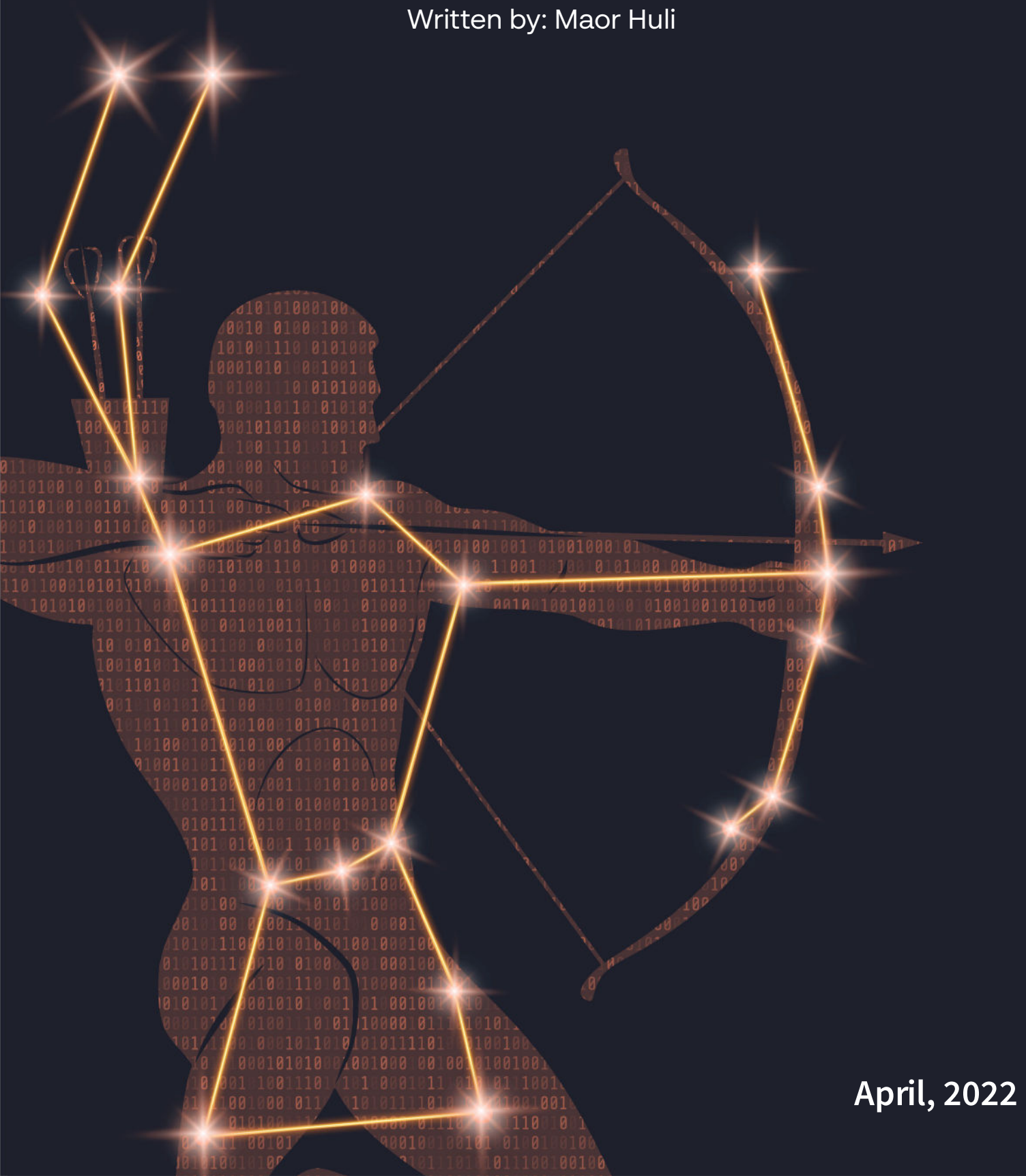


Orion Team

Monthly Ransomware Activity

Written by: Maor Huli



April, 2022



Contents

Executive Summary	3
Axxes	5
Blaze	6
BlockZ	7
DemocracyWhisperers	8
Medusa	9
Snatch	10
Parker	11



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 - April 29th 2022 - New operations emerge

This week we have discovered numerous new ransomware operations that have begun operating, with one appearing to be a rebrand of previous operations.

