

Orion Team

Monthly Ransomware Activity

Written by: Maor Huli



January, 2023



The ransomware from January to introduce are:

1. Upsilon	5
2. KoRyA	6
3. Bettercallsaul	7
4. Sickfile	8



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.

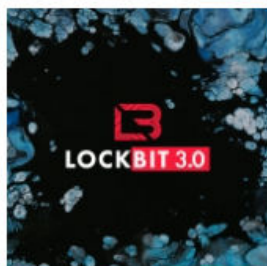
LAWRENCE ABRAMS JANUARY 27, 2023 07:08 PM 0



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.

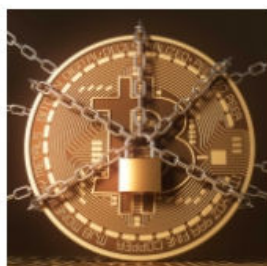
LAWRENCE ABRAMS JANUARY 20, 2023 05:08 PM 0



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.

LAWRENCE ABRAMS JANUARY 13, 2023 07:17 PM 0



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.

LAWRENCE ABRAMS JANUARY 06, 2023 07:51 PM 1

Orion Team



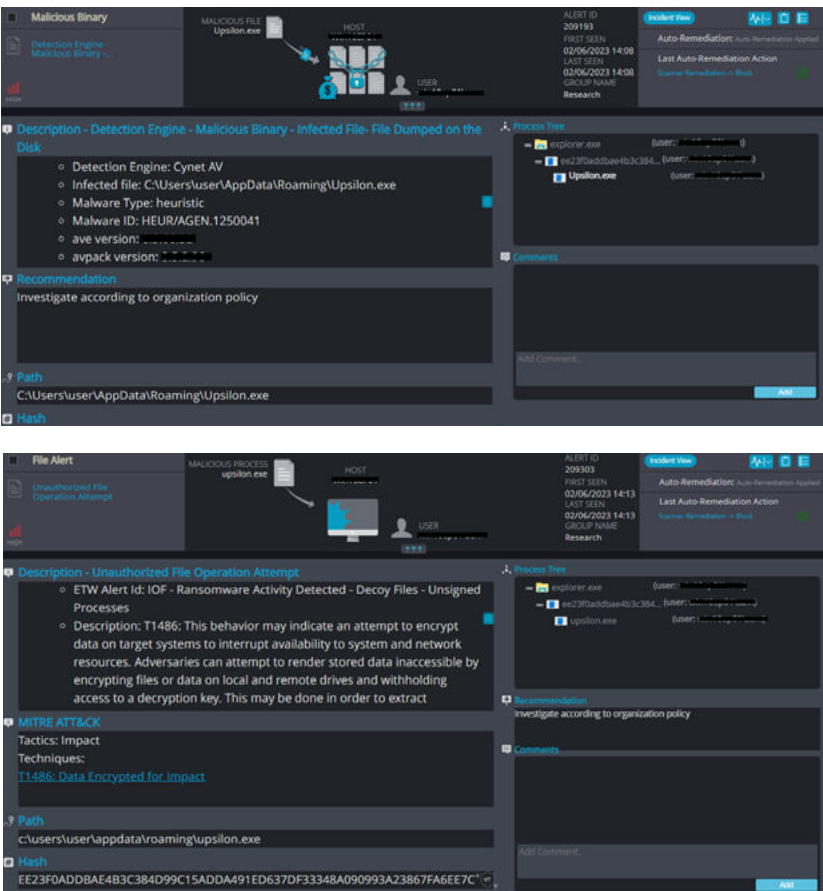
Cynet 360 AutoXDR™ VS Ransomware



Upsilon Ransomware

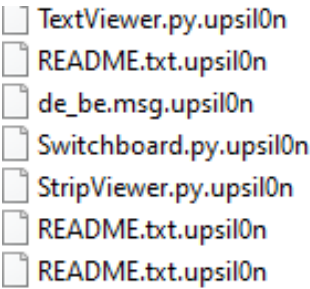
- Observed since: Jan 2023
- Ransomware encryption method: AES + RSA
- Ransomware extension: .upsilon
- Ransomware note: Upsilon.txt
- Sample hash: ee23f0addbae4b3c384d99c15adda491ed637df33348a090993a23867fa6ee7c

Cynet 360 AutoXDR™ Detections:

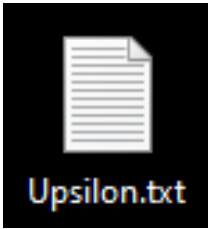


Upsilon Overview

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

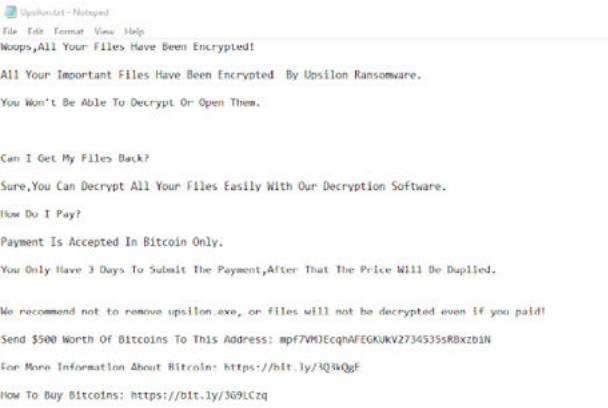


Once a computer’s files have been encrypted and renamed, Upsilon drops a note named “Upsilon.txt”:



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:





KoRyA Ransomware

- Observed since: Mid-2019
- Ransomware encryption method: AES + RSA
- Ransomware extension: .KoRyA
- Ransomware note: HOW TO DECRYPT FILES.txt
- Sample hash: b2447bb9ef759c890d75e31eb07f0553065d74403f654c9757635b02f1b753be

Cynet 360 AutoXDR™ Detections:

Xorist Ransomware variant

Malicious Binary

Detection Engine - Malicious Binary ...

HIGH

MALICIOUS FILE

b2447bb9ef759c...

HOST

USER

ALERT ID

209188

FIRST SEEN

02/06/2023 14:07

LAST SEEN

02/06/2023 14:20

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Detection Engine - Malicious Binary - Infected File- File Dumped on the Disk

- Detection Engine: Cynet AV
- Infected file: C:\Users\user\Desktop\jan 2023 ransomware\jan 2023 ransomware\KoRyA\b2447bb9ef759c890d75e31eb07f0553065d74403f654c9757635b02f1b753be
- Malware Type: trojan
- Malware ID: TR/Ransom.Xorist.EJ
- ave version:

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\jan 2023 ransomware\jan 2023 ransomware\KoRyA\b2447bb9ef759c890d75e31eb07f0553065d74403f654c9757635b02f1b753be

Hash

B2447BB9EF759C890D75E31EB07F0553065D74403F654C9757635B02F1B753BE

Process Tree

- explorer.exe (user:)
- winrar.exe (user:)
- b2447bb9ef759c890d... (user:)

Comments

Add Comment...

Add

Ransomware

Memory Pattern - Ransomware - Xorist v4

CRITICAL

MALICIOUS PROCESS

b2447bb9ef759c...

HOST

USER

ALERT ID

209305

FIRST SEEN

02/06/2023 14:20

LAST SEEN

02/06/2023 14:20

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Rena...

Description - Memory Pattern - Ransomware - Xorist v4

- Signature Name: Memory Pattern - Ransomware - Xorist v4
- Matched Memory Area Bounds : From - 0x400000 - To - 0x401000 - Area Size - 4096
- Matched Memory Area Info : Type - IMAGE, AllocationBase - 0x400000, AllocationProtect - WCX, Protect - R
- Pattern(1) Offset [Address]: 3081 [0x400c09]
- Pattern(1) Distance From Previous Pattern Start: 3081
- Pattern(1) Dump Captured From: 0 [0x400000] - To - 4096 [0x401000]

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\jan 2023 ransomware\jan 2023 ransomware\korya\b2447bb9ef759c890d75e31eb07f0553065d74403f654c9757635b02f1b753be

Hash

B2447BB9EF759C890D75E31EB07F0553065D74403F654C9757635B02F1B753BE

Process Tree

- explorer.exe (user:)
- winrar.exe (user:)
- b2447bb9ef759c890d... (user:)

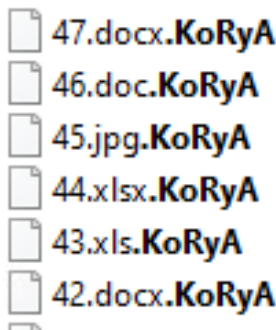
Comments

Add Comment...

