# Analysis of Phishing Activities Delivering Snake Keylogger via OneNote Documents

Time of first release: 18 April, 2023

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

## 1 Overview

Recently, Antiy CERT has detected a phishing activity that uses OneNote documents to deliver the Snake Keylogger spyware. The attackers send phishing emails to users, luring them to open the OneNote document attached, and execute the malicious file hidden beneath an image in the OneNote document, thereby running the Snake Keylogger spyware on the user's host.

Since Microsoft announced the default blocking of macros in Office documents, attackers have attempted to use other types of files as new media for spreading malware. Phishing activities that use OneNote documents to spread malicious files have increased since the end of 2022. Currently, multiple malware families are using OneNote documents for their distribution activities, including Snake Keylogger, AsyncRAT, QBot, Emotet, IcedID, Formbook, RedLineStealer, and AgentTesla. Attackers usually insert a blurry or relevant image to the phishing email's subject in the OneNote document, luring users to double-click a specified part of the image to view it. They can embed various types of malicious files in the document and hide multiple identical malicious files beneath the image to ensure that when users double-click the specified part of the image, they can click on any of the malicious files. If users ignore the risk warning and continue to execute, the malicious file will proceed with the subsequent attack process.

The Snake Keylogger spyware emerged at the end of 2020 and is a malicious software developed using .NET. This spyware can perform keylogging, take screenshots, obtain clipboard content, steal usernames and passwords saved in target applications, and has multiple data transmission methods on the victim's host. The spyware implements malicious behaviors such as hiding, persisting, collecting, and monitoring in the infected system, thereby transmitting sensitive data as required by the attacker, causing serious consequences such as income loss and reputation damage to users. Attackers can also use the data stolen from users to carry out subsequent attack activities.

It has been verified that the Antiy IEP (Intelligent Endpoint Protection System) can prevent OneNote from running malicious executables and effectively detect and remove this spyware.

# 2 ATT&CK Mapping graph of the event

For the complete process of the attackers' delivery of the spyware, Antiy has compiled the corresponding ATT&CK mapping graph for this attack incident as shown in the following figure.

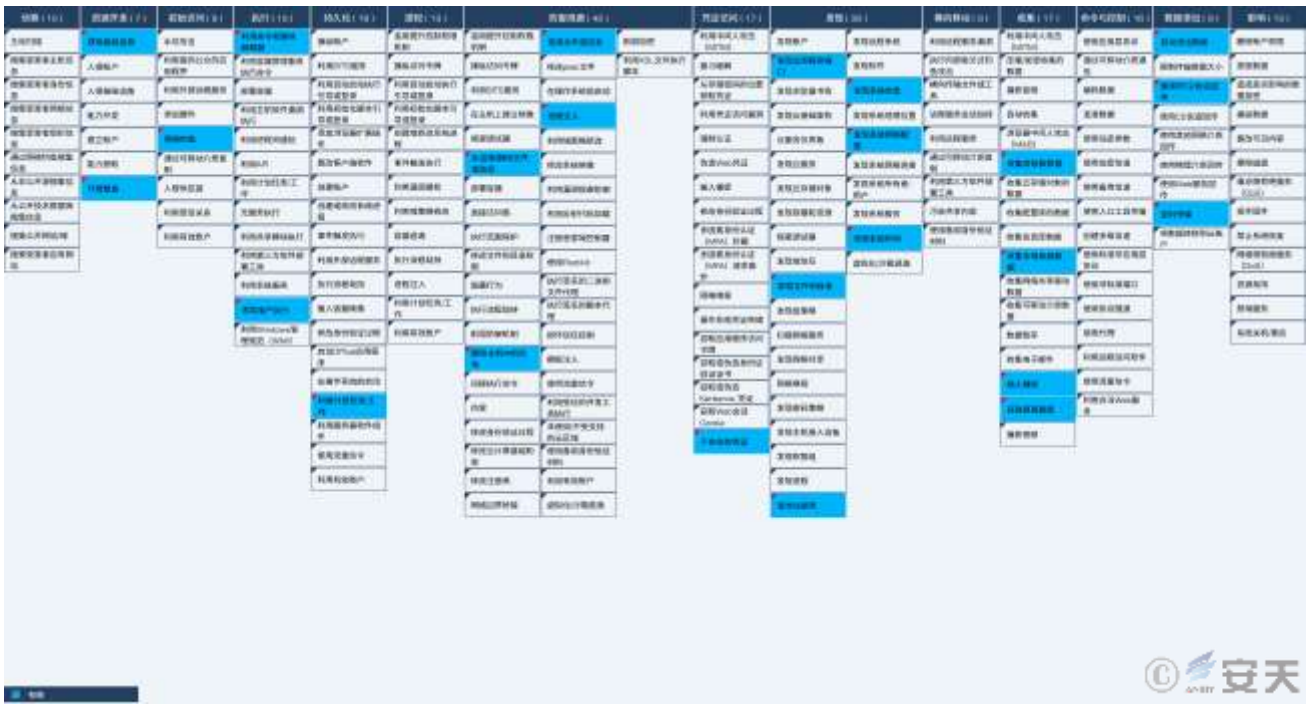

Figure 2-1 Mapping of Technical Features to ATT&CK 21

The technology points used by the attacker are shown in the table below.

Table 2-1 Technology points used by the attacker 2

| ATT&CK stages / categories | Specific behavior | Notes |
|---|---|---|
| Resource development | Access to infrastructure | Get the data back to the server |
| | Environmental preparation | Store malicious files in a file hosting site |
| Initial access | Phishing | Spread by phishing mail |
| Execution | Using command and script interpreters | Execute VBS script, PowerShell command |
| | Inducing the user to execute | Inducing a user to execute a malicious file |
| Persistence | Utilization of planned tasks / jobs | Create a scheduled task for persistence |

| | | |
|---|---|---|
| **Defensive evasion** | Anti-obfuscate / decode files or information | Decoding multi-layer payload information |
| | Remove the beacon from the host | Delete the XML file used to create the scheduled task |
| | Confusion of documents or information | Encrypt multi-layer payload information |
| | Process injection | Inject the final payload of the Trojan horse |
| **Credential Access** | Insecure credentials | Get unsecure application software, registry of credentials |
| **Findings** | Discover the application window | Gets window information for keyloggers |
| | Find files and directories | Application software is found in the specified directory |
| | Query the registry | Query the registry to obtain the application software information |
| | Discovery of system information | Discovery of system information |
| | Discovery system network configuration | Discovery system network configuration |
| | System discovery time | System discovery time |
| **Collection** | Collect clipboard data | Collect clipboard data |
| | Collect local system data | Collect local system data |
| | Input capture | Keylogger |
| | Get a screenshot | Get a screenshot |
| **Data seeps out** | Automatically seeps out data | Automatically seeps out stolen data |
| | Use non-c2 protocol to send back | Return data via FTP, SMTP and Telegram |
| | Timed transmission | Regular return of data |

# 3 Recommendations for protection

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

## 3.1 Identify phishing mail

1. Check mail senders: Watch out for non-organizational senders who send "business mail";
2. Check the addressee's address: Be alert to group email, and contact the sender for confirmation;
3. See the delivery time: Watch out for the non-working time sent mail;

4. Read the email title: Watch out for emails with the title of "order," "bill," "wage subsidy," "purchase" and other keywords;

5. See the wording of the text: Alert to "pro," "dear users," "dear colleagues" and other more general greetings of the mail;

6. Purpose of reading the text: Be alert to the emails that ask for the account password in the name of "system upgrade," "system maintenance" and "security setting";

7. Look at the main content: Alert to the attached web links, especially short links;

8. Content of the attachment: Before viewing, virus scanning and monitoring of the attachment shall be performed using anti-virus software.

