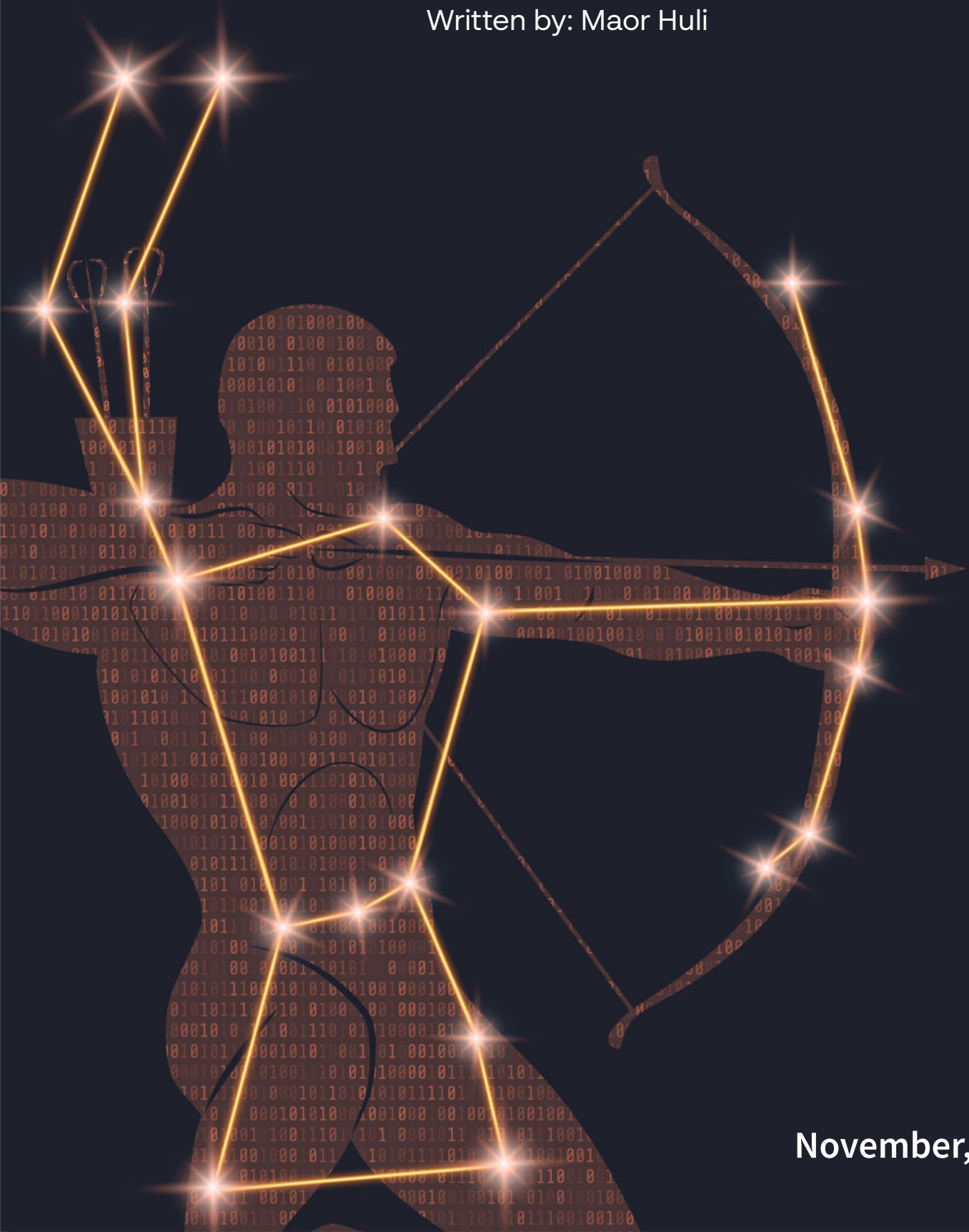


Orion Team

Monthly Ransomware Activity

Written by: Maor Huli



November, 2022



Contents

CrySpheRe	3
Inlock	6
Anon_by	7
Faust	8



Executive Summary

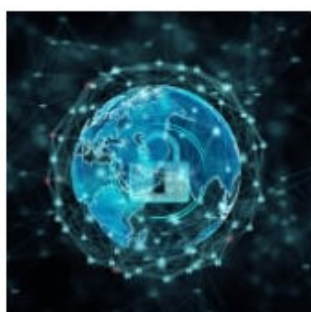
As an integral department in Cynet's research team, Orion works around the clock to track threat intelligence resources, analyze payloads, and automate labs to ensure that our customers are protected against the newest ransomware variants. In these monthly reports, Orion reviews the latest trends identified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



The Week in Ransomware - November 18th 2022 - Rising Operations

There have been some interesting developments in ransomware this week, with the arrest of a cybercrime ring leader and reports shedding light on two new, but up-and-coming, ransomware operations.

