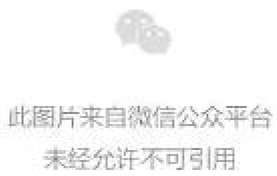
mp-weixin-qq-com.translate.goog /s/Nk2zml2d0HtK0hszyKW2Dw

[Advanced Threat Tracking (APT)] Patchwork organization update technology makes a comeback, launching another attack on domestic education and scientific research units



Shenzhan Intelligence Lab Sangfor *Qianlimu Security Technology Center 2023-04-20 11:45*
Sangfor Qianlimu Security Technology Center

gh_c644c6e98b08

Sangfor Qianlimu Security Technology Center focuses on the research and application of various technical fields of network security, including six technical laboratories and an innovation research institute, focusing on security technologies such as domestic and foreign vulnerabilities, offensive and defensive confrontation technologies, terminal security, advanced threats, and threat intelligence Professional research in the field, and finally empowered products.

published in Beijing

Included in the collection #Advanced Persistent Threat Tracking 51

overview

Recently, Sangfor Shenzhan Intelligence Laboratory and Sangfor Anfu Emergency Response Center have monitored the latest attack trends of APT organizations on domestic universities and scientific research institutions, and combined with the analysis of the AI model of Sangfor Innovation Research Institute, the sample is attributed to the Patchwork organization launched the attack. Patchwork organization, also known as Mahacao, White Elephant, APT-Q-36, APT-C-09, is an overseas APT organization from South Asia. The organization mainly conducts cyber espionage activities against China, Pakistan and other Asian countries, mainly stealing sensitive information. Related attacks can be traced back to November 2009, and are still very active. In the attacks against China, the organization mainly attacks government agencies, scientific research and education, and the scientific research and education are the main areas.

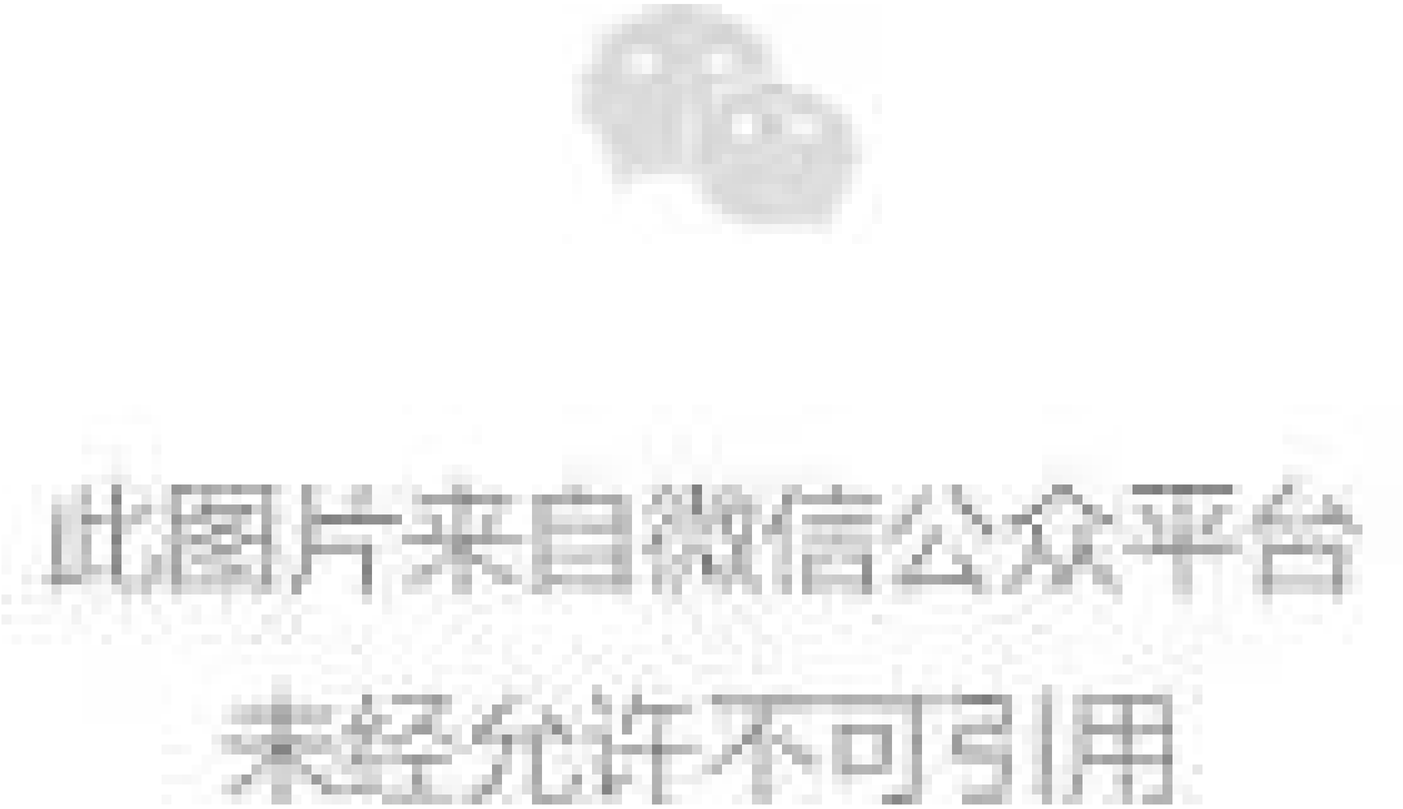
During this attack, we detected that Patchwork used phishing emails to attack universities and scientific research institutions. The email attachments related to this incident were titled "Guiding Opinions on the

Protection of Women's Rights and Interests Revised by the All-China Women's Federation in 2023", "Advanced Notice on 2023 Project Application Guidelines for 4 Key Special Projects including Structure and Composite Materials", "Changjiang Design Group Co., Ltd. 2023 Recruitment Announcement".

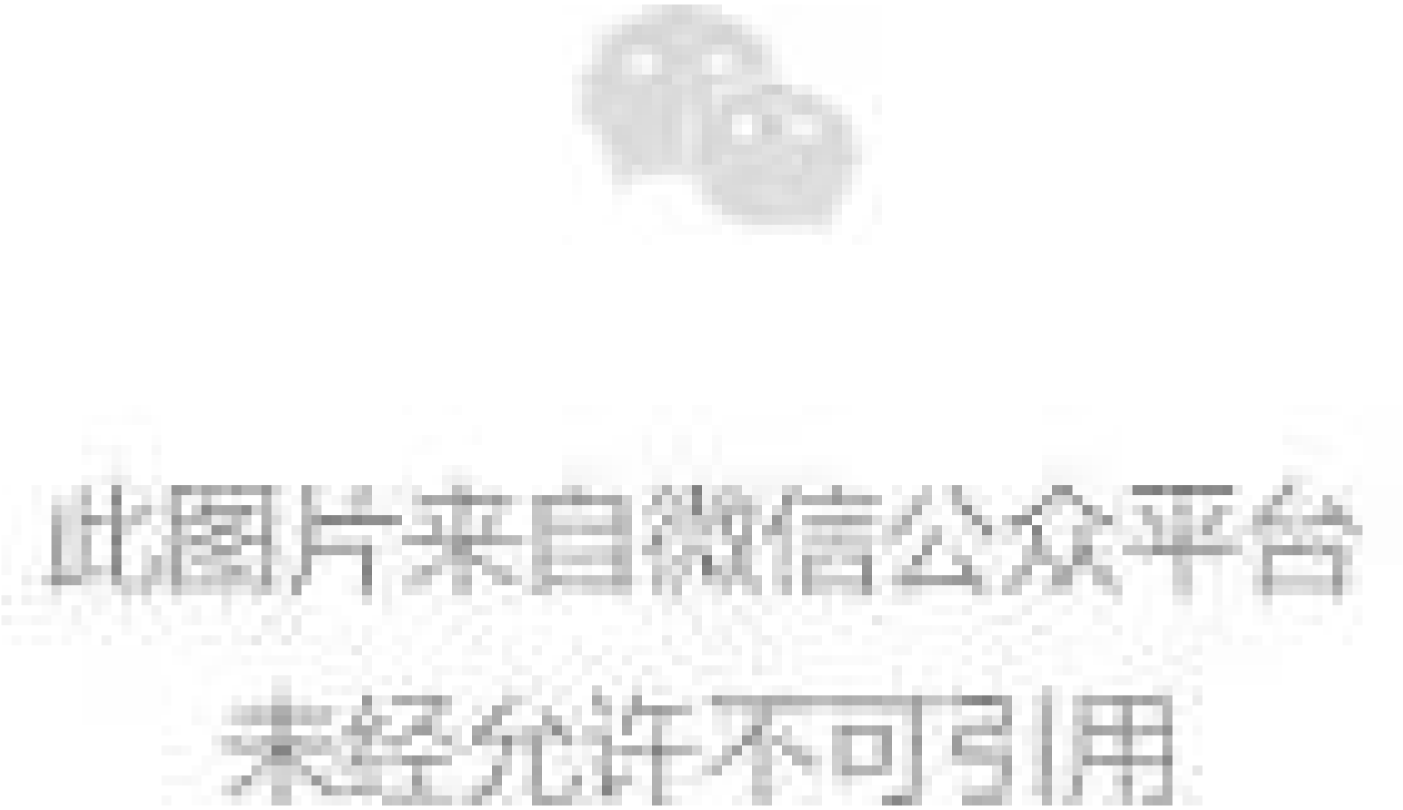
The content of the email lures users to open the compressed file with a password on the grounds of sexual harassment incidents in the workplace or project declaration notices. The compressed file contains a malicious lnk file, which is used to download the second stage of BADNEWS remote control. Through analysis, we found that the organization has updated the BADNEWS used in the past, improved the calling order and method of key functions, replaced the control instructions and adjusted the implementation of corresponding functions, and replaced some key strings.

