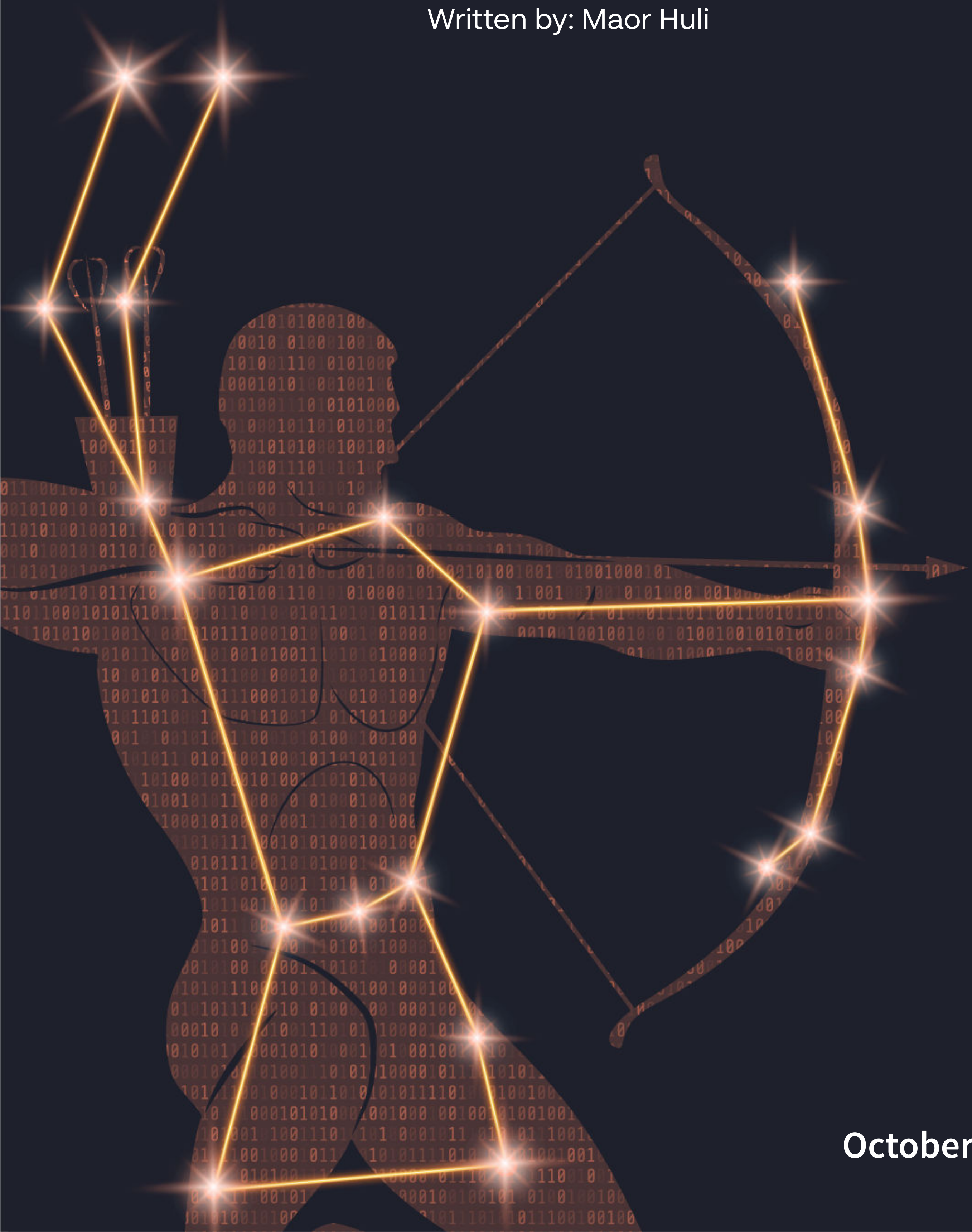
cynet

Orion Team

Monthly Ransomware Activity

Written by: Maor Huli



October, 2022

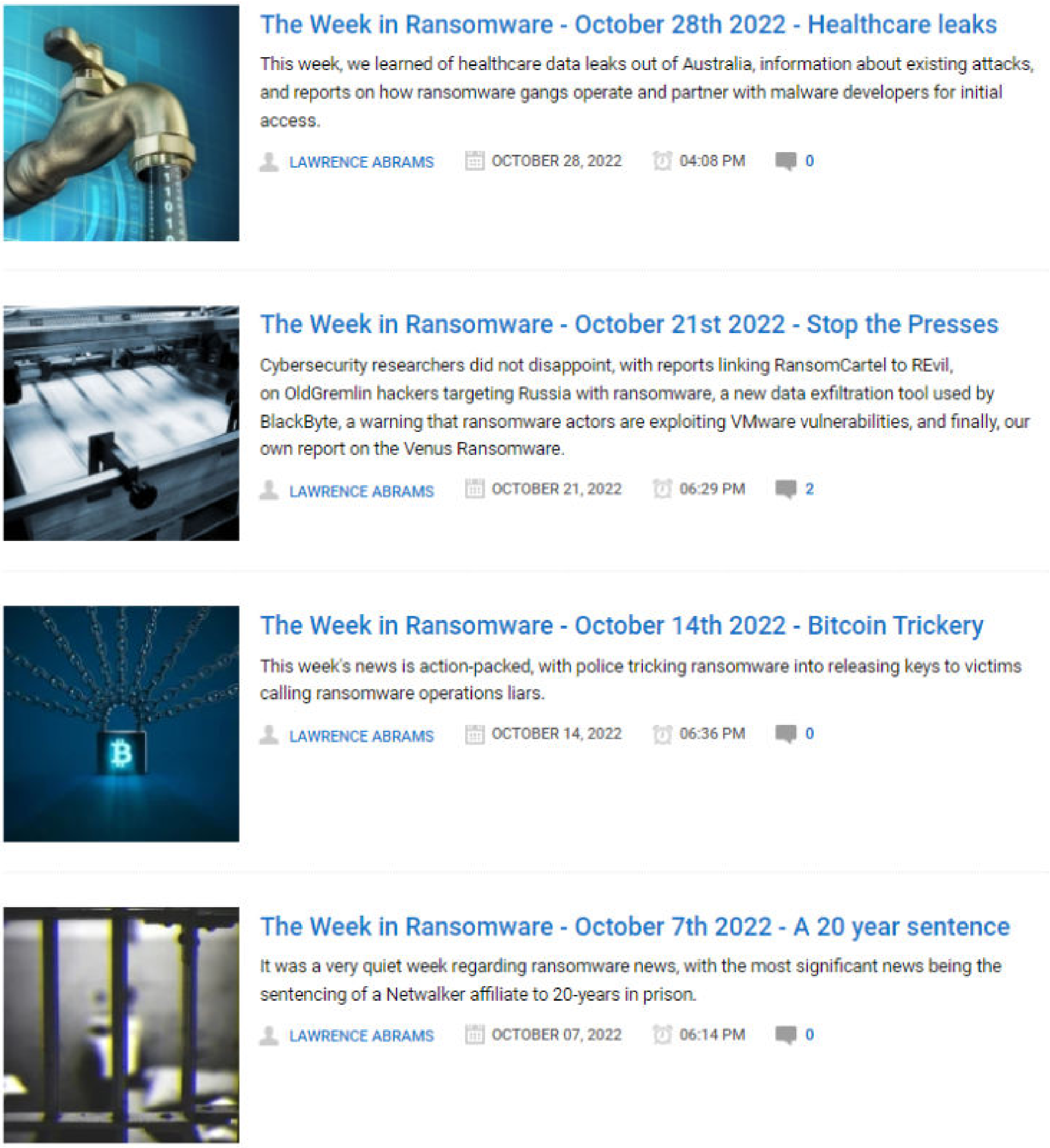
Orion Team

Contents

Orion Team

Executive Summary

As an integral department in Cynet's research team, Orion works around the clock to track threat intelligence resources, analyze payloads and automate labs to ensure 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 these threats.



The Week in Ransomware - October 28th 2022 - Healthcare leaks

This week, we learned of healthcare data leaks out of Australia, information about existing attacks, and reports on how ransomware gangs operate and partner with malware developers for initial access.

LAWRENCE ABRAMS OCTOBER 28, 2022 04:08 PM 0

The Week in Ransomware - October 21st 2022 - Stop the Presses

Cybersecurity researchers did not disappoint, with reports linking RansomCartel to REvil, on OldGremlin hackers targeting Russia with ransomware, a new data exfiltration tool used by BlackByte, a warning that ransomware actors are exploiting VMware vulnerabilities, and finally, our own report on the Venus Ransomware.

LAWRENCE ABRAMS OCTOBER 21, 2022 06:29 PM 2

The Week in Ransomware - October 14th 2022 - Bitcoin Trickery

This week's news is action-packed, with police tricking ransomware into releasing keys to victims calling ransomware operations liars.