LAWRENCE ABRAMS NOVEMBER 18, 2022 05:13 PM 0



The Week in Ransomware - November 11th 2022 - LockBit feeling the heat

This 'Week in Ransomware' covers the last two weeks of ransomware news, with new information on attacks, arrests, data wipers, and reports shared by cybersecurity firms and researchers.

LAWRENCE ABRAMS NOVEMBER 11, 2022 05:25 PM 0

Orion Team



Cynet 360 AutoXDR™ VS Ransomware



- Observed since: Nov 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .CrySpheRe
- Ransomware note: КАК РАСШИФРОВАТЬ ФАЙЛЫ.txt
- Sample hash: 9680ddca296d16b58ceb381308e58509d73eafb92d884b4a5865dcb843c0a63

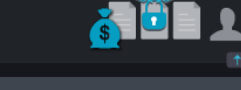
Malicious Binary		MALICIOUS FILE 9680ddca296d16...	HOST [REDACTED]	ALERT ID 144858	Incident View
Detection Engine - Malicious Binary ...				FIRST SEEN 12/11/2022 13:43 LAST SEEN 12/11/2022 13:43 GROUP NAME Research	Auto-Remediation: Auto-Remediation Applied Last Auto-Remediation Action Scanner Remediation -> Block
<p>Description - Detection Engine - Malicious Binary - Infected File- File Dumped on the Disk</p> <ul style="list-style-type: none"> Detection Engine: Cynet AV Infected file: C:\Users\user\Desktop\Nov ransomware\Nov ransomware\CrySpheRe\9680ddca296d16b58ceb381308e58509d73eafb92d884b4a5865dc843c0a63 Malware Type: trojan Malware ID: [REDACTED] ave version: [REDACTED] avpack version: [REDACTED] <p>Recommendation Investigate according to organization policy</p> <p>Path C:\Users\user\Desktop\Nov ransomware\Nov ransomware\CrySpheRe\9680ddca296d16b58ceb381308e58509d73eafb92d884b4a5865dc843c0a63</p> <p># Hash 9680DDCA296D16B58CEB381308E58509D73EAFBF92D884B4A5865DCB843C0A63</p>					

Ransomware

Ransomware Heuristic

CRITICAL

MALICIOUS PROCESS
9680ddca296d16...



ALERT ID
144913

FIRST SEEN
12/11/2022 13:51

LAST SEEN
12/11/2022 14:05

GROUP NAME
Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action
Scanner Remediation -> Block

Description - Ransomware Heuristic

- ETW Alert Id: Ransomware Heuristic
- Configuration Date (UTC): 2022-12-11 04:00:34
- Whitelist Configuration Date (UTC): 2022-12-07 07:19:23
- Detect PID of Ransomware: 9208
- Behavior Rule: 10 Decoy Files Renamed
- Description: 0
- Rename: \device\harddiskvolume2\ cynet ransom protection(don't delete)\bb\36.doc.cryosphere,\device\harddiskvolume2\ cynet

Recommendation

Investigate according to organization policy

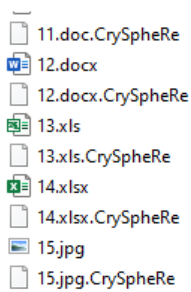
Path

c:\users\user\desktop\nov ransomware\nov ransomware\cryosphere\9680ddca296d16b58ceb381308e58509d73eafb92d884b4a5865dcb843c0a63

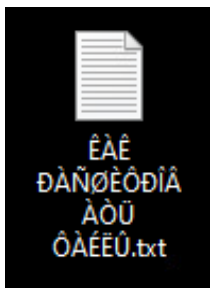
Hash

9680DDCA296D16B58CEB381308E58509D73EAFBF92D884B4A5865DCB843C0A63

CrySpheRe ransomware renames the encrypted files with .CrySpheRe in the extension:



