A Possible Re-brand of Rook Ransomware

Pandora ransomware came into the spotlight in March 2022 after targeting some high-profile victims on its leak site. The ransomware group announced its first victim on 21 Feb 2022 and has posted around five victims to date.

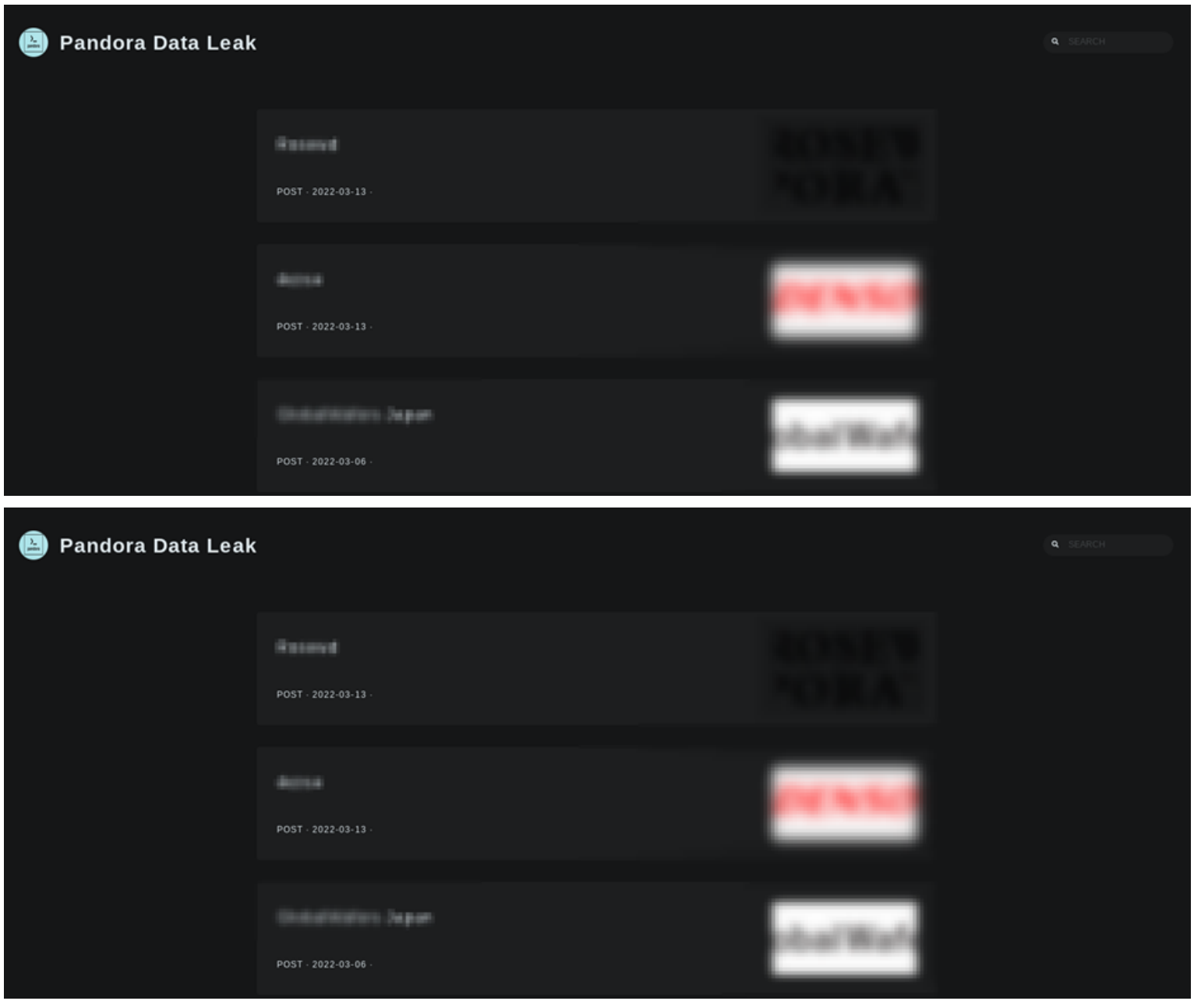


Figure 1: Pandora ransomware data leak site

During a routine threat hunting exercise, Cyble Research Labs came across the sample for this ransomware. Upon execution, the file encrypts the victim's system and drops the ransom note in each folder named "Restore_My_Files.txt." After encryption, the file is renamed with the extension ".Pandora".

