remote control instructions 4-8

Lilith botnet has the functions of DDoS attack, video "data swiping," stealing, mining, intranet scanning and remote control. the detailed control instructions are as follows.

- **Ddos attack**

Table 4-2 DDoS attack instructions 4-2

Instructions	Description
Ddos: Httpget: Link	Generate a random request parameter and initiate an HTTP GET flood attack
Ddos: Httppost: Link	Generate a random packet and initiate an HTTP POST flood attack
Ddos: Tcpflood: Host\: Port	Initiates a TCP flood attack to a specified host port, which defaults to 80 when no port is specified
Ddos: Udpflood: Host\: Port	Initiates a UDP flood attack to a specified host port, which defaults to 80 when no port is specified
Ddos: Stopattacks	Stop the ongoing DDoS attack

- **Video "swipe data"**

Table 4-3 Instruction of video "Brush data" function 4-3

Instructions	Description
Advertising: Youtube _ ViewVideo: Video link	Through the background silent broadcast designated network video, video brush playback volume
Advertising: Youtube _ ViewStream: Live link	Through the background silent broadcast designated network live broadcast, to live broadcast brush views
Advertising: Youtube _ Subscribe: Channel Link	Use the login information of the user's browser cookie to subscribe to the designated video channel, and swipe the subscription amount
Advertising: Youtube _ Like: Video link	Use the login information of the user browser cookie to like the designated network video
Advertising: Youtube _ Dislike: Video link	Click on the specified network video by using the login information of the user's browser cookie

- **Mining, mining, remote control, scanning**

Table 4-4 Functional instructions for mining, theft, remote control and scanning 4-4

Instructions	Description
Miner: Startminer	Start the excavation sequence
Miner: Stopminer	Stop the excavation process
Stealer: Recovercredentials: Turns on enhancement mode	Password credentials and digital assets in the system are stolen and returned, and enhanced mode will steal browser bookmarks

Hvnc: Start: Parameter 1: Parameter 2	Download and start the HVNC remote control tool using the parameters
Netdiscover: Scannetwork	Scanning of Intranet Host

- **Program release, self-update, uninstall, etc**

Table 4-5 Program distribution and maintenance instructions 4-5

Instructions	Description
Dropper: Downloadexecute: Download Link: Open Administrator Permission: Open to bypass UAC	Download and execute the program, the last two parameter values are true or false, indicating that the corresponding function is on or off
Dropper: Executescript: Script content: Script type	Write the contents of a script, either BAT or PS1, to% Temp% and execute
Lilith: Updateconfiguration	Retrieve configuration information
Lilith: Updateclient: Link	Download and update the botnet program
Lilith: Exitclient	End the botnet program
Lilith: Deleteclient	Uninstall the botnet program

5 Correlation analysis

Through the correlation analysis of the samples, it is found that the Lilith botnet in this analysis is the Jester hacker gang developed and sold by the former Antiy track analysis. The hacker gang will develop all the malicious software to carry on the function integration, the package sale at the higher price, formed Lilith botnet.

Figure 5-1: Lilith botnet selling ad page published by the Jester hacking gang 5-1

In February 2022, the Jester hacker group was renamed Eternity to continue the sale of malware and changed its operation strategy at the same time, because the Jester hacker group was blocked by several hacker forums after being impersonated by other hackers to commit fraud. So that the botnet program only includes remote control, DDoS and other functions, and other functions are purchased separately and then distributed for execution, instead of having to be purchased together.

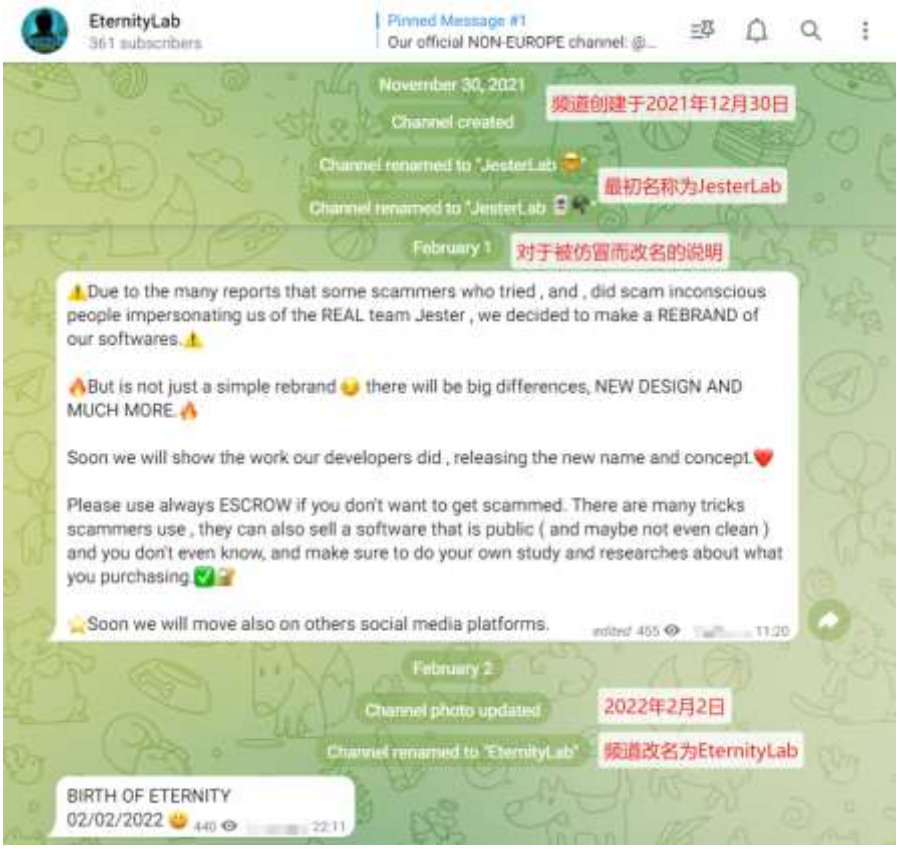

Figure 5-2 The name of the Jester organization is changed to Eterity 5-2

6 Summary

In addition to the persistence and remote control functions, the Lilith botnet also integrates all malicious functions of malicious code developed by the Jester hacker group, such as secret Trojan, clipboard hijacker and mining Trojan. It poses a great threat to the user system security. In pursuit of greater interests, the Jester Hacker Group may evolve into a more threatening hacker group in the future, as it continues to develop more malicious functions while constantly adjusting its operating strategy.

Antiy CERT will continue to track the relevant technical changes and characteristics of the hacker gang, and provide corresponding solutions. Antiy IEP not only has the functions of virus detection and killing, active defense and other functions, but also provides the capabilities of terminal control and network control, which can effectively defend against such threats and protect user data security.

7 IoCs

1cae8559447370016ff20da8f717db53
45.9.148.203: 4545

Appendix I: Reference

[1] An Analysis of the Active Jester Stealer Trojan and the Hacker Gang Behind It
https://www.antiy.cn/research/notice&report/research_report/20220510.html

Appendix II: 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.