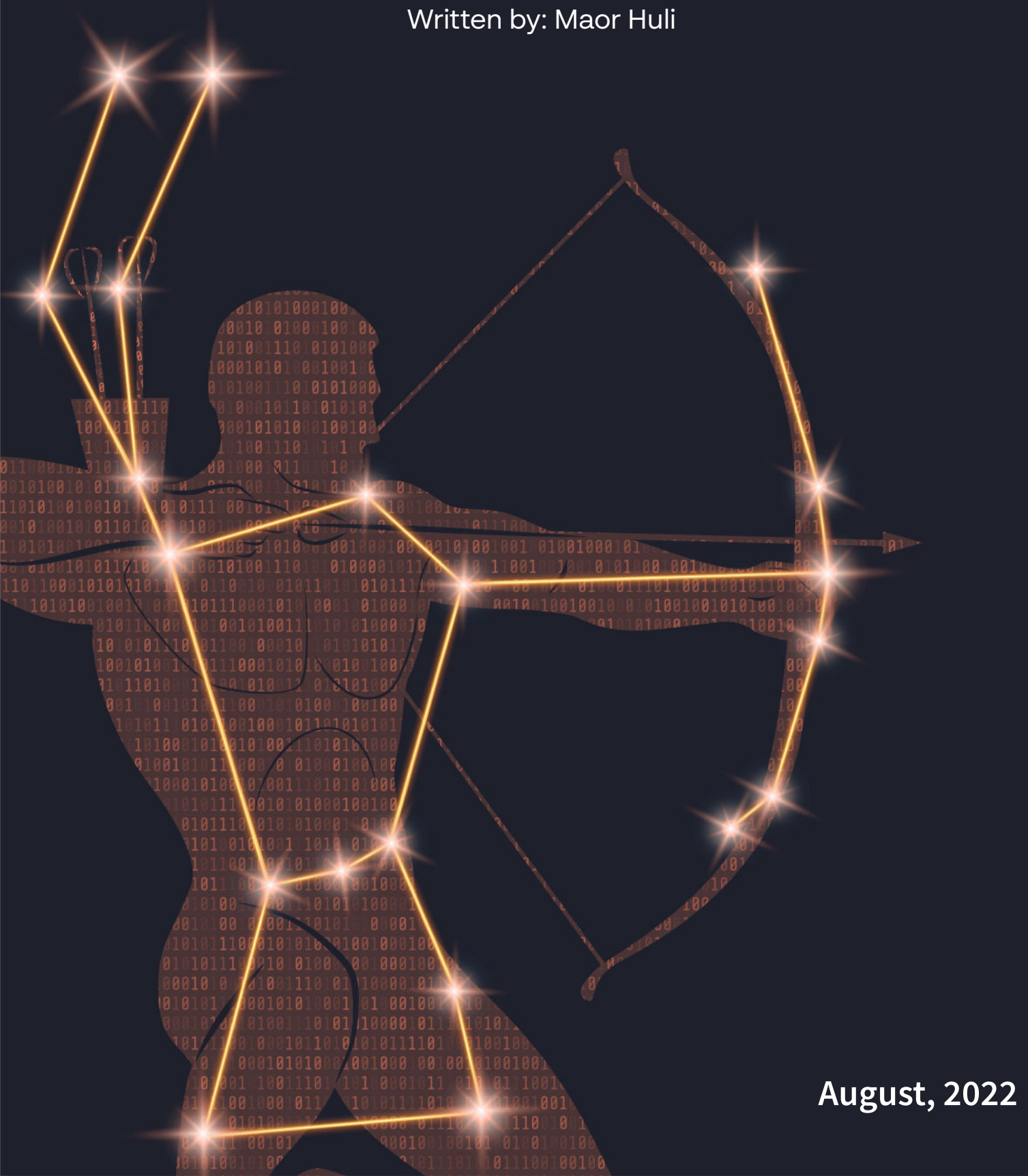


Orion Team

Monthly Ransomware Activity

Written by: Maor Huli



August, 2022



Contents

Payt	5
Hydrox	6
World2022decoding.....	7
Medusa	8
VoidCrypt	9



Executive Summary

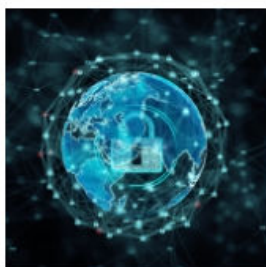
As an integral department of Cynet's research team, Orion works around the clock to track threat intelligence resources, analyze payloads and automate labs to protect customers against the newest ransomware variants. In these monthly reports, Orion reviews the latest trends identified in [Bleeping Computer](#) — the most up-to-date website that summarizes the newest ransomware variants — and shares how Cynet detects these threats.



