Analysis Report of Ransomware Pandora

Antiy CERT

Completion time of first draft: 18 March, 2022

Time of first release: 23 March, 2022

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

1 Overview

Recently, Antiy CERT (member of the CCTGA Ransomware Prevention and Response Working Group) has found a number of ransomware attacks against the automotive industry. These include: Bridgestone (tyre supplier), which suffered a Lockbit 2.0 ransomware attack on 27 February, and Denso (automotive parts and systems supplier), which suffered a Pandora ransomware attack on 10 March, Snap-on (maker of automotive-related tools) and Empire Electronics (supplier of automotive lighting components) were hit by a Conti ransomware attack on March 16.

In the above incident, the Pandora ransomware came to the attention of Antiy CERT. The ransomware, which first appeared in February 2022, was spread mainly through phishing emails, vulnerability exploitation and acquisition of the victim's system login credentials, and reverse analysis of control flow confusion and interference was set. Adopt the strategy of "double blackmail" ("Threatening exposure of enterprise data + extortion of encrypted data"), and divulge the stolen data when the system file is encrypted and the work cannot be operated normally. Through sample analysis and threat intelligence correlation, it is found that some code segments of Pandora ransomware are similar to Rook ransomware, so it is speculated that Pandora may have used Babuk's source code like Rook, or it may be a variant or successor of Rook.

The Terminal Defense System of Antiy IEP can effectively detect and kill the ransomware and effectively protect the user terminal.

2 Recent Attacks and Family Information

Ransomware Pandora, which appeared in February 2022, had attacked Denso on March 10 and posted the stolen information on the Tor website's data breach platform on March 13 (around March 16, the information has been deleted).

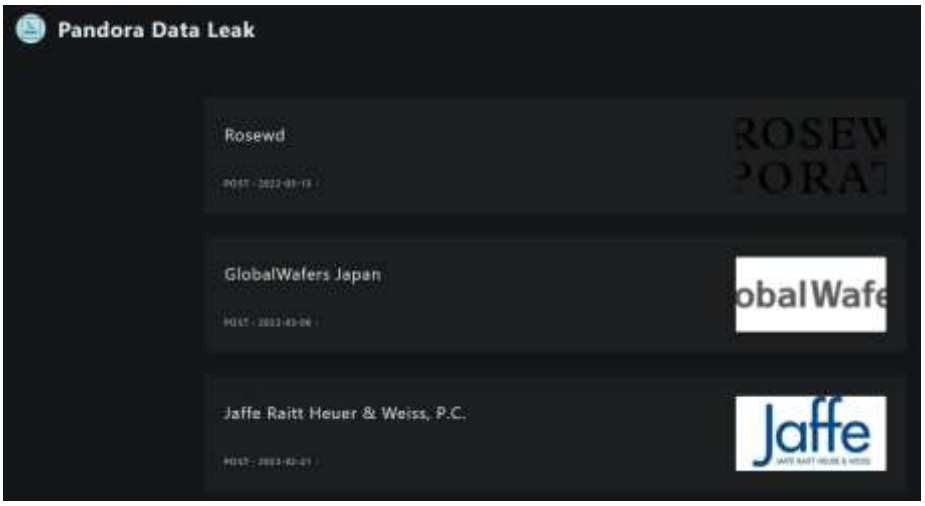


Figure 2-1: Pandora Data Leakage Platform (Partial Victim Information Deleted)1

The following is the victim's information page before Denso's information is deleted.