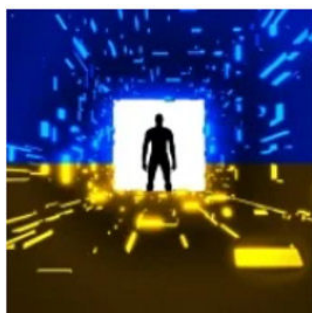
LAWRENCE ABRAMS APRIL 29, 2022 06:29 PM 0



The Week in Ransomware - April 15th 2022 - Encrypting Russia

While countries worldwide have been the frequent target of ransomware attacks, Russia and CIS countries have been avoided by threat actors. The tables have turned with the NB65 hacking group modifying the leaked Conti ransomware to use in attacks on Russian entities.

LAWRENCE ABRAMS APRIL 15, 2022 05:19 PM 0



The Week in Ransomware - April 1st 2022 - 'I can fight with a keyboard'

While ransomware is still conducting attacks and all companies must stay alert, ransomware news has been relatively slow this week. However, there were still some interesting stories that we outline below.

LAWRENCE ABRAMS APRIL 01, 2022 07:07 PM 0

Orion Team



Cynet 360 AutoXDR™ VS Ransomware



Axxes Ransomware

- Observed since: April 2022
- Ransomware encryption method: RSA + AES.
- Ransomware extension: .axxes
- Ransomware note: RESTORE_FILES_INFO.txt
- Sample hash: ec7fbd548bd27bb5076dd9589e1b87f3c5740da00e77c127eb4cd4541d7d6f7

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Malicious Binary

CRITICAL

MALICIOUS PROCESS

axxes.exe

HOST

Win10EP02

ALERT ID

51561

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> KILL...

Description - Malicious Binary

Known Process Fuzzy Hash:

3072:0Yy21Aj5egDFFQb3y0ynyUckfRBbuLHtoNyJ:0YyCkjbuLNJ

Malicious Threat Level: 100%

Process Details

Process SHA256:

EC7FBD548BD27BB5076DD9589E1B87F3C5740DA00E77C127EB4CD4541D7D6F7

Process PID: 5268

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\april\april\axxes.exe

Hash

EC7FBD548BD27BB5076DD9589E1B87F3C5740DA00E77C127EB4CD4541D7D6F7

Process Tree

explorer.exe

(user: win10ep02\sam)

axxes.exe

(user: win10ep02\sam)

Comments

Add Comment...

Add

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

axxes.exe

HOST

Win10EP02

ALERT ID

51562

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> KILL...

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 business cannot be recovered.

MITRE ATT&CK

Tactics: Impact

Techniques:

T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\april\april\axxes.exe

Hash

EC7FBD548BD27BB5076DD9589E1B87F3C5740DA00E77C127EB4CD4541D7D6F7

Process Tree

explorer.exe

(user: win10ep02\sam)

axxes.exe

(user: win10ep02\sam)

Recommendation

Investigate according to organization policy

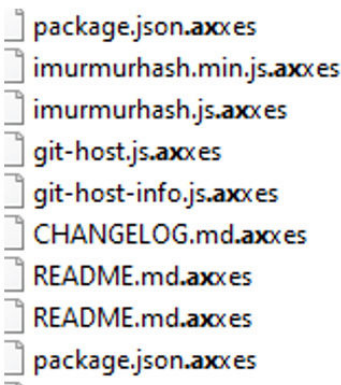
Comments

Add Comment...

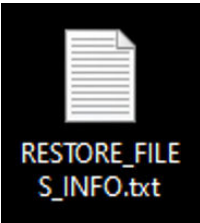
Add

Axxes Overview

Axxes ransomware renames the encrypted files with .axxes in the extension:



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



Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains only the encryption key:



Blaze Ransomware

- Observed since: December 2021
- Ransomware encryption method: RSA.
- Ransomware extension: .blaze
- Ransomware note: How To Decrypt.txt
- Sample hash: 25835a890a218fd26bfd8b23696576402b5eb8a4c9af4a51529e14c4f00a9cce

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary >...

High

MALICIOUS FILE

Blaze.bin

HOST

Win10EP02

USER

win10ep02\sam

ALERT ID

51564

FIRST SEEN

05/15/2022 11:03

LAST SEEN

05/15/2022 11:03

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

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

Detection Engine: Cynet AV

Infected file: C:\Users\user\Desktop\April\April\Blaze.bin

Malware Type: trojan

Malware ID: TR/Crypt.EPACK.Gen2

ave version: 0.0.0.0.0.0

avpack version: 0.0.0.0.0.0

vdf version: 0.0.0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\April\April\Blaze.bin

Hash

25835A890A218FD26BFD8B23696576402B5EB8A4C9AF4A51529E14C4F00A9CCE

Process Tree

explorer.exe (user: win10ep02\sam)

winrar.exe (user: win10ep02\sam)

Blaze.bin (user: win10ep02\sam)

Comments

Add Comment...

