Defensive Security 1

(INFO70243)

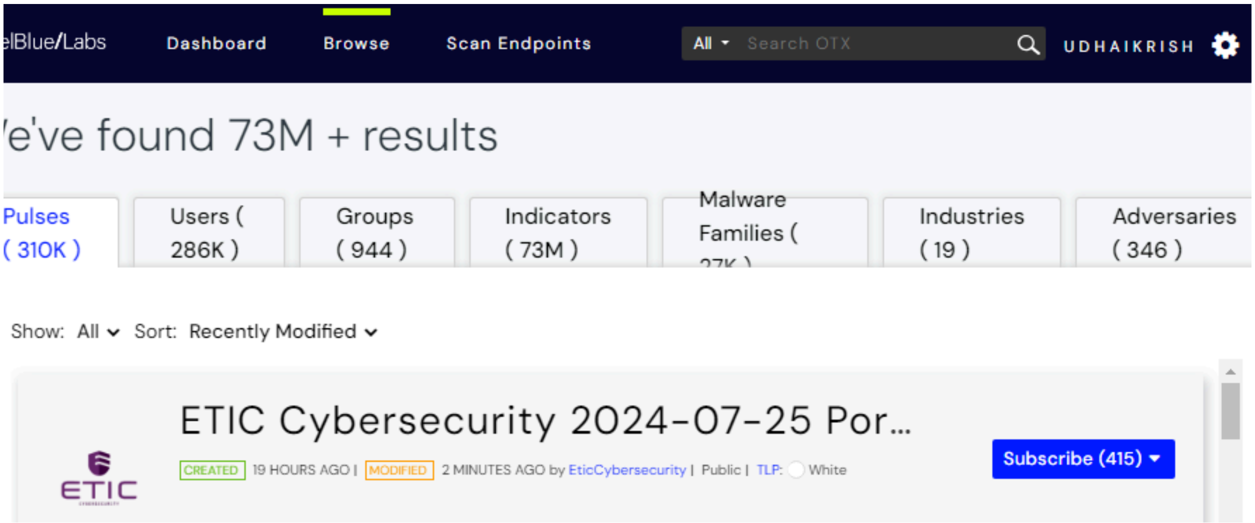
Assignment 2

by

Uthaya Krishnan
Sheridan College

Indicator of Compromise (IOC) creation

1. Account with AlienVault OTX platform

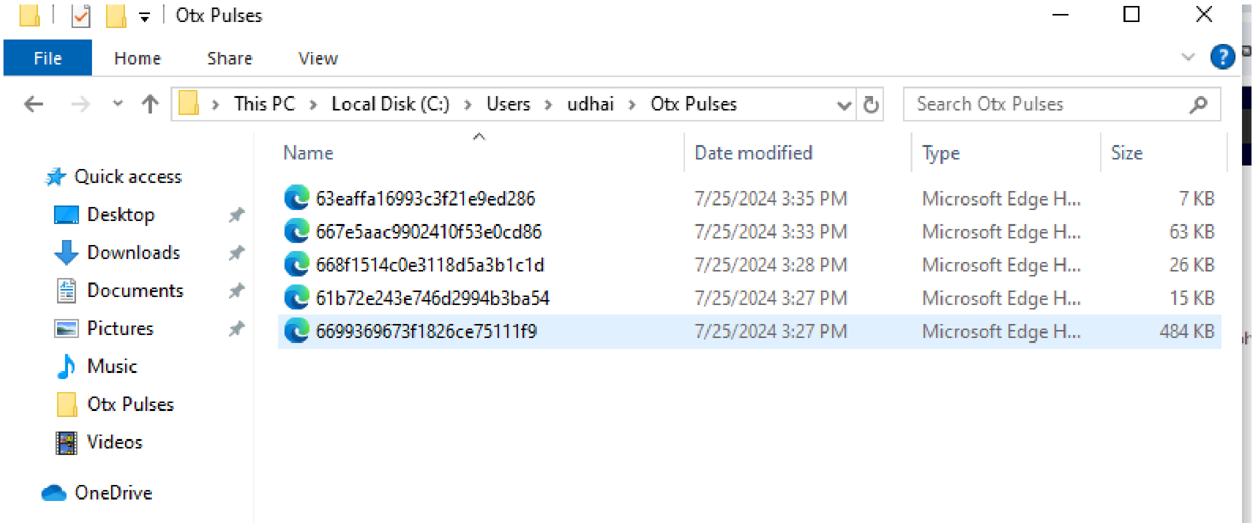


'e've found 73M + results

ETIC Cybersecurity 2024-07-25 Por...

