cynet

Orion Team

Monthly Ransomware Activity

Written by: Maor Huli

September, 2022

Orion Team

Contents

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 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 - September 30th 2022 - Emerging from the Shadows

This week's news primarily revolves around LockBit, BlackMatter, and the rising enterprise-targeting Royal ransomware operation.

LAWRENCE ABRAMS SEPTEMBER 30, 2022 04:48 PM 0

The Week in Ransomware - September 23rd 2022 - LockBit leak

This week we saw some embarrassment for the LockBit ransomware operation when their programmer leaked a ransomware builder for the LockBit 3.0 encryptor.

LAWRENCE ABRAMS SEPTEMBER 23, 2022 05:25 PM 2

The Week in Ransomware - September 16th 2022 - Iranian Sanctions

It has been a fairly quiet week on the ransomware front, with the biggest news being US sanctions on Iranians linked to ransomware attacks.

LAWRENCE ABRAMS SEPTEMBER 16, 2022 04:26 PM 0

The Week in Ransomware - September 9th 2022 - Schools under fire

Ransomware gangs have been busy this week, launching attacks against NAS devices, one of the largest hotel groups, IHG, and LAUSD, the second largest school district in the USA.

LAWRENCE ABRAMS SEPTEMBER 09, 2022 04:14 PM 0

Orion Team

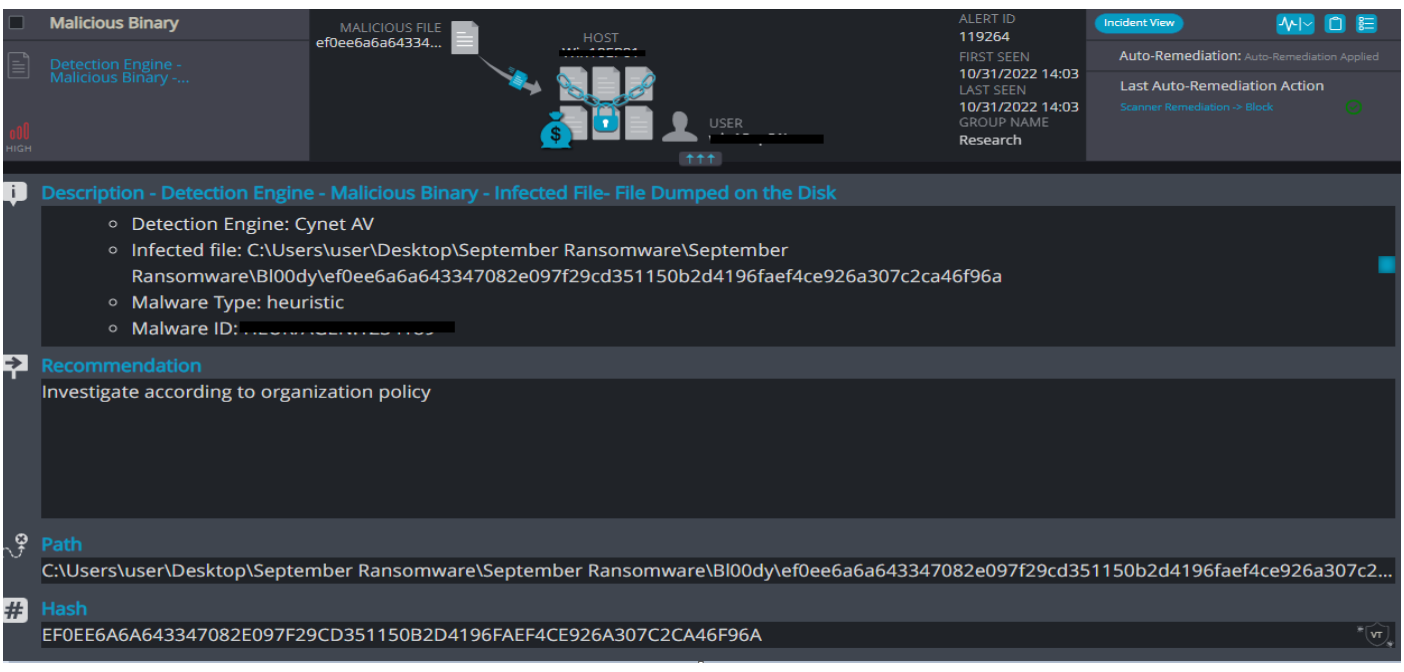
Cynet 360 AutoXDR™ VS Ransomware

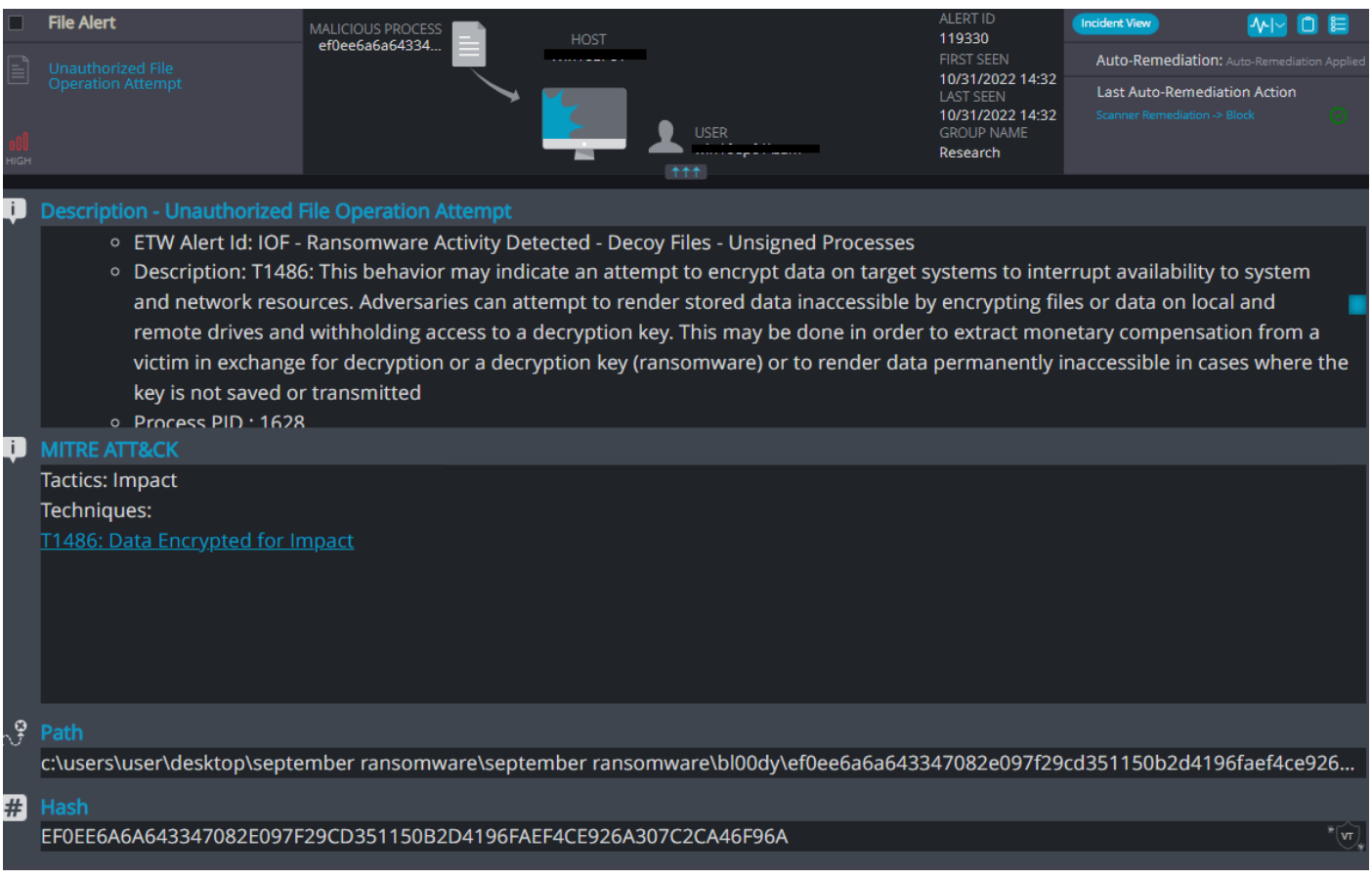
Orion Team

Bl00dy Ransomware

- Observed since: Sep 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .bl00dy
- Ransomware note: How To Restore Your Files.txt
- Sample hash: ef0ee6a6a643347082e097f29cd351150b2d4196faef4ce926a307c2ca46f96a

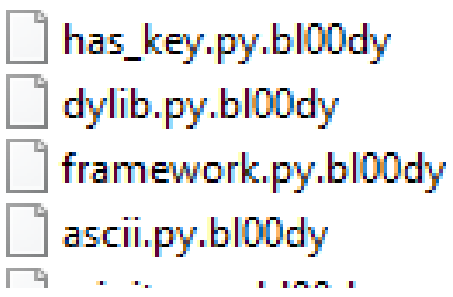
Cynet 360 AutoXDR™ Detections:





