

Orion Team

Monthly Ransomware Activity

Written by: Maor Huli



May, 2022



Contents

Executive Summary 3

Odaku 5

Kekpop 6

Japan 7

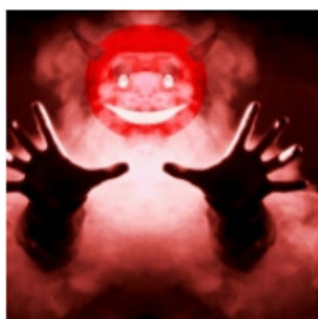
EarthGrass 8

CryptBIT 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 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 - May 20th 2022 - Another one bites the dust

Ransomware attacks continue to slow down, likely due to the invasion of Ukraine, instability in the region, and subsequent worldwide sanctions against Russia.

LAWRENCE ABRAMS MAY 20, 2022 08:08 PM 0



The Week in Ransomware - May 13th 2022 - A National Emergency

While ransomware attacks have slowed during Russia's invasion of Ukraine and the subsequent sanctions, the malware threat continues to affect organizations worldwide.

LAWRENCE ABRAMS MAY 13, 2022 04:58 PM 0



The Week in Ransomware - May 6th 2022 - An evolving landscape

Ransomware operations continue to evolve, with new groups appearing and others quietly shutting down their operations or rebranding as new groups.

LAWRENCE ABRAMS MAY 06, 2022 06:27 PM 0

Orion Team



Cynet 360 AutoXDR™ VS Ransomware



Odaku Ransomware

- Observed since: Late 2021
- Ransomware encryption method: RSA + AES.
- Ransomware extension: .[4 random characters]
- Ransomware note: read_it.txt
- Sample hash: d6799d0d74814958c4821509b0c4c83482f91d927d2d4ab8b53ce98146a0cacc

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary -...

MALICIOUS FILE

d6799d0d748149...

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

77704

FIRST SEEN

06/14/2022 12:31

LAST SEEN

06/14/2022 12:31

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\May Ransomware\May Ransomware\Odaku\d6799d0d74814958c4821509b0c4c83482f91d927d2d4ab8b53ce98146a0cacc

Malware Type: trojan

Malware ID: TR/ATRAPS.Gen

ave version: 0.0.0.0

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\May Ransomware\May Ransomware\Odaku\d6799d0d74814958c4821...

Hash

D6799D0D74814958C4821509B0C4C83482F91D927D2D4AB8B53CE98146A0CACC

Process Tree

explorer.exe (user: win10ep01\sam)

winlogon.exe (user: win10ep01\sam)

d6799d0d74814958c4821509b0c4c83482f91d927d2d4ab8b53ce98146a0cacc.exe (user: win10ep01\sam)

Comments

File Alert

Process Monitoring

MALICIOUS PROCESS

svchost.exe

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

23197

FIRST SEEN

02/08/2022 16:09

LAST SEEN

06/14/2022 12:34

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Process Monitoring

Detection Time Local: 2022-06-14 05:34:00

Alert Origin: DRIVER

ETW Alert Id: CyAlert Heuristic Activity - Masquerading Invalid Critical System File Path

Description: T1036.005: This behavior may indicate that an attempt was made to match or approximate the name or location of legitimate files when naming or placing their files. This is done for the sake of evading defenses and observation. This may be done by placing an executable in a commonly trusted directory or giving it the name of a legitimate trusted program.

MITRE ATT&CK

Tactics: Defense Evasion

Techniques: T1036.005: Masquerading: Match Legitimate Name or Location

Path

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

Hash

B103FC649787EB1F6121DF8174D0F16AAAC736FB53F5F078D312871189285956

Process Tree

explorer.exe (user: win10ep01\sam)

chrome.exe (user: win10ep01\sam)

svchost.exe (user: win10ep01\sam)

Recommendations

Investigate according to organization policy

Comments

Odaku Overview

Odaku ransomware is supposed to rename the encrypted files with .[4 random chars] in the extension but no encryption was observed.

