Analysis of the Phishing Activity of the Dridex Banking Trojan Delivered by a Certain Institution in China by the TA575 Group

Harbin Institute of Technology and Antiy Joint CERT Laboratory

First draft completed: November 9, 2021

First published: January 28, 2022

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

1 Overview

In early November 2021, **Harbin Institute of Technology and Antiy Joint CERT Laboratory,** discovered multiple phishing email delivery activities targeting a certain institution in China during network security monitoring. After correlation analysis, it was confirmed that the purpose of this attack activity was to deliver the Dridex banking trojan. Through the correlation and tracing of the relevant TTPs in the activity process, it was finally determined that this attack activity came from the TA575 group. In 2020, the organization was first disclosed by security vendors for its attack activities. It is one of the organizations that spread the Dridex banking trojan. Once the target (victim) attacked by it is implanted with the Dridex banking trojan, it may also be subjected to further ransomware attacks[1]. It belongs to the TA series of organizations. This series of organizations is a collection of cybercrime organizations for the purpose of illegal economic profit. Most of the members of the organization use the infrastructure they have built to spread banking trojans through phishing emails or other means, build a huge botnet, and steal information and send ransomware to the target.

In this phishing campaign, the TA575 group used documents containing Excel 4.0 macros as attachments to drop and execute HTA files, which then downloaded malicious samples stored on social and cloud file storage platforms such as Discord, Dropbox, and OneDrive. Furthermore, due to a domain control environment signature within the HTA file code, this phishing campaign only targeted **endpoint systems within domain control environments**. Throughout the attack, the attackers employed obfuscation, macro code hiding, encryption, and exception handling to thwart analysis and detection. Analysis revealed that the malicious samples downloaded to the target environment were essentially loader for the Dridex banking trojan, whose functions included obtaining basic information about the target system, connecting to and transmitting data back to the C2 command-and-control (C2)

server, obtaining a list of P2P nodes, participating in botnet construction, obtaining subsequent modules, and carrying out secret theft or ransomware attacks. This indicates that once a user is infected with this banking trojan, they face security threats such as sensitive information leakage and system failures caused by ransomware.

According to correlation analysis, attackers have been spreading the Dridex banking Trojan via phishing emails since November 1, 2021. During this process, they abused relevant platforms to host the banking trojan and generate corresponding download links, resulting in a continuous increase in the number of malicious URLs generated. The phishing campaign monitored this time bears a high degree of similarity in relevant TTPs with attacks conducted by the TA575 group from February to October 2021. **Based on this information, it can be inferred that this campaign is a new wave of phishing campaigns launched by the TA575 group to spread the Dridex banking trojan since November 2021.**

It has been verified that **Antiy Intelligent Endpoint Protection System (IEP) can** effectively detect and kill the banking Trojan and provide practical protection for user terminals.

2 ATT&CK Mapping Diagram Corresponding to the Incident

This security monitoring found that attackers used phishing emails to drop malicious macro documents, which in turn spread the Dridex banking trojan. The ATT&CK mapping corresponding to this attack incident is shown in the figure below:

