

# Deep Dive Analysis – Pandora Ransomware

---

 [blog.cyble.com/2022/03/15/deep-dive-analysis-pandora-ransomware/](https://blog.cyble.com/2022/03/15/deep-dive-analysis-pandora-ransomware/)

March 15, 2022



## 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.

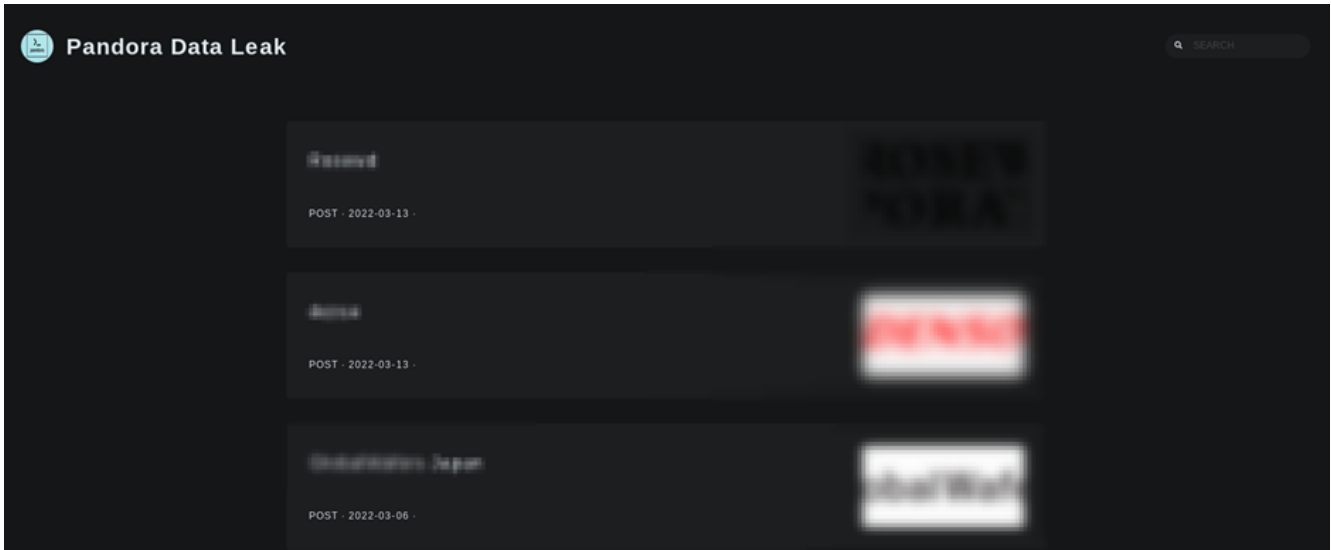


Figure 1: Pandora ransomware data leak site

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".