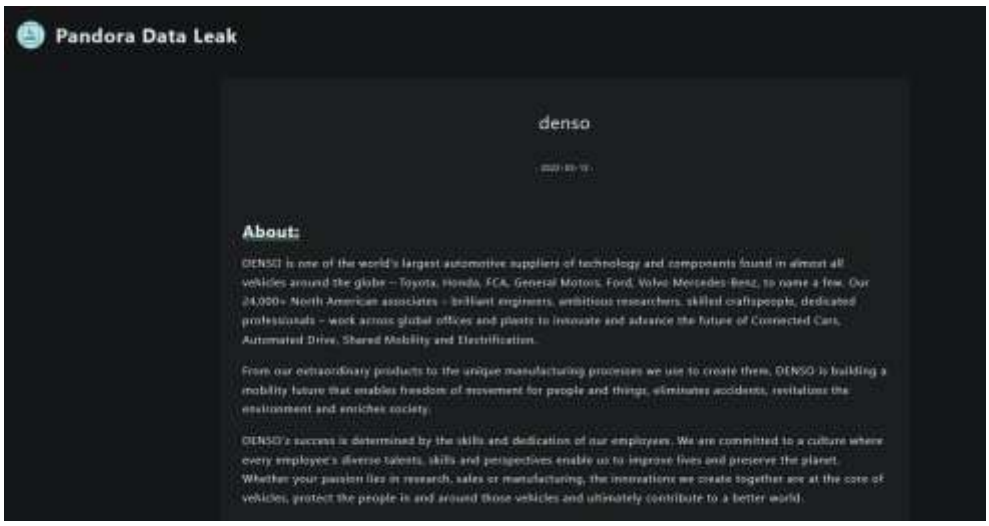


Figure 2-2 Victim Information Page

In order to prove that that data was successfully stolen from the victim's Denso system, the attacker publish the file name of the stolen data on the data breach platform. According to statistics of open file names, the number of stolen files is 157,585.

Figure 2-3 Number of files stolen

Presumably under pressure from the outside world, ransomware Pandora’ s links to the Tor victims' pages were disabled around March 17.

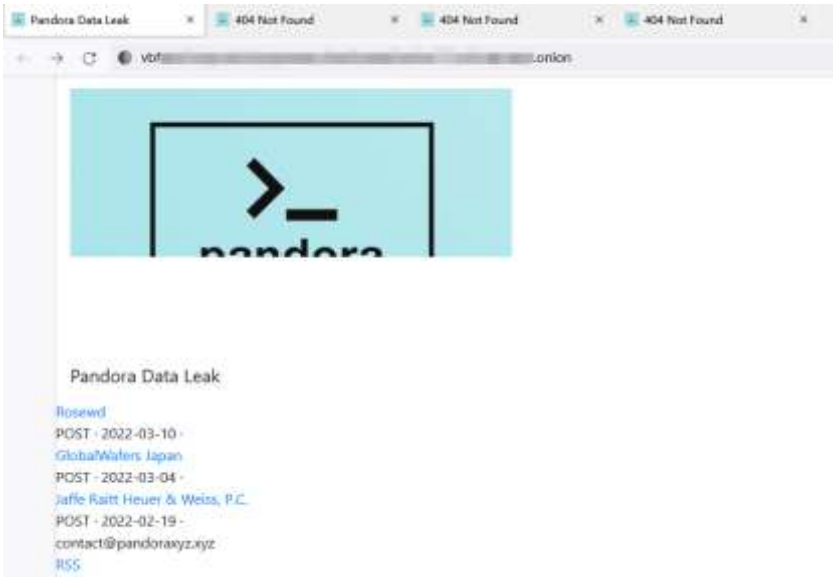


Figure 2-4 Invalid Page of Victim Information

The analysis of samples linked to threat intelligence revealed [1] that the Pandora ransomware was similar to the Rook ransomware in some code segments. The Rook appeared in November 2021, the branch of Denso had been hit by a Rook ransomware attack in December 2021, and there are claims to have previously warned that Denso's network access credentials were sold [2], Speculation that this could also be the reason that Denso has been hit twice in four months by ransomware.

The Rook ransomware uses the Babuk ransomware source code [3]. Babuk appeared in January 2021, initially operating as a ransomware-as-a-service (RaaS), and in April the organisation issued a statement to stop operating ransomware-as-a-service, The Babuk ransomware's builder file was leaked by an original creator in July, and the full source code for the Babuk ransomware was leaked in September. Since then, there have been different threat actors using source code to build ransomware payloads, and there have been many types of ransomware with the same attributes as the original Babuk. So presumably Pandora may have used Babuk's source code like Rook, or it may have been a variant or successor to Rook.

