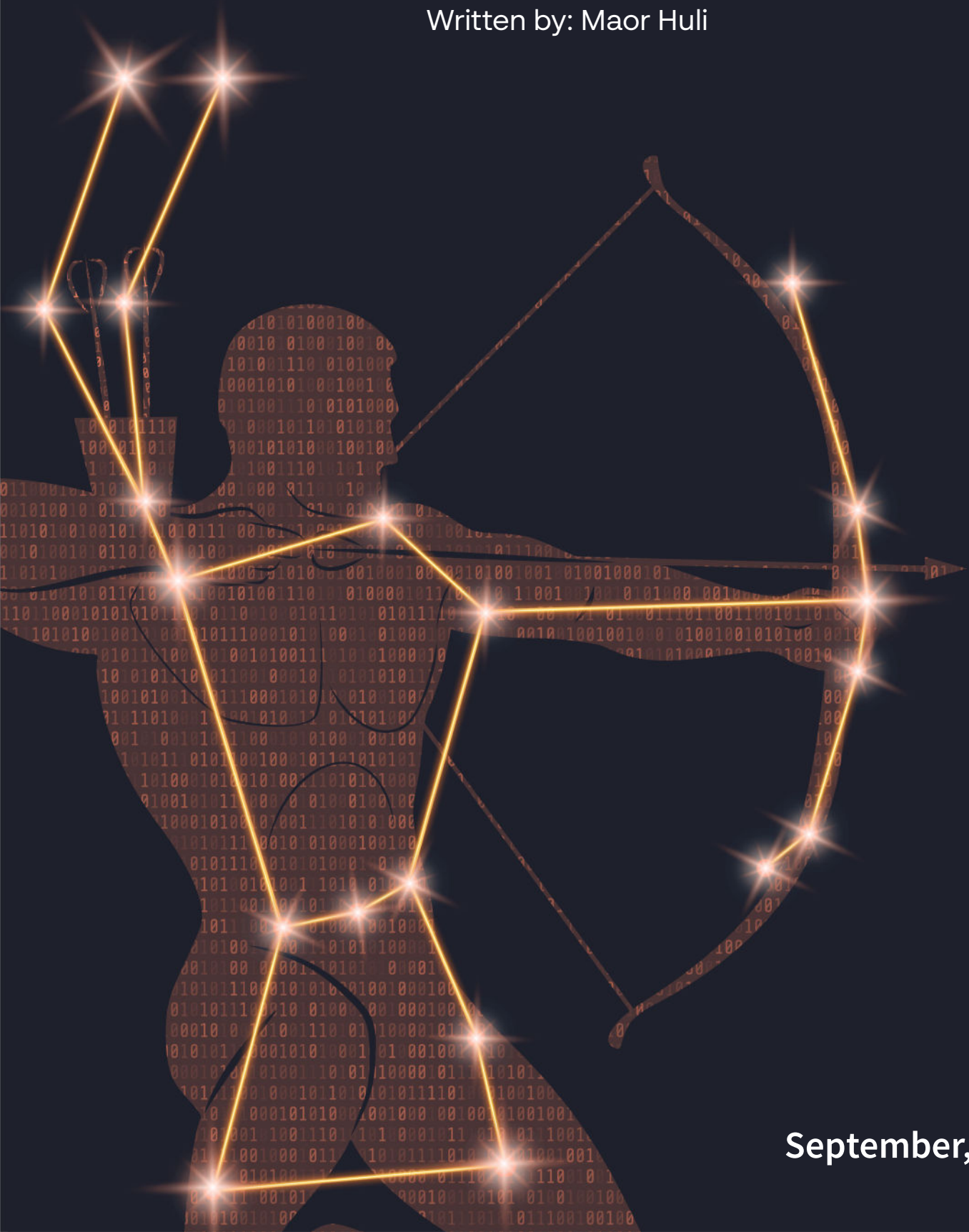


# Orion Team

## Monthly Ransomware Activity

Written by: Maor Huli



September, 2022



## Contents

<b>Executive Summary</b>	<b>3</b>
<b>Bl00dy</b>	<b>5</b>
<b>Ballacks</b>	<b>6</b>
<b>BISAMWARE</b>	<b>7</b>
<b>BlackBit</b>	<b>8</b>