## 3.2 Daily Email security usage protection

1. Install terminal protection software: Install terminal protection software, open the function of scanning and detecting email attachments in the protection software, regularly conduct security detection on the system, and repair system vulnerabilities.

2. Email login password: The email login password shall be set with certain complexity (including three character elements), the password shall not be recorded in an obvious place in the office area, and the login password shall be changed regularly.

3. Email account shall be bound with mobile phone: After the email account is bound with mobile phone, the user can not only retrieve the password, but also receive the SMS prompt of "abnormal login" for instant disposal.

4. Important documents shall be protected:

    1) Empty the inbox, outbox and trash of important mails that are no longer in use in time;

    2) Backup important files to prevent files from being lost after being attacked;

    3) Important emails or attachments shall be encrypted and sent, and no decryption password shall be attached to the text.

5. Sensitive information shall be protected: Do not release sensitive information on the Internet, and the information and data released by users on the Internet will be collected by attackers. By analyzing this information and data, attackers can send phishing emails to users in a targeted way.

## 3.3 Government, enterprise and institutional protection

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

2. Strengthen password strength: Avoid using weak passwords, and 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, 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;

4. Security service: In case of malware attack, it is suggested to isolate the attacked host in time, and protect the site and wait for the security engineer to check the computer; 7 * 24 service hotline: 400-840-9234.

**It has been proved that Antiy IEP can prevent OneNote from running malicious executors, and can effectively detect and kill the secret Trojan.**

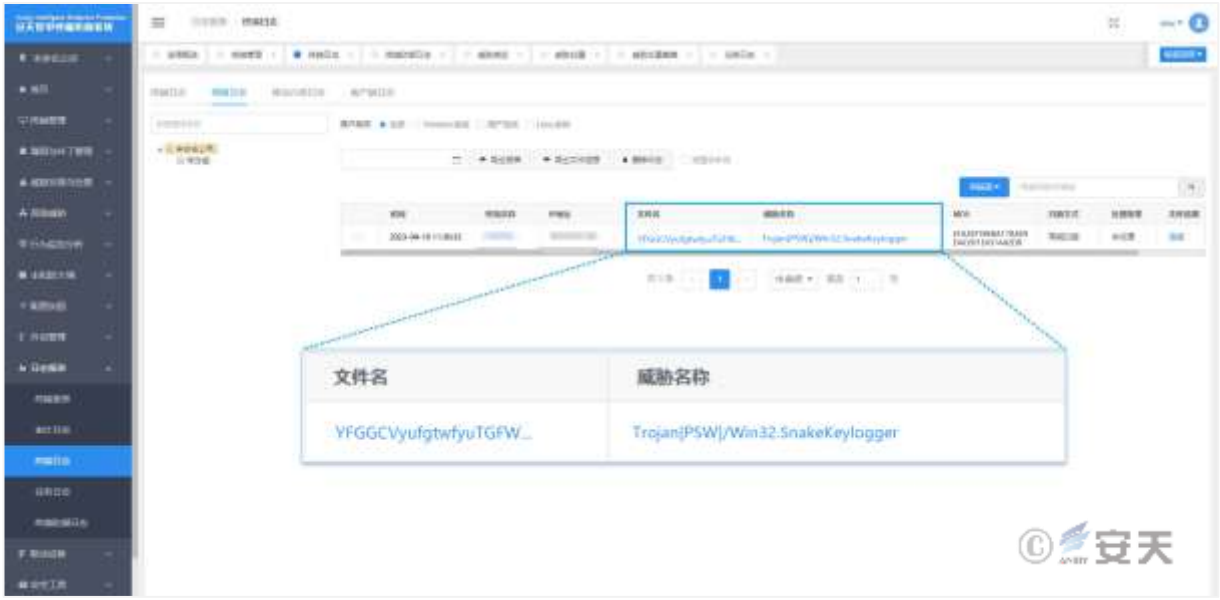


**Figure 3-1 The effective protection against the user system implemented by Antiy IEP1**

# 4 Attack process

## 4.1 Attack flowchart

The attacker drops a phishing email, induces the user to open the attached OneNote document, execute the ee.vbs script file hidden under the picture in the OneNote document, and download the eme.ps1 script from the file hosting website after the execution of the ee.vbs script. The PowerShell script releases and executes an executable program; after the executable program runs, it releases and loads multiple DLL files, and finally injects Snake Keylogger into the created child process to run. The Snake Keylogger has such functions as keyboard recording, screen capture, obtaining clipboard content, stealing user name and password of target application software, and has three data return modes as FTP return, SMTP return and Telegram return.

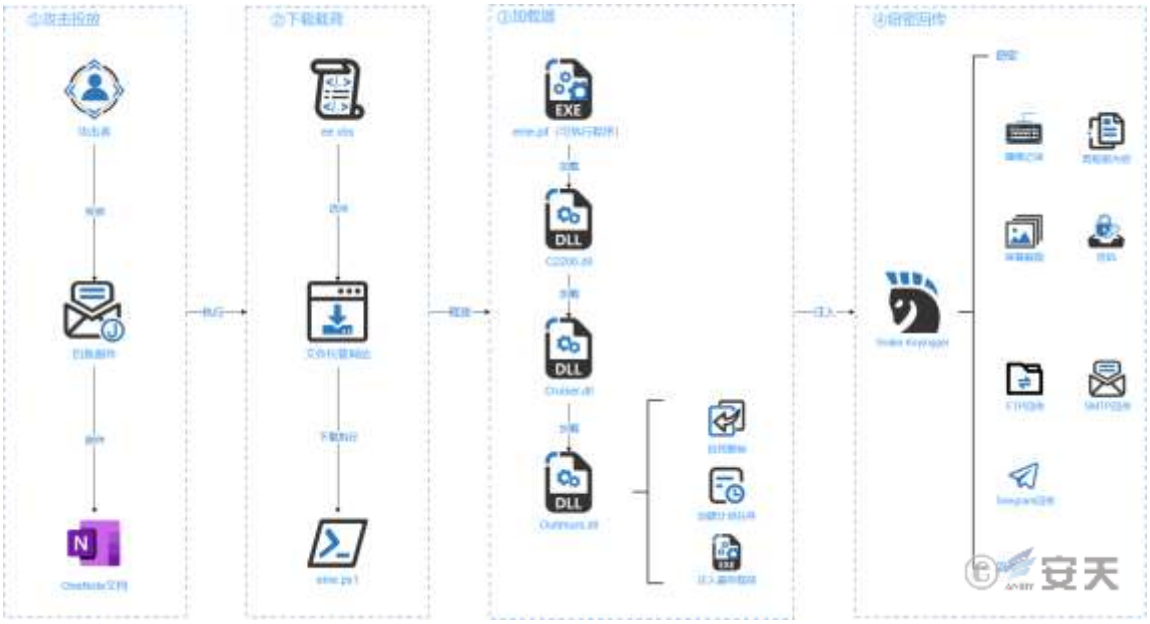


Figure 4-1 Attack flowchart 1

## 4.2 Using OneNote documents to spread malicious files

The attacker inserts a blurry image into the OneNote document, inducing the user to double-click the specified location to view it.