Figure 2-5 Same Key Storage Location

3 Recommendations for protection

In response to the ransomware, Antiy recommends that individuals and businesses take the following precautions:

3.1 Personal protection

(1) Installation of terminal protection: Installation of anti-virus software. It is suggested that Antiy IEP users open the ransomware defense tool module (open by default);

(2) Strengthen password strength: Avoid weak passwords, and it is recommended to use 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid the use of the same password by multiple servers;

(3) Change passwords on a regular basis: Change system passwords on a regular basis to avoid system intrusion due to password leakage;

(4) Timely update of patches: It is suggested to activate the automatic update function and install system patches, and update system patches for vulnerable parts such as servers, databases and middleware;

(5) Close high-risk ports: The principle of minimizing external services is to close unused high-risk ports such as 3389, 445, 139 and 135;

(6) Close PowerShell: If PowerShell command line tools are not used, it is recommended to close them;

(7) Regular data backup: Data backup of important files on a regular basis, and the backup data shall be isolated from the host computer.

3.2 Enterprise protection

(1) Open log: Open the key log collection function (security log, system log, PowerShell log, IIS log, error log, access log, transmission log and cookie log). To provide a basis for tracing and tracing the security incidents;

(2) Set IP whitelist rules: Configure advanced secure Windows firewall, set inbound rules for remote desktop connection, add the IP address or IP address range used to the rules, and prevent violent attack of non-rule IPs;

(3) mainframe reinforcement: Conduct penetration test and security reinforcement for the system;

(4) Deployment of Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of ransomware. Taking network traffic as the detection and analysis object, the Antiy Sea Threat Detection System (PTD) can accurately detect a mass of known malicious codes and network attack activities, and effectively detect suspicious behaviors, assets and various unknown threats on the network;

(5) Disaster backup plan: Establish a security disaster backup plan to ensure that backup business systems can be enabled quickly;

(6) Safety day service: In case of any ransomware attack, it is recommended to disconnect the network in time, and protect the site and wait for the security engineer to check the computer. Antiy 7 * 24 Service Hotline: 400-840-9234.

At present, Antiy IEP can realize the detection and effective protection of ransomware Pandora.

Figure 3-1 Effective protection of Atenone1

Figure 3-2 Antiy IEP prevents encryption2

4 Ransomware at a glance

Table 4-1 Ransomware Pandora overview 1

Time of occurrence	February 2022

Encryption algorithm	Aes + RSA
Encryption system	Windows
How to name encrypted files	Extension of the original file. pandora
Contact information	Contact @ pandoraxyz.xyz and Tor websites
Encrypted file type	Bypass files, folders, and file suffixes with specific names
Currency and amount of blackmail	After communicating with the attacker
Whether it is targeted	Yes
Whether it can be declassified	No
Whether internal network propagation or not	No
Ransom note interface	
Data leakage	

5 Sample analysis

5.1 Sample labels

Table 5-1 Label of Pandora Samples 2

Virus name	Trojan [Ransom] / Win32.Pandora
Original file name	M3do2.exe
Md5	0c4a84b66832a08dccc42b478d9d5e1b
Processor architecture	Intel 386 or later processors and compatible processors
File size	218.00 KB (223,232 bytes)
File format	Binexecute / Microsoft.EXE [: X86]
Time stamp	2022-03-10 00: 39: 27
Digital signature	None
Shell type	Upx
Compiled Language	Microsoft Visual C + +
Vt First Upload Time	2022-03-10 12: 00: 30
Vt test result	51 / 69

5.2 Sample analysis

After the ransomware program is executed, first check whether there is a ThisIsMutexa in the current host, and then judge whether to continue running the program.