The Week in Ransomware - August 26th 2022 - Fighting back

We saw a bit of ransomware drama this week, mostly centered around LockBit, who saw their data leak sites taken down by a DDoS attack after they started leaking the allegedly stolen Entrust data.

LAWRENCE ABRAMS AUGUST 26, 2022 04:32 PM 0



The Week in Ransomware - August 19th 2022 - Evolving extortion tactics

Bringing you the latest ransomware news, including new research, tactics, and cyberattacks. We also saw the return of the BlackByte ransomware operation, who has started to use new extortion tactics.

LAWRENCE ABRAMS AUGUST 19, 2022 07:08 PM 0



The Week in Ransomware - August 12th 2022 - Attacking the defenders

It was a very busy week for ransomware news and attacks, especially with the disclosure that Cisco was breached by a threat actor affiliated with the Yanluowang ransomware gang.

LAWRENCE ABRAMS AUGUST 12, 2022 07:19 PM 1



The Week in Ransomware - August 5th 2022 - A look at cyber insurance

For the most part, it has been a quiet week on the ransomware front, with a few new reports, product developments, and attacks revealed.

LAWRENCE ABRAMS AUGUST 05, 2022 05:35 PM 0

Orion Team



Cynet 360 AutoXDR™ VS Ransomware

Payt Ransomware

- Observed since: Aug 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .Payt
- Ransomware note: ReadthisforDecode.txt
- Sample hash: 3a3c882946ba931c47515463c64389df9d61a90c87d2a0d91ea9288175c7ff8e

Cynet 360 AutoXDR™ Detections:

Malicious Binary

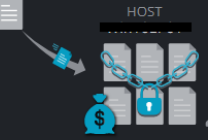
Detection Engine - Malicious Binary ...

HIGH

MALICIOUS FILE

3a3c882946ba93...

HOST



USER

www.user.sam

ALERT ID

99386

FIRST SEEN

09/07/2022 13:38

LAST SEEN

09/07/2022 13:38

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

Actual EPS Prevention: Nothing

Detection Time UTC: 2022-09-07 13:38:11

Detection Time Local: 2022-09-07 06:38:11

Detection Engine: Cynet AV

Infected file: C:\Users\user\Desktop\Aug Ransomware\Aug

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\Aug Ransomware\Aug Ransomware\Payt\3a3c882946ba931c47515463c64389df9d61a90c87d2a0d91ea9288175...

Hash

3A3C882946BA931C47515463C64389DF9D61A90C87D2A0D91EA9288175C7FF8E

Process Tree

explorer.exe

winrar.exe

3a3c882946ba931

Comments

Add Comment...

File Alert


Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

3a3c882946ba93...

HOST



USER

www.user.sam

ALERT ID

100116

FIRST SEEN

09/07/2022 14:03

LAST SEEN

09/07/2022 14:03

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 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\aug ransomware\aug ransomware\payt\3a3c882946ba931c47515463c64389df9d61a90c87d2a0d91ea9288175c7ff...

Process Tree

explorer.exe

winrar.exe

3a3c882946ba931

Comments

Add Comment...

Payt Overview

Payt ransomware renames the encrypted files with .Payt along with the attacker’s email and the host ID in the extension.

```
test_urllib2.py.[MJ-OK7283190645](wesleypeyt@tutanota.com).Payt
test_urllib.py.[MJ-OK7283190645](wesleypeyt@tutanota.com).Payt
test_unpack.py.[MJ-OK7283190645](wesleypeyt@tutanota.com).Payt
test_univnewlines2k.py.[MJ-OK7283190645](wesleypeyt@tutanota.com).Payt
test_univnewlines.py.[MJ-OK7283190645](wesleypeyt@tutanota.com).Payt
```

Once a computer’s files have been encrypted and renamed (in approximately 15 minutes), it drops a note as ReadthisforDecode.txt:



