Analysis of Attack Activities Using Spam to Spread Remote Control Trojans

Antiy CERT

First draft completed: February 10, 2023 First published: February 13, 2023 The original report is in Chinese, and this version is an AI-translated edition.

1 Overview

Recently, the Harbin Institute of Technology and Antiy Joint CERT Labs has monitored multiple attacks using spam to spread remote control Trojans. Attackers send emails with themes such as "order", "invoice", "receipt", etc., and combine the body of the email to induce users to click on phishing links, thereby downloading and executing malicious files. Phishing links are sharing links generated by attackers uploading bait compressed files named "order.rar", "electronic invoice.rar", etc. to file sharing platforms. This method can achieve the effect of reducing their own operating costs, avoiding tracing, and bypassing whitelists.

The decoy compressed package contains three files, of which the .data file and the .exe file have the same name, usually "order" and "electronic invoice", and the file named "cl32.dll" is the core malicious file. The attacker uses the running mechanism of white and black to induce the target to execute the exe file to load the dll file. After running, cl32.dll decrypts and executes the core malicious dll in the memory to connect to C2 and download the communication module. The communication module is named "client.dll". After correlation and source tracing analysis, it is confirmed that the dll file is a "communication transmission framework" shared on a forum, which can realize multi-protocol communication.

From the sample analysis, the sample is written in Easy Language. Based on the existing analysis results, it is confirmed that the sample has the process and network behavior characteristics of a remote control Trojan and has some malicious functions. Based on the characteristics of the relevant malicious samples and the sharing content of the communication module source forum, the researchers speculate that this attack activity is the attacker's malicious use of tools and technologies shared on a forum to construct a remote control Trojan and spread it through spam. Comprehensive sample analysis and tracing results, combined with the attacker's use of technology and malicious intentions, researchers believe that once the user executes the remote control Trojan spread by spam in this attack activity, the user's terminal will face remote control risks and data leakage risks.

2 ATT&CK Mapping of This Attack Activity

The distribution diagram of technical features corresponding to this attack activity:

- International States	BRAND	CHINESE COLORS	MINTER .	MARCHINE.	SCHOOL STREET, ST		MANADIANI		MADOUTT		- 10 1201		. ARITY .	011080-001	HEREIT	- Birtha think
2.040R	-	****	NO.O VALUE	inter-	2.000×119.00.20	AND VALUE		ettan.	NEWSIARS Intitui	858.*	BRUNDA.	HAIDSTAT	REPRINES INTER	-		MUR-NY
Calavau a	2.987	AUGENLARD AND	REASERSA BOOKS	NUMBER	****	milaiten 1	#4/1021	HADING ARRIVE	BOME	NUMBER OF STREET	1000	8	Assesses Ba	******	unterestory.	ouns
建重型清清粉分2. ·	XXMAX	NATIONAL STREET		ADDRESS OF	HARBORN !!	Renau		(****	UNNUT UNTUR	annease.	-	*********	-	unns	A STREET	ARACENET BEE
	815F5	2587	NRIBER AND	Distantion in the local distance in the loca	10001900		REEA		torniistaa		anameters.			UANE .		
E CREWNERS	8182	MHTA	REPORT OF	Number An	R CONTRACT	HMAKS	nauses.	1	-	amenam	RECOMMENT	PENARMA.	ASSEMBLY R.S.	-	AMARMANN IN	RECEIVE
ALMANNARE .	atile -	sumares.	100.01	MARPHEN.		TAXABLES .	*****		neurite	20181	ADAMMAN	ALCO-LINE.	ARTINES	ensine	-	-
ABUTERS:	ouns	Autor	AMPHENT O	HOMP.	NORMER	1813	PREMISSION		41HE	816-14719	ANADAMA A	NARTHERN RIS	NENDBOOK.	HEARLS	attraction in the	Coll Coll
ALTERNES .		HUULAR	anisasi	COLUMNSAL!	ADDRESS OF	Rank	NUMBER		няяннале	annana	******	SARANSE	OREELANDE.	MRAILIANS	20194	arga
instrontiani		ettermin-	-	-	0000	httmap	ABSTRACTOR		ABRMINE WAY IN	NEED	BRANNIS	entented.	******	102101	COLUMNIC I	BARREN .
TTTAASUA			RANDONNA RAN	SHOULAN	STREET	SUPPORTS OF	agreed.		ADDING OF	REALING	0011488		URACOME	Manager,		Autorge .
			NAMES	REARING	19822	NRON .	NYCOLOGIC AND INCOME	ř	n heav	870.9403			REASONER DE	SECTION 2		1000
			analaran .	81.0898	MATSHAL	Access	AVIENTIMAL		and strains	330295			ARCONTER.	semurate		-
			REALBORNESS		nasion:	*****	AFLESS.	2	ARCHREN'S	remean				anna .	1	SHARES.
				COCH-UNK		******	AREA	13 I		agents.		48	***18*	BRURNESS.		
				THISSNEED		HRADES	******		ACCN CRAND	mees .	1		NAME	onvays	1	
				"NINITURAL		701	ANERSONAL RATE		Carrow R.S.	*****				######################################		
				n and a state of the state of t		#560HAUN	+66792R		Teenna	BREFRARE			-		t.	
				duages		13/1/25400	assistentia	2	veanne	10100						
				NR338/		*****	KIRCHAP			****						
						MALTINE		2		*****						

