

# Orion Team

## Monthly Ransomware Activity

Written by: Maor Huli



December, 2022



## Contents

|                            |          |
|----------------------------|----------|
| <b>Medusa Locker .....</b> | <b>5</b> |
| <b>OBZ .....</b>           | <b>6</b> |
| <b>Lucknite .....</b>      | <b>7</b> |
| <b>HardBIT 2.0 .....</b>   | <b>8</b> |



## 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 - December 23rd 2022 - Targeting Microsoft Exchange

Reports this week illustrate how threat actors consider Microsoft Exchange as a prime target for gaining initial access to corporate networks to steal data and deploy ransomware.

LAWRENCE ABRAMS DECEMBER 23, 2022 03:51 PM 0



### The Week in Ransomware - December 16th 2022 - Losing Trust

Today's Week in Ransomware brings you the latest news and stories about the cyberattacks, new tactics, and reports related to ransomware operations.

LAWRENCE ABRAMS DECEMBER 16, 2022 05:59 PM 0



### The Week in Ransomware - December 9th 2022 - Wide Impact

This week has been filled with research reports and news of significant attacks having a wide impact on many organizations.

LAWRENCE ABRAMS DECEMBER 09, 2022 07:02 PM 0



### The Week in Ransomware - December 2nd 2022 - Disrupting Health Care

This week's big news was the Colombia health system being severely disrupted by a ransomware attack on Keralty, one of the country's largest healthcare providers.

LAWRENCE ABRAMS DECEMBER 02, 2022 05:51 PM 0

# Orion Team



# Cynet 360 AutoXDR™ VS Ransomware





Medusa Locker Ransomware

- Observed since: late 2019
- Ransomware encryption method: AES + RSA
- Ransomware extension: .cipher
- Ransomware note: !-Recovery\_instructions-!.html
- Sample hash: 8c0cc36cba7d54c1c225c95ef0a05f95ed317ffdb17e952e452e6555a719a927

Cynet 360 AutoXDR™ Detections:

Malicious Binary

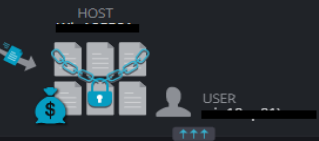
Detection Engine - Malicious Binary ~...

HIGH

MALICIOUS FILE

8c0cc36cba7d54...

HOST



ALERT ID

164543

FIRST SEEN

01/01/2023 10:24

LAST SEEN

01/01/2023 10:24

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\Dec Ransomware\Dec Ransomware\Medusa Locker\8c0cc36cba7d54c1c225c95ef0a05f95ed317ffdb17e952e452e6555a719a927
- Malware Type: heuristic
- Malware ID: MEDUSA-HEM-1010010
- ave version: 0.5.0.12
- avpack version: 0.5.0.00

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\Dec Ransomware\Dec Ransomware\Medusa Locker\8c0cc36cba7d54c1c225c95ef0a05f95ed317ffdb17e952e452e6555a719a927

Hash

8C0CC36CBA7D54C1C225C95EF0A05F95ED317FFDB17E952E452E6555A719A927

Ransomware

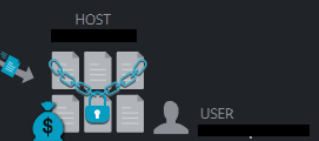
Ransomware Heuristic

CRITICAL

MALICIOUS PROCESS

8c0cc36cba7d54...

HOST



ALERT ID

164753

FIRST SEEN

01/01/2023 10:30

LAST SEEN

01/01/2023 10:32

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): 2022-12-31 19:00:31
- Whitelist Configuration Date (UTC): 2022-12-29 12:58:17
- Detect PID of Ransomware: 8728
- Behavior Rule: 10 Decoy Files Renamed
- Description: 0
- Rename: \device\harddiskvolume2\! cynet ransom protection(don't delete)\19.xlsx.cipher,\device\harddiskvolume2\! cynet ransom

Recommendation

Investigate according to organization policy

Path

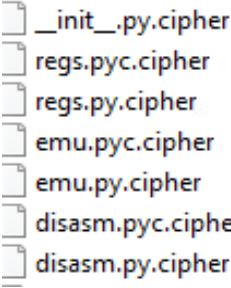
c:\users\user\desktop\dec ransomware\dec ransomware\medusa locker\8c0cc36cba7d54c1c225c95ef0a05f95ed317ffdb17e952e452e6555a719a927

Hash

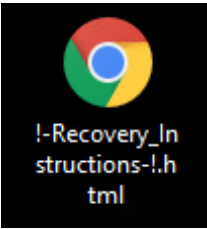
8C0CC36CBA7D54C1C225C95EF0A05F95ED317FFDB17E952E452E6555A719A927