## 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.

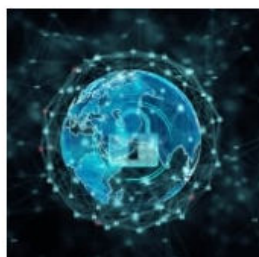
LAWRENCE ABRAMS SEPTEMBER 30, 2022 04:48 PM 0



### 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





## 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:

Malicious Binary

Detection Engine - Malicious Binary ...

MALICIOUS FILE

ef0ee6a6a64334...

HOST

...

ALERT ID

119264

FIRST SEEN

10/31/2022 14:03

LAST SEEN

10/31/2022 14:03

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\September Ransomware\September Ransomware\Bl00dy\ef0ee6a6a643347082e097f29cd351150b2d4196faef4ce926a307c2ca46f96a
- Malware Type: heuristic
- Malware ID: ...

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\September Ransomware\September Ransomware\Bl00dy\ef0ee6a6a643347082e097f29cd351150b2d4196faef4ce926a307c2...

Hash

EF0EE6A6A643347082E097F29CD351150B2D4196FAEF4CE926A307C2CA46F96A

File Alert

Unauthorized File Operation Attempt

MALICIOUS PROCESS

ef0ee6a6a64334...

HOST

...

ALERT ID

119330

FIRST SEEN

10/31/2022 14:32

LAST SEEN

10/31/2022 14:32

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 Activity Detected - Decoy Files - Unsigned Processes
- 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 where the key is not saved or transmitted
- Process PID : 1628

MITRE ATT&CK

Tactics: Impact

Techniques:  
[T1486: Data Encrypted for Impact](#)

Path

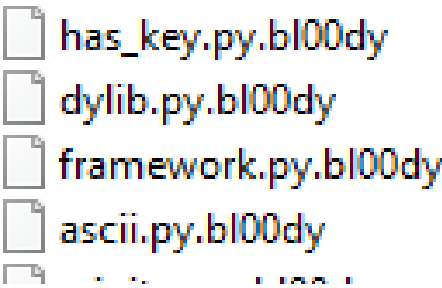
c:\users\user\desktop\september ransomware\september ransomware\bl00dy\ef0ee6a6a643347082e097f29cd351150b2d4196faef4ce926...

Hash

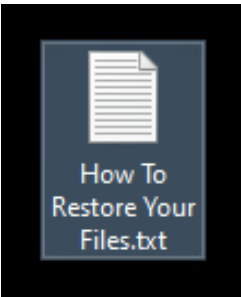
EF0EE6A6A643347082E097F29CD351150B2D4196FAEF4CE926A307C2CA46F96A

## Bl00dy Overview

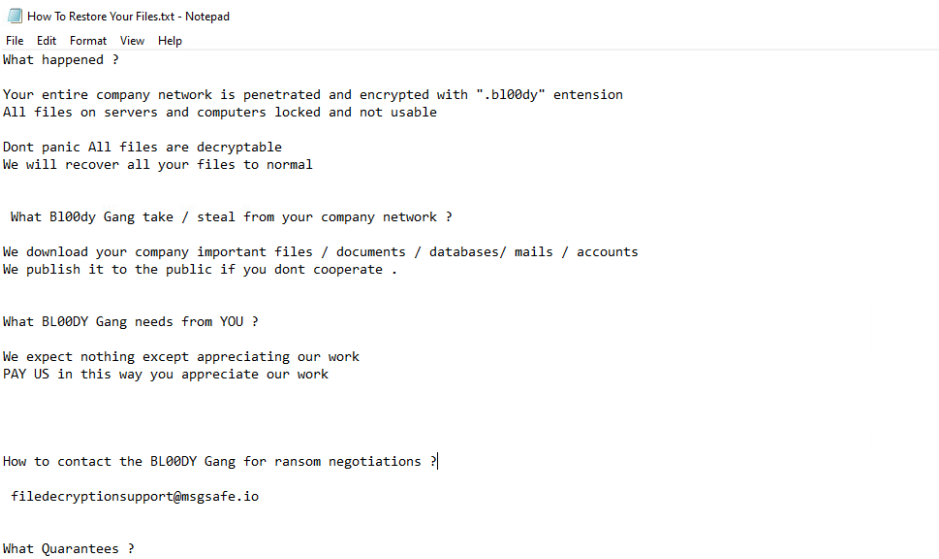
Bl00dy ransomware renames the encrypted files with .bl00dy in the extension.