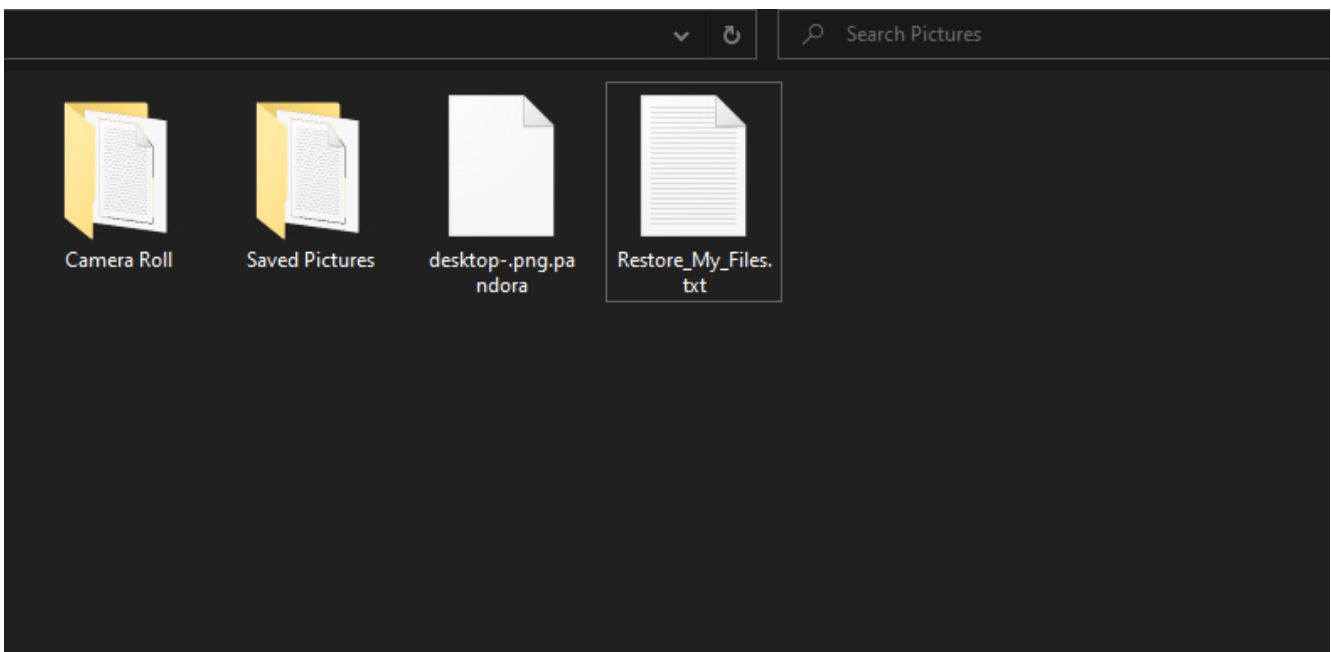


Figure 2: Encrypted Files

## 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.

```

v FFE2          JMP RDX
3D 2EAE0BC3    CMP EAX,C30BAE2E
BA A0010000    MOV EDX,1A0
49:0F4CD5      CMOVL RDX,R13
48:8B1411      MOV RDX,QWORD PTR DS:[RCX+RDX]
4C:01F2        ADD RDX,R14
v FFE2          JMP RDX
3D 272699A2    CMP EAX,A2992627
BA 08000000    MOV EDX,8
48:0F4CD6      CMOVL RDX,R13
48:8B1411      MOV RDX,QWORD PTR DS:[RCX+RDX]
4C:01F2        ADD RDX,R14
v FFE2          JMP RDX
3D AF162AA2    CMP EAX,A22A16AF
BA D0000000    MOV EDX,D0
BD D8010000    MOV ESP,1D8
48:0F4CD5      CMOVL RDX,RBP
48:8B1411      MOV RDX,QWORD PTR DS:[RCX+RDX]
4C:01F2        ADD RDX,R14
v FFE2          JMP RDX
3D 3404BC8C    CMP EAX,8CBC0434
BA 28000000    MOV EDX,28
BD 80000000    MOV ESP,80
48:0F44D5      CMOVE RDX,RBP
48:8B0C11      MOV RCX,QWORD PTR DS:[RCX+RDX]
4C:01F1        ADD RCX,R14
v FFE1          JMP RCX
48:8B8C24 90000000  MOV RCX,QWORD PTR SS:[RSP+90]
8B5424 30      MOV EDX,DWORD PTR SS:[RSP+30]
B8 45735DA8    MOV EAX,A85D7345
01C2          ADD EDX,EAX
8B4424 30      MOV EAX,DWORD PTR SS:[RSP+30]
BD 3392FB41    MOV EBX,41FB9233
01E8          ADD EAX,EBX
48:85C9        TEST RCX,RCX
0F45C2        CMOVNE EAX,EDX

```

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.

```

. 48:C1EE 20    SHR RSI,20
. 89D8         MOV EAX,EBX
. 29F0         SUB EAX,ESI
. D1E8         SHR EAX,1
. 01F0         ADD EAX,ESI
. C1E8 04      SHR EAX,4
. 8D3480      LEA ESI,QWORD PTR DS:[RAX+RAX*4]
. 8D0480      LEA EAX,QWORD PTR DS:[RAX+RSI*4]
. 89DF         MOV EDI,EBX
. 29C7         SUB EDI,EAX
. 0FB6043A    MOVZX EAX,BYTE PTR DS:[RDX+RDI]
. 41:32041E   XOR AL,BYTE PTR DS:[R14+RBX]
. 8B0419      MOV BYTE PTR DS:[RCX+RBX],AL
. 44:8D5B 01  LEA R10,QWORD PTR DS:[RBX+1]