Medusa Locker Overview

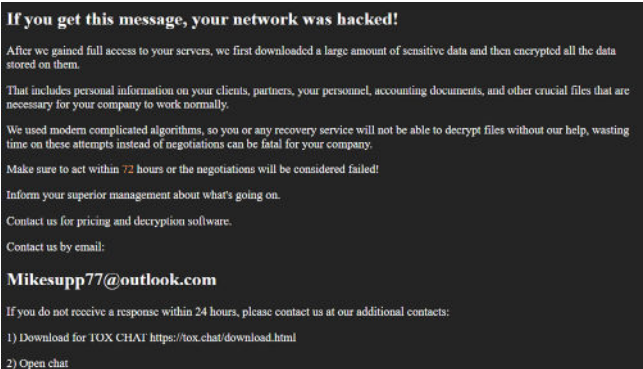
Medusa Locker ransomware renames the encrypted files with “.cipher” in the extension:



Once a computer’s files have been encrypted and renamed, Medusa Locker drops a note named “!-Recovery\_instructions-!.html”:



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





OBZ Ransomware

- Observed since: Dec 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .OBZ
- Ransomware note: ReadMe.txt
- Sample hash: 4cbd48893182071bbb208d732369b8ca73fb9fb027ef63b20a9bc6768aba3521

Cynet 360 AutoXDR™ Detections:

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

4cbd4889318207...

HOST

USER

ALERT ID

165316

FIRST SEEN

01/01/2023 10:54

LAST SEEN

01/01/2023 10:54

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 : 4992

MITRE ATT&CK

Tactics: Impact

Techniques:

T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\dec ransomware\dec ransomware\obz\4cbd48893182071bbb208d732369b8ca73fb9fb027ef63b20a9bc6768aba35...

Hash

4CBD48893182071BBB208D732369B8CA73FB9FB027EF63B20A9BC6768ABA3521

Ransomware

Ransomware Heuristic

CRITICAL

MALICIOUS PROCESS

4cbd4889318207...

HOST

USER

ALERT ID

165317

FIRST SEEN

01/01/2023 10:54

LAST SEEN

01/01/2023 10:54

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): 2022-12-31 19:00:31
- Whitelist Configuration Date (UTC): 2022-12-29 12:58:17
- Detect PID of Ransomware: 4992
- Behavior Rule: 7 Data Files Extensions Have Changed (Rename)
- Description: 0
- Rename Familiar Previous Extension: c:\! cynet ransom protection(don't delete)\19.xlsx.obz;c:\! cynet ransom protection(don't

Recommendation

Investigate according to organization policy

Path

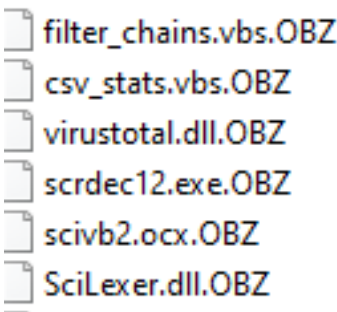
c:\users\user\desktop\dec ransomware\dec ransomware\obz\4cbd48893182071bbb208d732369b8ca73fb9fb027ef63b20a9bc6768aba35...

Hash

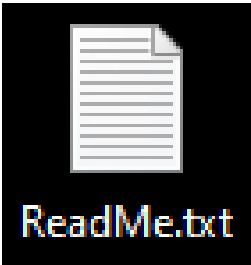
4CBD48893182071BBB208D732369B8CA73FB9FB027EF63B20A9BC6768ABA3521

OBZ Overview

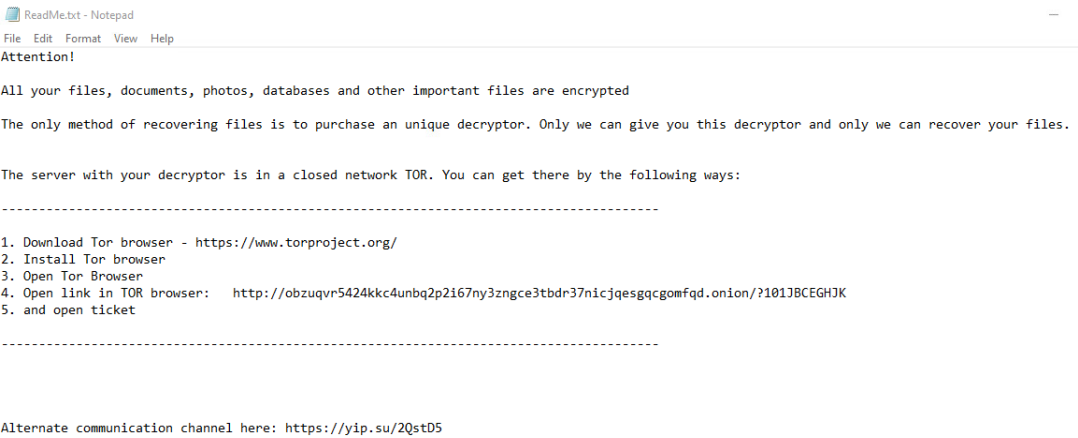
OBZ ransomware renames the encrypted files with “.OBZ” in the extension:



