Orion Team

Monthly Ransomware Activity

Written by: Maor Huli

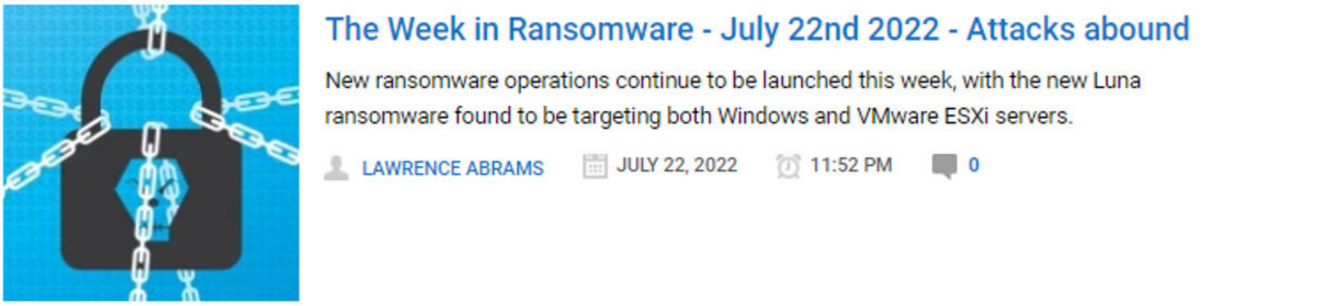
July, 2022

Contents

Orion Team

Executive Summary

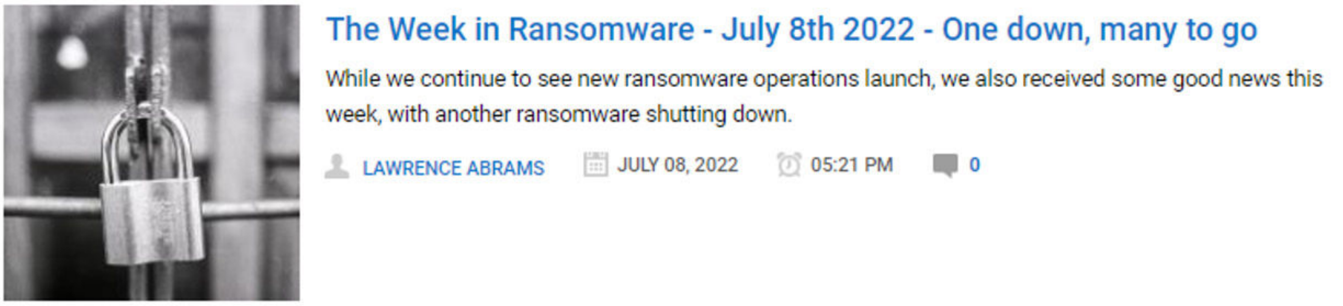
Orion is an integral department in Cynet's research team that works around the clock to track threat intelligence resources, analyze payloads, and automate labs to ensure that our customers are protected against the newest ransomware variants. In these monthly reports, Orion reviews the latest trends 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 - July 22nd 2022 - Attacks abound

New ransomware operations continue to be launched this week, with the new Luna ransomware found to be targeting both Windows and VMware ESXi servers.

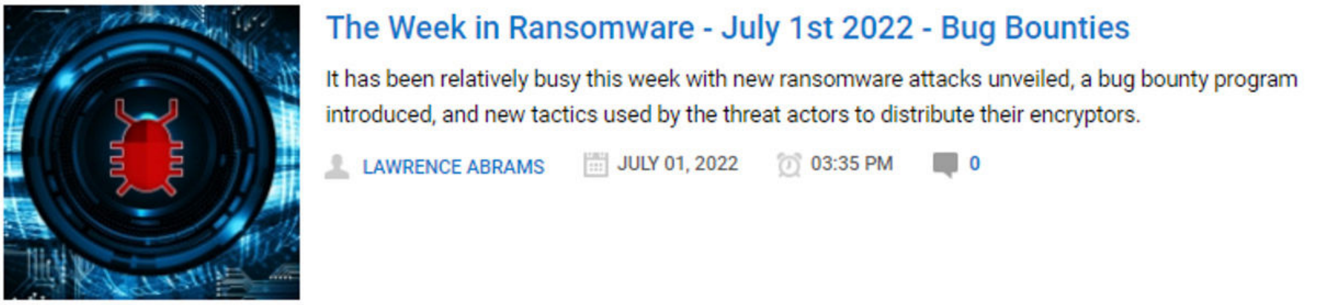
LAWRENCE ABRAMS JULY 22, 2022 11:52 PM 0



The Week in Ransomware - July 8th 2022 - One down, many to go

While we continue to see new ransomware operations launch, we also received some good news this week, with another ransomware shutting down.

LAWRENCE ABRAMS JULY 08, 2022 05:21 PM 0



The Week in Ransomware - July 1st 2022 - Bug Bounties

It has been relatively busy this week with new ransomware attacks unveiled, a bug bounty program introduced, and new tactics used by the threat actors to distribute their encryptors.

LAWRENCE ABRAMS JULY 01, 2022 03:35 PM 0

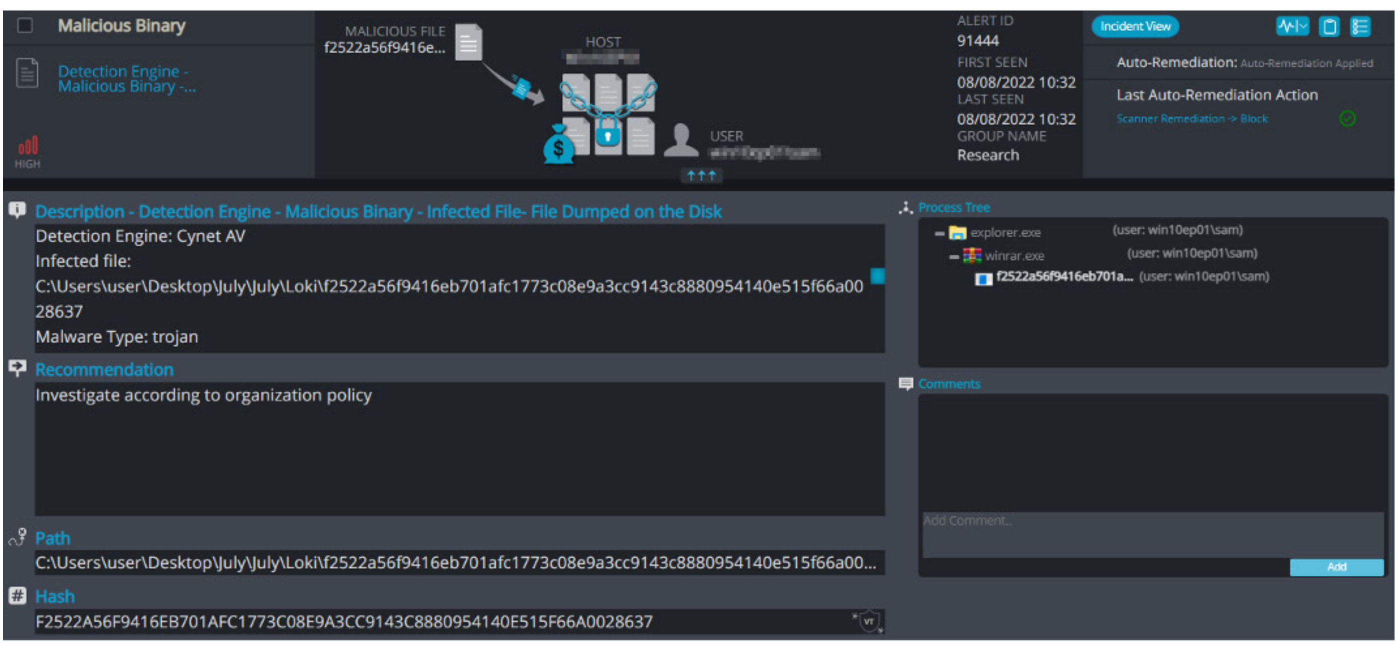
Orion Team

Cynet 360 AutoXDR™ VS Ransomware

Loki Ransomware

- Observed since: Late 2021
- Ransomware encryption method: AES + RSA
- Ransomware extension: .PayForKey
- Ransomware note: Restore-My-Files.txt
- Sample hash: f2522a56f9416eb701afc1773c08e9a3cc9143c8880954140e515f66a0028637

Cynet 360 AutoXDR™ Detections:



Malicious Binary

Detection Engine - Malicious Binary -...

HIGH

MALICIOUS FILE
f2522a56f9416e...

HOST
[redacted]

USER
[redacted]

ALERT ID
91444
FIRST SEEN
08/08/2022 10:32
LAST SEEN
08/08/2022 10:32
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\July\July\Loki\f2522a56f9416eb701afc1773c08e9a3cc9143c8880954140e515f66a0028637
Malware Type: trojan

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\July\July\Loki\f2522a56f9416eb701afc1773c08e9a3cc9143c8880954140e515f66a00...