Add

Ransomware

Memory Pattern - Ransomware - Blaze v57

Critical

MALICIOUS PROCESS

blaze.exe

HOST

Win10EP02

USER

win10ep02\sam

ALERT ID

51571

FIRST SEEN

05/15/2022 11:04

LAST SEEN

05/15/2022 11:04

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

Description - Memory Pattern - Ransomware - Blaze v57

Signature Name: Memory Pattern - Ransomware - Blaze v57

Matched Memory Area Bounds : From - 0xf01000 - To - 0xf14000 - Area Size - 77824

Matched Memory Area Info : Type - IMAGE, AllocationBase - 0xf00000, AllocationProtect - WCX, Protect - RX

Pattern(1) Offset [Address]: 2672 [0xf01a70]

Pattern(1) Distance From Previous Pattern Start: 2672

Pattern(1) Dump Captured From: 0 [0xf01000] - To - 8192 [0xf03000]

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\april\april\blaze.exe

Hash

25835A890A218FD26BFD8B23696576402B5EB8A4C9AF4A51529E14C4F00A9CCE

Process Tree

explorer.exe (user: win10ep02\sam)

blaze.exe (user: win10ep02\sam)

Comments

Add Comment...

Add

Blaze Overview

Blaze ransomware renames the encrypted files with .blaze in the extension:

A screenshot of a file explorer window showing a list of files. The files are: t_sne.py.blaze, stochastic_gradient.cpython-37.pyc.blaze, setup.cpython-37.pyc.blaze, sag.cpython-37.pyc.blaze, __init__.cpython-37.pyc.blaze, __init__.cpython-37.pyc.blaze, test_ridge.cpython-37.pyc.blaze, and ridge.cpython-37.pyc.blaze. The files are listed in a standard file explorer view with icons and names.

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

A black square icon with a white document symbol and the text "How To Decrypt.txt" in white.

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

A screenshot of a Notepad window titled "How To Decrypt.txt - Notepad". The text in the window reads: "blaze Ransomware", "Your data are stolen and encrypted", "The data will be published on TOR website http://imugmohnfb6akqz7jb6rqjusiwnthjgm37mjygon dgkwyw3hwudkd.onion if you do not pay the ransom", "You can contact us and decrypt one file for free.", "gosupp@email.cz", "Caution!!", "Do not modify encrypted files, otherwise you may lose all your files forever!".

cynet

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

Monthly Ransomware Activity – April 2022 6

- Observed since: April 2022
- Ransomware encryption method: AES + RSA.
- Ransomware extension: .blockZ
- Ransomware note: How To Restore Your Files.txt
- Sample hash: 856d9e698f240a21db57f404fea33ee65cd0458f31a9d0fca7044962204484c9

Ransomware
MALICIOUS PROCESS
noopen.exe

HOST Win10EP02

USER win10ep02\sam

Memory Pattern - Ransomware - BlockZ v2

Description - Memory Pattern - Ransomware - BlockZ v2

- Signature Name: Memory Pattern - Ransomware - BlockZ v2
- Matched Memory Area Bounds : From - 0x192000 - To - 0x1c6000 - Area Size - 212992
- Matched Memory Area Info : Type - IMAGE, AllocationBase - 0x190000, AllocationProtect - WCX, Protect - RWX
- Pattern(1) Offset [Address]: 3972 [0x192f84]
- Pattern(1) Distance From Previous Pattern Start: 3972

Process Tree

```

graph TD
    userinit[userinit.exe] --> explorer[explorer.exe]
    explorer --> noopen[noopen.exe]
            
```

(user: win10ep02\sam)
(user: win10ep02\sam)
(user: win10ep02\sam)

Recommendation

Investigate according to organization policy

Path

c:\users\user\AppData\Local\Temp\nooopen.exe

Hash

95A26A161AA1180D018F8C7DEE6F9F91DD3A6E104F53768A39C1372A6D03F7A3

Incident View

Alert ID
51581

FIRST SEEN
05/15/2022 11:16

LAST SEEN
05/15/2022 11:16

GROUP NAME
Research

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action
Scanner Remediation -> Kill...

