Contents

Executive Summary ................................................................................................................................. 3
Loki .................................................................................................................................................... 5
BlueSky .............................................................................................................................................. 6
Babuk .................................................................................................................................................. 7
LockBit 3.0 .......................................................................................................................................... 8
Matrix ............................................................................................................................................... 9
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 - July 22nd 2022 - Attacks abound
New ransomware operations continue to be launched this week, with the new Luna ransomware found to be targeting both Windows and VMware ESXi servers.

The Week in Ransomware - July 8th 2022 - One down, many to go
While we continue to see new ransomware operations launch, we also received some good news this week, with another ransomware shutting down.

The Week in Ransomware - July 1st 2022 - Bug Bounties
It has been relatively busy this week with new ransomware attacks unveiled, a bug bounty program introduced, and new tactics used by the threat actors to distribute their encryptors.
Loki Ransomware

- Observed since: Late 2021
- Ransomware encryption method: AES + RSA
- Ransomware extension: .PayForKey
- Ransomware note: Restore-My-Files.txt
- Sample hash: f2522a56f9416eb701afc1773c08e9a3cc9143c8880954140e515f66a0028637

Cynet 360 AutoXDR™ Detections:

Loki Overview

Loki ransomware renames the encrypted files with .PayForKey, along with the attacker’s email and the host ID in the extension.

The ransomware also encrypts the entire Drive C (the system drive).

Eventually, it shuts down the computer and locks out the user until a payment.

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

The ransomware note contains general information, warnings, and the attacker’s email address:

Before shutting down, the ransomware also changes the desktop background.
BlueSky Ransomware

- Observed since: 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: bluesky
- Ransomware note: # DECRYPT FILES BLUESKY #.txt | .html
- Sample hash: 3e035f2d7d30869ce5317e1e0a07f615b0c14b4d96e6a38e20b8d966c2b

BlueSky Overview

BlueSky ransomware renames the encrypted files with .bluesky in the extension:

Once a computer’s files have been encrypted and renamed, it attempts to drop the ransomware note named # DECRYPT FILES BLUESKY #.txt | .html:

That ransomware note contains general information, warnings, and the attacker’s tor website.
Babuk Ransomware

- Observed since: Early 2021
- Ransomware encryption method: AES + RSA
- Ransomware extension: .again
- Ransomware note: How To Restore Your Files.txt
- Sample hash: 047a6c39806168e7e66b2ef2297b7019cc3e5336dc0b33ec3af83f9e3aa1f798

Babuk Overview

Babuk ransomware renames the encrypted files with .again in the extension:

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

The ransom note contains only a Tor website with a chat token to contact the attacker:
LockBit 3.0 Ransomware

- Observed since: Mid 2022
- Ransomware encryption method: AES + RSA
- Ransomware format: .[a-zA-Z0-9]{9}
- Ransomware note: [a-zA-Z0-9]{9}.readme.txt
- Sample hash: 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce

LockBit 3.0 ransomware renames the encrypted files with .(9 characters) in the extension:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings, and several attacker's links:

LockBit 3.0 Overview

LockBit 3.0 needs to execute by a specific method for it to work.

The executable needs to be renamed to "{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe" and needs to be executed with the following parameters:

```
-k LocalServiceNetworkRestricted -pass db66023ab2abcb9957fb01ed50cdfa6a
```

via CMD or PowerShell:  

```
\4\Local\Service\\s\Net\w\Restricted -\p\ass\db66023ab2abcb9957fb01ed50cdfa6a
```

LockBit 3.0 AutoXDR™ Detections:
Matrix Ransomware

- Observed since Late 2016
- Ransomware encryption method: AES + RSA
- Ransomware extension: .KOK08
- Ransomware note: README_KOK08.txt
- Sample hash: 1006bb0f89f4780fb9920bff1b6692f6f0cc921fd7d561f6e0ecea501543a5cb

Matrix Overview

Matrix ransomware renames the encrypted files with .KOK08 in the extension:

Once a computer’s files have been encrypted and renamed, it drops a note as README_KOK08.txt:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings, and the attacker’s emails.
Thank you!

July, 2022