analyze

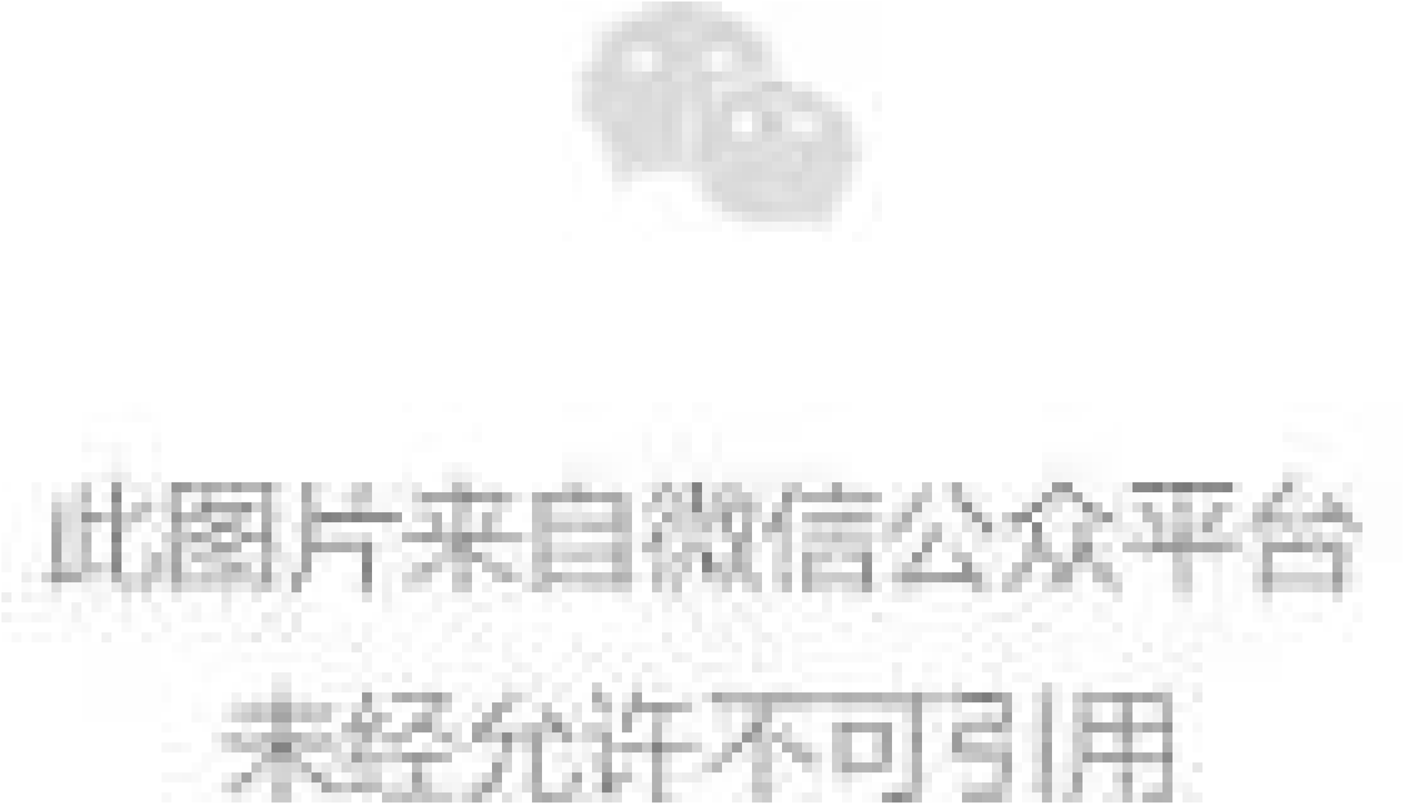
In this attack, the decompressed file is a double-suffix file of .pdf.lnk, which is actually an lnk file. After double-clicking, the powershell command in the file will be executed. Since the lnk file does not display the suffix name, you can use the "dir" command of cmd or right-click the file properties to view the file to prevent malicious phishing files from being executed. The following table shows the detailed information of the file.



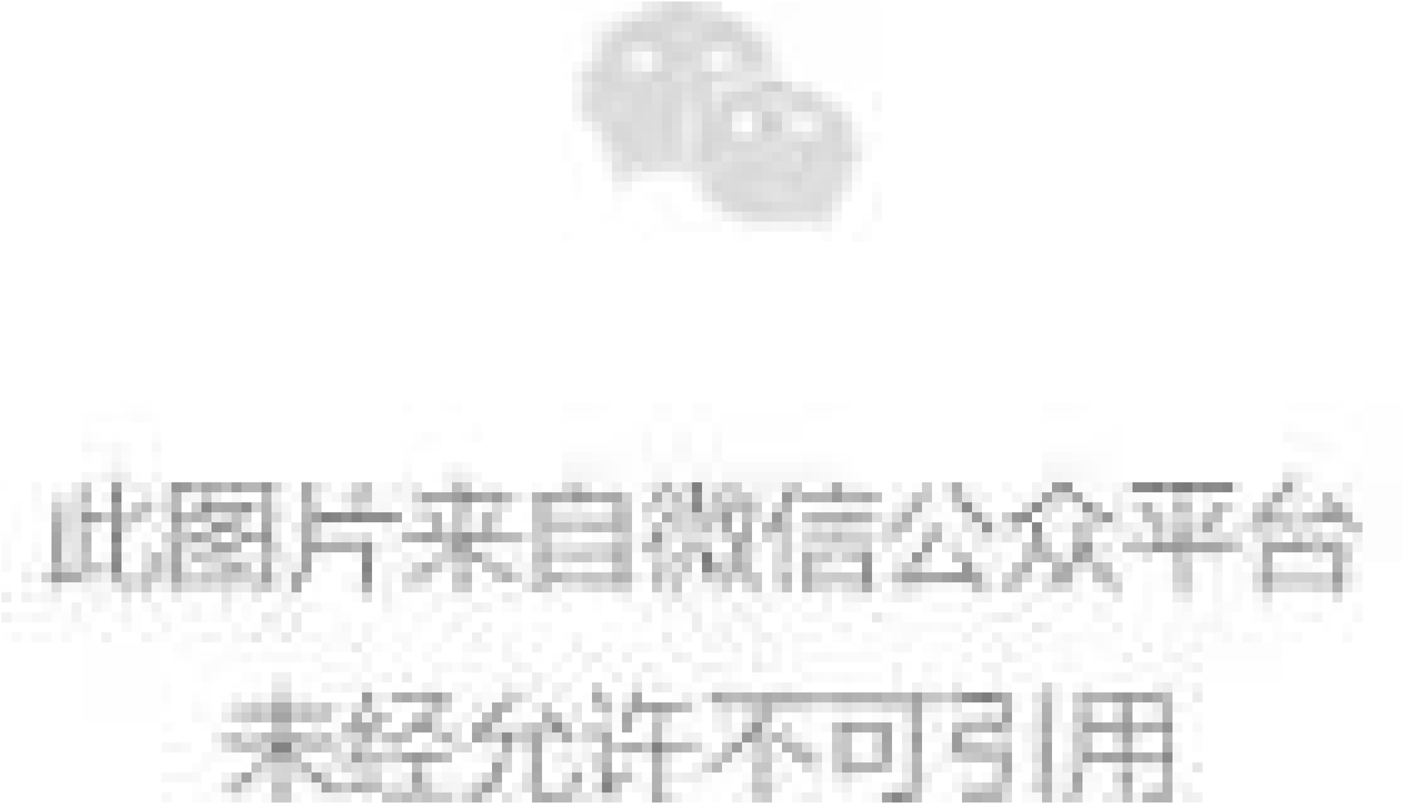
The LNK file will download the decoy file from https[:]//shhh2564.b-cdn.net/abc.pdf and open it, then download the file from https[:]//shhh2564.b-cdn.net/c to C: \ProgramData\Microsoft\DeviceSync\p, copy the p file to OneDrive.exe in the same path, delete the p file, and finally create a scheduled task to execute OneDrive.exe every 1 minute.



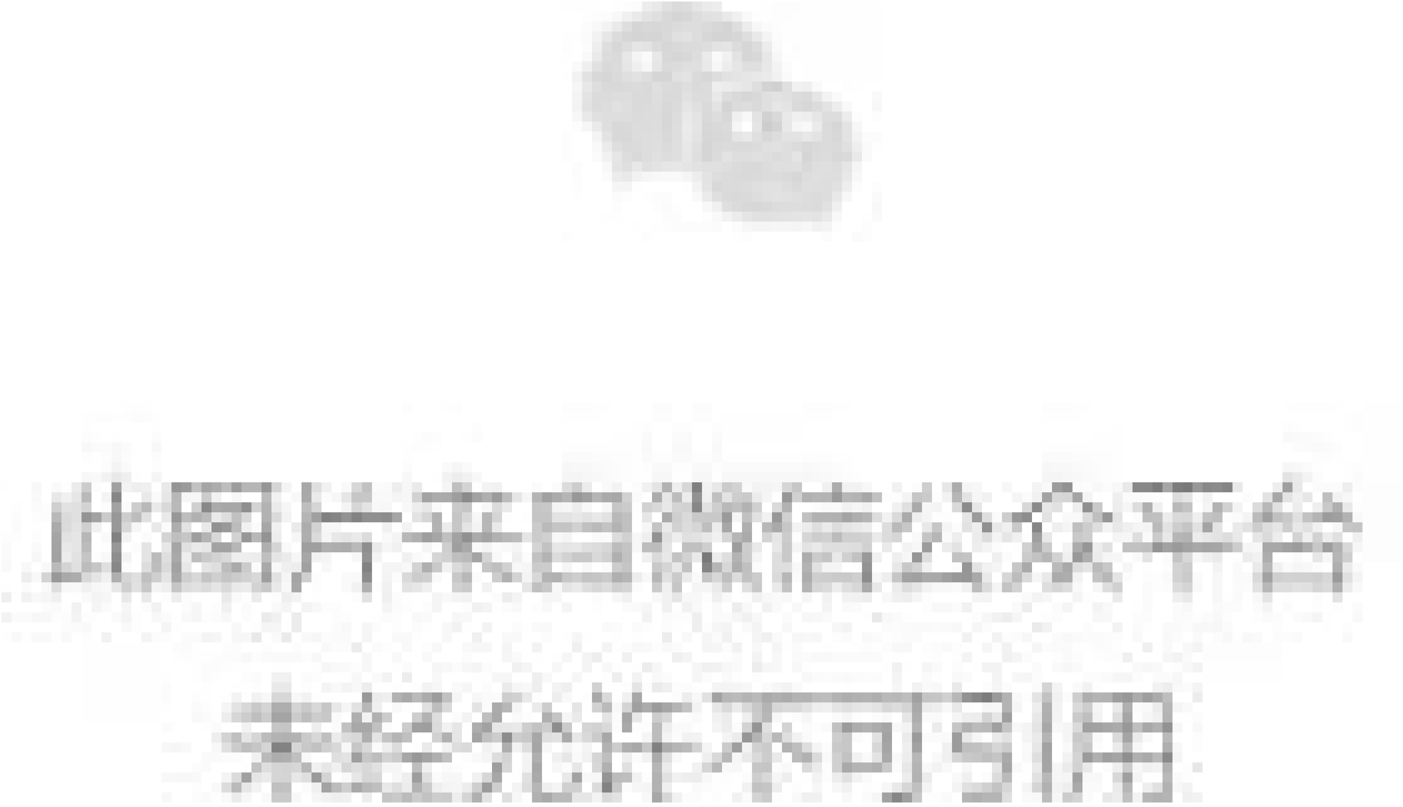
The downloaded OneDrive.exe is actually Patchwork’s BADNEWS remote control program, which provides functions such as file download and execution, file upload, command execution, stealing keyloggers, and obtaining screenshots. The detailed information is as follows.



