cynet

Orion Team

Monthly Ransomware Activity

Written by: Maor Huli

May, 2022

Orion Team

Contents

Executive Summary 3
Odaku 5
Kekpop 6
Japan 7
EarthGrass 8
CryptBIT 9

Orion Team

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 indentified 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 08:08 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 04:58 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

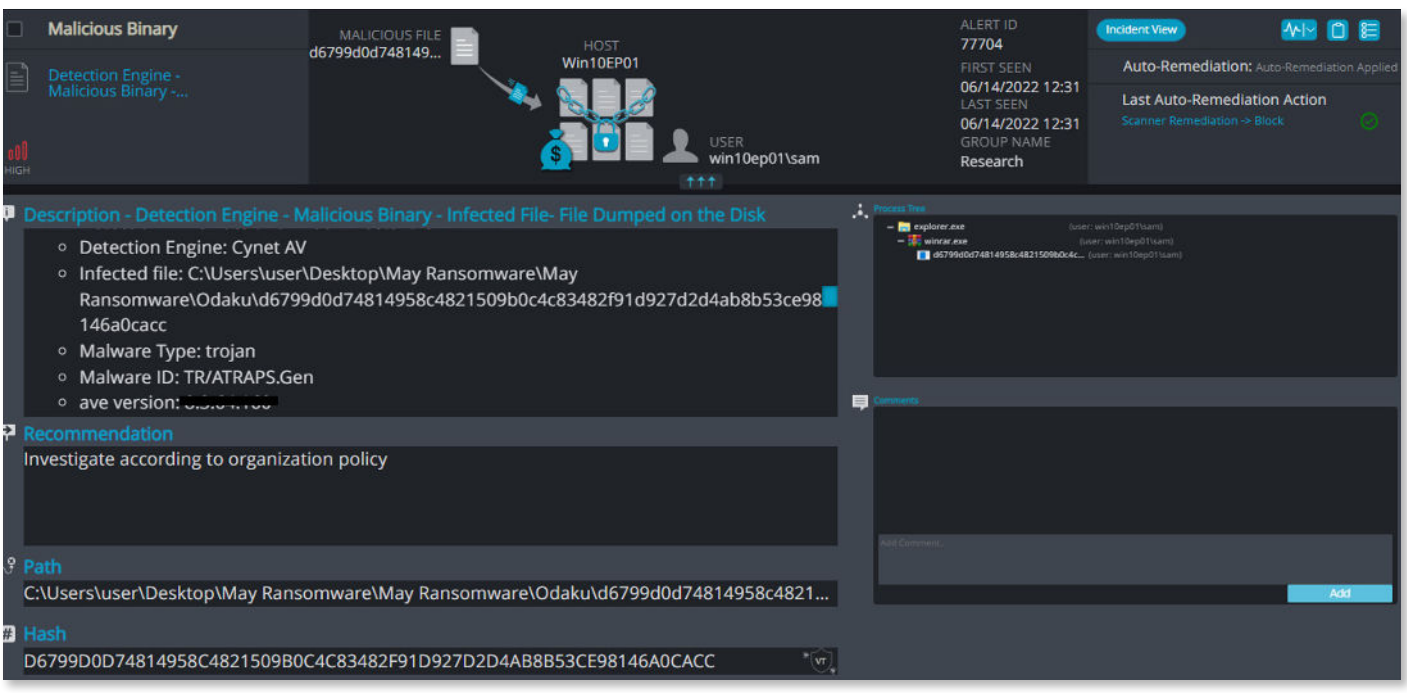
Cynet 360 AutoXDR™ VS Ransomware

Orion Team

Odaku Ransomware

- Observed since: Late 2021
- Ransomware encryption method: RSA + AES.
- Ransomware extension: .[4 random characters]
- Ransomware note: read_it.txt
- Sample hash: d6799d0d74814958c4821509b0c4c83482f91d927d2d4ab8b53ce98146a0cacc

Cynet 360 AutoXDR™ Detections:

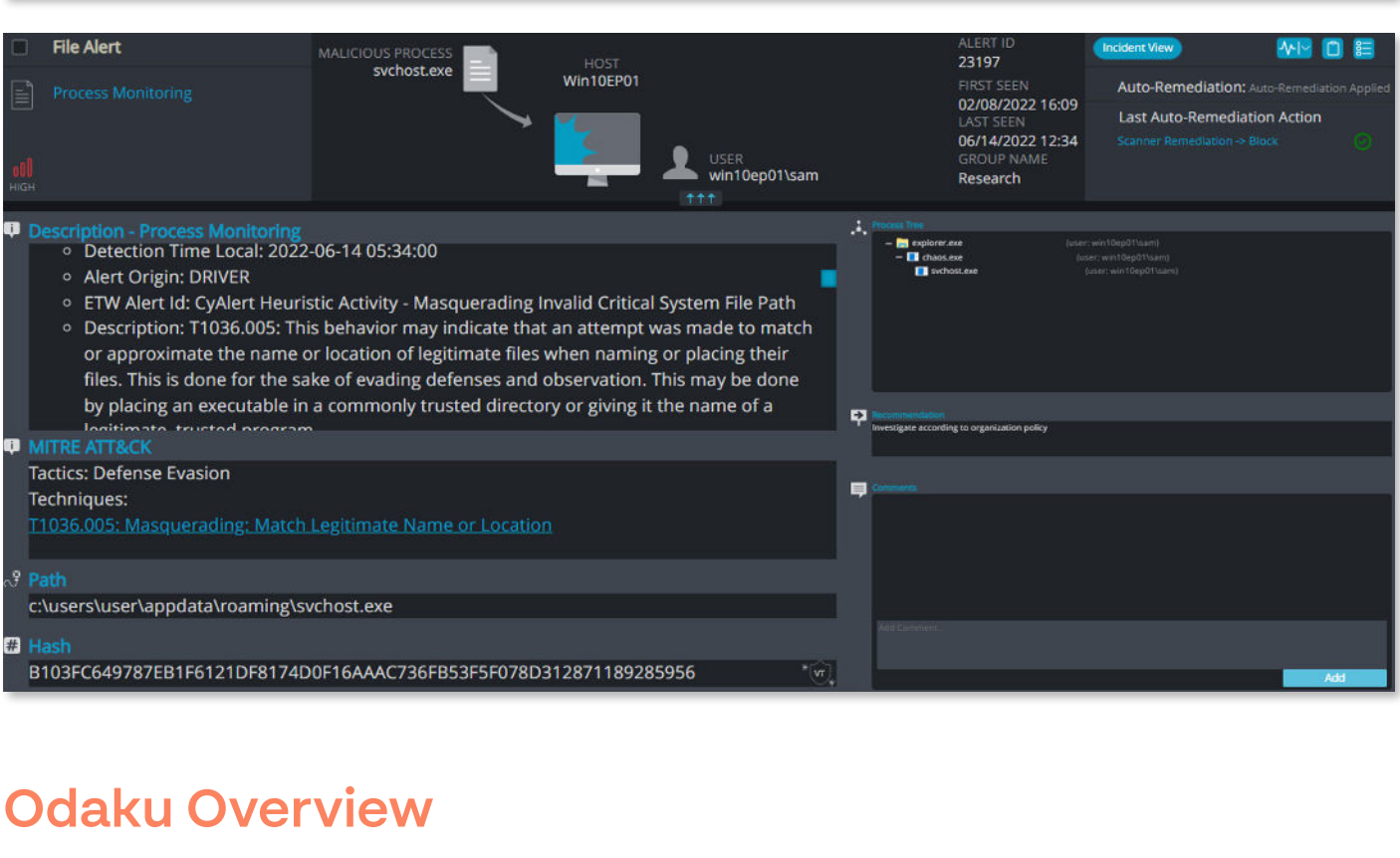


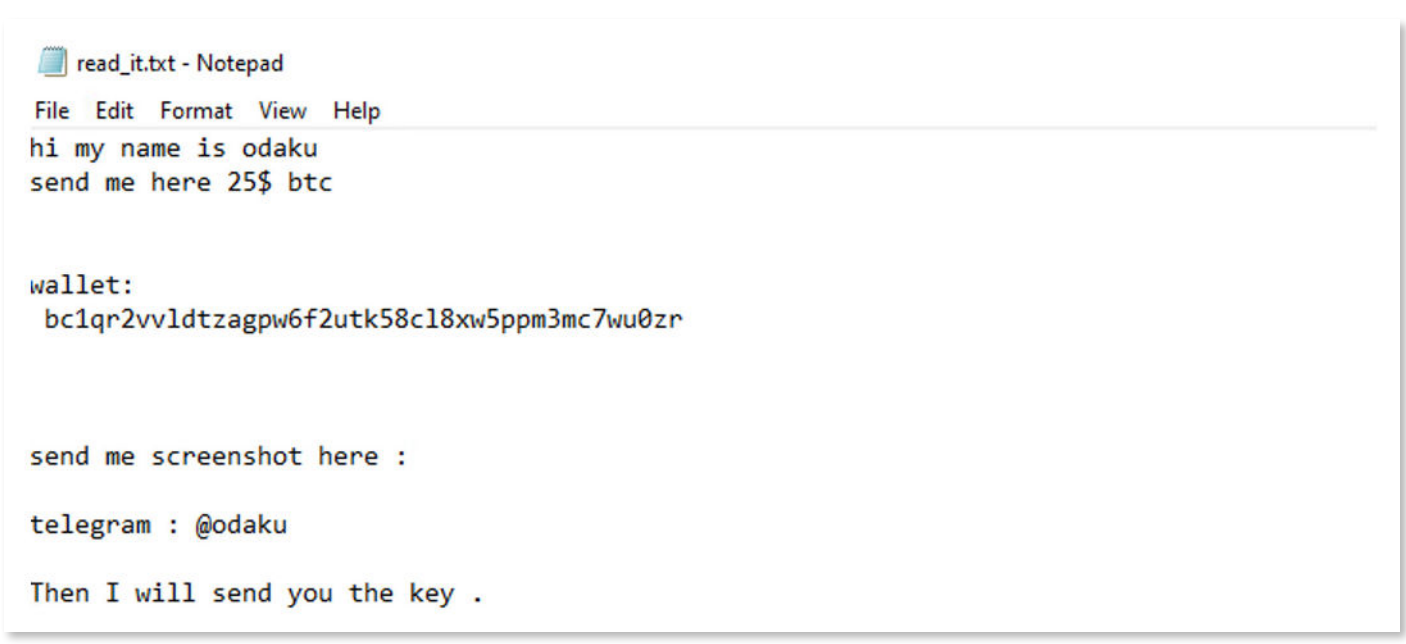
Odaku Overview

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

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

Upon execution, it immediately copies itself to the folder "C:\Users\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):