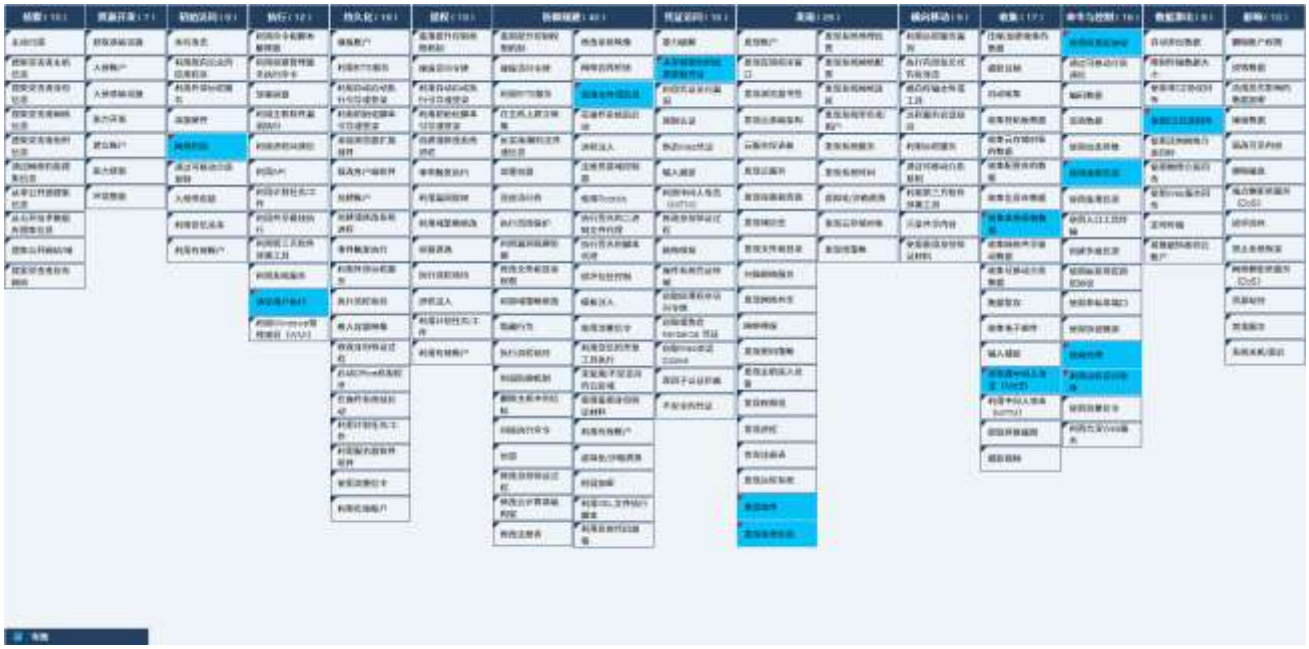


Figure 2

The following table lists the techniques used by the attackers in this incident:

Table 2-1 The incident corresponds to the ATT&CK technical behavior description table

ATT&CK Stage/Category	Specific Behavior	Notes
Initial access	Phishing	Deliver phishing emails
Execute	Induce users to execute	Trick the user into opening the document and enabling macros
Defense evasion	Obfuscate files or information	Use obfuscated VBS code
Credential access	Get the credentials from where the password is stored	Steal login credentials from web forms
Discover	Discover system information	Get the system machine name and domain name
	Discover Software	Get the list of installed software on the system
Collect	Collect local system data	Return system information
	Browser man-in-the-middle attack (MitB)	Hijack browser session information
Command and Control	Use application layer protocols	Transmit control commands via HTTP
	Use encrypted channels	Traffic encryption
	Use a proxy	The target host is used to proxy C2 traffic
	Use remote access software	The sample uses a V NC module

Data exfiltration	Use C2 channel for backhaul	Connect to C2 server and send back system information

3 Protection Recommendations

In response to this banking Trojan, Antiy recommends that enterprises take the following protective measures:

3.1 Enterprise Protection

(1) Strengthen terminal protection: Install anti-virus software. It is recommended to install **Antiy Intelligent Endpoint Protection System**;

(2) Strengthen 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. At the same time, avoid using the same password on multiple servers.

(3) Deploy an Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate timely detection of malicious code and its tracing back to its source. It is recommended to deploy the Antiy Persistent Threat Detection System (PTD), which uses network traffic as the detection and analysis object and can accurately detect a large amount of known malicious code and network attack activities, and effectively discover suspicious network behaviors, assets, and various unknown threats;

(4) Antiy Service: If you are attacked by malware, we recommend isolating the attacked host and securing the site while waiting for security engineers to investigate the computer. Antiy's 24/7 service hotline is: 400-840-9234.

3.2 Daily Mailbox Security Protection

(1) When receiving emails, confirm whether the source is reliable and avoid opening URLs and attachments in suspicious emails;

(2) It is recommended to use a sandbox environment to execute suspicious files, and then use the host to execute them when safety is ensured. It is recommended to use the Antiy Persistent Threat Analysis System (PTA), which uses a combination of deep static analysis and sandbox dynamic loading and execution to effectively detect, analyze and identify various known and unknown threats;

(3) 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.

(4) After binding your email account to your mobile phone, you can not only retrieve your password, but also receive SMS notifications of "abnormal login" and handle them immediately.

(5) Important documents should be well protected:

a) Empty the inbox, outbox and trash of important emails that are no longer used in a timely manner;

b) Back up important files to prevent file 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.

(6) Do not post sensitive information on the Internet. Information and data posted by users on the Internet are at risk of being collected by attackers. Attackers can analyze this information and data and send targeted phishing emails to users.