Figure 4-2: Onenote Document Page

Below the original text "Double click here to view", there are 3 ee.vbs files hidden. When the user clicks on this area, they will be able to select any of the script files. If the user ignores the risk warning and continues to execute, the script files will proceed with the subsequent attack process. The detailed attack process can be found in the "Sample Analysis" section of Chapter 5.


Figure 4-3 Malicious script hiding under the picture 2

# 5 Sample analysis

## 5.1 Sample labels

Table 5-1 Sample labels 1

| | |
|---|---|
| Name of malware | Trojan [PSW] / Win32.SnakeKeylogger |
| Original file name | Yfgcvyuffgtwfyutgfwtvfauyvf.exe |
| Md5 | Efa3ef59eba11bae9d4c691e431a42db |
| Processor architecture | Intel 386 or later, and compatibles |
| File size | 127.50kb (130,560 bytes) |
| File format | Binexecute / Microsoft.EXE [: X86] |

| | |
|---|---|
| **Time stamp** | 2022-11-11 13: 29: 43 |
| **Digital signature** | None |
| **Shell type** | None |
| **Compiled Language** | .net |
| **Vt First Upload Time** | 2023-04-10 09: 22: 01 |
| **Vt test result** | 58 / 70 |

## 5.2 Ee.vbs

After the VBS script is executed, download the PowerShell script pre-hosted by the attacker from the file hosting site to the specified path, and execute the script file.


**Figure 5-1 VBS script 1**

## 5.3 Eme.ps1

After the PowerShell script executes, it performs Base64 decoding on the string, saving the decoded content in the directory "C:\ Users\ Public" and naming it "eme.pif," which is an executable program written with. net.

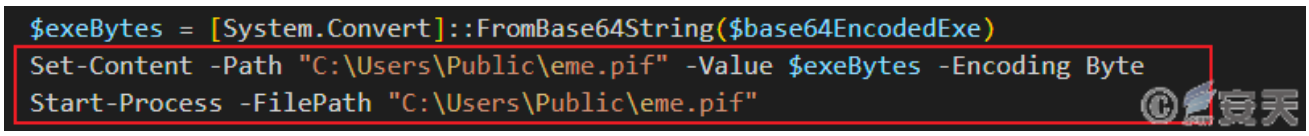


**Figure 5-2 PowerShell script2**

## 5.4 Eme.pif

After the executable program is run, the C2200 .dll file is obtained by obtaining the resource of the specified name, and the function specified in the DLL file is called.

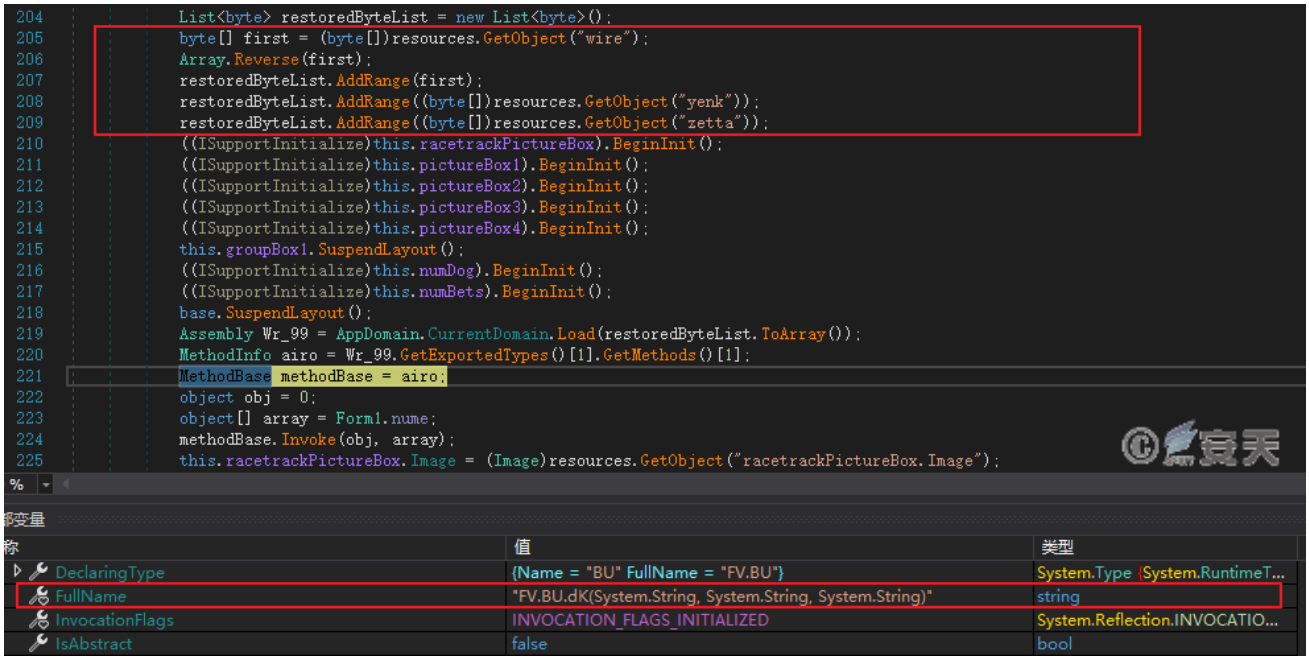


**Figure 5-3 Get the first stage DLL file and call the specified function 3**

Load the C2200 .dll file, sleep for 40 seconds, and then perform designated character substitution and Base64 decoding on the hard-coded string to obtain the Cruiser.dll file; load the Cruiser.dll file and decode to obtain two key strings. According to the string "UfVJ" to obtain the image resources in the eme. pif program, and according to the string "prh" to decode the image resources, to obtain the Outimurs. dll file.