LAWRENCE ABRAMS OCTOBER 14, 2022 06:36 PM 0

The Week in Ransomware - October 7th 2022 - A 20 year sentence

It was a very quiet week regarding ransomware news, with the most significant news being the sentencing of a Netwalker affiliate to 20-years in prison.

LAWRENCE ABRAMS OCTOBER 07, 2022 06:14 PM 0

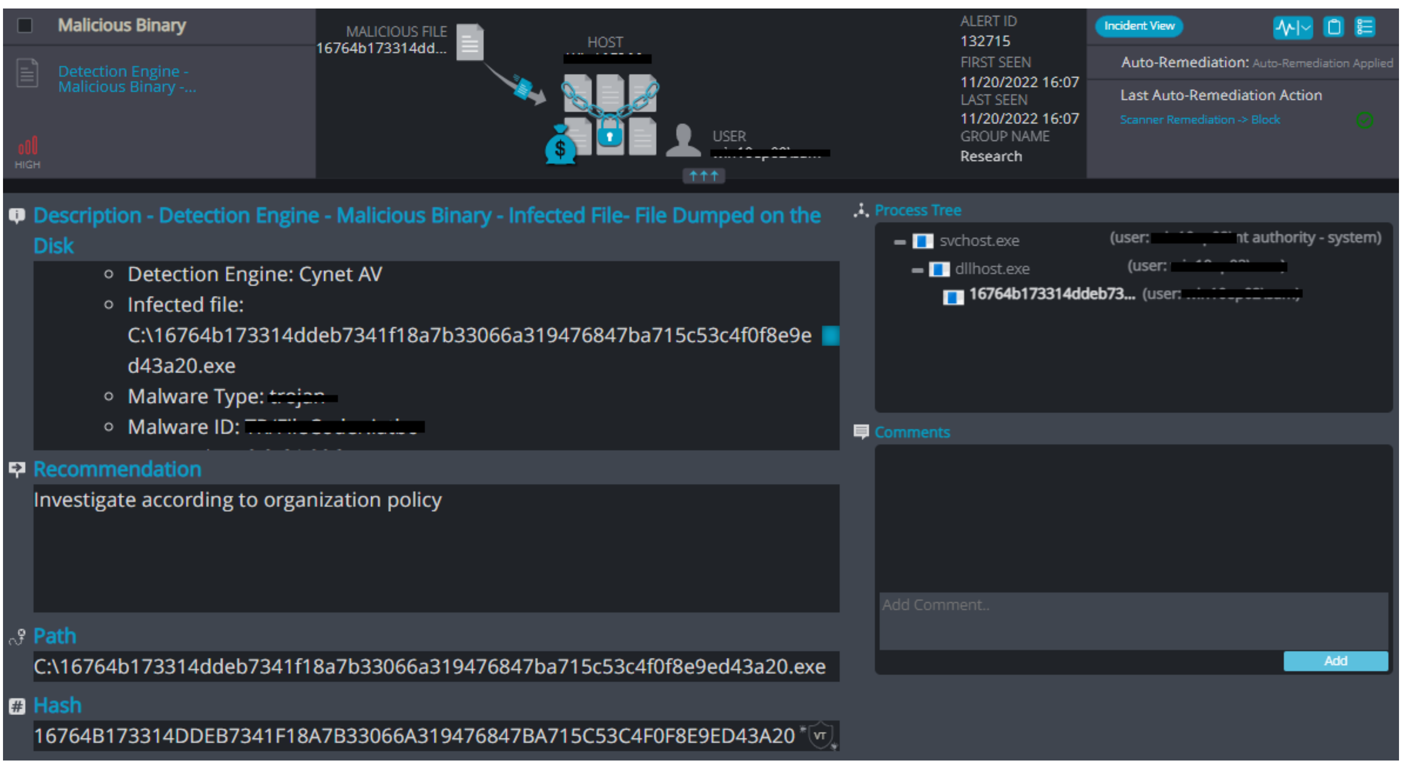
Orion Team

Cynet 360 AutoXDR™ VS Ransomware

RedKrypt Ransomware

- Observed since: Oct 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .redkrypt
- Ransomware note: RedKrypt-Notes-README.txt
- Sample hash: 16764b173314ddeb7341f18a7b33066a319476847ba715c53c4f0f8e9ed43a20

Cynet 360 AutoXDR™ Detections:



ALERT ID
132715
FIRST SEEN
11/20/2022 16:07
LAST SEEN
11/20/2022 16:07
GROUP NAME
Research

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:\16764b173314ddeb7341f18a7b33066a319476847ba715c53c4f0f8e9ed43a20.exe
- Malware Type: [redacted]
- Malware ID: [redacted]

Recommendation

Investigate according to organization policy

Path

C:\16764b173314ddeb7341f18a7b33066a319476847ba715c53c4f0f8e9ed43a20.exe

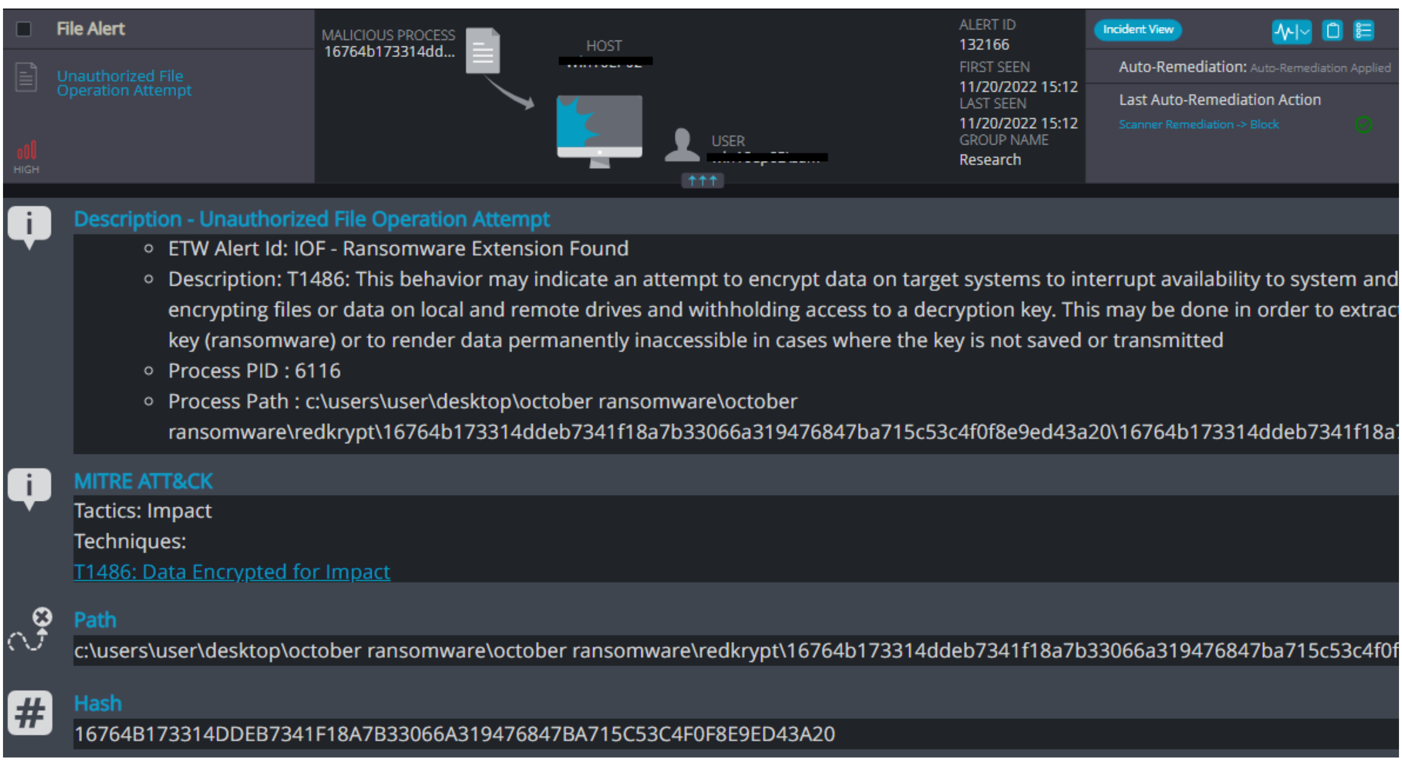
Hash

16764B173314DDEB7341F18A7B33066A319476847BA715C53C4F0F8E9ED43A20

Process Tree

```
- svchost.exe                 (user: [redacted]nt authority - system)
  - dllhost.exe               (user: [redacted]
      16764b173314ddeb73...   (user: [redacted]
```

Comments



ALERT ID
132166
FIRST SEEN
11/20/2022 15:12
LAST SEEN
11/20/2022 15:12
GROUP NAME
Research

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 encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extrac key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted
- Process PID : 6116
- Process Path : c:\users\user\desktop\october ransomware\october ransomware\redkrypt\16764b173314ddeb7341f18a7b33066a319476847ba715c53c4f0f8e9ed43a20\16764b173314ddeb7341f18a7