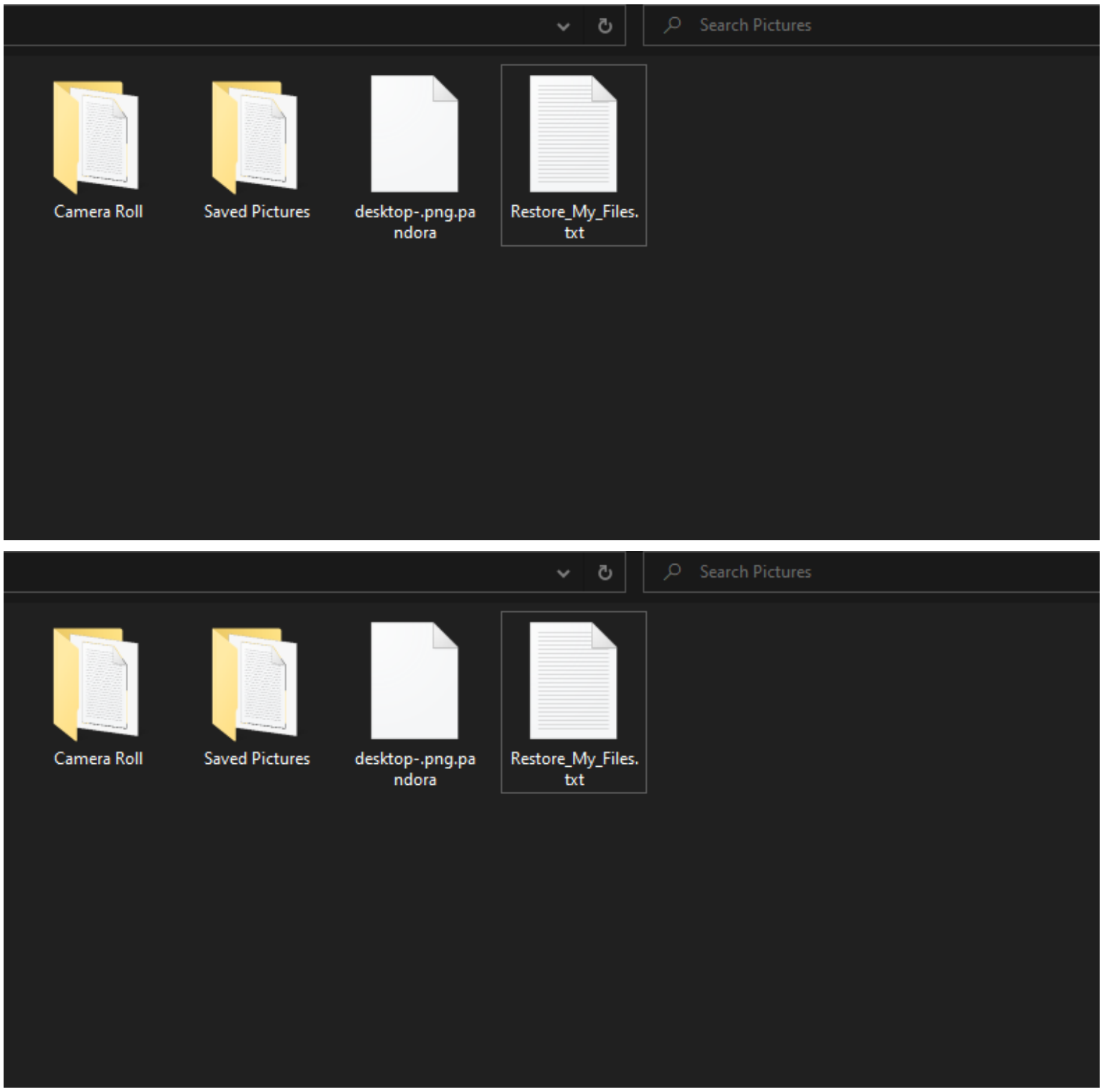


Figure 2: Encrypted Files

Technical Analysis

The malware (SHA 256: 5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b) is packed using the UPX packer. After unpacking, the payload is compiled using Visual C++. The file has encrypted strings and several jumps and calls that can make debugging difficult, as shown below.