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



Upon execution, it immediately copies itself to the folder “C:\Users\user\AppData\Roaming” with the name of “svchost.exe”, the icon of Netflix, and popup the ransomware note, the ransomware note contains only the attacker crypto-currency wallet and the telegram name (demands 25\$ in bitcoins):

This PC > Local Disk (C:) > Users > user > AppData > Roaming				
Name	Date modified	Type	Size	
Adobe	2/23/2020 2:11 AM	File folder		
dnSpy	8/9/2021 6:21 AM	File folder		
Everything	3/1/2022 2:13 AM	File folder		
JetBrains	8/7/2021 8:25 AM	File folder		
Microsoft	8/12/2021 5:18 AM	File folder		
Notepad++	8/7/2021 8:40 AM	File folder		
npm	8/7/2021 9:16 AM	File folder		
npm-cache	8/7/2021 9:16 AM	File folder		
NuGet	8/7/2021 7:26 AM	File folder		
Process Hacker 2	8/8/2021 5:45 AM	File folder		
Sun	8/7/2021 8:27 AM	File folder		
Teams	8/12/2021 5:18 AM	File folder		
Visual Studio Setup	8/7/2021 7:51 AM	File folder		
WinRAR	10/26/2021 2:43 AM	File folder		
read_it.txt	6/14/2022 5:34 AM	Text Document	1 KB	
svchost.exe	6/14/2022 4:37 AM	Application	32 KB	

```
read_it.txt - Notepad
File Edit Format View Help
hi my name is odaku
send me here 25$ btc

wallet:
bc1qr2vvldtzagpw6f2utk58c18xw5ppm3mc7wu0zr

send me screenshot here :

telegram : @odaku

Then I will send you the key .
```


Kekpop Ransomware

- Observed since: May 2022
- Ransomware encryption method: RSA + AES.
- Ransomware extension: .kektop
- Ransomware note: not exist
- Sample hash: 3560efa18b48f0e707f190c7f244be2a5080829d6710e8aee4c7e8767314b808

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

MALICIOUS FILE

kektop.bat

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

77740

FIRST SEEN

06/14/2022 12:52

LAST SEEN

06/14/2022 12:52

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\AppData\LocalTemp\IXP000.TMP\kektop.bat

Malware Type: trojan

Malware ID: TR/PSW.Stealer.BK

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\AppData\LocalTemp\IXP000.TMP\kektop.bat

Hash

EA81248FDDBF9080018845BF7862B9CEB8AB942526C1ADCF20030F043C57AD99

File Alert

Unauthorized File Operation Attempt

MALICIOUS PROCESS

cmd.exe

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

78837

FIRST SEEN

06/14/2022 13:07

LAST SEEN

06/14/2022 13:07

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Unauthorized File Operation Attempt

Volume Attributes: Boot

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

MITRE ATT&CK

Tactics: Impact

Techniques: T1486: Data Encrypted for Impact

Path

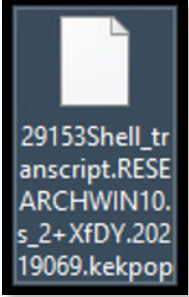
c:\windows\system32\cmd.exe

Hash

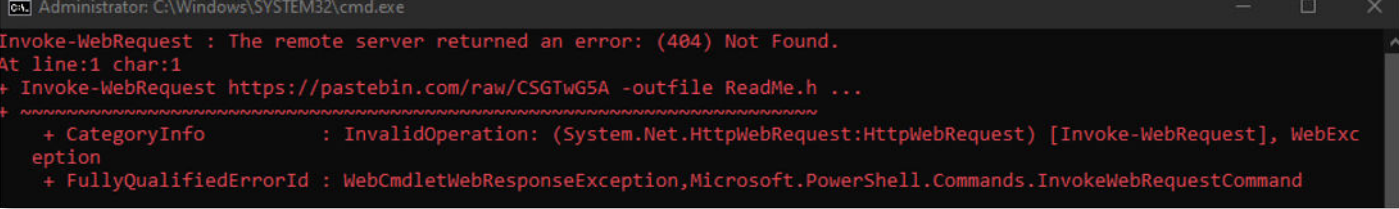
FF79D3C4A0B7EB191783C323AB8363EBD1FD10BE58D8BCC96B07067743CA81D5