CREATED 19 HOURS AGO | MODIFIED 2 MINUTES AGO by EticCybersecurity | Public | TLP: White

2. Download 5 pulses

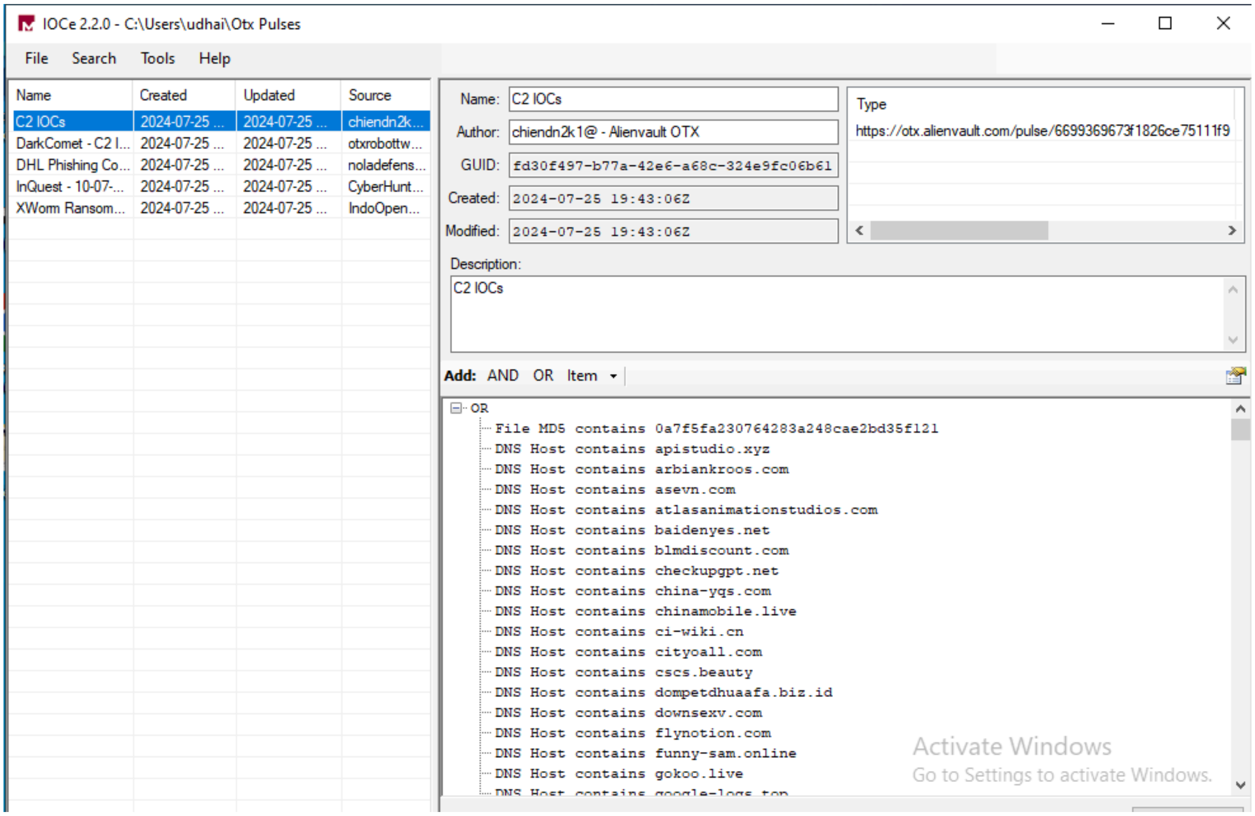


Name	Date modified	Type	Size
63eaffa16993c3f21e9ed286	7/25/2024 3:35 PM	Microsoft Edge H...	7 KB
667e5aac9902410f53e0cd86	7/25/2024 3:33 PM	Microsoft Edge H...	63 KB
668f1514c0e3118d5a3b1c1d	7/25/2024 3:28 PM	Microsoft Edge H...	26 KB
61b72e243e746d2994b3ba54	7/25/2024 3:27 PM	Microsoft Edge H...	15 KB
6699369673f1826ce75111f9	7/25/2024 3:27 PM	Microsoft Edge H...	484 KB