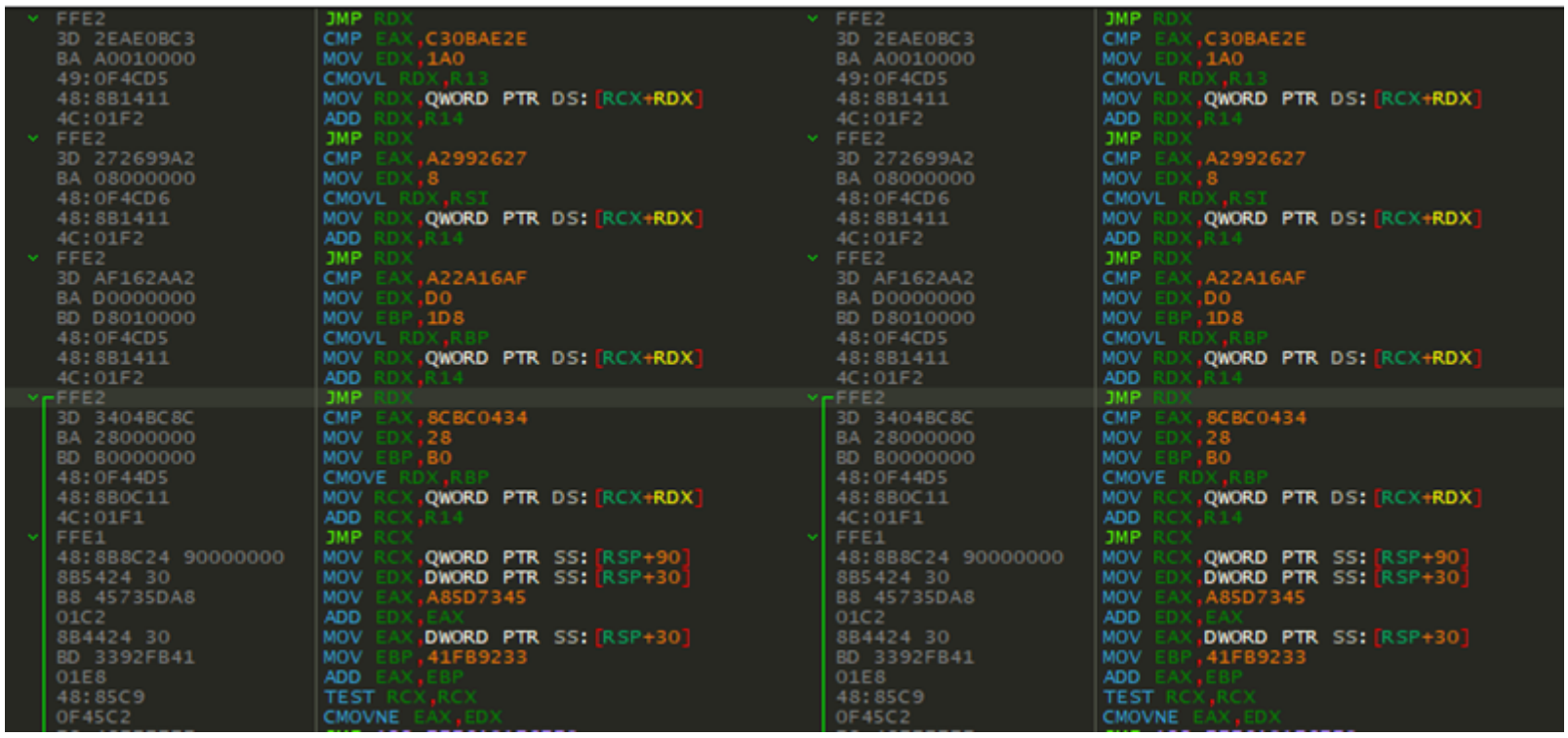


Figure 3: Code flow of Pandora Ransomware

The malware runs a decryption loop that decrypts the strings present in the file, as shown in Figure 4.