Figure 2-1 Mapping of technical features to ATT&CK

The specific ATT&CK technical behavior description is shown in Table 2-1.

ATT&CK Phase/Category	Specific Behavior	Notes					
Initial Access	Phishing	Sending spam emails to spread remote control Trojans					
Execute	Induce users to execute	Inducing users to execute in the name of "electronic invoice"					
Persistence	Booting or logging in with autostart	Create a shortcut to the system startup directory					
Defense Evasion	Obfuscating files or information	Encrypt dll files					
Discover	Discovery Process	Detection of protection software processes					
Discover	Discover system information	Detect system version and other information					

Table 2-1 ATT&CK technical behavior description table corresponding to the event



Use C2 channel for backhaul

Connect C 2 and transmit data back

3 Protection Recommendations

In response to this remote control Trojan, Antiy recommends that government agencies and enterprises take the following protective measures:

3.1 Identify Phishing Emails

- 1. View email senders: Be wary of non-organized senders who send "business mail";
- 2. View recipient address: Be wary of mass emails and contact the sender to confirm;
- 3. Check the delivery time: Be wary of emails sent outside of working hours;
- 4. View the email title: Be wary of emails with titles containing keywords such as "order", "invoice", "wage subsidy", "purchase", etc.
- View the text wording: Be wary of emails that begin with general greetings such as "Dear", "Dear User", "Dear Colleague", etc.
- View main text for purpose: Be wary of emails that ask for email account passwords in the name of "system upgrade", "system maintenance", "security settings", etc.
- 7. View the text content: Be wary of web links included in them, especially short links;
- 8. View the contents of attachments: Before viewing, you must use anti-virus software to scan the attachments for viruses.

3.2 Daily Mailbox Security Protection

- Install terminal protection software: Install terminal protection software, enable the scanning and detection function of email attachments in the protection software, perform security checks on the system regularly, and repair system vulnerabilities.
- Email login password: When setting the email login password, ensure that it has a certain degree of complexity (including three character elements), ensure that the password is not recorded in a conspicuous place in the office area, and modify the login password regularly.

- The email account must be bound to the mobile phone: After the email account is bound to the mobile phone, you can not only retrieve your password, but also receive SMS prompts of "abnormal login" and deal with it immediately.
- 4. Important files should be well protected:
 - a) important emails that are no longer used in your inbox, outbox, and trash in a timely manner;
 - b) loss after an attack;
 - c) important emails or attachments should be sent encrypted, and the decryption password should not be included in the body of the email.
- 5. Protect sensitive information: Do not post sensitive information on the Internet. Information and data posted by users on the Internet can be collected by attackers. Attackers can analyze this information and data and send targeted phishing emails to users.