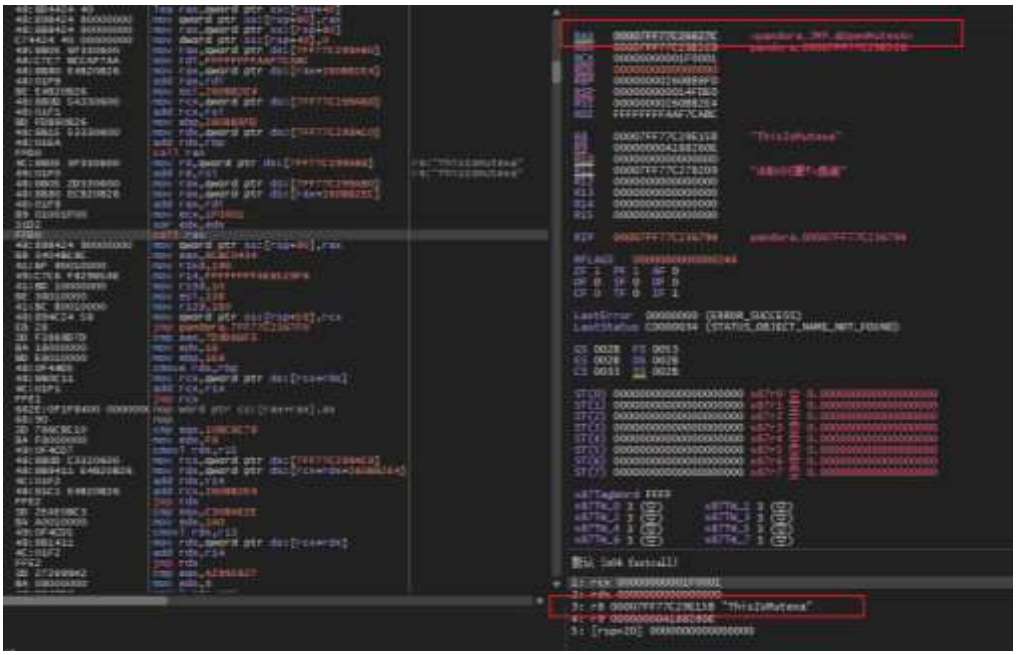


Figure 5-1 Detects whether the same mutex exists in the current host1

If that mutex ThisIsMutexa is not found in the current host, the mutex is create to ensure that only one instance is running.

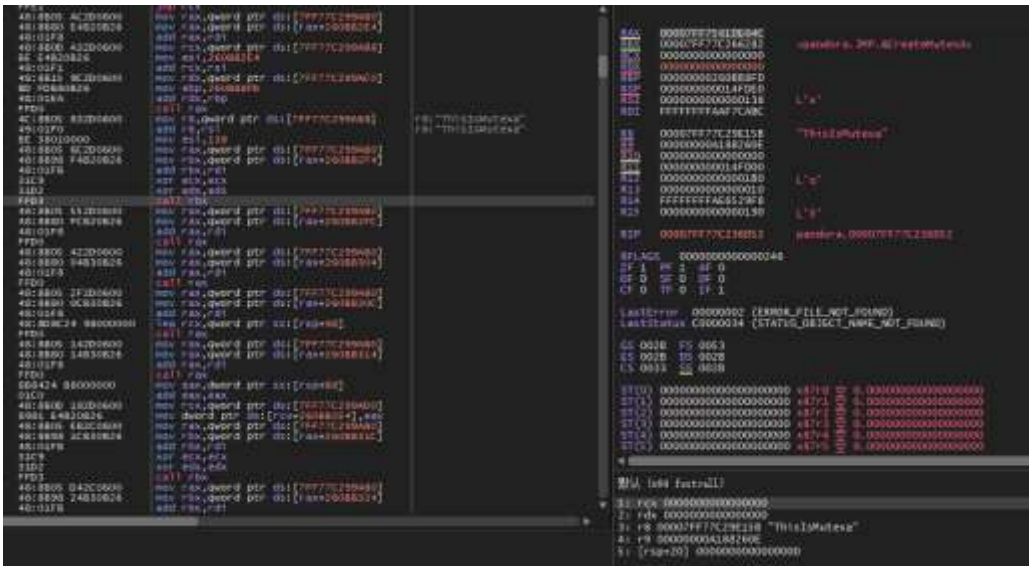


Figure 5-2 Creation of Mutex2

Generating an RSA key from the device information.