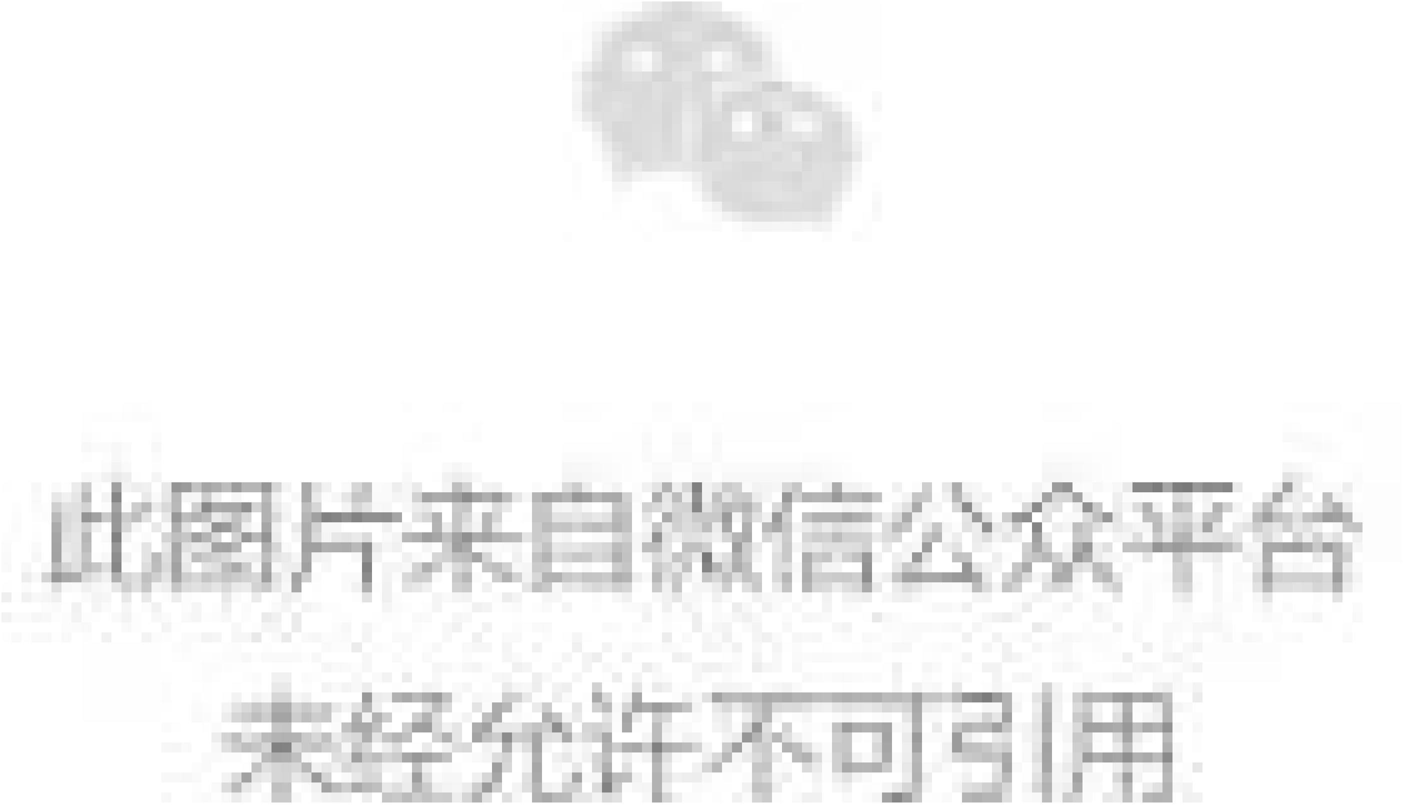
The remote control first obtains the time zone name of the machine, and only when the time zone name is "China Standard Time" will it perform subsequent malicious operations.



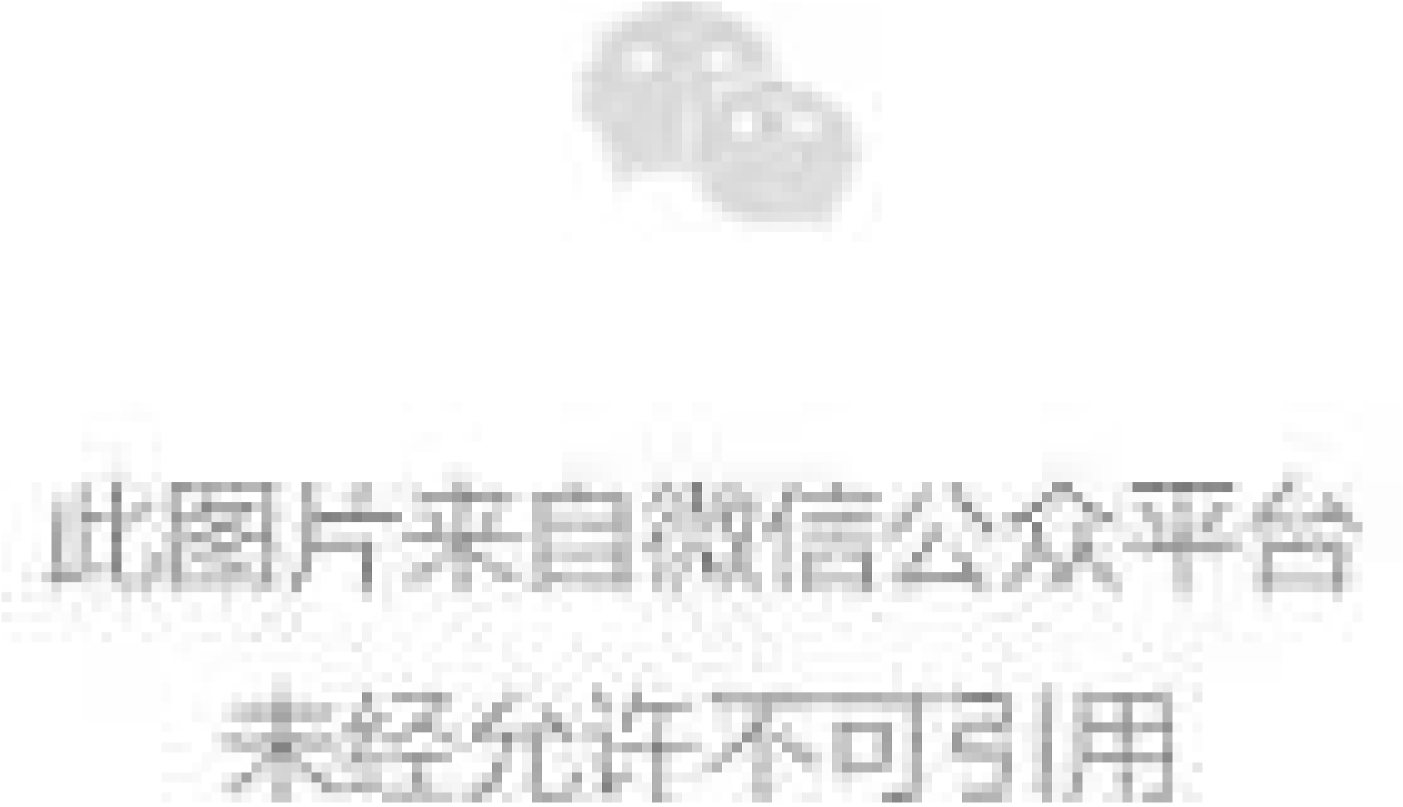
Then create a mutex "qaex" to maintain a single instance, and then use SetWindowsHookExW to register a keyboard hook.