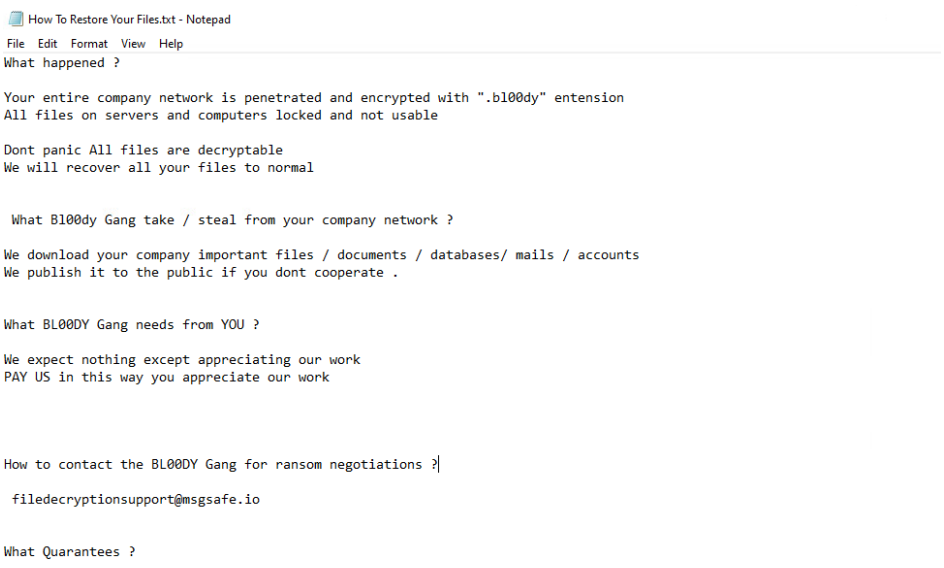
Bl00dy Overview

Bl00dy ransomware renames the encrypted files with .bl00dy in the extension.



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

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


How To Restore Your Files.txt - Notepad

File Edit Format View Help

What happened ?

Your entire company network is penetrated and encrypted with ".bl00dy" entension
All files on servers and computers locked and not usable

Dont panic All files are decryptable
We will recover all your files to normal

What Bl00dy Gang take / steal from your company network ?

We download your company important files / documents / databases/ mails / accounts
We publish it to the public if you dont cooperate .

What BL00DY Gang needs from YOU ?

We expect nothing except appreciating our work
PAY US in this way you appreciate our work

How to contact the BL00DY Gang for ransom negotiations ?

filedecryptionsupport@msgsafe.io

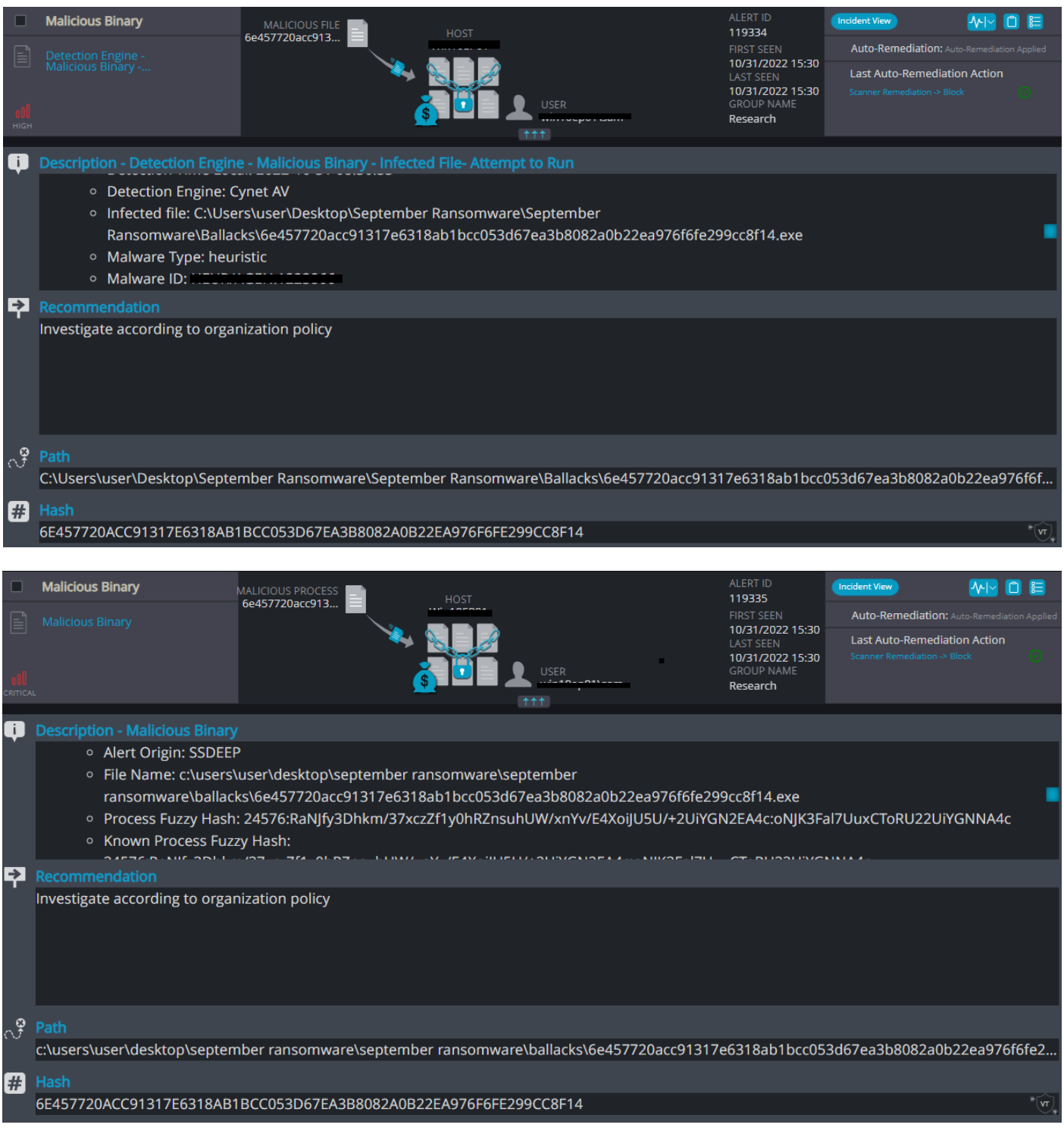
What Quarantees ?