Kekpop Overview

Kekpop ransomware renames the encrypted files with .kektop in the extension:



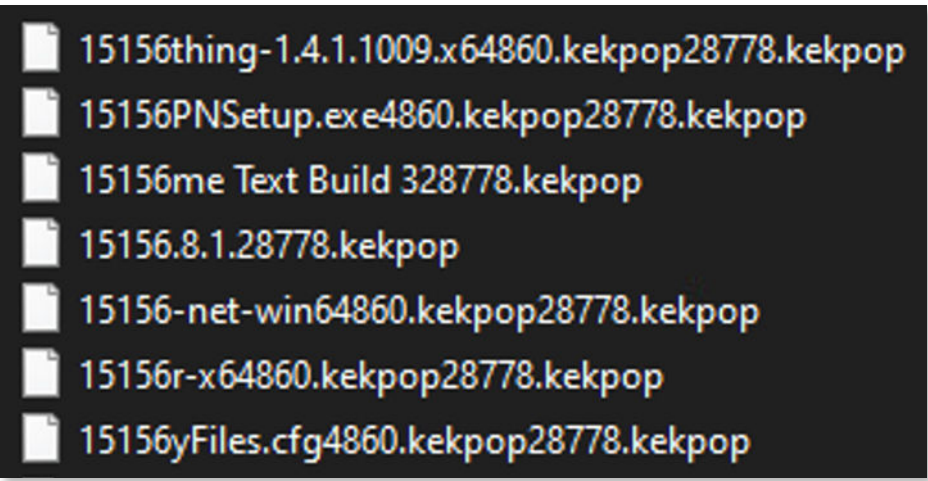
Once a computer’s files have been encrypted and renamed, it attempts to drop the ransomware note that is supposed to be ReadMe.html but since it’s using Pastebin to download the note, Pastebin blocked the account and it cannot be downloaded, which means, no encryption key or how to contact the attacker:



Upon execution, it immediately encrypts the endpoint using batch scripts:

Processes	Services	Network	Disk	
Name	PID	CPU	I/O total ...	Private b...
3560efa18b48f0e707f190...	8744			1.78 MB
cmd.exe	7512			9.7 MB
conhost.exe	5144			2.35 MB
cmd.exe	6224			2.38 MB
conhost.exe	1464			2.32 MB
cmd.exe	6236			2.07 MB
conhost.exe	1040			2.56 MB
cmd.exe	8368			2.06 MB
conhost.exe	1612			2.54 MB
cmd.exe	2876			2.07 MB
conhost.exe	8504			2.61 MB
cmd.exe	8608			2.07 MB
conhost.exe	7272			2.6 MB
cmd.exe	8000			2.07 MB
conhost.exe	5944			2.6 MB
cmd.exe	6344			2.08 MB
conhost.exe	4620			2.59 MB
cmd.exe	2700			2.07 MB
conhost.exe	3852			2.59 MB
cmd.exe	3012			2.07 MB
conhost.exe	7188			2.59 MB
cmd.exe	7432			2.07 MB
conhost.exe	4588			2.57 MB
cmd.exe	1632			2.07 MB
conhost.exe	1852			2.61 MB
cmd.exe	5860			2.06 MB
conhost.exe	2004			2.61 MB
cmd.exe	1316			2.08 MB
conhost.exe	7316			2.59 MB
cmd.exe	6776			2.07 MB
conhost.exe	8292			2.63 MB
cmd.exe	8464			2.07 MB
conhost.exe	9104			2.6 MB
cmd.exe	6632			2.06 MB
conhost.exe	8920			2.55 MB

