## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Odaku</td>
<td>5</td>
</tr>
<tr>
<td>Kekpop</td>
<td>6</td>
</tr>
<tr>
<td>Japan</td>
<td>7</td>
</tr>
<tr>
<td>EarthGrass</td>
<td>8</td>
</tr>
<tr>
<td>CryptBIT</td>
<td>9</td>
</tr>
</tbody>
</table>
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.

The Week in Ransomware - May 20th 2022 - Another one bites the dust
Ransomware attacks continue to slow down, likely due to the invasion of Ukraine, instability in the region, and subsequent worldwide sanctions against Russia.
LAWRENCE ABRAMS MAY 20, 2022 08:38 PM 0

The Week in Ransomware - May 13th 2022 - A National Emergency
While ransomware attacks have slowed during Russia’s invasion of Ukraine and the subsequent sanctions, the malware threat continues to affect organizations worldwide.
LAWRENCE ABRAMS MAY 13, 2022 04:56 PM 0

The Week in Ransomware - May 6th 2022 - An evolving landscape
Ransomware operations continue to evolve, with new groups appearing and others quietly shutting down their operations or rebranding as new groups.
LAWRENCE ABRAMS MAY 06, 2022 06:27 PM 0
Orion Team

Cynet 360 AutoXDR™ VS Ransomware

©ALL RIGHTS RESERVED TO CYNET 2022 WWW.CYNET.COM
Odaku Ransomware

- Observed since: Late 2021
- Ransomware enforcement method: RSA + AES.
- Ransomware extension: [4 random characters]
- Ransomware note: read_it.txt
- Sample hash: d6799d0d74814958c4821509b0c4c83482f91d927d2d4abbb53ce98146a0cacc

Cyben 360 AutoXDR™ Detections:

Odaku Overview

Odaku ransomware is supposed to rename the encrypted files with [4 random char], in the extension but no encryption was observed.

Upon execution, it immediately copies itself to the folder "C:saws\user\AppData\Roaming" with the name of "svchost.exe". The icon of Netflix, and popup the ransomware note, the ransomware note contains only the attacker crypto-currency wallet and the telegram name (demands 25$ in bitcoins):

Once a computer’s files have been supposed to be encrypted and renamed, it drops a note as read_it.txt.
Kekpop Ransomware

• Observed since: May 2022
• Ransomware encryption method: RSA + AES
• Ransomware extension: .kekpop
• Ransomware note: does not exist
• Sample hash: 3560efa18b48f0e707f190c7f244be2a5080829d6710e8aee4c7e8767314b808

Cynet 360 AutoXDR™ Detections:

Open a computer file has been encrypted and renamed, it attempts to drop the ransomware note that is supposed to be ReadMe.html but since it’s using Pastebin to download the note, Pastebin blocked the account and it cannot be downloaded, which means, no encryption key or how to contact the attacker.

Once a computer file has been encrypted and renamed, it attempts to drop the ransomware note that is supposed to be ReadMe.html but since it’s using Pastebin to download the note, Pastebin blocked the account and it cannot be downloaded, which means, no encryption key or how to contact the attacker.

Kekpop Overview

Kekpop ransomware renames the encrypted files with .kekpop in the extension:

Once a computer file has been encrypted and renamed, it attempts to drop the ransomware note that is supposed to be ReadMe.html but since it’s using Pastebin to download the note, Pastebin blocked the account and it cannot be downloaded, which means, no encryption key or how to contact the attacker.

Upon execution, it immediately encrypts the endpoint using batch scripts:

<table>
<thead>
<tr>
<th>Name</th>
<th>PID</th>
<th>CPU %</th>
<th>V/O total</th>
<th>Private %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>6343</td>
<td>4.77</td>
<td>0.53</td>
<td>1.79</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>3144</td>
<td>2.57</td>
<td>0.44</td>
<td>2.32</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>6243</td>
<td>2.34</td>
<td>0.42</td>
<td>2.12</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>1494</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>6268</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>1484</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>8398</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>1912</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>2878</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>2038</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>6006</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>7372</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>8000</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>5564</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>3634</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>4626</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>2706</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>3853</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>3612</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>7166</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>7432</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>4098</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>1623</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>1932</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>5694</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>2904</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>1176</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>7314</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>8263</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>5944</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>9194</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>6362</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>4523</td>
<td>2.14</td>
<td>0.39</td>
<td>2.07</td>
</tr>
</tbody>
</table>