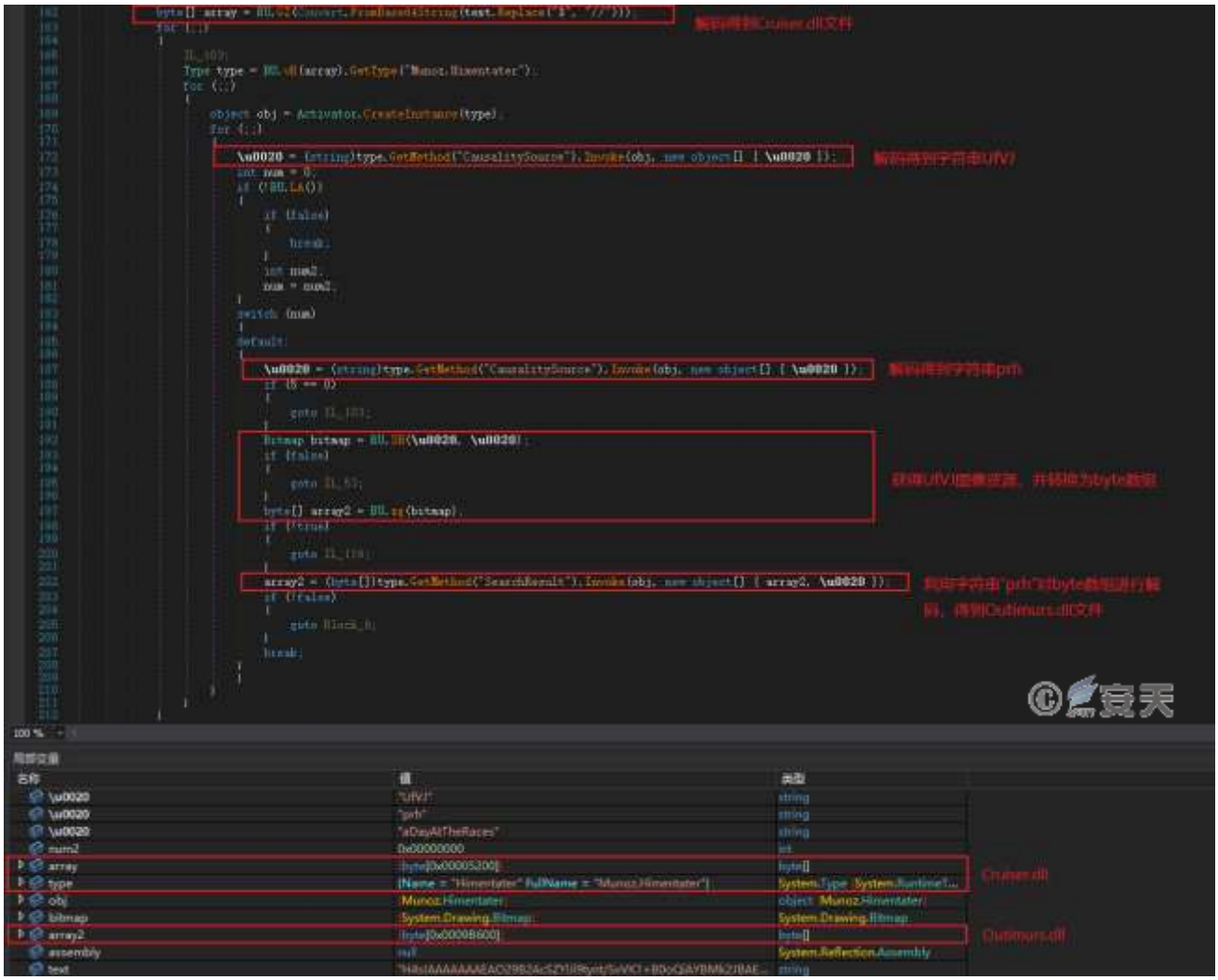

Figure 5-4 Get the Outimurs. dll file 4

Loads the Outimurs. dll file and calls the specified function in the DLL file.

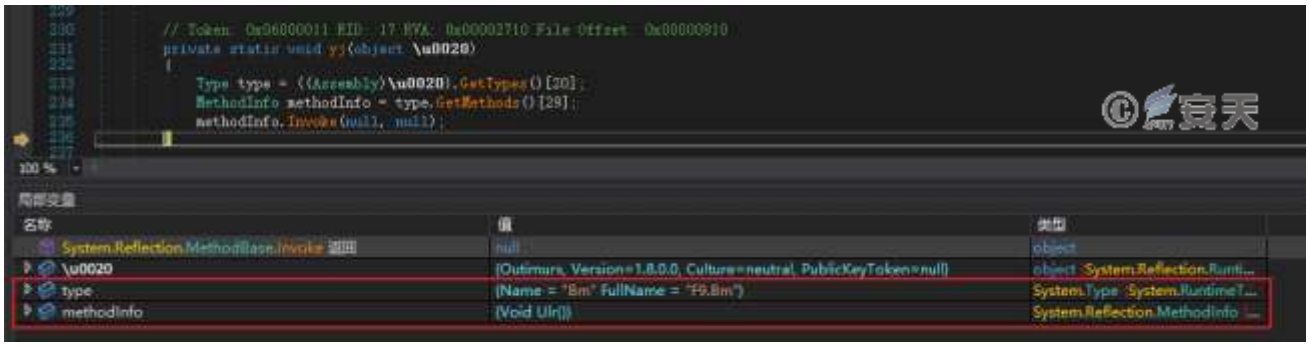

Figure 5-5 Calling the Outimurs. dll file to specify a function5

## 5.5 Outimurs.dll

The Outimurs. dll file performs three main functions: Self-replication, creating scheduled tasks, and injecting the final payload.

### 5.5.1 Self-replication

Copies its own program to the new path and renames the program.

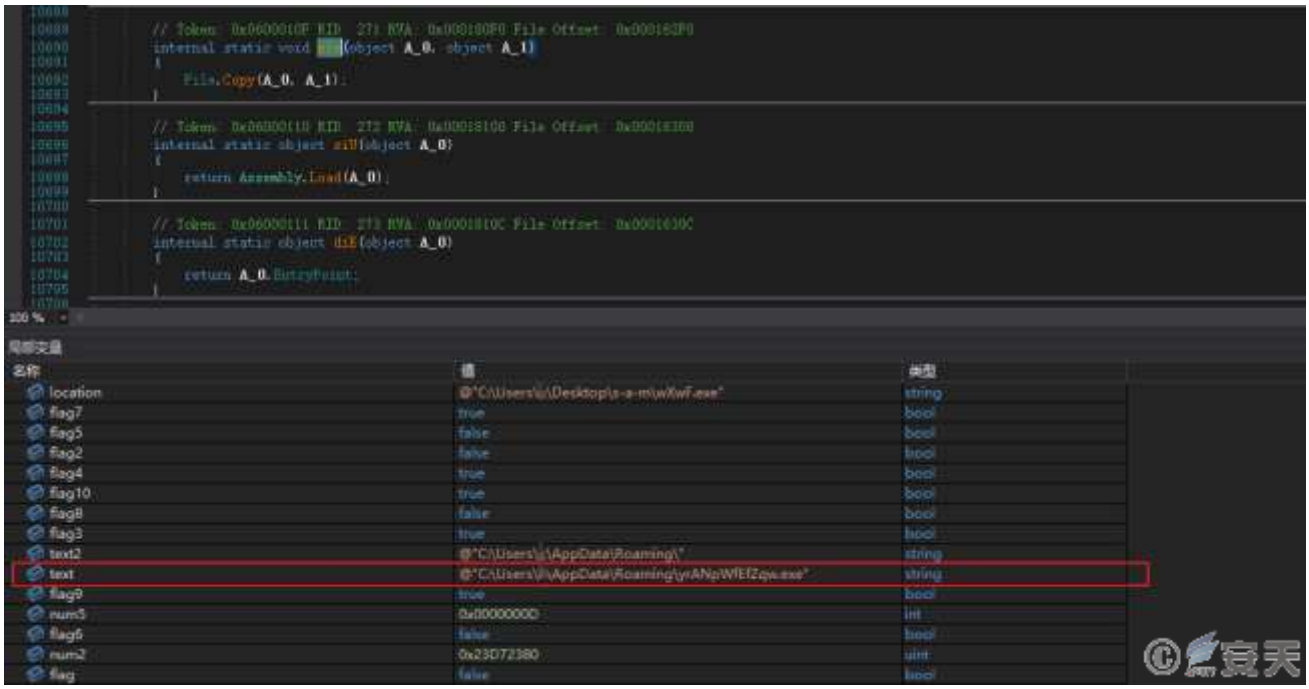


**Figure 5-6 Copy the self program to the new path6**

### 5.5.2 Create a scheduled task

Release the XML file to the% temp% directory from which the scheduled task is created.