3.Open Pulses with Mandiant IOC Editor and its Description

C2 IOCs

Command and Control (C2) Indicators of Compromise (IOCs) involves identifying and documenting the IP addresses, domains, URLs, and other related artifacts that C2 servers use to communicate with malware-infected systems


IOCe 2.2.0 - C:\Users\udhai\Otx Pulses
File
Search
Tools
Help
Add:
AND
OR
Item
Activate Windows
Go to Settings to activate Windows.

Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobottw...
DHL Phishing Co...	2024-07-25 ...	2024-07-25 ...	noladefens...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
XWorm Ransom...	2024-07-25 ...	2024-07-25 ...	IndoOpen...

Name: C2 IOCs
Author: chiendn2k1@ - Alienvault OTX
GUID: fd30f497-b77a-42e6-a68c-324e9fc06b61
Created: 2024-07-25 19:43:06Z
Modified: 2024-07-25 19:43:06Z

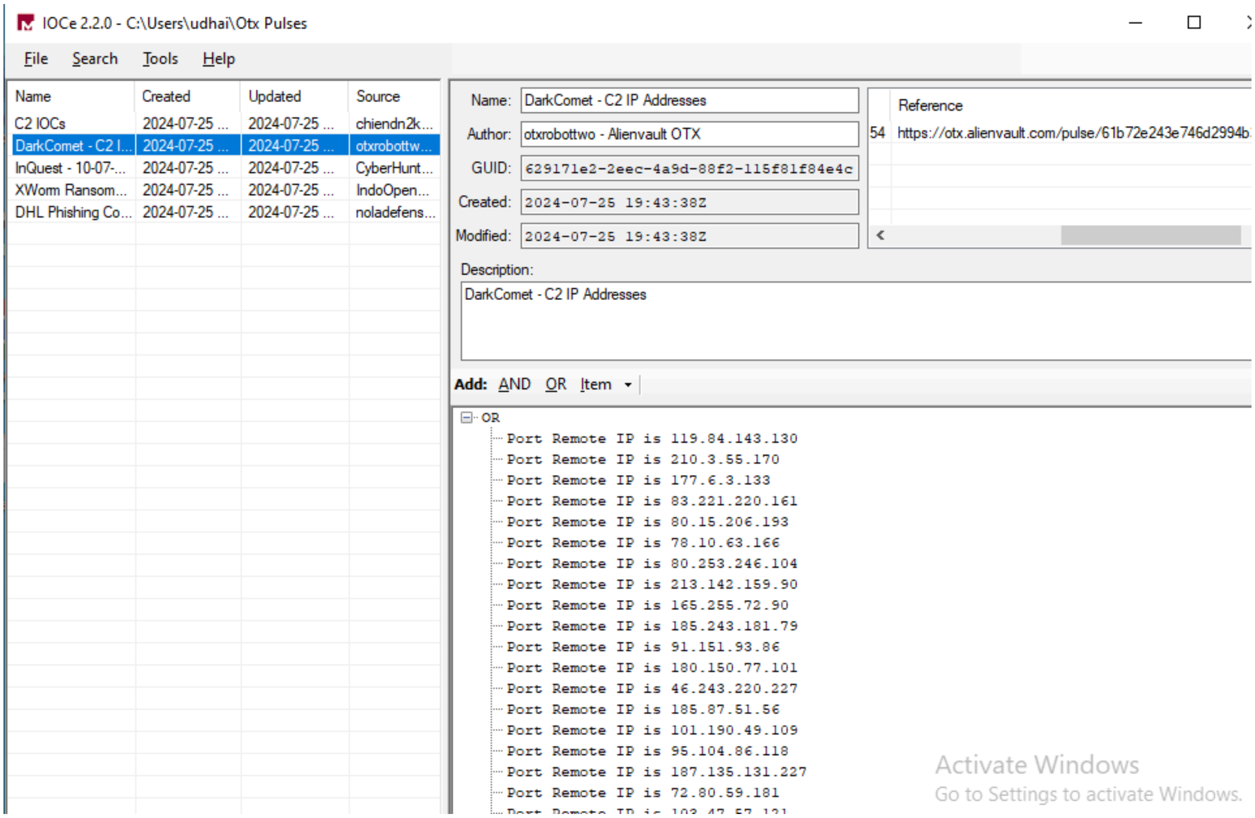
Type
https://otx.alienvault.com/pulse/6699369673f1826ce75111f9