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

schtasks.exe

HOST Win10EP02

USER win10ep02\sam

Alert ID 51611

FIRST SEEN 05/15/2022 11:20

LAST SEEN 05/15/2022 11:20

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

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

MITRE ATT&CK

Tactics: Impact

Techniques:

T1486: Data Encrypted for Impact

Path

c:\windows\systemow64\schtasks.exe

Hash

97CA3FAD547C40FEF797DB77C414213BA981BC439C05AA3E9E42C2A5D494139

Process Tree

- explorer.exe (user: win10ep02\sam)
 - noopen.exe (user: win10ep02\sam)
 - schtasks.exe (user: win10ep02\sam)

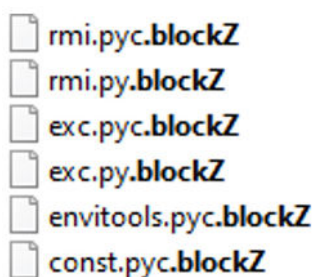
Recommendation

Investigate according to organization policy

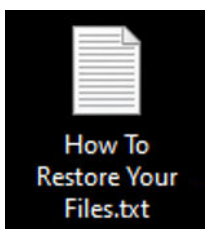
Comments

Add Comment...

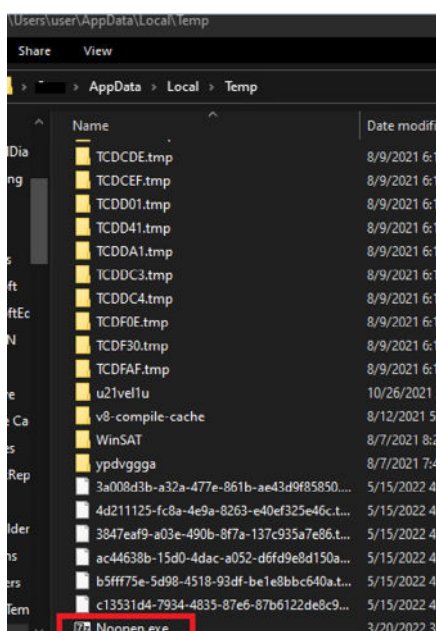
BlockZ ransomware renames the encrypted files with .blockZ in the extension:



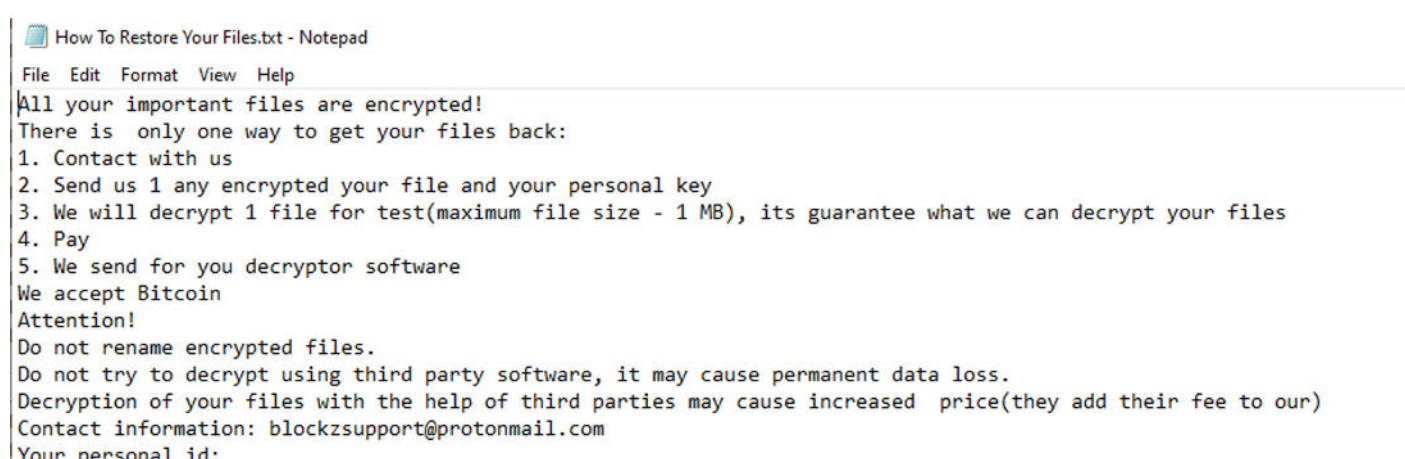
Once a computer's files have been encrypted and renamed, it drops a note as `How To Restore Your Files.txt`:



Upon execution, it first drop a file in the path “c:\users*user\appdata\local\temp\” with the name of Noopen.exe:



Once executed the dropped file it changes the process name to schtasks.exe and it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains contact information, warnings, and decryption test for 1 file:



DemocracyWhisperers Ransomware

- Observed since: April 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .democ
- Ransomware note: Restore Files.txt
- Sample hash: 59e0e38b068f736e7f618c714a116ad13fb50a1932942cff9e474de317fb4592

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

HIGH

MALICIOUS FILE

Democracy Whis...

