

Orion Team

Monthly Ransomware Activity

Written by: Maor Huli



June, 2022



Contents

Executive Summary	3
MoonShadow	5
Phobos	6
Linda	7
Sheeva	8
Ritzer	9



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 indentified 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 - June 24th 2022 - Splinter Cells

The Conti ransomware gang has finally ended their charade and turned off their Tor data leak and negotiation sites, effectively shutting down the operation.

LAWRENCE ABRAMS JUNE 24, 2022 06:20 PM 0



The Week in Ransomware - June 17th 2022 - Have I Been Ransomed?

Ransomware operations are constantly evolving their tactics to pressure victims to pay. For example, this week, we saw a new extortion tactic come into play with the creation of dedicated websites to extort victims with searchable data.

LAWRENCE ABRAMS JUNE 17, 2022 05:11 PM 0



The Week in Ransomware - June 10th 2022 - Targeting Linux

It has been relatively quiet this week with many companies and researchers at the RSA conference. However, we still had some interesting ransomware reports released this week.

LAWRENCE ABRAMS JUNE 10, 2022 06:18 PM 1



The Week in Ransomware - June 3rd 2022 - Evading sanctions

Ransomware gangs continue to evolve their operations as victims refuse to pay ransoms due to sanctions or other reasons.

LAWRENCE ABRAMS JUNE 03, 2022 04:41 PM 0

Orion Team



Cynet 360 AutoXDR™ VS Ransomware





MoonShadow Ransomware

- Observed since: June 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .moonshadow
- Ransomware note: Decryption-Guide.txt | .hta
- Sample hash: ac2d92c801261e1887ad6a9dbbf52e08d9e3193976de096fb361597736a8c1ac

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary ~...

MALICIOUS FILE

ac2d92c801261e...

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

82141

FIRST SEEN

07/03/2022 12:43

LAST SEEN

07/03/2022 12:43

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\June\June\MoonShadow\ac2d92c801261e1887ad6a9dbbf52e08d9e3193976de096fb361597736a8c1ac.exe

Malware Type: heuristic

Malware ID: HEUR/AGEN.1223866

ave version: 2022-07-03

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\June\June\MoonShadow\ac2d92c801261e1887ad6a9dbbf52e08d9e319...

Hash

AC2D92C801261E1887AD6A9DBBF52E08D9E3193976DE096FB361597736A8C1AC

Process Tree

explorer.exe

(user: win10ep01\sam)

ac2d92c801261e1887a...

(user: win10ep01\sam)

Comments

Add Comment...

Add

File Alert

Unauthorized File Operation Attempt

MALICIOUS PROCESS

ac2d92c801261e...

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

82562

FIRST SEEN

07/03/2022 12:48

LAST SEEN

07/03/2022 12:48

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 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

MITRE ATT&CK

Tactics: Impact

Techniques: T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\june\june\moonshadow\ac2d92c801261e1887ad6a9dbbf52e08d9e3193...

Hash

AC2D92C801261E1887AD6A9DBBF52E08D9E3193976DE096FB361597736A8C1AC

Process Tree

explorer.exe

(user: win10ep01\sam)

ac2d92c801261e1887a...

(user: win10ep01\sam)

Recommendation

Investigate according to organization policy

Comments

Add Comment...

Add

MoonShadow Overview

MoonShadow ransomware is supposed to rename the encrypted files with .moonshadow in the extension.

- 1 Dawson_Creek.(MJ-HD8542376091)(developer.110@tutanota.com).moonshadow
- 2 Dawson.(MJ-HD8542376091)(developer.110@tutanota.com).moonshadow
- 3 Danmarkshavn.(MJ-HD8542376091)(developer.110@tutanota.com).moonshadow
- 4 Curacao.(MJ-HD8542376091)(developer.110@tutanota.com).moonshadow

Once a computer’s files have been encrypted and renamed, it drops a note as Decryption-Guide.HTA|.txt:



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

Your Files Are Locked

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 : KEY-SE-24r6t523 or RSAKEY.KEY) to Make Sure Your Files Can be Restored