PU Usage: 3.58% Physical memory: 3.61 GB (30.05%) Processes: 178



Japan Ransomware

- Observed since: May 2022
- Ransomware encryption method: AES + RSA.
- Ransomware extension: .japan
- Ransomware note: how to decrypt.txt
- Sample hash: 4089e7b0a0469bd5877c830f962f8243dc1311349271e45e9b15cd6d97e0a2ea

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

MALICIOUS FILE

4089e7b0a0469b...

HOST

Win10EP01

ALERT ID

77701

Incident View

FIRST SEEN

06/14/2022 12:31

LAST SEEN

06/14/2022 12:31

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\May Ransomware\May Ransomware\Japan\4089e7b0a0469bd5877c830f962f8243dc1311349271e45e9b15cd6d97e0a2ea

Malware Type: trojan

Malware ID: TR/Ransom.tztsm

ave version: 8.3.64.160

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\May Ransomware\May Ransomware\Japan\4089e7b0a0469bd5877c83...

Hash

4089E7B0A0469BD5877C830F962F8243DC1311349271E45E9B15CD6D97E0A2EA

Malicious Binary

Threat Intelligence Detection Malicious...

MALICIOUS PROCESS

4089e7b0a0469b...

HOST

FTest13

ALERT ID

68984

Incident View

FIRST SEEN

06/10/2022 10:30

LAST SEEN

06/10/2022 10:30

GROUP NAME

Manually Ins...

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Threat Intelligence Detection Malicious Binary

Detection Time Local: 2022-06-10 03:30:58.225

Process Details

Process SHA256:

4089E7B0A0469BD5877C830F962F8243DC1311349271E45E9B15CD6D97E0A2EA

Process PID:

8404

Process Path:

c:\users\user\desktop\4089e7b0a0469bd5877c830f962f8243dc1311349271e45e9b15cd...

Recommendation

Investigate according to organization policy

Path

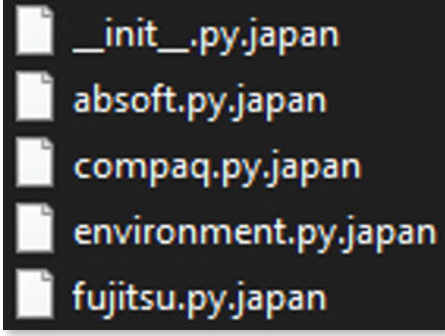
c:\users\user\desktop\4089e7b0a0469bd5877c830f962f8243dc1311349271e45e9b15cd6d97e...

Hash

4089E7B0A0469BD5877C830F962F8243DC1311349271E45E9B15CD6D97E0A2EA

Japan Overview

Japan ransomware renames the encrypted files with .japan in the extension:



Once a computer’s files have been encrypted and renamed, it drops a note named how to decrypt.txt:



Once executed the dropped file it copies the file to the folder “C:\Users\user\AppData\Roaming” and changes the name to “svchost.exe” and it immediately encrypts the endpoint and drops the ransomware note. The ransomware note is written in Vietnamese:



After translating, the ransom note contains the attacker's BTC address and “guarantees” only for 4 days for the decryption (demand 2000\$ in bitcoin):

Hii!!