3.3 Identifying Phishing Emails

Table 3

Identify objects	Specific methods
View email sender	Be wary of non-organized senders of "business mail";
View recipient address	Be wary of mass emails and contact the sender to confirm;
Check the shipping time	Be wary of emails sent outside of working hours.
Look at the email title	Be wary of emails with titles containing keywords such as "order," "invoice," "wage subsidy," and "purchase."
Look at the wording of the text	Be wary of emails that use general greetings such as "Dear," "Dear User," or "Dear Colleague."
See the purpose of the text	Be wary of emails requesting your email account password under the guise of "system upgrade," "system maintenance," or "security settings."
Read the main text	Be wary of any web links included, especially short links;
See the attached content	Before viewing, you must use anti-virus software to scan the attachments for viruses.

It has been verified that **Antiy Intelligent Endpoint Protection System (IEP) can** effectively detect and kill the banking Trojan and provide practical protection for user terminals.

Figure 3-1Antiy IEP test results

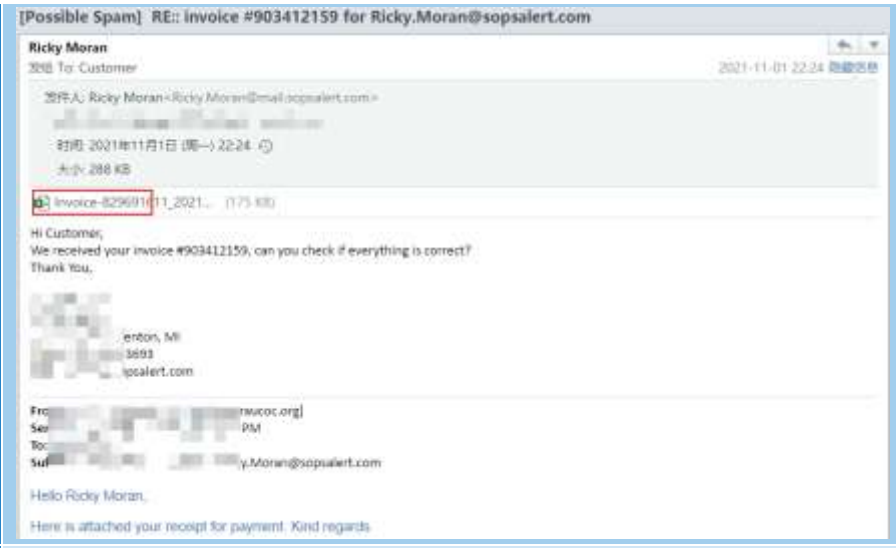
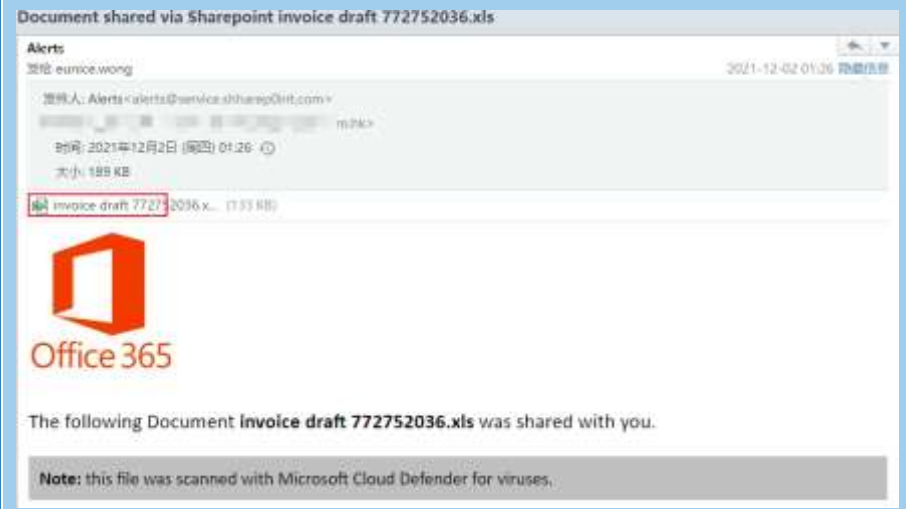
4 Phishing Email Analysis

The phishing emails involved in this phishing campaign primarily use content related to the attachment file name to trick users into clicking on the attachment, opening the malicious document, and triggering macro code. According to Antiy CERT's correlation analysis, this type of phishing email has been extremely active since early November, primarily targeting countries such as the United States, Singapore, China, Mexico, South Korea, and Germany.