Make an Agreement on Price with me and Pay

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

4-Do Not Always Trust to Middle mans and negotiators (some of them are good but some of them agree on 4000usd for example and Asked 10000usd From Client) this Was happened

Your Case ID : MJ-HD8542376091

Our Email:developer.110@tutanota.com

ACCESS DENIED

Decryption-Guide.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 Make Sure Your Files Can be Re

Make an Agreement on Price with me and Pay

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

4-Do Not Always Trust to Middle mans and negotiators (some of them are good but some of them agree on 4000usd for example and Asked 10000usd From Client)

Your Case ID :MJ-HD8542376091

OUR Email :developer.110@tutanota.com

- Observed since: late 2017
- Ransomware encryption method: AES
- Ransomware extension: .decrypt
- Ransomware note: info.txt
- Sample hash: e63bfc04792f9f4b921ef182b83f03a5212f061a7c7d8cfe3c51f4fbc0032cba

Ransomwareware

Memory Pattern - Ransomware - BTCWare v7

CRITICAL

MALICIOUS PROCESS
mshta.exe

HOST
Win10EP01

USER
win10ep01\sam

Alert ID
82867

FIRST SEEN
07/03/2022 13:14

LAST SEEN
07/03/2022 13:14

GROUP NAME
Research

Description - Memory Pattern - Ransomware - BTCWare v7

- Signature Name: Memory Pattern - Ransomware - BTCWare v7
- Matched Memory Area Bounds : From - 0x2c40000 - To - 0x2d3f000 - Area Size - 1044480
- Matched Memory Area Info : Type - PRIVATE, AllocationBase - 0xc240000, AllocationProtect - RW, Protect - RW
- Pattern(1) Offset [Address]: 293473 [0x2c87a61]
- Pattern(1) Distance From Previous Pattern Start: 293473

Recommendation

Investigate according to organization policy

Path

c:\windows\systemow64\mshta.exe

Hash

4B82CFC44029D3D8462D60322FA0DBDE20F36C9C6791FA6F9B9F6A96FE44BF09

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action
Scanner Remediation -> Block

Process Tree

```

graph TD
    A[e63bfc04792f9f4b921... (user: win10ep01\sam)] --> B[e63bfc04792f9f4b921... (user: win10ep01\sam)]
    B --> C[mshta.exe (user: win10ep01\sam)]
        
```


Comments

Add Comment..

Add

Phobos Overview

```
tutor.ru.utf-8.id[E07BA3DD-3349].[johnhelper@gmx.de].decrypt
tutor.ru.id[E07BA3DD-3349].[johnhelper@gmx.de].decrypt
tutor.ru.cp1251.id[E07BA3DD-3349].[johnhelper@gmx.de].decrypt
tutor.pt.utf-8.id[E07BA3DD-3349].[johnhelper@gmx.de].decrypt
tutor.pt.id[E07BA3DD-3349].[johnhelper@gmx.de].decrypt
```



info.txt

encrypted

!!!All of your files are encrypted and downloaded files!!!

All your files (contacts, clients, accounting, sql, base, payments and other documents with share) are downloaded to our servers, if you do not make contact, they will be distributed to the public and local media will also be informed. If

you want to restore them, write us to the e-mail: johnhelper@gmx.de

Write this ID in the title of your message: E07BA3DD-3349

Our online operator is available in the messenger Telegram: [@restoredata77](#)

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 tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 4Mb (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.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

<http://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.

Linda Ransomware

- Observed since: June 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .linda
- Ransomware note: linfo.hta
- Sample hash: 307e8a3de3047022e27b1178e04f2ffce51a2c5a89767290e7326281bbba71e6

Cynet 360 AutoXDR™ Detections:

Malicious Binary

307e8a3de30470...

HOST Win10EP01

USER win10ep01\sam

ALERT ID 82875

FIRST SEEN 07/03/2022 13:27

LAST SEEN 07/03/2022 13:27

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\307e8a3de3047022e27b1178e04f2ffce51a2c5a89767290e7326281bbba71e6.exe
- Malware Type: heuristic
- Malware ID: HEUR/AGEN.1223862
- ave version: 1.0.0.0

Recommendation Investigate according to organization policy

Path C:\Users\user\Desktop\307e8a3de3047022e27b1178e04f2ffce51a2c5a89767290e7326281bbba71e6.exe

Hash 307E8A3DE3047022E27B1178E04F2FFCE51A2C5A89767290E7326281BBBA71E6

Process Tree

explorer.exe (user: win10ep01\sam)

307e8a3de3047022e27b1178e04f2ffce51a2c5a89767290e7326281bbba71e6.exe (user: win10ep01\sam)

Comments

Add Comment...