CPU Usage: 1.08%. Physical memory: 1.81 GB (33.02%). Processes: 173.
Japan Ransomware
- **Observed since**: May 2022
- **Ransomware encryption method**: AES + RSA
- **Ransomware extension**: .japan
- **Ransomware note**: how to decrypt.txt
- **Sample hash**: 4089e7b0a0469bd5877c830f962f8243dc1311349271e45e9b15cd6d97e0a2ea

Cynet 360 AutoXDR™ Detections:

**Japan Overview**

Japan ransomware renames the encrypted files with .japan in the extension.

Once a computer’s files have been encrypted and renamed, it drops a note named how to decrypt.txt.

Once executed, the dropped file will rename the files to the folder “C:\Users\user\AppData\Roaming” and changes the name to “svchost.exe”. In order to encrypt, it skips the endpoint and drops the ransomware note. The ransomware note is written in Vietnamese:

> After translating, the ransom note contains the attacker’s BTC address and “guarantees” only for 4 days for the decryption (demand 2000$ in bitcoin):

> In the end, it also changes the background.

---

**Japan Overview**

Japan ransomware renames the encrypted files with .japan in the extension.

Once a computer’s files have been encrypted and renamed, it drops a note named how to decrypt.txt.

Once executed, the dropped file will rename the files to the folder “C:\Users\user\AppData\Roaming” and changes the name to “svchost.exe”. In order to encrypt, it skips the endpoint and drops the ransomware note. The ransomware note is written in Vietnamese:

> After translating, the ransom note contains the attacker’s BTC address and “guarantees” only for 4 days for the decryption (demand 2000$ in bitcoin):

> In the end, it also changes the background.

---

**Japan Overview**

Japan ransomware renames the encrypted files with .japan in the extension.

Once a computer’s files have been encrypted and renamed, it drops a note named how to decrypt.txt.

Once executed, the dropped file will rename the files to the folder “C:\Users\user\AppData\Roaming” and changes the name to “svchost.exe”. In order to encrypt, it skips the endpoint and drops the ransomware note. The ransomware note is written in Vietnamese:

> After translating, the ransom note contains the attacker’s BTC address and “guarantees” only for 4 days for the decryption (demand 2000$ in bitcoin):

> In the end, it also changes the background.
EarthGrass Ransomware
- Observed since: May 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .34r7hGr455
- Ransomware note: Read ME (Decryptor).txt
- Sample hash: 248cdaf6abdf84a90acba1a1ae86a4764568f46aa893bc747c3cd3f2d613bb

Cynet 360 AutoXDR™ Detections:

EarthGrass Overview
EarthGrass ransomware renames the encrypted files with .34r7hGr455 in the extension:

Once a computer's files have been encrypted and renamed, it drops a note as ReadME (Decryptor).txt.

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

WORLD GRASS

All your files have been encrypted due to a security problem with your PC. To avoid the potential loss of data, the attacker's instructions are as follows:
1. Send 5MB EVE to mcrypto@e-mail.com
2. Open the note created by the script
3. Execute the instructions contained in the note
4. Send 5MB EVE to mcrypto@e-mail.com

- To learn more about EarthGrass, visit the website:
- To report EarthGrass-related activity, contact the cybersecurity team at Cynet.
CryptBIT Ransomware

- Observed since: May 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .cryptbit
- Ransomware note: CryptBIT-restore-files.txt
- Sample hash: edf4a4444890ea957099f94822c9fa5b859ade205ea5a5d187c1e5f88badc6dd

CyNet 360 AutoXDR™ Detections:

CryptBIT Overview

CryptBIT ransomware encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker's bitcoin wallet address:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker's bitcoin wallet address:

When the encryption ends, the ransomware also changes the wallpaper:

All your files are encrypted and stolen by us.
Your documents, photos, music, videos, and more are now a permanent part of the ransomware's database.

To recover your files, follow these steps:

1. Transfer the ransomware's bitcoin wallet address to your bank account.
2. Contact your local law enforcement agency to report the ransomware attack.
3. Contact your insurance provider to determine if your policy covers ransomware attacks.

By following these steps, you will be able to recover your files and protect yourself from future ransomware attacks.
Thank you!

May, 2022