Orion Team

Monthly Ransomware Activity

Written by: Maor Huli

April, 2022
Contents

Executive Summary .................................................................................................................. 3
Axxes .................................................................................................................................. 5
Blaze ..................................................................................................................................... 6
BlockZ ..................................................................................................................................... 7
DemocracyWhisperers .......................................................................................................... 8
Medusa .................................................................................................................................. 9
Snatch .................................................................................................................................... 10
Parker .................................................................................................................................... 11
Executive Summary

Orion is an integral department in Cynet’s research team that works around the clock to track threat intelligence resources, analyze payloads, and automate labs to ensure that our customers are protected against the newest ransomware variants. In these monthly reports, Orion reviews the latest trends identified in Bleeping Computer – the most up-to-date website that summarizes the newest ransomware variants – and shares how Cynet detects against these threats.
Orion Team

Cynet 360 AutoXDR™ VS Ransomware
Axxes Ransomware

- Observed since: April 2022
- Ransomware encryption method: RSA + AES.
- Ransomware extension: .axxes
- Ransomware note: RESTORE_FILES_INFO.txt
- Sample hash: ec7fbdf548bd27bb5076dd9e1b8f3c570da80ed7c127eb4cd4541d76f7

Cynet 360 AutoXDR™ Detections:

Axxes Overview

Axxes ransomware renames the encrypted files with .axxes in the extension:

Once a computer’s files have been encrypted and renamed, it drops a note as RESTORE_FILES_INFO.txt:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains only the encryption key.
Blaze Ransomware
- Observed since: December 2021
- Ransomware encryption method: RSA.
- Ransomware extension: .blaze
- Ransomware note: How To Decrypt.txt
- Sample hash: 25835a890a218fd26bfd8b23696576402b5eb8a4c3af4a51512e44c4f00a9fcco

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information and the attacker’s contact information:

Blaze Overview
Blaze ransomware renames the encrypted files with .blaze in the extension:

Once a computer’s files have been encrypted and renamed, it drops a note as How To Decrypt.txt:
BlockZ Ransomware
- Observed since: April 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .blockZ
- Ransomware note: How To Restore Your Files.txt
- Sample hash: 856d9e698f240a21db57f404fea33ee65cd0458f31a9d0fca7044962204484c9

Once a computer's files have been encrypted and renamed, it drops a note as How To Restore Your Files.txt:

Upon execution, it first drops a file in the path "c:\users\*user\appdata\local\temp\" with the name of Noopen.exe

Once executed the dropped file it changes the process name to schtasks.exe and it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains contact information, warnings, and decryption test for 1 file:
DemocracyWhisperers Ransomware

- Observed since: April 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .democ
- Ransomware note: Restore Files.txt
- Sample hash: 59e0e38b068f736e7f618c714a116ad13fb50a1932942c0f89474d6317fb4592

Once a computer's files have been encrypted and renamed, it drops a note as Restore Files.txt:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker's contact info.
Medusa Ransomware
- Observed since: Late 2019
- Ransomware encryption method: AES + RSA
- Ransomware extension: .stopfiles
- Ransomware note: Recovery_instructions.html
- Sample hash: 2ca49be7f3eac14dfbf086ad11ce1235079b4fa96b7d863403cfcf592969

Once a computer’s files have been encrypted and renamed, it drops a note as Recovery_instructions.html:

Upon execution, it injects itself to svchost and it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker’s contact info:

<table>
<thead>
<tr>
<th>Orion Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monthly Ransomware Activity – April 2022 ©ALL RIGHTS RESERVED TO CYNET 2022 <a href="http://WWW.CYNET.COM">WWW.CYNET.COM</a></td>
</tr>
</tbody>
</table>
Snatch Ransomware

- **observed since**: December 2018
- **Ransomware encryption method**: AES + RSA
- **Ransomware extension**: .sdhvqq
- **Ransomware note**: HOW TO RESTORE YOUR FILES

**Sample hash**: 25835a890a218fd26bfd8b23696576402b5eb8a4c9af4a51529e14c4f00a9cce

Once a computer’s files have been encrypted and renamed, it drops a note as HOW TO RESTORE YOUR FILES. TXT:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker’s contact info:

Cynet 360 AutoXDR™ Detections:

Snatch Overview

Snatch ransomware renames the encrypted files with .sdhvqq in the extension:

Once a computer’s files have been encrypted and renamed, it drops a note as HOW TO RESTORE YOUR FILES. TXT:
Parker Ransomware
- Observed since: April 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .PARKER
- Ransomware note: RESTORE_FILES_INFO.txt
- Sample hash: 39a044db72d3ca39122af249cd60660d7e200366af958c762910605eaed020cb

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions, threats for data publication, and the attacker's contact info:

Once a computer's files have been encrypted and renamed, it drops a note as RESTORE_FILES_INFO.txt.