MITRE ATT&CK

Tactics: Impact
Techniques:
T1486: Data Encrypted for Impact

Path

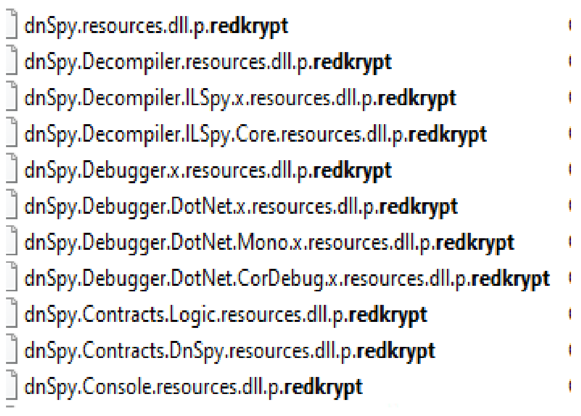
c:\users\user\desktop\october ransomware\october ransomware\redkrypt\16764b173314ddeb7341f18a7b33066a319476847ba715c53c4f0f

Hash

16764B173314DDEB7341F18A7B33066A319476847BA715C53C4F0F8E9ED43A20

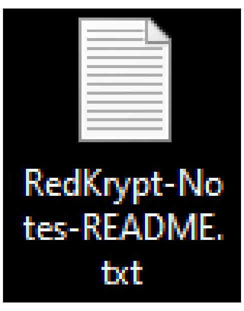
RedKrypt Overview

RedKrypt ransomware renames the encrypted files with .redkrypt in the extension.

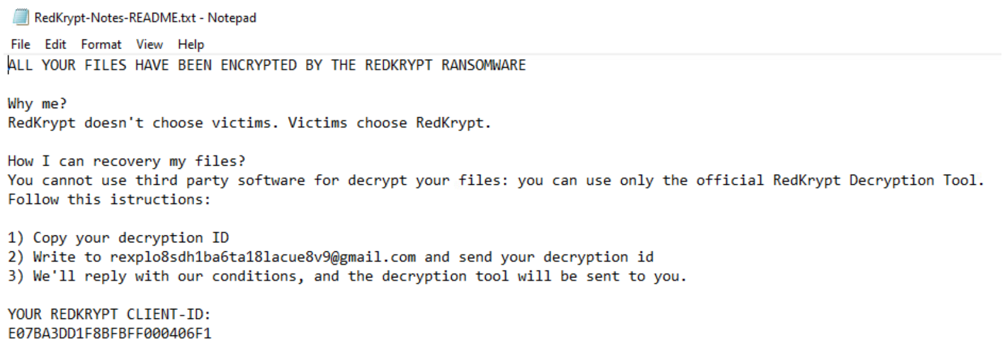


```
dnSpy.resources.dll.p.redkrypt
dnSpy.Decompiler.resources.dll.p.redkrypt
dnSpy.Decompiler.ILSpy.x.resources.dll.p.redkrypt
dnSpy.Decompiler.ILSpy.Core.resources.dll.p.redkrypt
dnSpy.Debugger.x.resources.dll.p.redkrypt
dnSpy.Debugger.DotNet.x.resources.dll.p.redkrypt
dnSpy.Debugger.DotNet.Mono.x.resources.dll.p.redkrypt
dnSpy.Debugger.DotNet.CorDebug.x.resources.dll.p.redkrypt
dnSpy.Contracts.Logic.resources.dll.p.redkrypt
dnSpy.Contracts.DnSpy.resources.dll.p.redkrypt
dnSpy.Console.resources.dll.p.redkrypt
```

Once a computer's files have been encrypted and renamed, it drops a note as "RedKrypt-Notes-README.txt":



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

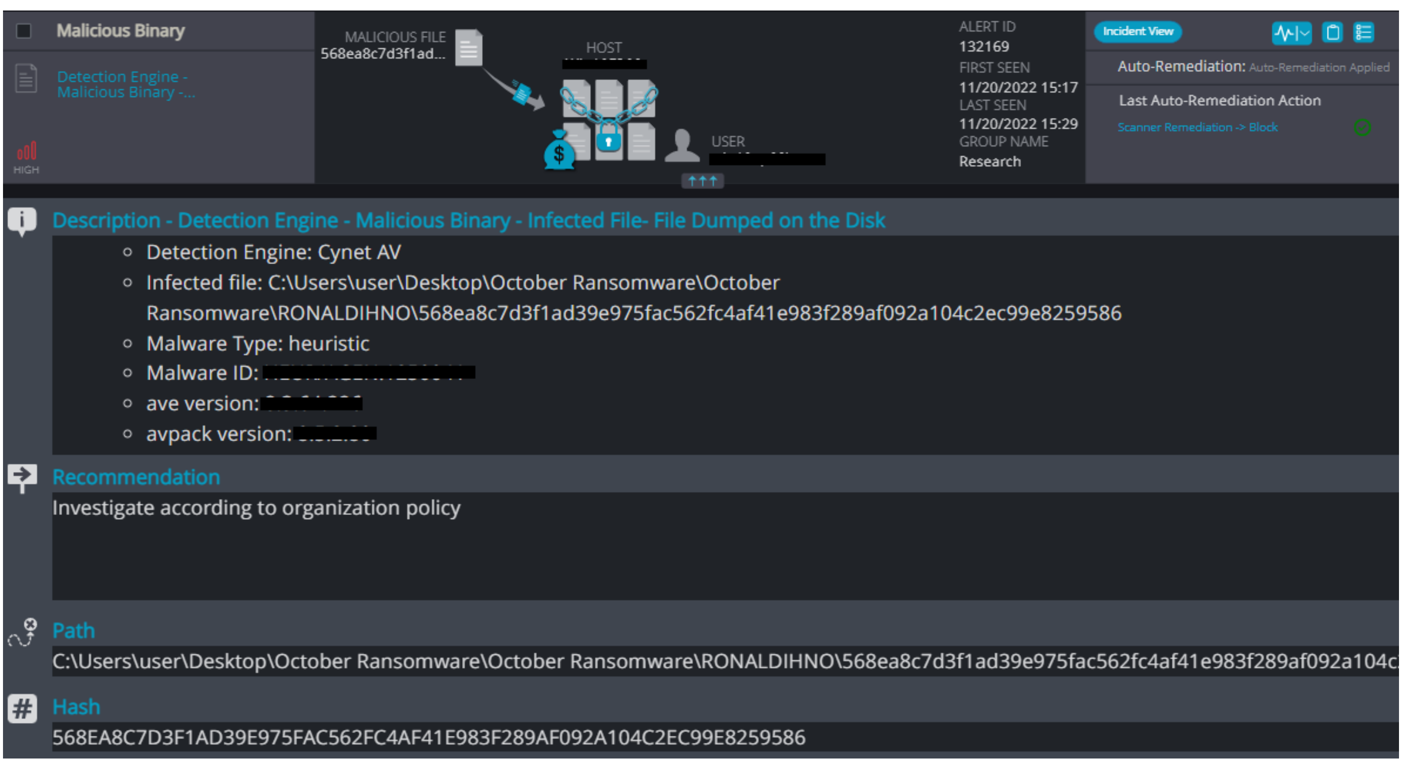


```
ALL YOUR FILES HAVE BEEN ENCRYPTED BY THE REDKRYPT RANSOMWARE

Why me?
RedKrypt doesn't choose victims. Victims choose RedKrypt.

How I can recovery my files?
You cannot use third party software for decrypt your files: you can use only the official RedKrypt Decryption Tool.
Follow this istructions:

1) Copy your decryption ID
2) Write to rexplo8sdh1ba6ta18lacue8v9@gmail.com and send your decryption id
3) We'll reply with our conditions, and the decryption tool will be sent to you.

YOUR REDKRYPT CLIENT-ID:
E07BA3DD1F8BFBFF000406F1
```

RONALDIHNO Ransomware

- Observed since: Oct 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .r7
- Ransomware note: READ_THIS.txt
- Sample hash: 568ea8c7d3f1ad39e975fac562fc4af41e983f289af092a104c2ec99e8259586

Cynet 360 AutoXDR™ Detections:



ALERT ID
132169
FIRST SEEN
11/20/2022 15:17
LAST SEEN
11/20/2022 15:29
GROUP NAME
Research

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\October Ransomware\October Ransomware\RONALDIHNO\568ea8c7d3f1ad39e975fac562fc4af41e983f289af092a104c2ec99e8259586
- Malware Type: heuristic
- Malware ID: [redacted]
- ave version: [redacted]
- avpack version: [redacted]