Hash

F2522A56F9416EB701AFC1773C08E9A3CC9143C8880954140E515F66A0028637

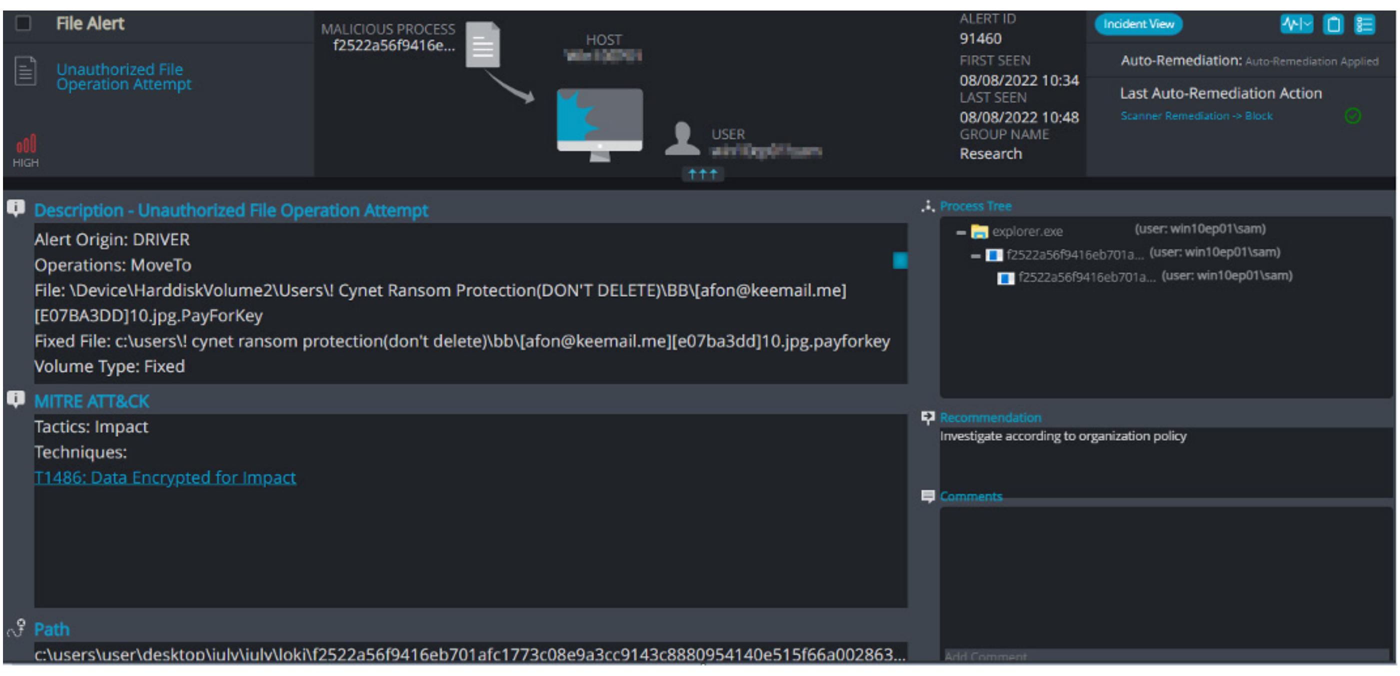
Process Tree

```
− explorer.exe                 (user: win10ep01\sam)
  − winrar.exe                 (user: win10ep01\sam)
      f2522a56f9416eb701a...  (user: win10ep01\sam)
```

Comments

Add Comment...

Add



File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS
f2522a56f9416e...

HOST
[redacted]

USER
[redacted]

ALERT ID
91460
FIRST SEEN
08/08/2022 10:34
LAST SEEN
08/08/2022 10:48
GROUP NAME
Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action
Scanner Remediation -> Block

Description - Unauthorized File Operation Attempt

Alert Origin: DRIVER
Operations: MoveTo
File: \Device\HarddiskVolume2\Users\! Cynet Ransom Protection(DON'T DELETE)\BB\[afon@keemail.me][E07BA3DD]10.jpg.PayForKey
Fixed File: c:\users\! cynet ransom protection(don't delete)\bb\[afon@keemail.me][e07ba3dd]10.jpg.payforkey
Volume Type: Fixed

MITRE ATT&CK

Tactics: Impact
Techniques:
T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\july\july\loki\f2522a56f9416eb701afc1773c08e9a3cc9143c8880954140e515f66a002863...

Process Tree

```
− explorer.exe                 (user: win10ep01\sam)
  − f2522a56f9416eb701a...    (user: win10ep01\sam)
      f2522a56f9416eb701a...  (user: win10ep01\sam)
```

Recommendation

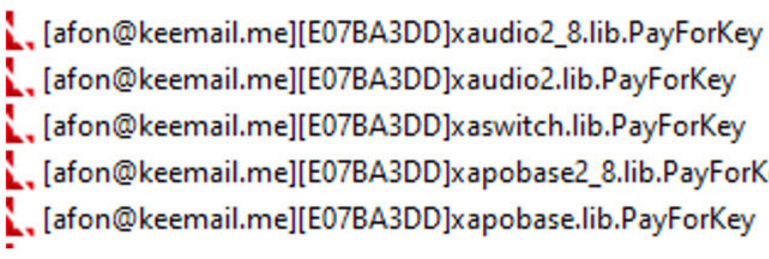
Investigate according to organization policy

Comments

Add Comment

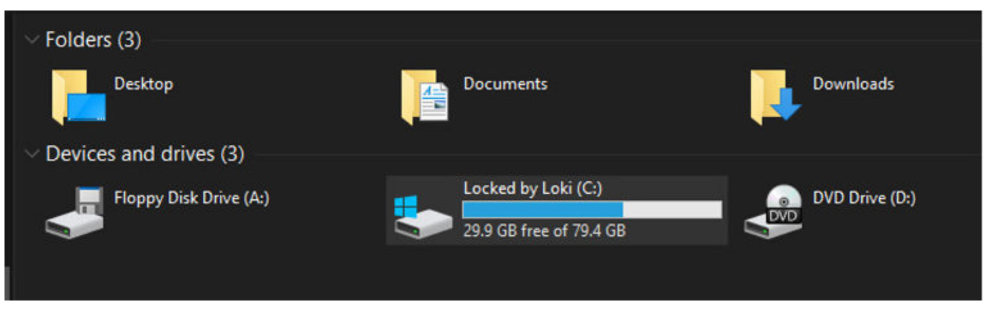
Loki Overview

Loki ransomware renames the encrypted files with .PayForKey, along with the attacker's email and the host ID in the extension.



```
[afon@keemail.me][E07BA3DD]xaudio2_8.lib.PayForKey
[afon@keemail.me][E07BA3DD]xaudio2.lib.PayForKey
[afon@keemail.me][E07BA3DD]xaswitch.lib.PayForKey
[afon@keemail.me][E07BA3DD]xapobase2_8.lib.PayForKey
[afon@keemail.me][E07BA3DD]xapobase.lib.PayForKey
```

The ransomware also encrypts the entire Drive C: (the system drive):



Folders (3)

Desktop · Documents · Downloads

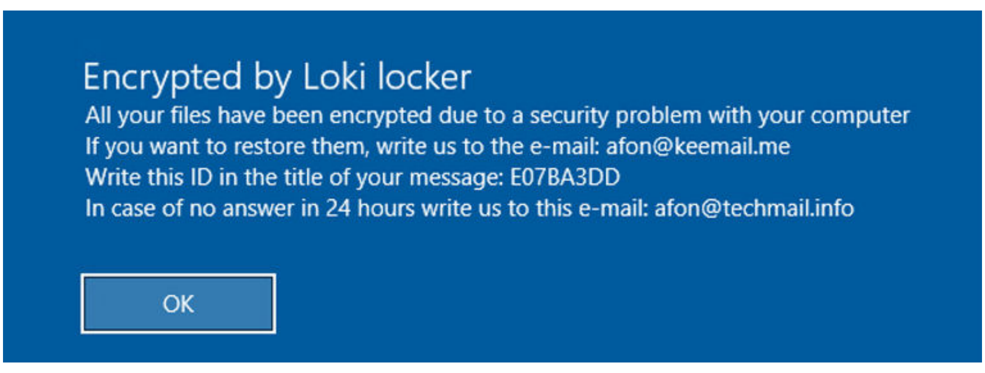
Devices and drives (3)

Floppy Disk Drive (A:)

Locked by Loki (C:)
29.9 GB free of 79.4 GB

DVD Drive (D:)

Eventually, it shuts down the computer and locks out the user until a payment:

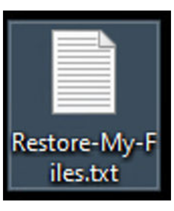


Encrypted by Loki locker

All your files have been encrypted due to a security problem with your computer
If you want to restore them, write us to the e-mail: afon@keemail.me
Write this ID in the title of your message: E07BA3DD
In case of no answer in 24 hours write us to this e-mail: afon@techmail.info

