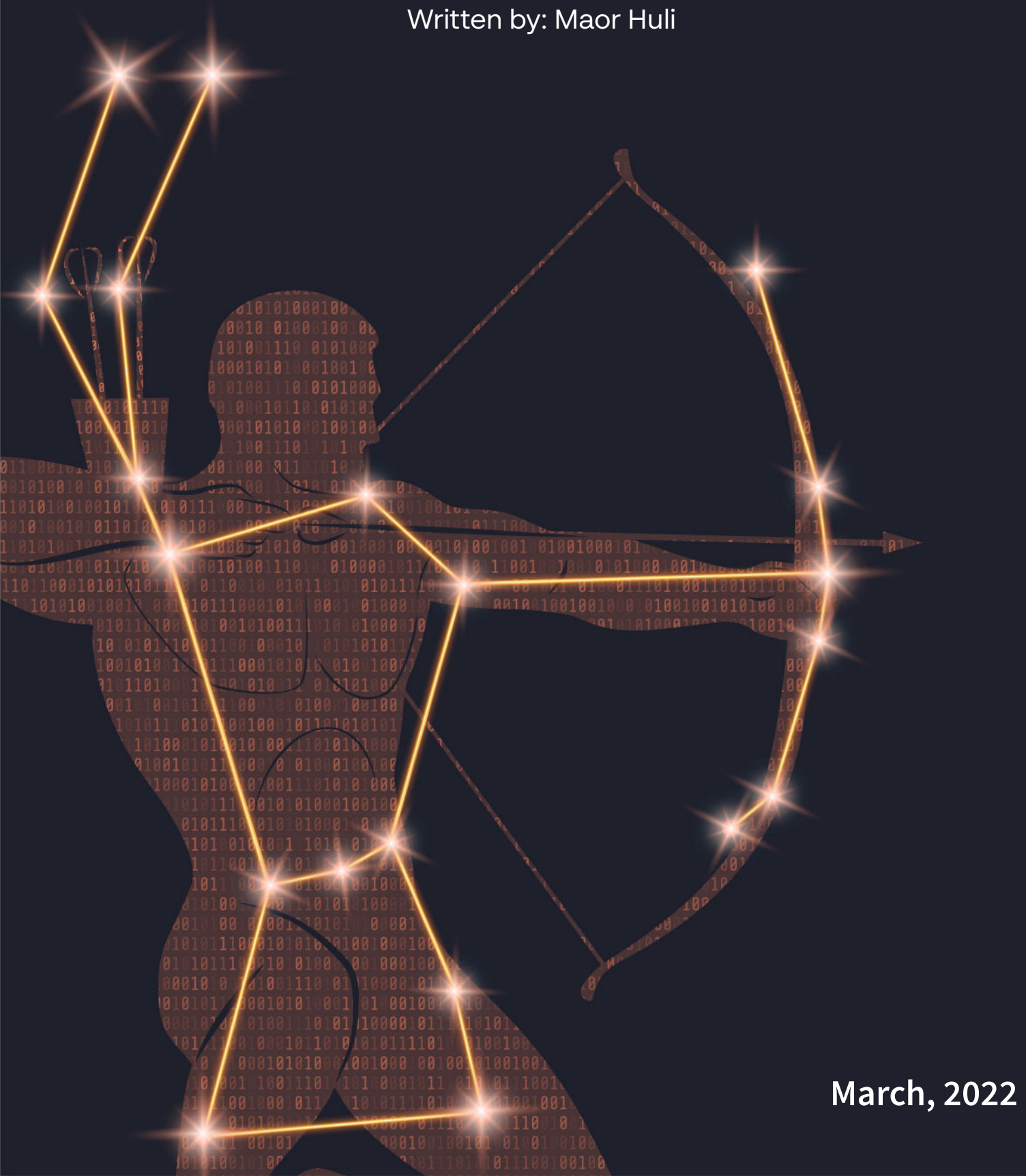


Orion Team

Monthly Ransomware Activity

Written by: Maor Huli



March, 2022



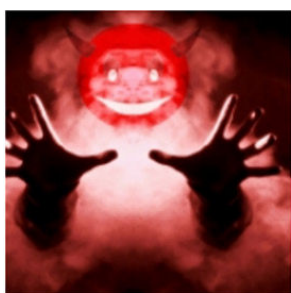
Contents

Executive Summary	3
Acepy	5
Pandora	6
LockBit 2.0	7
BlackCat	8



Executive Summary

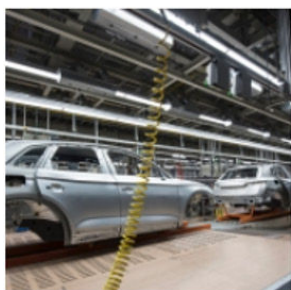
Orion is an integral department in Cynet's research team that works around the clock to track threat intelligence resources, analyze payloads, and automate labs to ensure that our customers are protected against the newest ransomware variants. In these monthly reports, Orion reviews the latest trends 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 - March 25th 2022 - Critical infrastructure

With the US providing military aid to Ukraine and its sanctions damaging the Russian economy, the US government disclosed this week that there is intelligence that Russia is preparing for potential cyberattacks against US interests.

 [LAWRENCE ABRAMS](#)  MARCH 25, 2022  05:06 PM  0



The Week in Ransomware - March 18th 2022 - Targeting the auto industry

This week, the automotive industry has been under attack, with numerous companies exhibiting signs of breaches or ransomware activity.

 [LAWRENCE ABRAMS](#)  MARCH 18, 2022  04:11 PM  0



The Week in Ransomware - March 4th 2022 - The Conti Leaks

This week's biggest story is the massive data leak from the Conti ransomware operation, including over 160,000 internal messages between members and source code for the ransomware and TrickBot operation.

 [LAWRENCE ABRAMS](#)  MARCH 04, 2022  06:46 PM  0

Orion Team



Cynet 360 AutoXDR™ VS Ransomware



Acepy Ransomware

- Observed since: March 2022
- Ransomware encryption method: RSA + AES.
- Ransomware extension: .acepy