4.1 Email Information Case

Table 4-1 2email information

Phishing emails delivered by attackers in early November 2021	Use the invoice information as the subject of the email to deliver the macro document:

	
Phishing emails delivered by attackers in mid - November 2021	Use bank card transaction information as the email subject to deliver macro documents: 
Phishing emails delivered by attackers in early December 2021	Use the invoice information as the subject of the email to deliver the macro document: 

5 Malicious Macro Document Analysis

The malicious macro document captured in this phishing campaign primarily acts as a dropper and downloader, leveraging Excel 4.0 macros to drop an HTML file containing VBS code. This file then invokes the MSHTA command to execute the file, downloading and executing the Dridex banking trojan. This process utilizes code obfuscation to thwart analysis and evade detection.

5.1 Sample Tags

Table 5-1Sample tags

Virus name	Trojan/Win32.Generic
Original file name	Invoice-829691611_20211101.xlsb
MD5	E89B443426FD6D13211C16658D09EB4E
File size	198.07 KB (202,824 bytes)
File format	Document/Microsoft.XLSX[:Excel 2007-2012]
File creator	user
File creation time	2021-10-27 18:31:49
VT first upload time	2021-11-01 17:00:32
VT test results	twenty one / 62

5.2 Sample Analysis

After the malicious macro document is opened, clicking on the image triggers a pop-up message, which tricks the target into clicking the "Enable Macros" button. After enabling, clicking the document again triggers the macro code.

Figure 5-1Malicious macro document

This sample hides a worksheet named "Macro1".

Figure 5-2 Hidden worksheets

This worksheet contains code related to Excel 4.0 macro technology (an early version of macro code, different from existing VBA macro code). The multiple lines of code were written in separate cells, making it difficult to visually view. By using the characteristics of Excel 4.0 macro code, we searched for cells with "=" and found the following code:

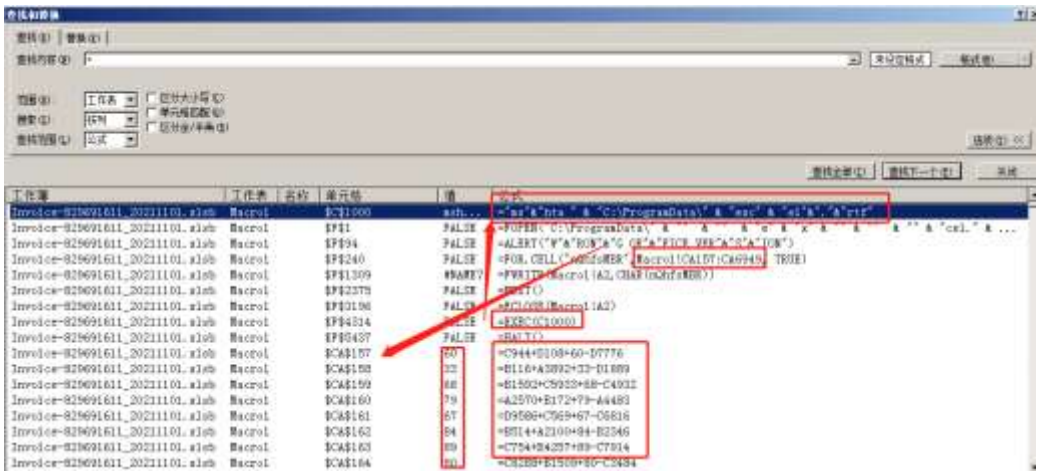


Figure 5-3 Excel 4.0 macro code

The above code does the following:

1. Create the C:\ProgramData\excel.rtf and write the contents of CA157:CA6949 in the worksheet into the file.
2. Call the MSHTA command to execute the created Excel .rtf file.
3. Set a pop-up window prompt "WRONG OFFICE VERSION" to confuse the target.

The excel.rtf file is actually a malicious VBS code that has been obfuscated.