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

```
Your Files Are Has Been Locked

Your Files Has Been Encrypted with cryptography Algorithms

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-24n6t523 pr RSAKEY.KEY) to Make Sure Your Files Can be Re

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

Your Case ID :MJ-OK7283190645

OUR Email :wesleypeyt@tutanota.com

in Case of no answer: wesleypeyt@gmail.com
```

Hydrox Ransomware

- Observed since: Aug 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .hydrox
- Ransomware note: Hydrox Ransomware.txt
- Sample hash: 24d49f947f968c4f654ebfa2d4c0bdd3a8ddf45cfa909dc8b36b557724b14361

Cynet 360 AutoXDR™ Detections:

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

3a3c882946ba93...

HOST

USER

...sam

ALERT ID

100116

FIRST SEEN

09/07/2022 14:03

LAST SEEN

09/07/2022 14:03

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 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\aug ransomware\aug ransomware\payt\3a3c882946ba931c47515463c64389df9d61a90c87d2a0d91ea9288175c7ff...

Process Tree

explorer.exe

3a3c882946ba931c47515463c64389df9d61a90c87d2a0d91ea9288175c7ff...

Recommendation

Investigate according to organization policy

Comments

Add Comment...

Malicious Binary

Malicious Binary

CRITICAL

MALICIOUS PROCESS

setup.exe

HOST

USER

...sam

ALERT ID

100127

FIRST SEEN

09/07/2022 14:31

LAST SEEN

09/07/2022 14:31

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\appdata\roaming\setup.exe

Process Fuzzy Hash: 1536:wNHH0sq9jpnHJaYOnEKbgOr6uKjbZ00erwgf:m0sq9jpbOnz67G

Known Process Fuzzy Hash:

1536:wNHH0sq9jpnHJaYOnEKbgOr6uKjbZ00erwgf:m0sq9jpbOnz67G

Recommendation

Investigate according to organization policy

Path

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

Hash

24D49F947F968C4F654EBFA2D4C0BDD3A8DDF45CFA909DC8B36B557724B14361

Process Tree

explorer.exe (user: ...sam)

24d49f947f968c4f654ebfa2d4c0bdd3a8ddf45cfa909dc8b36b557724b14361 (user: ...sam)

setup.exe (user: ...sam)

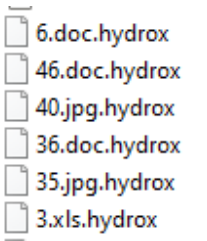
Comments

Add Comment...

Add

Hydrox Overview

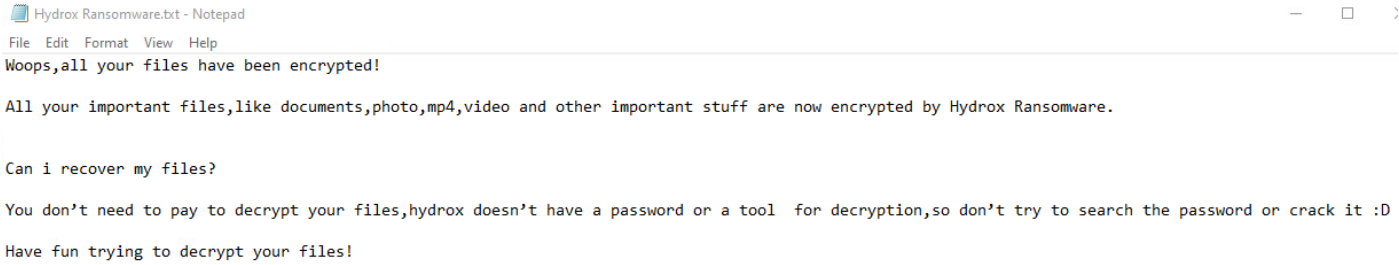
Hydrox ransomware renames the encrypted files with .hydrox in the extension:



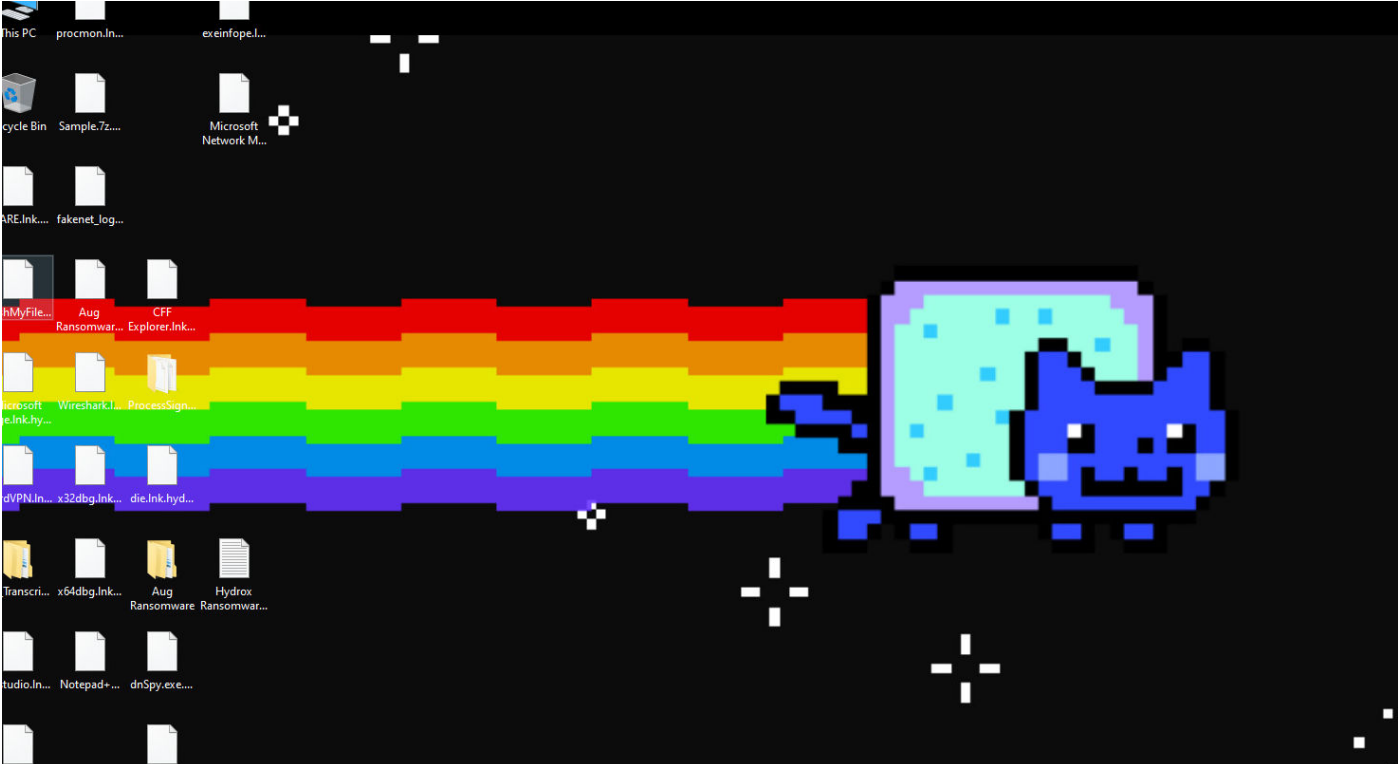
Once a computer’s files have been encrypted and renamed, it attempts to drop the ransomware note named Hydrox Ransomware:



Ransomware note contains general information, warnings and no option whatsoever to decrypt the files:



The ransomware also changes the desktop background:



World2022decoding Ransomware

- Observed since: Aug 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .world2022decoding
- Ransomware note: WE CAN RECOVER YOUR DATA.MHT
- Sample hash: 0737ddbd894f37316eee04c6739ac32f0c888535783a1af8c873023bcebbb8e8

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

Malicious File

0737ddbd894f37...

HOST

USER

...

isam

ALERT ID

100212

FIRST SEEN

09/07/2022 14:53

LAST SEEN

09/07/2022 14:53

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\Aug Ransomware\Aug Ransomware\World2022decoding\0737ddbd894f37316eee04c6739ac32f0c888535783a1af8c873023bcebbb8e8.exe

Malware Type: heuristic

Malware ID: ...

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\Aug Ransomware\Aug Ransomware\World2022decoding\0737ddbd894f37316eee04c6739ac32f0c888535783a1af8c873023bcebbb...

Hash

0737DDBD894F37316EEE04C6739AC32F0C888535783A1AF8C873023BCEBBB8E8

Malicious Binary

Threat Intelligence Detection Malicious...