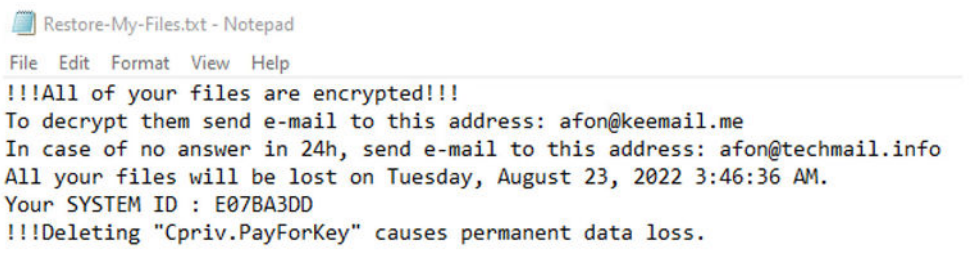
OK

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



Restore-My-Files.txt

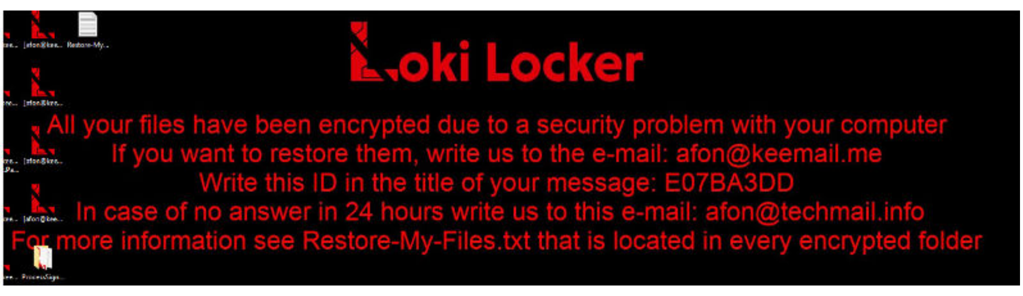
The ransomware note contains general information, warnings, and the attacker's email address:



Restore-My-Files.txt - Notepad

```
!!!All of your files are encrypted!!!
To decrypt them send e-mail to this address: afon@keemail.me
In case of no answer in 24h, send e-mail to this address: afon@techmail.info
All your files will be lost on Tuesday, August 23, 2022 3:46:36 AM.
Your SYSTEM ID : E07BA3DD
!!!Deleting "Cpriv.PayForKey" causes permanent data loss.
```

Before shutting down, the ransomware also changes the desktop background:



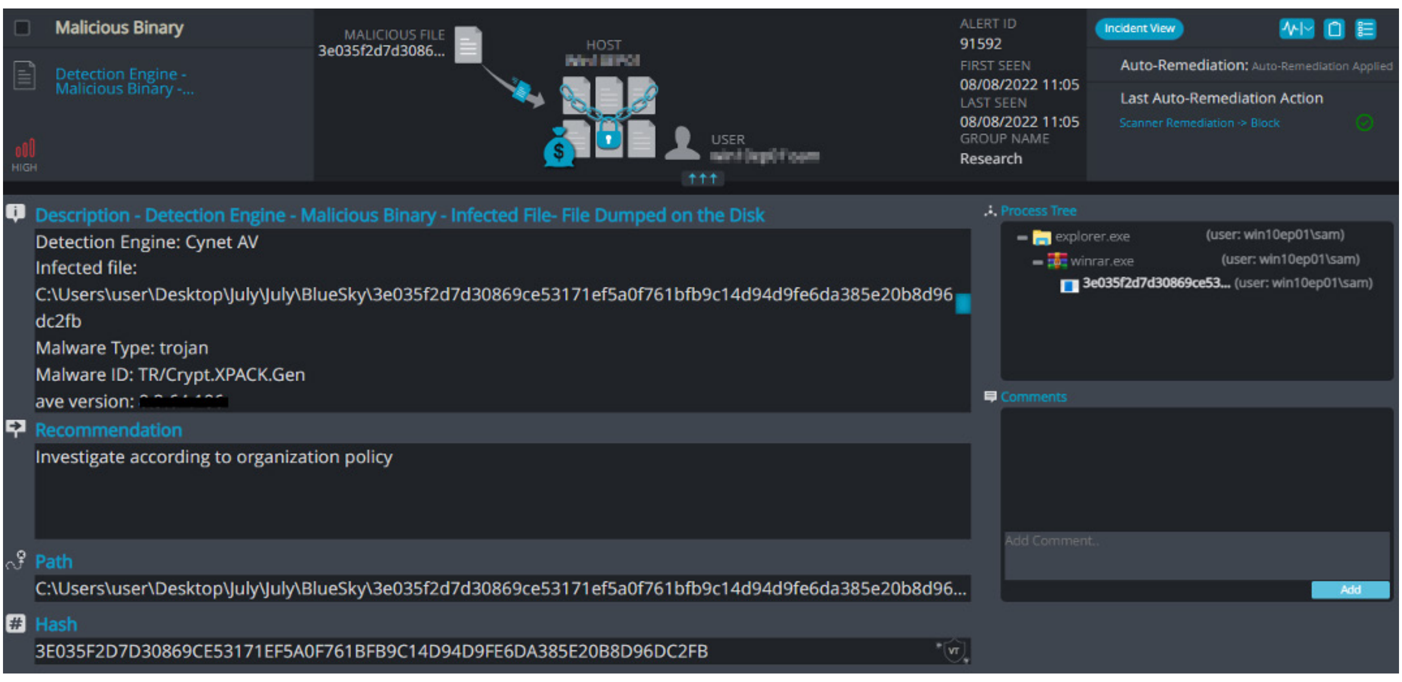
Loki Locker

All your files have been encrypted due to a security problem with your computer
If you want to restore them, write us to the e-mail: afon@keemail.me
Write this ID in the title of your message: E07BA3DD
In case of no answer in 24 hours write us to this e-mail: afon@techmail.info
For more information see Restore-My-Files.txt that is located in every encrypted folder

BlueSky Ransomware

- Observed since: 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .bluesky
- Ransomware note: # DECRYPT FILES BLUESKY #.txt | .html
- Sample hash: 3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96dc2fb

Cynet 360 AutoXDR™ Detections:



Malicious Binary

Detection Engine - Malicious Binary -...

HIGH

MALICIOUS FILE 3e035f2d7d3086...

HOST [redacted]

USER [redacted]

ALERT ID 91592

FIRST SEEN 08/08/2022 11:05

LAST SEEN 08/08/2022 11:05

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\July\July\BlueSky\3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96dc2fb
Malware Type: trojan
Malware ID: TR/Crypt.XPACK.Gen
ave version: [redacted]

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\July\July\BlueSky\3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96...

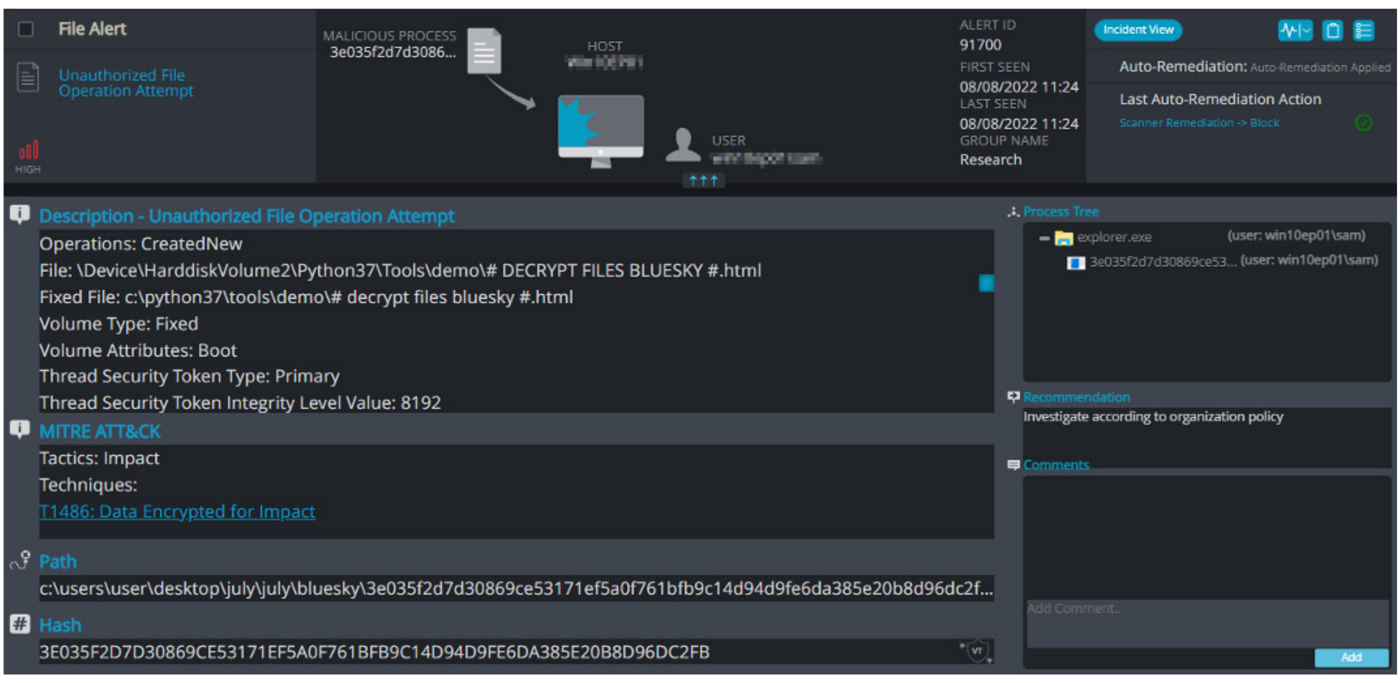
Hash

3E035F2D7D30869CE53171EF5A0F761BFB9C14D94D9FE6DA385E20B8D96DC2FB

Process Tree

```
- explorer.exe            (user: win10ep01\sam)
  - winrar.exe            (user: win10ep01\sam)
      3e035f2d7d30869ce53... (user: win10ep01\sam)
```

Comments



File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS 3e035f2d7d3086...

