Confucius: The Angler Hidden Under CloudFlare

Antiy CERT Antiy Group *2022-07-13 12:04*

A few days ago, Antiy Deputy Chief Engineer Li Bosong was interviewed by a reporter from the Global Times, and disclosed that the Indian APT organization "Confucius" recently discovered by Antiy CERT, and its attack activities against the Pakistani government and military institutions (see the article on Global Network for details today). Article 2 reproduced article). This article is a detailed analysis report.

0 1
Overview

Recently, when Antiy CERT tracked and sorted out the attacks from the direction of the South Asian subcontinent, it found an attack by the Confucius group against the Pakistani government and military institutions.

The name of the organization first came from an analysis report released by foreign security vendor Palo Alto Networks in 2016 [1] . In this report, Palo Alto Networks disclosed the attack activities of an Indian attack group, which can be traced back to 2013. In 2010, he was good at using spear-phishing emails, watering hole attacks and phishing websites, and cooperated with rich social engineering methods to conduct attacks on the governments, military, energy and other fields of China, Pakistan, Bangladesh and other neighboring countries of India for the purpose of stealing sensitive information. attack activities. In the early attack activities, the organization used internationally renowned websites (such as Quora, similar to my country's Zhihu) with the function of message interaction, and

entrained the encrypted remote control server address of the Trojan in the public messages. After the Trojan used by the organization is implanted into the victim host, it can obtain the content from such public messages, decrypt and restore the real remote control server address. Therefore, the first network access behavior of the Trojan on the victim host will be regarded as a normal web page request, but the attacker can use these internationally renowned websites to continuously change the remote control address or issue other instructions. On a Quora page linked to the malicious code, Palo Alto Networks found that the content posted by the attackers contained the words "Confucius says", that is, "Confucius Says", or "Zi Yue", so it called the group Confucius. It can be seen that in the process of continuously attacking China, the attackers also conducted research on Chinese culture.

In this attack activity discovered by Antiy CERT, the organization mainly disguised as Pakistani government staff to deliver spear-phishing emails to the target, and tricked the target into downloading and opening the document embedded with malicious macro code through the content of the phishing email, so as to send the target machine to the target machine. Implant the open source Trojan QuasarRAT, self-developed C++ backdoor Trojan, C# stealing Trojan and JScript downloader Trojan.

At present, the attack has attracted the attention of the relevant departments of the Pakistani government. Among them, the National Telecommunications and Information Technology Security Board (NTISB) of Pakistan has repeatedly issued a national cyber threat warning [2] [3], saying that the attackers are sending government officials and the public to the public. Mimicking a fake phishing email from the Pakistan Prime Minister's Office, government officials and the public are asked to remain vigilant and refrain from providing any information via emails and social media links.

This report summarizes the attack activities, tactics and tools of the Confucius organization from 2021 to the present. The characteristics of the overall activities can be briefly summarized in the following table:

Table 1-1 Summary of overall attack activity characteristics

Attack time	2021-present
attack intent	continuous control, stealing
target	Pakistan
For industry/sector	government, military
Attack method	Spear-phishing emails, phishing websites, using third-party cloud storage services to store malicious payloads
target system platform	Windows
type of bait	Decoy PDF files, malicious macro documents, malicious RTF files, malicious shortcuts, etc.
Development language	C++, VBScript, C# and JScript
Weaponry	C++ backdoor Trojan, C# stealing Trojan, C# downloader Trojan, open source Trojan QuasarRAT, JScript downloader Trojan

0 2

activity analysis

From the second half of 2021 to the present, Antiy CERT has successively captured sample files of Confucius' attacks against Pakistan. The attack timeline of the captured samples is as follows:

Attacked in June 2021 using malicious RTF documents related to the list of victims of the Pakistan Army;

An August 2021 attack using a macro document from the Pakistani military on the content of Pegasus spyware warnings;

In August 2021, the attack was carried out using the macro document related to the tax declaration of the Pakistan Federal Tax Service;

Attacks using malicious shortcut files disguised as image files in February 2022;

In February 2022, the attack was carried out using macro documents related to the COVID-19 vaccination status table of Pakistani government employees and the audit table of digital assets;

In May 2022, the attack was carried out using a macro document related to the application form of the Pakistani Prime Minister's Office employee;

Attacked in June 2022 using malicious macro documents related to the Pakistani Ministry of Foreign Affairs.

In this attack, the attackers mainly delivered spear-phishing emails to the target in the name of Pakistani government staff. COVID-19 vaccination status.

Figure 2-1 Phishing email

The attacker embeds different types of malicious links in the body of the phishing email and in the attached PDF file. When the target views the phishing email, they will be deceived by the content of the email body and PDF file carefully designed by the attacker, so that they can click the malicious link to download the malicious link. Documentation for macro code.

There are three main types of malicious links used by attackers:

▶ Links to phishing websites that imitate government websites: Attackers use website cloning tools such as HTTrack to build phishing websites that imitate the official websites of government departments (such as the Office of the Prime Minister of Pakistan, the Journal of the National Defense University of Pakistan, and the Federal Tax Service of Pakistan). When the target accesses through the phishing website When linking to a phishing website, the attacker tricks the target into downloading a document with malicious macros through the content of the website.

Table 2-1 Phishing Domain Names

domain name	**counterfeit object**
pmogov.info	Office of the Prime Minister of Pakistan
pmogov.online	Office of the Prime Minister of Pakistan
ndu-edu.digital	National Defense University of Pakistan
psca-gop-pk.digital	Pakistan Punjab Safe City Authority
nadra.digital	Pakistan National Database and Registration Authority
mofa-pk-server.live	Ministry of Foreign Affairs of Pakistan
fbr-notice.com	Federal Revenue Service of Pakistan
fbr-tax.info	Federal Revenue Service of Pakistan
notice-fbr.tax	Federal Revenue Service of Pakistan
fbr-mail.online	Federal Revenue Service of Pakistan
csd-pk.online	Pakistan Canteen Department Store (a chain retail enterprise under the Ministry of Defense of Pakistan)

Figure 2-2 Phishing website imitating the Pakistan Prime Minister's Office

Figure 2-3 Phishing website imitating the Journal of Pakistan National Defense University

▶ File download link to a third-party cloud storage service: The attacker stores the malicious macro file in the third-party cloud storage service website Dropbox network disk. When the target accesses the link with a browser, the browser will automatically request to download the stored file. Malicious macro document.

▶ Access links to third-party Deep Linking [4] (deep linking) services: Deep linking refers to the linking service provided by the linking website, so that users can obtain the information on the linked website without leaving the page of the linking website. content, the URL of the linking website is displayed in the address bar of the page, not the URL of the linked website. Attackers can use the deep link service provided by Branch to customize the characteristics of subdomains and disguise the subdomains as official websites of the Pakistani government (such as ncoc-update.app.link, pmoffice.app.link, moitt-auditform.app. link), when the target accesses the access link created by the attacker through the browser, the Branch server will automatically request to download the malicious macro document stored in the third-party cloud storage service. At the same time, when downloading a malicious macro document, the address bar of the target browser still displays the access link created by the attacker, not the download link of the third-party cloud storage service that downloads the malicious macro document. The credibility of the downloaded file in the target's mind.

The overall attack flow of this attack activity is shown in the following figure:

Figure 2-4 The overall attack process of this attack

Figure 2-5 Decoy PDF file embedded with malicious download links

Figure 2-6 Malicious RTF document related to the list of victims of the Pakistan Army

In this attack, in order to prevent security analysts from analyzing and tracing the source of the attack, the attackers used the following methods to evade detection:

● Deliberately forge the timestamps of C# downloader Trojans and C# stealing Trojans into unreal time to counter time zone analysis.

● Using encrypted malicious macro code documents, the password is generally located in the body of the email, the body of the PDF and the page of the phishing website. By encrypting the malicious macro document, the attacker ensures that when the non-target group obtains the malicious macro document, the malicious macro document cannot be opened and analyzed without the password.

● The domain names all use the CDN acceleration service of CloudFlare (US Content Delivery Network and DDoS Mitigation Company), which can effectively hide the real IP address of the server to which the domain name resolves.

● Using the CloudFlare firewall function to filter the address location of the access IP, only when the access IP is located in a specific country, the access page will jump to the real malicious macro document download page.

