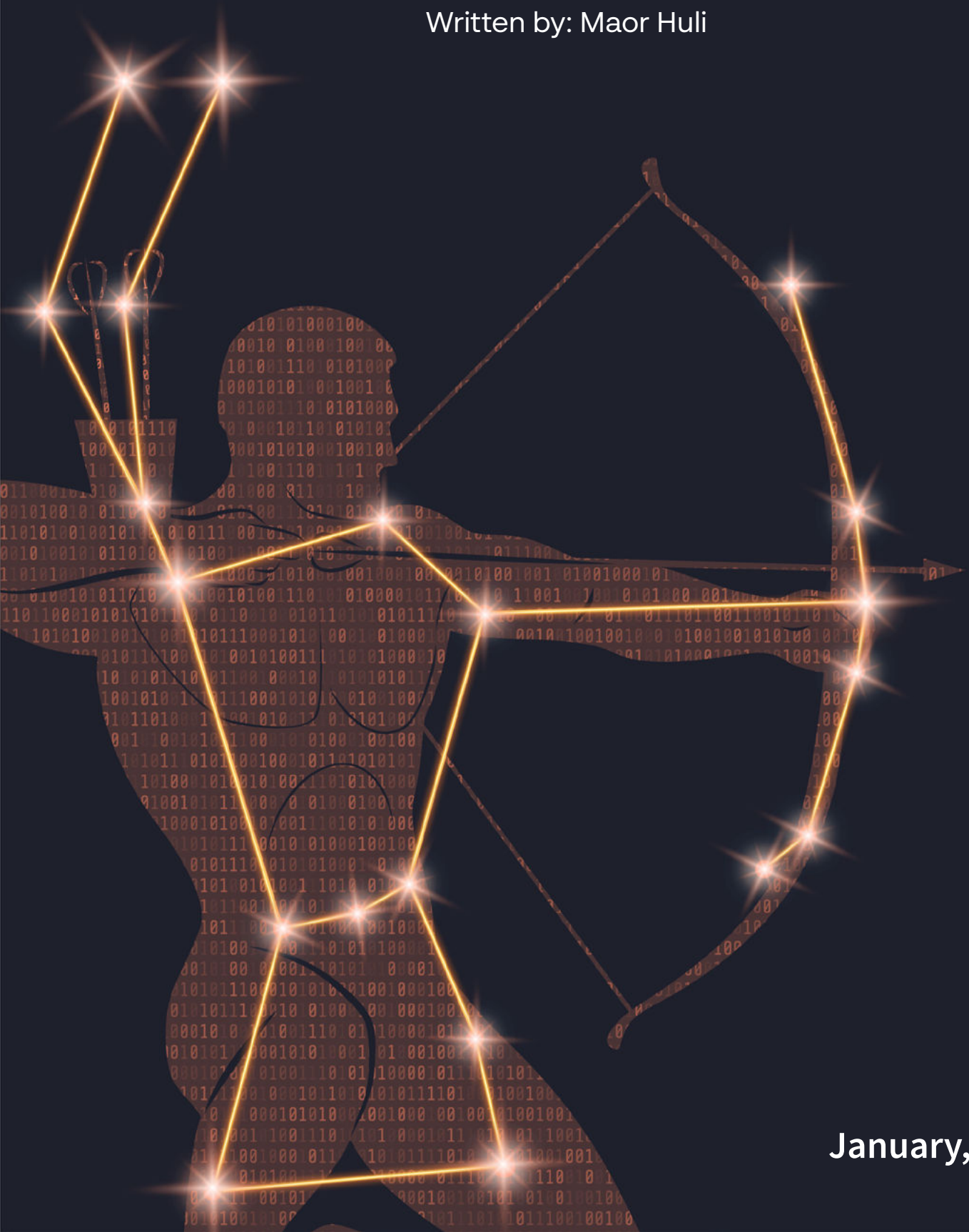
cynet

Orion Team

Monthly Ransomware Activity

Written by: Maor Huli



January, 2023

Orion Team

The ransomware from January to introduce are:

Orion Team

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

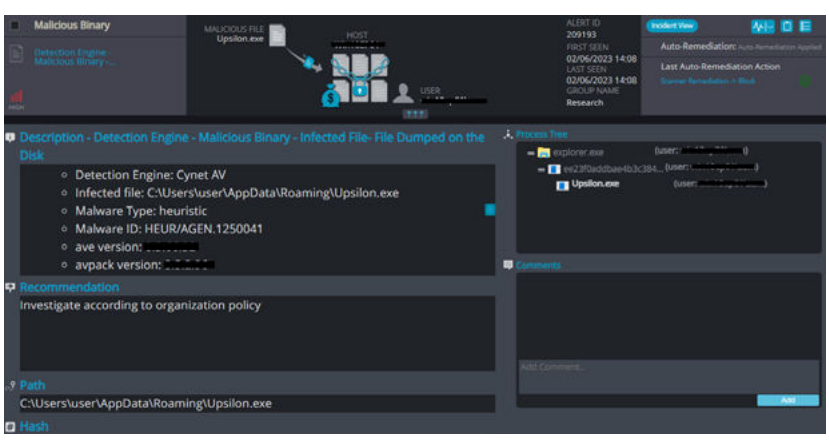
Cynet 360 AutoXDR™ VS Ransomware

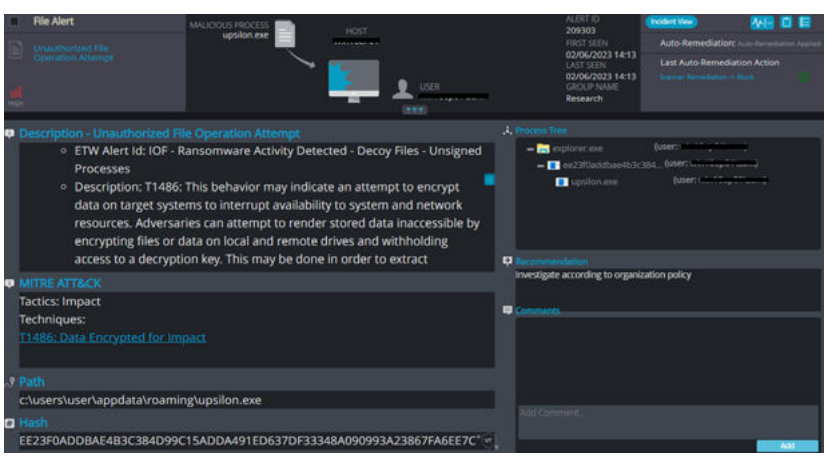
Orion Team

Upsilon Ransomware

- Observed since: Jan 2023
- Ransomware encryption method: AES + RSA
- Ransomware extension: .upsil0n
- Ransomware note: Upsilon.txt
- Sample hash: ee23f0addbae4b3c384d99c15adda491ed637df33348a090993a23867fa6ee7c

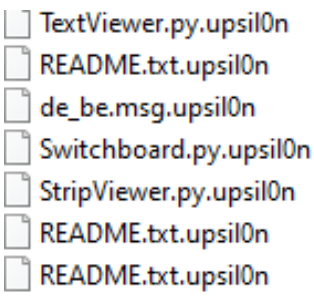
Cynet 360 AutoXDR™ Detections:



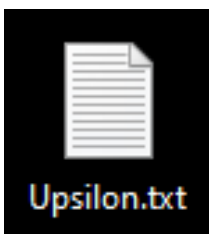


Upsilon Overview

Upsilon ransomware renames the encrypted files with “.upsil0n” in the extension:

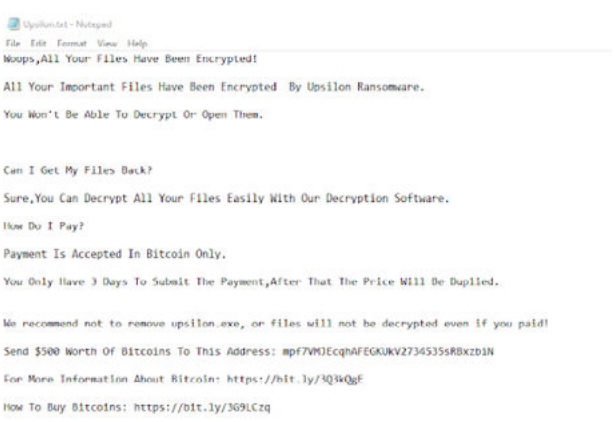


Once a computer’s files have been encrypted and renamed, Upsilon drops a note named “Upsilon.txt”:



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:

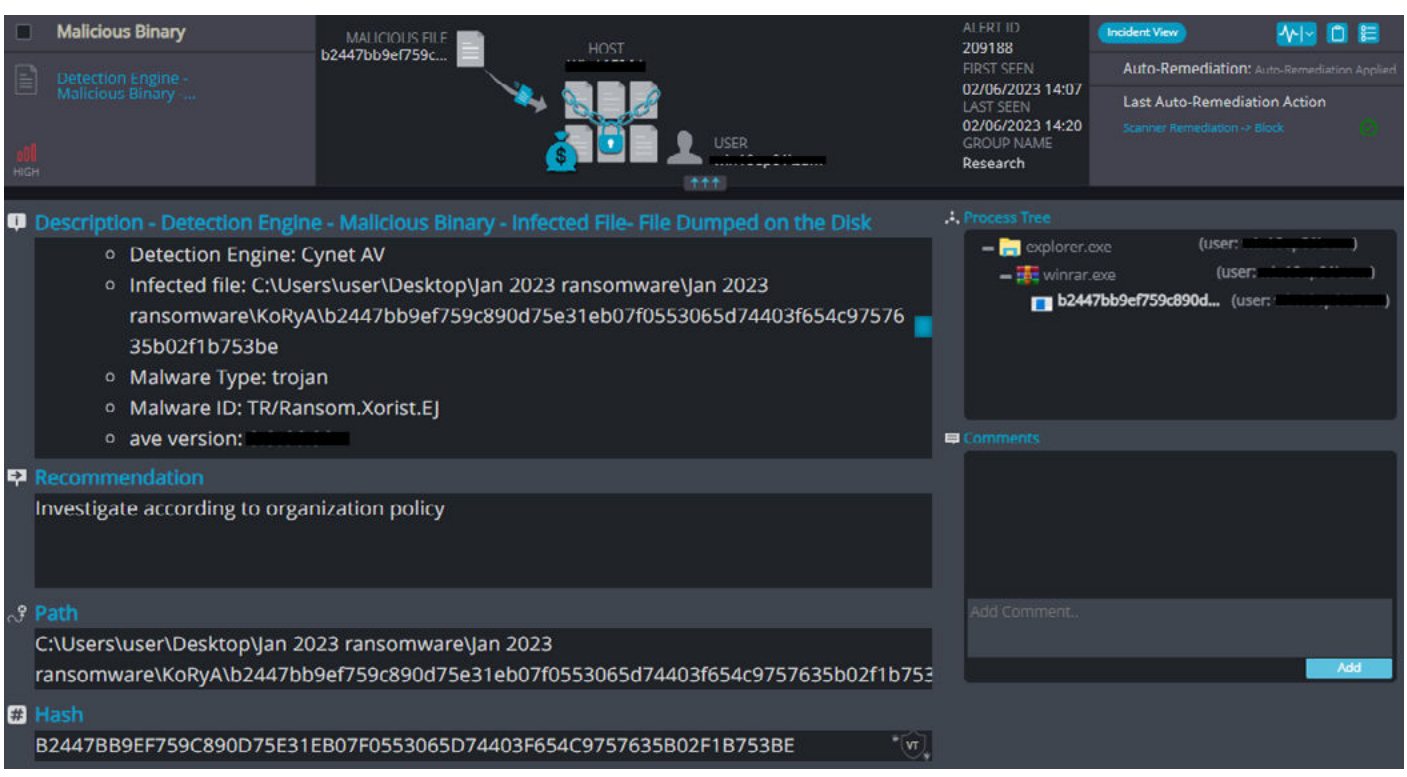
Orion Team

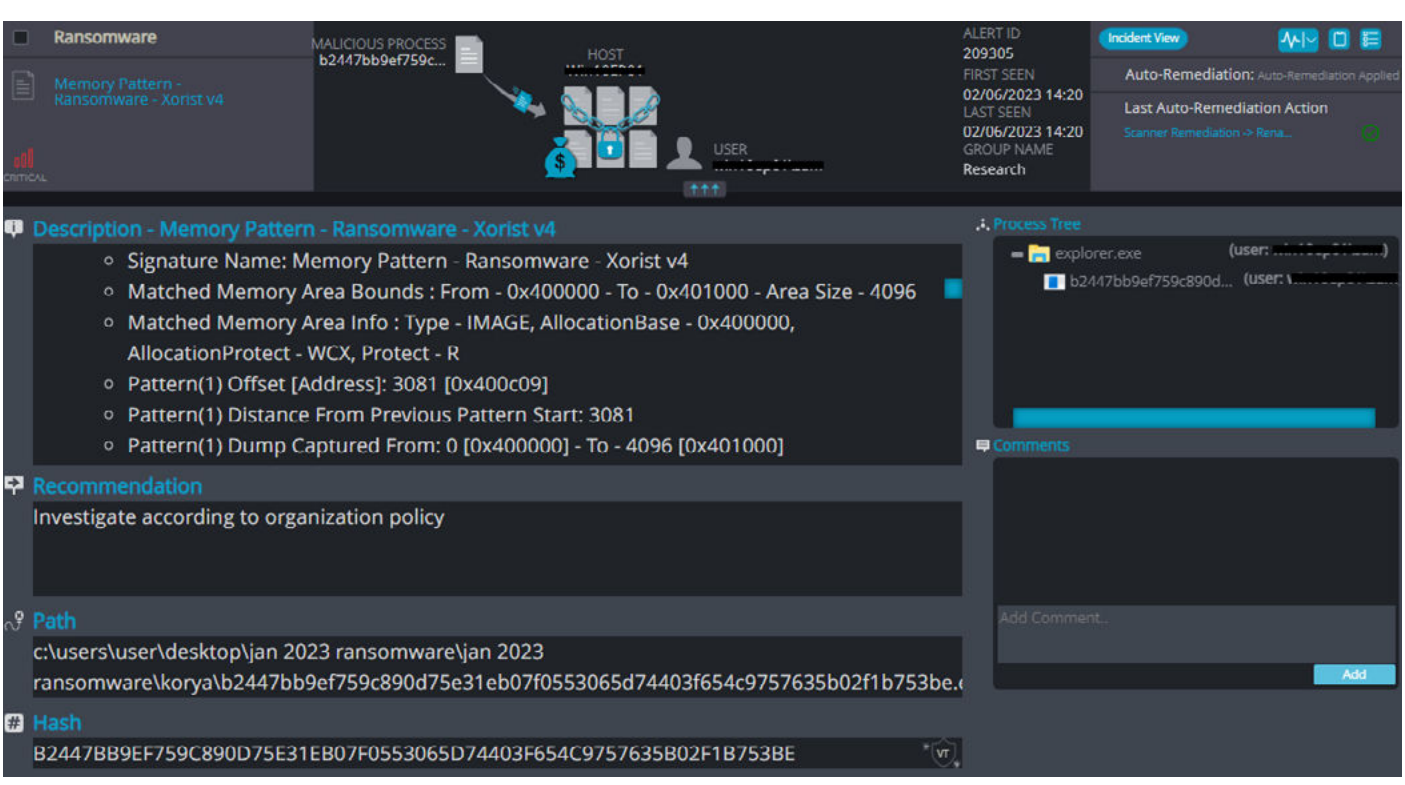
KoRyA Ransomware

- 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:

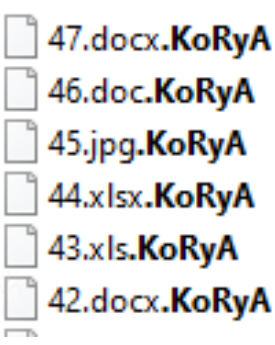
Xorist Ransomware variant



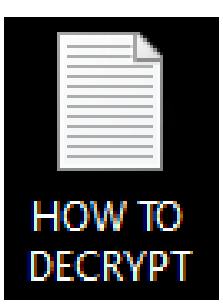


KoRyA Overview

KoRyA ransomware renames the encrypted files with ".KoRyA" in the extension:

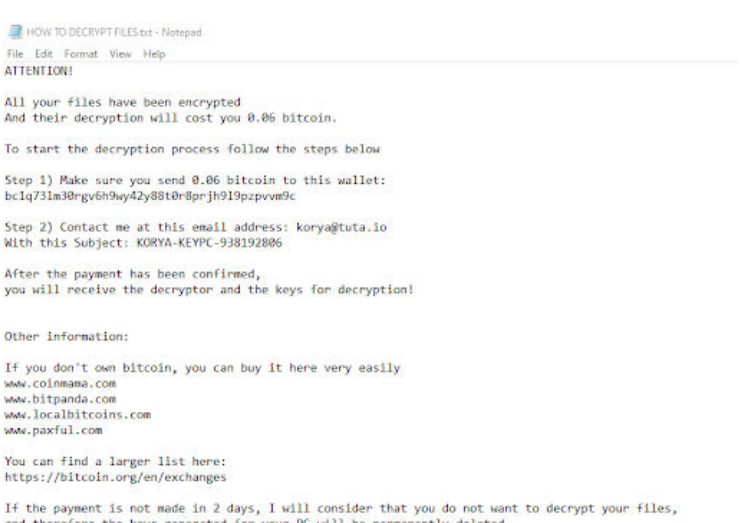


Once a computer's files have been encrypted and renamed, KoRyA drops a note named "HOW TO DECRYPT FILES.txt":



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:



HOW TO DECRYPT FILES.txt - Notepad

File Edit Format View Help

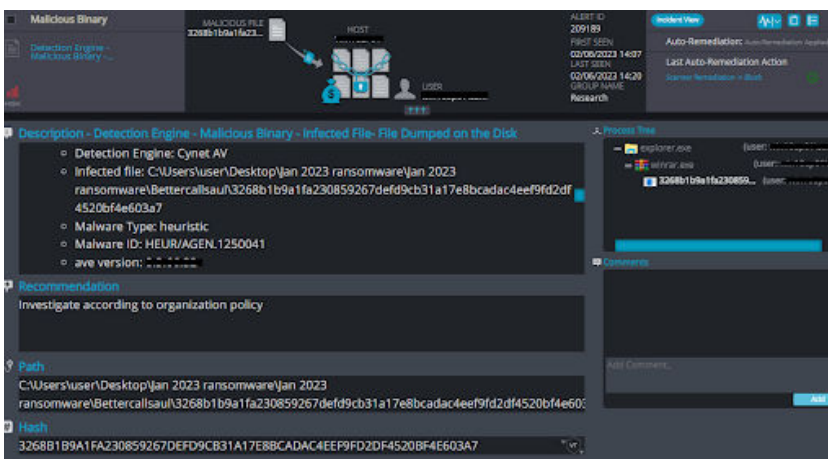
```
ATTENTION!

All your files have been encrypted
And their decryption will cost you 0.06 bitcoin.

To start the decryption process follow the steps below

Step 1) Make sure you send 0.06 bitcoin to this wallet:
bc1q731m30rgv6h9wy42y88t0r8prjh9l9pzpvvm9c

Step 2) Contact me at this email address: korya@tuta.io
With this Subject: KORYA-KEYPC-938192806

After the payment has been confirmed,
you will receive the decryptor and the keys for decryption!


Other information:

If you don't own bitcoin, you can buy it here very easily
www.coinmama.com
www.bitpanda.com
www.localbitcoins.com
www.paxful.com

You can find a larger list here:
https://bitcoin.org/en/exchanges

If the payment is not made in 2 days, I will consider that you do not want to decrypt your files,
and therefore the keys generated for your PC will be permanently.deleted.
```