3.3 Protection for Government and Enterprise Organizations

- Install terminal protection software: Install anti-virus software. It is recommended to install Antiy Intelligent Endpoint Protection System;
- Improve password strength: Avoid using weak passwords. It is recommended to use a password of 16 characters or longer, including a combination of uppercase and lowercase letters, numbers, and symbols. Avoid using the same password on multiple servers.
- 3. Deploy intrusion detection system (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracking of malicious code. Antiy Persistent Threat Detection System (PTD) uses network traffic as the detection and analysis object, and can accurately detect a large number of known malicious codes and network attack activities, and effectively discover suspicious network behaviors, assets and various unknown threats;
- Antiy Service: If you are attacked by malware, it is recommended to isolate the attacked host in time and protect the site while waiting for security engineers to check the computer; Antiy 7*24 hours service hotline: 400-840-9234.



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



Figure 3-1Antiy IEP achieves effective protection for users

4 Email Analysis

Spam mainly uses subjects such as "order", "invoice", "receipt" and so on to construct the email body and embed phishing links in it, which exist in an implicit way (that is, the displayed link is inconsistent with the actual link), showing that after the link is accessed, it is indeed an invoice file.

注意验查单据!	
A Real Property of the Propert	
发件人:	
收件人:	
时间: 2023年2月7日 (周二) 09:09	
大小: 4 KB https://drfs.ctcontents F	82/387ffd/025003000422_56184836.rar
尊敬的用户,您好:	实际链接
您的发票已成功出具,数量共计1张,如下:	○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○
下载地址: https://dlj.51fapia	1631198971e51f9fe3b35d248.pdf



Phishing links are mainly generated by document sharing platforms, such as "Kingsoft Documents", "NetEase Mailbox Master", "Lanzo Cloud Storage", etc. The bait compressed files are stored on multiple document sharing platforms, and corresponding links are generated. They are continuously sent to the target mailbox via spam emails, inducing the target to click and download the corresponding compressed files.

5 Sample Analysis

5.1 Analysis of the Decoy Compressed Package

The compressed package contains three files, namely "electronic invoice.exe", "electronic invoice.data", and " cl32.dll". Two of the executable programs have U PX shells. After analysis, it was verified that the files in the compressed package used the white-on-black technology to implement malicious code execution. The specific malicious file is cl32.dll.

🕌 ▶ 【电子-发票】												
包含到库中 ▼	共享 ▼ 新建文件夹											
E	名称	修改日期	类型	大小								
5	🛅 电子发票.exe	2012/12/9 0:03	应用程序	1,722 KB								
ī	📄 电子发票.data	2023/2/6 13:43	DATA 文件	1 KB								
访问的位置	🚳 cl32.dll	2023/1/9 9:36	应用程序扩展	⁶⁴¹ [®] ≦ 安天								

Figure 5-1Decoy compressed file

5.2 Analysis of cl32.dll

5.2.1 Sample Tags

Table 5-1cl32.dll sample tags

Malicious code name	Trojan/Win32.FlyStudio.a
Original file name	cl32.dll
MD5	297180F60A3E70896BBE17CCA0E9C501
Processor architecture	Intel 386 or later processors and compatible processors
File size	640.50 KB (655,872 字节)
File format	BinExecute/Microsoft.EXE[:X86]
Timestamp	2023-01-09 01:36:31



Analysis of Attack Activities Using Spam to Spread Remote Control Trojans

Digital signature	None						
Packer type	UPX						
Compiled language	Easy Language						
VT first upload time	2023-02-06 03:52:36						
VT test results	22 / 69						

5.2.2 Dynamically Decrypt and Load Dll

c 132.dll is loaded, it decrypts and loads another dll file in memory, which is named "DLL.dll" below.