HOST [redacted]

USER [redacted]

ALERT ID 91700

FIRST SEEN 08/08/2022 11:24

LAST SEEN 08/08/2022 11:24

GROUP NAME Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Unauthorized File Operation Attempt

Operations: CreatedNew
File: \Device\HarddiskVolume2\Python37\Tools\demo\# DECRYPT FILES BLUESKY #.html
Fixed File: c:\python37\tools\demo\# decrypt files bluesky #.html
Volume Type: Fixed
Volume Attributes: Boot
Thread Security Token Type: Primary
Thread Security Token Integrity Level Value: 8192

MITRE ATT&CK

Tactics: Impact
Techniques:
T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\july\july\bluesky\3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96dc2f...

Hash

3E035F2D7D30869CE53171EF5A0F761BFB9C14D94D9FE6DA385E20B8D96DC2FB

Process Tree

```
- explorer.exe            (user: win10ep01\sam)
    3e035f2d7d30869ce53... (user: win10ep01\sam)
```

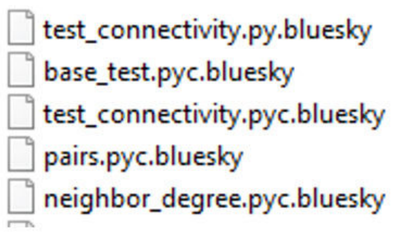
Recommendation

Investigate according to organization policy

Comments

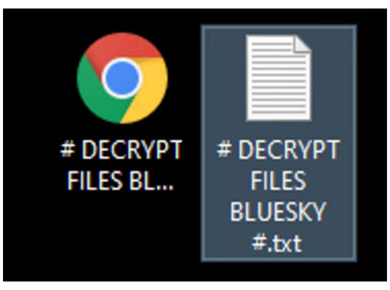
BlueSky Overview

BlueSky ransomware renames the encrypted files with .bluesky in the extension:

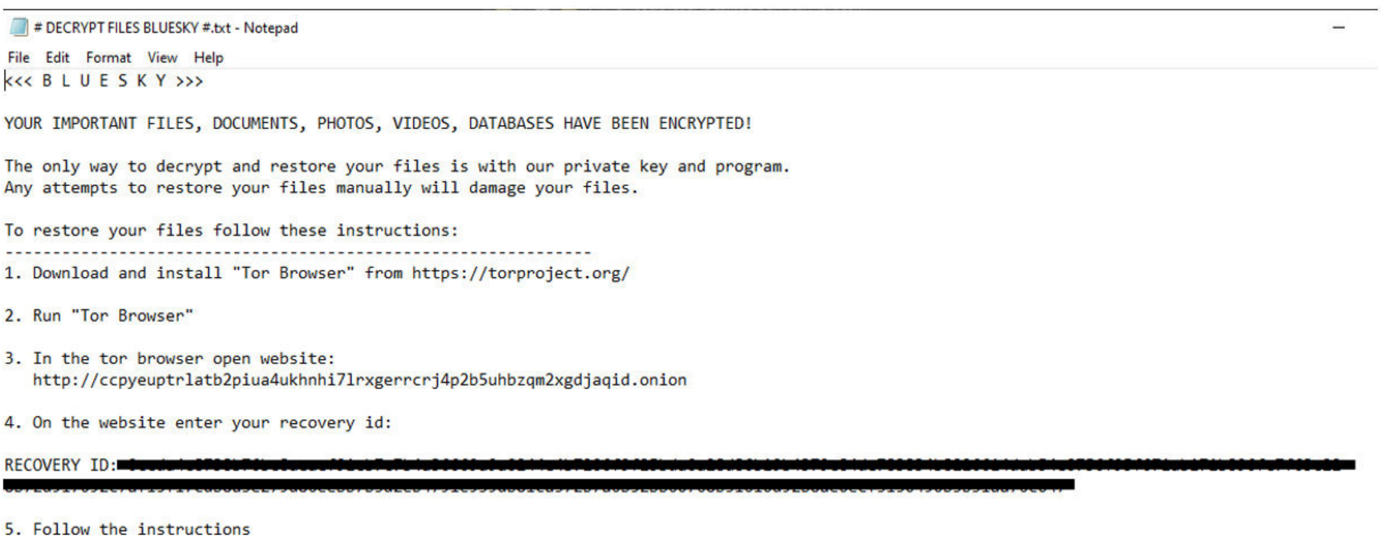


test_connectivity.py.bluesky
base_test.pyc.bluesky
test_connectivity.pyc.bluesky
pairs.pyc.bluesky
neighbor_degree.pyc.bluesky

Once a computer's files have been encrypted and renamed, it attempts to drop the ransomware note named # DECRYPT FILES BLUESKY #.txt | .html:



That ransomware note contains general information, warnings, and the attacker's tor website:



# DECRYPT FILES BLUESKY #.txt - Notepad

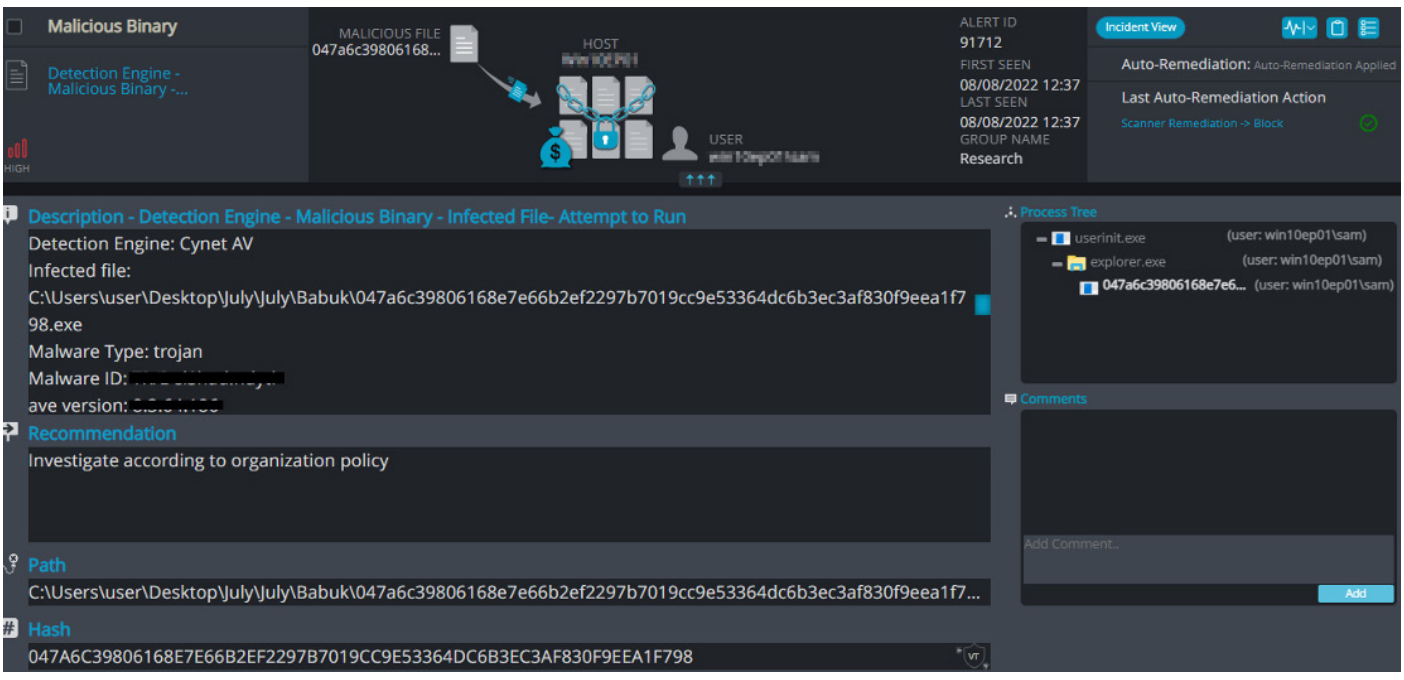
```
<<< B L U E S K Y >>>

YOUR IMPORTANT FILES, DOCUMENTS, PHOTOS, VIDEOS, DATABASES HAVE BEEN ENCRYPTED!

The only way to decrypt and restore your files is with our private key and program.
Any attempts to restore your files manually will damage your files.

To restore your files follow these instructions:
--------------------------------------------------------------
1. Download and install "Tor Browser" from https://torproject.org/

2. Run "Tor Browser"

3. In the tor browser open website:
   http://ccpyeuptrlatb2piua4ukhnhi7lrxgerrcrj4p2b5uhbzqm2xgdjaqid.onion

4. On the website enter your recovery id:

RECOVERY ID:[redacted]

5. Follow the instructions
```

Orion Team

Babuk Ransomware

- Observed since: Early 2021
- Ransomware encryption method: AES + RSA
- Ransomware extension: .again
- Ransomware note: How To Restore Your Files.txt
- Sample hash: 047a6c39806168e7e66b2ef2297b7019cc9e53364dc6b3ec3af830f9eea1f798

Cynet 360 AutoXDR™ Detections:



Malicious Binary

Detection Engine - Malicious Binary -...