Figure 2-7 Restricting access countries through the CloudFlare firewall function

0 3
Sample analysis

3.1 Execution process analysis

3.1.1 Use Word macro document to release comprehensive stealing components

Attackers use malicious Word macro documents to release and execute Stage 1 and Stage 3 C# downloader Trojans, and then download subsequent attack payloads through the released downloader Trojans. At the same time, the attack payload returned by the attacker's mount server is essentially an ASCII file. The downloader Trojan at each stage will convert the ASCII file into a binary file, then load it into memory and jump to a dynamic function for execution.
The overall flow chart of using the Word macro document to release the integrated stealing component is shown in the following figure:

Figure 3-1 The overall process of using the Word macro document to release the integrated stealing component

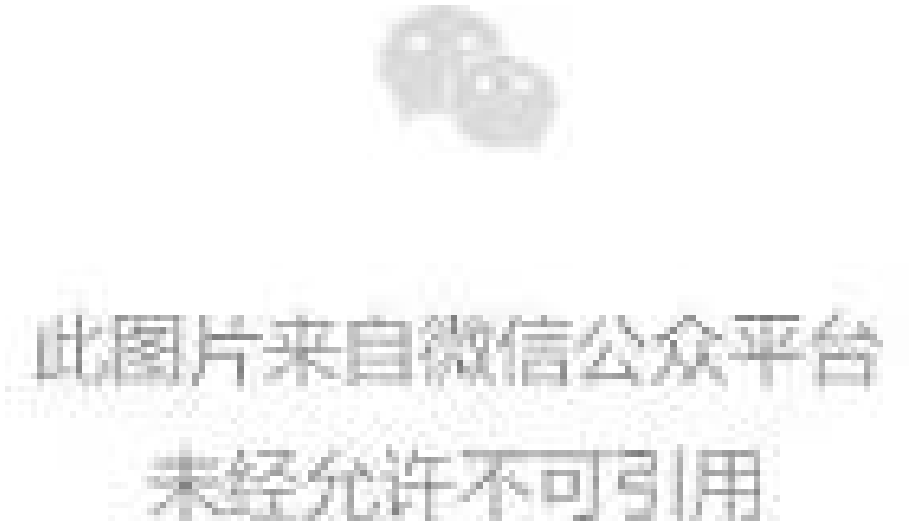

Figure 3-2 Petition.docm (petition)

Figure 3-3 Jobs_in_GHQ_Rawalpindi_2022.docm

3.1.2 Use Excel macro document to release backdoor components

Attackers use Excel documents that carry malicious macro codes to release backdoor components (such as the open source Trojan QuasarRAT, self-developed C++ backdoor Trojan) to the %ProgramData% directory of the host. For the open source Trojan QuasarRAT, the attacker will use the system tool PowerShell to execute. As for the C++ backdoor Trojan, the attacker uses the system tool Rundll32 to execute it.
The overall flow chart of using the Excel macro document to release the backdoor component is shown in the following figure:

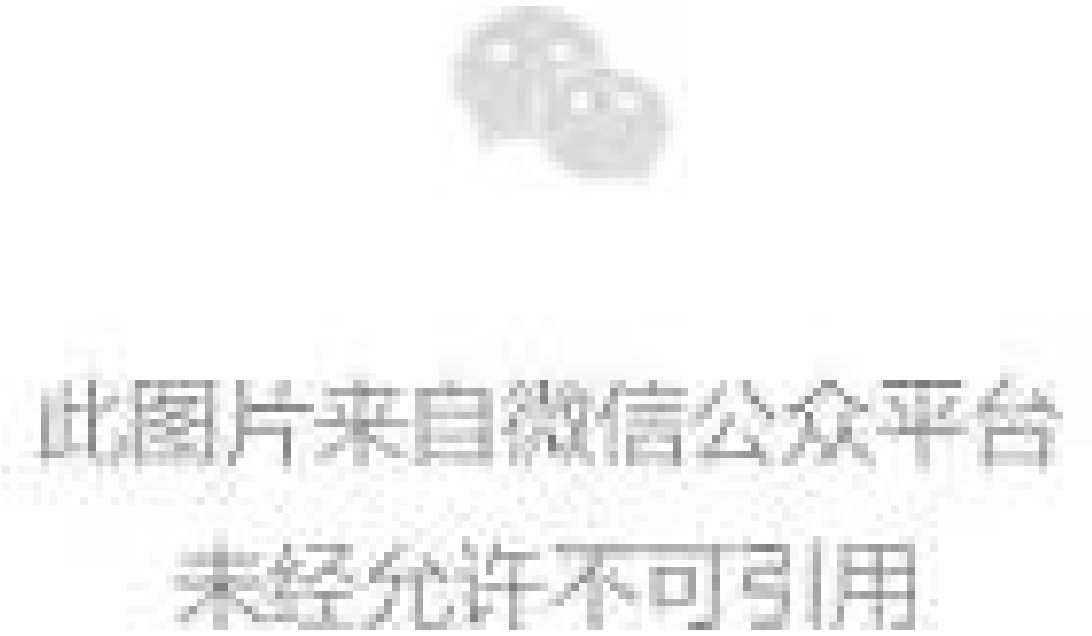

Figure 3-4 The overall process of releasing backdoor components using Excel macro files

Figure 3-5 DEPT_NCOC-3-31.xlsm

Figure 3-6 DigitalAssestsAudit.xlsm

3.2 Analysis of Attack Weapons

3.2.1 Malicious Word Macro Document

In this attack, the attackers mainly used malicious Word macro documents and malicious Excel macro documents. The malicious Word macro documents mainly implanted the integrated stealing components developed by the attackers into the host computer, while the malicious Excel macro documents were used by the host computer. The host is implanted with backdoor components (open source Trojan QuasarRAT, self-developed C++ backdoor Trojan).

3.2.1.1 Malicious Word Macro Document

Table 3-1 Examples of malicious macro documents

virus name	Trojan[Dropper]/MSOffice.Agent.ccd
original file name	SRIU-AppForm.docm
MD5	41CDCEC8311F735E1ED8D3BAB9192173
File size	87.5KB (89,600 bytes)
file format	Document/Microsoft.DOCM[:doc 2007-2013]
creation time	2022-05-19 11:50:00 +00:00
Last Modified	2022-05-27 09:02:00 +00:00
creator	SO-PAU
last modified	Windows User

Figure 3-7 SRIU-AppForm.docm

By analyzing the macro code embedded in the malicious Word document, it is found that the structure and function of the macro code written by the attacker are very simple, and the main functions are as follows:

1. When the victim triggers the "DOWNLOAD FORM" button, the white file is downloaded to the "Download" directory of the host computer, and a pop-up message pops up indicating the location of the file.

Figure 3-8 Pop-up message, download white file

2. The attacker releases the C# downloader Trojan at different stages according to whether the host computer has the installation folder of the antivirus software McAfee.

Figure 3-9 Release of different C# downloader Trojans

When the installation folder of the antivirus software McAfee exists on the host, extract the Stage 3 C# downloader Trojan ASCII data from the "Comments" attribute in the document (in this sample, due to the attacker's mistake, the Trojan data is actually stored In the "Description" property of the document), after converting the ASCII data into

binary data, name it "sdjkfhkjsdh.txt" and release it to the %TEMP% directory of the host, and create a Trojan that is released and execute it every 20 minutes. The scheduled tasks are persisted.

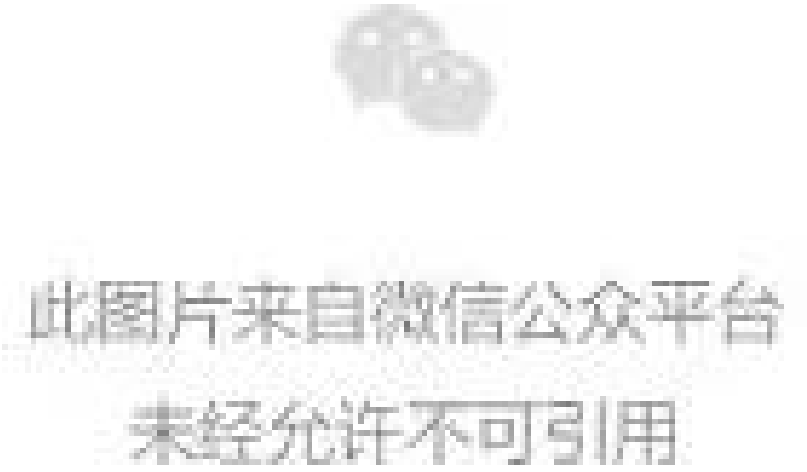

Figure 3-10 Release the Stage 3 C# downloader Trojan

Figure 3-11 ASCII data hidden in subject and description attributes

Figure 3-12 Create a scheduled task

When the host computer does not have the installation folder of the antivirus software McAfee, it will extract the Stage 1 C# downloader Trojan ASCII data from the "Subject" attribute in the document, convert the ASCII data into binary data, and name it "" sdjkfhkjsdh.txt" is released to the %TEMP% directory of the host computer, and use PowerShell to execute the Trojan.