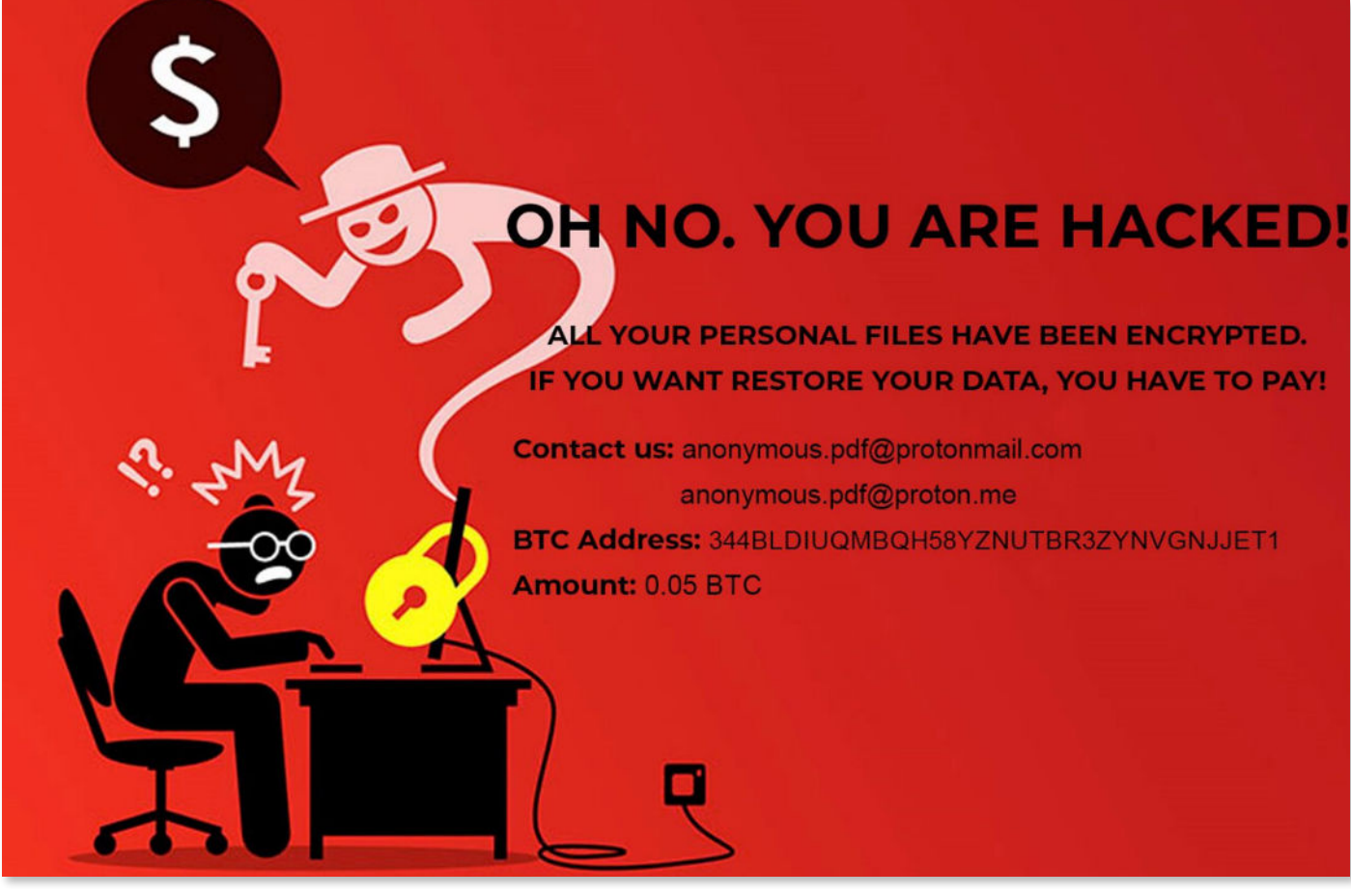
We have discovered a security hole at your server.
And not. All your data has been successfully encrypted by us to keep them secure.
Rest assured, your data can still be reopened thanks to a private key and unlocking software.
You have 4 days to be able to unlock your data again. After 4 days, the private keys will expire and you will not be able to unlock them. So do it quickly.
We accept payment via bitcoin for 2000 USD. After receiving the receipt of BTC receipt from the wallet, we will send the private and unlock software to you.