Recommendation

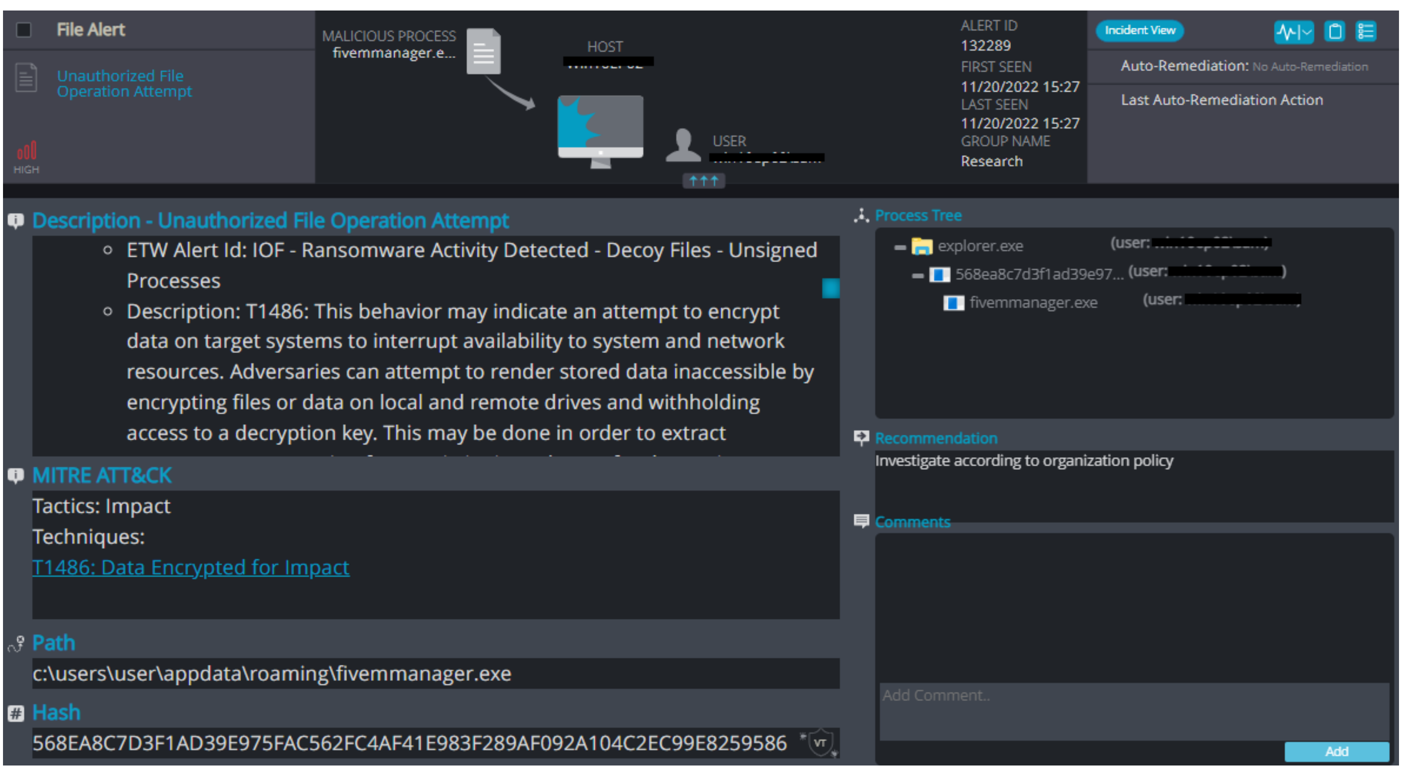
Investigate according to organization policy

Path

C:\Users\user\Desktop\October Ransomware\October Ransomware\RONALDIHNO\568ea8c7d3f1ad39e975fac562fc4af41e983f289af092a104c

Hash

568EA8C7D3F1AD39E975FAC562FC4AF41E983F289AF092A104C2EC99E8259586



ALERT ID
132289
FIRST SEEN
11/20/2022 15:27
LAST SEEN
11/20/2022 15:27
GROUP NAME
Research

Auto-Remediation: No Auto-Remediation

Last Auto-Remediation Action

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

MITRE ATT&CK

Tactics: Impact

Techniques:

T1486: Data Encrypted for Impact

Path

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

Hash

568EA8C7D3F1AD39E975FAC562FC4AF41E983F289AF092A104C2EC99E8259586

Process Tree

```
− explorer.exe              (user: [redacted])
  − 568ea8c7d3f1ad39e97...  (user: [redacted])
      fivemmanager.exe      (user: [redacted])
```

Recommendation

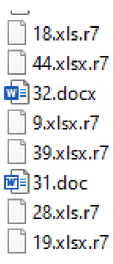
Investigate according to organization policy

Comments

Add Comment..

RONALDIHNO Overview

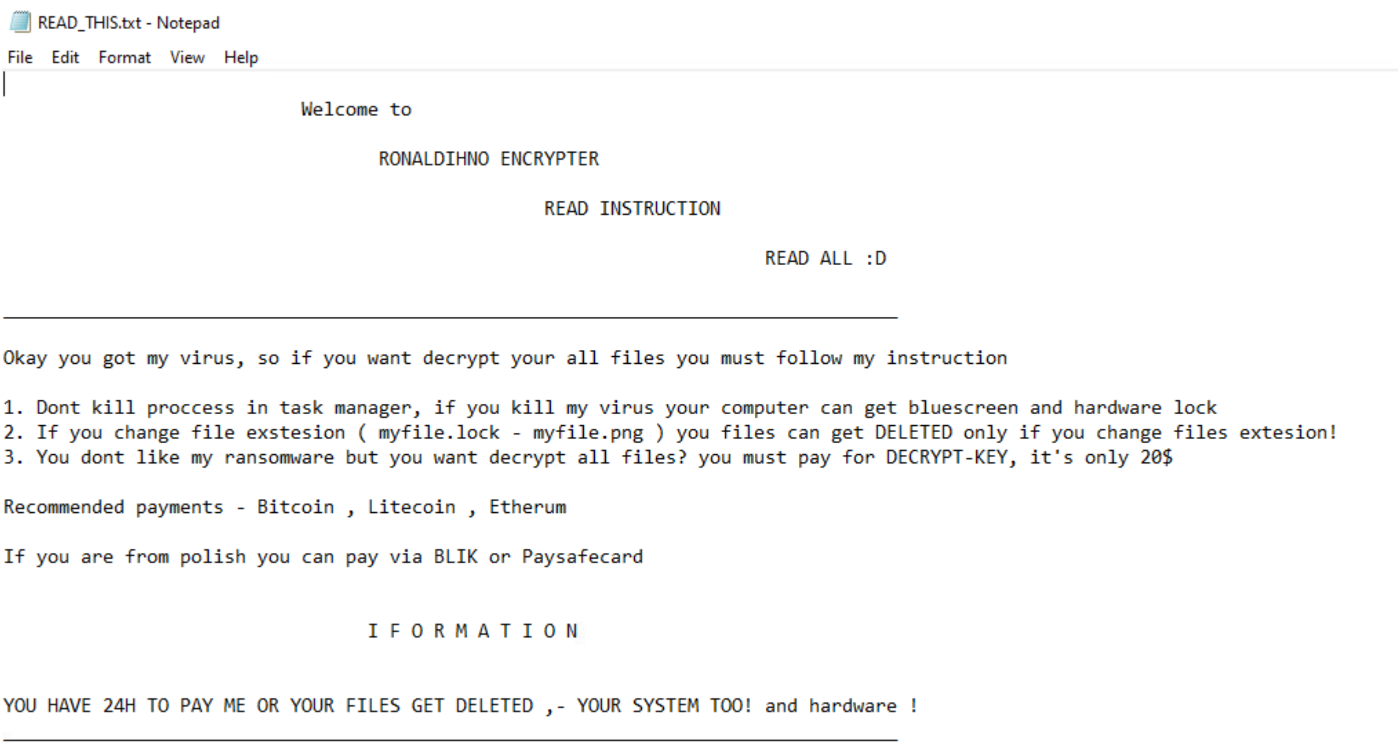
RONALDIHNO ransomware renames the encrypted files with .r7 in the extension:



```
18.xls.r7
44.xlsx.r7
32.docx
9.xlsx.r7
39.xlsx.r7
31.doc
28.xls.r7
19.xlsx.r7
```