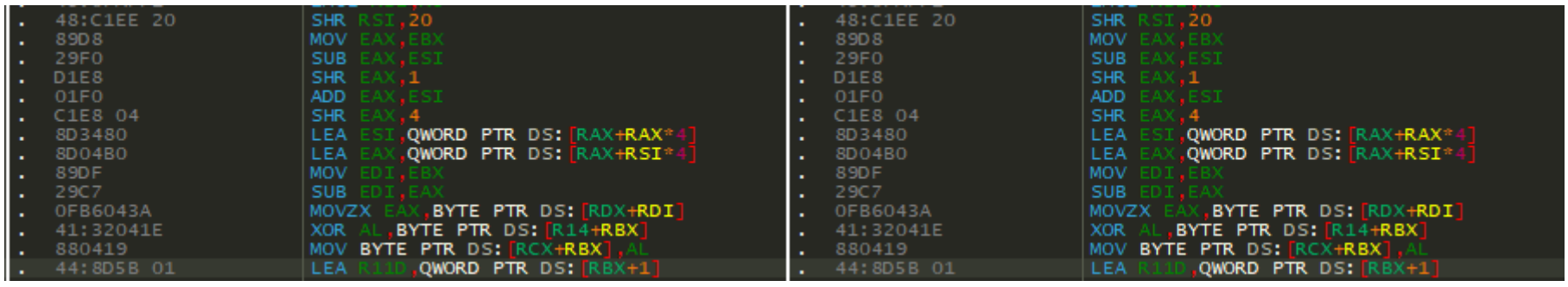


Figure 4: Decryption Loop

Initially, the malware creates a mutex named "ThisIsMutexa" using CreateMutexA() API to ensure that only one instance of the malware is running in the system.

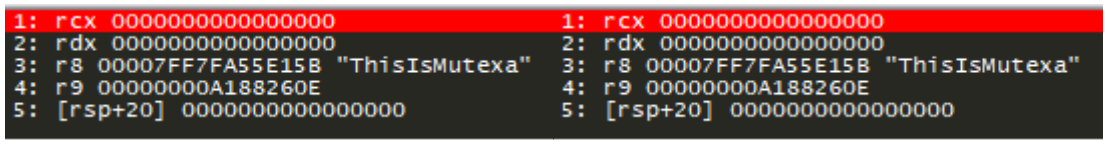


Figure 5: Creates Mutex

The malware then loads ntdll.dll and calls the NtSetInformationProcess () API, which changes the privilege level and sets the malware file as a critical process. The malware then disables the Event Tracing for Windows (ETW) by patching the EtwEventWrite() function and further bypasses Antimalware Scan Interface (AMSI) to evade detection by Anti-Virus products.

The AMSI allows the integration of applications and processes with the anti-malware solution present on a system. AMSI scans files that are executed through PowerShell, Jscript, VBA, VBScript, etc.

The malware also calls SetProcessShutdownParameters() to reduce the process's priority, i.e., set it to zero. This means that malware will be terminated last before the system shutdown so that the malware gets the maximum amount of time possible to execute in the compromised machine.

After altering the priority, the malware calls SHEmptyRecycleBinA() API to empty the recycle bin to ensure no deleted files are restored after encryption.

Like other ransomware, the malware deletes shadow copies using vssadmin using ShellExecuteW() API, as shown in Figure 6.

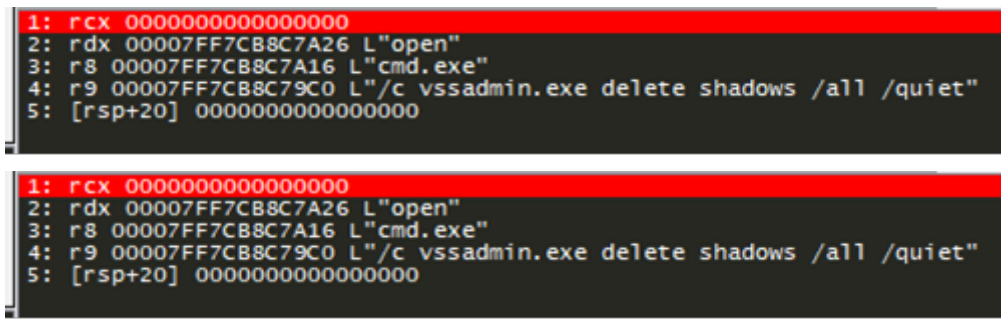


Figure 6: Deletes shadow copies

Before encrypting the machine, the malware gets the Volume details by calling the APIs such as:

- GetDriveTypeW()
- FindFirstVolumeW()
- FindNextVolumeW()
- GetVolumePathNamesForVolumeNameW()
- GetLogicalDrives()

Before initiating encryption, the ransomware checks and excludes specific folders from encryption — such as AppData, Boot, Windows, Windows.old, Tor Browser, Internet Explorer, Google, Opera, Opera Software, Mozilla, Mozilla Firefox, ProgramData, Program Files, Program Files (x86).

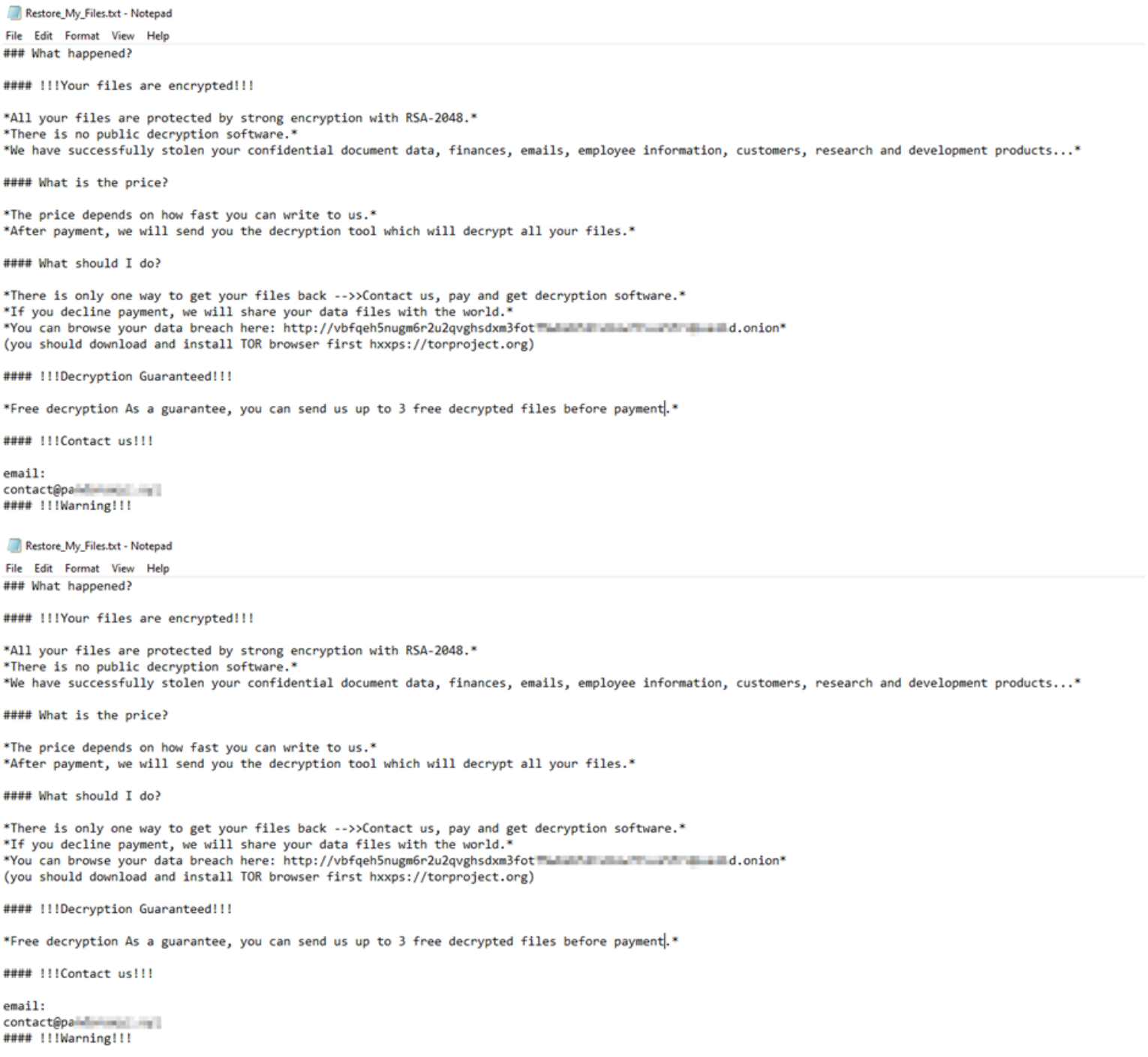
The Ransomware also excludes certain files from encryption such as autorun.inf, boot.ini, bootfont.bin, bootsect.bak, bootmgr, bootmgr.efi, bootmgfw.efi, desktop.ini, iconcache.db, ntldr, ntuser.dat.