Orion Team

Ballacks Ransomware

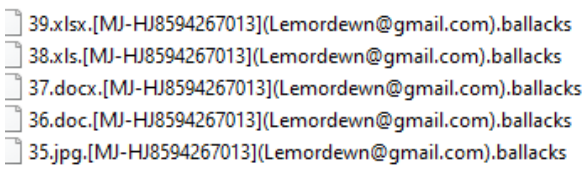
- Observed since: Sep 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .ballacks
- Ransomware note: ReadthisforDecode.txt
- Sample hash: 6e457720acc91317e6318ab1bcc053d67ea3b8082a0b22ea976f6fe299cc8f14

Cynet 360 AutoXDR™ Detections:



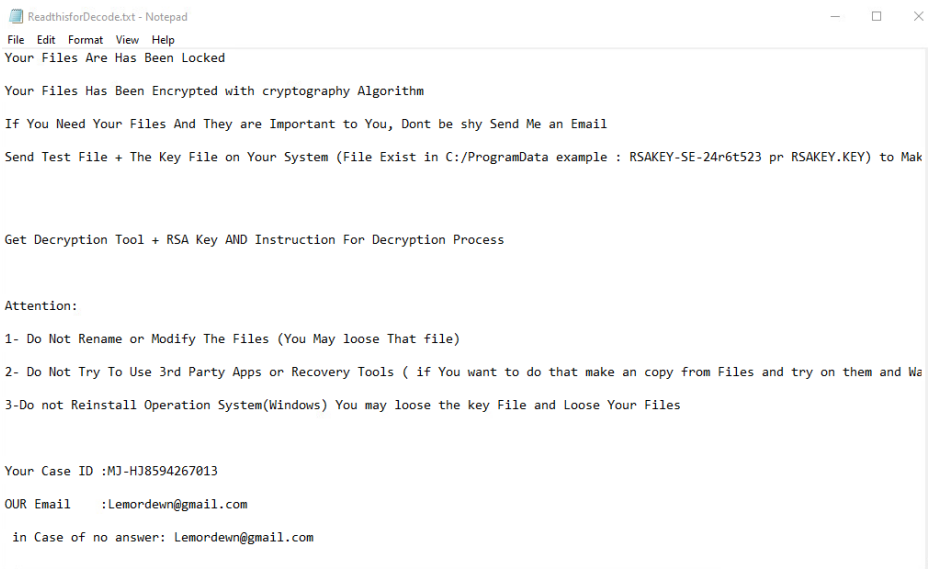
Ballacks Overview

Ballacks ransomware renames the encrypted files with .ballacks in the extension:



Once a computer's files have been encrypted and renamed, it drops the ransomware note named ReadthisforDecode.txt:

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


ReadthisforDecode.txt - Notepad

File Edit Format View Help

Your Files Are Has Been Locked

Your Files Has Been Encrypted with cryptography Algorithm

If You Need Your Files And They are Important to You, Dont be shy Send Me an Email

Send Test File + The Key File on Your System (File Exist in C:/ProgramData example : RSAKEY-SE-24r6t523 pr RSAKEY.KEY) to Mak