Figure 5-4 Obfuscated vbs code

After deobfuscation, the code is as follows. Its specific functions are as follows: It initially checks whether the system login domain server name matches the current account domain. If not, it triggers the subsequent code. This determination **clearly indicates the attacker's intent to target only terminals under the domain controller**. It then loops through the files corresponding to three URLs, checks the access status and retrieved file size. If the required conditions are met, it saves the file to the local path: C:\\ProgramData\Wlaninst.mp4 (actually a DLL file).

It then calls rundll32.exe to execute the exported function named "KdSendPacket" within the DLL file, and then exits the loop.

Figure 5-5Deobfuscated vbs code

The relevant file paths are as follows:

File name	File path	File type
excel.rtf	C:\ProgramData\	HTML file with malicious obfuscated VBS code
Wlaninst.mp4	C:\ProgramData\	DLL file downloaded by vbs code

5.3 Malicious Documents from the Same Source

By correlating malicious documents created in the same way, we found that a large number of malicious documents have continued to appear since November 1, 2021. These malicious documents have the same creation time and similar embedded Excel 4.0 macro codes, all of which have the behavior of calling the MSHTA command to execute the HTA file.

Malicious document file names also have various naming characteristics, as follows:

Table 5-2 3

Malicious document naming characteristics	Early_Access.-*****_yyyymmdd.xlsb
	Invoice-***** _yyyymmdd.xlsb
	Threats Survey *****.xlsb
	Holiday Survey Threats *****.xlsb
	Scam Survey *****.xlsb
	Holiday Survey Fraud *****.xlsb

	Complaint details *****.xlsb
	……

5.4 Dridex Banking Trojan Hosting Platform

URL that downloads the Dridex banking trojan from the malicious macro document. The URL belongs to a social software platform called "Discord", which can store various files and generate corresponding sharing links.

According to monitoring data from a malicious URL platform[2], from November 1 to November 4, 2021, the number of URLs spreading the Dridex banking Trojan continued to grow, and the corresponding number of samples also continued to rise.

Figure 5-6 Dridex-related URL activity

Data source: urlhaus.abuse.ch

The corresponding number of samples also increased in early November 2021:

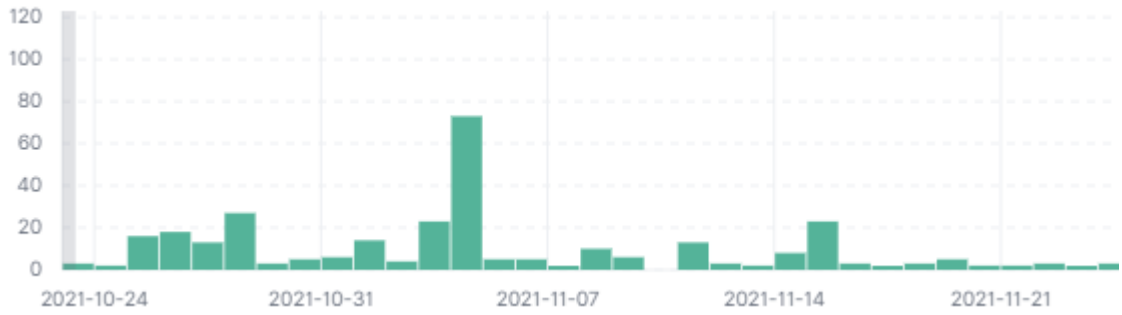


Figure 5-7 Dridex sample size

In addition, the Dridex banking trojan also uses other platforms to spread:

Table 5-4Using other platforms for dissemination

Platform name	Platform usage	URL storing the Dridex banking trojan (currently invalid)
Dropbox	Provides online storage services and realizes	https://www.dropbox.com/s/wgboc0fhqj8qjon/dctGR.mp3?dl=1

	Internet file synchronization through cloud computing, allowing users to store and share files and folders.	https://www.dropbox.com/s/sf1agdykf5jo131/NDRVuq.mp3?dl=1
OneDrive	A network drive and cloud service launched by Microsoft. Users can upload their files to a network server and browse those files through a web browser.	https://onedrive.live.com/download?resid=F7F5D19FC93443B1%21139&authkey=!AA8JSY1RL5hVgfs https://onedrive.live.com/download?resid=359213FFBD695EC9%21163&authkey=!ABRTeRpsnkYNROQ

Based on the technical points such as the creation time, naming characteristics, document behavior, and propagation methods of the malicious documents used in the attacker's phishing activities detected this time, after correlation analysis and judgment, it was found that there was a certain overlap with some technical points used by the TA575 group (a cybercrime organization) to spread the Dridex banking Trojan in early 2021. Based on this, it was preliminarily determined that the attacker behind this phishing activity was the TA 575 organization.