You can contact us by email: anonymous.pdf@protonmail.com
BTC Address: 344BLDiUqMbqh58yZnuTBR3ZYnVGnjjEt1
Amount: 0.05 BTC

We will only guarantee decrypted data from 4 days and beyond. Will not be.

You must not shut down your computer, or restart it, update it, or use antivirus software. If used, the data key will be lost and cannot be recovered.

In the end, it also changes the background:





EarthGrass Ransomware

- Observed since: May 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: . 34r7hGr455
- Ransomware note: Read ME (Decryptor).txt
- Sample hash: 248cdaf6abdf84a90acba1a1ae86a47644568f46aa893bc747c9cddfaf2613bb

Cynet 360 AutoXDR™ Detections:

File Alert

Unauthorized File Operation Attempt

HIGH

MALICIOUS PROCESS

windows anti-m...

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

79220

FIRST SEEN

06/19/2022 08:39

LAST SEEN

06/19/2022 08:39

GROUP NAME

Research

Incident View

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Unauthorized File Operation Attempt

Volume Attributes: Boot

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

MITRE ATT&CK

Tactics: Impact

Techniques: T1486: Data Encrypted for Impact

Path

c:\users\user\appdata\roaming\windows anti-malware servise.exe

Hash

248CDAF6ABDF84A90ACBA1A1AE86A47644568F46AA893BC747C9CDDFAF2613BB

Process Tree

explorer.exe (user: win10ep01\sam)

248cdaf6abdf84a90acba1a1ae86a47644568f46aa893bc747c9cddfaf2613bb (user: win10ep01\sam)

windows anti-malware servise.exe (user: win10ep01\sam)

Recommendation

Investigate according to organization policy

Comments

Ransomware

Memory Pattern - Ransomware - Fonix v6

CRITICAL

MALICIOUS PROCESS

windows anti-m...

HOST

Win10EP01

USER

win10ep01\sam

ALERT ID

79177

FIRST SEEN

06/19/2022 08:39

LAST SEEN

06/19/2022 08:39

GROUP NAME

Research

Incident View

Auto-Remediation: No Auto-Remediation

Last Auto-Remediation Action

Description - Memory Pattern - Ransomware - Fonix v6

Signature Name: Memory Pattern - Ransomware - Fonix v6

Matched Memory Area Bounds : From - 0x862000 - To - 0xa0f000 - Area Size - 1757184

Matched Memory Area Info : Type - IMAGE, AllocationBase - 0x860000, AllocationProtect - WCX, Protect - RWX

Pattern(1) Offset [Address]: 1753042 [0xa0dfd2]

Pattern(1) Distance From Previous Pattern Start: 1753042

Pattern(1) Dump Captured From: 1748992 [0xa0d000] - To - 1757184 [0xa0f000]

Recommendation

Investigate according to organization policy

Path

c:\users\user\appdata\roaming\windows anti-malware servise.exe

Hash

248CDAF6ABDF84A90ACBA1A1AE86A47644568F46AA893BC747C9CDDFAF2613BB

Process Tree

explorer.exe (user: win10ep01\sam)

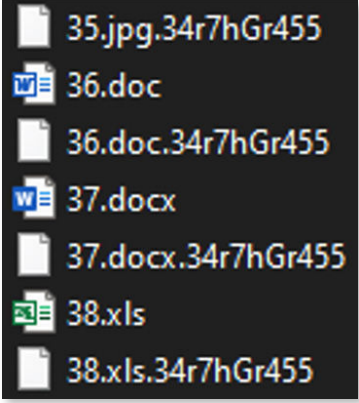
248cdaf6abdf84a90acba1a1ae86a47644568f46aa893bc747c9cddfaf2613bb (user: win10ep01\sam)

windows anti-malware servise.exe (user: win10ep01\sam)

Comments

EarthGrass Overview

EarthGrass ransomware renames the encrypted files with .34r7hGr455in the extension:



Once a computer’s files have been encrypted and renamed, it drops a note as Read ME (Decryptor).txt:



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



CryptBIT Ransomware

- Observed since: May 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .cryptbit
- Ransomware note: CryptBIT-restore-files.txt
- Sample hash: edf4a4444890ea957099f94822c9fa5b859ade205ea5a5d187c1e6f0b8a6cb6d

Cynet 360 AutoXDR™ Detections:

Malicious Binary

Detection Engine - Malicious Binary - ...