Description:
C2 IOCs

```
OR
    File MD5 contains 0a7f5fa230764283a248cae2bd35f121
    DNS Host contains apistudio.xyz
    DNS Host contains arbiankroos.com
    DNS Host contains asevn.com
    DNS Host contains atlasanimationstudios.com
    DNS Host contains baidenyes.net
    DNS Host contains blmdiscount.com
    DNS Host contains checkupgpt.net
    DNS Host contains china-yqs.com
    DNS Host contains chinamobile.live
    DNS Host contains ci-wiki.cn
    DNS Host contains cityoall.com
    DNS Host contains cscs.beauty
    DNS Host contains dompetdhuaafa.biz.id
    DNS Host contains downsexv.com
    DNS Host contains flynotion.com
    DNS Host contains funny-sam.online
    DNS Host contains gokoo.live
    DNS Host contains google-logs.top
```

DarkComet - C2 IP Addresses

DarkComet, a known Remote Access Trojan (RAT), involves gathering indicators of compromise (IOCs) such as command and control (C2) IP addresses, domains, and other artifacts related to DarkComet activities



Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobottw...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
XWorm Ransom...	2024-07-25 ...	2024-07-25 ...	IndoOpen...
DHL Phishing Co...	2024-07-25 ...	2024-07-25 ...	noladefens...

Name: DarkComet - C2 IP Addresses
Author: otxrobottwo - Alienvault OTX
GUID: 629171e2-2eec-4a9d-88f2-115f81f84e4c
Created: 2024-07-25 19:43:38Z
Modified: 2024-07-25 19:43:38Z

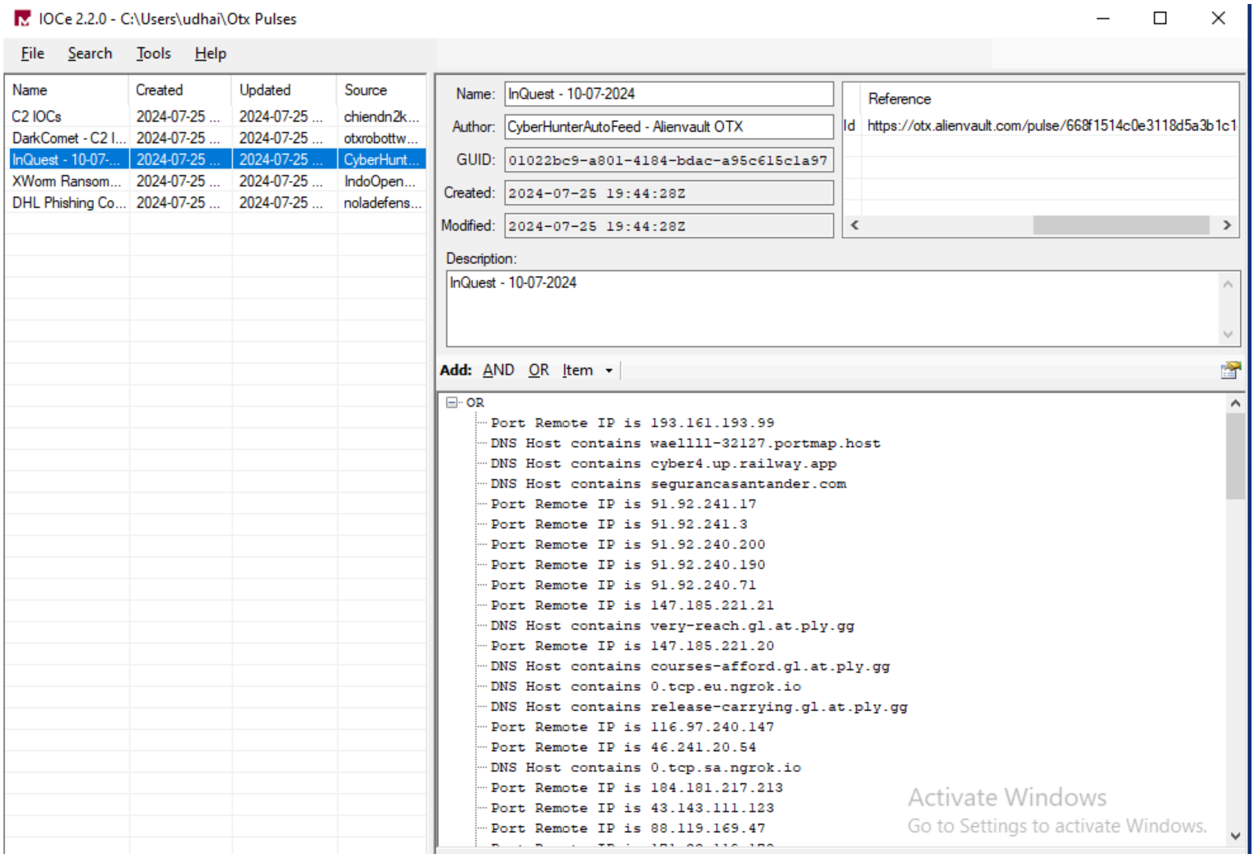
	Reference
54	https://otx.alienvault.com/pulse/61b72e243e746d2994b