Table 5TA575 group attack activity association

Time	Attack activities	Related points (same points as the samples found this time)
February 2021	The TA575 organization launched a Qakbot campaign targeting American medical and law firms and other institutions	Utilize phishing emails to deliver macro documents and download and execute Qak bot payloads via MSHTA
July - August 2021	TA575 organization launched Dridex campaign targeting relevant institutions in the United States and South Korea	The malicious documents used during this period were mostly named "Invoice_*****.xls", "* ***_Invoice_*****.xls", etc.
October 2021	TA575 uses "Squid Game" lure to distribute Dridex malware	The creation time of the malicious document used is consistent with the creation time of the captured sample

6 Analysis of the Dridex Banking Trojan

The sample captured this time contained numerous anomalies and encrypted payloads, thwarting analysis and debugging. Analysis revealed that the sample is essentially a Dridex banking trojan loader. Its functions include collecting system information, connecting to a C2 and transmitting it back; issuing commands, obtaining a list of P2P nodes, and participating in the construction of a botnet; and obtaining subsequent modules for stealing secrets or extortion.

6.1 Sample Tags

Table 6-1Sample tags

Virus name	Trojan[Downloader]/Win32.Cridex
Original file name	ohma.dll
MD5	A42ADC9E3E7E43479C020E1E0F44390C
Processor architecture	Intel 386 or later, and compatibles
File size	456.00 KB (466,944 bytes)
File format	BinExecute /Microsoft.DLL[:X86]
Timestamp	2021-11-01 12:06:45
Digital signature	None
Packer type	None
Compiled language	Microsoft C/C++ Visual Studio 2013
VT first upload time	2021-11-01 16:19:12
VT test results	42 / 66

6.2 Adversarial Analysis and Detection

After executing from the entry point, the sample sets up a nonfunctional SEH exception handler and cyclically triggers a large number of int 3 exceptions, causing the exception handler to execute for a long time and disrupting the debugging process, thereby achieving anti-sandbox and anti-analysis debugging. The sample is then decrypted in memory. The decrypted module registers a VEH exception handler and captures exceptions triggered by int 3, thereby achieving the effect of indirectly calling the API.