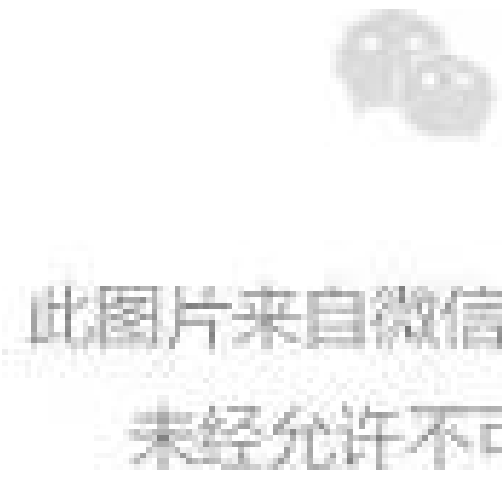

Figure 3-13 Release the Stage 1 C# downloader Trojan

Figure 3-14 Execute Trojan using PowerShell

3.2.1.2 Malicious Excel Macro Document

Table 3-2 Examples of malicious Excel macro documents

virus name	Trojan[Dropper]/MSOffice.Agent.ccd
original file name	FBR5323-Notice.xlsm
MD5	06B5A67BF37FED5B92C2211F342D7F0A
File size	937KB (959,488 bytes)
file format	Document/Microsoft.XLSM[:xls 2007-2013]
creation time	2015-06-05 18:17:00 +00:00
Last Modified	2022-05-10 09:17:00 +00:00
creator	TAX&FBR
last modified	Abbasi

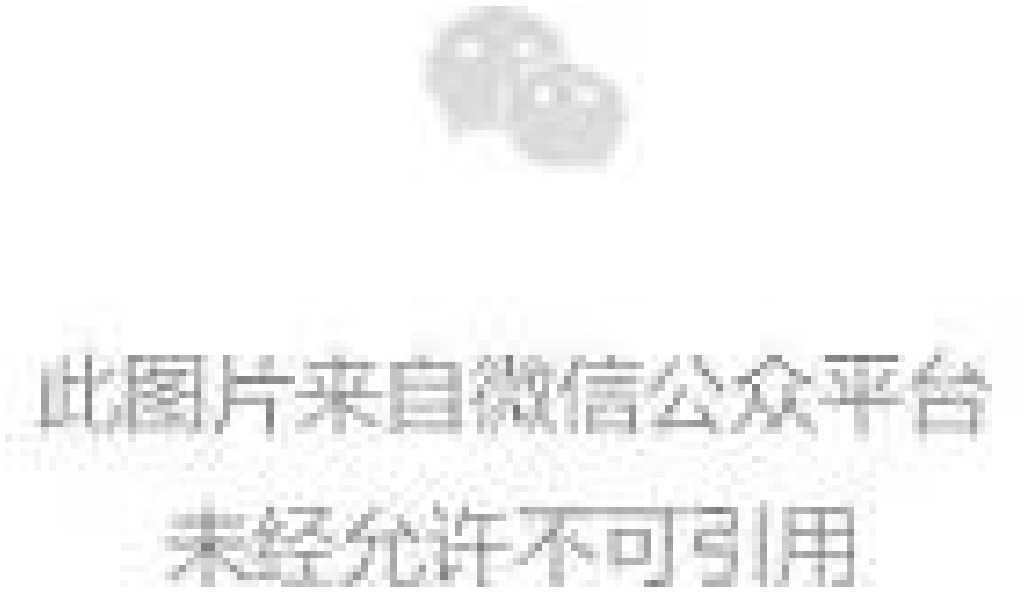

Figure 3-15 FBR5323-Notice.xlsm

The function of the macro code embedded in the malicious Excel document is also very simple, mainly to release the open source Trojan QuasarRAT obfuscated by .NET Reactor, and then use the system tool PowerShell to load and run the released QuasarRAT.

Figure 3-16 Extracting the Base64-encrypted QuasarRAT data hidden in the sheet

Figure 3-17 Base64 encrypted QuasarRAT data

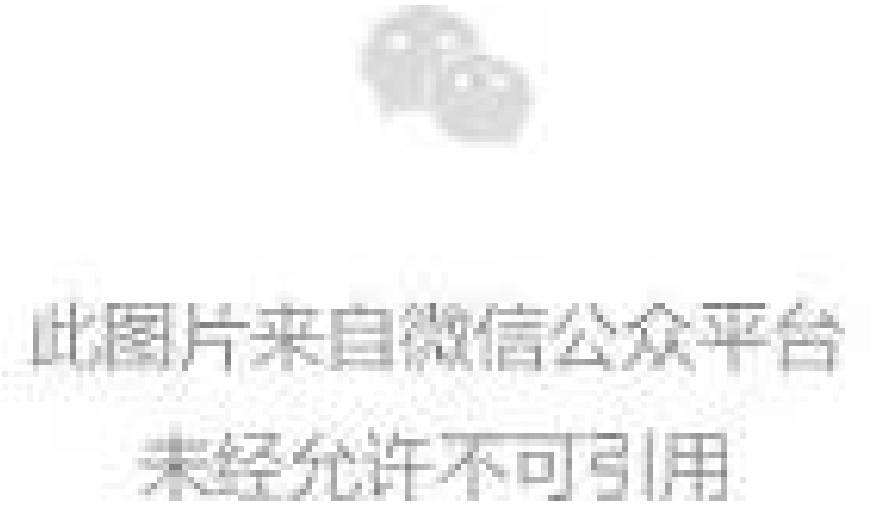

Figure 3-18 Decrypt and release QuasarRAT

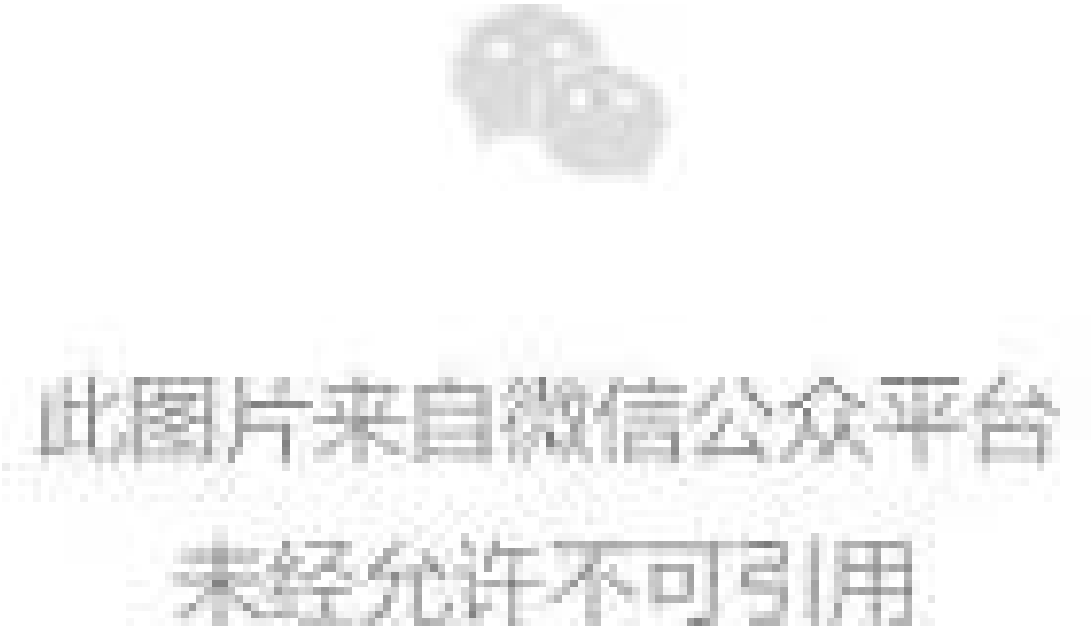

Figure 3-19 Using PowerShell to load and execute QuasarRAT

At the same time, the analysis of the entire macro code shows that there are some functions in the macro code that the attacker has not enabled. The unenabled functions include using the registry to persist the released QuasarRAT, and message pop-ups that can be used to confuse victims. .

Figure 3-20 Features not enabled

3.2.2 Integrated stealing components

Table 3-3 Stage 1 C# Downloader Trojan

virus name	Trojan/Win32.Downloader
original file name	PoryaenFuaQzye.dll
MD5	C676EB09E74308A879658FDA6FCB74FC
processor architecture	Intel 386 or later, and compatibles
File size	8.50KB (8,704 bytes)
file format	Win32 DLLs
timestamp	2076-10-03 02:38:51 +00:00 (forged)
digital signature	none
Packing type	none
compiled language	Microsoft Visual C# / Basic .NET

The function of Stage 1 C# downloader Trojan is relatively simple. It mainly obtains the Stage 2 C# downloader Trojan ASCII file from the attacker's mount server, then converts the ASCII file into a binary file, and finally loads it into memory and jumps to dynamic function to execute.