DLL.dll:02EB87F0	;					
DLL.dll:02EB87F0	cmp	byte ptr	[esp+8],	1		
DLL.dl1:02EB87F5	jnz	loc_2EB93	DF			
DLL.dll:02EB87FB	pusha					
DLL.dll:02EB87FC	mov	esi, offs	et unk_2E	70000		
DLL.dll:02EB8801	lea	edi, [esi	-9F000h]			
DLL.dl1:02EB8807	push	edi				
DLL.dl1:02EB8808	mov	ebp, esp				
DLL.dl1:02EB880A	lea	ebx, [esp	-3E80h]			
DLL.dll:02EB8811	xor	eax, eax				
DLL.dll:02EB8813						
DLL.dll:02EB8813	loc_2EB8	8813:			; CODE XREF:DLL.d	11:
DLL.dll:02EB8813		eax				
DLL.dll:02EB8814						
DLL.dll:02EB8816	jnz	short loc	_2EB8813			
DLL.dll:02EB8818						
DLL.dll:02EB8819						
DLL.dll:02EB881A						
DLL.dll:02EB881B			k_E6B4A			
DLL.dll:02EB8820		edi				
DLL.dll:02EB8821		ebx, 4				
DLL.dll:02EB8824						
DLL.dll:02EB8825			k_487E2			
DLL.dll:02EB882A		esi				
DLL.dll:02EB882B		ebx, 4				
DLL.dl1:02EB882E		ebx			◎‴安天	
DLL.dll:02EB882F		eax				
DLL.dll:02EB8830		dword ptr	[ebx], 3			
DLL.dll:02EB8836	push	ebp				

Figure 5-2Decrypting and loading the dll

5.2.3 Download Communication Module

Decrypting and loading the DLL.dll, it reads the .data file in the current directory and decrypts it in memory.

The decrypted content is the C2 connection address and the communication module download address.





Figure 5-3Decryption of C2 and communication module download address configuration information

Connect the U RL download communication module.

push	80000004h
push	0
push	offset aWinhttpWinhttp ; "WinHttp.WinHttpRequest.5.1"
push	10030h
push	0
mov	ebx, [ebp+var_4]
push	dword ptr [ebx] ① <i>会</i> 天
push	3

Figure 5-4Download communication module

5.2.4 Process Behavior

After the communication module is downloaded, a child process is created with the newly copied exe file as the

carrier, and the own process is terminated.

	uojoulugione	2070	-	naorong bora (bogingin	naorong oyoalag ri
	SGTool.exe	3104	3104	Sogou.com Inc.	搜狗输入法 工具
E	🔲 电子发票.exe	1844	1844		
	K7497O839QD4LF3F65J877.e	3208	1844		
Ð	🕉 GoogleUpdate.exe	472	472	Google LLC	Google 安装程序
_	🐻 GoogleCrashHandler.exe	1576	472	Google LLC	Google Crash Hand

Figure 5-5Process behavior

5.2.5 Persistence

After the program is run, a shortcut will be created and copied to the startup directory to achieve persistent

operation.

				-
C:\Users\MA\	AppData\Roaming\Microsoft\V	Vindows\Start Menu\Programs\Startup		
🗹 💼 <mark>41P</mark> 97	9SGPS4960150T		c:\users\ma\appdata\local\temp\m105k\41p975	
🔽 🔲 电子发	支票. <mark>lnk</mark>		c:\users\ma\desktop\【电子发票】\电子发	鼎 exe
HKI M\SOFTV	WARE\Microsoft\Active Setup\	Installed Components		- with Sec 1





5.2.6 Connect C2 Address

After the communication module is downloaded successfully, it will connect to C2 and send an online packet.

43* 130	192.100 194.132	ICK	TOTA 0800 + 44X0X [MrV] 26d=X3T24X1 MCK=X31 MJU=04540 F6U=1400 [irs
43. 196	192. 4.132	TCP	1514 8080 - 49202 [ACK] Seg=2517381 Ack=251 Win=64240 Len=1460 [TCP
43. 196	192. 44.132	HTTP	393 HTTP/1.1 200 OK
192 4.132	43.1 196	TCP	54 49202 + 8080 [ACK] Seg-251 Ack-2519181 Win-64240 Len-0
192 4,132	43.1 196	TCP	5- 19282 - 8888 [FIN, ACK] Seq-251 Ack-2519181 Win-64248 Len-0
43. 196	192. 4.132	TCP	54 8888 49202 [ACK] Seq-2519181 Ack-252 Win-64239 Len-0
192 4.132	43.1 196	TCP	66 49203 - 12345 [SYN] Seq-@ WIN-8192 Len-@ MSS-1468 WS-256 SACK_
43. 196	192. 4.132	TCP	58 12345 + 49203 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192 4.132	43.1 196	TCP	54 49203 + 12345 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192 4.132	43.1 196	TCP	70 49203 + 12345 [PSH, ACK] Seq=1 Ack=1 Win=64248 Len=16
43. 196	192. 194.132	TCP	54 12345 + 49203 [ACK] Seq=1 Ack=17 Win=64240 Len=0
43. 196	192. 4.132	TCP	70 12345 + 49203 [PSH, ACK] Seq=1 Ack=17 Win 042 [cm 14]
192 4.132	43.1 196	TCP	444 49203 - 12345 [PSH, ACK] Seg=17 Ack=17 Win=64224 Len=390
73 196	197	TEP	5/ 131/5 + /9781 1ACK1 Spru17 Arks/07 Wins6/3/A LansA