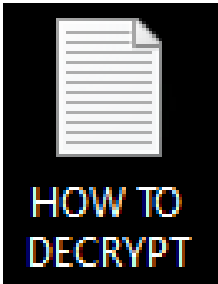
Add

KoRyA Overview

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

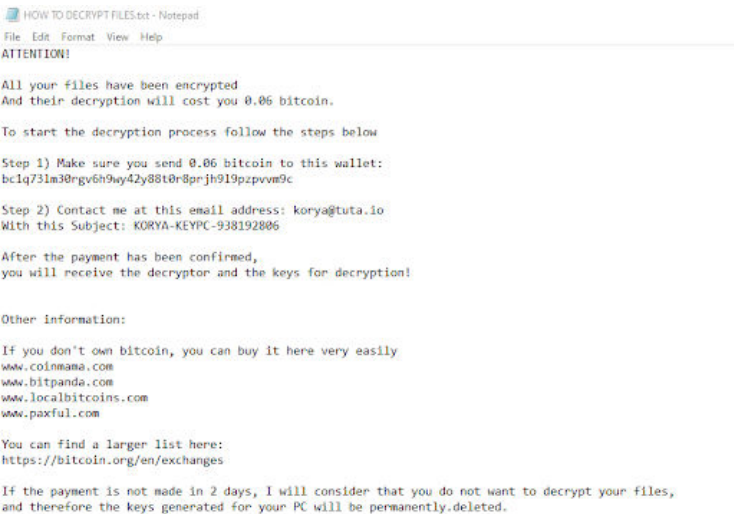


Once a computer’s files have been encrypted and renamed, KoRyA drops a note named “HOW TO DECRYPT FILES.txt”:



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

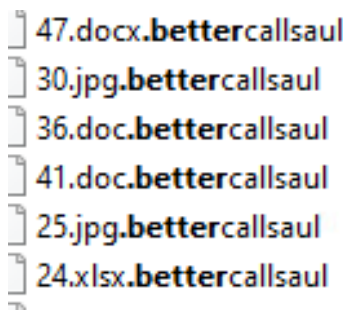
- Observed since: Mid-2021
- Ransomware encryption method: AES-256
- Ransomware extension: .bettercallsaul
- Ransomware note: DECRYPT_MY_FILES.txt
- Sample hash: 3268b1b9a1fa230859267defd9cb31a17e8bcadac4eef9fd2df4520bf4e603a7

Cynet 360 AutoXDR™ Detections:

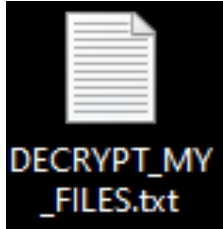


Bettercallsaul Overview

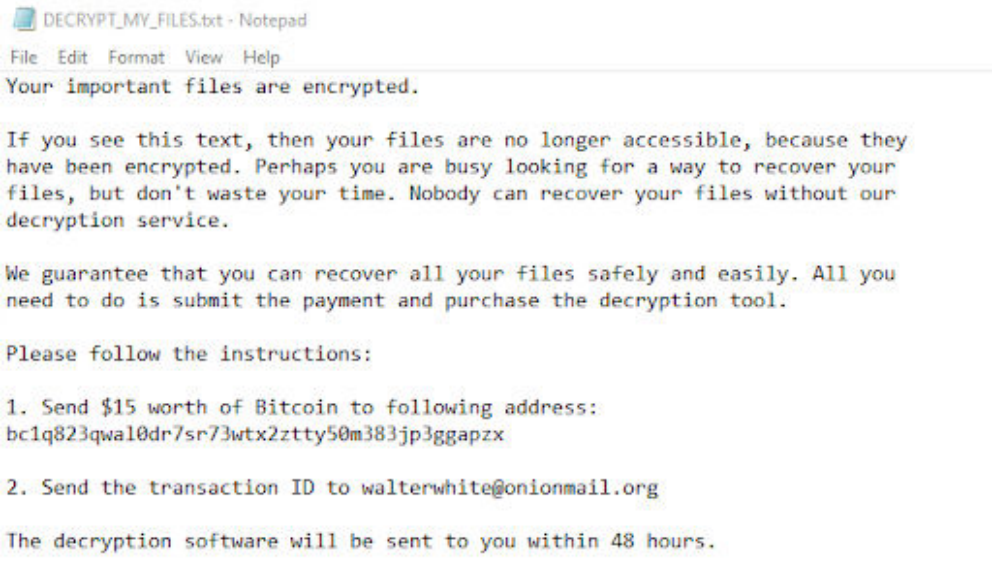
Bettercallsaul ransomware renames the encrypted files with “bettercallsaul” in the extension:



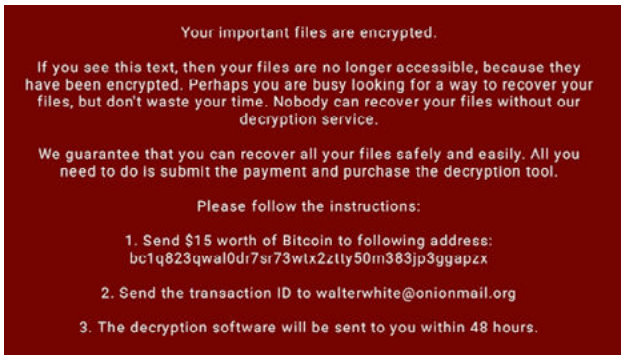
Once a computer’s files have been encrypted and renamed, Bettercallsaul drops a note named “DECRYPT_MY_FILES.txt”:



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: 1c2d5cccca58b469351980895c8a2080c8346de09c2f1ab7a123deb3d3e4a539

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

HIGH

MALICIOUS FILE

1c2d5cccca58b4...