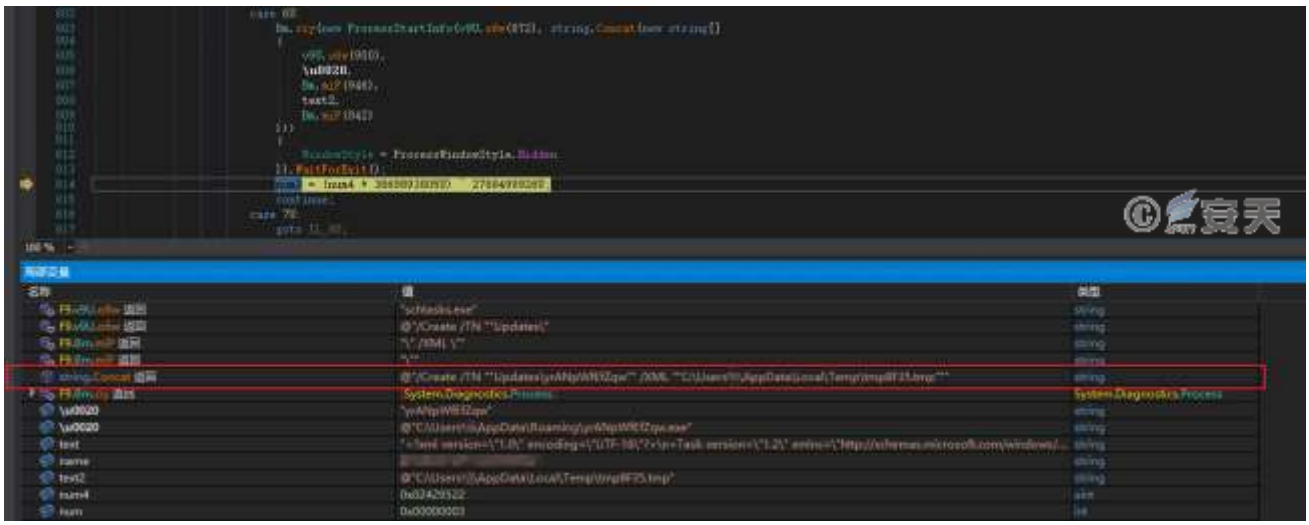

Figure 5-7 Create a scheduled task using an XML file 7

After the scheduled task is created, the XML file is deleted.

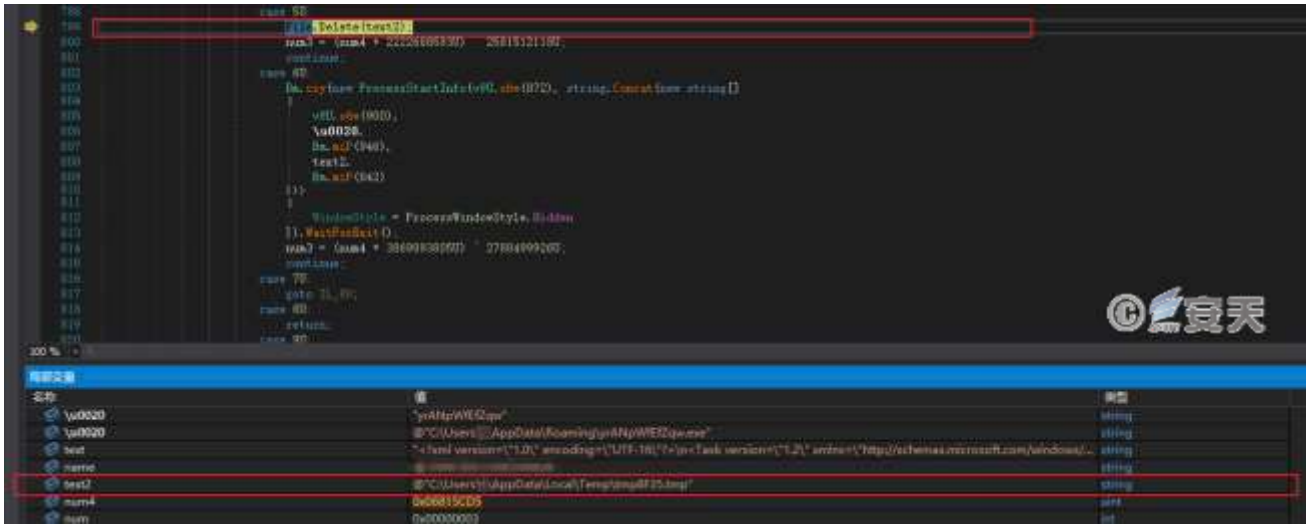

Figure 5-8 Delete an XML file 8

### 5.5.3 Injection final load

Obtaining the specified resource, and decoding the resource to obtain the final payload. Create a child process and inject the Snake Keylogger stolen Trojan horse obtained by decoding into the child process to run.

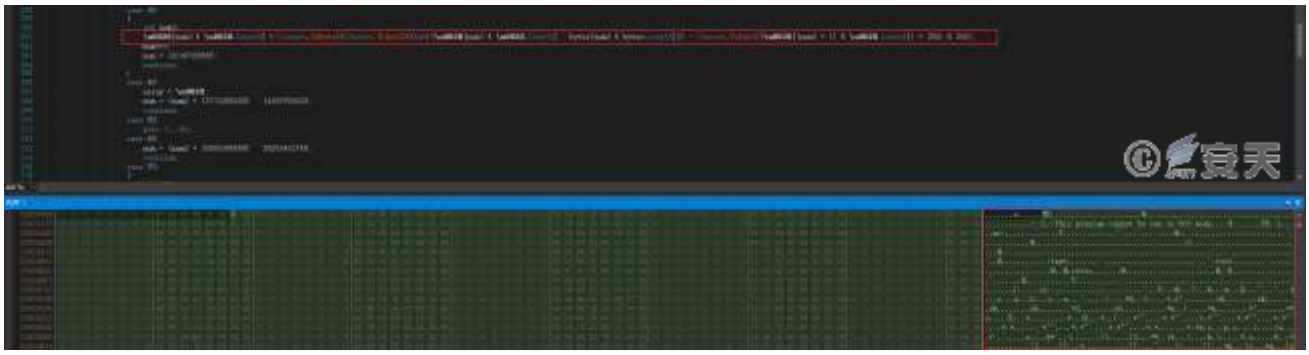

Figure 5-9 Decoding to obtain the final payload 9

## 5.6 Snake Keylogger's secret Trojan

The Snake Keylogger Trojan has the functions of stealing secrets such as keyboard recording, screen capture, obtaining clipboard contents and stealing user name and password of target application software, and has three return modes: Ftp return, SMTP return and Telegram return.