Figure 5-7Connect C2

The encrypted information is then continuously sent.

									_		_			_	_	
00000170		1 e3														
00000180	af b	Ъ 82	d1	8c	a7	05	28	- 4 d	11	0f	6f	ed	ee	59	af	Ч.
00000190	50 f	ኬ 57	96	05	he											P. W
00000196	02 0	0 00	00	З£	00	00	00	- 32	$1 \mathrm{c}$	4e	83	30	$1\mathrm{c}$	4e	83	?
000001A6	aa 1	e 4e	83	6Ъ	a7	аŨ	35	- 98	ad	96	70	8Ъ	d5	2c	43	N.k5p,C
000001B6	56 e	a 86	bd	0a	94	23	OЪ	be	а5	43	dЗ	£7	70	57	16	V#СрW.
000001C6	d7 5	be4	Oď	83	Ъ£	04	a0	83	57	еŨ	90	41	71	al	8d	[
000001D6	73 e	Ъ 38	42	eb	25	c2										s. 8B. %.
000001DD	02 0	0 00	00	З£	00	00	00	- 31	19	17	82	33	19	17	82	
000001ED	a9 1	Ъ 17	82	68	a2	£9	34	6e	c4	ff	$d\mathbf{f}$	0a	d9	80	7£	h4 n
000001FD	d3 4	8 36	fЪ	c4	9£	45	e7	44	2e	fe	78	88	45	13	ea	.H6E. D, .x.E.
0000020D	ee 3	8 2£	9c	fe	c8	c6	8c	8a	c4	85	dЗ	83	4c	9d	6d	.8/L.m
0000021D	ef 9	a 43	еа	ae	5f	66										C
00000224	02/0	0 00	00	З£	00	00	00	- 34	15	$d\mathbf{f}$	81	36	15	$d\mathbf{f}$	81	
00000234	ac 1	7 df	81	6d	ae	31	37	- a3	72	e7	4e	8a	dd	£7	ab	m. 17 .r. N
00000244	6c a	e 66	31	86	86	7e	c2	ef	ab	16	86	9d	9a	dO	4e	1. f1. N
00000254	e5 9	9 76	2e	55	51	80	d8	-b2	Ъ5	a6	0e	de	ab	£9	c1	
00000264	4a 4	5 db	72	6c	71	ce										(JE.rlq
0000026B	02/0	0 00	00	З£	00	00	00	- 38	11	a7	81	3a	11	a7	81	Crigg F
0000027B	a0 1	3 a7	81	61	aa	49	37	£9	a9	10	Зď	0a	21	6Ъ	c7	
00000288	- AQ - O	a aa	64	40	89	97	ka.	77	32	AF	2£	aa	e.f.		23	

Figure 5-8Sending encrypted information

5.3 Analysis of client.dll

5.3.1 Sample Tags

Table 5-2client .dll sample tags

Malicious code name	Trojan/Win32.FlyStudio.a
Original file name	client.dll
MD5	77679E51504F2B94565B6E974D29FFFF
Processor architecture	Intel 386 or later processors and compatible processors
File size	2.40 MB (2,519,040 bytes)
File format	BinExecute /Microsoft.DLL[:X86]



Timestamp	2023-01-10 10:52:55
Digital signature	None
Packer type	None
Compiled language	Easy Language
VT first upload time	2023-01-16 15:36:15
VT test results	41 / 68

5.3.2 Communication Function

After analyzing the client.dll file, it was confirmed that the file was a communication transmission framework shared in a forum.