Figure 3-21 Stage 1 C# downloader Trojan horse function

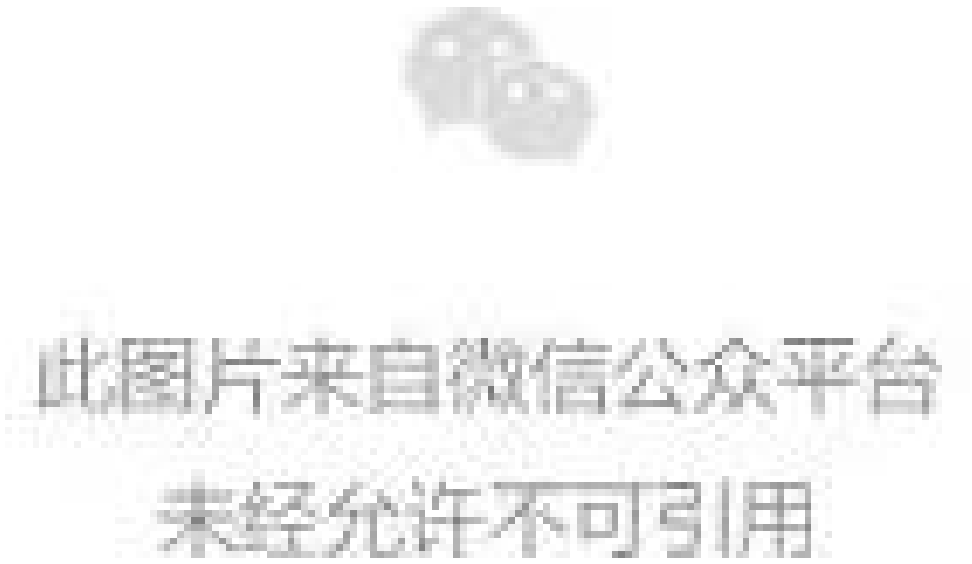

Figure 3-22 The Stage 2 C# downloader Trojan ASCII file returned by the mount server

Table 3-4 Stage 2 C# Downloader Trojan

virus name	Trojan/Win32.Downloader
original file name	SowpnTdb.dll
MD5	31A5973AFABF2FEBE9690F20AC045973
processor architecture	Intel 386 or later, and compatibles
File size	348KB (356,864 bytes)
file format	Win32 DLLs
timestamp	2022-04-22 13:02:49 +00:00
digital signature	none
Packing type	none
compiled language	Microsoft Visual C# / Basic .NET

The Stage 2 C# downloader Trojan function is to download the Stage 3 C# downloader Trojan, and create a scheduled task named "YunoHonow" for the Stage 3 C# downloader Trojan. The scheduled task will use the system tool PowerShell to load and execute Stage 3 C# every 20 minutes. Downloader Trojan.

Figure 3-23 Stage 2 C# downloader Trojan horse function

Table 3-5 Stage 3 C# Downloader Trojan

virus name	Trojan/Win32.Downloader
original file name	RioucXkjdiEjkhd.dll
MD5	FD7555A617420B42BA946FCC5248D07F
processor architecture	Intel 386 or later, and compatibles
File size	10.0KB (10,240 bytes)
file format	Win32 DLLs
timestamp	2083-02-05 20:09:11 +00:00 (forged)
digital signature	none
Packing type	none
compiled language	Microsoft Visual C# / Basic .NET

The function of Stage 3 C# downloader Trojan is to download Stage 4 C# stealing Trojan, and load the C# stealing Trojan into memory and jump to the dynamic function for execution. At the same time, in order to ensure that the Stage 4 C# stealing Trojan can be successfully downloaded, the attacker also uses an alternate download link.

Figure 3-24 Stage 3 C# downloader Trojan horse function

Table 3-6 Stage 4 C# stealing Trojans

virus name	Trojan[Spy]/Win32.Stealer
original file name	Rwlksdnasjd.dll
MD5	53C5FCDD09A53BAE6C21E0CADD85AEC2
processor architecture	Intel 386 or later, and compatibles
File size	11.5KB (11,776 bytes)
file format	Win32 DLLs
timestamp	2067-12-02 18:52:44 +00:00 (forged)
digital signature	none
Packing type	none
compiled language	Microsoft Visual C# / Basic .NET

The Stage 4 C# Trojan is a stealing Trojan. Its main function is to steal the Documents, Downloads, Desktop, Pictures directories in the Users folder of the C drive of the host computer and all files of the same type in the other drives.

Figure 3-25 The overall function of C# stealing Trojans

At the same time, in order to avoid uploading files repeatedly, the Trojan will return the MD5 value of the file to the C2 server when uploading the file. Whenever the Trojan restarts, it will download the MD5 list of uploaded files from the C2 server according to the host's unique identifier (machine name__username) (the MD5 list file is located in the server's har1 directory). When the Trojan uploads files later, it avoids repeated uploading of files by judging whether the MD5 value of the current file exists in the MD5 list of uploaded files.

Figure 3-26 Obtain the MD5 file list of uploaded files based on the unique identifier

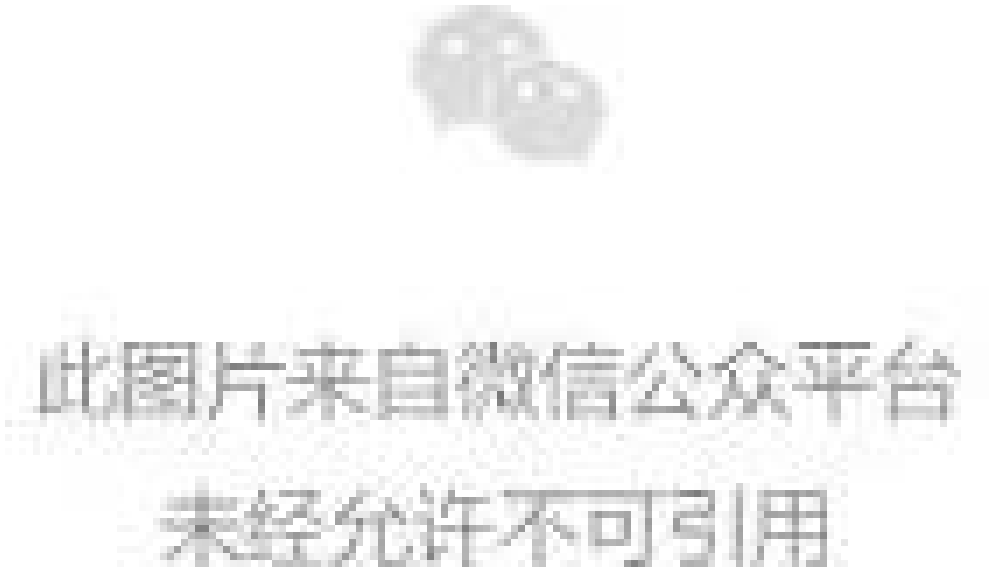

Figure 3-27 Upload file, file MD5

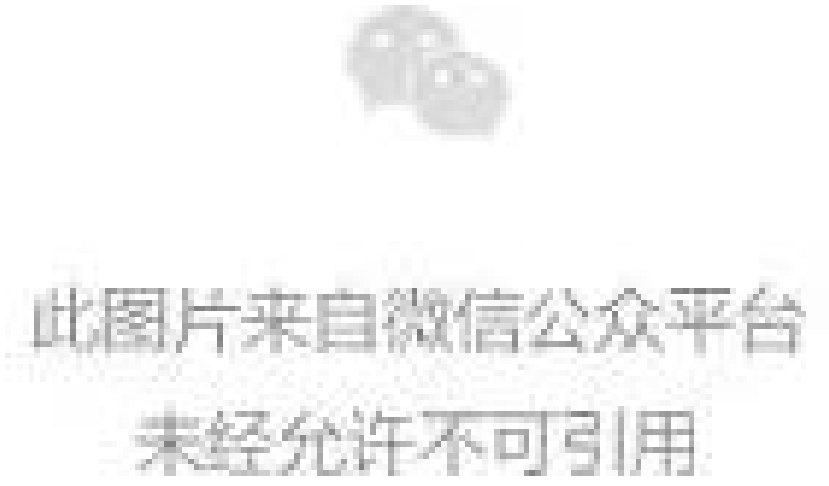

Figure 3-28 Search for all files of the same type in the current directory

Figure 3-29 Upload file and file MD5, and continue to search subdirectories

3.2.3 Backdoor Components

Table 3-7 C++ backdoor Trojans

virus name	Backdoor/win32.Agentb
original file name	Print.dll
MD5	46417AD0FC33783C298B7441ACED2C1A
processor architecture	Intel 386 or later, and compatibles
File size	220KB (225,792 bytes)
file format	Win32 DLLs
timestamp	2022-04-12 05:09:50 +00:00
digital signature	none
Packing type	none
compiled language	Microsoft Visual C/C++(2013)[DLL32]

The C++ backdoor Trojan was first discovered in an attack by Confucius in September 2020. By comparing the new version of the backdoor Trojan captured this time with the previous version, it was found that its functions have not changed much from the previous version. The Trojan just makes adjustments to the overall code structure.
Its main functions include creating scheduled tasks, retrieving process information, retrieving network adapter information, retrieving disk drive information, uploading files, downloading files, executing files, and rebounding Shell.
After the backdoor Trojan is executed, it will first determine whether the file name and path of itself and the loader are specific to decide whether to continue execution.