- Ransomware note: ACEPY_README.txt
- Sample hash: 84BCC4AE912F0378CC5148799B33650FE358820B5F4AD8A33BDB4CEEE0D1EB1

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

HIGH

MALICIOUS FILE

Acepy.bin

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

49586

FIRST SEEN

05/09/2022 14:43

LAST SEEN

05/09/2022 14:43

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\March\March\Acepy.bin
- Malware Type: trojan
- Malware ID: TR/FileCoder.ilyde
- ave version: 0.0.0.0
- avpack version: 0.0.0.0
- vdf version: 0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\March\March\Acepy.bin

Hash

84BCC4AE912F0378CC5148799B33650FE358820B5F4AD8A33BDB4CEEE0D1EB11

Process Tree

explorer.exe

winrar.exe

Acepy.bin

Comments

Add Comment...

Add

Ransomware

Memory Pattern - Ransomware - Acepy

CRITICAL

MALICIOUS PROCESS

acepy.exe

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

49526

FIRST SEEN

05/09/2022 13:50

LAST SEEN

05/09/2022 13:51

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

Description - Memory Pattern - Ransomware - Acepy

- Signature Name: Memory Pattern - Ransomware - Acepy
- Matched Memory Area Bounds : From - 0x402000 - To - 0x403000 - Area Size - 4096
- Matched Memory Area Info : Type - IMAGE, AllocationBase - 0x400000, AllocationProtect - WCX, Protect - RW
- Pattern(1) Offset [Address]: 26 [0x40201a]
- Pattern(1) Distance From Previous Pattern Start: 26
- Pattern(1) Dump Captured From: 0 [0x402000] - To - 4096 [0x403000]
- Pattern(1) Zipped Dump:

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\march\march\acepy.exe

Hash

84BCC4AE912F0378CC5148799B33650FE358820B5F4AD8A33BDB4CEEE0D1EB11

Process Tree

explorer.exe

acepy.exe

Comments

Add Comment...