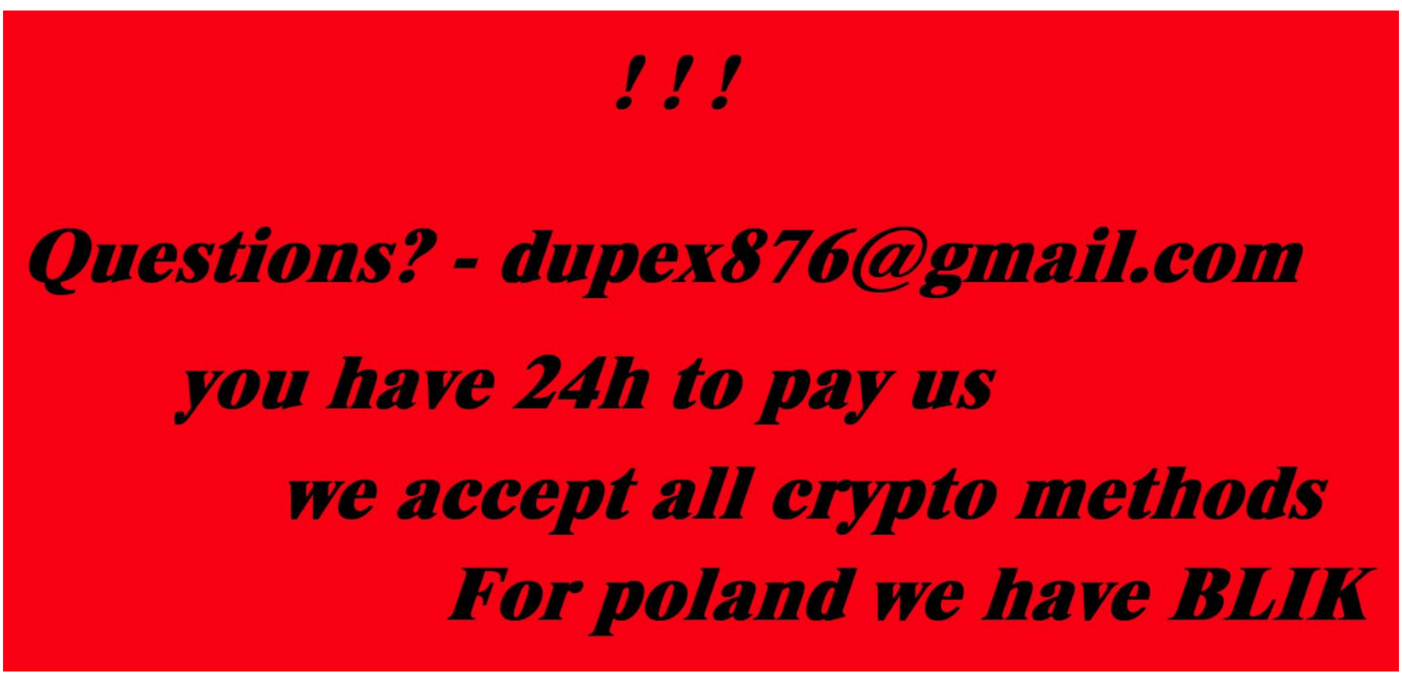
Once a computer's files have been encrypted and renamed, it drops a note named "READ_THIS.txt":

The ransomware note contains general information and warnings:



```
                         Welcome to

                                RONALDIHNO ENCRYPTER

                                             READ INSTRUCTION

                                                              READ ALL :D

________________________________________________________________

Okay you got my virus, so if you want decrypt your all files you must follow my instruction

1. Dont kill proccess in task manager, if you kill my virus your computer can get bluescreen and hardware lock
2. If you change file exstesion ( myfile.lock - myfile.png ) you files can get DELETED only if you change files extesion!
3. You dont like my ransomware but you want decrypt all files? you must pay for DECRYPT-KEY, it's only 20$

Recommended payments - Bitcoin , Litecoin , Etherum

If you are from polish you can pay via BLIK or Paysafecard


                                I F O R M A T I O N


YOU HAVE 24H TO PAY ME OR YOUR FILES GET DELETED ,- YOUR SYSTEM TOO! and hardware !
________________________________________________________________
```

The attacker's contact information will eventually appear as a desktop background:



! ! !

Questions? - dupex876@gmail.com

you have 24h to pay us

we accept all crypto methods

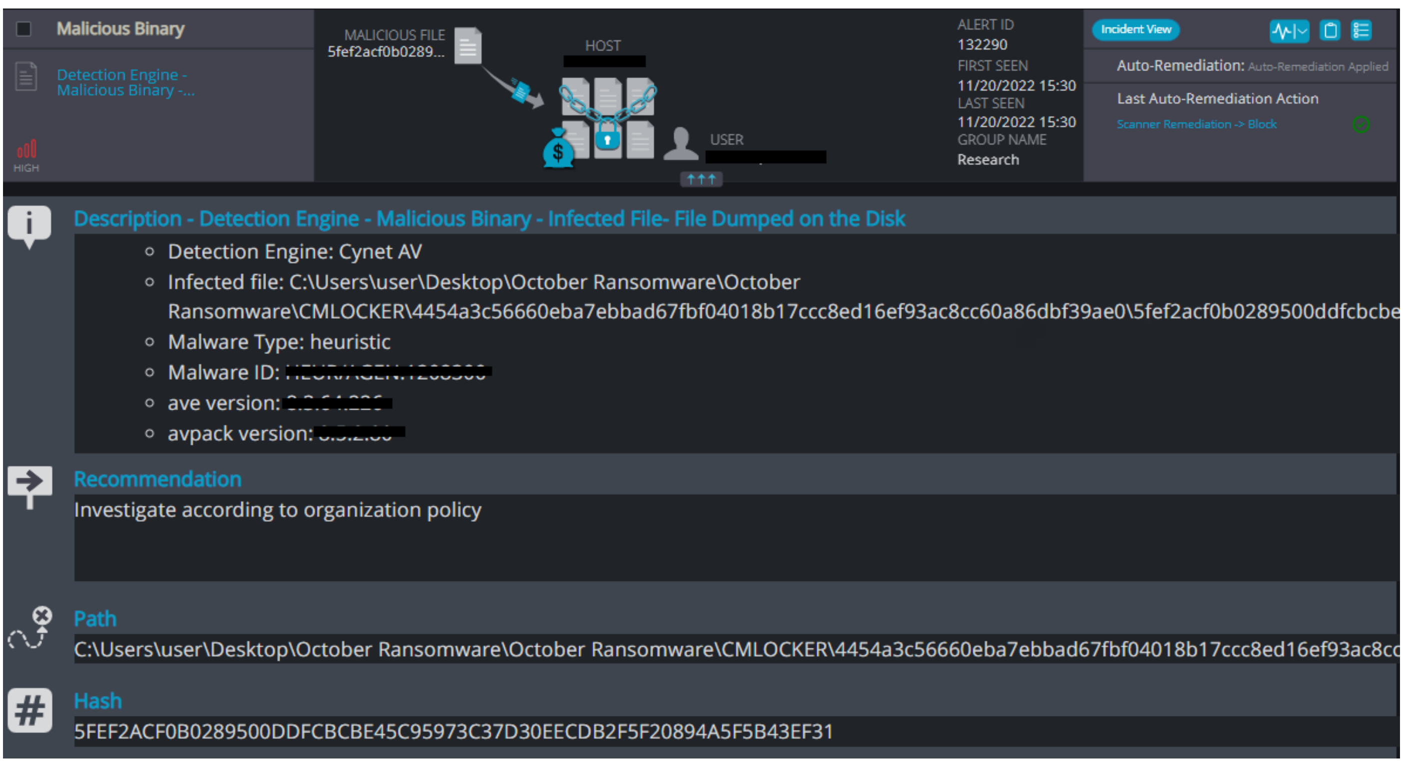
For poland we have BLIK

Orion Team

CMLOCKER Ransomware

- Observed since: 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .CMLOCKER
- Ransomware note: HELP_DECRYPT_YOUR_FILES.txt
- Sample hash: 5fef2acf0b0289500ddfcbcbe45c95973c37d30eecdb2f5f20894a5f5b43ef31

Cynet 360 AutoXDR™ Detections:


Malicious Binary
Detection Engine - Malicious Binary -...
HIGH
MALICIOUS FILE
5fef2acf0b0289...
HOST
USER
Incident View
Auto-Remediation: Auto-Remediation Applied
Last Auto-Remediation Action
Scanner Remediation -> Block

HOST [redacted]

USER [redacted]