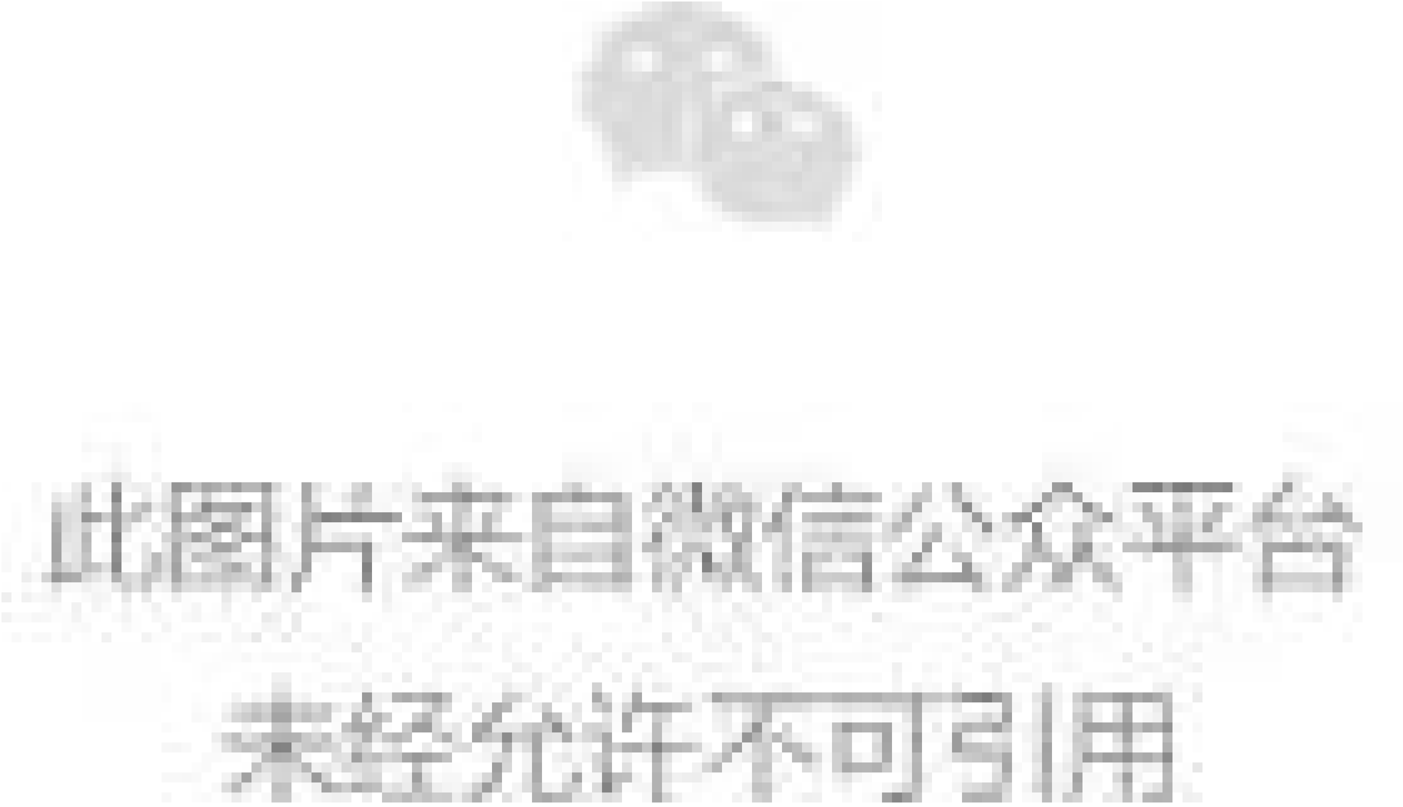
Save the captured keylogger as text in the kednfbdnfby.dat file in the %temp% directory, instead of the previously used "kpro98.dat" file name.



Use normal WEB services (myexternalip.com, api.ipify.org, ifconfig.me) to obtain the host IP external network address.

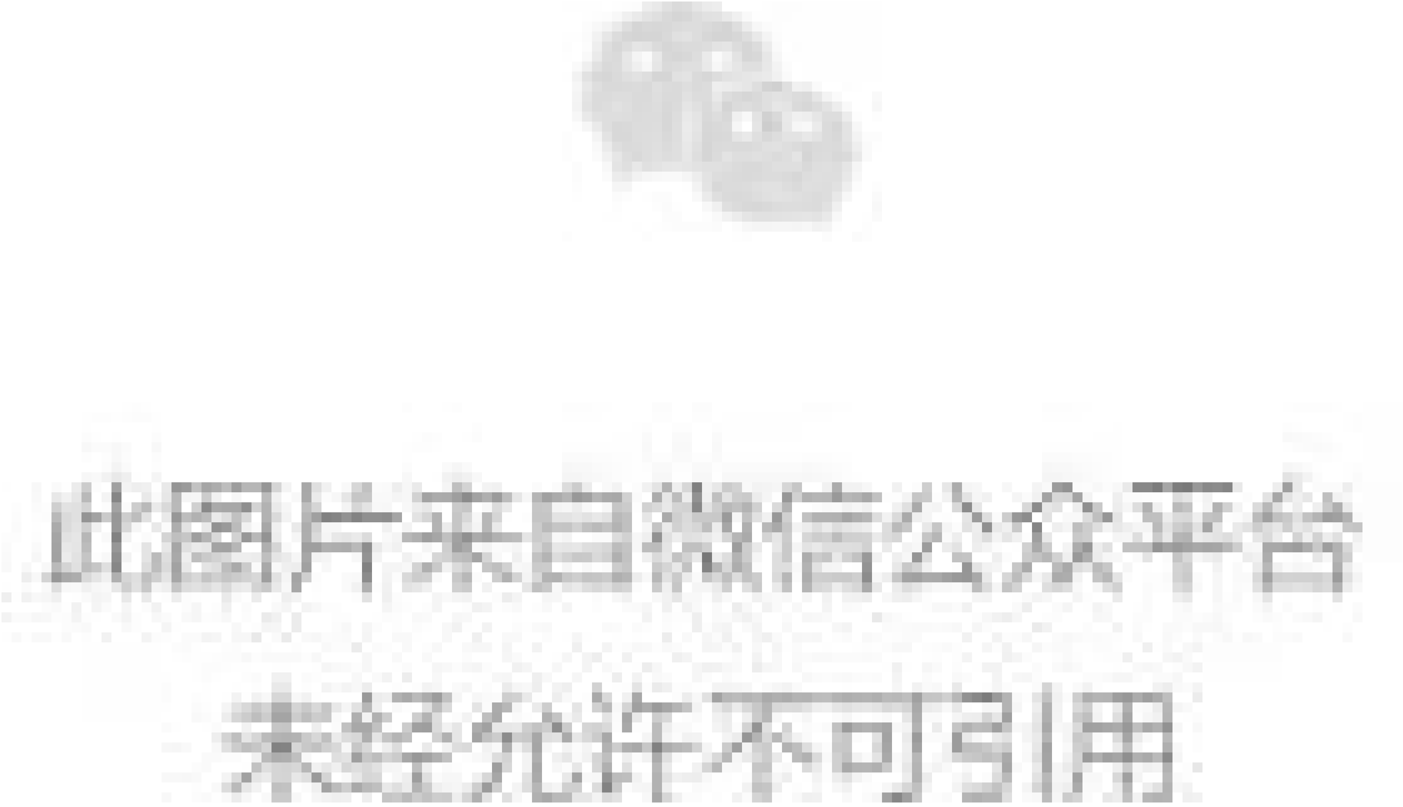


Use the external network IP address obtained in the previous step to query the name of the country to which it belongs in WEB services such as (api.iplocation.net, ipapi.co)

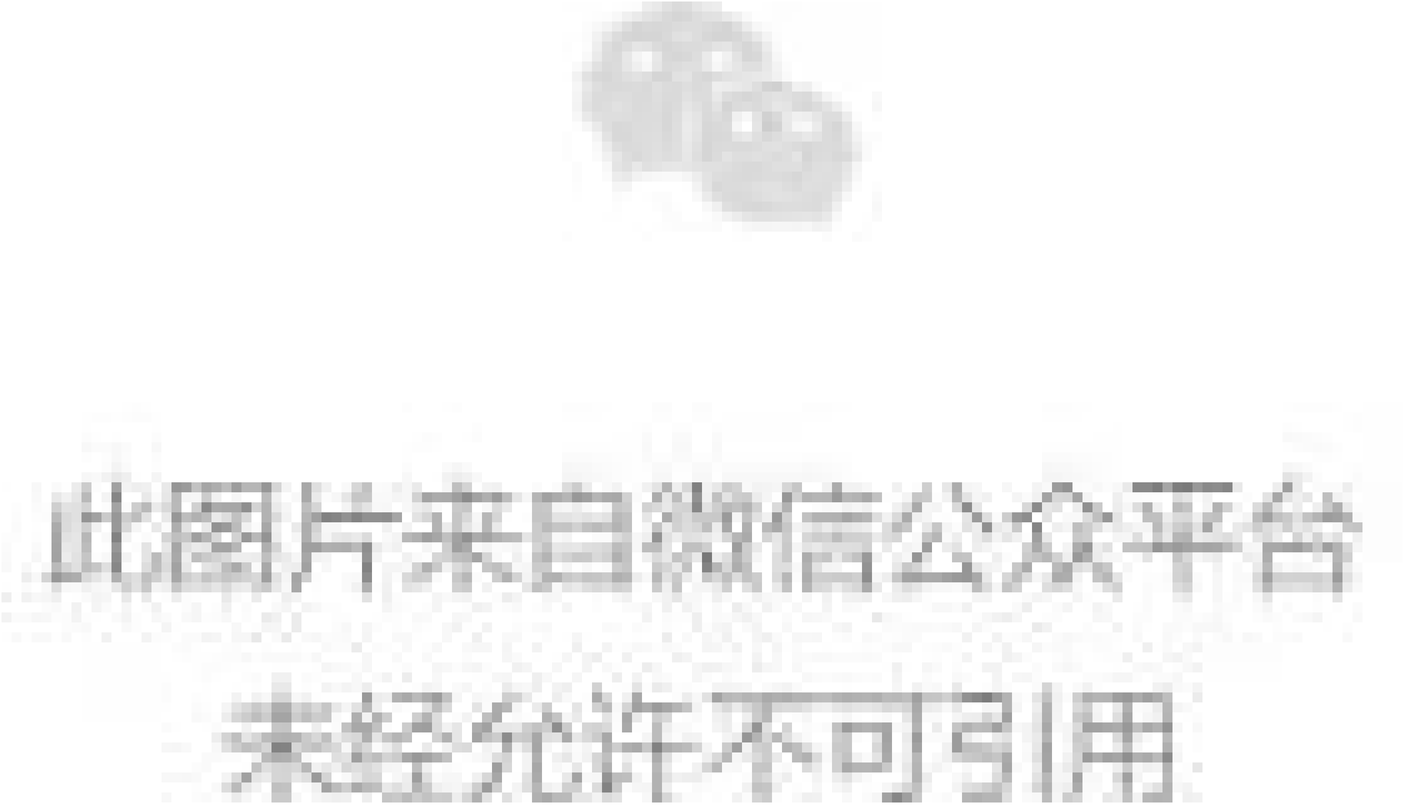


Finally, the obtained information is encrypted and stored in a string.