Figure 3-30 Get the loader path

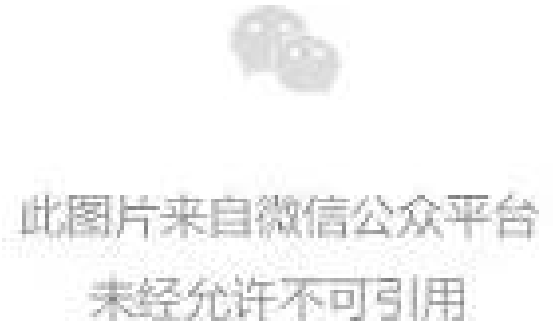

Figure 3-31 Determine the path where it is located

Second, ensure that only one Trojan program is running in the host by creating a mutex. The mutex used by this sample Trojan is "v2.1.1". In the follow-up, Antiy CERT captured the C++ backdoor Trojan whose mutex is "v2.1.4". From this, it can be inferred that the mutex used by the backdoor Trojan is the current Trojan version number.

Figure 3-32 Mutexes of different versions of Trojans

At the same time, the attacker creates a scheduled task named "Windows Logging Service" and uses the system tool Rundll32 to load and execute itself every fifteen minutes, so as to achieve the purpose of persistent monitoring of the host.

Figure 3-33 Scheduled task name

Figure 3-34 Scheduled task files stored in the Task directory

Then, the Trojan will generate a unique identity for the host and send it back to the C2 server. The composition of the identity is shown in Figure 3-35:

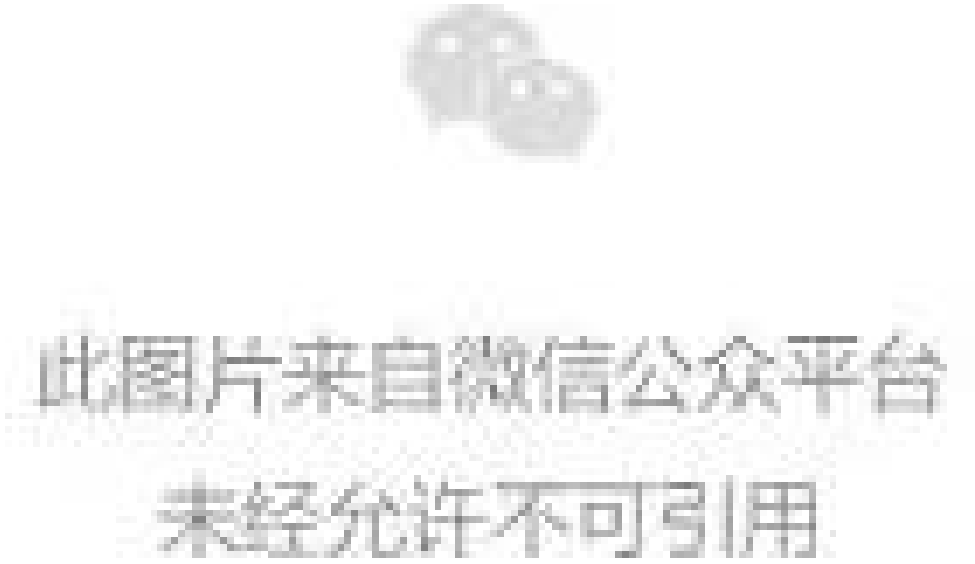

Figure 3-3 5 Identification

Figure 3-36 Sample ID

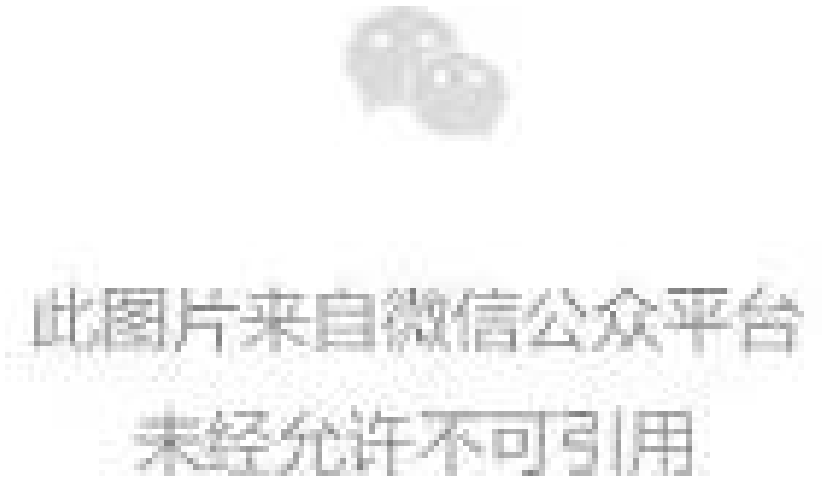

Figure 3-37 Determine the operating system version

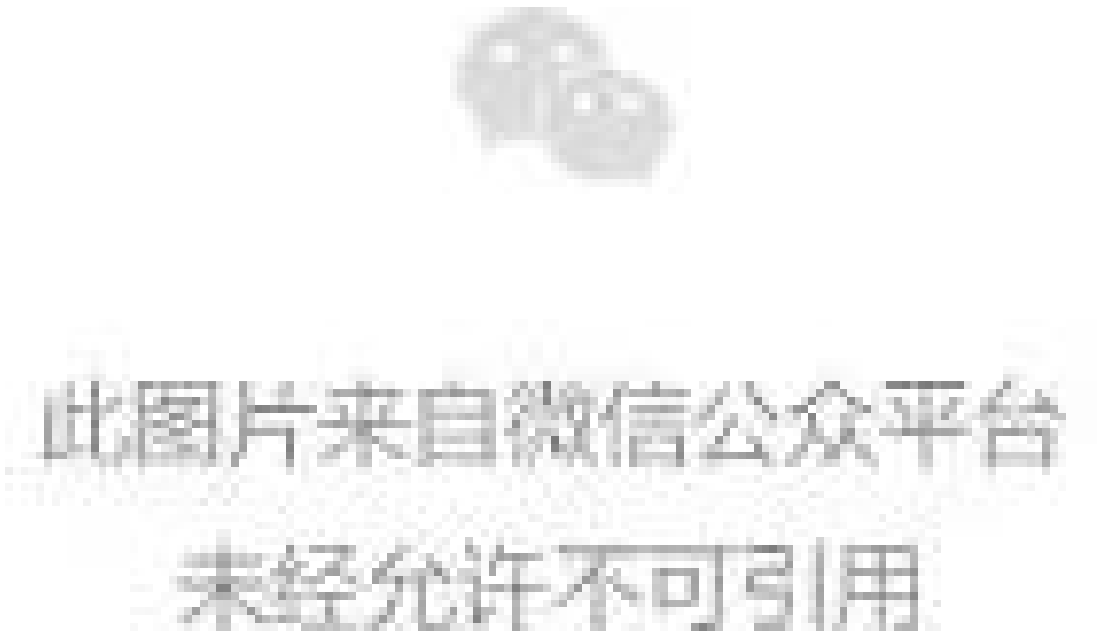

Figure 3-38 Determine whether the running environment is a virtual machine or a physical machine

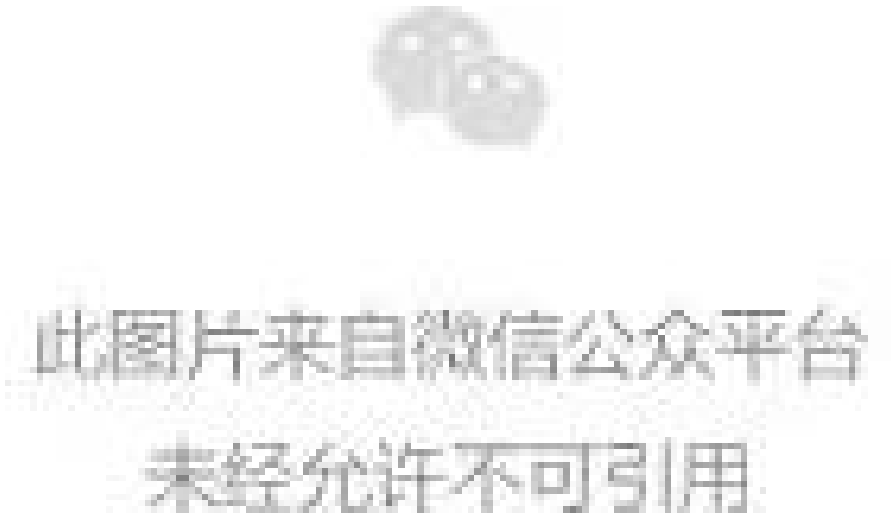

Figure 3-39 Determine the number of operating system bits

Figure 3-40 Splicing the ID and sending it back to the C2 server

The Trojan then sends the retrieved host information back to the attacker's C2 server. The retrieved information includes processes, network adapters, disk drives, installed applications, and files of the appropriate type.