ALERT ID
132290
FIRST SEEN
11/20/2022 15:30
LAST SEEN
11/20/2022 15:30
GROUP NAME
Research

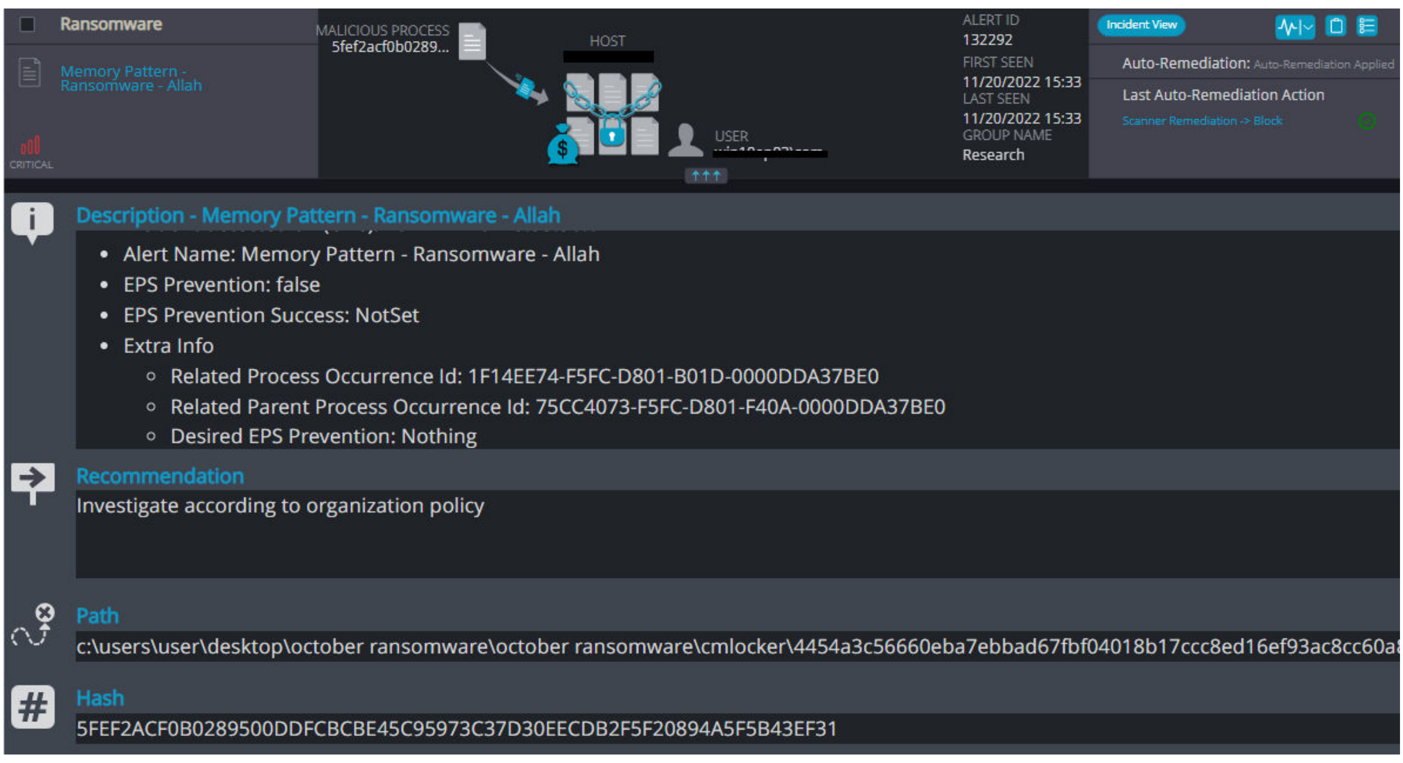
Description - Detection Engine - Malicious Binary - Infected File- File Dumped on the Disk

- Detection Engine: Cynet AV
- Infected file: C:\Users\user\Desktop\October Ransomware\October Ransomware\CMLOCKER\4454a3c56660eba7ebbad67fbf04018b17ccc8ed16ef93ac8cc60a86dbf39ae0\5fef2acf0b0289500ddfcbcbe
- Malware Type: heuristic
- Malware ID: [redacted]
- ave version: [redacted]
- avpack version: [redacted]

Recommendation
Investigate according to organization policy

Path
C:\Users\user\Desktop\October Ransomware\October Ransomware\CMLOCKER\4454a3c56660eba7ebbad67fbf04018b17ccc8ed16ef93ac8cc

Hash
5FEF2ACF0B0289500DDFCBCBE45C95973C37D30EECDB2F5F20894A5F5B43EF31


Ransomware
Memory Pattern - Ransomware - Allah
CRITICAL
MALICIOUS PROCESS
5fef2acf0b0289...
HOST
USER
Incident View
Auto-Remediation: Auto-Remediation Applied
Last Auto-Remediation Action
Scanner Remediation -> Block

HOST [redacted]

USER [redacted]

ALERT ID
132292
FIRST SEEN
11/20/2022 15:33
LAST SEEN
11/20/2022 15:33
GROUP NAME
Research

Description - Memory Pattern - Ransomware - Allah

- Alert Name: Memory Pattern - Ransomware - Allah
- EPS Prevention: false
- EPS Prevention Success: NotSet
- Extra Info
  - Related Process Occurrence Id: 1F14EE74-F5FC-D801-B01D-0000DDA37BE0
  - Related Parent Process Occurrence Id: 75CC4073-F5FC-D801-F40A-0000DDA37BE0
  - Desired EPS Prevention: Nothing

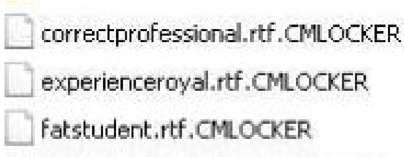
Recommendation
Investigate according to organization policy

Path
c:\users\user\desktop\october ransomware\october ransomware\cmlocker\4454a3c56660eba7ebbad67fbf04018b17ccc8ed16ef93ac8cc60a

Hash
5FEF2ACF0B0289500DDFCBCBE45C95973C37D30EECDB2F5F20894A5F5B43EF31

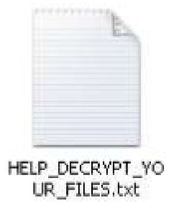
CMLOCKER Overview

CMLOCKER ransomware renames the encrypted files with .CMLOCKER in the extension **(screenshot has been taken from an outsource sandbox):**



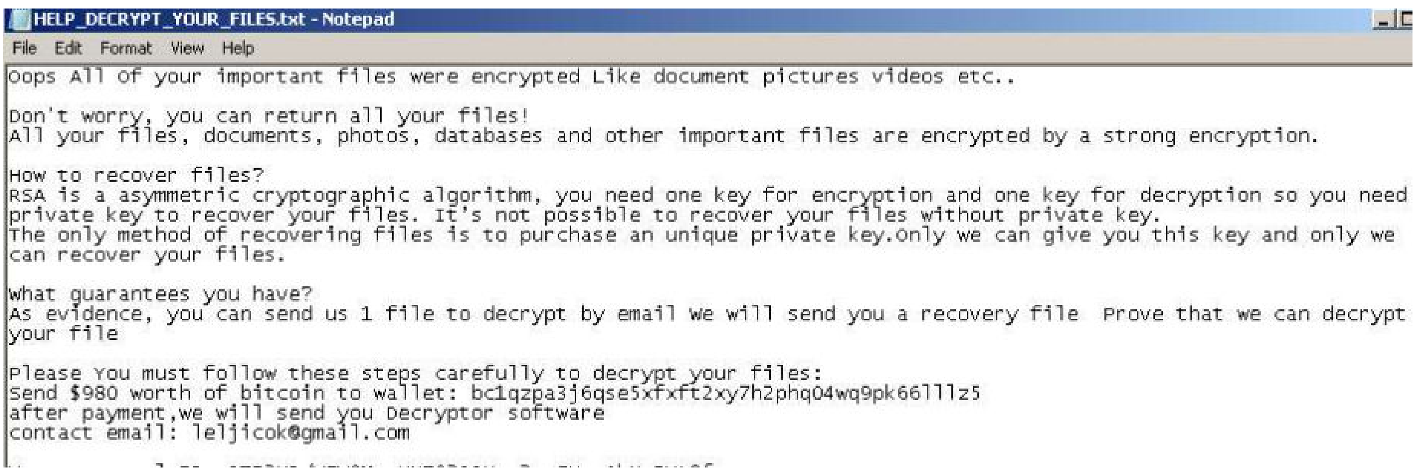
correctprofessional.rtf.CMLOCKER
experienceroyal.rtf.CMLOCKER
fatstudent.rtf.CMLOCKER

Once a computer's files have been encrypted and renamed, it drops a note named "HELP_DECRYPT_YOUR_FILES.txt" **(screenshot has been taken from an outsource sandbox):**



HELP_DECRYPT_YOUR_FILES.txt

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings and several attacker's links **(a screenshot has been taken from an outsource sandbox):**