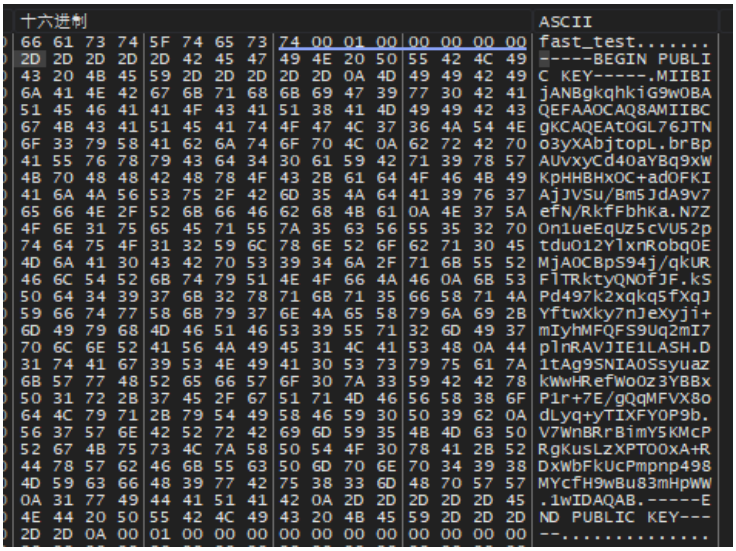


Figure 5-3 Generation of RSA Key3

Create registry keys named Public and Private under HKEY _ CURRENT _ USER\ SOFTWARE to store public and private keys.

Figure 5-4 Registry Storage Key4

Set the priority when the system shuts down to 0, so that it is finally shut down when the system shuts down, and extend the execution time before shutting down to the maximum extent.

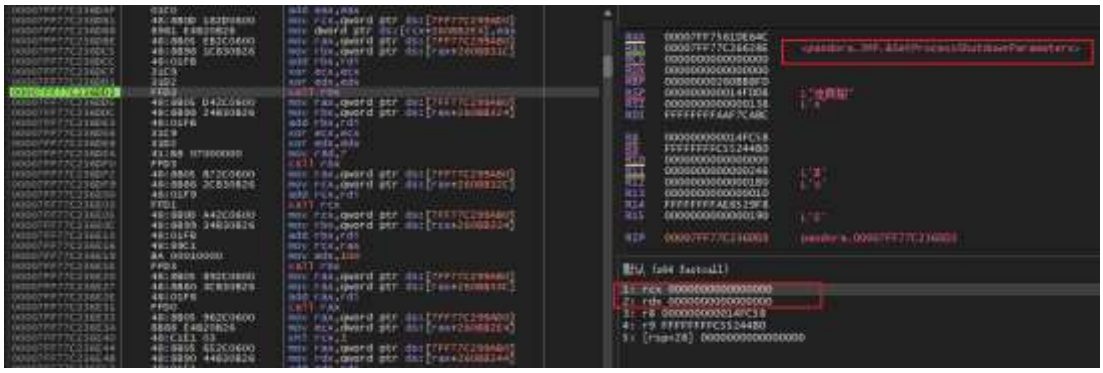


Figure 5-5 Set self-program end priority5

Delete the data in the Recycle Bin.

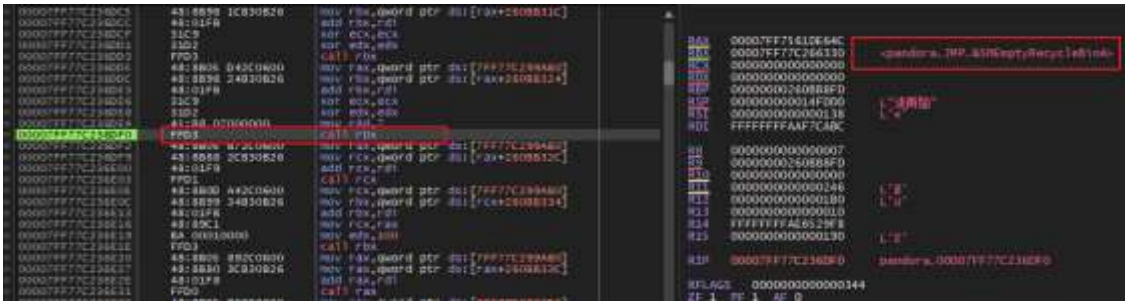


Figure 5-6 Emptying the Recycle Bin6

Use vssadmin. exe to delete the system shadow, so as to prevent the victim host from restoring the encrypted file by restoring the shadow.

