Orion Team

Monthly Ransomware Activity

Written by: Maor Huli

January, 2023
The ransomware from January to introduce are:

1. Upsilon
2. KoRyA
3. Bettercallsaul
4. Sickfile
Executive Summary

As an integral department in Cynet’s research team, Orion 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 these threats.

The Week in Ransomware - January 27th 2023 - 'We hacked the hackers'
For the most part, this week has been relatively quiet regarding ransomware attacks and researcher — that is, until the FBI announced the disruption of the Hive ransomware operation.

The Week in Ransomware - January 20th 2023 - Targeting Crypto Exchanges
There has been quite a bit of ransomware news this week, with crypto exchanges being seized for alleged money laundering and researchers providing fascinating reports on the behavior of ransomware operators.

The Week in Ransomware - January 13th 2023 - LockBit in the spotlight
The LockBit ransomware operation has again taken center stage in the ransomware news, as we learned yesterday they were behind the attack on Royal Mail.

The Week in Ransomware - January 6th 2023 - Targeting Healthcare
This week saw a lot of ransomware news, ranging from new extortion tactics, to a ransomware gang giving away a free decryptor after attacking a children’s hospital.
Orion Team

Cynet 360 AutoXDR™ VS Ransomware
**Upsilon Ransomware**

- **Observed since:** Jan 2023
- **Ransomware encryption method:** AES + RSA
- **Ransomware extension:** .upsilon
- **Ransomware note:** Upsilon.txt
- **Sample hash:** ee23f0addbae4b3c384d99c15adda491ed637df33348a090993a23867f6ee7c

**Cynet 360 AutoXDR™ Detections:**

**Upsilon Overview**

Upsilon ransomware renames the encrypted files with “.upsilon” in the extension:

Once a computer’s files have been encrypted and renamed, Upsilon drops a note named “Upsilon.txt”:

Upon execution, Upsilon immediately encrypts the endpoint and drops the ransomware note.

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

The ransomware also changes the desktop’s background:
Cynet 360 AutoXDR™ Detections:

KoRyA Overview

KoRyA ransomware renames the encrypted files with “.KoRyA” in the extension:

Once a computer’s files have been encrypted and renamed, KoRyA drops a note named “HOW TO DECRYPT FILES.txt”:

Upon execution, KoRyA immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings, and the attacker’s email address and Bitcoin wallet:
Bettercallsaul Ransomware

- Observed since: Mid-2021
- Ransomware encryption method: AES-256
- Ransomware extension: .bettercallsaul
- Ransomware note: DECRYPT_MY_FILES.txt
- Sample hash: 3268b1b9a1fa23085926ddef9cbb31a7de8bcadc4eeff9f2dfe520bf4e603a7

Once a computer’s files have been encrypted and renamed, Bettercallsaul drops a note named “DECRYPT_MY_FILES.txt”:

Upon execution, Bettercallsaul immediately encrypts the endpoint and drops the ransomware note.

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

The ransomware also changes the desktop background:
SickFile Ransomware

- Observed since: Jan 2023
- Ransomware encryption method: AES + RSA
- Ransomware extension: .sickfile
- Ransomware note: how_to_back_files.html
- Sample hash: 1c2d5ccc5bb4635198b895c8a206c346de09c2f1ab7a123deb3d3e4a539

Once a computer's files have been encrypted and renamed, SickFile drops a note named "how_to_back_files.html":

Upon execution, SickFile immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings, and the attacker's email address:
Thank you!