Description:
DarkComet - C2 IP Addresses

```
OR
  Port Remote IP is 119.84.143.130
  Port Remote IP is 210.3.55.170
  Port Remote IP is 177.6.3.133
  Port Remote IP is 83.221.220.161
  Port Remote IP is 80.15.206.193
  Port Remote IP is 78.10.63.166
  Port Remote IP is 80.253.246.104
  Port Remote IP is 213.142.159.90
  Port Remote IP is 165.255.72.90
  Port Remote IP is 185.243.181.79
  Port Remote IP is 91.151.93.86
  Port Remote IP is 180.150.77.101
  Port Remote IP is 46.243.220.227
  Port Remote IP is 185.87.51.56
  Port Remote IP is 101.190.49.109
  Port Remote IP is 95.104.86.118
  Port Remote IP is 187.135.131.227
  Port Remote IP is 72.80.59.181
  Port Remote IP is 103.47.57.121
```

InQuest 10-07-2024

InQuest, a known threat intelligence platform, requires collecting indicators of compromise (IOCs) associated with specific threats or campaigns identified on the date 10-07-24 (July 10, 2024).



Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobottw...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
XWorm Ransom...	2024-07-25 ...	2024-07-25 ...	IndoOpen...
DHL Phishing Co...	2024-07-25 ...	2024-07-25 ...	noladefens...