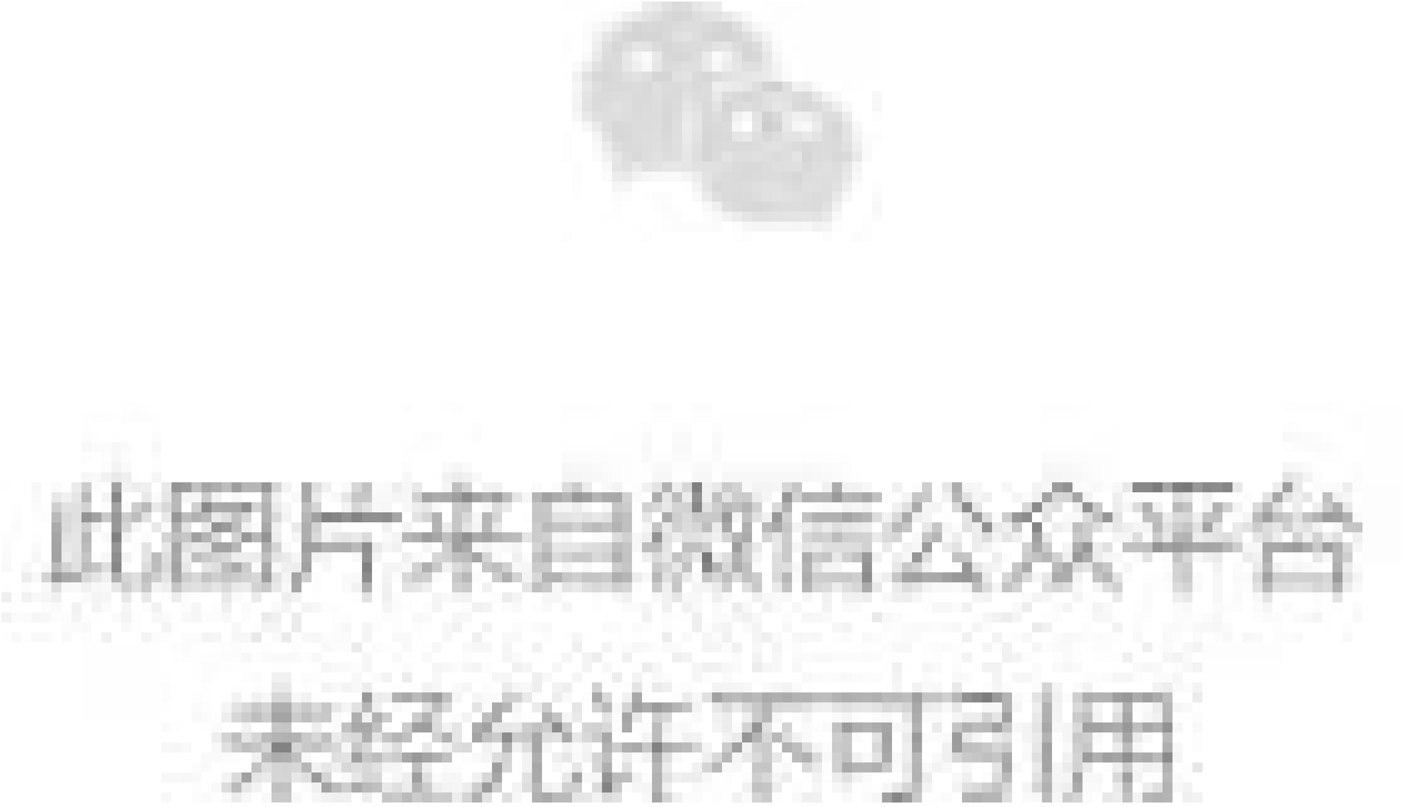
The information collected through the analysis is as follows:



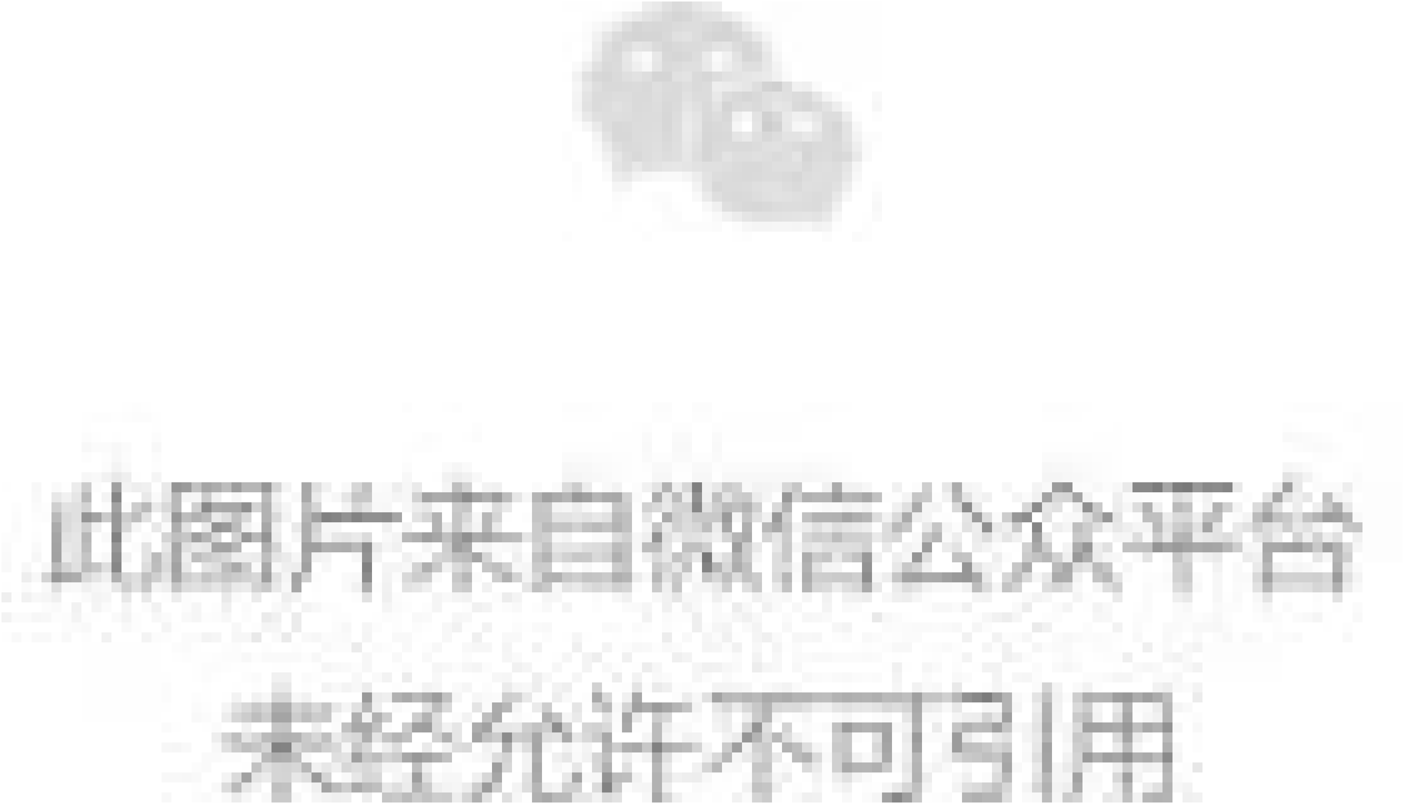
The collected information will be base64-encoded and encrypted in AES-128 CBC mode, and finally the encrypted data will be base64-encoded. The key used for AES-128 encryption is "qgdrbn8kloiuytr3", and the IV is "feitrt74673ngbfj". This encryption method is also applied to the data delivered by C2, which is hereinafter referred to as AES-128 encryption.