HOST

Win10EP02

USER

win10ep02\sam

ALERT ID

51844

FIRST SEEN

05/15/2022 11:56

LAST SEEN

05/15/2022 11:56

GROUP NAME

Research

Incident View

Auto-Remediation:

Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

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

Detection Engine: Cynet AV

Infected file: C:\Users\user\Desktop\April\April\Democracy Whisperers.bin

Malware Type: trojan

Malware ID: TR/Crypt.EPACK.Gen2

ave version: 0.0.0.11.10

avpack version: 0.0.0.10

vdf version: 0.0.0.10.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\April\April\Democracy Whisperers.bin

Hash

59E0E38B068F736E7F618C714A116AD13FB50A1932942CFF9E474DE317FB4592

Process Tree

explorer.exe

(user: win10ep02\sam)

winrar.exe

(user: win10ep02\sam)

Democracy Whisperer...

(user: win10ep02\sam)

Comments

Add Comment...

Add

Ransomware

Memory Pattern - Ransomware - Democracy...

CRITICAL

MALICIOUS PROCESS

democracy whis...

HOST

Win10EP02

USER

win10ep02\sam

ALERT ID

51849

FIRST SEEN

05/15/2022 12:01

LAST SEEN

05/15/2022 12:01

GROUP NAME

Research

Incident View

Auto-Remediation:

Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

Description - Memory Pattern - Ransomware - Democracy Whisperers v1

Signature Name: Memory Pattern - Ransomware - Democracy Whisperers v1

Matched Memory Area Bounds : From - 0x251000 - To - 0x264000 - Area Size - 77824

Matched Memory Area Info : Type - IMAGE, AllocationBase - 0x250000, AllocationProtect - WCX, Protect - RX

Pattern(1) Offset [Address]: 2850 [0x251b22]

Pattern(1) Distance From Previous Pattern Start: 2850

Pattern(1) Dump Captured From: 0 [0x251000] - To - 8192 [0x253000]

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\april\april\democracy whisperers.exe

Hash

59E0E38B068F736E7F618C714A116AD13FB50A1932942CFF9E474DE317FB4592

Process Tree

explorer.exe

(user: win10ep02\sam)

democracy whisperers...

(user: win10ep02\sam)

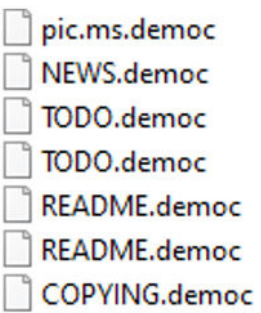
Comments

Add Comment...

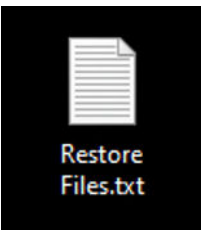
Add

DemocracyWhisperers Overview

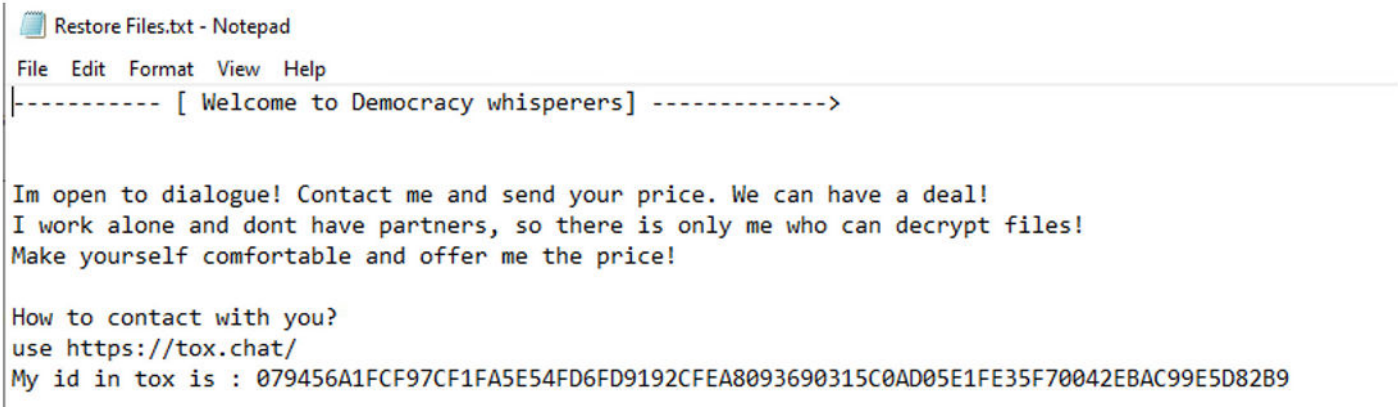
DemocracyWhisperers ransomware renames the encrypted files with .democ in the extension:



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



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





Medusa Ransomware

- Observed since: Late 2019
- Ransomware encryption method: AES + RSA
- Ransomware extension: .stopfiles
- Ransomware note: Recovery_instructions.html
- Sample hash: 2ca49be7f3eac14dfbf086ad11ce1235079b4fa96b7d8634a53403cfcf592969

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Malicious Binary

CRITICAL

MALICIOUS PROCESS

medusa.exe

HOST

Win10EP02

USER

win10ep02\sam

ALERT ID

51858

FIRST SEEN

05/15/2022 12:12

LAST SEEN

05/15/2022 12:12

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

Description - Malicious Binary

Alert Origin: SSDEEP

File Name: c:\users\user\desktop\april\april\medusa.exe

Process Fuzzy Hash: 12288:Ko/lae+Jl4PpEaojvYSwwyEOjML3ERSixKSbtG7Stfah2fAroM7:d3ulc6aojvYSwwyEGMzIxTGJ+M

Known Process Fuzzy Hash: 12288:Ko/lae+Jl4PpEaojvYSwwyEOjML3ERSixKSbtG7Stfah2fAroM7:d3ulc6aojvYSwwy

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\april\april\medusa.exe

Hash

2CA49BE7F3EAC14DFBF086AD11CE1235079B4FA96B7D8634A53403CFCF592969

Process Tree

userinit.exe (user: win10ep02\sam)

explorer.exe (user: win10ep02\sam)

medusa.exe (user: win10ep02\sam)

Comments

Add Comment...

Add

Ransomware

Memory Pattern - Ransomware - Medusa v82

CRITICAL

MALICIOUS PROCESS

svchost.exe

HOST

Win10EP02

USER

win10ep02\sam

ALERT ID

51866

FIRST SEEN

05/15/2022 12:15

LAST SEEN

05/15/2022 12:15

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

Description - Memory Pattern - Ransomware - Medusa v82

Signature Name: Memory Pattern - Ransomware - Medusa v82

Matched Memory Area Bounds : From - 0x395000 - To - 0x3c2000 - Area Size - 184320

Matched Memory Area Info : Type - IMAGE, AllocationBase - 0x320000, AllocationProtect - WCX, Protect - R

Pattern(1) Offset [Address]: 76182 [0x3a7996]

Pattern(1) Distance From Previous Pattern Start: 76182

Recommendation

Investigate according to organization policy

Path

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

Hash

2CA49BE7F3EAC14DFBF086AD11CE1235079B4FA96B7D8634A53403CFCF592969

Process Tree

wininit.exe (user: N/A)

services.exe (user: win10ep02\nt authority - system)

svchost.exe (user: win10ep02\nt authority - system)

svchost.exe (user: win10ep02\sam)

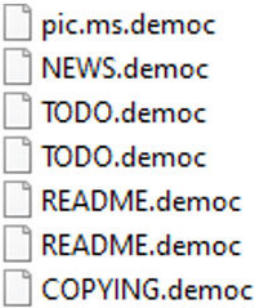
Comments

Add Comment...

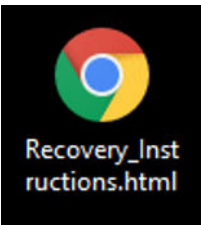
Add

Medusa Overview

Medusa ransomware renames the encrypted files with .stopfiles in the extension:



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



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

YOUR PERSONAL ID:

/! YOUR COMPANY NETWORK HAS BEEN PENETRATED !/
ALL YOUR IMPORTANT FILES HAVE BEEN ENCRYPTED!

YOUR FILES ARE SAFE! JUST MODIFIED ONLY. (RSA+AES)

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

NO SOFTWARE AVAILABLE ON INTERNET CAN HELP YOU! WE ONLY HAVE
SOLUTION TO 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. WE ONLY SEEK MONEY
AND DO NOT WANT TO DAMAGE YOUR REPUTATION. IF YOU DECIDE TO
NOT PAY, WE WILL RELEASE THIS DATA TO PUBLIC OR RE-SELLER.

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.

http://gvlay6u4g53rxd15.onion/21-NcpaKMSaMCUSib3actrmLJpQMfHx9uAQX-D1e61iF56bGWW6iDp5hDiSJ1sMO1xyBw

* Note that this server is available via Tor browser only

Snatch Ransomware

- Observed since: December 2018
- Ransomware encryption method: AES + RSA
- Ransomware extension: .sdhvvq
- Ransomware note: HOW TO RESTORE YOUR FILES.TXT
- Sample hash: 25835a890a218fd26bfd8b23696576402b5eb8a4c9af4a51529e14c4f00a9cce

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary ~...