Name: InQuest - 10-07-2024

Author: CyberHunterAutoFeed - Alienvault OTX

GUID: 01022bc9-a801-4184-bdac-a95c615c1a97

Created: 2024-07-25 19:44:28Z

Modified: 2024-07-25 19:44:28Z

	Reference
Id	https://otx.alienvault.com/pulse/668f1514c0e3118d5a3b1c1

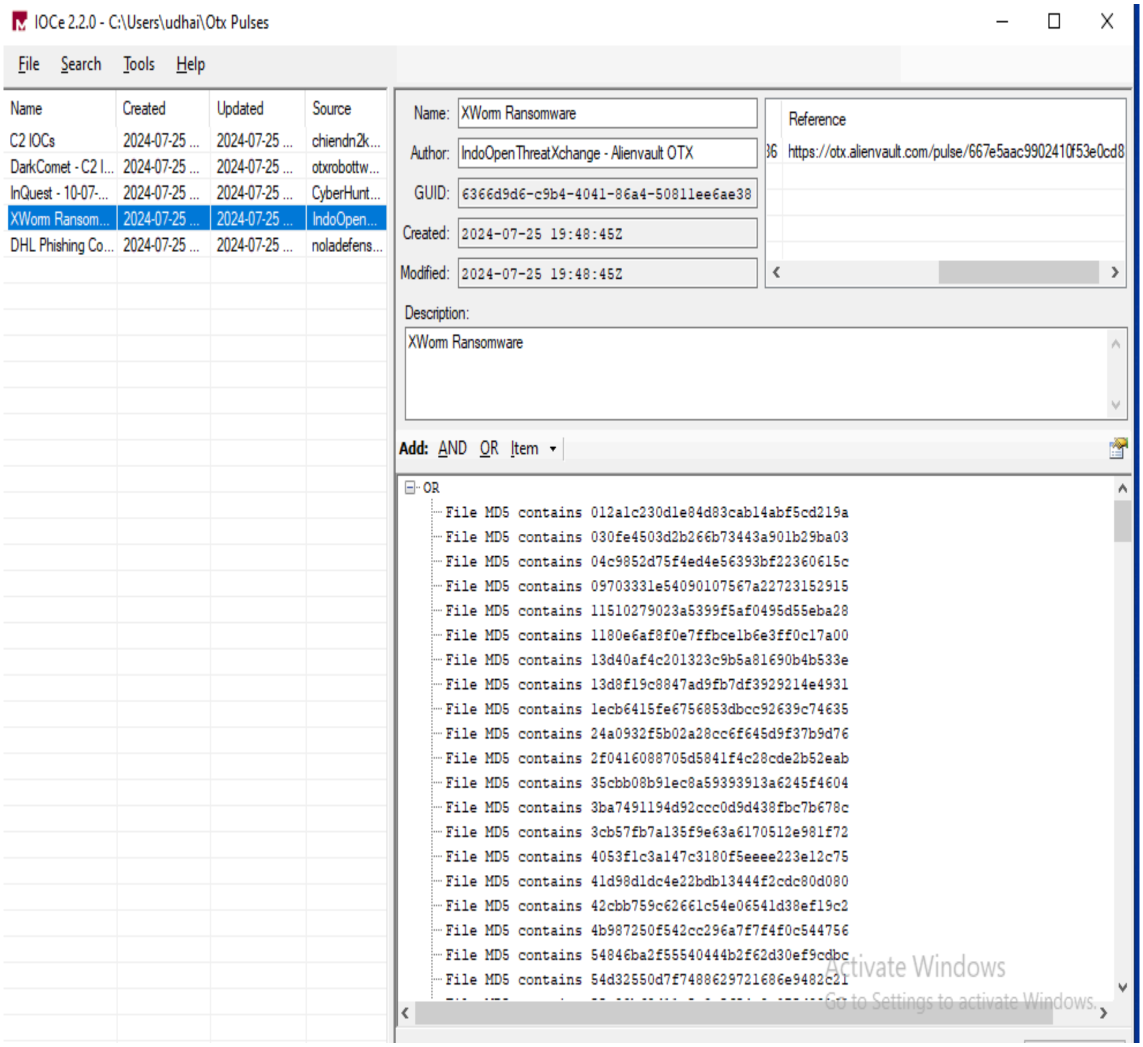
Description:

InQuest - 10-07-2024

```
OR
  Port Remote IP is 193.161.193.99
  DNS Host contains waellll-32127.portmap.host
  DNS Host contains cyber4.up.railway.app
  DNS Host contains segurancasantander.com
  Port Remote IP is 91.92.241.17
  Port Remote IP is 91.92.241.3
  Port Remote IP is 91.92.240.200
  Port Remote IP is 91.92.240.190
  Port Remote IP is 91.92.240.71
  Port Remote IP is 147.185.221.21
  DNS Host contains very-reach.gl.at.ply.gg
  Port Remote IP is 147.185.221.20
  DNS Host contains courses-afford.gl.at.ply.gg
  DNS Host contains 0.tcp.eu.ngrok.io
  DNS Host contains release-carrying.gl.at.ply.gg
  Port Remote IP is 116.97.240.147
  Port Remote IP is 46.241.20.54
  DNS Host contains 0.tcp.sa.ngrok.io
  Port Remote IP is 184.181.217.213
  Port Remote IP is 43.143.111.123
  Port Remote IP is 88.119.169.47
```

xWorm ransomware pulses

xWorm ransomware involves gathering indicators of compromise (IOCs) such as file hashes, IP addresses, domains, and other artifacts related to xWorm ransomware activities.