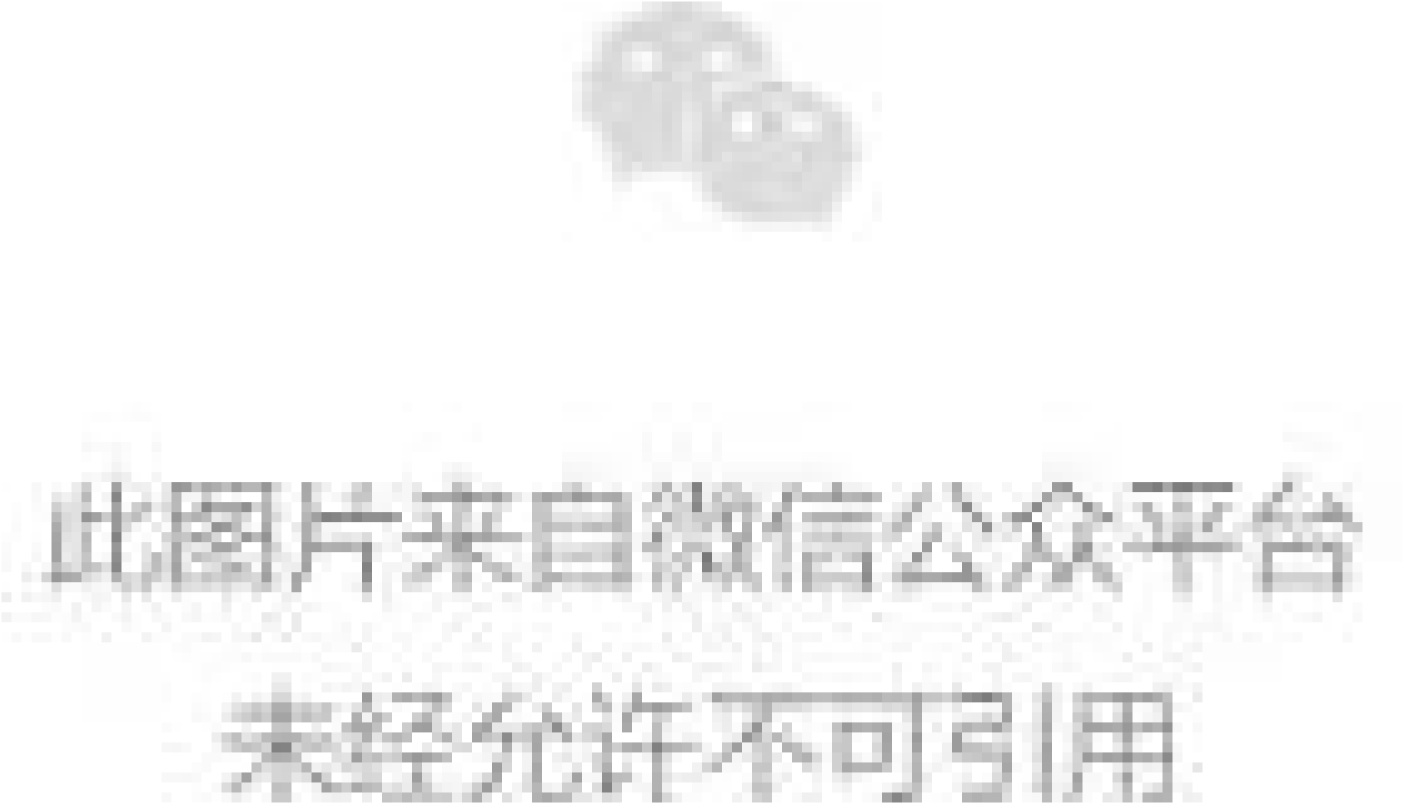
Then get the address of the CreateThread function, create 3 threads to communicate with port 443 of C2: charliezard.shop, the uri is /tagpdjjarzajgt/cooewlzafloumm.php, the communication content will use AES-128 encrypted data, and the maximum data transmitted each time is 5000 words before encryption Festival.



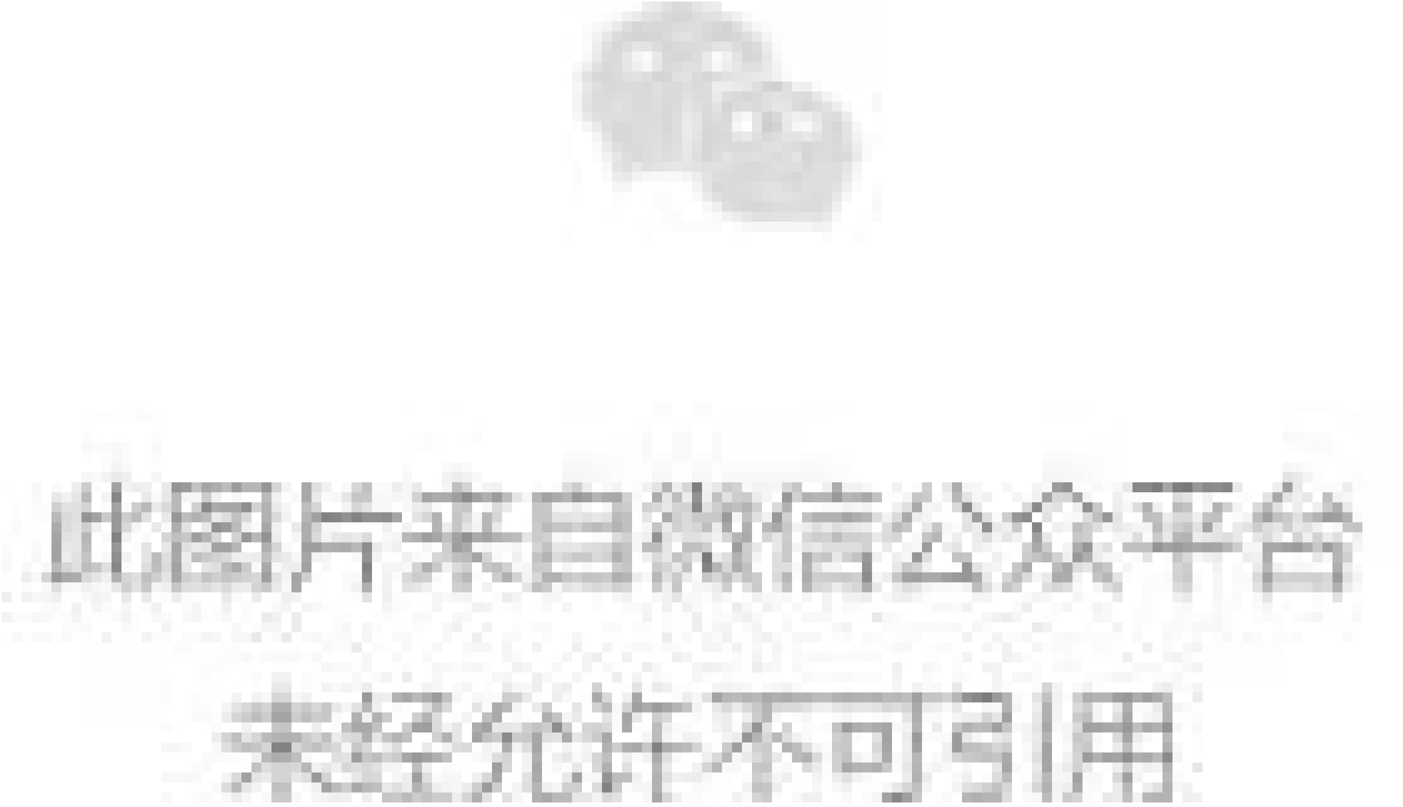
The thread FUN_00409900 is responsible for sending the collected information to C2 by POST, and the content is the encrypted data of the collected system information. After the sending is completed, it enters a random sleep of 1-101 seconds. After the sleep is over, the process of sending information is repeated to verify whether the host is online.



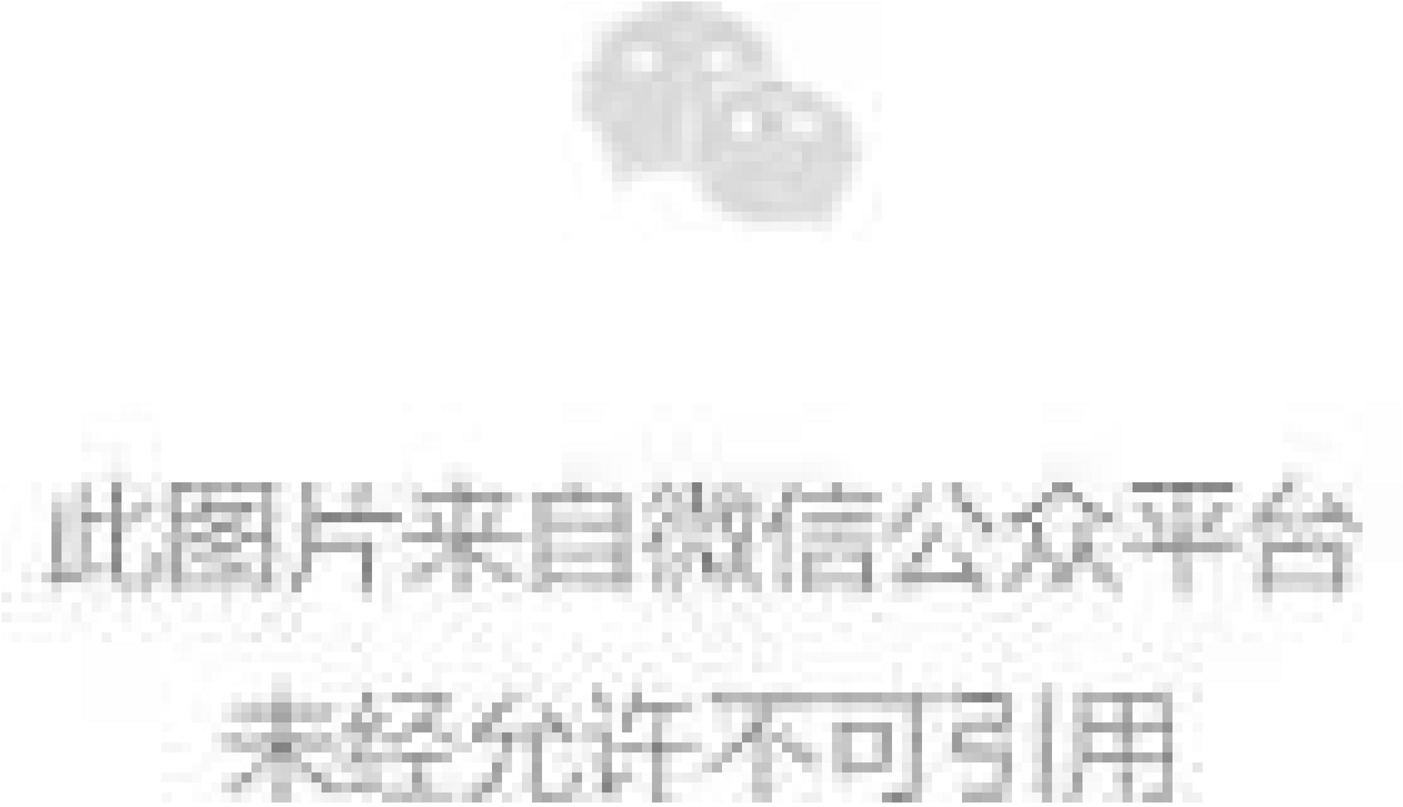
The thread FUN_00409440 is responsible for collecting more complete system information. It encrypts the SmBIOS uuid value as the unique identifier of the machine using the above method and sends it to C2 as the uidfguu parameter value. After receiving the same uuid encrypted data, it will further collect system information.