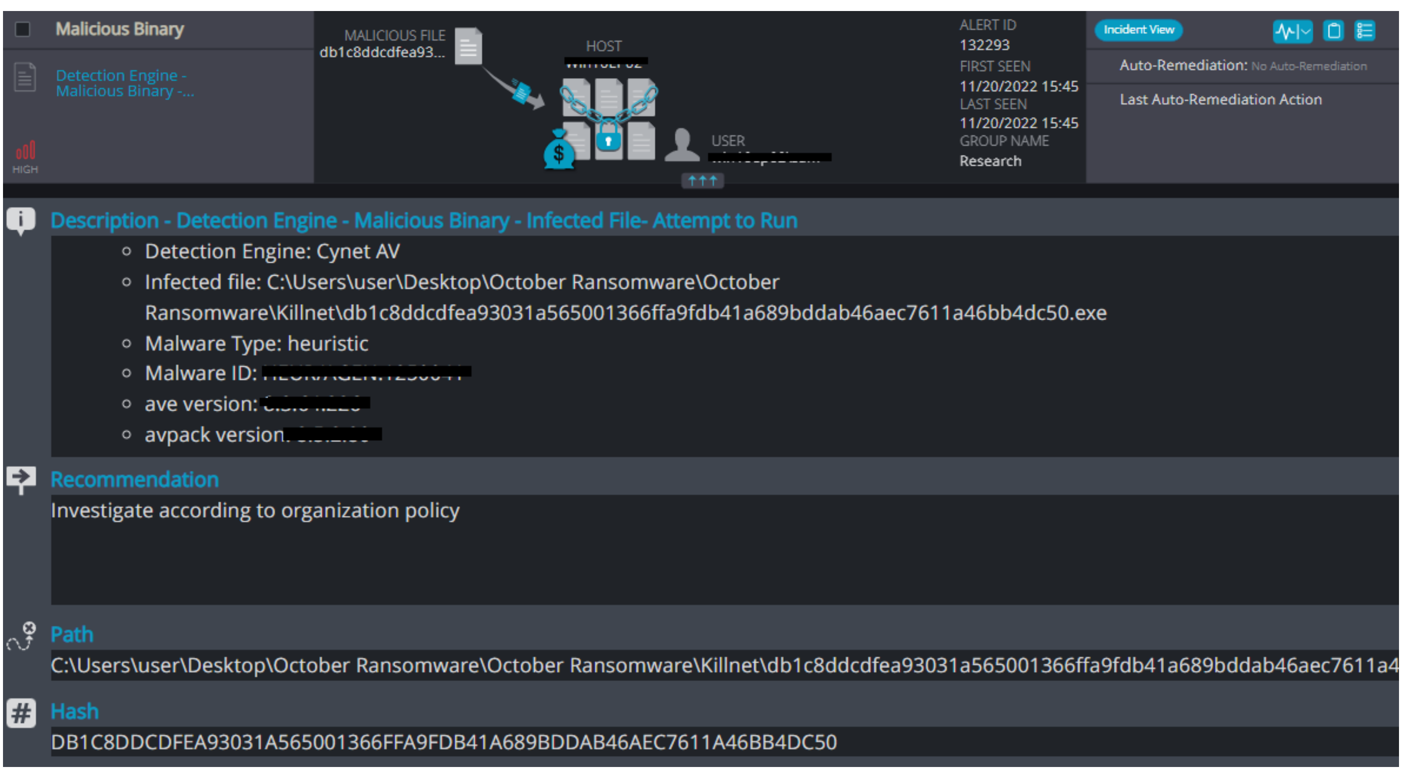

HELP_DECRYPT_YOUR_FILES.txt - Notepad
File Edit Format View Help

```
Oops All of your important files were encrypted Like document pictures videos etc..

Don't worry, you can return all your files!
All your files, documents, photos, databases and other important files are encrypted by a strong encryption.

How to recover files?
RSA is a asymmetric cryptographic algorithm, you need one key for encryption and one key for decryption so you need
private key to recover your files. It's not possible to recover your files without private key.
The only method of recovering files is to purchase an unique private key.Only we can give you this key and only we
can recover your files.

What guarantees you have?
As evidence, you can send us 1 file to decrypt by email We will send you a recovery file  Prove that we can decrypt
your file

Please You must follow these steps carefully to decrypt your files:
Send $980 worth of bitcoin to wallet: bc1qzpa3j6qse5xfxft2xy7h2phq04wq9pk66l1lz5
after payment,we will send you Decryptor software
contact email: leljicok@gmail.com
```

Killnet Ransomware

- Observed since: 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .killnet
- Ransomware note: Ru.txt
- Sample hash: db1c8ddcdfea93031a565001366ffa9fdb41a689bddab46aec7611a46bb4dc50

Cynet 360 AutoXDR™ Detections:



HOST [redacted]

USER [redacted]

ALERT ID
132293
FIRST SEEN
11/20/2022 15:45
LAST SEEN
11/20/2022 15:45
GROUP NAME
Research

Auto-Remediation: No Auto-Remediation

Last Auto-Remediation Action

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

- Detection Engine: Cynet AV
- Infected file: C:\Users\user\Desktop\October Ransomware\October Ransomware\Killnet\db1c8ddcdfea93031a565001366ffa9fdb41a689bddab46aec7611a46bb4dc50.exe
- Malware Type: heuristic
- Malware ID: [redacted]
- ave version: [redacted]
- avpack version [redacted]

Recommendation

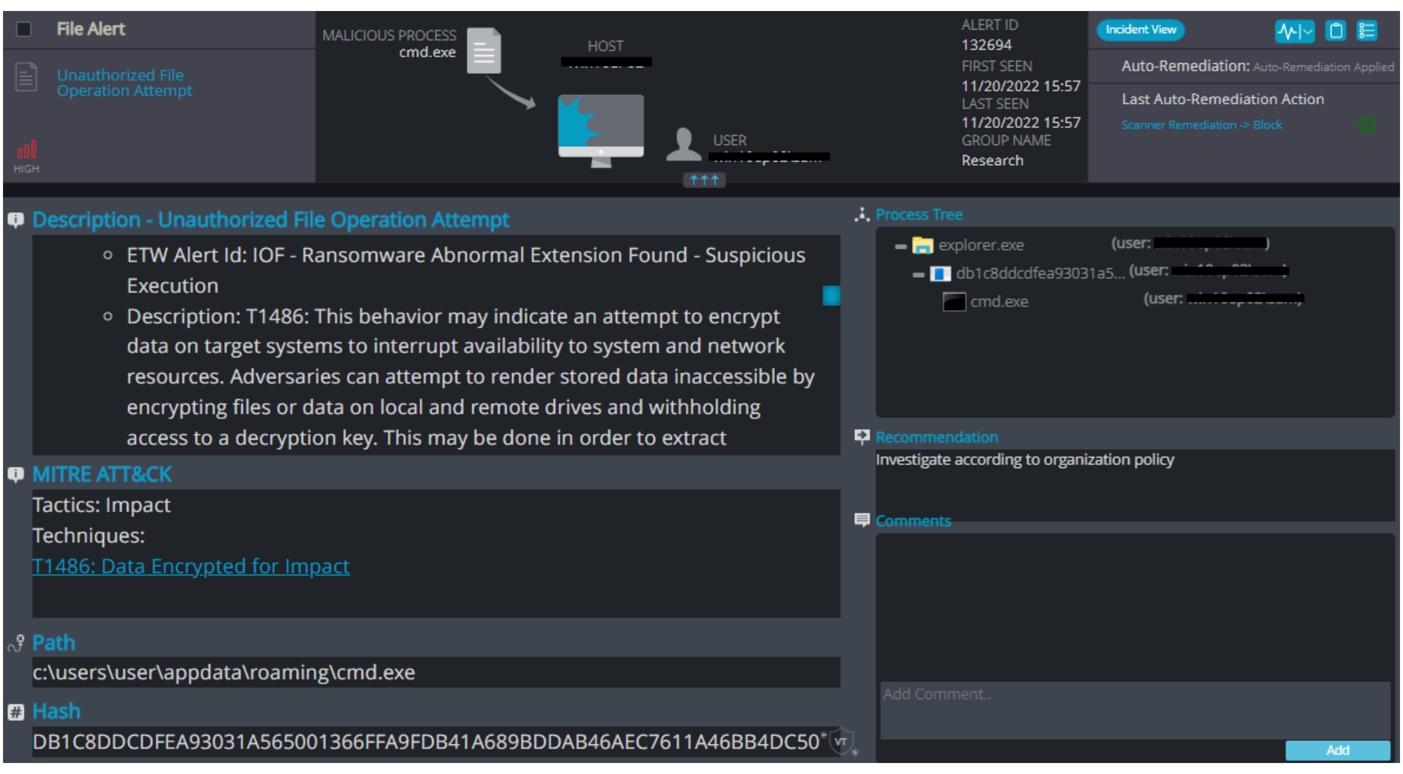
Investigate according to organization policy

Path

C:\Users\user\Desktop\October Ransomware\October Ransomware\Killnet\db1c8ddcdfea93031a565001366ffa9fdb41a689bddab46aec7611a4

Hash

DB1C8DDCDFEA93031A565001366FFA9FDB41A689BDDAB46AEC7611A46BB4DC50



HOST [redacted]

USER [redacted]

ALERT ID
132694
FIRST SEEN
11/20/2022 15:57
LAST SEEN
11/20/2022 15:57
GROUP NAME
Research

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Unauthorized File Operation Attempt

- ETW Alert Id: IOF - Ransomware Abnormal Extension Found - Suspicious Execution
- 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

MITRE ATT&CK

Tactics: Impact

Techniques:

T1486: Data Encrypted for Impact

Path

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

Hash

DB1C8DDCDFEA93031A565001366FFA9FDB41A689BDDAB46AEC7611A46BB4DC50

Process Tree

```
- explorer.exe            (user: [redacted])
  - db1c8ddcdfea93031a5... (user: [redacted])
      cmd.exe              (user: [redacted])
```