HIGH

MALICIOUS FILE
047a6c39806168...

HOST
[redacted]

USER
[redacted]

ALERT ID
91712
FIRST SEEN
08/08/2022 12:37
LAST SEEN
08/08/2022 12:37
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\July\July\Babuk\047a6c39806168e7e66b2ef2297b7019cc9e53364dc6b3ec3af830f9eea1f7
98.exe
Malware Type: trojan
Malware ID: [redacted]
ave version: [redacted]
```

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\July\July\Babuk\047a6c39806168e7e66b2ef2297b7019cc9e53364dc6b3ec3af830f9eea1f7...

Hash

047A6C39806168E7E66B2EF2297B7019CC9E53364DC6B3EC3AF830F9EEA1F798

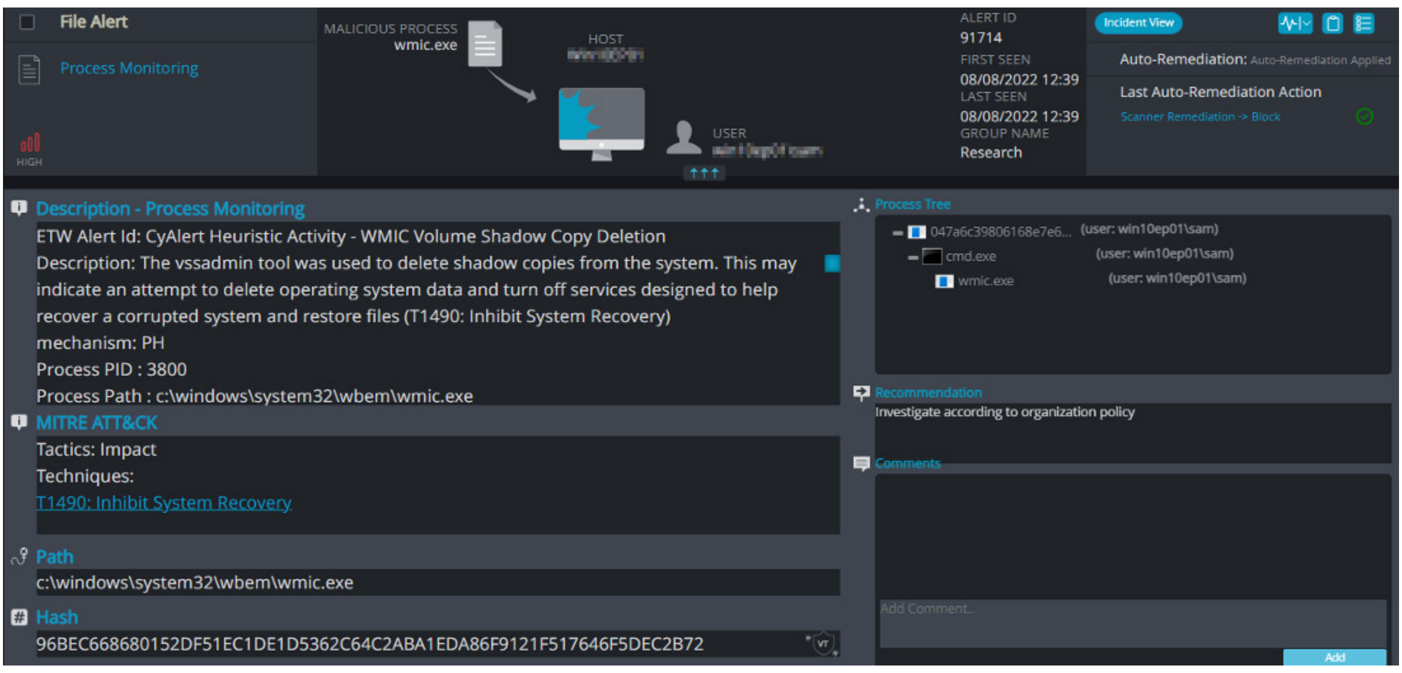
Process Tree

```
- userinit.exe                 (user: win10ep01\sam)
  - explorer.exe               (user: win10ep01\sam)
      047a6c39806168e7e6...    (user: win10ep01\sam)
```

Comments

Add Comment..

Add



File Alert

Process Monitoring

HIGH

MALICIOUS PROCESS
wmic.exe

HOST
[redacted]

USER
[redacted]

ALERT ID
91714
FIRST SEEN
08/08/2022 12:39
LAST SEEN
08/08/2022 12:39
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 - WMIC Volume Shadow Copy Deletion
Description: The vssadmin tool was used to delete shadow copies from the system. This may
indicate an attempt to delete operating system data and turn off services designed to help
recover a corrupted system and restore files (T1490: Inhibit System Recovery)
mechanism: PH
Process PID : 3800
Process Path : c:\windows\system32\wbem\wmic.exe
```

MITRE ATT&CK

Tactics: Impact
Techniques:
T1490: Inhibit System Recovery

Path

c:\windows\system32\wbem\wmic.exe

Hash

96BEC668680152DF51EC1DE1D5362C64C2ABA1EDA86F9121F517646F5DEC2B72

Process Tree

```
- 047a6c39806168e7e6...   (user: win10ep01\sam)
  - cmd.exe               (user: win10ep01\sam)
      wmic.exe            (user: win10ep01\sam)
```

Recommendation

Investigate according to organization policy

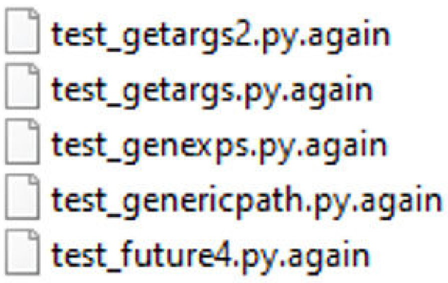
Comments

Add Comment..

Add

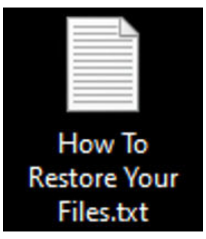
Babuk Overview

Babuk ransomware renames the encrypted files with .again in the extension:



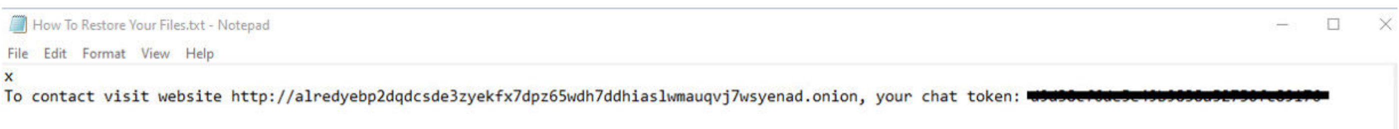
test_getargs2.py.again
test_getargs.py.again
test_genexps.py.again
test_genericpath.py.again
test_future4.py.again

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



How To Restore Your Files.txt

The ransom note contains only a tor website with a chat token to contact the attacker:



How To Restore Your Files.txt - Notepad

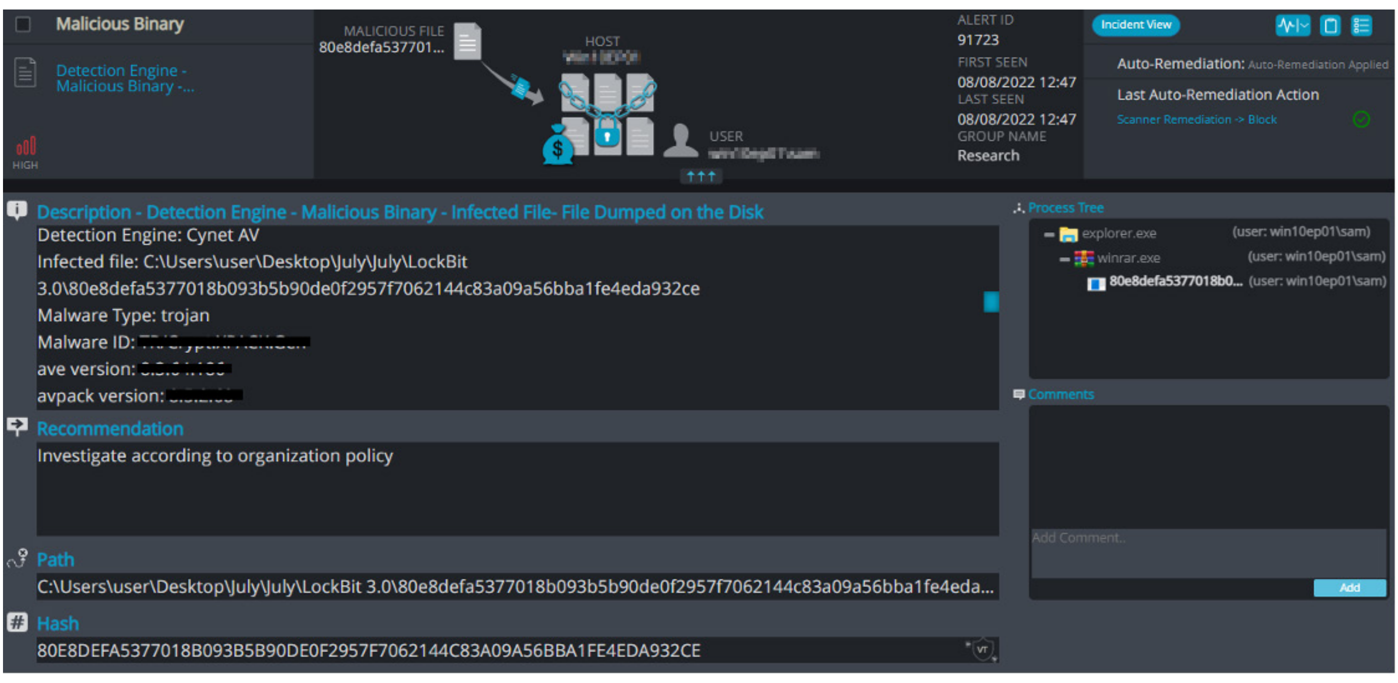
File Edit Format View Help

```
x
To contact visit website http://alredyebp2dqdcsde3zyekfx7dpz65wdh7ddhiaslwmauqvj7wsyenad.onion, your chat token: [redacted]
```

LockBit 3.0 Ransomware

- Observed since: Mid 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .[a-zA-Z0-9]{9}
- Ransomware note: [a-zA-Z0-9]{9}.readme.txt
- Sample hash: 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce

Cynet 360 AutoXDR™ Detections:



Malicious Binary
Detection Engine - Malicious Binary -...
HIGH
MALICIOUS FILE 80e8defa537701...
HOST [redacted]
USER [redacted]
ALERT ID 91723
FIRST SEEN 08/08/2022 12:47
LAST SEEN 08/08/2022 12:47
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\July\July\LockBit 3.0\80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce
Malware Type: trojan
Malware ID: [redacted]
ave version: [redacted]
avpack version: [redacted]

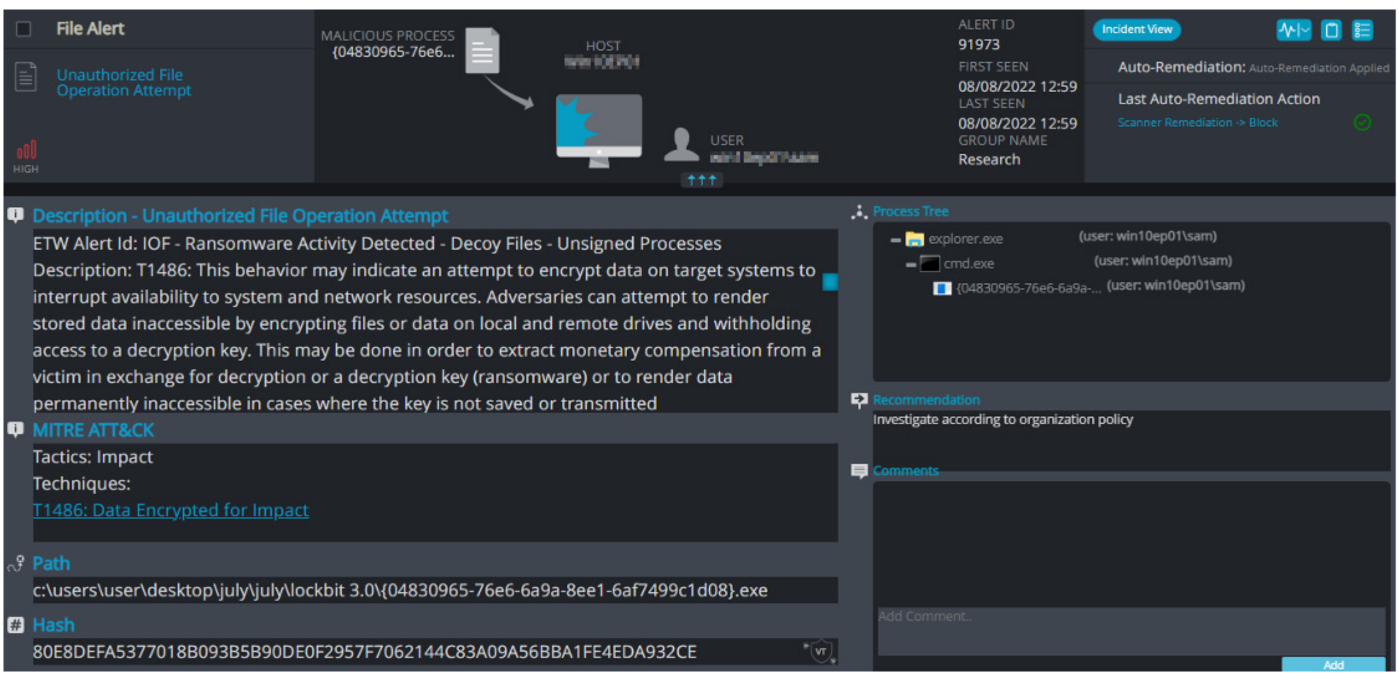
Recommendation
Investigate according to organization policy

Path
C:\Users\user\Desktop\July\July\LockBit 3.0\80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda...

Hash
80E8DEFA5377018B093B5B90DE0F2957F7062144C83A09A56BBA1FE4EDA932CE

Process Tree
- explorer.exe (user: win10ep01\sam)
  - winrar.exe (user: win10ep01\sam)
    - 80e8defa5377018b0... (user: win10ep01\sam)

Comments
Add Comment..
Add



File Alert
Unauthorized File Operation Attempt
HIGH
MALICIOUS PROCESS {04830965-76e6...
HOST [redacted]
USER [redacted]
ALERT ID 91973
FIRST SEEN 08/08/2022 12:59
LAST SEEN 08/08/2022 12:59
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

MITRE ATT&CK
Tactics: Impact
Techniques:
T1486: Data Encrypted for Impact

Path
c:\users\user\desktop\july\july\lockbit 3.0\{04830965-76e6-6a9a-8ee1-6af7499c1d08}.exe

Hash
80E8DEFA5377018B093B5B90DE0F2957F7062144C83A09A56BBA1FE4EDA932CE

Process Tree
- explorer.exe (user: win10ep01\sam)
  - cmd.exe (user: win10ep01\sam)
    - {04830965-76e6-6a9a-... (user: win10ep01\sam)

Recommendation
Investigate according to organization policy

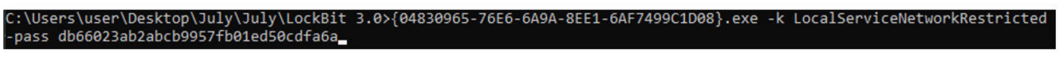
Comments
Add Comment..
Add

LockBit 3.0 Overview

LockBit 3.0 needs to execute by a specific method for it to work,

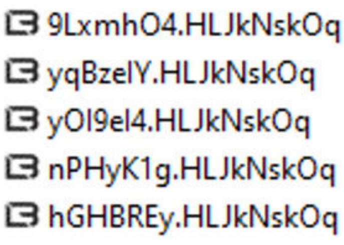
The executable needs to be renamed to “{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe” and needs to be executed with the following parameters:

“-k LocalServiceNetworkRestricted -pass db66023ab2abcb9957fb01ed50cdfa6a” via CMD or PowerShell:



```
C:\Users\user\Desktop\July\July\LockBit 3.0>{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe -k LocalServiceNetworkRestricted
-pass db66023ab2abcb9957fb01ed50cdfa6a_
```

LockBit 3.0 ransomware renames the encrypted files with .(9 characters) in the extension:

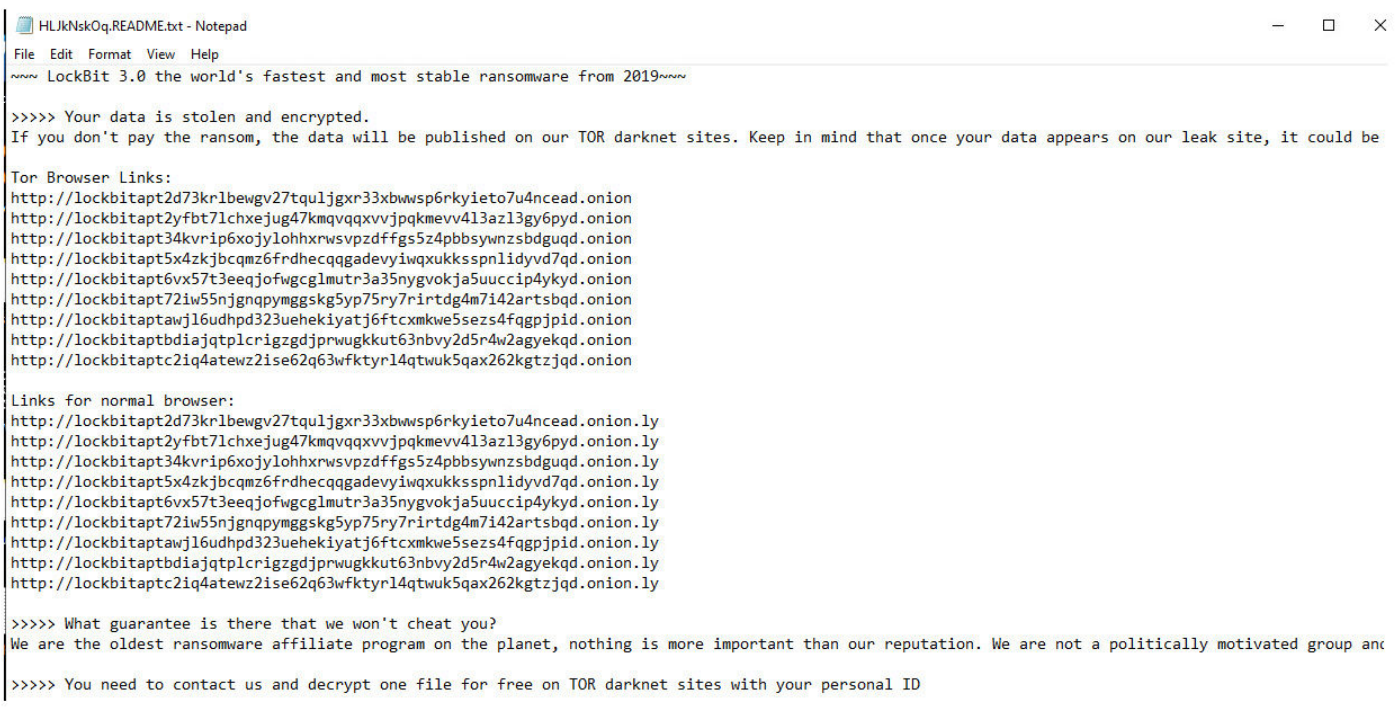


9LxmhO4.HLJkNskOq
yqBzelY.HLJkNskOq
yOl9el4.HLJkNskOq
nPHyK1g.HLJkNskOq
hGHBREy.HLJkNskOq

Once a computer’s files have been encrypted and renamed, it drops a note as (9 characters).readme.txt:

HLJkNskOq.R
EADME.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:

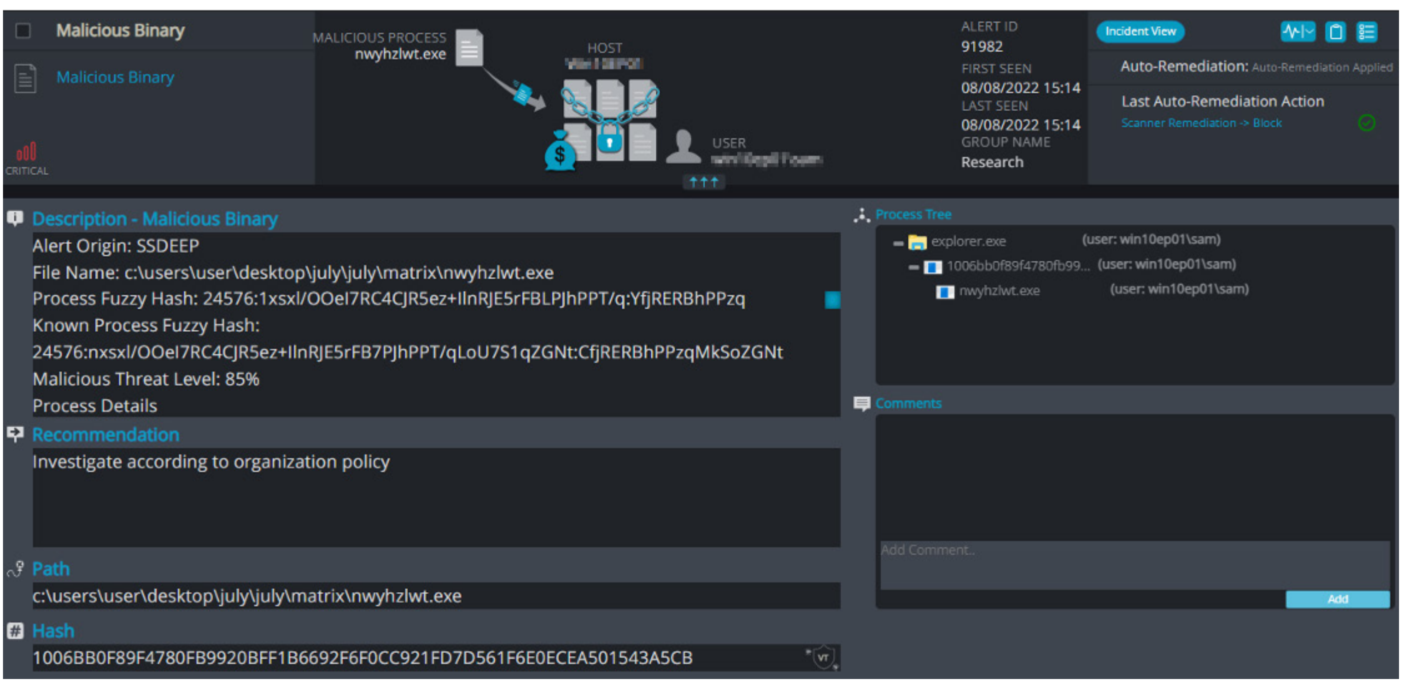


```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group anc

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID
```

Matrix Ransomware

- Observed since: Late 2016
- Ransomware encryption method: AES + RSA
- Ransomware extension: .KOK08
- Ransomware note: !README_KOK08!.rtf
- Sample hash: 1006bb0f89f4780fb9920bff1b6692f6f0cc921fd7d561f6e0ecea501543a5cb

Cynet 360 AutoXDR™ Detections:



Malicious Binary

Malicious Binary

CRITICAL

MALICIOUS PROCESS
nwyhzlwt.exe

HOST
[redacted]

USER
[redacted]

ALERT ID
91982
FIRST SEEN
08/08/2022 15:14
LAST SEEN
08/08/2022 15:14
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\july\july\matrix\nwyhzlwt.exe
Process Fuzzy Hash: 24576:1xsxl/OOeI7RC4CJR5ez+IlnRJE5rFBLPJhPPT/q:YfjRERBhPPzq
Known Process Fuzzy Hash:
24576:nxsxl/OOeI7RC4CJR5ez+IlnRJE5rFB7PJhPPT/qLoU7S1qZGNt:CfjRERBhPPzqMkSoZGNt
Malicious Threat Level: 85%
Process Details
```

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\july\july\matrix\nwyhzlwt.exe

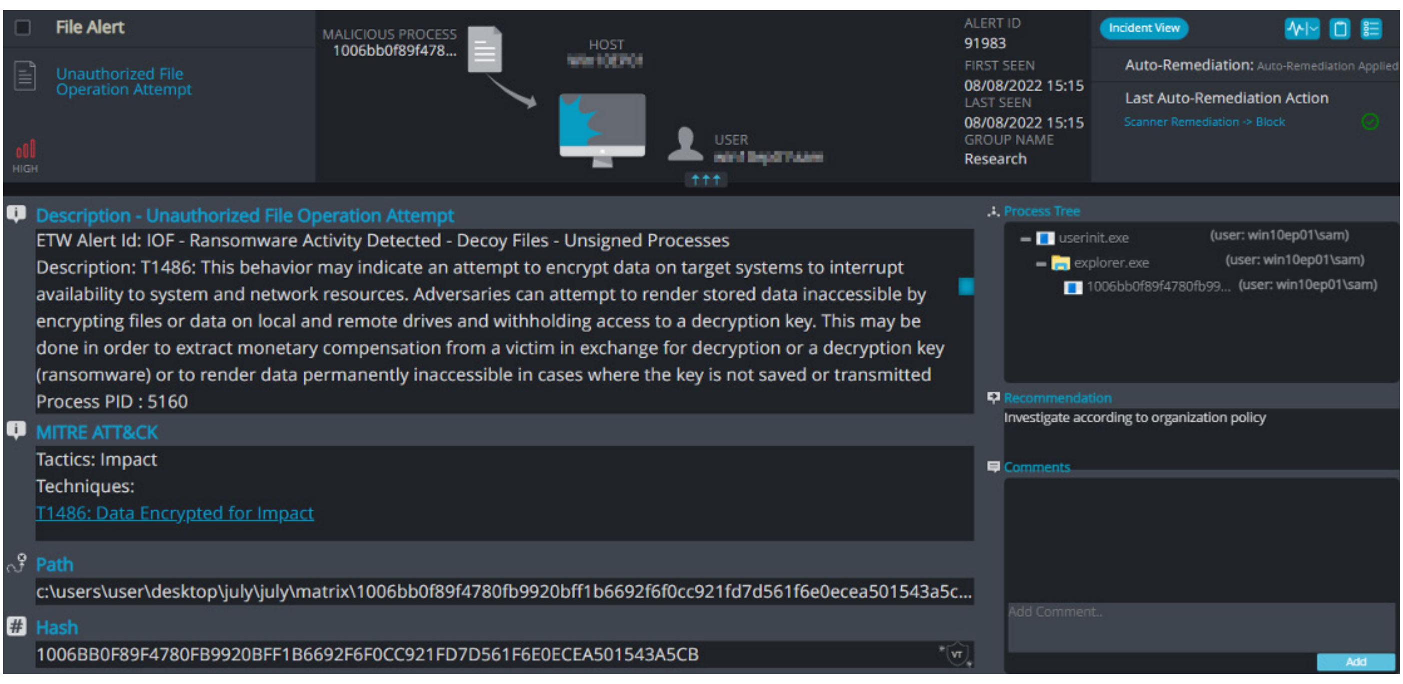
Hash

1006BB0F89F4780FB9920BFF1B6692F6F0CC921FD7D561F6E0ECEA501543A5CB

Process Tree