Get Decryption Tool + RSA Key AND Instruction For Decryption Process

Attention:

1- Do Not Rename or Modify The Files (You May loose That file)

2- Do Not Try To Use 3rd Party Apps or Recovery Tools (if You want to do that make an copy from Files and try on them and Wa

3-Do not Reinstall Operation System(Windows) You may loose the key File and Loose Your Files

Your Case ID :MJ-HJ8594267013

OUR Email :Lemordewn@gmail.com

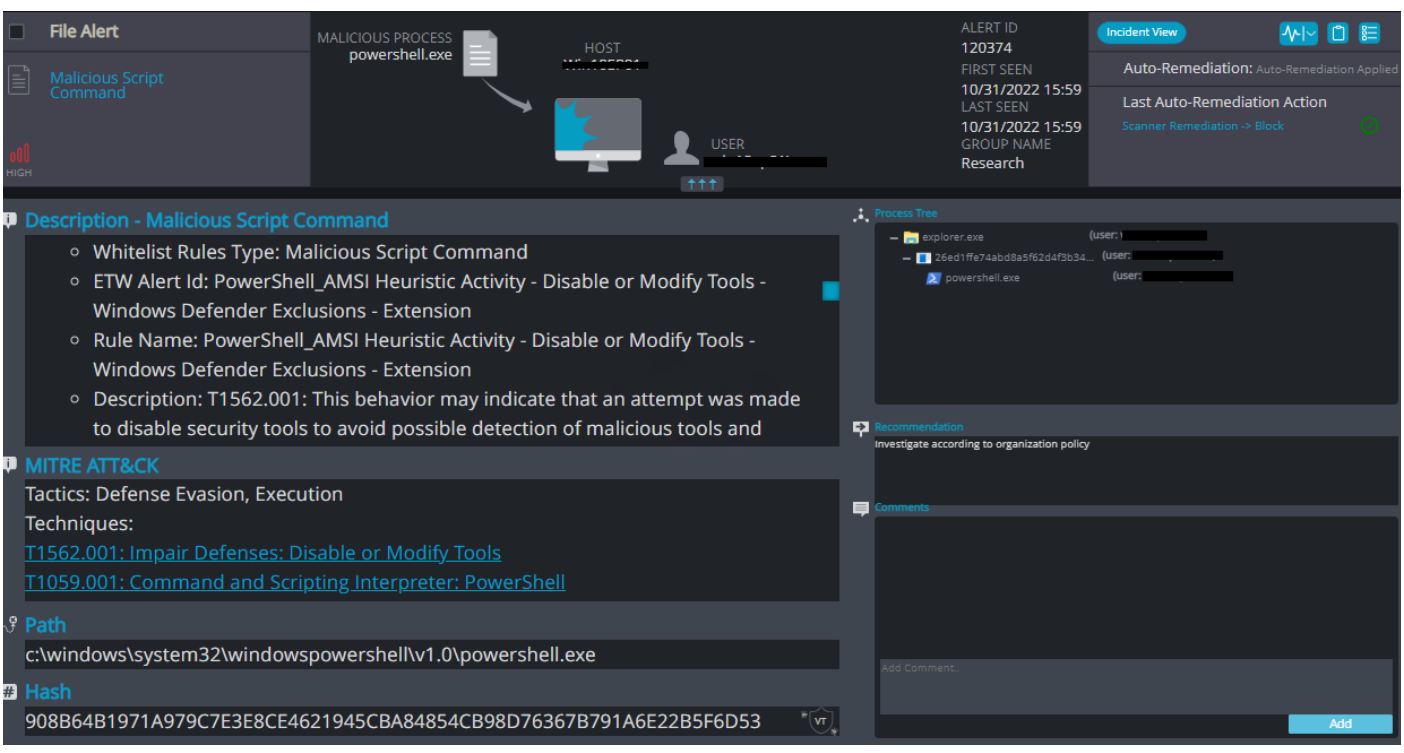
in Case of no answer: Lemordewn@gmail.com