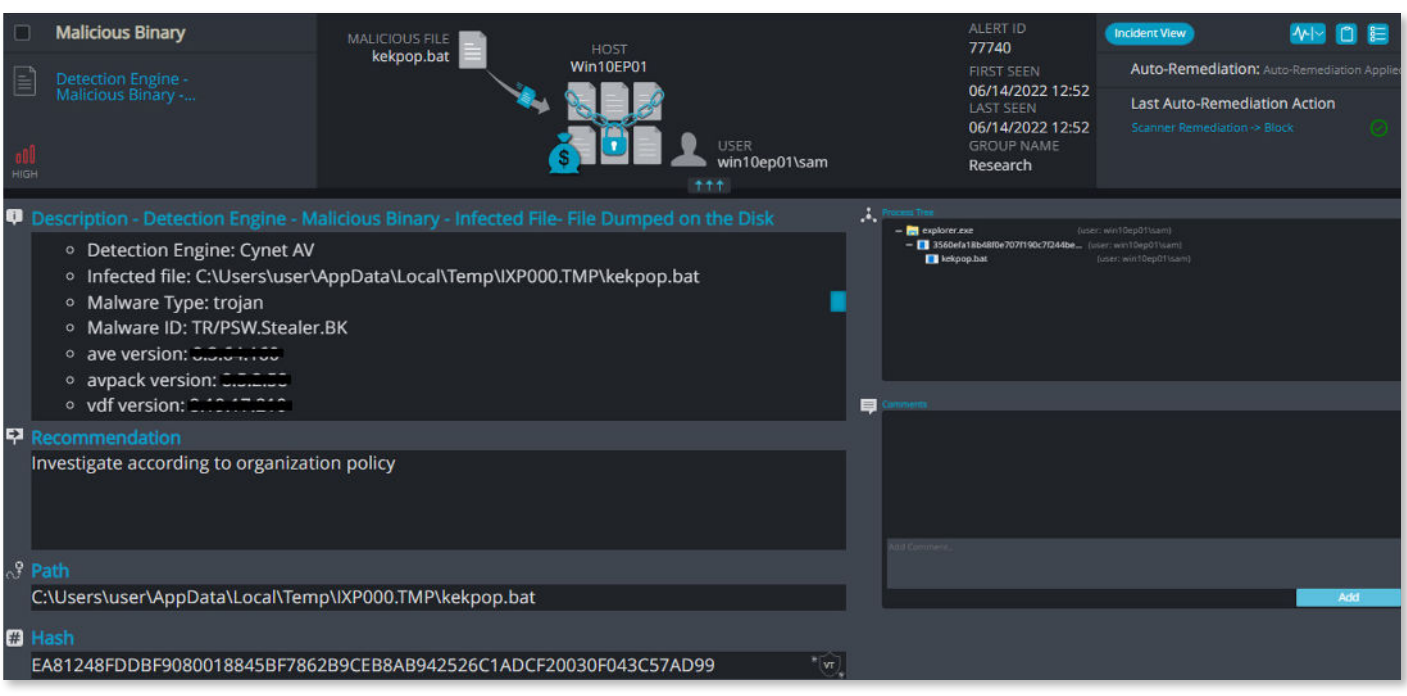


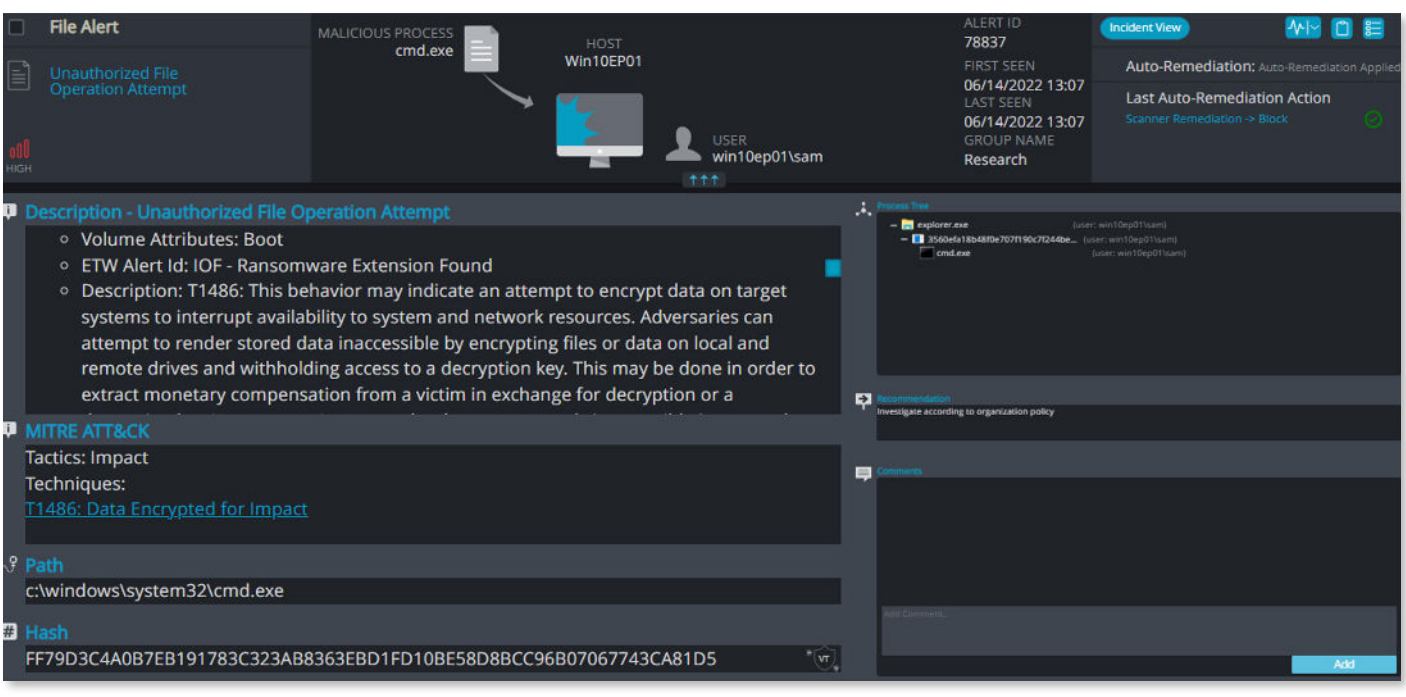
Orion Team

Kekpop Ransomware

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

Cynet 360 AutoXDR™ Detections:

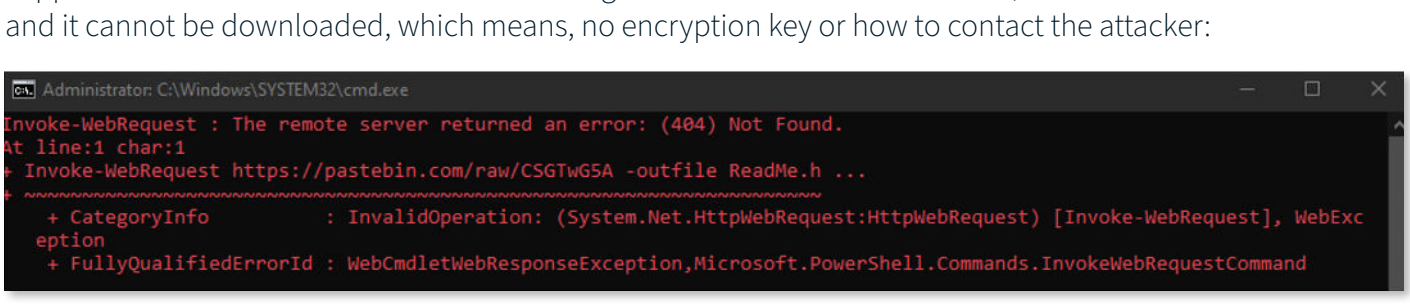




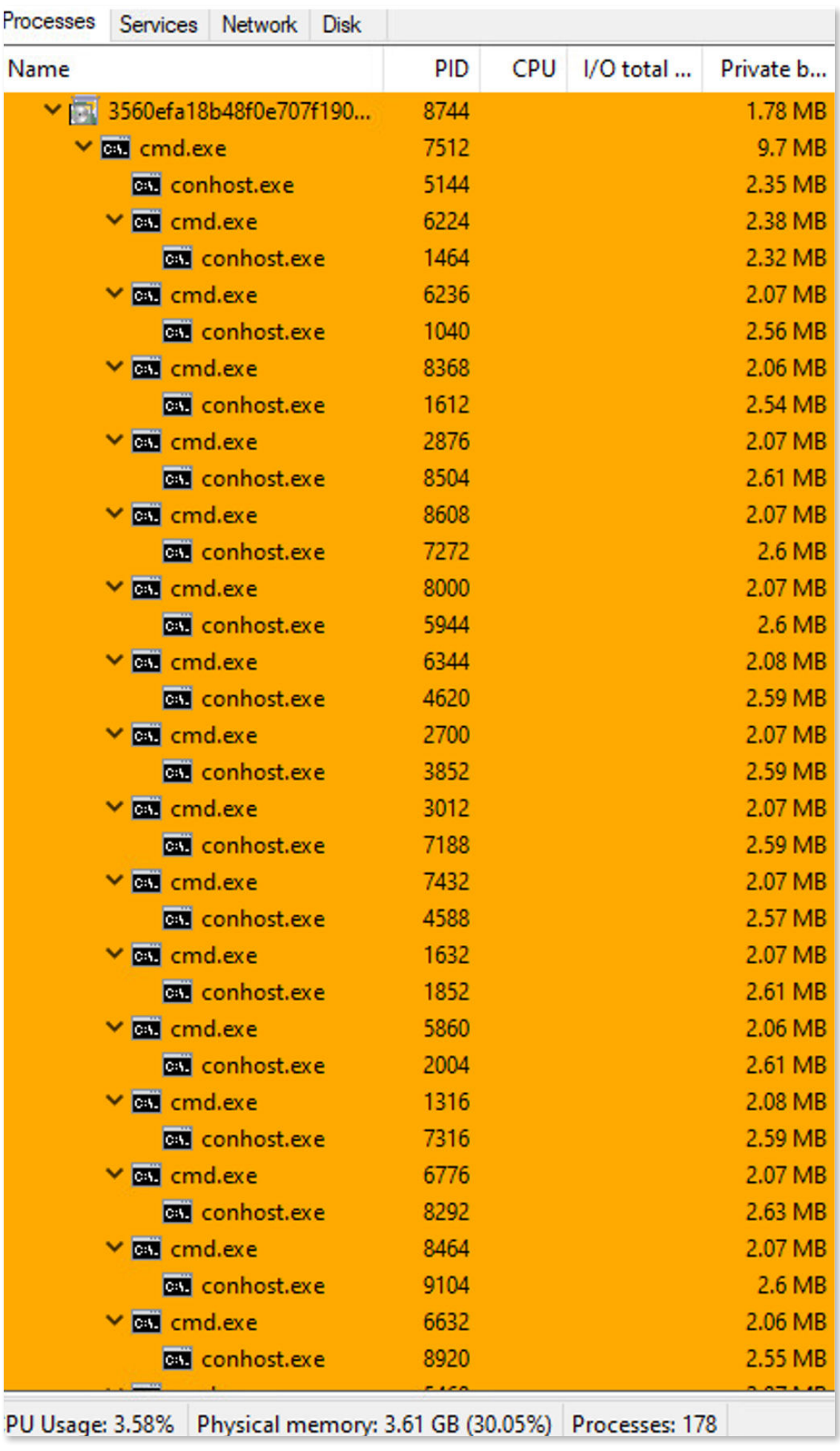
Kekpop Overview

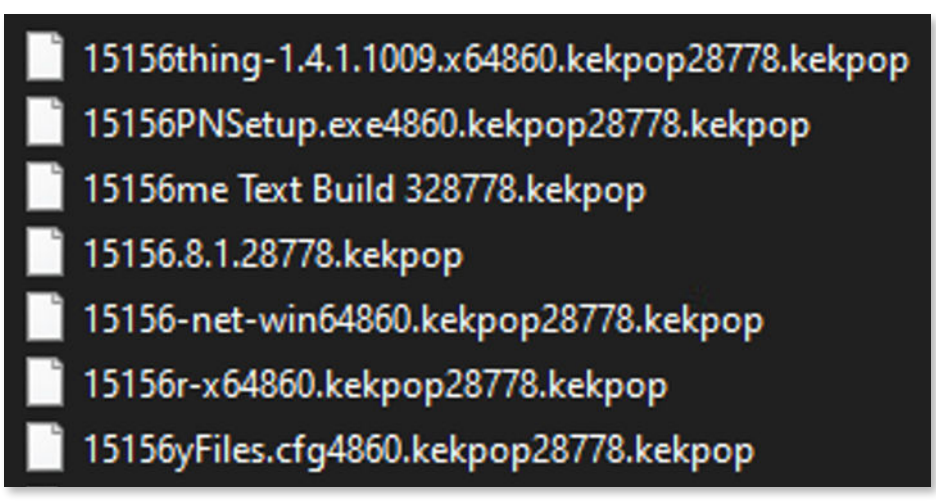
Kekpop ransomware renames the encrypted files with .kekpop in the extension:

Once a computer's files have 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:



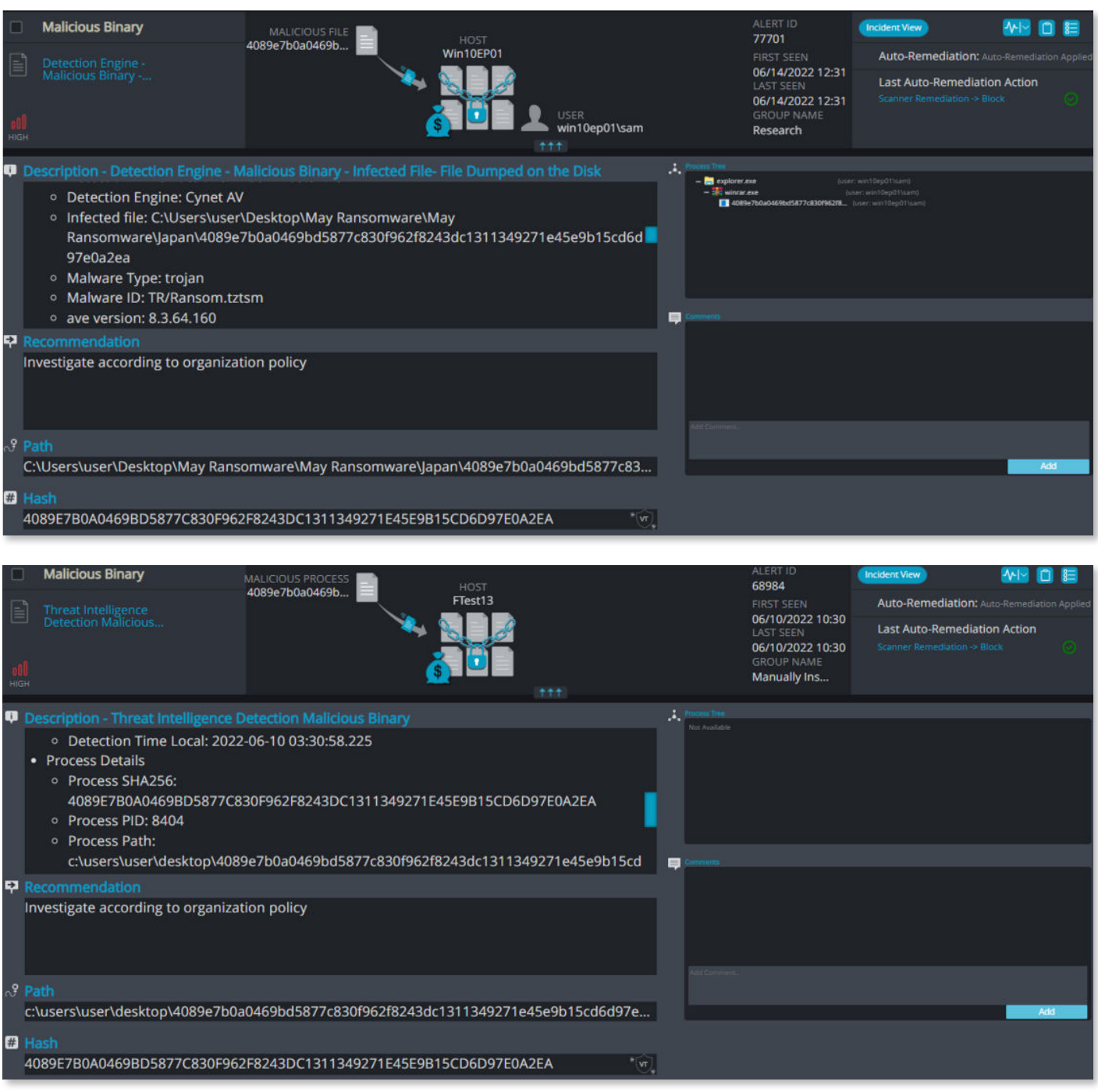


Orion Team

Japan Ransomware

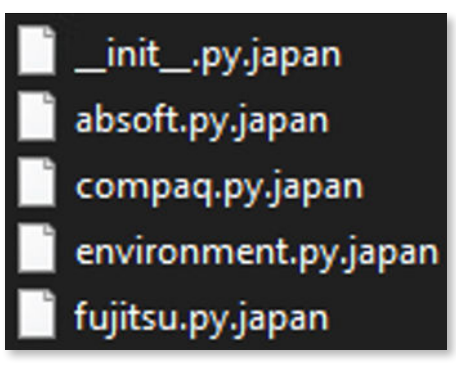
- Observed since: May 2022
- Ransomware encryption method: AES + RSA.
- Ransomware extension: .japan
- Ransomware note: how to decrypt.txt
- Sample hash: 4089e7b0a0469bd5877c830f962f8243dc1311349271e45e9b15cd6d97e0a2ea

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 it copies the file to the folder "C:\Users\user\AppData\Roaming" and changes the name to "svchost.exe" and it immediately encrypts 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):

Hi!!