HIGH

MALICIOUS FILE

Snatch.bin

HOST

Win10EP02

ALERT ID

51905

FIRST SEEN

05/15/2022 12:37

LAST SEEN

05/15/2022 12:37

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

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

- Detection Engine: Cynet AV
- Infected file: C:\Users\user\Desktop\April\April\Snatch.bin
- Malware Type: heuristic
- Malware ID: HEUR/AGEN.1211840
- ave version: 0.0.0.0.0.0
- avpack version: 0.0.0.0.0
- vdf version: 0.0.0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\April\April\Snatch.bin

Hash

F7F85240EFA2EBE980A83DF6C3D834699703BA1C3C5F38EC58687ABA219A0C03

Process Tree

- explorer.exe (user: win10ep02\sam)
- winrar.exe (user: win10ep02\sam)
- Snatch.bin (user: win10ep02\sam)

Comments

Add Comment...

Add

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

snatch.exe

HOST

Win10EP02

ALERT ID

51919

FIRST SEEN

05/15/2022 13:03

LAST SEEN

05/15/2022 13:03

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

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

MITRE ATT&CK

Tactics: Impact

Techniques: T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\april\april\snatch.exe

Hash

F7F85240EFA2EBE980A83DF6C3D834699703BA1C3C5F38EC58687ABA219A0C03

Process Tree

- userinit.exe (user: win10ep02\sam)
- explorer.exe (user: win10ep02\sam)
- snatch.exe (user: win10ep02\sam)

Recommendation

Investigate according to organization policy

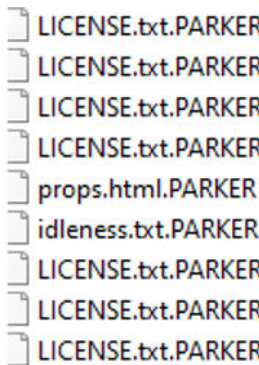
Comments

Add Comment...

Add

Snatch Overview

Snatch ransomware renames the encrypted files with .sdhvvq in the extension:



Once a computer’s files have been encrypted and renamed, it drops a note as HOW TO RESTORE YOUR FILES.TXT:



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

HOW TO RESTORE YOUR FILES.TXT - Notepad

File Edit Format View Help

Dear Management of Dellner Couplers AB!

We inform you that your network has undergone a penetration test, during which we encrypted your files and downloaded more than 240 GB of your and your customers data, including:

Confidential documents
Copy of some mailboxes
Accounting
Databases backups
Marketing data

We understand that if this information gets to your clients or to media directly, it will cause reputational and financial damage to your business, which we wouldn't want, therefore, for our part, we guarantee that information about what happened will not get into the media (but we cannot guarantee this if you decide to turn to third-party companies for help or ignore this message).

Important! Do not try to decrypt the files yourself or using third-party utilities. The only program that can decrypt them is our decryptor, which you can request from the contacts below. Any other program will only damage files in such a way that it will be impossible to restore them.

You can get all the necessary evidence, discuss with us possible solutions to this problem and request a decryptor by using the contacts below. Please be advised that if we don't receive a response from you within 3 days, we reserve the right to publish files to the public.

Contact me:
RichardSHibbs@seznam.cz or RichardSHibbs@protonmail.com

Additional ways to communicate in tox chat
https://tox.chat/
contact our tox id:

Parker Ransomware

- Observed since: April 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .PARKER
- Ransomware note: RESTORE_FILES_INFO.txt
- Sample hash: 39a044db72d3ca39122af249cd60660d7e200366af958c762910605eaed020cb

Cynet 360 AutoXDR™ Detections:

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

parker.exe

HOST

Win10EP02

USER

win10ep02\sam

ALERT ID

51881

FIRST SEEN

05/15/2022 12:24

LAST SEEN

05/15/2022 12:24

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

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

MITRE ATT&CK

Tactics: Impact

Techniques:

T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\april\april\parker.exe

Hash

39A044DB72D3CA39122AF249CD60660D7E200366AF958C762910605EAED020CB

Process Tree

userinit.exe

(user: win10ep02\sam)

explorer.exe

(user: win10ep02\sam)

parker.exe

(user: win10ep02\sam)

Recommendation

Investigate according to organization policy

Comments

Add Comment...