Add

Malicious Binary

307e8a3de30470...

HOST Win10EP01

USER win10ep01\sam

ALERT ID 82876

FIRST SEEN 07/03/2022 13:27

LAST SEEN 07/03/2022 13:27

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\june\june\linda\307e8a3de3047022e27b1178e04f2ffce51a2c5a89767290e7326281bbba71e6.exe
- Process Fuzzy Hash: 24576:bVixzMTfNIbZ91iI/GhHE5UEL9v9Tju4BAkeOdb+AYBPTBuoZIP6QNEY:GxWfiWG W5UKg1FFB6uH

Recommendation Investigate according to organization policy

Path c:\users\user\desktop\june\june\linda\307e8a3de3047022e27b1178e04f2ffce51a2c5a89767290e7326281bbba71e6.exe

Hash 307E8A3DE3047022E27B1178E04F2FFCE51A2C5A89767290E7326281BBBA71E6

Process Tree

explorer.exe (user: win10ep01\sam)

307e8a3de3047022e27b1178e04f2ffce51a2c5a89767290e7326281bbba71e6.exe (user: win10ep01\sam)

Comments

Add Comment...

Add

Linda Overview

Linda ransomware renames the encrypted files with .linda in the extension:

- ✖ xorbrute.exe.[xxdecryptxx@cock.li][UIH02W76CRBLQ8M].linda
- ✖ unsupported_filters.vbs.[xxdecryptxx@cock.li][UIH02W76CRBLQ8M].linda
- ✖ string_scan.vbs.[xxdecryptxx@cock.li][UIH02W76CRBLQ8M].linda
- ✖ README.txt.[xxdecryptxx@cock.li][UIH02W76CRBLQ8M].linda
- ✖ pdfbox_extract_text_page_by_page.vbs.[xxdecryptxx@cock.li][UIH02W76CRBLQ8M].linda
- ✖ pdfbox_extract.vbs.[xxdecryptxx@cock.li][UIH02W76CRBLQ8M].linda
- ✖ obfuscated_headers.vbs.[xxdecryptxx@cock.li][UIH02W76CRBLQ8M].linda

Once a computer’s files have been encrypted and renamed, it drops a note named !INFO.HTA:



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





Sheeva Ransomware

- Observed since: June 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .sheeva
- Ransomware note: sheeva.txt
- Sample hash: 991d018090cfd0b39d562010abf24b169ed55bea2d1bfc3044622e2ade3827d7

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

MALICIOUS FILE

991d018090cfd0...

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

83806

FIRST SEEN

07/05/2022 12:53

LAST SEEN

07/05/2022 12:53

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Rena...

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

Detection Engine: Cynet AV

Infected file: C:\Users\user\Desktop\June\June\Ritzer\991d018090cfd0b39d562010abf24b169ed55bea2d1bfc3044622e2ade3827d7.exe

Malware Type: trojan

Malware ID: TR/Ransom.njyif

ave version: ...

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\June\June\Ritzer\991d018090cfd0b39d562010abf24b169ed55bea2d1bf...

Hash

991D018090CFD0B39D562010ABF24B169ED55BEA2D1BFC3044622E2ADE3827D7

Process Tree

explorer.exe (user: win10ep01\sam)

991d018090cfd0b39d... (user: win10ep01\sam)

Comments

Add Comment...

Add

File Alert

Unauthorized File Operation Attempt

MALICIOUS PROCESS

991d018090cfd0...

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

83794

FIRST SEEN

07/05/2022 11:54

LAST SEEN

07/05/2022 11:54

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 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

MITRE ATT&CK

Tactics: Impact

Techniques: T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\june\june\sheeva\991d018090cfd0b39d562010abf24b169ed55bea2d1b...