Add

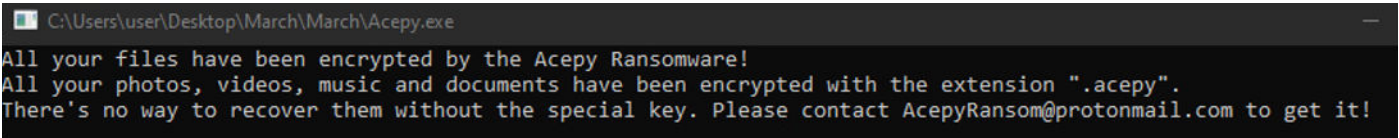
Acepy Overview

Acepy ransomware renames the encrypted files with .acepy in the extension:

a.bin.acepy.acepy
a.bin.acepy
.bin.acepy.acepy
.bin.acepy
at.bin.acepy.acepy
at.bin.acepy

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

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains the the attacker information and generic information about the encrypted files:





Pandora Ransomware

- Observed since: March 2022
- Ransomware encryption method: RSA.
- Ransomware extension: .pandora
- Ransomware note: Restore_My_Files.txt
- Sample hash: 2C940A35025DD3847F7C954A282F65E9C2312D2ADA28686F9D1DC73D1C500224

Cynet 360 AutoXDR™ Detections:

Ransomware

Ransomware - Cynet Classification

CRITICAL

MALICIOUS FILE

pandora.bin

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

49530

FIRST SEEN

05/09/2022 13:55

LAST SEEN

05/09/2022 13:55

GROUP NAME

Research

Auto-Remediation:

Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

Description - Ransomware - Cynet Classification

- Associated with Ransomware type malware.

- Encrypts all of the files on the system

- Prevents access to documents and data

- Steals sensitive information.

Recommendation

- Use Cynet built-in remediation options to delete the file.

- Use Cynet built-in remediation option to disconnect the HOST from the network.

- Investigate incident according to organizations policy.

- If necessary Format the End-Point.

Path

c:\users\user\desktop\march\march\pandora.bin

Hash

2C940A35025DD3847F7C954A282F65E9C2312D2ADA28686F9D1DC73D1C500224

Process Tree

Not Available

Comments

Add Comment...

Add

Malicious Binary

Malicious Binary

CRITICAL

MALICIOUS PROCESS

pandora.exe

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

49531

FIRST SEEN

05/09/2022 14:07

LAST SEEN

05/09/2022 14:08

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\march\march\pandora.exe

Process Fuzzy Hash: 6144:9V+XZ+t6L3cYw5fcqQhBTK9jB2Cimot3eJ99p9SpR3h82WUF8ZVku8jvLn:9UXZ+tgCXtcqQhpKpQC5otOHZ3uR

Known Process Fuzzy Hash: 6144:9V+XZ+t6L3cYw5fcqQhBTK9jB2Cimot3eJ99p9SpR3h82WUF8ZVku8jvLn:9UXZ+tgCXtcqQhpKpQC5otOHZ3uR

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\march\march\pandora.exe

Hash

2C940A35025DD3847F7C954A282F65E9C2312D2ADA28686F9D1DC73D1C500224

Process Tree

explorer.exe (user: win10ep01\sam)

pandora.exe (user: win10ep01\sam)

Comments

Add Comment...

Add

Pandora Overview

Pandora ransomware renames the encrypted files with .pandora in the extension, Once a computer’s files have been encrypted and renamed, it drops a note as Restore_My_Files.txt.

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains warnings, information, and the attacker’s contact information (the ransomware couldn’t run in the labs properly due to the remediation):

What happened?

!!!Your files are encrypted!!!

All your files are protected by strong encryption with RSA-2048.
There is no public decryption software.
We have successfully stolen your confidential document data, finances, emails, employee information, customers, research and development products...

What is the price?

The price depends on how fast you can write to us.
After payment, we will send you the decryption tool which will decrypt all your files.