### 5.6.1 Keylogger

Monitor the keyboard input events, obtain the window information currently used by the user, and return the keyboard record and the window information to the C2 server.


Figure 5-10 Keyboard Record10

### 5.6.2 Screen Shot

Save the screenshot to the "My Files\ SnakeKeylogger" folder, named as Screenshot. png, return it to the C2 server, and then delete the screenshot file.

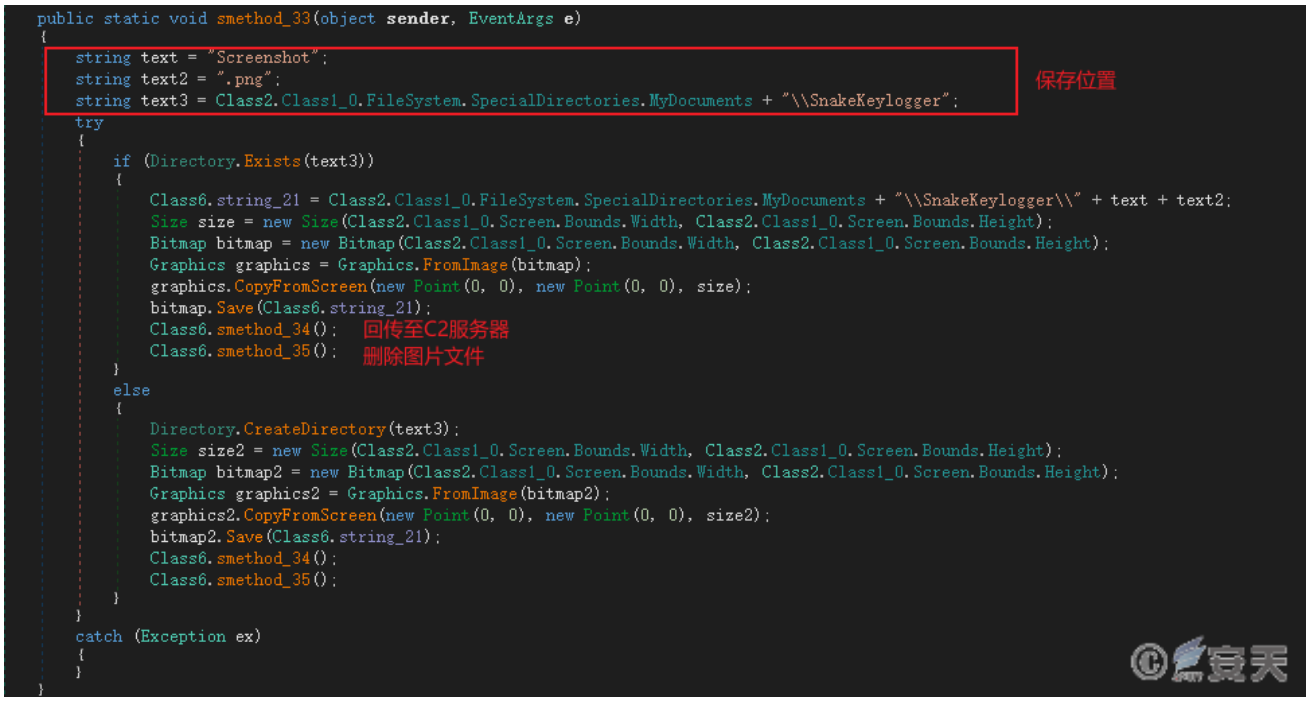


Figure 5-11 Screen capture 11

### 5.6.3 Gets the contents of the clipboard

Gets the contents of the system clipboard and returns them to the C2 server.

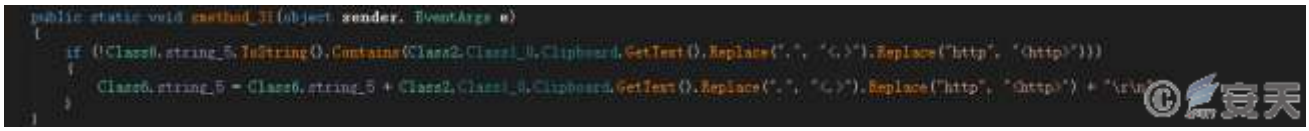

Figure 5-12 Obtaining the contents of the clipboard 12

### 5.6.4 Target theft

The Snake Keylogger Trojan horse steals the user name, password and other information stored in email box clients, browsers, instant messaging platforms, FTP tools and other application software. the specific objectives are shown in the table below.

Table 5-2 Application software theft targets 5-2

| | | | | |
|---|---|---|---|---|
| **Email client** | Outlook | Foxmail | Thunderbird | Postbox |
| **Browser** | Yandex | Amigo | Xpom | Kometa |
| | Nicchrome | Chrome | Coccoc | Qqbrowser |

| | | | | |
|---|---|---|---|---|
| | Orbitum | Slimjet | Iridium | Vivaldi |
| | Iron | Chromium | Ghostbrowser | Centbrowser |
| | Xvast | Chedot | Superbird | 360browser |
| | 360chrome | Comodo | Brave | Torch |
| | Ucbrowser | Blisk | Epic Privacy Browser | Opera |
| | Liebao7 | Avast Browser | Kinza | Blackhawk |
| | Citrio | Uran | Coon | 7star |
| | Qip Surf | Sleipnir | Chrome Canary | Coolnovo |
| | Salamweb | Sputnik | Falkon | Elements Browser |
| | Microsoft Edge | Icecat | Slimbrowser | Firefox |
| | Seamonkey | Ice Dragon | Cyberfox | Palemoon |
| | Waterfox | | | |
| **Instant messaging platform** | Pidgin | Discord | | |
| **Ftp tool** | Filezilla | | | |

### 5.6.5 Return mode

The Snake Keylogger Trojan horse selects whether to encrypt the return message according to the configuration information at the time of construction.

```
public static void smethod_71()
{
    if (Operators.ConditionalCompareObjectEqual(Class6.object_3, "ProtectTrue", false))
    {
        if (Operators.CompareString(Class6.string_0, "", false) != 0)
        {
            Class6.smethod_48();   加密信息后进行回传
            Thread.Sleep(8000);
            Class6.smethod_76();
            Thread.Sleep(3000);
            Class6.smethod_73();
            Thread.Sleep(3000);
            Class6.smethod_74();
            Thread.Sleep(3000);
            Class6.smethod_75();
        }
    }
    else if (Operators.CompareString(Class6.string_0, "", false) != 0)
    {
        Class6.smethod_51();      不加密回传信息
        Thread.Sleep(8000);
        Class6.smethod_77();
        Thread.Sleep(3000);
        Class6.smethod_73();
        Thread.Sleep(3000);
        Class6.smethod_74();
        Thread.Sleep(3000);
        Class6.smethod_75();
    }
}
```