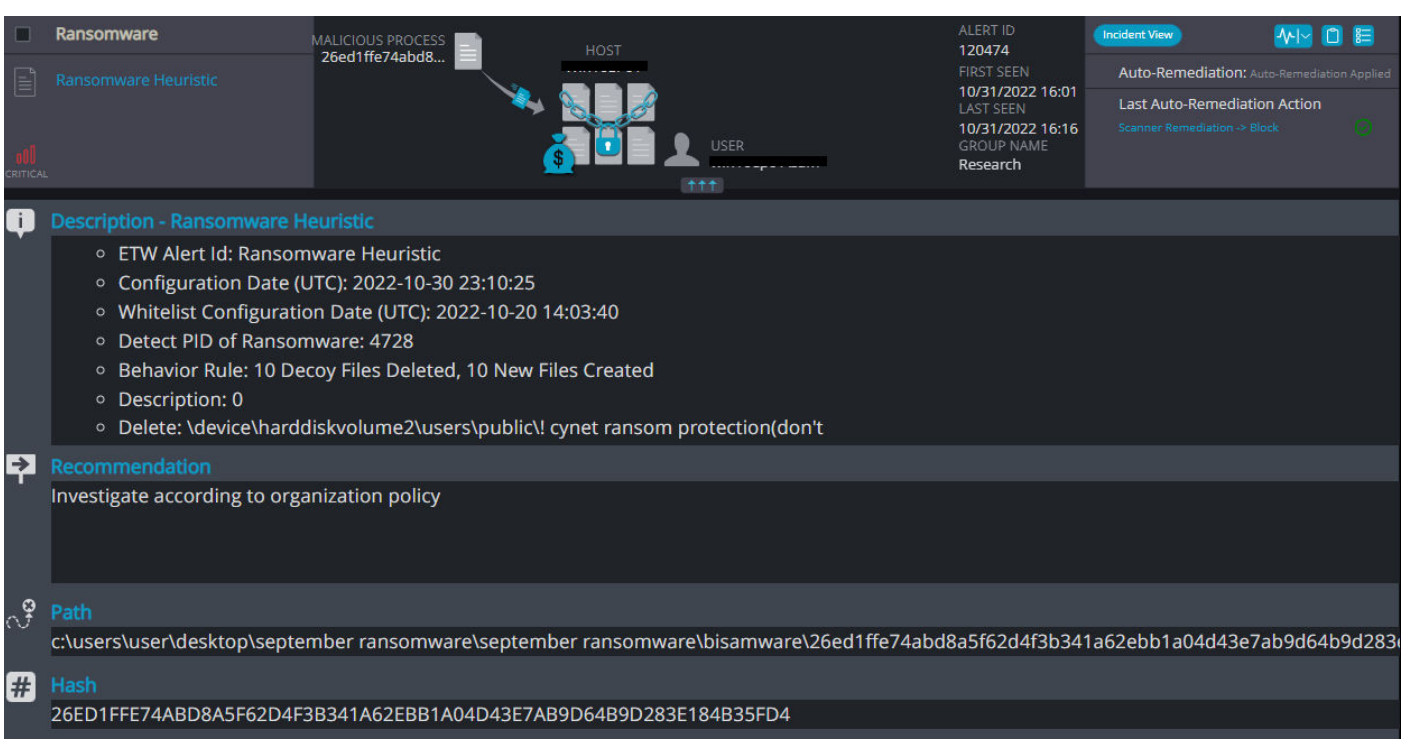
Orion Team

BISAMWARE Ransomware

- Observed since: Sep 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .BISAMWARE
- Ransomware note: SYSTEM=RANSOMWARE=INFECTED.TXT
- Sample hash: 26ed1ffe74abd8a5f62d4f3b341a62ebb1a04d43e7ab9d64b9d283e184b35fd4

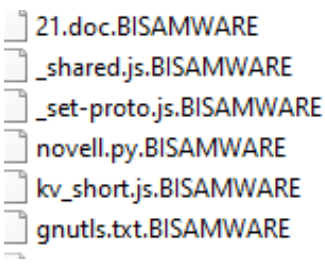
Cynet 360 AutoXDR™ Detections:



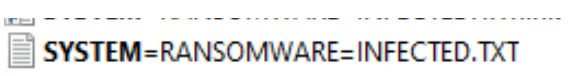


BISAMWARE Overview

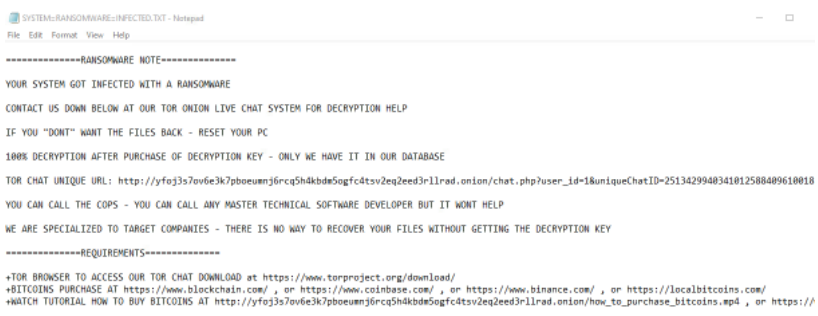
BISAMWARE ransomware renames the encrypted files with .BISAMWARE in the extension:



Once a computer's files have been encrypted and renamed, it drops a note named: SYSTEM=RANSOMWARE=INFECTED.TXT



The ransomware note contains general information, warnings, and the attacker's Tor chat:

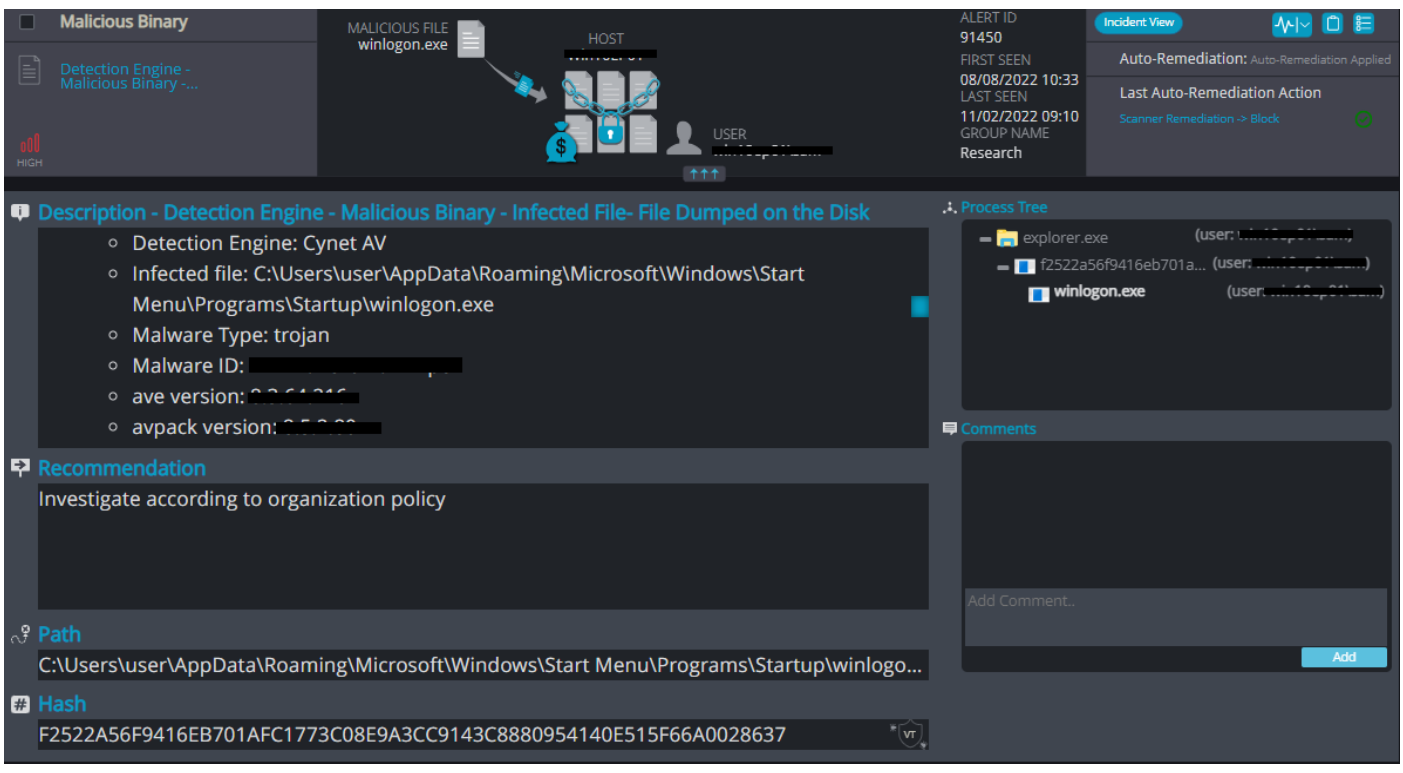


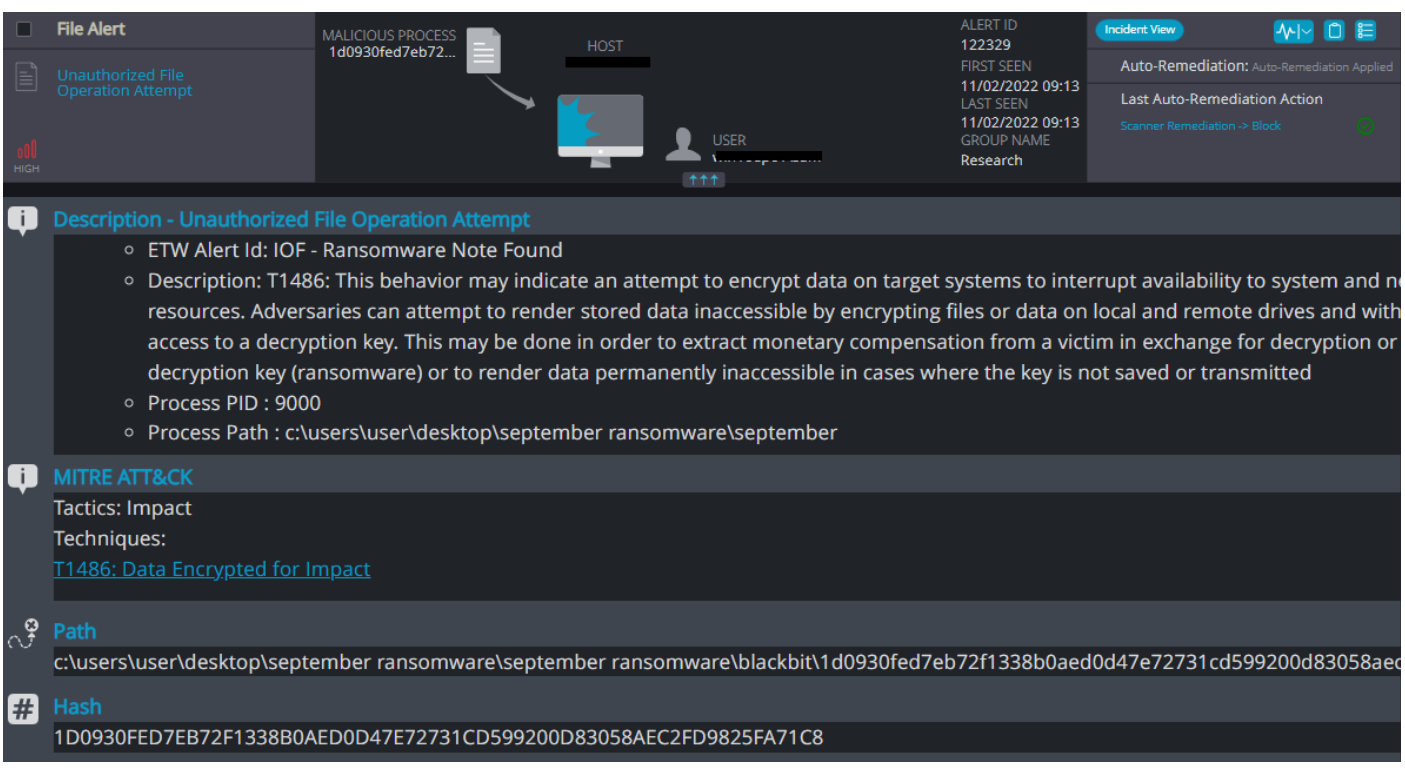
Orion Team

BlackBit Ransomware

- Observed since: 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .BlackBit
- Ransomware note: Restore-My-Files.txt
- Sample hash: 1d0930fed7eb72f1338b0aed0d47e72731cd599200d83058aec2fd9825fa71c8

Cynet 360 AutoXDR™ Detections:



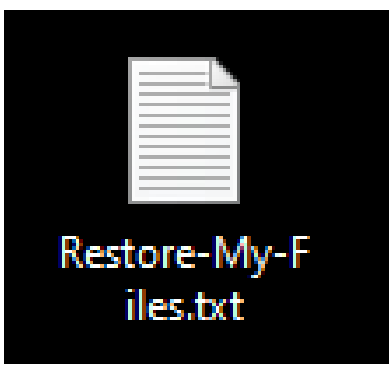


BlackBit Overview

BlackBit ransomware renames the encrypted files with .BlackBit in the extension:

[spystar@onionmail.org][E07BA3DD]17.docx.**Black**Bit
[spystar@onionmail.org][E07BA3DD]16.doc.**Black**Bit
[spystar@onionmail.org][E07BA3DD]15.jpg.**Black**Bit
[spystar@onionmail.org][E07BA3DD]14.xlsx.**Black**Bit
[spystar@onionmail.org][E07BA3DD]13.xls.**Black**Bit
[spystar@onionmail.org][E07BA3DD]12.docx.**Black**Bit
[spystar@onionmail.org][E07BA3DD]11.doc.**Black**Bit

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



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

Restore-My-Files.txt - Notepad

File Edit Format View Help

```
!!!All of your files are encrypted!!!
To decrypt them send e-mail to this address: spystar@onionmail.org
In case of no answer in 24h, send e-mail to this address: spystar1@onionmail.com
You can also contact us via Telegram: @Spystar_Support
All your files will be lost on Friday, December 2, 2022 2:10:42 AM.
Your SYSTEM ID : E07BA3DD
!!!Deleting "Cpriv.BlackBit" causes permanent data loss.
```

cynet

Thank you!

September, 2022