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



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





## Lucknite Ransomware

- Observed since: June 2021
- Ransomware encryption method: AES + RSA
- Ransomware extension: .lucknite
- Ransomware note: README.txt
- Sample hash: 0f36909d803b00afa7ec5c925651bbf9980f64318d55e9f4db7994aa1d2a1815

## Cynet 360 AutoXDR™ Detections:

File Alert

Process Monitoring

HIGH

MALICIOUS PROCESS

svchost.exe

HOST

USER

win10ep01\sam

ALERT ID

23197

FIRST SEEN

02/08/2022 16:09

LAST SEEN

01/01/2023 11:17

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Process Monitoring

ETW Alert Id: CyAlert Heuristic Activity - Masquerading Invalid Critical System File Path

Description: T1036.005: This behavior may indicate that an attempt was made to match or approximate the name or location of legitimate files when naming or placing their files. This is done for the sake of evading defenses and observation. This may be done by placing an executable in a commonly trusted directory or giving it the name of a legitimate,

MITRE ATT&CK

Tactics: Defense Evasion

Techniques:

T1036.005: Masquerading: Match Legitimate Name or Location

Path

c:\users\user\appdata\roaming\svchost.exe

Hash

B103FC649787EB1F6121DF8174D0F16AAAC736FB53F5F078D312871189285956

Process Tree

explorer.exe

chaos.exe

svchost.exe

Recommendation

Investigate according to organization policy

Comments

Add Comment..

Add

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

svchost.exe

HOST

USER

win10ep01\sam

ALERT ID

166143

FIRST SEEN

01/01/2023 11:21

LAST SEEN

01/01/2023 11:21

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

MITRE ATT&CK

Tactics: Impact

Techniques:

T1486: Data Encrypted for Impact

Path

c:\users\user\appdata\roaming\svchost.exe

Hash

0F36909D803B00AFA7EC5C925651BBF9980F64318D55E9F4DB7994AA1D2A1815

Process Tree

explorer.exe

0F36909d803b00afa7e... (user: win10ep01\sam)

svchost.exe

Recommendation

Investigate according to organization policy

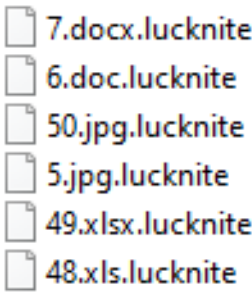
Comments

Add Comment..

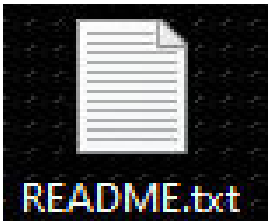
Add

## Lucknite Overview

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

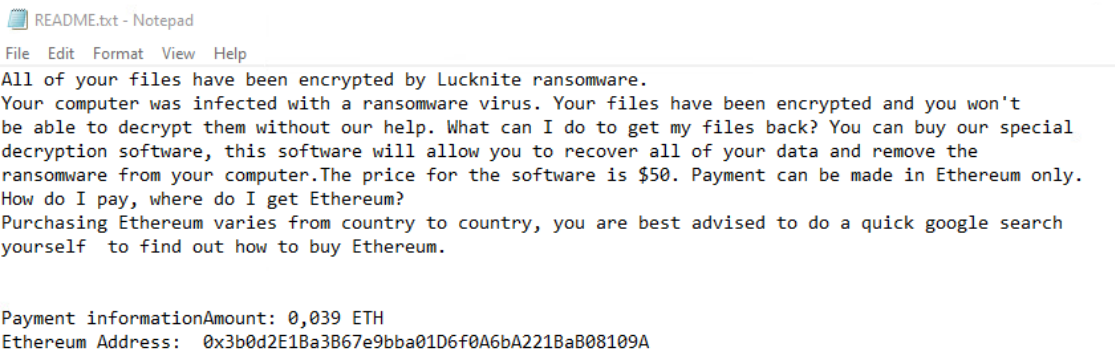


Once a computer’s files have been encrypted and renamed, Lucknite drops a note named “README.txt”:



Upon execution, it immediately encrypts the endpoint and drops the ransomware note.