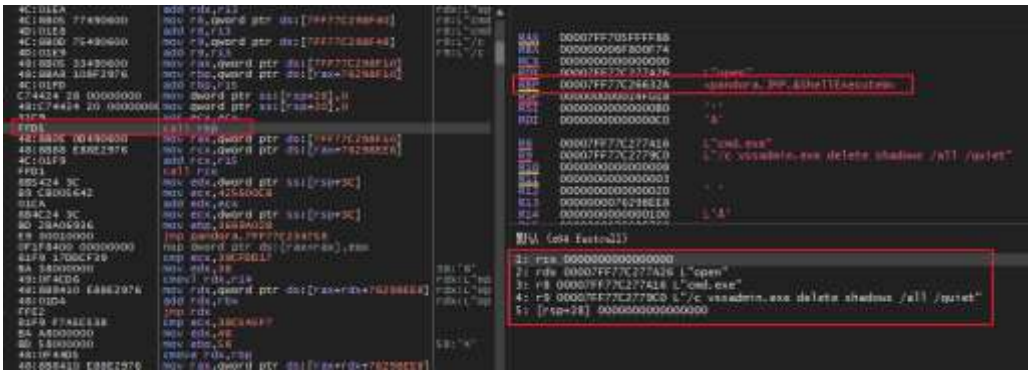


Figure 5-7 Remove Disk Volume Shadow7

Use the GetDriveTypeW function to check the type of the corresponding disk character in alphabetical order of the keyboard layout.