	1	00000047	-		
's'	.rdata:101DDCC5	0000001E	-	Kai	m_TCP_Client_GetState
's' 's'	.rdata:101DDCE3	0000002B		Kai	
's'	.rdata:101DDDOE	0000001A		Kai	in_WS_Server_Start
's'	.rdata:101DDD28	00000022		Kai	in_STCP_Server_GetOnAccept
's'	.rdata:101DDD4A	00000026		Kai	In_TCP_Server_GetKeepAliveTime
's'	.rdata:101DDD70	00000022		Kai	
ʻs' ʻs'	.rdata:101DDD92	0000002B	С	Kai	
's'	.rdata:101DDDBD	00000022	С	Kai	
's'	.rdata:101DDDDF	0000002B	С	Kai	n_STCP_Server_GetFreeSocketObjPool
ʻs'	.rdata:101DDEOA	00000024	С	Kai	
's'	.rdata:101DDE2E	00000025	С	Kai	
's'	.rdata:101DDE53	00000030	С	Kai	In_HTTP_Server_DisconnectLongConnections
's'	.rdata:101DDE83	00000021	С	Kai 💼	pn_BTCP_Server_Disconnect
's' 's'	.rdata:101DDEA4	00000029	С	Kai	m_HTTP_Server_SetConnectionExtra
's'	.rdata:101DFCB3	00000052	C (16 bits)	hti	vww. ka n. com/list-127-1. html
ʻs' ʻs'	.rdata:101DFD1F	00000052	C (16 bits)	hti	www.kal n.com/list-127-1.html
's'	.rdata:101E3AAB	000000E	С	Kai	n_Key
ʻs' ʻs'	.rdata:1022B072	0000001D	С	Kai	un_STCP_Client_Create
's'	.rdata:1022B08F	00000025	С	Kai 📃	
's'	.rdata:1022B0B4	0000001E	С	Kai 📰	In_STCP_Client_Destroy
's'	.rdata:1022B0D2	00000022	С	Kai	n_STCP_Client_SetSafeCode
ʻs' ʻs'	.rdata:1022B0F4	00000022	С	Kai	n_STCP_Client_GetSafeCode
's'	.rdata:1022B116	0000001F	С	Kai	un_STCP_Client_SetExtra
's'	.rdata:1022B135	0000001F	С	Kai	n_STCP_Client_GetExtra
's' 's' 's'	.rdata:1022B154	0000001E	С	Kai	n_STCP_Client_Connect
's'	.rdata:1022B172	0000001B	С	Kai	un_STCP_Client_Stop
's'	.rdata:1022B18D	00000021	С	Kai	n_STCP_Client_HasStarted 👝 🚄 🛖
's'	.rdata:1022B1AE	0000002A	С	Kai	n_STCP_Client_SetSocketBufferSize 🦟
6 ₁₀ 3	rdoto:10228178	0000028		Kai	In STEP Cliant GatSnebatBuffarSiza



5.3.3 Terminal Protection Process Detection

The communication module also comes with a detection function for the core process of the target host terminal protection software.