The ransomware note contains general information, warnings, and the attacker's wallet number (no decryption guaranteed):





HardBIT 2.0 Ransomware

- Observed since: Dec 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .hardbit2
- Ransomware note: How To Restore Your Files.txt
- Sample hash: a0138b24593483f50ae7656985b6d6cfe77f7676ba374026199ad49ad26f2992

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

HIGH

MALICIOUS FILE

a0138b24593483...

HOST

ALERT ID

164544

FIRST SEEN

01/01/2023 10:24

LAST SEEN

01/01/2023 11:17

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\Dec Ransomware\Dec Ransomware\HardBIT\A0138b24593483f50ae7656985b6d6cfe77f7676ba374026199ad49ad26f2992
- Malware Type: trojan
- Malware ID: T32423999-00000000-00000000-00000000
- ave version: 0.0.0.0
- avpack version: 0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\Dec Ransomware\Dec Ransomware\HardBIT\A0138b24593483f50ae7656985b6d6cfe77f7676ba374026199ad49ad2...

Hash

A0138B24593483F50AE7656985B6D6CFE77F7676BA374026199AD49AD26F2992

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

svchost.exe

HOST

ALERT ID

166664

FIRST SEEN

01/01/2023 11:36

LAST SEEN

01/01/2023 11:36

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

MITRE ATT&CK

Tactics: Impact

Techniques:

T1486: Data Encrypted for Impact

Path

c:\users\user\appdata\roaming\svchost.exe

Hash

0F36909D803B00AFA7EC5C925651BBF9980F64318D55E9F4DB7994AA1D2A1815

Process Tree

- explorer.exe (user: user)
- 0F36909d803b00afa7e... (user: user)
- svchost.exe (user: user)

Recommendation

Investigate according to organization policy

Comments

Add Comment...

Add

HardBIT Overview

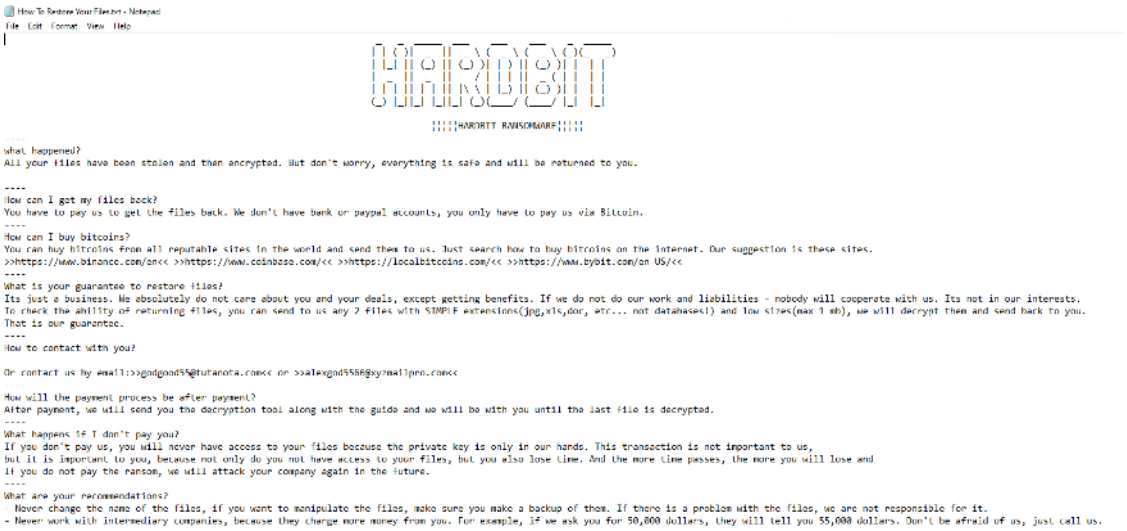
HardBIT ransomware renames the encrypted files with “.hardbit2” in the extension:

```
3p5424c6f8.[id-1F8BF8FF000406F1, 1F8BF8FF000006F1].[godgood55@tutanota.com].hardbit2
ftvh33j68v.[id-1F8BF8FF000406F1, 1F8BF8FF000006F1].[godgood55@tutanota.com].hardbit2
uiwk247nd0.[id-1F8BF8FF000406F1, 1F8BF8FF000006F1].[godgood55@tutanota.com].hardbit2
vc1057i2pg.[id-1F8BF8FF000406F1, 1F8BF8FF000006F1].[godgood55@tutanota.com].hardbit2
j13c880cl0.[id-1F8BF8FF000406F1, 1F8BF8FF000006F1].[godgood55@tutanota.com].hardbit2
7iifo3715a.[id-1F8BF8FF000406F1, 1F8BF8FF000006F1].[godgood55@tutanota.com].hardbit2
```

Once a computer’s files have been encrypted and renamed, HardBIT drops a note named “How To Restore Your Files.txt”:



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





# Thank you!



December, 2022