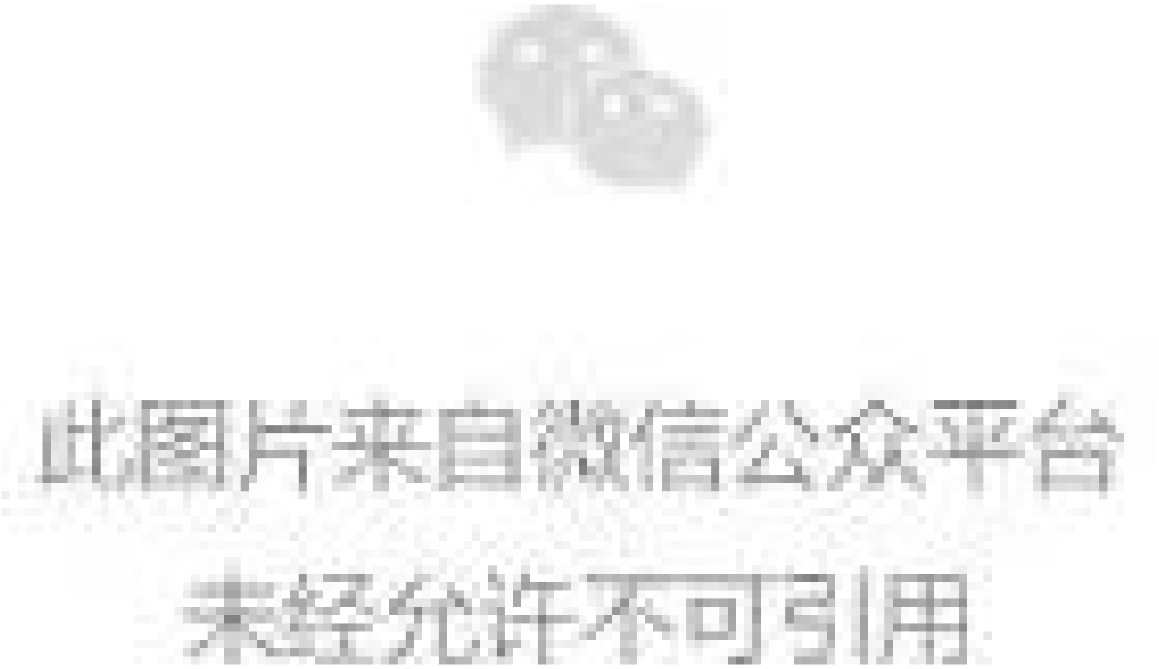
Create a cmd process to execute the whoami command, ipconfig /all command, ipconfig /displaydns command, systeminfo command, and tasklist command. After collecting the current user name, complete network configuration information, DNS cache information, complete system information, and ongoing process information, use AES-128 to encrypt the data, add it to the endfh parameter and send it to the C2 with the unique identifier uubsin parameter.



The thread FUN_00451a8 is responsible for responding to the instructions issued by C2, sending the uugmkis parameter with the machine unique identifier to obtain the instructions issued by C2.



The command format is: command$option1$option2, command and option 1 need to be decrypted by AES-128, option 2 is not used, and the data returned to C2 is also encrypted by AES-128, compared with the previous BADNEWS For the implementation of each control command, we found that the organization abandoned the original link of saving the execution result to a file, and directly encrypted the data and sent it back to C2. After analysis, the functions of all commands are as follows:

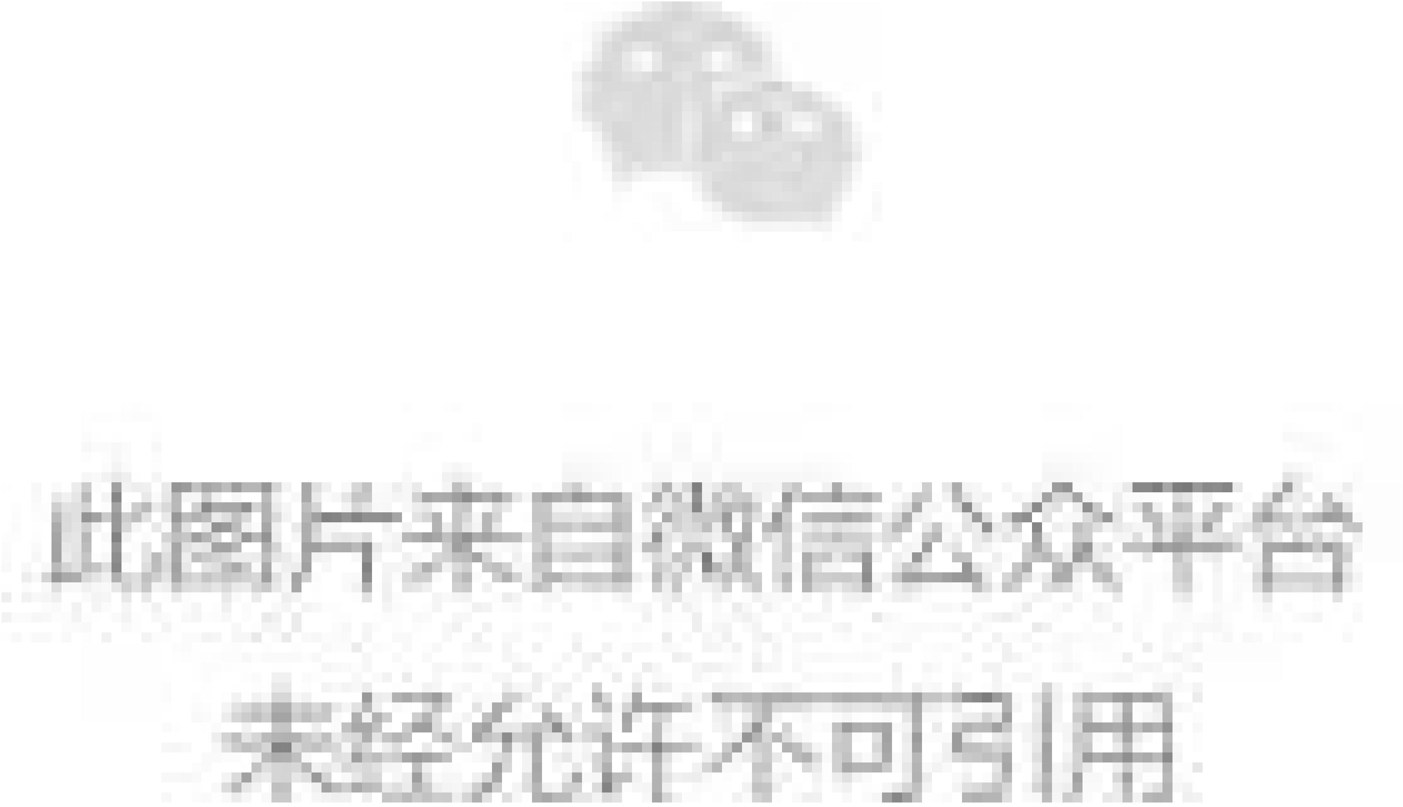


Attribution

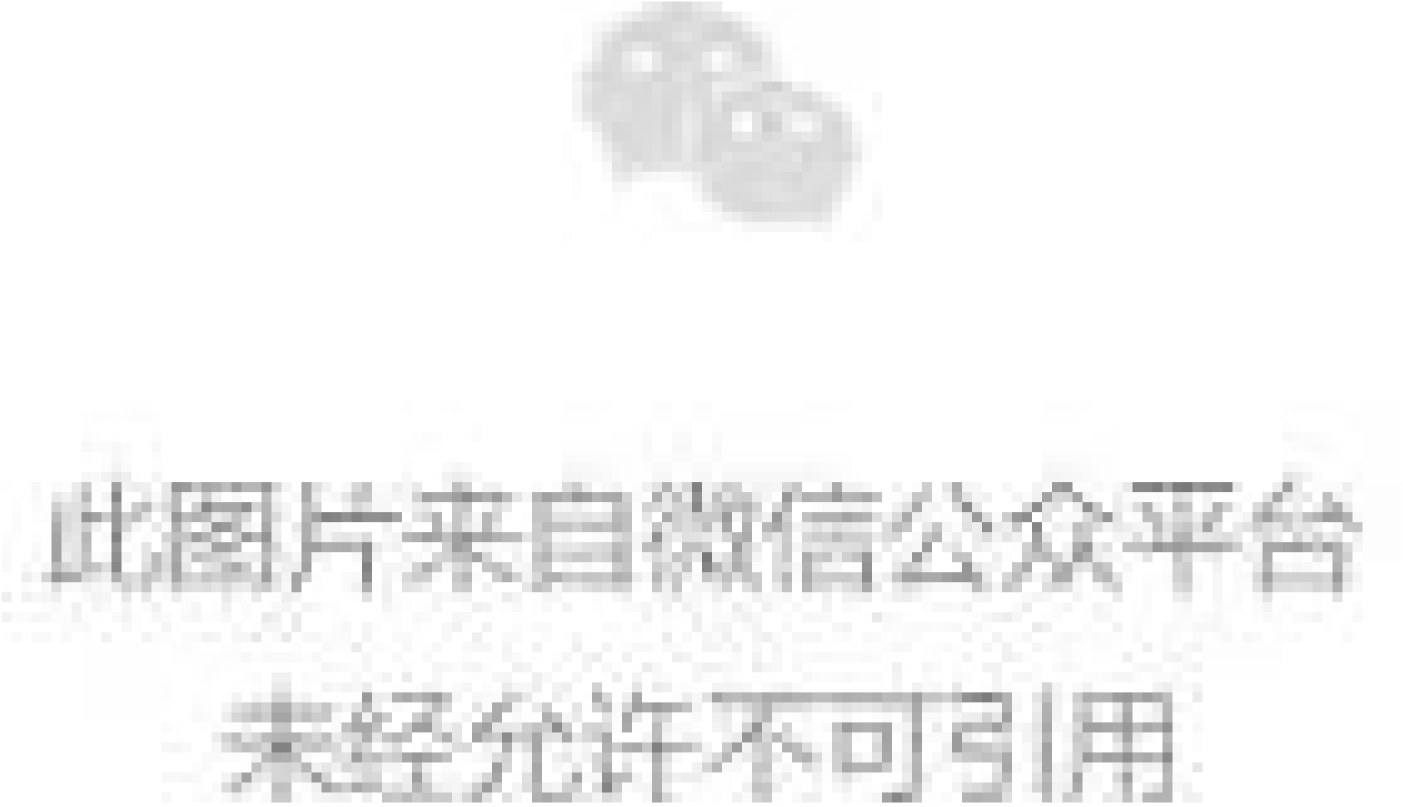
Traceability Attribution - File Attribution:

By analyzing the storage path C:\ProgramData\Microsoft\DeviceSync of OneDrive.exe, which is one of the commonly used file paths of the organization, and analyzing the downloaded RAT components, its code logic, communication mode, and URL format conform to the organization’s proprietary far Control the characteristics of BADNEWS.