Figure 3-41 Return information

Retrieve process information: Retrieve the process information that the host is running, and the obtained information is returned to the C2 server in the form of "program name - program PID - path where the program is located".

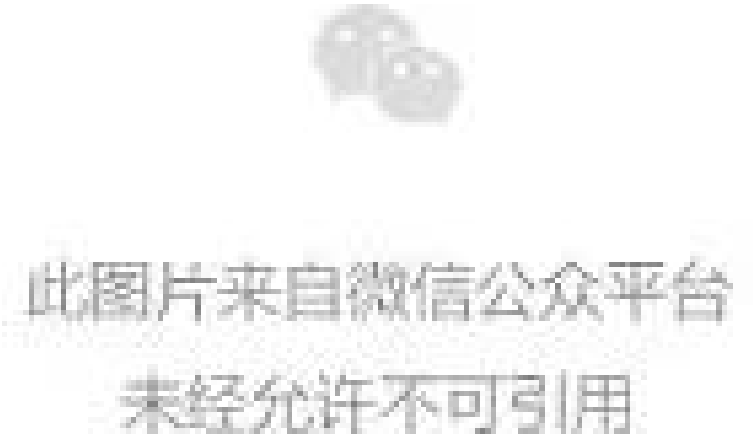

Figure 3-42 Retrieving the active process information of the host

Figure 3-43 Get the full path of the process program

Figure 3-44 Process information format returned

Retrieve disk drive information: Obtain the host disk drive information, so that the Trojan can retrieve the qualified file information in the disk drive subsequently.

Figure 3-45 Retrieving disk information

Retrieve network adapter information: contains adapter type, name, description, Mac address, IPv4 address, gateway, subnet mask, etc.

Figure 3-46 Retrieving Network Adapter Information

Figure 3-47 Network information to be retrieved

Retrieve application information: Obtain information such as the name, version, and path of the software installed on the host by retrieving the subkeys of the registry HKLM\Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall.

Figure 3-48 Retrieving the registry

Retrieve files of matching type from disk drives: The file types that attackers are interested in are doc, docx, pdf, txt, ppt, pptx, xls, xlsx, zip, rar, 7z, and axx.

Figure 3-49 Retrieving files

Figure 3-50 File types targeted by attackers

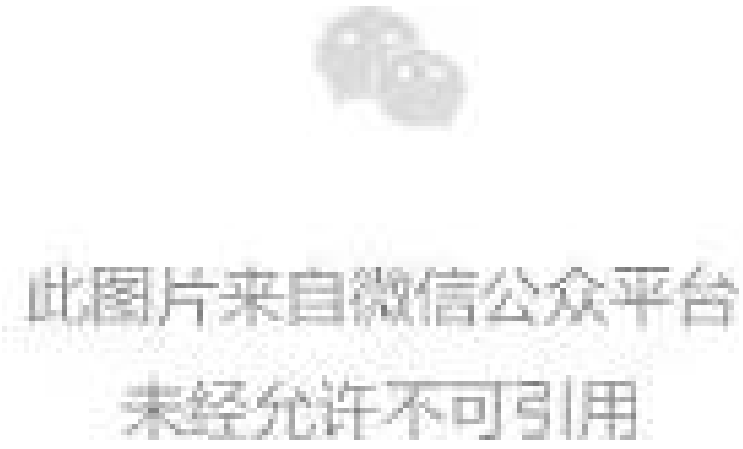

Figure 3-51 Directories to be excluded

Finally, after the above information is returned, the Trojan enters the backdoor state and waits for the C2 server to issue an instruction to execute the corresponding function.

Through the analysis of the Trojan, it is found that the attacker mainly uses multiple While loops to achieve backdoor operations, and each designed While loop can perform one or more functions.

Figure 3-52 Using multiple While loops to implement backdoor operations

The instructions issued by the attacker can be divided into first-level and second-level instructions. The first-level instruction represents an overall function, and the second-level instruction represents the branch function under the overall function.

When the attacker controls the target, he first issues a first-level instruction to enter the overall function, and then issues a specific instruction to implement the branch function. The specific instructions are separated by "," characters, that is, in the form of "second-level instructions, specific operations,", and the Trojan will decompose the specific instructions through the Strtok function after receiving them. At the same time, after the Trojan completes the command, it will send back specific characters to the C2 server to identify the result of the command execution.

Figure 3-53 Level 1 command issued by the attacker

Figure 3-54 The second-level command issued by the attacker

Table 3-8 lists the commands and functions sent by the attacker through the C2 server:

Table 3-8 Command function table

first order	Secondary Instructions	specific function	return ID	Logo meaning
Wait	none	Waiting for C2 to issue a command	Hi	A wait command has been received, waiting for subsequent commands.
CFEx	JE	Execute the specified executable	ExFl	Executable failed to execute
			ExSu	Executable file executed

				successfully
	CFE	Retrieve the specified executable	FNoF	No file retrieved
			FiFo	File retrieved successfully
	JD	Download the executable file according to the URL issued by the C2	JuDo	file download successfully
			DowF	File download failed
	DE	Download the executable file according to the URL issued by the C2, and execute the file	DnEx	The file is downloaded and executed successfully
			ExeF	File download succeeded, but execution failed
			DowF	File download failed
			FiNF	file not found
DelF	none	delete the specified file	FiDS	file deleted successfully
			FiDF	Complete the delete operation
ReSh	none	Bounce Shell	BC	Successfully connected to C2, but C2 did not reply
			UC	Failed to connect to C2
	GetF	get file	Done	file upload complete
GetF	Send	return file	none	none
	Skip	Skip the current file, i.e. do not upload	none	none
	Next	Skip the current file, i.e. do not upload it.	none	none
			FNoF	The specified file was not retrieved
FeFi	none	Upload the specified file	FeFi	The file was read successfully, and the file data will be returned soon
			AcDe	file read failed
			FNNR	file write failed
	DWNL	Receive data from C2 and write to file	DowF	Download file failed
			JuDo	just download the file
DWNL				
	DWNE	Receive data from C2, write to file, and execute	DnEx	The file was downloaded successfully and executed successfully
			ExeF	file execution failed
LiFi	none	After sleeping for 5 minutes, re-enter the backdoor function and receive new commands	none	none
Exit	none	exit the program	Exit	exit successfully
ReST	none	exit the program	ReST	exit successfully

Figure 3-55 Download files and execute executable files through URL

Figure 3-56 Retrieving files and executing files

Figure 3-57 Delete the specified file

Figure 3-58 Upload the specified file

Figure 3-59 Download file and execute file

Figure 3-60 Rebound Shell

3.2.4 Downloader component

JScript is a scripting language from Microsoft specifically designed for use in Web pages. It adheres to the ECMAScript standard and is primarily a Microsoft language that corresponds to Netscape's earlier and widely used JavaScript. Like many other programming languages, Microsoft JScript is written in text and organized into statements, blocks of related sets of statements, and comments.

The attacker uses the downloader component written in the JScript language to implant the C++ launcher Trojan, VBS script and comprehensive stealing components into the target machine.

Its complete execution process is shown in the following figure:

Figure 3-61 JScript downloader execution flow

Table 3-9 JScript downloader Trojans

virus name	Trojan[Downloader]/JScripts.Agent
original file name	157720846
MD5	157C6E86D68D98F777D37C3753322F69
File size	2.41KB (2,474 bytes)
interpreted language	JScript
VT first upload time	2022-04-08 16:09:11 +00:00
VT test results	10/58

The JScript downloader Trojan will identify the host system version according to the browser kernel information, and then execute different commands according to different systems.

When the system version is Windows7, that is, the browser kernel is "Windows NT 6.1", the subsequent attack payloads (a C++ launcher Trojan, a C# downloader Trojan, a VBS script, a name The file is "ZeroToleranceMonth.jpg", the ZeroToleranceMonth.jpg file is suspected to be a decoy image file), and a scheduled task named "calcure42" is created through the schtasks command.

When the system version is not Windows7, the subsequent attack payload will be downloaded by curl.exe through the CMD command line tool, and a scheduled task named "WinEvent5" will be created through the schtasks command.

Figure 3-62 JScript downloader Trojan

The function of the downloaded VBS script is to use the system tool Rundll32 to run the C++ launcher Trojan.