Once a computer's files have been encrypted and renamed, it drops a note as "КАК РАСШИФРОВАТЬ ФАЙЛЫ.txt"(No Russian Language in the machine):



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

```
All of your files have been encrypted
Your computer was infected with a ransomware virus. Your files have been encrypted.
What can I do to get my files back? You can buy our special
decryption software, this software will allow you to recover all of your data and remove the
ransomware from your computer.The price for the software is $30.

Contact for buying decryption software: march20222021@proton.me
```


Inlock Ransomware

- Observed since: Nov 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .inlock
- Ransomware note: READ_IT.txt
- Sample hash: 96e48ea92e40ebe25e26aa769b38cbe27f26f2718d184a6ba2fd3bb900992ebd

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

HIGH

MALICIOUS FILE

96e48ea92e40eb...

HOST



ALERT ID

144859

FIRST SEEN

12/11/2022 13:43

LAST SEEN

12/13/2022 13:05

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\Nov ransomware\Nov ransomware\Inlock\96e48ea92e40ebe25e26aa769b38cbe27f26f2718d184a6ba2fd3bb900992ebd
- Malware Type: trojan
- Malware ID: TR/Trojan.Agent
- ave version: 0.0.0.0
- avpack version: 0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\Nov ransomware\Nov ransomware\Inlock\96e48ea92e40ebe25e26aa769b38cbe27f26f2718d184a6ba2fd3bb9009...

Hash

96E48EA92E40EBE25E26AA769B38CBE27F26F2718D184A6BA2FD3BB900992EBD

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

96e48ea92e40eb...

HOST



ALERT ID

148028

FIRST SEEN

12/13/2022 11:23

LAST SEEN

12/13/2022 11:23

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 - Abnormal Extension Found - Data Files
- Description: T1486: This behavior may indicate an attempt to encrypt data on target systems to interrupt availability to system and network resources. Adversaries can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted
- Process PID : 3848

MITRE ATT&CK

Tactics: Impact

Techniques: T1486: Data Encrypted for Impact

Path

c:\users\user\Desktop\nov ransomware\nov ransomware\inlock\96e48ea92e40ebe25e26aa769b38cbe27f26f2718d184a6ba2fd3bb900992e...

Hash

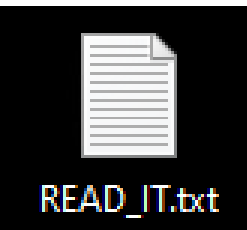
96E48EA92E40EBE25E26AA769B38CBE27F26F2718D184A6BA2FD3BB900992EBD

Inlock Overview

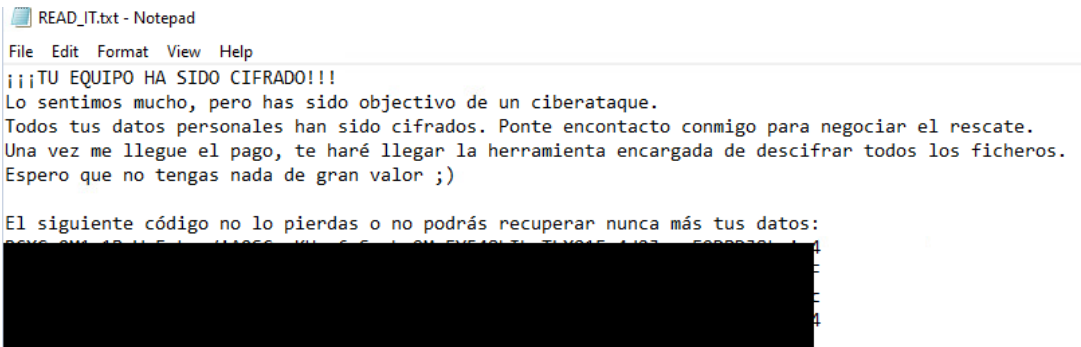
Inlock ransomware renames the encrypted files with .inlock in the extension:

- setup.log.inlock
- utmp.inlock
- CBroker.log.inlock
- ClickToRunPackageLocker.inlock
- 12.docx.inlock
- pyc.ico.inlock
- abc.pyo.inlock
- UserDeploymentConfiguration.xml.inlock
- 353be8f91891a6a5761b9ac157fa2ff1.cab.inlock
- 47133212c2f5ccf49392d7762293a075.cab.inlock

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



The ransomware note contains general information, and warnings, seemingly in Spanish:



After Translation:

The attacker says the decryption key will be sent once the payment arrives.