**Figure 5-13 Select whether to encrypt the backhaul information according to the configuration 13**

If the transmission information is encrypted during construction, DES algorithm is used to encrypt the information, and Base64 encoding processing is performed on the encrypted data.

```
public static string smethod_14(string string_22, string string_23)
{
    DESCryptoServiceProvider descryptoServiceProvider = new DESCryptoServiceProvider();
    MD5CryptoServiceProvider md5CryptoServiceProvider = new MD5CryptoServiceProvider();
    byte[] array = new byte[8];
    Array.Copy(md5CryptoServiceProvider.ComputeHash(Encoding.ASCII.GetBytes(string_23)), 0, array, 0, 8);
    descryptoServiceProvider.Key = array;
    descryptoServiceProvider.Mode = CipherMode.ECB;
    ICryptoTransform cryptoTransform = descryptoServiceProvider.CreateEncryptor();
    byte[] bytes = Encoding.ASCII.GetBytes(string_22);
    return Convert.ToBase64String(cryptoTransform.TransformFinalBlock(bytes, 0, bytes.Length));
}
```

**Figure 5-14 Encrypted messages 14**

The Snake Keylogger Trojan horse has three backtracking modes: Ftp backtracking, SMTP backtracking and Telegram backtracking, and the specific backtracking mode is selected according to the configuration information during construction.

```
private static string string_3;

// Token: 0x04000018 RID: 24
private static string string_4 = "$%TelegramDv$";

// Token: 0x04000019 RID: 25
public static string string_5 = "";
```

**Figure 5-15 The return mode of the sample selection 15**

#### 5.6.5.1 Return via FTP

If the information is returned through FTP, the system will connect with the FTP server of the attacker, and return the file storing the stolen data to the server by using the STOR command.

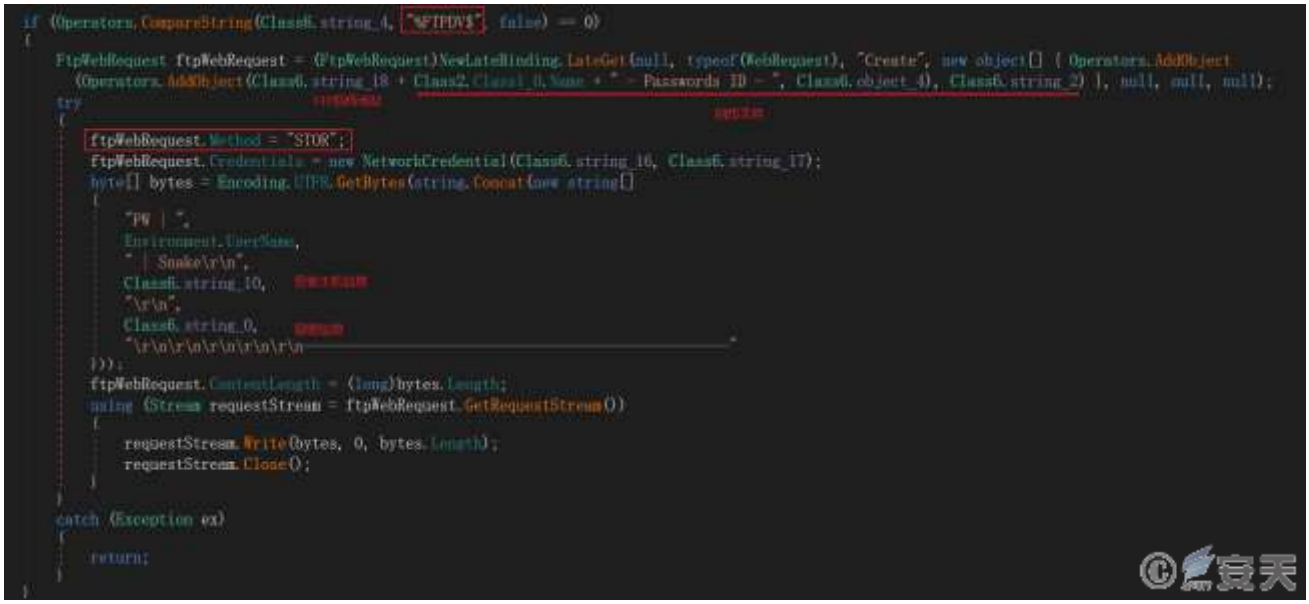


Figure 5-16 Falling Back Through FTP 16

According to the different information stolen, the return file is different, as shown in the following table.

Table 5-3 FTP Return File 3

| Theft of information | Return file |
|---|---|
| User name and password | < Device Name > - Passwords ID - < Identification ID > .txt |
| Keylogger | Device Name - Keystroke Logs ID - < ID > .txt |
| Clipboard contents | Device Name > - Clipboard Logs ID - < ID > .txt |
| Screen Shot | < Device Name > -Screenshot Logs ID - < ID > .png |

#### 5.6.5.2 Return via SMTP

If that message is sent back through SMTP, a return mail is sent to a malicious email address, and the attachment of the mail is a file save the stolen data.

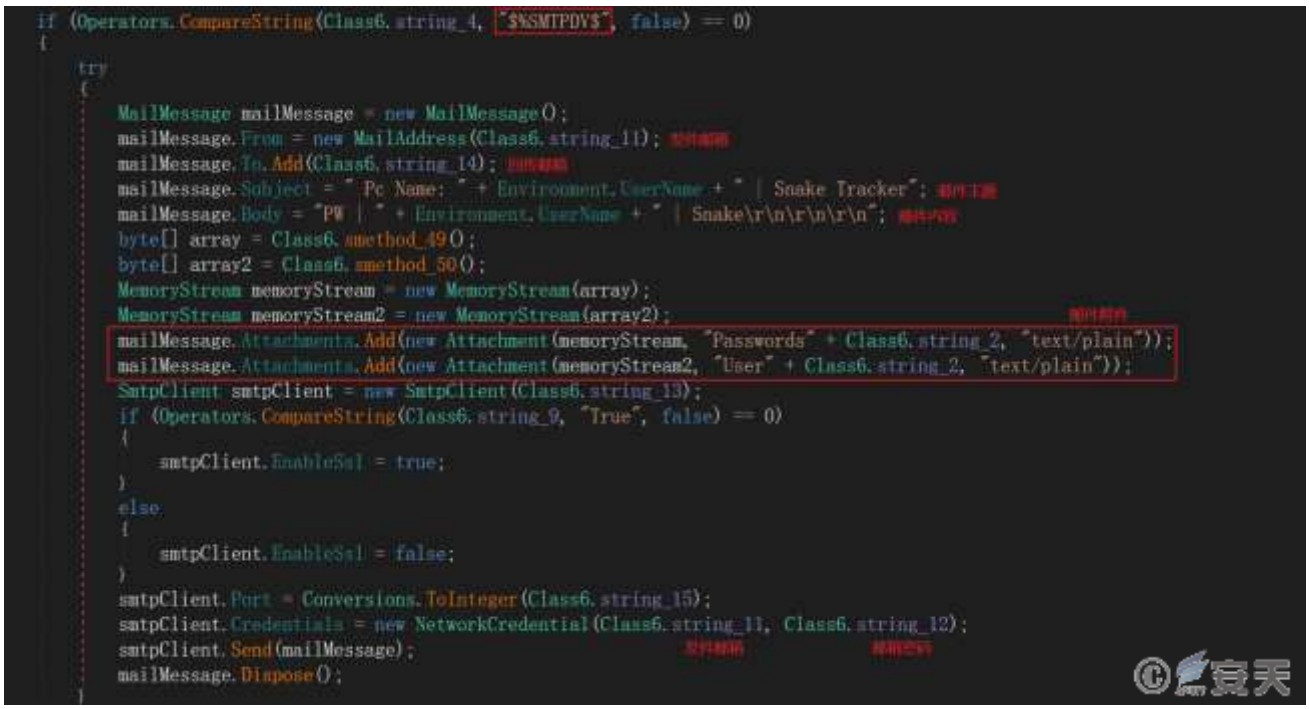


**Figure 5-17 Return by SMTP**

According to the different information stolen, the contents and attachments of their emails are different, as shown in the following table.