MALICIOUS FILE

edf4a4444890ea...

HOST

Win10EP01

ALERT ID

79349

Incident View

Auto-Remediation: Auto-Remediation Applied

First Seen

06/19/2022 08:47

Last Seen

06/19/2022 08:47

GROUP NAME

Research

USER

win10ep01\sam

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

Detection Engine: Cynet AV

Infected file: C:\Users\user\Desktop\May Ransomware\May Ransomware\CryptBIT\edf4a4444890ea957099f94822c9fa5b859ade205ea5a5d187c1e6f0b8a6cb6d

Malware Type: heuristic

Malware ID: HEUR/AGEN.1250041

ave version: 8.3.64.160

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Desktop\May Ransomware\May Ransomware\CryptBIT\edf4a4444890ea957099f...

Hash

EDF4A4444890EA957099F94822C9FA5B859ADE205EA5A5D187C1E6F0B8A6CB6D

Process Tree

explorer.exe

winlogon.exe

edf4a4444890ea957099f94822c9fa5b859ade205ea5a5d187c1e6f0b8a6cb6d

Comments

Add Comments...

Add

Malicious Binary

Malicious Binary

MALICIOUS PROCESS

svchost.exe

HOST

Win10EP01

ALERT ID

23200

Incident View

Auto-Remediation: Auto-Remediation Applied

First Seen

02/08/2022 16:09

Last Seen

06/19/2022 08:50

GROUP NAME

Research

USER

win10ep01\sam

Description - Malicious Binary

Alert Origin: SSDEEP

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

Process Fuzzy Hash: 12288:IPfOgHtgKr8QKRvOjX5zgxsfanITOE+Ud/cYsAw:9ON3j+ncYsAw

Known Process Fuzzy Hash: 12288:IPfOgHtgKr8QKRvOjX5zgxsfanITOE+Ud/cYsAw:9ON3j+ncYsAw

Malicious Threat Level: 100%

Recommendation

Investigate according to organization policy

Path

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

Hash

B103FC649787EB1F6121DF8174D0F16AAAC736FB53F5F078D312871189285956

Process Tree

explorer.exe

svchost.exe

svchost.exe

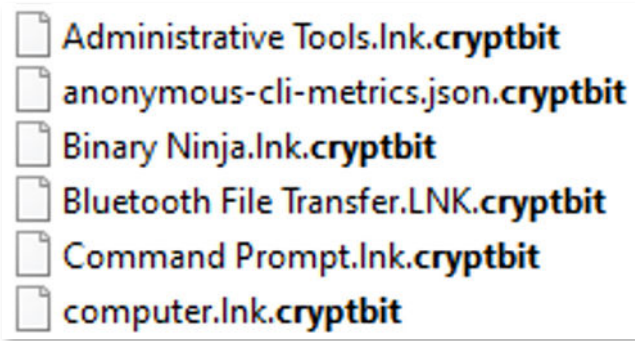
Comments

Add Comments...

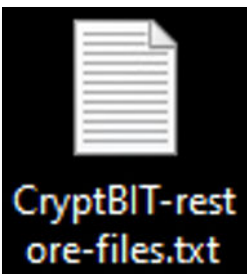
Add

CryptBIT Overview

CryptBIT ransomware renames the encrypted files with .cryptbit in the extension:



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



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



When the encryption ends, the ransomware also changes the wallpaper:



Thank you!



May, 2022