What should I do?

There is only one way to get your files back -->>Contact us, pay and get decryption software.
If you decline payment, we will share your data files with the world.
*You can browse your data breach here:
<http://vbfqeh5nugm6r2u2qvghsdxm3fotf5wbxb5ltv6vw77vus5frdpuaiid.onion>*
(you should download and install TOR browser first hxxps://torproject.org)


!!!Decryption Guaranteed!!!

Free decryption As a guarantee, you can send us up to 3 free decrypted files before payment.

!!!Contact us!!!

email:
contact@pandoraxyz.xyz
!!!Warning!!!

Do not attempt to decrypt your data using third-party software, this may result in permanent data loss.
Decrypting your files with the help of a third party may result in a price increase (they charge us a fee), or you may fall victim to a scam.
Don't try to delete programs or run antivirus tools. It won't work.
Attempting to self-decrypt the file will result in the loss of your data.

cynet

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

Monthly Ransomware Activity – March 2022 6



LockBit 2.0 Ransomware

- Observed since: Mid 2021
- Ransomware encryption method: AES + RSA.
- Ransomware extension: .lockbit
- Ransomware note: Restore-My-Files.txt
- Sample hash: 9FEED0C7FA8C1D32390E1C168051267DF61F11B048EC62AA5B8E66F60E8083AF

Cynet 360 AutoXDR™ Detections:

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

lockbit.exe

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

49584

FIRST SEEN

05/09/2022 14:33

LAST SEEN

05/09/2022 14:33

GROUP NAME

Research

Incident View

Auto-Remediation:

Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

Description - Unauthorized File Operation Attempt

- Volume Attributes: Boot
- 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 case...

MITRE ATT&CK

Tactics: Impact

Techniques: T1486: Data Encrypted for Impact

Path

c:\users\user\desktop\march\march\lockbit.exe

Hash

9FEED0C7FA8C1D32390E1C168051267DF61F11B048EC62AA5B8E66F60E8083AF

Process Tree

unknown-process (user: N/A)

lockbit.exe (user: win10ep01\sam)

Recommendation

Investigate according to organization policy

Comments

Add Comment...

Add

Ransomware

Memory Pattern - Ransomware - LockBit...

CRITICAL

MALICIOUS PROCESS

lockbit.exe

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

49534

FIRST SEEN

05/09/2022 14:27

LAST SEEN

05/09/2022 14:27

GROUP NAME

Research

Incident View

Auto-Remediation:

Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Kill...

Description - Memory Pattern - Ransomware - LockBit v60

- Signature Name: Memory Pattern - Ransomware - LockBit v60
- Matched Memory Area Bounds : From - 0x401000 - To - 0x4e1000 - Area Size - 917504
- Matched Memory Area Info : Type - IMAGE, AllocationBase - 0x400000, AllocationProtect - WCX, Protect - RX
- Pattern(1) Offset [Address]: 11848 [0x403e48]
- Pattern(1) Distance From Previous Pattern Start: 11848
- Pattern(1) Dump Captured From: 8192 [0x403000] - To - 16384 [0x405000]

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\march\march\lockbit.exe

Hash

9FEED0C7FA8C1D32390E1C168051267DF61F11B048EC62AA5B8E66F60E8083AF

Process Tree

explorer.exe (user: win10ep01\sam)

lockbit.exe (user: win10ep01\sam)

Comments

Add Comment...

Add

LockBit Overview

LockBit ransomware renames the encrypted files with .lockbit in the extension, Once a computer’s files have been encrypted and renamed, it drops a note as Restore-My-Files.txt.

integral.thmx.lockbit
gallery.thmx.lockbit
facet.thmx.lockbit
wb02201_.gif.lockbit
wb02106_.gif.lockbit
wb00780l.gif.lockbit
wb00760l.gif.lockbit
wb00703l.gif.lockbit
wb00673l.gif.lockbit
wb00531l.gif.lockbit

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains contact information and warnings:

Restore-My-Files.txt

LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

Any attempts to restore your files with the third-party software will be fatal for your files!