**Table 5-4 SMTP Return Messages**

| Theft of information | Content of Email | Attachment to Email |
|---|---|---|
| User name and password | Pw? User name? Snake | Passwords.txt, User.txt |
| Keylogger | Kp user name "Snake | Keystrokes.txt |
| Clipboard contents | Clipboard user name "Snake\ r\ n Relevant information of victim host | Clipboard.txt |
| Screen Shot | Screenshot user name "Snake\ r\ n Related information of the victim host | Screenshot.png |

#### 5.6.5.3 Return via Telegram

This sample sends back information through Telegram, and submits the file storing the stolen data to the Telegram server created by the attacker in the form of POST.

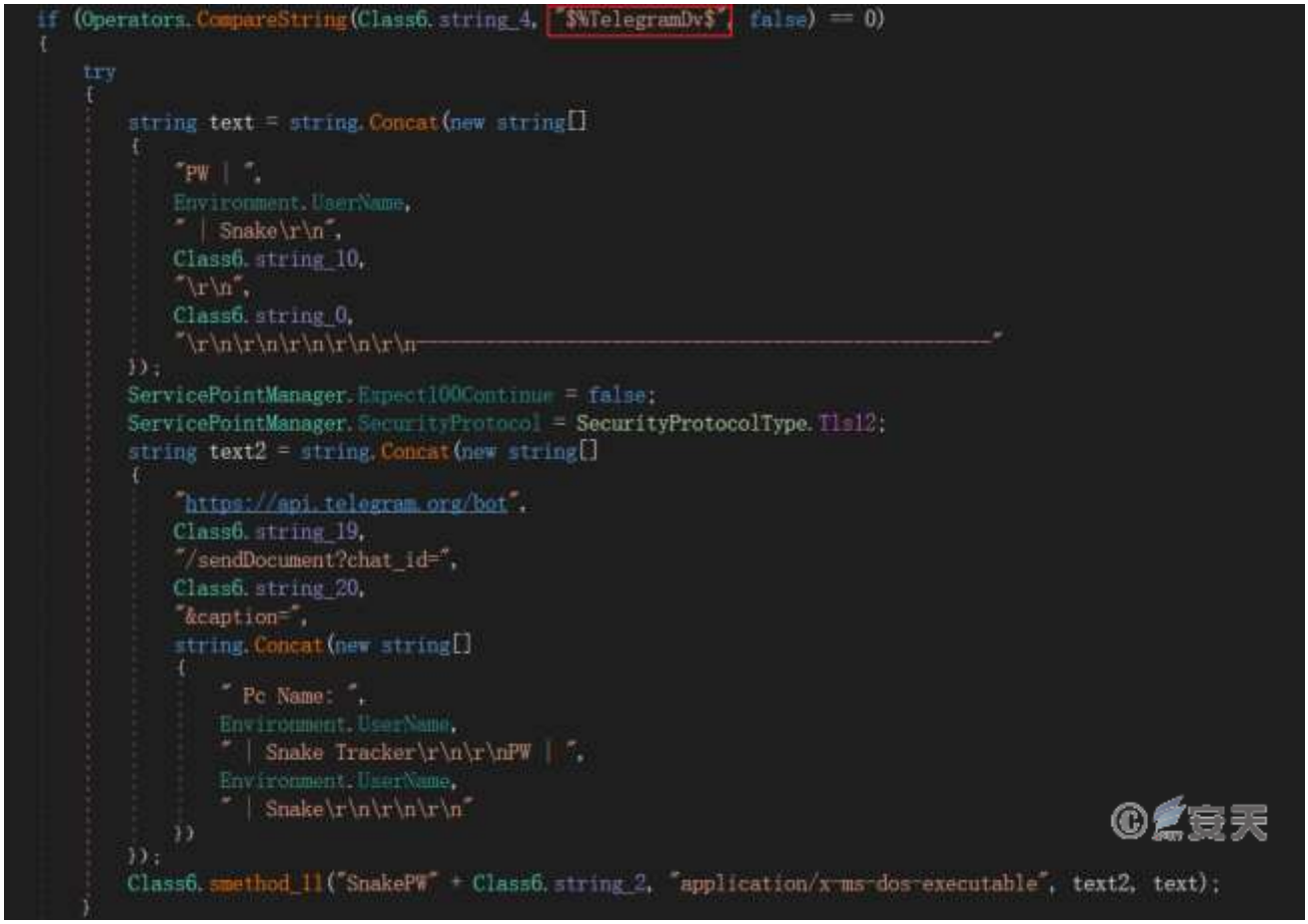


**Figure 5-18 Returned via Telegram 17**

According to the different information stolen, the return file is different, as shown in the following table.

**Table 5-5 Telegram Return File**

| Theft of information | Return file |
|---|---|
| User name and password | Snakepw .txt |
| Keylogger | Snakekeylogger .txt |
| Clipboard contents | Clipboard.txt |
| Screen Shot | Screenshot.png |

# 6 Summary

Since Microsoft announced that macros in Office documents are blocked by default, attackers have switched to delivering malicious files, using OneNote documents as a new medium for distributing malicious files. The attacker sends a phishing email to the user, induces the user to open the OneNote document in the attachment, and

executes the malicious file hidden under the picture in the OneNote document, so as to run malicious software such as secret Trojan and remote control Trojanon the user host.

It is suggested that the user should not easily believe the contents in the unknown mail, confirm the source of the mail, and be alert to the guiding contents in the mail. Antiy CERT will continue to pay attention to the new attack methods of attackers, and conduct in-depth analysis and research on related attack activities.

## Appendix I: IoCs

| IoCs |
| --- |
| 554f1a13a1ed03aa6eca2cb81defc242 |
| 67463b588ae33879f50fd43185af8be6 |
| B9611fdaa214df556ad6c8fc582a45f6 |
| 8481fb36fe2375802264e3255c421629 |
| 8d369299a047f228593293887092e43d |
| 0fb6061f7d37424fb9e6d0e76b019c19 |
| D7a88c5383f2c5f5f63eba55aa264c6f16 |
| Efa3ef59eba11bae9d4c691e431a42db |
| Https [:] / / bitbucket.org /! Api / 2.0 / snippets / mounmeinlilo / zqz9zj / a0908238e134ad5a36922c163d2c986a8584d33a / files / emefamstartup.ps1 |
| Https [:] / api.telegraph.org / bot6287986251: Aagcsj3tazwv7scc7x0dmhgcs3euo4j9 _ Ww / sendMessage? Chat _ id = 6218388203 |

## 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.