HOST

ALERT ID

209878

FIRST SEEN

02/06/2023 14:52

LAST SEEN

02/06/2023 14:52

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Rana

Description - Detection Engine - Malicious Binary - Infected File- File Dumped on the Disk

- Detection Engine: Cynet AV
- Infected file: C:\Users\User\AppData\Local\1c2d5cccca58b469351980895c8a2080c8346de09c2f1ab7a123deb3d3e4a539.exe
- Malware Type: heuristic
- Malware ID: HEUR/AGEN.1238858
- ave version: 0.0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\AppData\Local\1c2d5cccca58b469351980895c8a2080c8346de09c2f1ab7a123deb3d3e4a539.

Hash

1C2D5CCCCA58B469351980895C8A2080C8346DE09C2F1AB7A123DEB3D3E4A539

Process Tree

- explorer.exe (user: ...)
- 1c2d5cccca58b469351... (user: ...)
- 1c2d5cccca58b469351... (user: ...)

Comments

Add Comment...

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

1c2d5cccca58b4...

HOST

ALERT ID

211480

FIRST SEEN

02/06/2023 15:43

LAST SEEN

02/06/2023 15:43

GROUP NAME

Research

Incident View

Auto-Remediation: Auto Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Unauthorized File Operation Attempt

- ETW Alert Id: IOF - Ransomware Note Found
- Description: T1486: This behavior may indicate an attempt to encrypt data on target systems to interrupt availability to system and network resources. Adversaries can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases

MITRE ATT&CK

Tactics: Impact

Techniques: T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\jan 2023 ransomware\jan 2023 ransomware\sickfile\1c2d5cccca58b469351980895c8a2080c8346de09c2f1ab7a123deb3d3e4a539.

Hash

1C2D5CCCCA58B469351980895C8A2080C8346DE09C2F1AB7A123DEB3D3E4A539

Process Tree

- explorer.exe (user: ...)
- 1c2d5cccca58b469351... (user: ...)

Recommendation

Investigate according to organization policy

Comments

Add Comment...

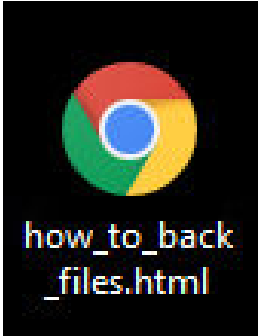
Add

SickFile Overview

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

- 3cfbe066ab600b15e17c72f65cc25bcd6defd684bb72e5d9aa577fbad8f5.sickfile
- f22fa31b850d07f8d92263849db0d7019715081c71c9f9d45d4e901eec73.sickfile
- 0d94357fd618d8c92ac670720530216961f35b9d649369bbfa5e0bf89fa5.sickfile
- 4b320068be667cb85ced241d5311571d9d4199a9c342180d60f6f4b341e5.sickfile
- 45a9ed8633b8df196c98020df2a9d80537ba8f189eb439665eff8ea0dff6.sickfile
- 7ca6d392c6ab89683c4e748a1e346caa3442eac25da32e76ff7464a315c2.sickfile
- 9f5e6196c4aff975b74d4aab924ab2416c48679ed9bb91e08bec18e547b4.sickfile

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:

YOUR PERSONAL ID:

⚠ YOUR COMPANY NETWORK HAS BEEN PENETRATED ⚠

All your important files have been encrypted!

Your files are safe! Only modified. (AES+RSA)

ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE WILL PERMANENTLY CORRUPT IT. DO NOT ATTEMPT TO ENCRYPTED FILES. DO NOT RENAME ENCRYPTED FILES.

No software available on internet can help you. We are the only ones able to solve your problem.

We preferred highly confidential personal data. These data are currently stored on a private server. This server will be immediately destroyed after your payment. If you decide to not pay, we will release your data to public or on online. So you can expect your data to be publicly available in the near future.

We only work money and our goal is not to damage your reputation or prevent your business from running.

You will can send us 2-3 most important files and we will decrypt it for free to prove we are able to give your files back.

Contact us for price and get decryption software.

Follow the instructions to open the link.

1. Start a chat and follow the further instructions.

If you can not use the above link, use the email:

doctorhelpers@gmail.com

helpersdoctor@outlook.com

* To contact us, create a new free email account on the site protonmail.com

IF YOU DON'T CONTACT US WITHIN 72 HOURS, PRICE WILL BE HIGHER.

Thank you!



January, 2023