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:





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:

Malicious Binary

Detection Engine - Malicious Binary - ...

HIGH

MALICIOUS FILE

6e457720acc913...

HOST

USER

ALERT ID

119334

FIRST SEEN

10/31/2022 15:30

LAST SEEN

10/31/2022 15:30

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Detection Engine - Malicious Binary - Infected File- Attempt to Run

- Detection Engine: Cynet AV
- Infected file: C:\Users\user\Desktop\September Ransomware\September Ransomware\Ballacks\6e457720acc91317e6318ab1bcc053d67ea3b8082a0b22ea976f6fe299cc8f14.exe
- Malware Type: heuristic
- Malware ID: [REDACTED]

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\September Ransomware\September Ransomware\Ballacks\6e457720acc91317e6318ab1bcc053d67ea3b8082a0b22ea976f6f...

Hash

6E457720ACC91317E6318AB1BCC053D67EA3B8082A0B22EA976F6FE299CC8F14

Malicious Binary

Malicious Binary

CRITICAL

MALICIOUS PROCESS

6e457720acc913...

HOST

USER

ALERT ID

119335

FIRST SEEN

10/31/2022 15:30

LAST SEEN

10/31/2022 15:30

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Malicious Binary

- Alert Origin: SSDEEP
- File Name: c:\users\user\desktop\september ransomware\september ransomware\ballacks\6e457720acc91317e6318ab1bcc053d67ea3b8082a0b22ea976f6fe299cc8f14.exe
- Process Fuzzy Hash: 24576:RaNjfy3Dhkm/37xczZf1y0hRZnsuhUW/xnYv/E4XoiJUSU/+2UiYGN2EA4c:oNJK3Fal7UuxCToRu22UiYGNN4c
- Known Process Fuzzy Hash: [REDACTED]

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\september ransomware\september ransomware\ballacks\6e457720acc91317e6318ab1bcc053d67ea3b8082a0b22ea976f6fe2...

Hash

6E457720ACC91317E6318AB1BCC053D67EA3B8082A0B22EA976F6FE299CC8F14

Ballacks Overview

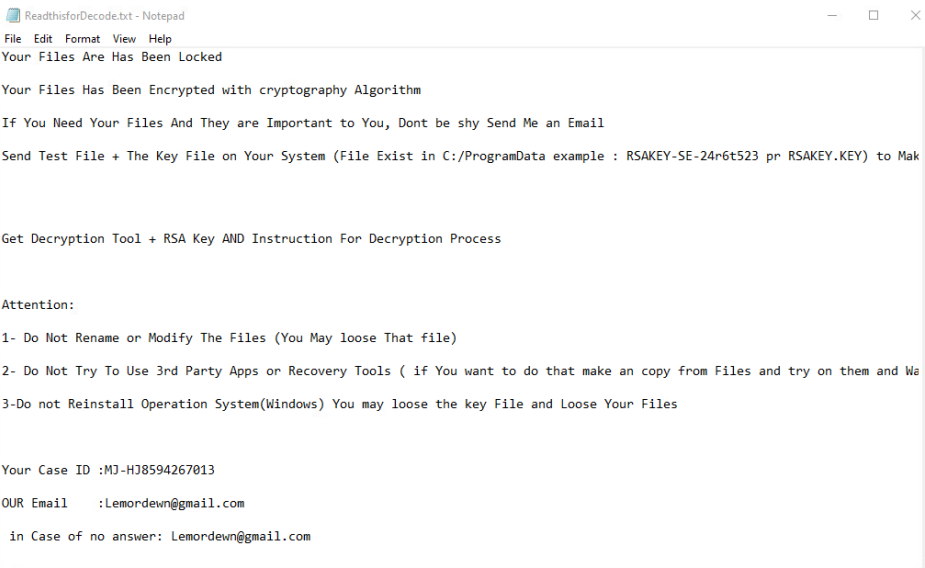
Ballacks ransomware renames the encrypted files with .ballacks in the extension:

- 39.xlsx.[MJ-HJ8594267013](Lemordewn@gmail.com).ballacks
- 38.xls.[MJ-HJ8594267013](Lemordewn@gmail.com).ballacks
- 37.docx.[MJ-HJ8594267013](Lemordewn@gmail.com).ballacks
- 36.doc.[MJ-HJ8594267013](Lemordewn@gmail.com).ballacks
- 35.jpg.[MJ-HJ8594267013](Lemordewn@gmail.com).ballacks

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:



## 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:

File Alert

Malicious Script Command

HIGH

MALICIOUS PROCESS

powershell.exe

HOST

██████████

ALERT ID

120374

FIRST SEEN

10/31/2022 15:59

LAST SEEN

10/31/2022 15:59

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Malicious Script Command

- Whitelist Rules Type: Malicious Script Command
- ETW Alert Id: PowerShell\_AMSI Heuristic Activity - Disable or Modify Tools - Windows Defender Exclusions - Extension
- Rule Name: PowerShell\_AMSI Heuristic Activity - Disable or Modify Tools - Windows Defender Exclusions - Extension
- Description: T1562.001: This behavior may indicate that an attempt was made to disable security tools to avoid possible detection of malicious tools and

MITRE ATT&CK

Tactics: Defense Evasion, Execution

Techniques:  
[T1562.001: Impair Defenses: Disable or Modify Tools](#)  
[T1059.001: Command and Scripting Interpreter: PowerShell](#)

Path

c:\windows\system32\windowspowershell\v1.0\powershell.exe

Hash

908B64B1971A979C7E3E8CE4621945CBA84854CB98D76367B791A6E22B5F6D53

Process Tree

explorer.exe (user: ██████████)

26ed1ffe74abd8a5f62d4f3b341a62ebb1a04d43e7ab9d64b9d283e184b35fd4 powershell.exe (user: ██████████)

Recommendation

Investigate according to organization policy

Comments

Add Comment...

Add

Ransomware

Ransomware Heuristic

CRITICAL

MALICIOUS PROCESS

26ed1ffe74abd8...

HOST

██████████

ALERT ID

120474

FIRST SEEN

10/31/2022 16:01

LAST SEEN

10/31/2022 16:16

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Ransomware Heuristic

- ETW Alert Id: Ransomware Heuristic
- Configuration Date (UTC): 2022-10-30 23:10:25
- Whitelist Configuration Date (UTC): 2022-10-20 14:03:40
- Detect PID of Ransomware: 4728
- Behavior Rule: 10 Decoy Files Deleted, 10 New Files Created
- Description: 0
- Delete: \device\harddiskvolume2\users\public\! cynet ransom protection(don't

Recommendation

Investigate according to organization policy

Path

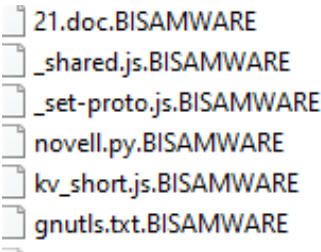
c:\users\user\desktop\september ransomware\september ransomware\bisamware\26ed1ffe74abd8a5f62d4f3b341a62ebb1a04d43e7ab9d64b9d283e184b35fd4