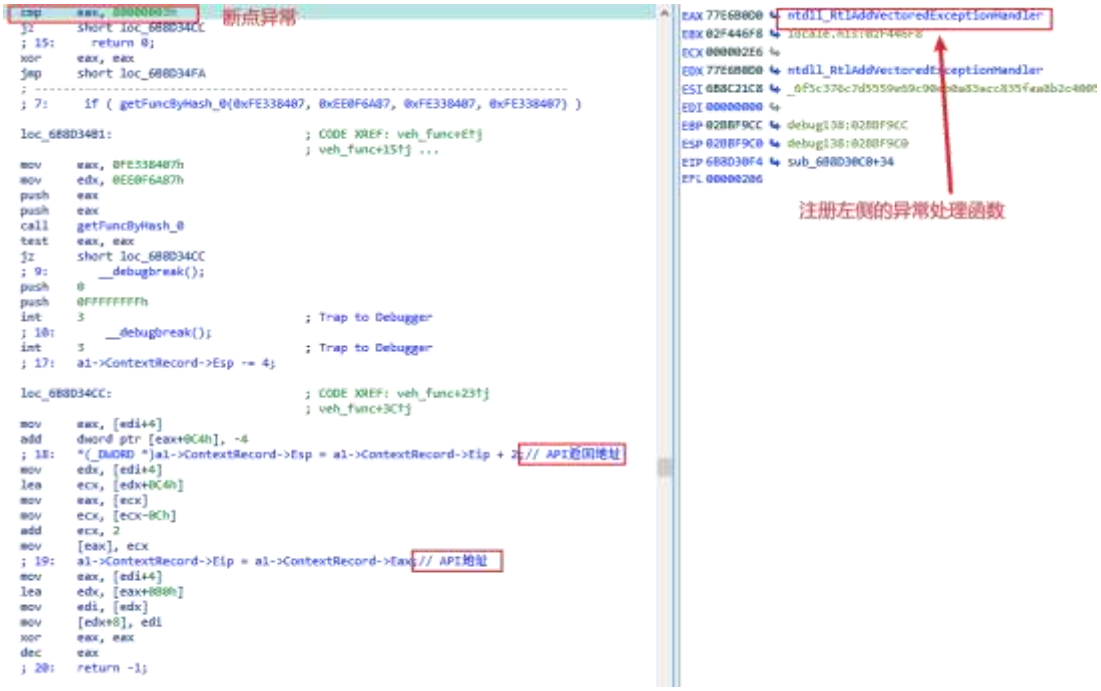


Figure 6-1Registering VEH function to capture exception

The APIs in the sample are dynamically obtained through CRC32 hash values after XOR, and are executed by the above VEH exception handling program by triggering an int 3 exception. This API call disrupts the execution flow, affects analysis tools, interferes with dynamic debugging, and increases the difficulty of analysis.