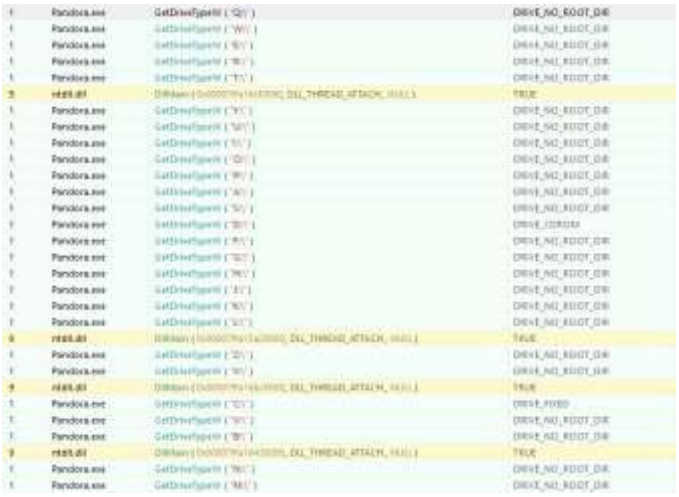


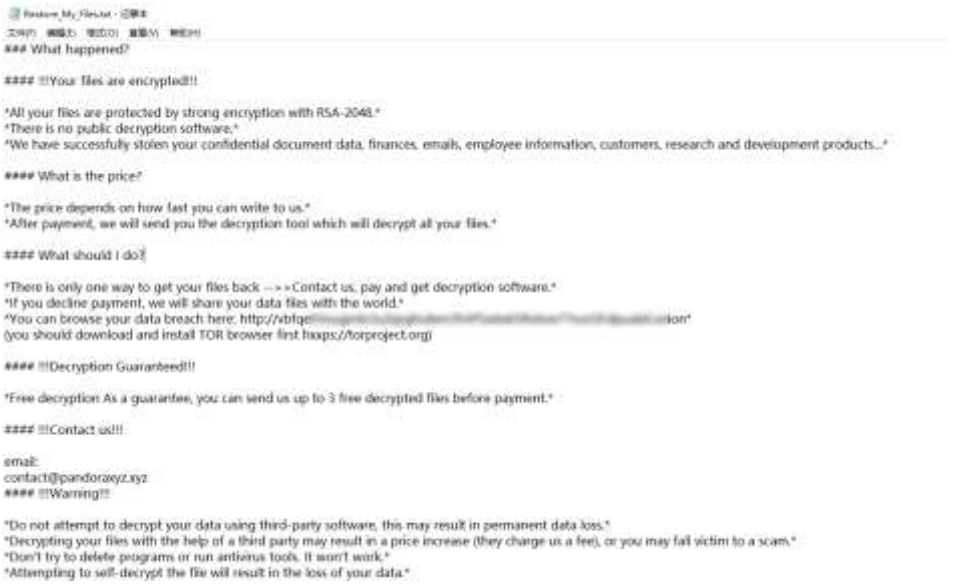
Figure 5-8 Checking Disk Type8

Bypass unencrypted folder, file name and file, the extension of the following table:

Table 5-2 Bypass Unencrypted Folders, Files, and Extensions

File / Folder Name	**Appdata**	**Boot**	**Windows**	**Windows.old**
	Tor Browser	Internet Explorer	Google	Opera
	Opera Software	Mozilla	Mozilla Firefox	$Recycle.Bin
	Programdata	All Users	Autorun.inf	Boot.ini
	Bootfont.bin	Bootsect.bak	Bootmgr	Bootmgr.efi
	Bootmgfw.efi	Desktop.ini	Iconcache.db	Ntldr
	Ntuser.dat	Ntuser.dat. log	Ntuser.ini	Thumbs.db
	Program Files	Program Files (x86)	# Recycle	
File extension	.hta	.exe	.dll	.cpl
	.ini	.cab	.cur	.sys
	.idx	.drv	.hlp	.icl
	.icns	.ico	.ocx	Pandora
	.spl			

A ransom note is generated when the encrypted file is finished, which contains a ransom note, contact information and the Tor website address.



What happened?

!!Your files are encrypted!!!

All your files are protected by strong encryption with RSA-2048.
There is no public decryption software.
We have successfully stolen your confidential document data, finances, emails, employee information, customers, research and development products...

What is the price?

The price depends on how fast you can write to us.
After payment, we will send you the decryption tool which will decrypt all your files.

What should I do?

There is only one way to get your files back --> >Contact us, pay and get decryption software.
If you decline payment, we will share your data files with the world.
You can browse your data breach here: http://vbfge[redacted]ion
(you should download and install TOR browser first https://torproject.org)

!!Decryption Guaranteed!!!

Free decryption As a guarantee, you can send us up to 3 free decrypted files before payment.

!!Contact us!!!

email:
contact@pandoraxyz.xyz
!!Warning!!!

Do not attempt to decrypt your data using third-party software, this may result in permanent data loss.
Decrypting your files with the help of a third party may result in a price increase (they charge us a fee), or you may fall victim to a scam.
Don't try to delete programs or run antivirus tools. It won't work.
Attempting to self-decrypt the file will result in the loss of your data.

Figure 5-9 A ransom note9

6 IoCs

0c4a84b66832a08dccc42b478d9d5e1b

Appendix I: Reference

[1]. Quick revs: Pandora Ransomware - The Box has been open for a while.

https://dissectingmalwa.re/blog/pandora/

[2]. I warned DENSO of threat actor selling access to their network

https://twitter.com/radvadva/status/1503003017150349318

[3]. New Rook Ransomware Feeds Off the Code of Babuk

https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/

Appendix II: Special Working Group for Ransomware Prevention and Response of China Internet Network Security Threat Governance Alliance

The National Internet Emergency Response Center (CNCERT) has jointly established the "China Internet Cybersecurity Threat Governance Alliance Ransomware Prevention and Response Professional Working Group" (referred to as "CCTGA Ransomware Prevention and Response Working Group") with leading domestic security enterprises. This working group focuses on ransomware prevention and response efforts in areas such as ransomware information notification, intelligence sharing, daily prevention, and emergency response. It also regularly releases ransomware updates to the official website (https://www.cert.org.cn/publish/main/44/index.html) or the WeChat official account (National Internet Emergency Response Center CNCERT).