YOUR COMPUTER HAS BEEN ENCRYPTED!!!
We are very sorry, but you have been the target of a cyber attack.
All your personal data has been encrypted. Get in touch with me to negotiate the ransom.
Once the payment arrives, I will send you the tool in charge of decrypting all the files.
I hope you don't have anything of great value ;)|

Anon_by Ransomware

- Observed since: Nov 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .anon_by
- Ransomware note: anon_by.txt
- Sample hash: 057824bbb1dca42df1af0cacde596f8a5d3bbf09a71bdbee5d2b48168b533e35

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

HIGH

MALICIOUS FILE

057824bbb1dca4...

HOST

USER

ALERT ID

144857

FIRST SEEN

12/11/2022 13:43

LAST SEEN

12/13/2022 13:05

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\Nov ransomware\Nov ransomware\Anon_by\057824bbb1dca42df1af0cacde596f8a5d3bbf09a71bdbee5d2b48168b533e35
- Malware Type: heuristic
- Malware ID: HEUR/ANON_BY.200011
- ave version: 0.0.0.0
- avpack version: 0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\Nov ransomware\Nov ransomware\Anon_by\057824bbb1dca42df1af0cacde596f8a5d3bbf09a71bdbee5d2b48168b5...

Hash

057824BBB1DCA42DF1AF0CACDE596F8A5D3BBF09A71BDBEE5D2B48168B533E35

File Alert

Process Monitoring

HIGH

MALICIOUS PROCESS

bcdedit.exe

HOST

USER

ALERT ID

132175

FIRST SEEN

11/20/2022 15:21

LAST SEEN

12/13/2022 12:26

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Process Monitoring

- ETW Alert Id: CyAlert Heuristic Activity - Disable System Recovery
- Description: T1490: Adversaries may 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
- mechanism: PH NG
- Process PID : 18352
- Process Path : c:\windows\system32\bcdedit.exe

MITRE ATT&CK

Tactics: Execution

Techniques:

T1490: Inhibit System Recovery

Path

c:\windows\system32\bcdedit.exe

Hash

1EE229900C128119A122F9A7B3FF8CA2AB35154B314FC6B37CDA6CE041E4277D

Process Tree

- fivemanager.exe (user: ...)
- cmd.exe (user: ...)
- bcdedit.exe (user: ...)

Recommendation

Investigate according to organization policy

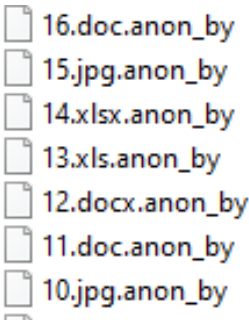
Comments

Add Comment...

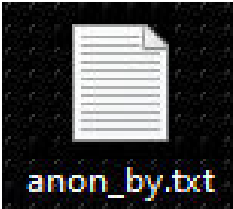
Add

Anon_by Overview

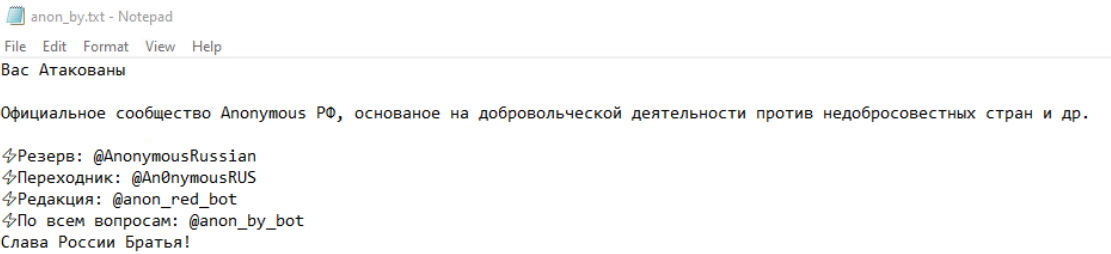
Anon_by ransomware renames the encrypted files with .anon_by in the extension:



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



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



Translated:

you are attacked

The official Anonymous RF community, based on volunteering against unscrupulous countries, etc.

⚡Reserve: @AnonymousRussian
⚡Adapter: @An0nymousRUS
⚡Editorial: @anon_red_bot
⚡For all questions: @anon_by_bot
Glory to Russian Brothers!]