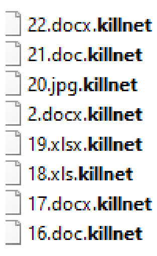
Recommendation

Investigate according to organization policy

Comments

Killnet Overview

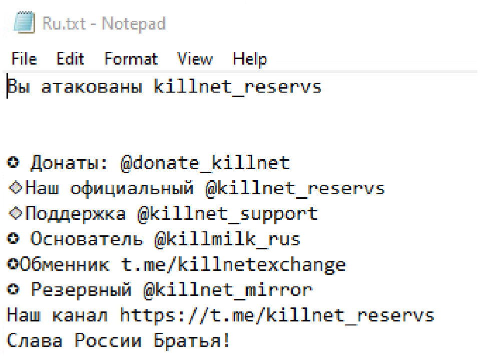
Killnet ransomware renames the encrypted files with .killnet in the extension:



```
22.docx.killnet
21.doc.killnet
20.jpg.killnet
2.docx.killnet
19.xlsx.killnet
18.xls.killnet
17.docx.killnet
16.doc.killnet
```

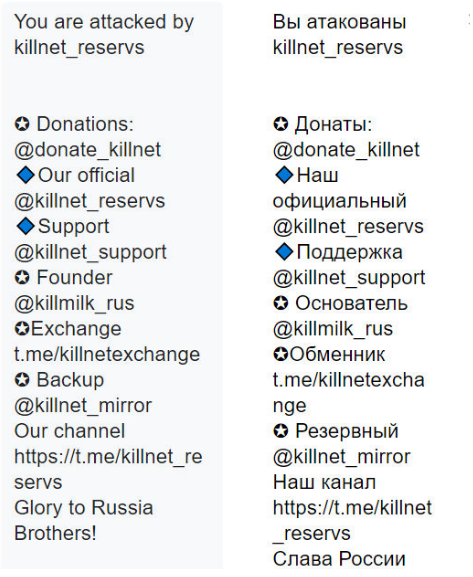
Once a computer's files have been encrypted and renamed, it drops a note named “Ru.txt”:

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



```
Вы атакованы killnet_reservs


✪ Донаты: @donate_killnet
◇Наш официальный @killnet_reservs
◇Поддержка @killnet_support
✪ Основатель @killmilk_rus
✪Обменник t.me/killnetexchange
✪ Резервный @killnet_mirror
Наш канал https://t.me/killnet_reservs
Слава России Братья!
```

Google Translate:



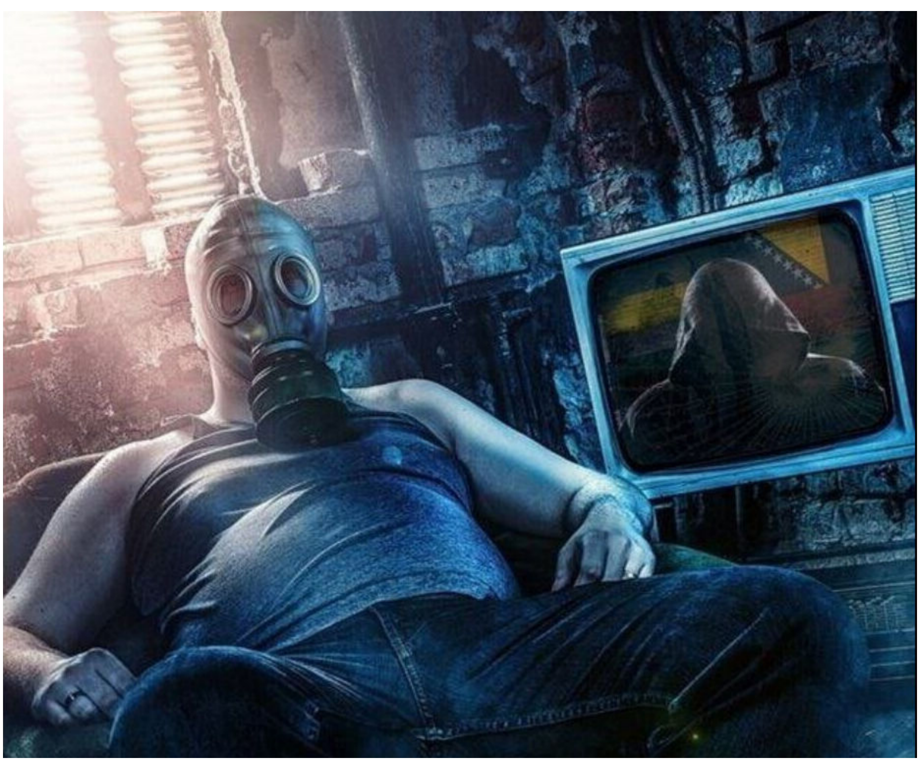
You are attacked by killnet_reservs

✪ Donations: @donate_killnet
◆Our official @killnet_reservs
◆Support @killnet_support
✪ Founder @killmilk_rus
✪Exchange t.me/killnetexchange
✪ Backup @killnet_mirror
Our channel https://t.me/killnet_reservs
Glory to Russia Brothers!

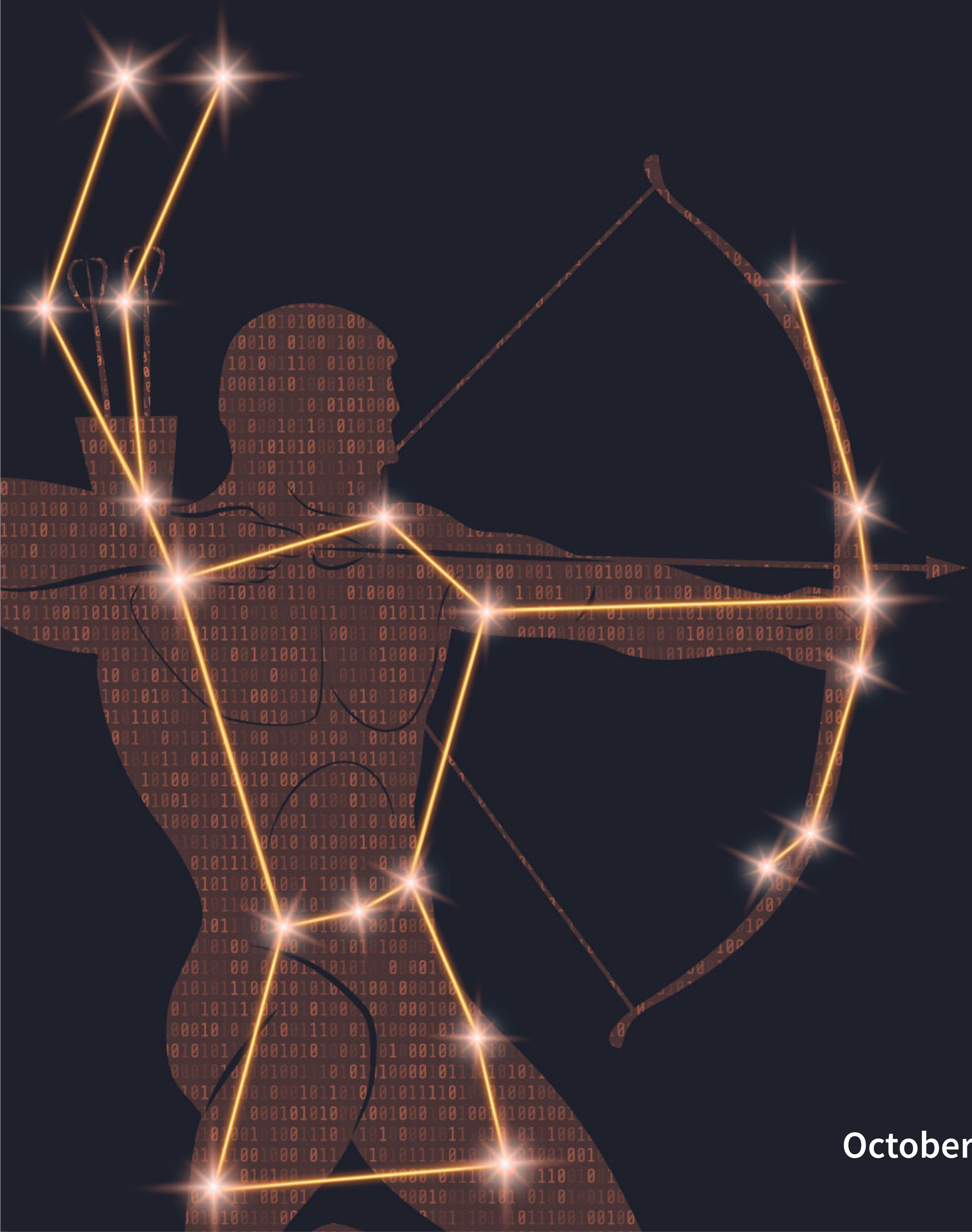
Вы атакованы killnet_reservs

✪ Донаты: @donate_killnet
◆Наш официальный @killnet_reservs
◆Поддержка @killnet_support
✪ Основатель @killmilk_rus
✪Обменник t.me/killnetexchange
✪ Резервный @killnet_mirror
Наш канал https://t.me/killnet_reservs
Слава России

The ransomware also changes the desktop wallpaper:



Thank you!



October, 2022