```
- explorer.exe                      (user: win10ep01\sam)
  - 1006bb0f89f4780fb99...          (user: win10ep01\sam)
      nwyhzlwt.exe                  (user: win10ep01\sam)
```

Comments



File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS
1006bb0f89f478...

HOST
[redacted]

USER
[redacted]

ALERT ID
91983
FIRST SEEN
08/08/2022 15:15
LAST SEEN
08/08/2022 15:15
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 : 5160

MITRE ATT&CK

Tactics: Impact
Techniques:
T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\july\july\matrix\1006bb0f89f4780fb9920bff1b6692f6f0cc921fd7d561f6e0ecea501543a5c...

Hash

1006BB0F89F4780FB9920BFF1B6692F6F0CC921FD7D561F6E0ECEA501543A5CB

Process Tree

```
- userinit.exe                      (user: win10ep01\sam)
  - explorer.exe                    (user: win10ep01\sam)
      1006bb0f89f4780fb99...        (user: win10ep01\sam)
```

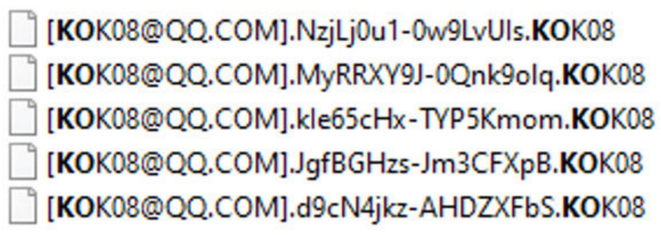
Recommendation

Investigate according to organization policy

Comments

Matrix Overview

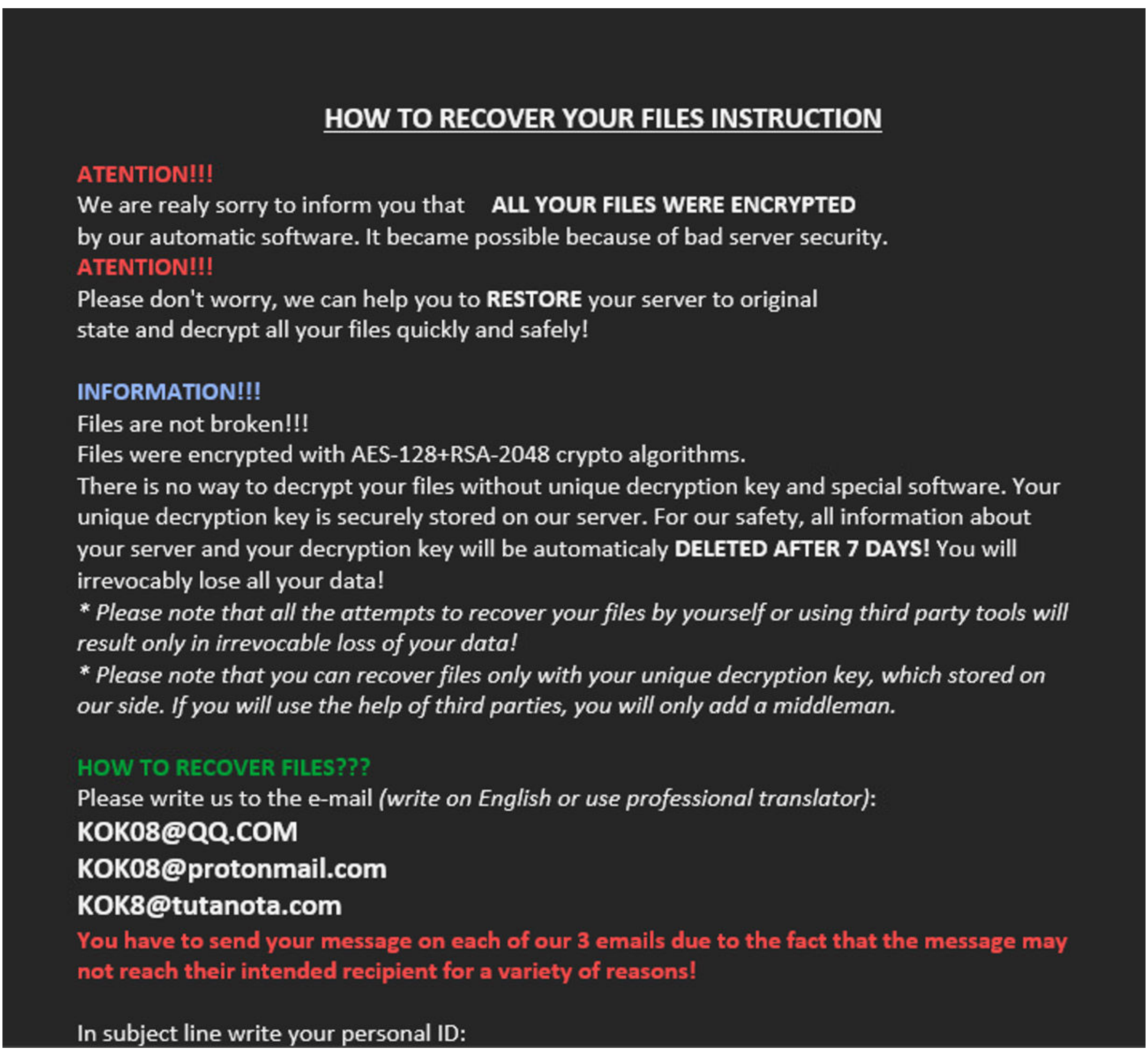
Matrix ransomware renames the encrypted files with .KOK08 in the extension:



[KOK08@QQ.COM].NzjLj0u1-0w9LvUls.KOK08
[KOK08@QQ.COM].MyRRXY9J-0Qnk9olq.KOK08
[KOK08@QQ.COM].kle65cHx-TYP5Kmom.KOK08
[KOK08@QQ.COM].JgfBGHzs-Jm3CFXpB.KOK08
[KOK08@QQ.COM].d9cN4jkz-AHDZXFbS.KOK08

Once a computer's files have been encrypted and renamed, it drops a note as !README_KOK08!.rtf:

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



HOW TO RECOVER YOUR FILES INSTRUCTION

ATENTION!!!
We are realy sorry to inform you that **ALL YOUR FILES WERE ENCRYPTED**
by our automatic software. It became possible because of bad server security.
ATENTION!!!
Please don't worry, we can help you to **RESTORE** your server to original
state and decrypt all your files quickly and safely!

INFORMATION!!!
Files are not broken!!!
Files were encrypted with AES-128+RSA-2048 crypto algorithms.
There is no way to decrypt your files without unique decryption key and special software. Your unique decryption key is securely stored on our server. For our safety, all information about your server and your decryption key will be automaticaly **DELETED AFTER 7 DAYS!** You will irrevocably lose all your data!
** Please note that all the attempts to recover your files by yourself or using third party tools will result only in irrevocable loss of your data!*
** Please note that you can recover files only with your unique decryption key, which stored on our side. If you will use the help of third parties, you will only add a middleman.*

HOW TO RECOVER FILES???
Please write us to the e-mail *(write on English or use professional translator)*:
KOK08@QQ.COM
KOK08@protonmail.com
KOK8@tutanota.com
You have to send your message on each of our 3 emails due to the fact that the message may not reach their intended recipient for a variety of reasons!

In subject line write your personal ID:

Thank you!

July, 2022