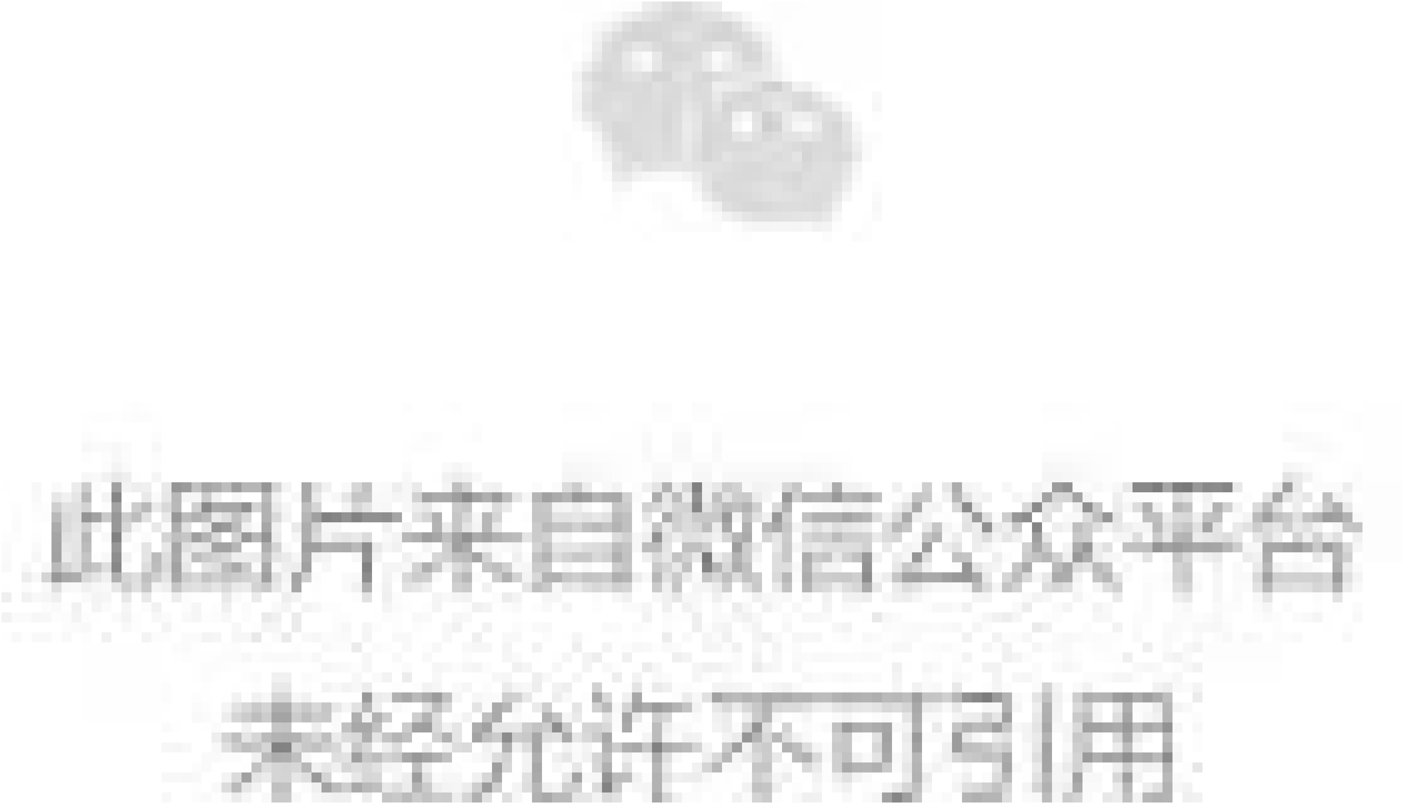
The similarity to BADNEWS is in the code procedure for getting the time zone name.



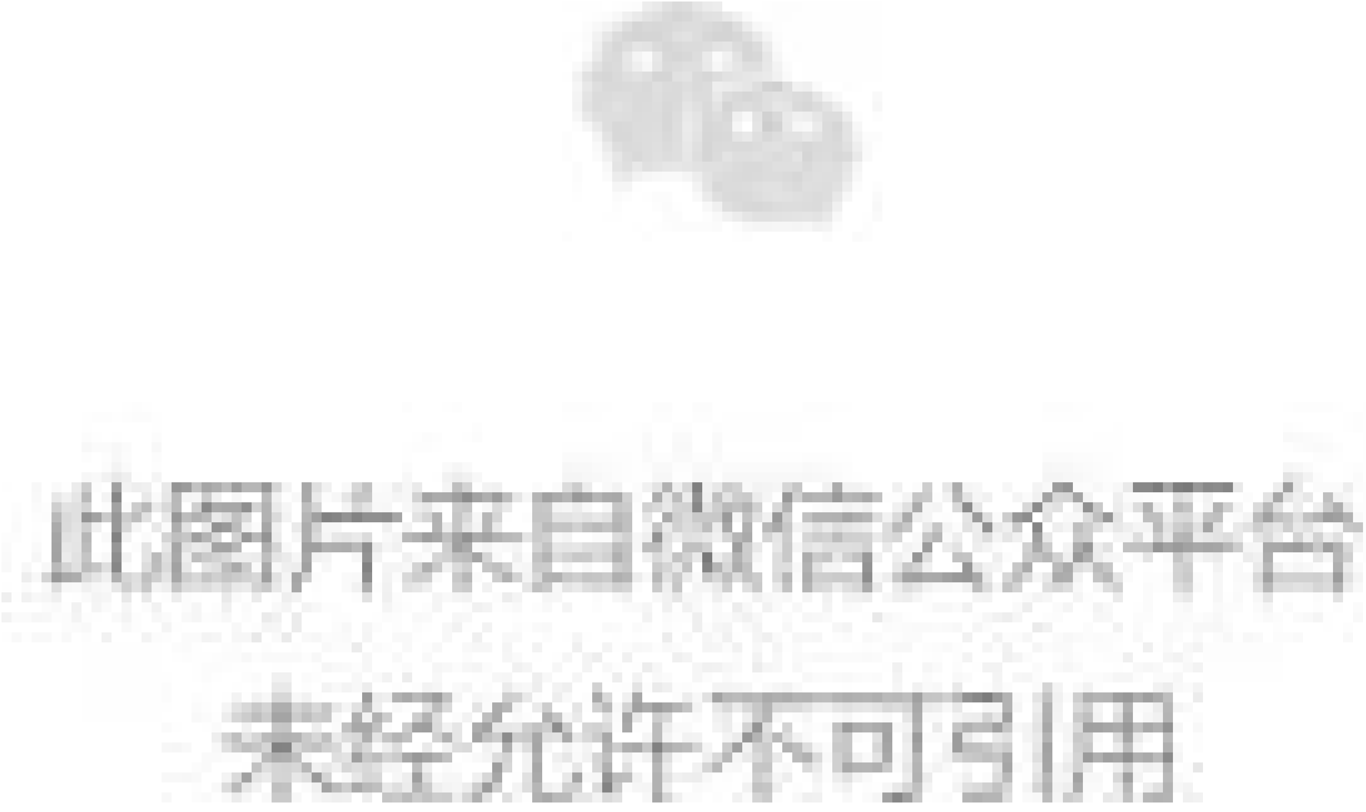
Check if it is the time zone of the target country



In addition, through the intelligence data accumulated by the Shenzhan Intelligence Laboratory, the AI model of the Sangfor Innovation Research Institute also attributed the sample to Maha Grass, which is the Patchwork organization.



IOCS



Summarize

Patchwork often uses harpoon attacks to attack targets, which is dangerous. Attacks are mainly aimed at industries such as education and scientific research institutions, and steal high-tech research materials or planning information of such units. Relevant industries and units need to be vigilant and strengthen network defenses. In this incident, the organization transformed the BADNEWS attack components and continuously strengthened its secret stealing, anti-analysis and anti-evidence capabilities. Security companies should strengthen the detection of related technologies.

Sangfor Blue Army Advanced Threat (APT) team focuses on the tracking and analysis of global advanced threat events . It has a complete set of automatic analysis and traceability system and external threat monitoring system, which can quickly and accurately analyze and correlate the attack samples used by APT organizations At the same time, it has accumulated and improved the detailed portraits of dozens of APT and cybercrime threat organizations, and successfully helped customers respond to and deal with many APT and cybercrime threat organization attacks. In the future, with the continuous escalation of security confrontation, threat organizations will study And using more new TTPs, **Sangfor Advanced Threat Team will continue to monitor and conduct in-depth analysis and research on new security incidents discovered around the world.**

reference link

https://www.freebuf.com/articles/paper/348148.html