Malicious Process

0737ddbd894f37...

HOST

USER

...

isam

ALERT ID

100211

FIRST SEEN

09/07/2022 14:53

LAST SEEN

09/07/2022 14:53

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Threat Intelligence Detection Malicious Binary

Process Details

Process SHA256: 0737DDBD894F37316EEE04C6739AC32F0C888535783A1AF8C873023BCEBBB8E8

Process PID: 5860

Process Path: c:\users\user\desktop\0737ddbd894f37316eee04c6739ac32f0c888535783a1af8c873023bcebbb8e...

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\0737ddbd894f37316eee04c6739ac32f0c888535783a1af8c873023bcebbb8e...

Hash

0737DDBD894F37316EEE04C6739AC32F0C888535783A1AF8C873023BCEBBB8E8

Process Tree

Not Available

Comments


Add Comment...

Add

World2022decoding Overview

World2022decoding ransomware renames the encrypted files with .world2022decoding in the extension. Once a computer’s files have been encrypted and renamed, it drops a note named: WE CAN RECOVER YOUR DATA.MHT

Note: the ransomware was unable to encrypt the host and collapsed the machine. Therefore, no encryption was detected.

cynet

©ALL RIGHTS RESERVED TO CYNET 2022 WWW.CYNET.COM

Monthly Ransomware Activity – August 2022 7

Medusa Locker Ransomware

- Observed since: 2019
- Ransomware encryption method: AES + RSA
- Ransomware extension: .readlockfiles
- Ransomware note: HOW_TO_RECOVER_DATA.html
- Sample hash: e9df1201269429887bac3d2ae4069b7ac718306316853d2b3c7b2f4d4e92e09a

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary ~...

HIGH

MALICIOUS FILE

e9df1201269429...

HOST

USER

ALERT ID

101580

FIRST SEEN

09/19/2022 14:28

LAST SEEN

09/19/2022 15:23

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Rena...

Description - Detection Engine - Malicious Binary - Infected File- File Dumped on the Disk

Detection Engine: Cynet AV

Infected file: C:\Users\user\Desktop\Aug Ransomware\Aug Ransomware\Medusa Locker\e9df1201269429887bac3d2ae4069b7ac718306316853d2b3c7b2f4d4e92e09a

Malware Type: heuristic

Malware ID: [REDACTED]

ave version: [REDACTED]

avpack version: [REDACTED]

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\Aug Ransomware\Aug Ransomware\Medusa Locker\e9df1201269429887bac3d2ae4069b7ac718306316853d2b3c7b2f4d4e...

Hash

E9DF1201269429887BAC3D2AE4069B7AC718306316853D2B3C7B2F4D4E92E09A

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

e9df1201269429...

HOST

USER

ALERT ID

101921

FIRST SEEN

09/19/2022 15:34

LAST SEEN

09/19/2022 15:34

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Rena...

Description - Unauthorized File Operation Attempt

ETW Alert Id: IOF - Ransomware Extension Found

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 : 9472

MITRE ATT&CK

Tactics: Impact

Techniques:

T1486: Data Encrypted for Impact

Path

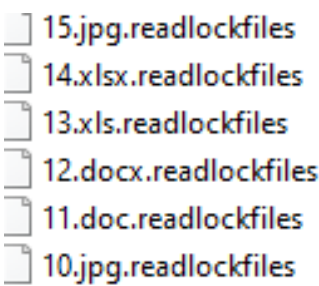
c:\users\user\desktop\aug ransomware\aug ransomware\medusa locker\e9df1201269429887bac3d2ae4069b7ac718306316853d2b3c7b2f4d4e92e0...

Hash

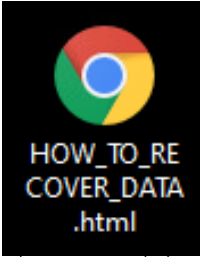
E9DF1201269429887BAC3D2AE4069B7AC718306316853D2B3C7B2F4D4E92E09A

Medusa Locker Overview

Medusa Locker ransomware renames the encrypted files with .readlockfiles in the extension:



Once a computer’s files have been encrypted and renamed, it drops a note as: HOW_TO_RECOVER_DATA.html



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

YOUR PERSONAL ID:

[REDACTED]

/! YOUR COMPANY NETWORK HAS BEEN PENETRATED !/
All your important files have been encrypted!