<pre>v61 - &unk_100D7482; lpMenk = (void *)sub 100552DB(1, (char)v61);</pre>	a360sdExe	db	'360sd.exe',0	74	DATA XREF: check_EDR_proc+D6%
v162 = (void *)sub_10055208(1, (char)*QQPCRTP.exe*);	a360rpsExe	db	'360rps.exe',0		<pre>check_EDR_proc2+D610 DATA_XREF: check_EDR_proc+1C91</pre>
v139 = sub_1000134A((int))pHemk, (int)v162) 0; 16 (lpHemk)	a360rpExe	db	'360rp.exe'.0		<pre>check_EDR_proc2+1CB1o DATA XREF: check EDR proc+2AD1</pre>
<pre>sub_100552C9(1pMemk); if (v162)</pre>	a360trayExe	-	'360Tray.exe'.0		check_EDR_proc2+2ACto DATA_XREF: check_EDR_proc+3811
<pre>sub_100552C9(v162); if (v139)</pre>	and the a		'ZhuDongFangYu.exe		check_EDR_proc2+3AFto
{ dword 1024F758 = 1;					DATA XREF: check_EDR_proc+4A41
) else	aHipsdaemonExe aUsysdiagExe	40	'usysdiag.exe',0		DATA XREF: check_EDR_proc+5971 DATA XREF: check_EDR_proc+68A1
{ v62 = v198;	aWsctrlsvcExe aHipstrayExe		'wsctrlsvc.exe',0 'HipsTray.exe',0		DATA XREF: check_EDR_proc+76E1 DATA XREF: check_EDR_proc+8721
sub_10002792(); v64 = v197 - 1;	aQmsignscanExe	db	'QMSignScan.exe',0		; check_EDR_proc2+4A1to ; DATA_XREF: check_EDR_proc+9651
if (v197 - 1 < 0) sub 100552CF(4, 67225901, (LPCSTR)0x8C0);	aQmdlExe	de	'QMDL.exe',0		sub_10017860+2341o ; DATA XREF: check_EDH_proc+A581
if (v64 >= v63)	aQqrepairExe	db	'QQRepair.exe',0		sub_10017860+3921o DATA XREF: check_EDB_proc+8461
<pre>sub_100552CF(1, 67225901, (LPCSTR)0x8C0); v65 = *(vold **)(v62[v64] + 8);</pre>	aOgpctrayExe	db	'QOPETray.exe',8		sub_10017860+4F01o DATA XREF: check_EDR_proc+C3E1
<pre>if (1v65) v65 = &unk_10007482; lpHeml = (void *)sub_10055200(1, (char)v65);</pre>	aQqpcrtpExe	dþ	'QQPCRTP.exe',0		<pre>check_EDR_proc2+59310 DATA_XREF: check_EDR_proc+D311</pre>
<pre>v163 = (v014 ")s00_10055200(1, (Char]005); v163 = (v014 ")sub_10055200(1, (Char]00bins.exe") v140 = sub_1000134A((int)lpfem1, (int)v163) == 0;</pre>	aQmbinsExe	db	'qmbins.exe',0		sub_10017860+7ACto DATA_YREF_rcheck_EDR_proc+E241
if (1pMen1) sub_100552C9(1pMen1);	aQqpcrealtimesp	db	*QQPCRealTimeSpeed		
if (v163)					<pre>DATA XREF: check_EDN_proc+F171 sub_10017860+4681n</pre>
sub_100552C9(v163);					