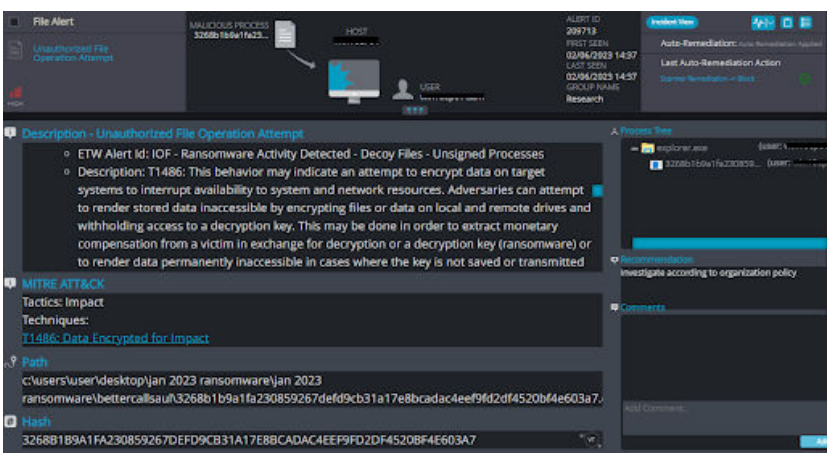
Orion Team

Bettercallsaul Ransomware

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

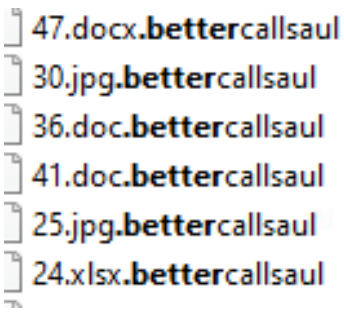
Cynet 360 AutoXDR™ Detections:



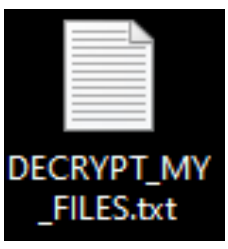


Bettercallsaul Overview

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

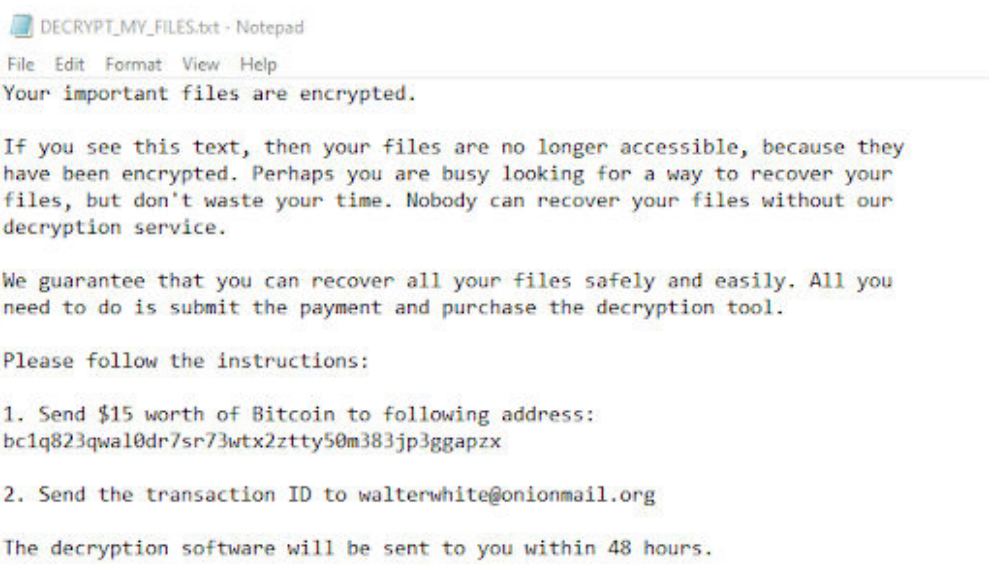


Once a computer’s files have been encrypted and renamed, Bettercallsaul drops a note named “DECRYPT_MY_FILES.txt”:



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:



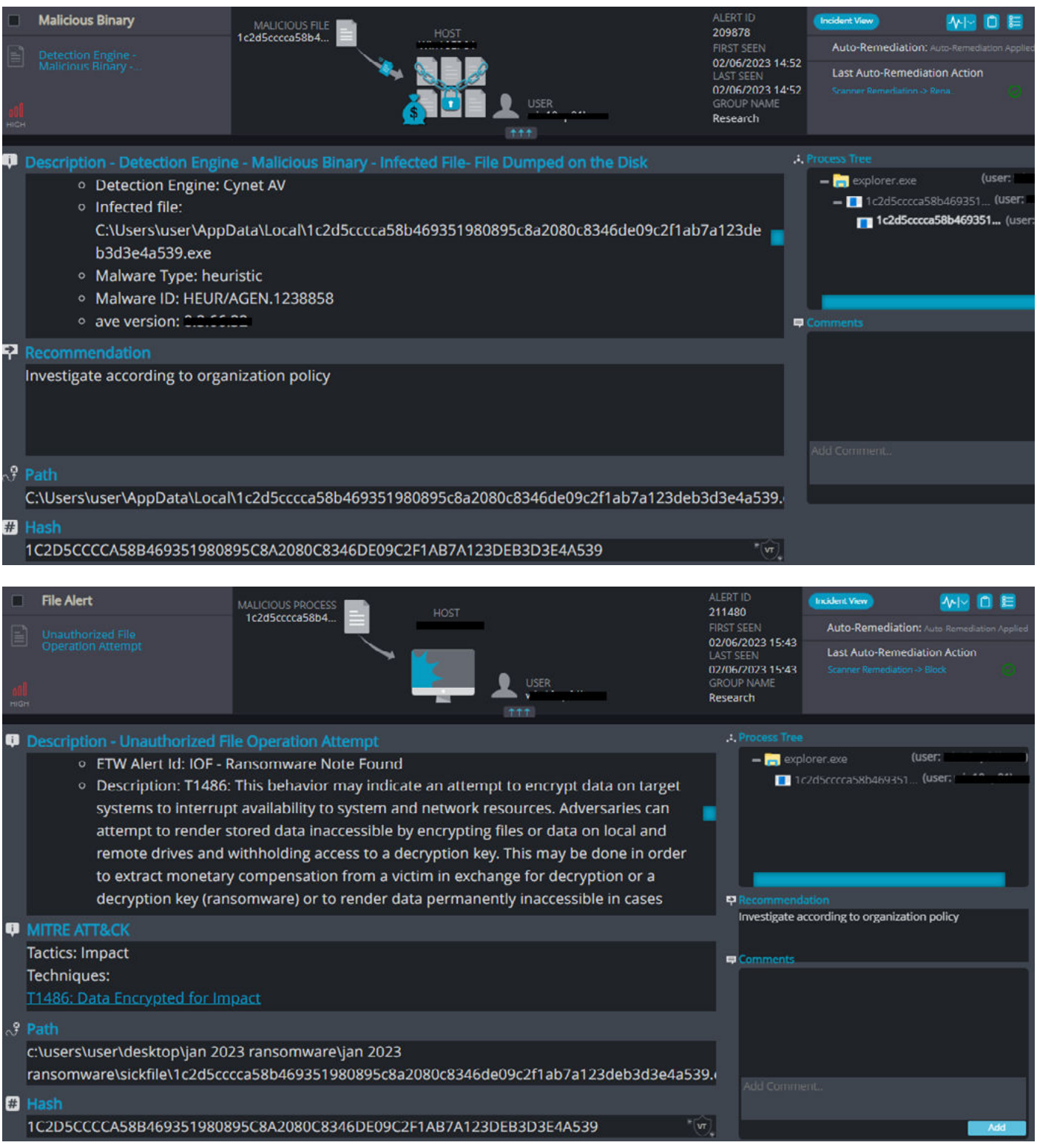
The ransomware also changes the desktop background:

Orion Team

SickFile Ransomware

- Observed since: Jan 2023
- Ransomware encryption method: AES + RSA
- Ransomware extension: .sickfile
- Ransomware note: how_to_back_files.html
- Sample hash: 1c2d5cccca58b469351980895c8a2080c8346de09c2f1ab7a123deb3d3e4a539

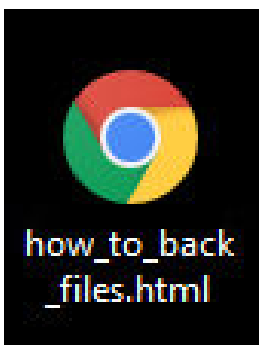
Cynet 360 AutoXDR™ Detections:



SickFile Overview

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

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:

[redacted]

!!! YOUR COMPANY NETWORK HAS BEEN PENETRATED !!!
All your important files have been encrypted!

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

ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE
WILL PERMANENTLY CORRUPT IT.
DO NOT MODIFY 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 gathered 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 re-seller.
So you can expect your data to be publicly available in the near future.

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

You will can send us 2-3 non-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:

4. Start a chat and follow the further instructions.

If you can not use the above link, use the email:
doctorhelperzz@gmail.com
helperzdoctor@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.

cynet

Thank you!

January, 2023