Hash

991D018090CFD0B39D562010ABF24B169ED55BEA2D1BFC3044622E2ADE3827D7

Process Tree

userinit.exe (user: win10ep01\sam)

explorer.exe (user: win10ep01\sam)

991d018090cfd0b39d... (user: win10ep01\sam)

Recommendation

Investigate according to organization policy

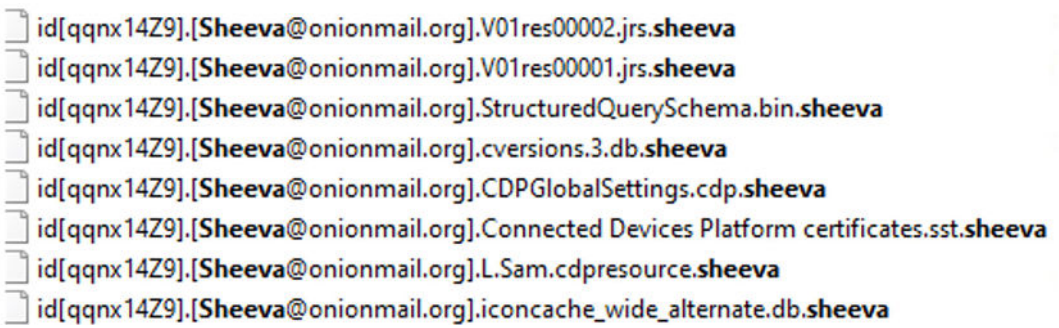
Comments

Add Comment...

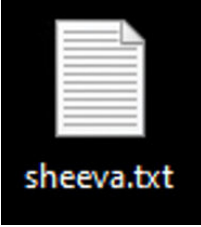
Add

Sheeva Overview

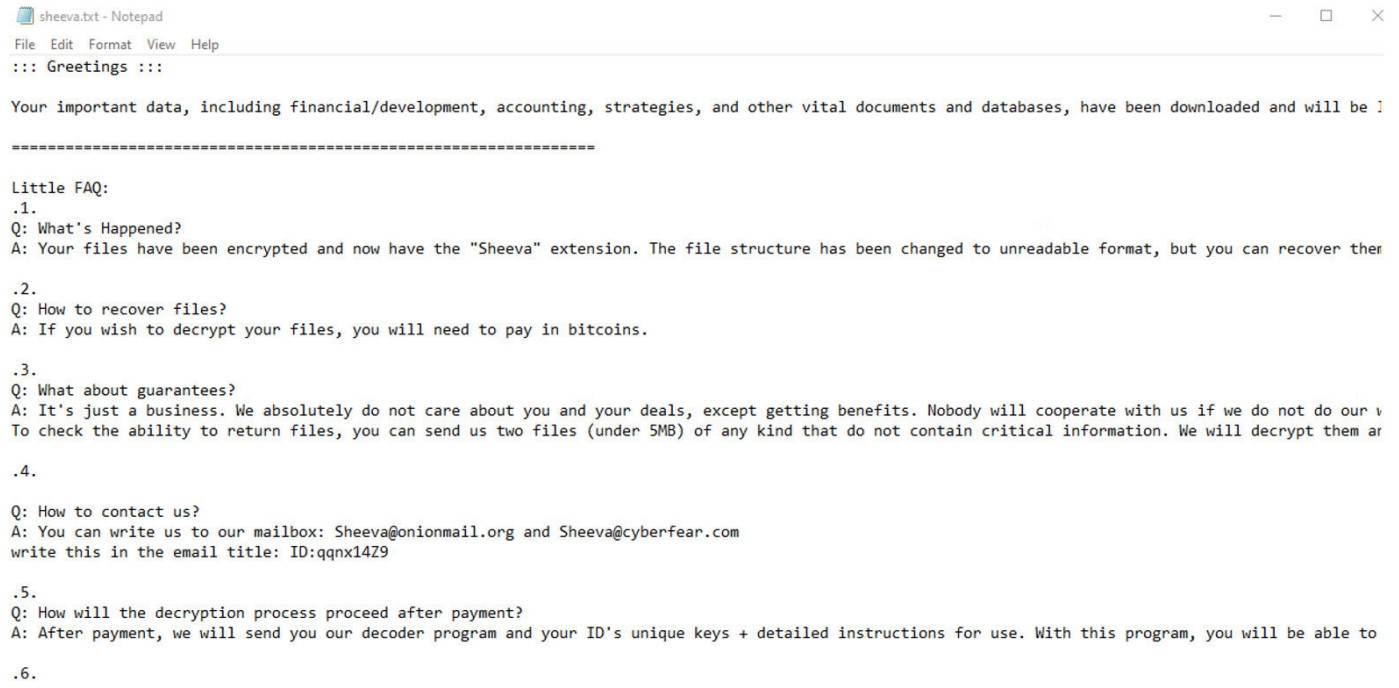
Sheeva ransomware renames the encrypted files with .sheeva in the extension:



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



Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker’s contact info:



Ritzer Ransomware

- Observed since: June 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .ritzer
- Ransomware note: read_it.txt
- Sample hash: fe5b33909638954acc556be872ee86f0e2a926f96ead41392923d31e9221ff10

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Threat Intelligence Detection Malicious...

MALICIOUS PROCESS

fe5b3390963895...

HOST

Win10EP01

ALERT ID

83809

FIRST SEEN

07/05/2022 12:59

LAST SEEN

07/05/2022 12:59

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Threat Intelligence Detection Malicious Binary

Extra Info

Created File Path:

c:\users\user\desktop\fe5b33909638954acc556be872ee86f0e2a926f96ead41392923d31e9221ff10\fe5b33909638954acc556be872ee86f0e2a926f96ead41392923d31e9221ff10.exe

Created File Attribute:

32

Created File Creation Time:

2022-07-05 05:59:31

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\fe5b33909638954acc556be872ee86f0e2a926f96ead41392923d31e9221...

Hash

FE5B33909638954ACC556BE872EE86F0E2A926F96EAD41392923D31E9221FF10

Process Tree

Not Available

Comments

Add Comment..

Add

File Alert

Process Monitoring

MALICIOUS PROCESS

vssadmin.exe

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

77716

FIRST SEEN

06/14/2022 12:34

LAST SEEN

07/05/2022 13:02

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Process Monitoring

Detection Time Local:

2022-07-05 06:02:42

Alert Origin:

DRIVER

ETW Alert Id:

CyAlert Heuristic Activity - Volume Shadow Copy Deletion

Description:

T1490: This behavior may indicate that an attempt was made to delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery

Process PID :

8916

Process Path :

c:\windows\system32\vssadmin.exe

MITRE ATT&CK

Tactics:

Impact

Techniques:

[T1490: Inhibit System Recovery](#)

Path

c:\windows\system32\vssadmin.exe

Hash

ACDCC96D628EE8FF7F07FC5D795A05C22EB239BE0D44A9F01727B6124A9619A9

Process Tree

svchost.exe (user: win10ep01\sam)

cmd.exe (user: win10ep01\sam)

vssadmin.exe (user: win10ep01\sam)

Recommendation

Investigate according to organization policy

Comments

Add Comment..

Add

Ritzer Overview

Ritzer ransomware renames the encrypted files with .ritzer in the extension:

- class_weight.py.ritzer
- test_helper.py.ritzer
- sax.py.ritzer
- sanitizer.py.ritzer
- pdist-seuclidean-ml-iris.txt.ritzer
- pdist-minkowski-3.2-ml-iris.txt.ritzer

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



Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker’s contact information:

read_it.txt - Notepad

File Edit Format View Help

Don't worry, you can return all your files!

All your files like documents, photos, databases and other important are encrypted

What guarantees do we give to you?

You can send 3 of your encrypted files and we decrypt it for free.

You must follow these steps To decrypt your files :

1) Write on our e-mail apivovarov453@protonmail.com(In case of no answer in 24 hours check your spam folder or write us to this e-mail: apivovarov453@protonmail.com)

2) Obtain Bitcoin (You have to pay for decryption in Bitcoins. After payment we will send you the tool that will decrypt all your files.)

Thank you!



June, 2022