Additionally, specific extensions are also exempted from encryption — such as
.pandora, .hta, .exe, .dll, .cpl, .ini, .cab, .cur, .drv, .hlp, .icl, .icns, .ico, .idx, .sys, .spl, .ocx.

Finally, the ransomware searches for files using FindFirstFileW() and FindNextFileW () APIs and then proceeds to encrypt them.

The malware uses multithreading approach for faster encryption. It calls CreateThread(), SetThreadAffinityMask(), ResumeThread(), CreteIOCompletionPort() and GetQueuedCompletionStatus() APIs for multithreading.

Finally, the ransom note is displayed, as shown in Figure 7.



Restore_My_Files.txt - Notepad

File Edit Format View Help

```
### 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://vbfqeh5nugm6r2u2qvghsdxm3fot[redacted]d.onion*
(you should download and install TOR browser first hxxps://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@pa[redacted]
#### !!!Warning!!!
```

Restore_My_Files.txt - Notepad

File Edit Format View Help

```
### 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://vbfqeh5nugm6r2u2qvghsdxm3fot[redacted]d.onion*
(you should download and install TOR browser first hxxps://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@pa[redacted]
#### !!!Warning!!!
```

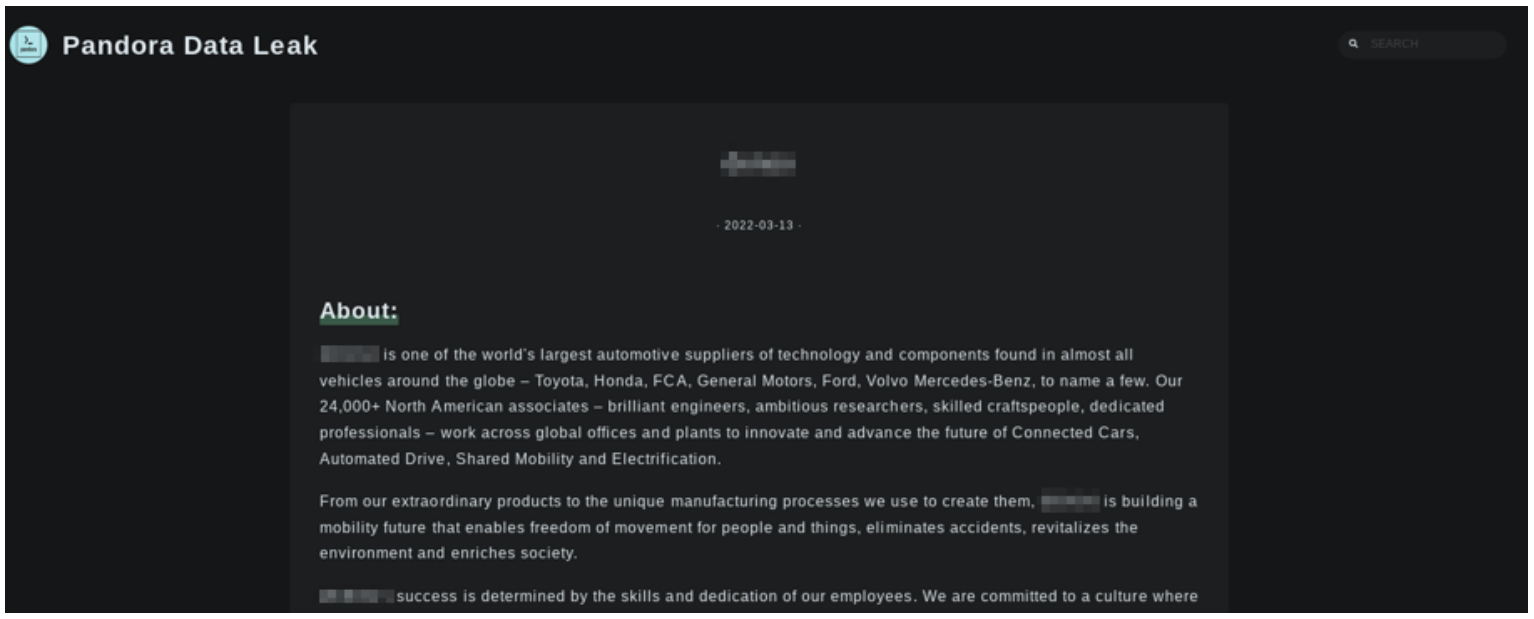
Figure 7: Ransom note

Possible ROOK ransomware re-brand:

During our analysis, we found that the Tactic Technique and Procedures (TTPs) of the Pandora and ROOK ransomware shared a lot of similarities.

In Dec 2021, ROOK ransomware posted on their leak site claiming to have attacked one of the world's largest automotive suppliers of technology and components. Following this, their leak site went down around the end of Jan 2022.

Pandora ransomware in March 2022 posted the same victim on their leak site. Due to this incident and the similarities in how they operate, it is suspected that Pandora might be a re-brand of ROOK ransomware.



Pandora Data Leak
SEARCH
· 2022-03-13 ·
About:
is one of the world's largest automotive suppliers of technology and components found in almost all vehicles around the globe – Toyota, Honda, FCA, General Motors, Ford, Volvo Mercedes-Benz, to name a few. Our 24,000+ North American associates – brilliant engineers, ambitious researchers, skilled craftspeople, dedicated professionals – work across global offices and plants to innovate and advance the future of Connected Cars, Automated Drive, Shared Mobility and Electrification.
From our extraordinary products to the unique manufacturing processes we use to create them, is building a mobility future that enables freedom of movement for people and things, eliminates accidents, revitalizes the environment and enriches society.