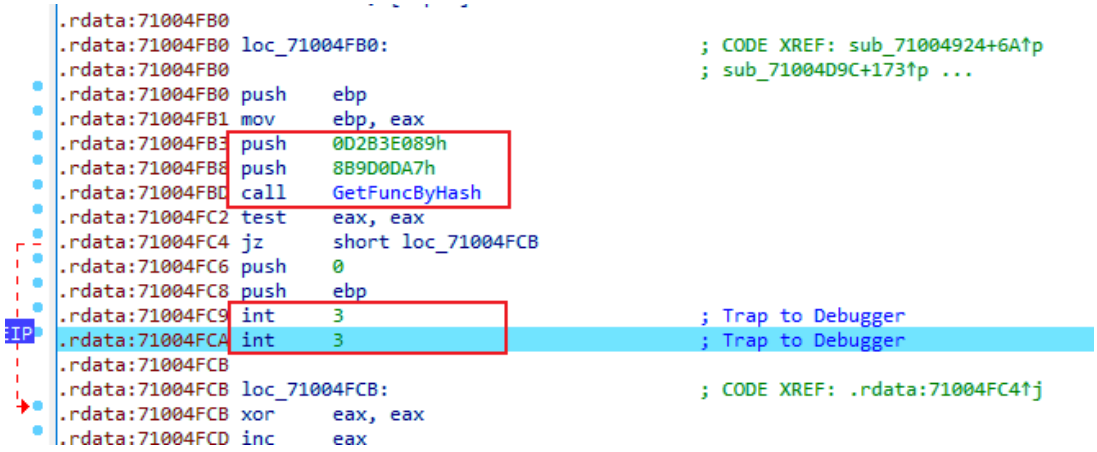


Figure 6-2Dynamically obtain API and call it using int 3

6.3 Information Collection

Use multiple functions including GetSystemInfo to read basic information such as system computer name, environment variables, system architecture, etc.


```
aAllusersprofil_0 db 'ALLUSERSPROFILE=C:\ProgramData',0
aAppdataCUsersV db 'APPDATA=C:\U                ppData\Roaming',0
aCommonprogramf_2 db 'CommonProgramFiles=C:\Program Files (x86)\Common Files',0
aCommonprogramf_3 db 'CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files',0
aCommonprogramw_0 db 'CommonProgramW6432=C:\Program Files\Common Files',0
aComputernameDe db 'COMPUTERNAME=                ',0        计算机名称
aComspecCWindow db 'ComSpec=C:\Windows\system32\cmd.exe',0
aDriverdataCWin db 'DriverData=C:\Windows\System32\Drivers\DriverData',0
aFpsBrowserAppP db 'FPS_BROWSER_APP_PROFILE_STRING=Internet Explorer',0
aFpsBrowserUser db 'FPS_BROWSER_USER_PROFILE_STRING=Default',0
aHomedriveC db 'HOMEDRIVE=C:',0
aHomepathUsersV db 'HOMEPATH=\Users                ',0
aLocalappdataCU db 'LOCALAPPDATA=C:\Users                AppData\Local',0
aLogonserverDes db 'LOGONSERVER=\\                ',0
aNumberOfProces_0 db 'NUMBER_OF_PROCESSORS=4',0        CPU核心数
aOnedriveCUsers db 'OneDrive=C:\U                neDrive',0
aOsWindowsNt db 'OS=Windows_NT',0
aPathCWindowsSy db 'Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\W'
db '                '
db '                '
db '                '
aPathextComExeB db 'PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC',0
aProcessorArchi_1 db 'PROCESSOR_ARCHITECTURE=x86',0        CPU架构
aProcessorArchi_2 db 'PROCESSOR_ARCHITEW6432=AMD64',0
aProcessorIdent db 'PROCESSOR_IDENTIFIER=Intel64 Family 6                Genui'
db 'neIntel',0
aProcessorLevel db 'PROCESSOR_LEVEL=6',0
aProcessorRevis db 'PROCESSOR_REVISION=a505',0
aProgramdataCPr db 'ProgramData=C:\ProgramData',0
aProgramfilesCP db 'ProgramFiles=C:\Program Files (x86)',0
aProgramfilesX8_0 db 'ProgramFiles(x86)=C:\Program Files (x86)',0
aProgramw6432CP db 'ProgramW6432=C:\Program Files',0
aPsmodulepathCP db 'PSModulePath=C:\Program Files\WindowsPowerShell\Modules;C:\Window'
db 's\system32\WindowsPowerShell\v1.0\Modules',0
aPublicCUsersPu db 'PUBLIC=C:\Users\Public',0
aSessionnameCon db 'SESSIONNAME=Console',0
aSystemdriveC db 'SystemDrive=C:',0
aSystemrootCWin db 'SystemRoot=C:\Windows',0
aTempCUsersVW10 db 'TEMP=C:\Use                AppData\Local\Temp',0
aTmpCUsersVW10A db 'TMP=C:\User                ppData\Local\Temp',0
aUserdomainDesk db 'USERDOMAIN=                ',0
aUserdomainRoam db 'USERDOMAIN_ROAMINGPROFILE=                ',0
aUsernameVW10 db 'USERNAME=                ',0        用户名
aUserprofileCUs db 'USERPROFILE=C:\Users                ',0
aWindirCWindows db 'windir=C:\Windows',0
```

Figure 6-3Collecting system information

6.4 Connect to C2 to Obtain Subsequent Stealing or Ransomware Modules

Sends information to a hardcoded C2 server.

```
6B3FD022  62          db 62
6B3FD023  81          db 81
6B3FD024  BA          db BA          僵尸网络ID: 22202
6B3FD025  56          db 56
6B3FD026  D3          db D3
6B3FD027  00          db 0
6B3FD028  00          db 0
6B3FD029  52          db 52
6B3FD02A  01          db 1
6B3FD02B  03          db 3           C2数量
6B3FD02C  68F89B85    dd 859BF868    104.248.155.133
6B3FD030  BB01        dw 1BB         443
6B3FD032  2E65623C    dd 3C62652E    46.101.98.60
6B3FD036  2803        dw 328         808
6B3FD038  25BB720F    dd F72BB25     37.187.114.15
6B3FD03C  EC1F        dw 1FEC        8172
6B3FD03E  FB          db FB
```

Figure 6-4 Three hardcoded C2 addresses

Following C2 instructions, it retrieves a list of P2P nodes, participates in building a botnet, and downloads additional payloads for further theft or ransomware. Currently, all three C2 addresses are invalid, making it impossible to retrieve subsequent attack payloads for analysis.


```
v14 = 300;
v6 = (char **)sub_75C2EC68(v10);
if ( (unsigned __int8)sub_75C37C4C(v12, v6) )
{
  sub_75C3804C(v18, v17);
  sub_75C2F458(v18);
  sub_75C2F678();
  if ( !v12[0] && (v13 == 200 || v13 == 404) )
  {
    if ( !a2 )
      break;
    sub_75C236A4(a3);
    sub_75C2F458(v19);
    sub_75C2F678();
    if ( !(unsigned __int8)sub_75C2F4F4(v15) )
      break;
  }
}
```

Figure 6-5Read the C2 reply result

7 IoCs

Malicious documents	E89B443426FD6D13211C16658D09EB4E
Dridex banking Trojan sample	A42ADC9E3E7E43479C020E1E0F44390C
C2 address (expired)	104.248.155.133:443 46.101.98.60:808 37.187.114.15:8172

Appendix 1: References

[1]. The First Step: Initial Access Leads to Ransomware

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

[2]. URL activity of the Dridex banking trojan in the URLhaus Database

https://urlhaus.abuse.ch/browse/tag/Dridex/

Appendix 2: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has

developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in

the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced 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.