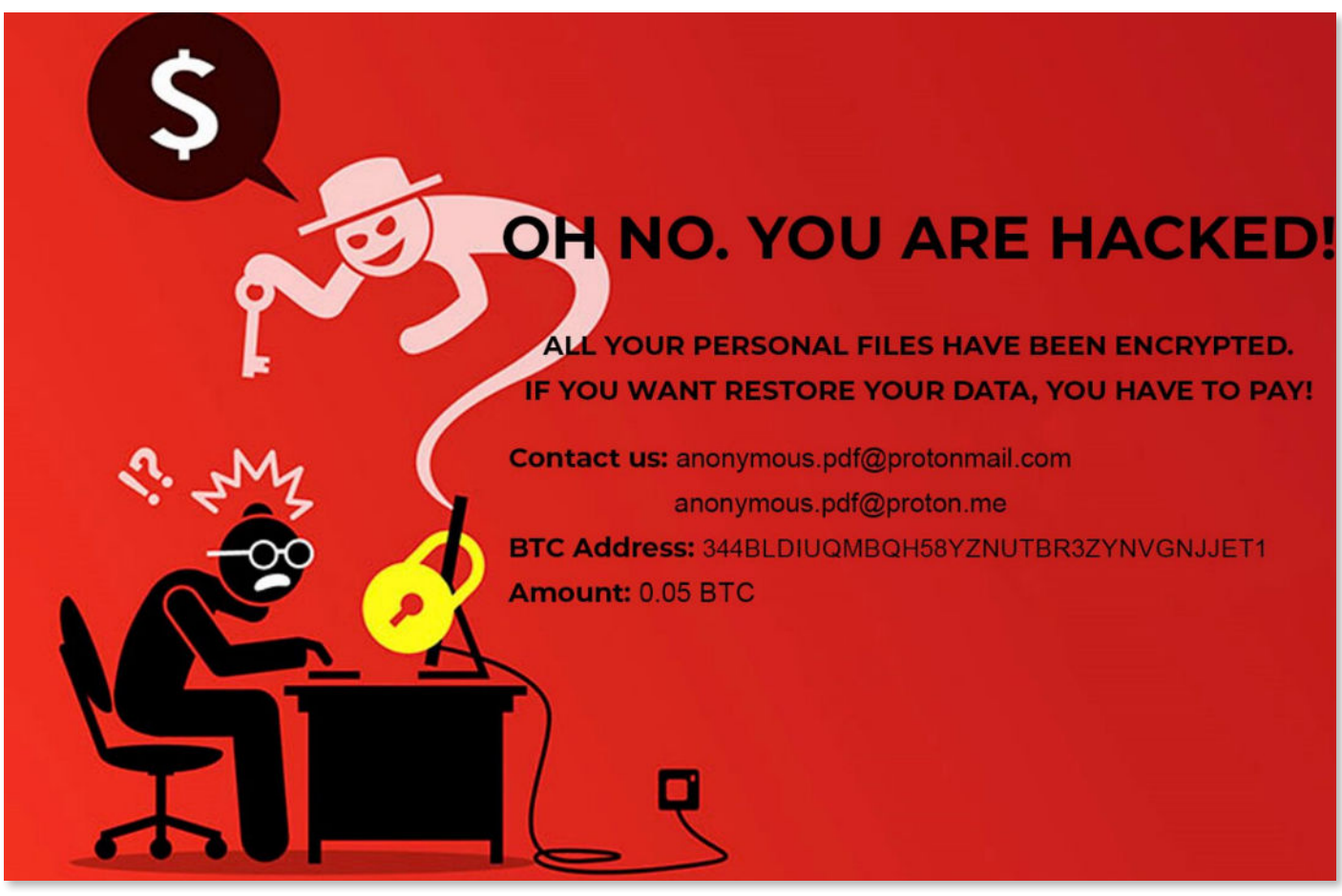
We have discovered a security hole at your server.
And not. All your data has been successfully encrypted by us to keep them secure.
Rest assured, your data can still be reopened thanks to a private key and unlocking software.
You have 4 days to be able to unlock your data again. After 4 days, the private keys will expire and you will not be able to unlock them. So do it quickly.
We accept payment via bitcoin for 2000 USD. After receiving the receipt of BTC receipt from the wallet, we will send the private and unlock software to you.

You can contact us by email: anonymous.pdf@protonmail.com
BTC Address: 344BLDiUqMbqh58yZnuTBR3ZYnVGnjjEt1
Amount: 0.05 BTC

We will only guarantee decrypted data from 4 days and beyond. Will not be.

You must not shut down your computer, or restart it, update it, or use antivirus software. If used, the data key will be lost and cannot be recovered.

In the end, it also changes the background:

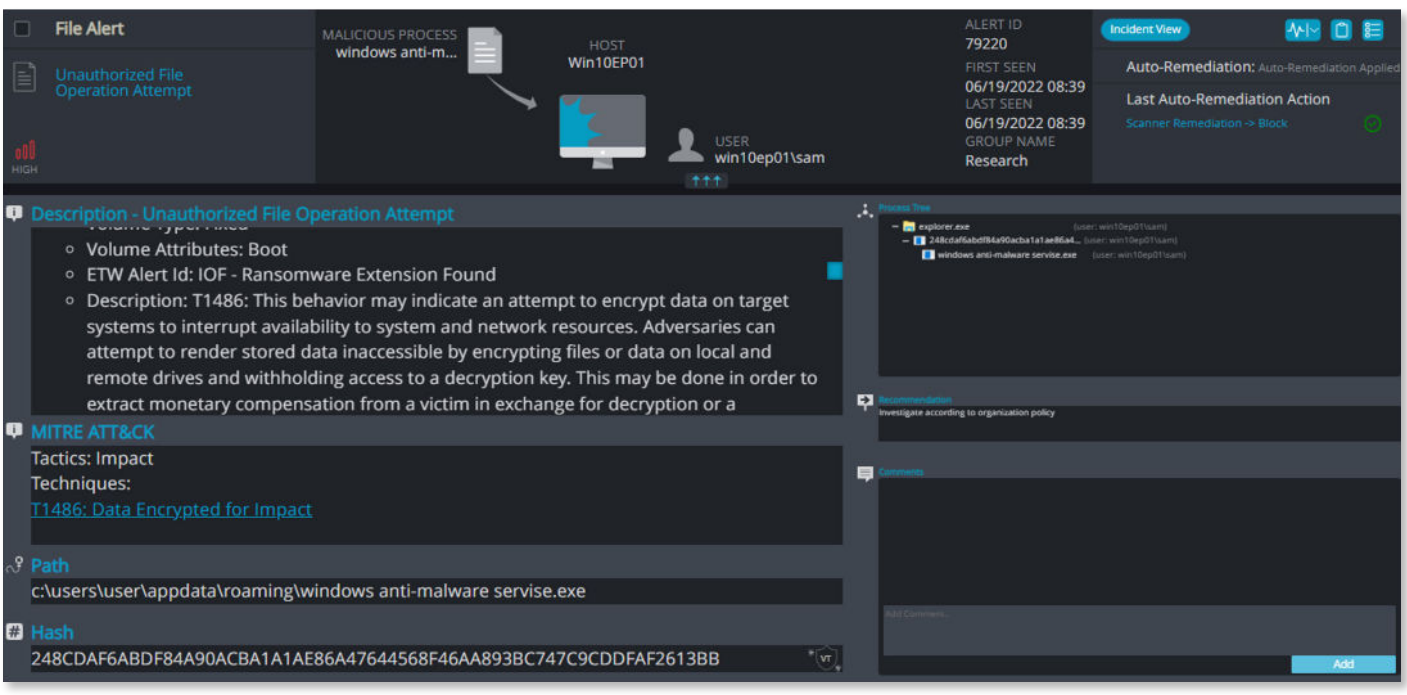


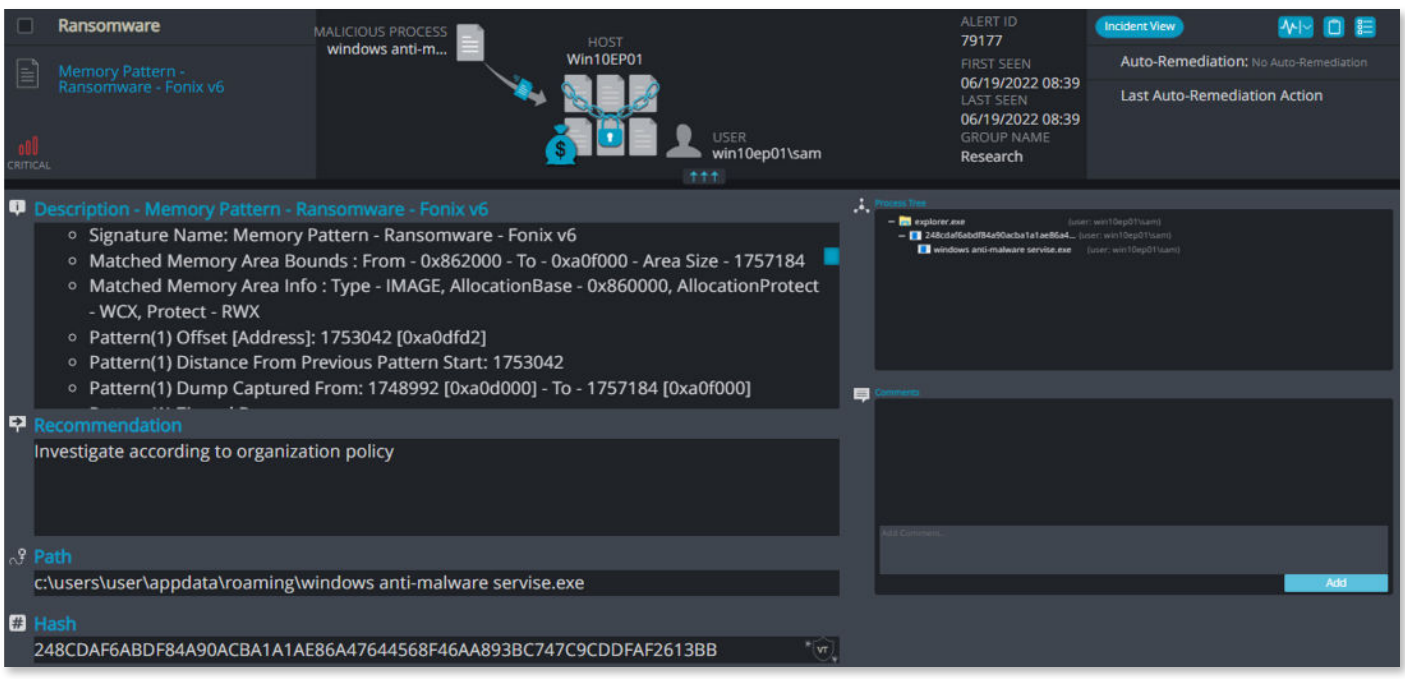
Orion Team

EarthGrass Ransomware

- Observed since: May 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: . 34r7hGr455
- Ransomware note: Read ME (Decryptor).txt
- Sample hash: 248cdaf6abdf84a90acba1a1ae86a47644568f46aa893bc747c9cddfaf2613bb

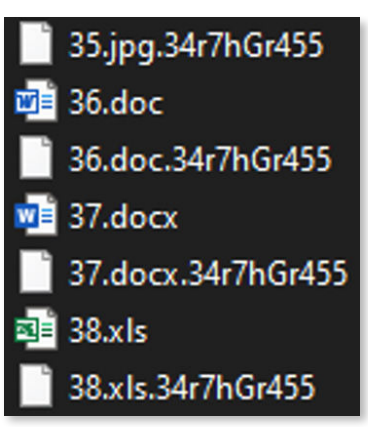
Cynet 360 AutoXDR™ Detections:





EarthGrass Overview

EarthGrass ransomware renames the encrypted files with .34r7hGr455in the extension:



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

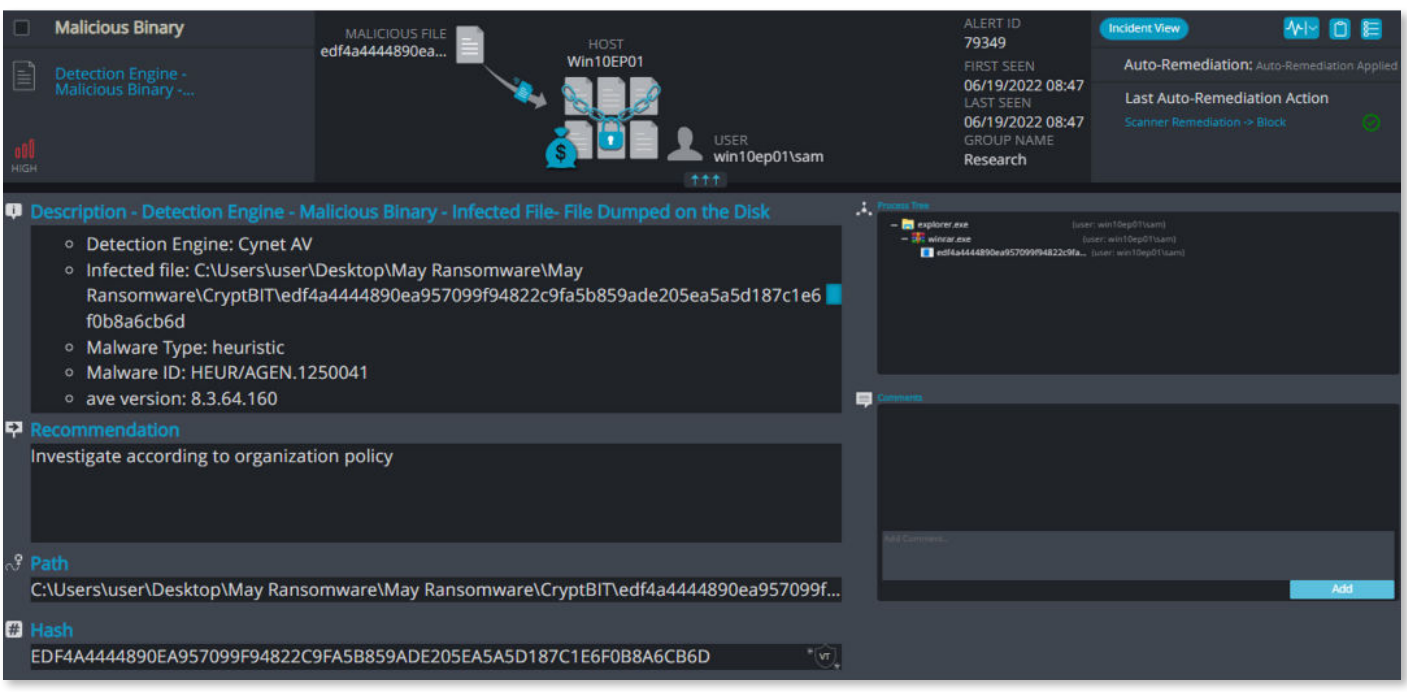
Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker's contact info:

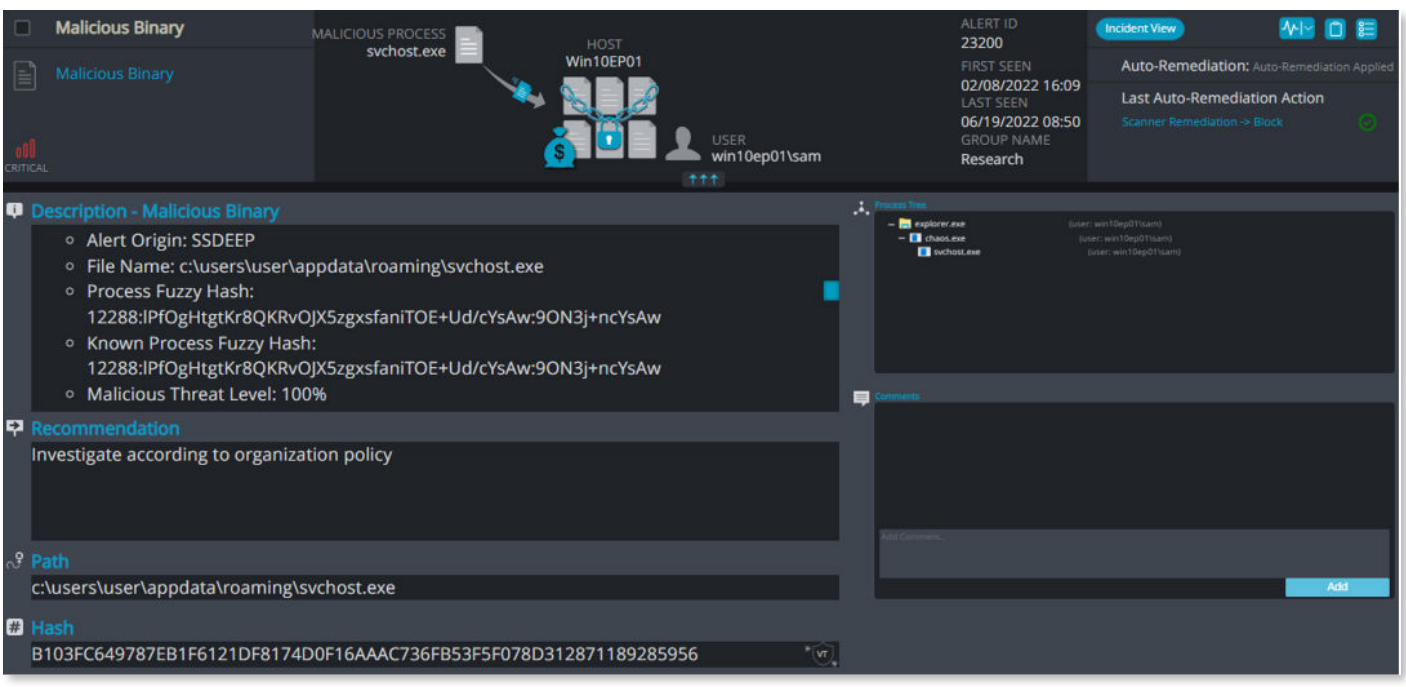
Orion Team

CryptBIT Ransomware

- Observed since: May 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .cryptbit
- Ransomware note: CryptBIT-restore-files.txt
- Sample hash: edf4a4444890ea957099f94822c9fa5b859ade205ea5a5d187c1e6f0b8a6cb6d

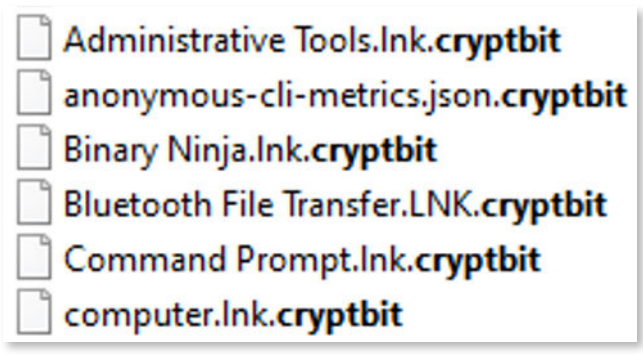
Cynet 360 AutoXDR™ Detections:



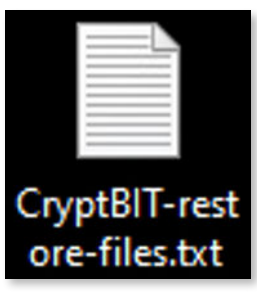


CryptBIT Overview

CryptBIT ransomware renames the encrypted files with .cryptbit in the extension:



Once a computer's files have been encrypted and renamed, it drops a note as CryptBIT-restore-files.txt:



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:

cynet

Thank you!

May, 2022