success is determined by the skills and dedication of our employees. We are committed to a culture where

Figure 8: Pandora ransomware leak site

Conclusion

There's a good chance that Pandora ransomware is a re-brand of ROOK ransomware. We had observed similar behavior in the past when ransomware groups were coming up with new aliases when they were under scrutiny.

Pandora ransomware gang is suspected of leveraging the double extortion method where the TAs exfiltrate the victim's data followed by data encryption. Then, they threaten to leak the exfiltrated data on their leak site or on cybercrime forums.

Organizations can mitigate such attacks by monitoring the darkweb and acting upon early warning indicators such as compromised credentials, data breaches, and identifying vulnerabilities traded on cybercrime forums.

Our Recommendations:

- Enforce password change policies for the network and critical business applications or consider implementing multi-factor authentication for all remote network access points.
- Reduce the attack surface by ensuring that sensitive ports are not exposed on the Internet.
- Conduct cybersecurity awareness programs for employees and contractors.
- Implement a risk-based vulnerability management process for IT infrastructure to ensure that critical vulnerabilities and security misconfigurations are identified and prioritized for remediation.
- Instruct users to refrain from opening untrusted links and email attachments without verifying their authenticity.
- Deploy reputed anti-virus and internet security software package on your company-managed devices, including PCs, laptops, and mobile devices.
- Turn on the automatic software update features on computers, mobiles, and other connected devices wherever possible and pragmatic.
- Define and implement a backup process and secure those backup copies by keeping them offline or on a separate network

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
Privilege Escalation	T1548 T1134	Abuse Elevation Control Mechanism Access Token Manipulation

Defense Evasion	T1112 T1027 T1562.001	Modify Registry Obfuscated Files or Information Impair Defenses: Disable or Modify Tools
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Impact	T1490 T1489 T1486	Inhibit System Recovery Service Stop Data Encrypted for Impact

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
0c4a84b66832a08dccc42b478d9d5e1b 160320b920a5ef22ac17b48146152ffbef60461f	Md5 SHA-1	Executable
5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b	SHA-256	binary

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.