Figure 3-63 z.vbs

Table 3-10 C++ Launcher Trojans

virus name	Trojan/Win32.Agent
original file name	jdsuifyiusdyf.txt
MD5	E05AF60FBB3EC9110ACBF38CD1071F52
processor architecture	Intel 386 or later, and compatibles
File size	111KB (114,176 bytes)
file format	Win32 DLLs
timestamp	2022-04-01 12:51:45 +00:00
digital signature	none
Packing type	none
compiled language	Microsoft Visual C++ v.7.10 - 14.27

The main function of the downloaded C++ launcher Trojan is to create a scheduled task named "Daily Trigger Test Task", which uses the system tool PowerShell to execute the Stage 3 C# downloader Trojan every fifteen minutes.

Figure 3-64 The command to be executed by the scheduled task

Figure 3-65 Names of scheduled tasks

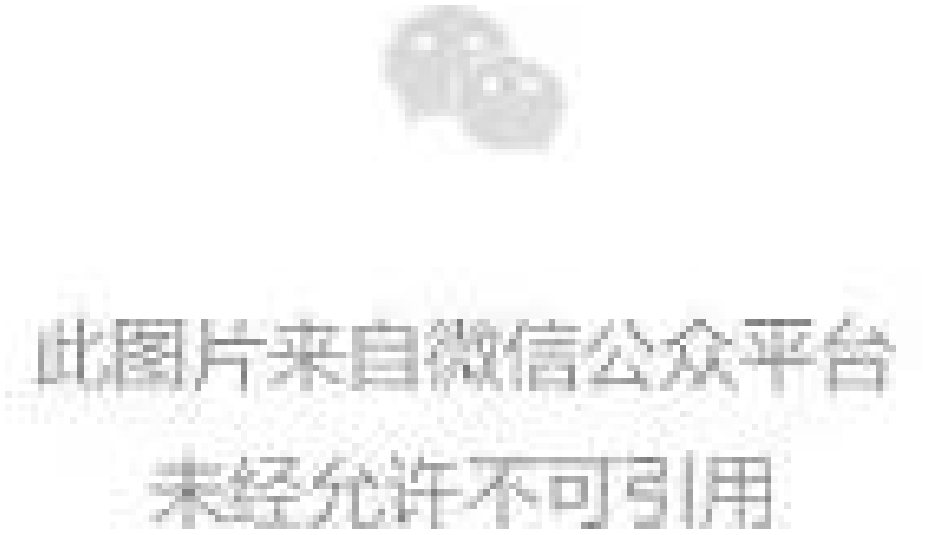

Figure 3-66 Scheduled task Task file

04
Association attribution

Antiy CERT conducts line extension analysis on the captured samples through the Antiy Cyber Ultra Brain Correlation Subsystem, and finds that the C++ backdoor Trojan captured this time can be associated with many previous attack activities of the attacker.

Figure 4-1 Correlation diagram

When analyzing the associated attack activity samples, it was found that many of them were DeMnu obfuscators organized by Confucius. The DeMnu obfuscator was first published by the friend Qi Anxin in September 2020, and it was disclosed in the report "Operation Tibu: A Retaliation Targeted Attack from the South Asian APT Organization "Mo Luo Shu" [5] that "Mo Luo Shu" is a friend Shangqi Anxin's nickname for the Confucius organization.

The Confucius organization mainly uses the DeMnu obfuscator to load its unique loader program Polyloader, and then decrypts and loads the open source remote control Trojan AsyncRat through the Polyloader.

Figure 4-2 The decryption function used by the DeMnu obfuscator associated this time

Figure 4-3 The decryption function used by the DeMnu obfuscator disclosed in the Qi Anxin report

At the same time, the malicious payload mount links used by attackers in previous attacks are highly similar to those used by Confucius in previous attacks.

Table 4-1 Comparison of malicious payload mount links

Associated Attack Activity	Past Confucius attacks
http://wordupdate.net/micro/upload	http://wordupdate.com/refresh/content
http://webinstaller.online/office/updates	http://wordupdate.com/recent/update
https://webinstaller.online/temp/KB4783	http://the-moondelight.96.lt/followup/update/KB756324
http://release.wordupdate.net/object/encode	http://recent.wordupdate.com/cloud/sync/upgrade

Based on the above information, Antiy CERT determines that this attack activity belongs to the Confucius organization.

05

Links with the SideWinder organization

During the correlation analysis of this attack activity, a malicious shortcut sample named "WhatsApp.jpeg.lnk" was associated with the Antiy Cyber Ultrain Threat Intelligence Analysis Subsystem. The malicious shortcut sample uses the system tool MSHTA Load and execute the remote HTA script, but because the remote HTA script link has expired, it is impossible to know the specific function of the HTA script.

Table 5-1 Examples of malicious shortcuts

virus name	Trojan[Downloader]/Win32.Agent.LNK
original file name	WhatsApp.jpeg.lnk

MD5	931A598836097496F21443AE864D160B
File size	2.07KB (2,121 bytes)
file format	Windows shortcut
creation time	2021-01-02 03:07:30 +00:00
Change the time	2021-01-02 03:07:30 +00:00
VT upload time	2022-02-03 15:21:42 +00:00
machine ID	user-pc

Figure 5-1 WhatsApp.jpeg.lnk

Subsequently, the Antiy Cyber Ultrain Threat Intelligence Analysis Subsystem is associated with a batch of malicious shortcut samples used by attackers for testing, and the batch of test samples are all submitted to the VirusTotal platform by the same uploader.

Analysis of this batch of test samples shows that the attackers began to test malicious shortcut samples roughly in August 2021, and the early malicious shortcuts mainly invoked MSHTA through CMD to execute remote HTA script files, and later used MSHTA directly. Execute remote HTA script files.

Table 5-2 Attacker test samples

MD5	file name	MachineID	Change the time	VT upload time
5ACF14897F3EFFF3D60AEE7A76C4753D	WhatsApp.jpeg.lnk	user-pc	2021-01-02 03:07:30 +00:00	2021-11-04 19:34:46 +00:00
34A84FA5EF9E5F388D7FEA9D91140FC5	WhatsApp.lnk	user-pc	2021-01-02 03:07:30 +00:00	2022-02-12 13:09:35 +00:00
62FE722B2BF323B318BA1D9C24FDEC51	WhatsApp.lnk	desktop-41oq5ea	2021-08-06 18:52:32 +00:00	2022-02-12 13:10:49 +00:00
CC53E7AEF38AC57499AEB0B1ED3909C9	WhatsApp.lnk	desktop-41oq5ea	2021-08-06 18:52:32 +00:00	2022-02-12 13:12:28 +00:00
4D12C03CE1F90E329F28CA194ABAB826	WhatsApp.lnk	desktop-41oq5ea	2021-08-06 18:52:32 +00:00	2022-02-12 13:14:29 +00:00

Through a comprehensive analysis of the malicious shortcut samples of the Confucius organization captured this time, it is found that the malicious LNK samples used by the SideWinder organization have differences in "machine name", "creation time", "modification time" and "disk drive identifier", etc. There is a lot of overlap where the "disk drive identifier" as the disk identifier of the machine that creates the malicious shortcut file is unique in itself. Therefore, Antiy CERT guessed that there is a shared tool between the SideWinder organization and the Confucius organization.

In fact, it is not uncommon for major Indian APT organizations to share code and tools with each other. For example, Trend Micro, a foreign security vendor, has repeatedly disclosed that there is a relationship between Confucius, Urpage and White Elephant to share code and assets [6] .

Now, from Antiy CERT finding that there are tools shared between SideWinder and Confucius, it can be seen that more and more Indian APT attack organizations will share tools and codes.

Table 5-3 Metadata comparison of malicious LNK samples used by Confucius and SideWinder

	The Confucius malicious LNK sample captured this time	Malicious LNK sample used by SideWinder group
MD5	931A598836097496F21443AE864D160B	DCFC26743D5E2897112626F67612067D
file name	WhatsApp.jpeg.lnk	luckydrawaugust2021.pdf.lnk
machine name	user-pc	user-pc
local base path	C:\Windows\System32\hsmta.exe	C:\Windows\System32\hsmta.exe
relative path	..\..\..\..\Windows\System32\mshta.exe	..\..\..\Windows\System32\hsmta.exe
command line arguments	https://t7g5c.app.link/qweqweqw	https://luckydraw.csd-pk.co/137/1/39/2/0/0/1812896830/tFUcuCDhCs3bJtZXyEgIY7JY0qsxlMwp0909d81c/hta
creation time	2021-01-02 03:07:30 +00:00	2021-01-02 03:07:30 +00:00
Change the time	2021-01-02 03:07:30 +00:00	2021-01-02 03:07:30 +00:00
interview time	2021-01-02 03:07:30 +00:00	2021-01-02 03:07:30 +00:00
Disk Drive Identifier	29ebe0d2-885f-4b6f-9277-80f9904dafe4	29ebe0d2-885f-4b6f-9277-80f9904dafe4

0 6

Attack Mapping from Threat Framework Perspective

This series of attacks involves 27 technical points in 12 stages in the ATT&CK framework. The specific behaviors are described in the following table:

Table 6-1 Description of technical behavior of Confucius' attack activities

ATT&CK stage	specific behavior	Notes
reconnaissance	Collect victim identification information	Collect target email account information for targeted delivery of emails in subsequent phishing attacks
	Search victim-owned websites	Search the target official website for subsequent phishing attacks to build counterfeit websites
resource development	Get infrastructure	Purchase servers for phishing websites, mount servers, C2 servers, etc.
initial visit	Phishing	Deliver spear-phishing emails with malicious links to targets
implement	Utilize command and script interpreters	Downloader Trojan using PowerShell to load malicious payload, written in JScript language
	Utilize scheduled tasks / jobs	Use Windows Task Scheduler to regularly execute C# stealing Trojans and C++ backdoor Trojans
	induce users to execute	Use malicious macro documents with lure content to induce target execution
Persistence	Utilize scheduled tasks / jobs	Use Windows Task Scheduler to regularly execute C# stealing Trojans and C++ backdoor Trojans
	Bootstrap or login with autostart	Using the registry run key to execute a C++ backdoor trojan
defensive evasion	Obfuscated files or information	Using QuasarRAT obfuscated with Eziriz .NET Reactor obfuscator
	Execute signed binary proxy	Use the system tool Rundll32 to execute the C++ backdoor Trojan, and use the system tool M shta to execute the malicious HTA file
credential access	Get credentials from where passwords are stored	Use C# stealing Trojans and C++ backdoor Trojans to steal target password files
	input capture	Using a keystroke stealer trojan collects the target's keystrokes for credentials
Find	discovery process	Use the C++ backdoor Trojan to obtain information about the currently running process of the target
	Discover files and directories	Use C# stealing Trojan and C++ backdoor Trojan to obtain target file and directory information
	discover network shares	Use C++ backdoor trojan to get target shared folders and drives

	Query the registry	Use C++ backdoor Trojan to query target registry information
	discovery software	Use C++ backdoor Trojan to obtain target installation software information
	Discover system information	Use C++ backdoor Trojan to obtain target system information
	Discover system network configuration	Use the C++ backdoor Trojan to obtain the network configuration information of the target system
Lateral movement	Transfer files or tools laterally	It is speculated that the attacker will use the penetration tool to move laterally on the intranet
	automatic collection	Use C# stealing Trojan and C++ backdoor Trojan to automatically collect target file information
collect	input capture	Use the keystroke stealer to collect the host's keystroke behavior
	Collect removable media data	Use C# stealing Trojan, C++ backdoor Trojan to collect target removable media data
command and control	Use application layer protocols	C# downloader Trojans and C# stealth Trojans use application layer protocols such as HTTP/HTTPS
	Automatic exfiltration data	Most of the tools in this activity automatically transmit the stolen data to the outside world
data exfiltration	Limit transfer data size	When using the C++ backdoor Trojan to upload files, limit the size of each upload to 1 byte

The ATT&CK framework diagram of the behavioral technical points of the Confucius organization-related attack activities is shown in the following figure:

Figure 6-1 ATT&CK mapping map corresponding to Confucius attack activities

0 7

Summarize

Among the APT attack groups from India, Confucius has no special features in attack weapons, code quality and vulnerability exploitation, but in the use of social engineering methods, it can be said to be "out of the pack". Especially in the attack activities in recent years, the Confucius group used more abundant social engineering methods to The phishing websites, spear-phishing emails, bait PDF files and malicious macro documents it constructed are all harmful to the target. Full of allure.

At the same time, the organization used CloudFlare's CDN acceleration service to hide the real IP address of assets, restrict access to IP geolocation, modify the timestamp of malicious payloads, and use encrypted malicious macro files in the attack activities, which also greatly improved security analysis. It is difficult for personnel to analyze and trace it.

Appendix 1: Some IOCs

Part MD5

021C535B8E70E9EFA74512DB647EF011
04F9B8DDD038E3D3DA3AB54AEBE73687
06B5A67BF37FED5B92C2211F342D7F0A
08B9C6AEFF78A30BE44694BB650EC198
0A1C6D9CD67172995D22FA54946662F0
15AE0E6E5B449797F4080E1E9A1ECC3F
17CB582F64A32C584DF68AEEF23E25F6
3DA30534B377B01CCAA3BF25F93AF1BA
3E3EC6645D75ED83C0C57E3151917B96
3FCFE20A4D3C5CD07944328DF25C81C2
457101EA5C30C53F9381D7E9AA6432A4
46417AD0FC33783C298B7441ACED2C1A
78EA0072E01F9BEC53D414C2CAD7C497
84D68E7B3AACF245D0C60F94A8D0AC4A
8736492918F8836D13DEFC6525540610
9120216CAE280E802FA22AB29A346119
92A0947B1A2CB8CFD645ED585E2001D1
A52E4EEB2BF7F1BFDAC3E3C0673ECE5F
A8169881B8552852F0D117FDD743F5E0
B426CE9179226681043CE8ED3ABCA862
BDF4DEF26EFBF676BB020B4BE49F9011
BEC908D62554CD16BD857A692BEF6FC6
C004DC680A8B74B3C99137A73AFE46D7
C676EB09E74308A879658FDA6FCB74FC
C7E1B92397E1C563E9FAA222CBF39BE7
DEF6F71E3A21F99F9494A4CB1D8D4279
E05AF60FBB3EC9110ACBF38CD1071F52
F6DE9D853EF1B802FC1EF34BD0787ABA
FFCEF12B4AB6DE46454D9AFA1E55379E

Partial URL

http://185.203.*.42/uphta/z.vbs
http://classcentral-*.ddns.net/TNC/Class_Central.zip
http://dump*ngs.ml/Jdsuifyiusdyf.txt
http://dump*ngs.ml/Kewuiuryjd.txt
http://dump*ngs.ml/ZeroToleranceMonth.jpg
http://fil*oni.digital/HprodXprnvlm1.php
http://fil*oni.digital/VueWsxpogcjwq1.php
http://fu*tifu.live/ksjdSudh/hsfuYNm.txt
http://msd*igns.site/google/goopdate.dll
http://office*oud.store/update.dotm
http://pirna*m.xyz/Bdsfunklo.php
http://pirna*m.xyz/Vksufnduw.php
http://pirna*m.xyz/YblSNyirp/
http://release.word*date.net/object/encode
http://thak*aiya.xyz/Bdsfunklo.php
http://thak*aiya.xyz/SuMkdsfui.php
http://thak*aiya.xyz/Vksufnduw.php
http://webi*taller.online/V6.exe
http://webi*taller.online/office/updates
http://word*date.net/micro/upload
http://word*date.net/wordpress
https://www.fbr-no*ce.com/iris/file.php?file=FBR
https://t7g*c.app.link/Kit8V9GsIqb
https://t7g*c.app.link/RKQX1PtSJqb
https://t7g*c.app.link/qweqweqw

Partial Domain

classcentral-*.ddns.net

dump*ngs.ml
fil*oni.digital
fu*tifu.live
msd*igns.site
office*oud.store
pirna*m.xyz
release.word*date.net
thak*aiya.xyz
webi*taller.online
word*date.net
fbr-no*ce.com
t7g*c.app.link

Appendix II: References

[1] Palo Alto Networks : Confucius Says...Malware Families Get Further By Abusing Legitimate Websites

https://unit42.paloaltonetworks.com/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

[2] Pakistan NTISB: Spam Mails for Govt Jobs/Recruitments (Advisory No 13)

https://download1.fbr.gov.pk/Docs/202242912443472AdvisoryNo13-2022.pdf

[3] Pakistan NTISB: Cyber Security Advisory No. 21 Spam Email-PMO

https://download1.fbr.gov.pk/Docs/20226271462135426Advisoryno21-2022.pdf

[4] Baidu Encyclopedia: Deep Links

https://baike.baidu.com/item/%E6%B7%B1%E5%B1%82%E9%93%BE%E6%8E%A5/8441834?fr=aladdin

[5] Qi Anxin: Operation Tibu - A retaliatory targeted attack from the South Asian APT organization "Moruoshu"
https://ti.qianxin.com/uploads/2020/09/17/69da886eecc7087e9dac2d3ea4c66ba8.pdf
[6] Trend Micro: Linking cyberespionage groups targeting victims in South Asia

https://www.first.org/resources/papers/tallinn2019/Linking_South_Asian_cyber_espionnage_groups-to-publish.pdf

past review

此图片来自微信公众平台
未经允许不可引用

此图片来自微信公众平台
未经允许不可引用

此图片来自微信公众平台
未经允许不可引用

此图片来自微信公众平台
未经允许不可引用

此图片来自微信公众平台
未经允许不可引用

预览时标签不可点

收录于合集 #

个

上一篇 下一篇

微信扫一扫
关注该公众号