```

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.

```

1: rcx 0000000000000000
2: rdx 0000000000000000
3: r8 00007FF7FA55E15B "ThisIsMutexa"
4: r9 00000000A188260E
5: [rsp+20] 0000000000000000

```

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.

```
1: rcx 0000000000000000
2: rdx 00007FF7CB8C7A26 L"open"
3: r8 00007FF7CB8C7A16 L"cmd.exe"
4: r9 00007FF7CB8C79C0 L"/c vssadmin.exe delete shadows /all /quiet"
5: [rsp+20] 0000000000000000
```

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()*, *CreateIoCompletionPort()* 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...*
```

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.

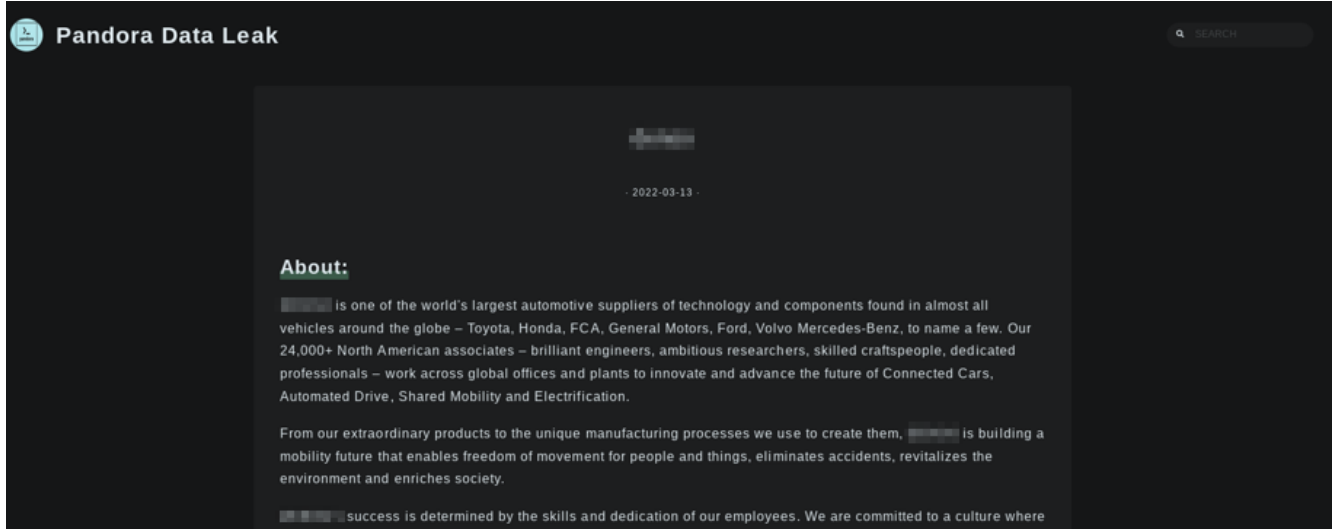


Figure 8: Pandora ransomware leak site

### 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
<b>Execution</b>	<u>T1059</u>	Command and Scripting Interpreter
<b>Privilege Escalation</b>	<u>T1548</u> <u>T1134</u>	Abuse Elevation Control Mechanism Access Token Manipulation
<b>Defense Evasion</b>	<u>T1112</u> <u>T1027</u> <u>T1562.001</u>	Modify Registry Obfuscated Files or Information Impair Defenses: Disable or Modify Tools
<b>Discovery</b>	<u>T1082</u> <u>T1083</u>	System Information Discovery File and Directory Discovery
<b>Impact</b>	<u>T1490</u> <u>T1489</u> <u>T1486</u>	Inhibit System Recovery Service Stop Data Encrypted for Impact

## Indicators of Compromise (IoCs):

---

Indicators	Indicator type	Description
0c4a84b66832a08dccc42b478d9d5e1b 160320b920a5ef22ac17b48146152ffbef60461f 5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b	<b>Md5</b> <b>SHA-1</b> <b>SHA-256</b>	Executable 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](http://www.cyble.com).