Your files are safe! Only modified. (RSA+AES)

ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE WILL PERMANENTLY CORRUPT IT.
DO NOT MODIFY ENCRYPTED FILES.
DO NOT RENAME ENCRYPTED FILES.

No software available on internet can help you. We are the only ones able to solve your problem.

We gathered highly confidential personal data. These data are currently stored on a private server. This server will be immediately destroyed after your payment.
If you decide to not pay, we will release your data to public or re-seller.
So you can expect your data to be publicly available in the near future..

We only seek money and our goal is not to damage your reputation or prevent your business from running.

You will can send us 2-3 non-important files and we will decrypt it for free to prove we are able to give your files back.

Contact us for price and get decryption software.

.onion

* Note that this server is available via Tor browser only:

Follow the instructions to open the link:
1. Type the address "https://www.torproject.org" in your Internet browser. It opens the Tor site.
2. Press "Download Tor", then press "Download Tor Browser Bundle", install and run it.
3. Now you have Tor browser. In the Tor Browser open .onion
4. Start a chat and follow the further instructions.

If you can not use the above link, use the email:
internationalassistance@tutanota.com
reasonablehelp@outlook.com

* To contact us, create a new free email account on the site: protonmail.com

©ALL RIGHTS RESERVED TO CYNET 2022 WWW.CYNET.COM

Monthly Ransomware Activity – August 2022 8

VoidCrypt Ransomware

- Observed since: 2020
- Ransomware encryption method: AES + RSA
- Ransomware extension: .dark
- Ransomware note: unlock-info.txt
- Sample hash: 50586ef722c6a5c7b28d7b348dcf7003ea458bb1c3e659ddfb182be735daeb3d

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary -...

HIGH

MALICIOUS FILE

50586ef722c6a5...

HOST

USER

ALERT ID

101582

FIRST SEEN

09/19/2022 14:28

LAST SEEN

09/19/2022 15:44

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Rena...

Description - Detection Engine - Malicious Binary - Infected File- File Dumped on the Disk

Detection Engine: Cynet AV

Infected file: C:\Users\user\Desktop\Aug Ransomware\Aug Ransomware\VoidCrypt\50586ef722c6a5c7b28d7b348dcf7003ea458bb1c3e659ddfb182be735daeb3d

Malware Type: heuristic

Malware ID:

ave version:

avpack version:

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\Aug Ransomware\Aug Ransomware\VoidCrypt\50586ef722c6a5c7b28d7b348dcf7003ea458bb1c3e659ddfb182be735d...

Hash

50586EF722C6A5C7B28D7B348DCF7003EA458BB1C3E659DDFB182BE735DAEB3D

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

50586ef722c6a5...

HOST

USER

ALERT ID

102421

FIRST SEEN

09/19/2022 15:52

LAST SEEN

09/19/2022 15:52

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Rena...

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 : 10192

MITRE ATT&CK

Tactics: Impact

Techniques: T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\aug ransomware\aug ransomware\voidcrypt\50586ef722c6a5c7b28d7b348dcf7003ea458bb1c3e659ddfb182be735daeb...

Hash

50586EF722C6A5C7B28D7B348DCF7003EA458BB1C3E659DDFB182BE735DAEB3D

VoidCrypt Overview

VoidCrypt ransomware renames the encrypted files with .dark in the extension:

- 50.jpg.(CW-KY3246958071)(Darksight@tutanota.com).dark
- 49.xlsx.(CW-KY3246958071)(Darksight@tutanota.com).dark
- 48.xls.(CW-KY3246958071)(Darksight@tutanota.com).dark
- 47.docx.(CW-KY3246958071)(Darksight@tutanota.com).dark
- 46.doc.(CW-KY3246958071)(Darksight@tutanota.com).dark
- 45.jpg.(CW-KY3246958071)(Darksight@tutanota.com).dark
- 44.xlsx.(CW-KY3246958071)(Darksight@tutanota.com).dark

Once a computer’s files have been encrypted and renamed, it drops a note as unlock-info.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:

unlock-info.txt - Notepad

File Edit Format View Help

all your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail; Darksight@tutanota.com
Write this ID in the title of your message : -
In case of no answer in 24 hours write us to these e-mails: darksight@mailfence.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
hxxps://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
hxxp://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Thank you!



August, 2022