Faust Ransomware

- Observed since: Nov 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .faust
- Ransomware note: info.txt | .hta
- Sample hash: 0385dd2419adf0fe1a1e5d5ed28aaecbceb1411010fb06a1b0798d84eca4732e

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary ~...

MALICIOUS FILE

0385dd2419adf0...

HOST

ALERT ID

144860

FIRST SEEN

12/11/2022 13:43

LAST SEEN

12/13/2022 11:42

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\Nov ransomware\Nov ransomware\Faust\0385dd2419adf0fe1a1e5d5ed28aaecbceb1411010fb06a1b0798d84eca4732e

Malware Type: trojan

Malware ID: [REDACTED]

ave version: [REDACTED]

avpack version: [REDACTED]

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\Nov ransomware\Nov ransomware\Faust\0385dd2419adf0fe1a1e5d5ed28aaecbceb1411010fb06a1b0798d84eca...

Hash

0385DD2419ADF0FE1A1E5D5ED28AAECBCEB1411010FB06A1B0798D84ECA4732E

Malicious Binary

Malicious Binary

MALICIOUS PROCESS

0385dd2419adf0...

HOST

ALERT ID

149444

FIRST SEEN

12/13/2022 12:02

LAST SEEN

12/13/2022 12:02

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\nov ransomware\nov ransomware\faust\0385dd2419adf0fe1a1e5d5ed28aaecbceb1411010fb06a1b0798d84eca4732e.exe

Process Fuzzy Hash: 768:1vrNNeRBI5JFTXqwXrkgrn/9/HiDKGwRj4RcTdyH4pYT3nPKVU1E5mGF9rLG:nNeRBI5PT/rx1mzwRMSTdLpJ5XPrL

Known Process Fuzzy Hash: 768:xvrNNeRBI5JFTXqwXrkgrn/9/HiDKGwRj4RcTdyH4pYT3nPKVU1EyjeZKU+McPsY:LNNeRBI5PT/rx1mzwRMSTdLpJyxiuo3

Recommendation

Investigate according to organization policy

Path

c:\users\user\desktop\nov ransomware\nov ransomware\faust\0385dd2419adf0fe1a1e5d5ed28aaecbceb1411010fb06a1b0798d84eca473...

Hash

0385DD2419ADF0FE1A1E5D5ED28AAECBCEB1411010FB06A1B0798D84ECA4732E

Faust Overview

Faust ransomware renames the encrypted files with the attacker's contact email and .faust in the extension:

- 21.doc.id[E07BA3DD-3421].[gardex_recofast@zohomail.eu].faust
- unsupported_filters.vbs.id[E07BA3DD-3421].[gardex_recofast@zohomail.eu].faust
- unins000.dat.id[E07BA3DD-3421].[gardex_recofast@zohomail.eu].faust
- 2.docx.id[E07BA3DD-3421].[gardex_recofast@zohomail.eu].faust
- 19.xlsx.id[E07BA3DD-3421].[gardex_recofast@zohomail.eu].faust
- string_scan.vbs.id[E07BA3DD-3421].[gardex_recofast@zohomail.eu].faust
- README.txt.id[E07BA3DD-3421].[gardex_recofast@zohomail.eu].faust

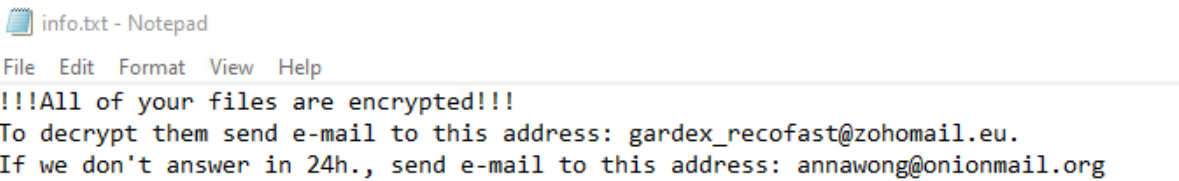
Once a computer’s files have been encrypted and renamed, it drops a note named “info.txt”:



And opens the note as a .hta file:



Upon execution, it immediately encrypts the endpoint. Then, after a while (approximately 15 minutes), it drops the ransomware note. The ransomware note contains general information and the attacker’s contact information:



The hta file contains additional information, along with the general information in the text file. It also contains information on a free decryption option, how to buy bitcoins, and generic warnings:



Thank you!



November, 2022