To recovery your data and not to allow data leakage, It is possible only through purchase of a private key from us

There is only one way to get your files back:

Through a standard browser

- Brave (supports Tor links) Firefox Chrome Edge Opera
- Open link - https://decoding.at/

Through a Tor Browser - recommended

- Download Tor Browser - https://www.torproject.org/ and install it.
- Open one of links in Tor browser and follow instructions on these pages:
http://lockbitzap2oanphcum3evcbgfin5nzt7fopscfjdlmeflu7ka4k2did.onion/
or mirror
http://lockbitoup4yezof5enk5ummx3ccy7hw6n/vgmlyhwang352jeyid.onion/
These links work only in the Tor browser!
- Follow the instructions on this page

ATTENTION!

- https://decoding.at may be blocked. We recommend using a Tor browser (or Brave) to access the TOR site
- Do not rename encrypted files.
- Do not try to decrypt 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).
- Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
- Tor Browser user manual https://tp-manual.torproject.org/about/
- All your stolen important data will be loaded into our blog if you do not pay ransom.
- Our blog http://lockbitap6vxs713eeqjofwgcgmtr3a35mynvokja5uuccip4kykd.onion or https://bigblog.at where you can see data of the companies which refused to pay ransom.

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

Monthly Ransomware Activity – March 2022 7



BlackCat Ransomware

- Observed since: Early 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .yicrlka
- Ransomware note: RECOVER-yicrlka-FILES.txt
- Sample hash: 6DD995D896A9A593B2C48D09DA60BD83866D8577273F36D38788D83AD8173E68

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary ~...

HIGH

MALICIOUS FILE

BlackCat.bin

HOST Win10EP01

USER win10ep01\sam

ALERT ID

49587

FIRST SEEN

05/09/2022 14:43

LAST SEEN

05/09/2022 14:43

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\March\March\BlackCat.bin
- Malware Type: heuristic
- Malware ID: HEUR/AGEN.1235532
- ave version: 0.0.0.0.0.0.0
- avpack version: 0.0.0.0.0.0.0
- vdf version: 0.0.0.0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\March\March\BlackCat.bin

Hash

6DD995D896A9A593B2C48D09DA60BD83866D8577273F36D38788D83AD8173E68

Process Tree

- explorer.exe (user: win10ep01\sam)
- winrar.exe (user: win10ep01\sam)
- BlackCat.bin (user: win10ep01\sam)

Comments

Add Comment...

Add

Malicious Binary

Malicious Binary

CRITICAL

MALICIOUS PROCESS

blackcat.exe

HOST Win10EP01

USER win10ep01\sam

ALERT ID

49590

FIRST SEEN

05/09/2022 14:43

LAST SEEN

05/09/2022 14:43

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\march\march\blackcat.exe
- Process Fuzzy Hash: 49152:OQMStZChL9rV/HFHVnR3/sTUfCgUdbdNALjnzVghyW9itX6e/7SM:HghLfH1xR3/ZqgL3mtitX6
- Known Process Fuzzy Hash: 49152:BQMStZChL9rV/HFHVnR3/sTUfCgUdbdNza8keltX6e/7SM:CghLfH1xR3/ZqTaltX6

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\march\march\blackcat.exe

Hash

6DD995D896A9A593B2C48D09DA60BD83866D8577273F36D38788D83AD8173E68

Process Tree

- userinit.exe (user: win10ep01\sam)
- explorer.exe (user: win10ep01\sam)
- blackcat.exe (user: win10ep01\sam)

Comments

Add Comment...

Add

BlackCat Overview

BlackCat ransomware renames the encrypted files with .yicrlka in the extension and once a computer’s files have been encrypted and renamed, it drops a note as RECOVER-[variant name]-FILES.txt.

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

>> What happened?

Important files on your network was ENCRYPTED and now they have "yicrlka" extension. In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED. If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:

- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and install Tor Browser from: <https://torproject.org/>

Thank you!



March, 2022