Add

Description - Process Monitoring

Alert Origin: DRIVER

ETW Alert Id: CyAlert Heuristic Activity - Vssadmin Shadowstorage Enum

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 : 2112

Process Path : c:\windows\system32\vssadmin.exe

MITRE ATT&CK

Tactics: Impact

Techniques:

T1490: Inhibit System Recovery

Path

c:\windows\system32\vssadmin.exe

Hash

ACDC96D628EE8FF7F07FC5D795A05C22EB239BE0D44A9F01727B6124A9619A9

Process Tree

explorer.exe

(user: win10ep02\sam)

parker.exe

(user: win10ep02\sam)

vssadmin.exe

(user: win10ep02\sam)

Recommendation

Investigate according to organization policy

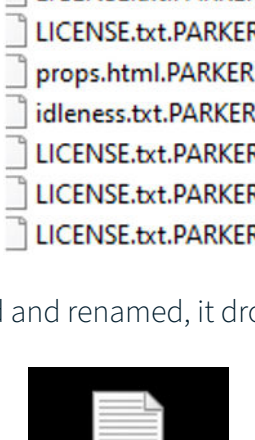
Comments

Add Comment...

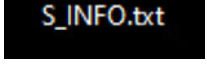
Add

Parker Overview

Parker ransomware renames the encrypted files with .PARKER in the extension:



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



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

File in process: C:\Users\user\Downloads\flare-vm-master\flare-vm-master\flarevm.win10.config.fireeye\tools\flarevm.pr
File Size: 52869 bytes
Total Files / Done / Errors: 15, 14, 0
Time elapsed: 00:00:07.1987440

File in process: C:\Users\user\Downloads\flare-vm-master\flare-vm-master\flarevm.win10.config.fireeye\tools\readme.txt
File Size: 1611 bytes
Total Files / Done / Errors: 16, 15, 0
Time elapsed: 00:00:07.2154701

File in process: C:\Users\user\Downloads\flare-vm-master\flare-vm-master\flarevm.config.flare\tools\flarevm.jpg - File
Size: 136698 bytes
Total Files / Done / Errors: 17, 16, 0
Time elapsed: 00:00:07.2648783

File in process: C:\Users\user\Downloads\flare-vm-master\flare-vm-master\flarevm.config.flare\tools\flarevm.png - File
Size: 52869 bytes
File in process: C:\Users\user\Downloads\flare-vm-master\flare-vm-master\flarevm.config.flare\tools\readme.txt - File
Size: 1613 bytes
Total Files / Done / Errors: 18, 18, 0
Total Files / Done / Errors: 19, 19, 0
Time elapsed: 00:00:07.7186639

Time elapsed: 00:00:07.7989198

File in process: C:\Users\user\Downloads\dnSpy-net-win64\bin\LicenseInfo\ApacheV2.txt - File Size: 11560 bytes
Total Files / Done / Errors: 20, 19, 0
Time elapsed: 00:00:07.9548069

File in process: C:\Users\user\Downloads\dnSpy-net-win64\bin\LicenseInfo\CREDITS.txt - File Size: 1303 bytes
File in process: C:\Users\user\Downloads\dnSpy-net-win64\bin\LicenseInfo\GPLv3.txt - File Size: 35821 bytes
File in process: C:\Users\user\Downloads\dnSpy-net-win64\bin\LicenseInfo\LICENSE.txt - File Size: 807 bytes
File in process: C:\Users\user\Downloads\dnSpy-net-win64\bin\LicenseInfo\OtherLicenses.txt - File Size: 9522 bytes
Total Files / Done / Errors: 24, 24, 0
Time elapsed: 00:00:08.3451858

RESTORE_FILES_INFO.txt - Notepad

File Edit Format View Help

| What happened? |

Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED:
- Contracts
- Customers data
- Finance
- HR
- Databases
- And more other...

| What does it mean? |

It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.

| How it can be avoided? |

In order to avoid this issue,
you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and breach fixing AGREEMENT.

| What if I do not contact you in 3 days? |

If you do not contact us in the next 3 DAYS we will begin DATA publication.

It is your RIGHT, but in this case all your data will be published for public USAGE.

| I do not fear your threats! |

That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
That is the EXACT AMOUNT of money you will spend for recovery and payouts because of PUBLICATION.
You are exposing yourself to huge penalties with lawsuits and government if we both don't find an agreement.
We have seen it before cases with multi million costs in fines and lawsuits,
not to mention the company reputation and losing clients trust and the medias calling non-stop for answers.

| You have convinced me! |

Then you need to CONTACT US, there is few ways to DO that.

---Secure method---

a) Download a qTOX client: https://tox.chat/download.html
b) Install the qTOX client and register account
c) Add our qTOX ID: 671263E78C06103C77146A5ABB802A63F53A42B4C4766329A5F04D2660C99A3611635CC36B3A
or qTOX ID: BC6934E2991F54988DF5D852F10EB4F7E1459693A2C1EF11026EE5A2598BA3593769D766A275
d) Write us extension of your encrypted files .PARKER

Our LIVE SUPPORT is ready to ASSIST YOU on this chat.

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

Monthly Ransomware Activity – April 2022 11

Thank you!



April, 2022