Figure 5-10Terminal protection process detection

6 IoCs

5d561153af1589bd1d64556bdd257c0 297180f60a3c70896bbe17cca0e9c501 77679c51504f2b94565b6e974d29ffff 2f49e81d731dc4ed960c546a57b06f4a 6e47449010e84f52736fa9033820fdb6 43.**.*196:12345 175.**.*96:12345 150.**.**.96:12345 150.**.**.22:12345 http[:]//27.**.*194:8080/7X/client.dll http[:]//43.**.**.80:8080/7X/client.dll http[:]/134.**.**.80:8080/7X/client.dll http[:]/134.**.**.215:8080/7X/client.dll	
77679e51504f2b94565b6e974d29ffff 2f49e81d731dc4ed960e546a57b06f4a 6e47449010e84f52736fa9033820fdb6 43.**.*196:12345 175.**.*96:12345 150.**.*22:12345 http[:]//27.**.*194:8080/7X/client.dll http[:]//13.**.**.80:8080/7X/client.dll http[:]//134.**.**.215:8080/7X/client.dll	5d561153af1589bd1d64556bddd257e0
77679e51504f2b94565b6e974d29ffff 2f49e81d731dc4ed960e546a57b06f4a 6e47449010e84f52736fa9033820fdb6 43.**.*196:12345 175.**.*96:12345 150.**.*22:12345 http[:]//27.**.*194:8080/7X/client.dll http[:]//13.**.**.80:8080/7X/client.dll http[:]/134.**.**.215:8080/7X/client.dll	297180f60a3e70896bbe17cca0e9c501
2f49e81d731dc4ed960e546a57b06f4a 6c47449010e84f52736fa9033820fdb6 43.**.**.196:12345 175.**.*96:12345 150.**.**.22:12345 http[:]//27.**.**.194:8080/7X/client.dll http[:]//43.**.**.80:8080/7X/client.dll http[:]//192.**.*6.0:8080/7X/client.dll http[:]/134.**.**.80:8080/7X/client.dll	
6e47449010e84f52736fa9033820fdb6 43.**.**.196:12345 175.**.*9.6:12345 150.**.**.22:12345 http[:]//27.**.**.194:8080/7X/client.dll http[:]//43.**.**.80:8080/7X/client.dll http[:]//192.**.**.60:8080/7X/client.dll http[:]/134.**.**.215:8080/7X/client.dll	77679e51504f2b94565b6e974d29ffff
43.**.**.196:12345 175.**.*96:12345 150.**.**.22:12345 http[:]//27.**.**.194:8080/7X/client.dll http[:]//43.**.**.80:8080/7X/client.dll http[:]/192.**.*60:8080/7X/client.dll http[:]/134.**.**.215:8080/7X/client.dll	2f49e81d731dc4ed960e546a57b06f4a
175.**.**.96:12345 150.**.**.22:12345 http[:]//27.**.**.194:8080/7X/client.dll http[:]//43.**.**.80:8080/7X/client.dll http[:]//192.**.**.60:8080/7X/client.dll http[:]//134.**.**.215:8080/7X/client.dll	6e47449010e84f52736fa9033820fdb6
150.**.**.22:12345 http[:]//27.**.*194:8080/7X/client.dll http[:]//43.**.**.80:8080/7X/client.dll http[:]//192.**.**.60:8080/7X/client.dll http[:]//134.**.**.215:8080/7X/client.dll	43.**.**.196:12345
http[:]//27.**.**.194:8080/7X/client.dll http[:]//43.**.**.80:8080/7X/client.dll http[:]//192.**.**.60:8080/7X/client.dll http[:]//134.**.**.215:8080/7X/client.dll http[:]//43.**.**.85:8080/7X/client.dll	175.**.**.96:12345
http[:]//43.**.**.80:8080/7X/client.dll http[:]//192.**.**.60:8080/7X/client.dll http[:]//134.**.**.215:8080/7X/client.dll http[:]//43.**.**.85:8080/7X/client.dll	150.**.**.22:12345
http[:]//192.**.**.60:8080/7X/client.dll http[:]//134.**.**.215:8080/7X/client.dll http[:]//43.**.**.85:8080/7X/client.dll	http[:]//27.**.**.194:8080/7X/client.dll
http[:]//134.**.**.215:8080/7X/client.dll http[:]//43.**.**.85:8080/7X/client.dll	http[:]//43.**.**.80:8080/7X/client.dll
http[:]//43.**.**.85:8080/7X/client.dll	http[:]//192.**.**.60:8080/7X/client.dll
	http[:]//134.**.**.215:8080/7X/client.dll
	http[:]//43.**.**.85:8080/7X/client.dll
http[:]//47.**.**.161:8080/7X/client.dll	http[:]//47.**.**.161:8080/7X/client.dll
http[:]//43.**.**.194:8080/7X/client.dll	http[:]//43.**.**.194:8080/7X/client.dll



http[:]//43.**.**.8:8080/7X/client.dll
http[:]//150.**.**.22:8080/7X/client.dll
http[:]//43.**.**.196:8080/7X/client.dll
http[:]//175.**.**.96:8080/7X/client.dll
https://www.kdocs.cn/view/l/crE7FLdvYnGN
https://dashi.163.com/html/cloud-attachment-download/?key=djAycC8yc05PUU82cjV5ZUVPUG9QNzBWQT09
https://wwpb.lanzoue.com/ibyhc0mu6myc

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.

Analysis of Attack Activities Using Spam to Spread Remote Control Trojans

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.