Hash

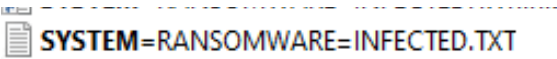
26ED1FFE74ABD8A5F62D4F3B341A62EBB1A04D43E7AB9D64B9D283E184B35FD4

## BISAMWARE Overview

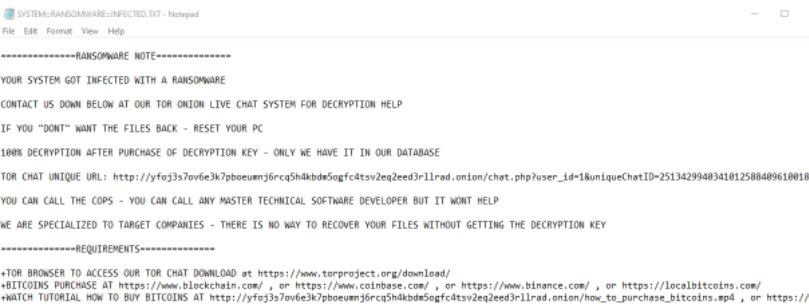
BISAMWARE ransomware renames the encrypted files with .BISAMWARE in the extension:



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:





## 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:

Malicious Binary

Detection Engine - Malicious Binary - ...

MALICIOUS FILE

winlogon.exe

HOST

USER

ALERT ID

91450

FIRST SEEN

08/08/2022 10:33

LAST SEEN

11/02/2022 09:10

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\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winlogon.exe
- Malware Type: trojan
- Malware ID: [REDACTED]
- ave version: 0.0.0.0
- avpack version: 0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winlogo...

Hash

F2522A56F9416EB701AFC1773C08E9A3CC9143C8880954140E515F66A0028637

Process Tree

- explorer.exe (user: [REDACTED])
  - f2522a56f9416eb701a... (user: [REDACTED])
    - winlogon.exe (user: [REDACTED])

Comments

Add Comment...

Add

File Alert

Unauthorized File Operation Attempt

MALICIOUS PROCESS

1d0930fed7eb72...

HOST

USER

ALERT ID

122329

FIRST SEEN

11/02/2022 09:13

LAST SEEN

11/02/2022 09:13

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 resources. Adversaries can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and with access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted
- Process PID : 9000
- Process Path : c:\users\user\desktop\september ransomware\september

MITRE ATT&CK

Tactics: Impact

Techniques:  
[T1486: Data Encrypted for Impact](#)

Path

c:\users\user\desktop\september ransomware\september ransomware\blackbit\1d0930fed7eb72f1338b0aed0d47e72731cd599200d83058aec...

Hash

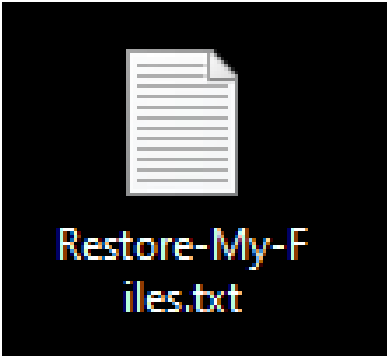
1D0930FED7EB72F1338B0AED0D47E72731CD599200D83058AEC2FD9825FA71C8

## BlackBit Overview

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

- 🔴 [spystar@onionmail.org][E07BA3DD]17.docx.BlackBit
- 🔴 [spystar@onionmail.org][E07BA3DD]16.doc.BlackBit
- 🔴 [spystar@onionmail.org][E07BA3DD]15.jpg.BlackBit
- 🔴 [spystar@onionmail.org][E07BA3DD]14.xlsx.BlackBit
- 🔴 [spystar@onionmail.org][E07BA3DD]13.xls.BlackBit
- 🔴 [spystar@onionmail.org][E07BA3DD]12.docx.BlackBit
- 🔴 [spystar@onionmail.org][E07BA3DD]11.doc.BlackBit

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.



# Thank you!



September, 2022