IOCe 2.2.0 - C:\Users\udhai\Otx Pulses
File
Search
Tools
Help
Add: AND OR Item
Activate Windows
Go to Settings to activate Windows.

Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobottw...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
XWorm Ransom...	2024-07-25 ...	2024-07-25 ...	IndoOpen...
DHL Phishing Co...	2024-07-25 ...	2024-07-25 ...	noladefens...

Name: XWorm Ransomware

Author: IndoOpenThreatXchange - Alienvault OTX

GUID: 6366d9d6-c9b4-4041-86a4-50811ee6ae38

Created: 2024-07-25 19:48:45Z

Modified: 2024-07-25 19:48:45Z

	Reference
36	https://otx.alienvault.com/pulse/667e5aac9902410f53e0cd8

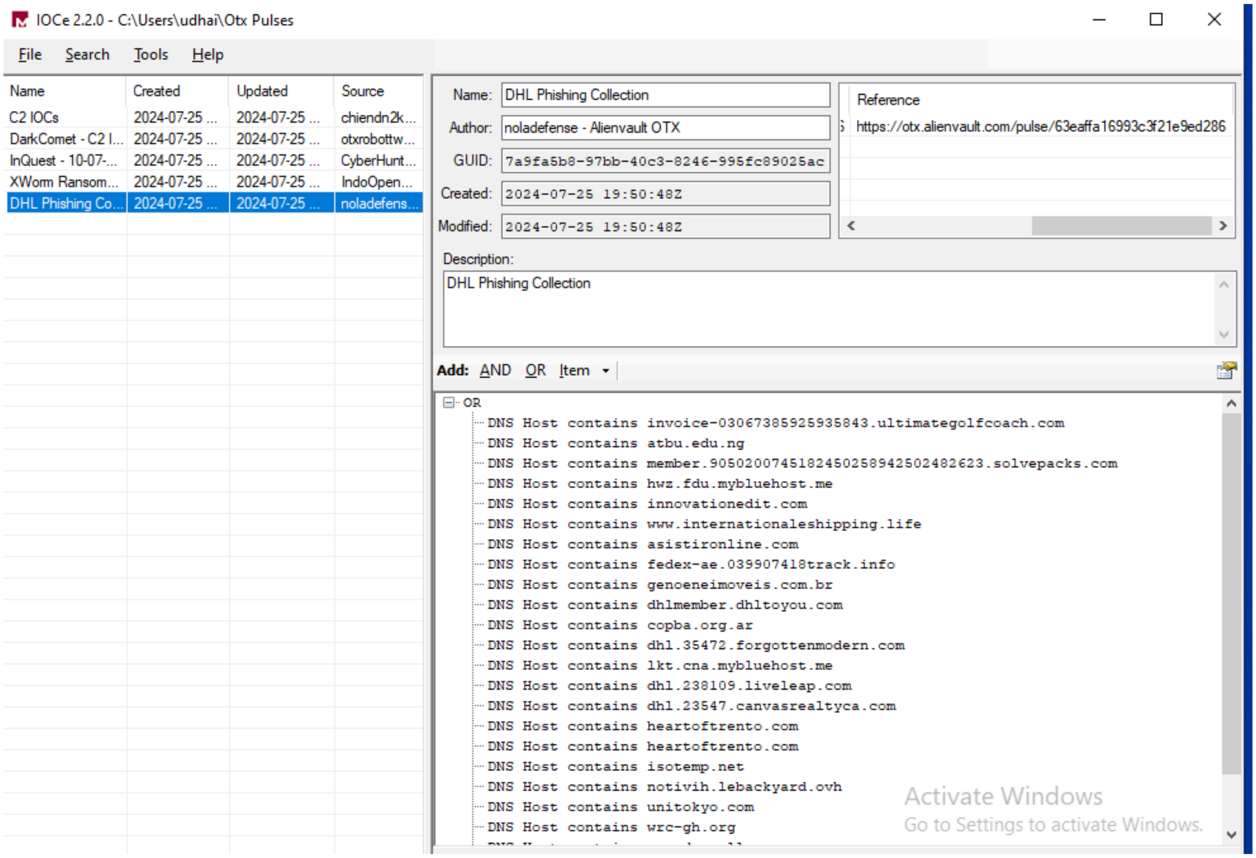
Description:

XWorm Ransomware

```
OR
  File MD5 contains 012a1c230d1e84d83cab14abf5cd219a
  File MD5 contains 030fe4503d2b266b73443a901b29ba03
  File MD5 contains 04c9852d75f4ed4e56393bf22360615c
  File MD5 contains 09703331e54090107567a22723152915
  File MD5 contains 11510279023a5399f5af0495d55eba28
  File MD5 contains 1180e6af8f0e7ffbce1b6e3ff0c17a00
  File MD5 contains 13d40af4c201323c9b5a81690b4b533e
  File MD5 contains 13d8f19c8847ad9fb7df3929214e4931
  File MD5 contains 1ecb6415fe6756853dbcc92639c74635
  File MD5 contains 24a0932f5b02a28cc6f645d9f37b9d76
  File MD5 contains 2f0416088705d5841f4c28cde2b52eab
  File MD5 contains 35cbb08b91ec8a59393913a6245f4604
  File MD5 contains 3ba7491194d92ccc0d9d438fbc7b678c
  File MD5 contains 3cb57fb7a135f9e63a6170512e981f72
  File MD5 contains 4053f1c3a147c3180f5eeee223e12c75
  File MD5 contains 41d98d1dc4e22bdb13444f2cdc80d080
  File MD5 contains 42cbb759c62661c54e06541d38ef19c2
  File MD5 contains 4b987250f542cc296a7f7f4f0c544756
  File MD5 contains 54846ba2f55540444b2f62d30ef9cdbc
  File MD5 contains 54d32550d7f7488629721686e9482c21
```

DHL phishing collection pulses

DHL phishing attacks involve gathering indicators of compromise (IOCs) that are typically associated with phishing campaigns targeting DHL customers. These can include phishing email subjects, sender addresses, URLs, IP addresses, and other artifacts that help identify and block such attacks.



Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobottw...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
XWorm Ransom...	2024-07-25 ...	2024-07-25 ...	IndoOpen...
DHL Phishing Co...	2024-07-25 ...	2024-07-25 ...	noladefens...

Name: DHL Phishing Collection
Author: noladefense - Alienvault OTX
GUID: 7a9fa5b8-97bb-40c3-8246-995fc89025ac
Created: 2024-07-25 19:50:48Z
Modified: 2024-07-25 19:50:48Z

Reference
https://otx.alienvault.com/pulse/63eaffa16993c3f21e9ed286

Description:
DHL Phishing Collection

```
OR
  DNS Host contains invoice-030673859259358843.ultimategolfcoach.com
  DNS Host contains atbu.edu.ng
  DNS Host contains member.9050200745182450258942502482623.solvepacks.com
  DNS Host contains hwz.fdu.mybluehost.me
  DNS Host contains innovationedit.com
  DNS Host contains www.internationaleshipping.life
  DNS Host contains asistironline.com
  DNS Host contains fedex-ae.039907418track.info
  DNS Host contains genoeneimoveis.com.br
  DNS Host contains dhlmember.dhltoyou.com
  DNS Host contains copba.org.ar
  DNS Host contains dhl.35472.forgottenmodern.com
  DNS Host contains lkt.cna.mybluehost.me
  DNS Host contains dhl.238109.liveleap.com
  DNS Host contains dhl.23547.canvasrealtyca.com
  DNS Host contains heartoftrento.com
  DNS Host contains heartoftrento.com
  DNS Host contains isotemp.net
  DNS Host contains notivih.lebackyard.ovh
  DNS Host contains unitokyo.com
  DNS Host contains wrc-gh.org
```

4. IOC Creation of Chrome.exe, Notepad.exe, iexplorer.exe

IOC - Chrome.exe

File Attributes of Chrome

MD5-9E38837050E379D1D0F2801230109F89

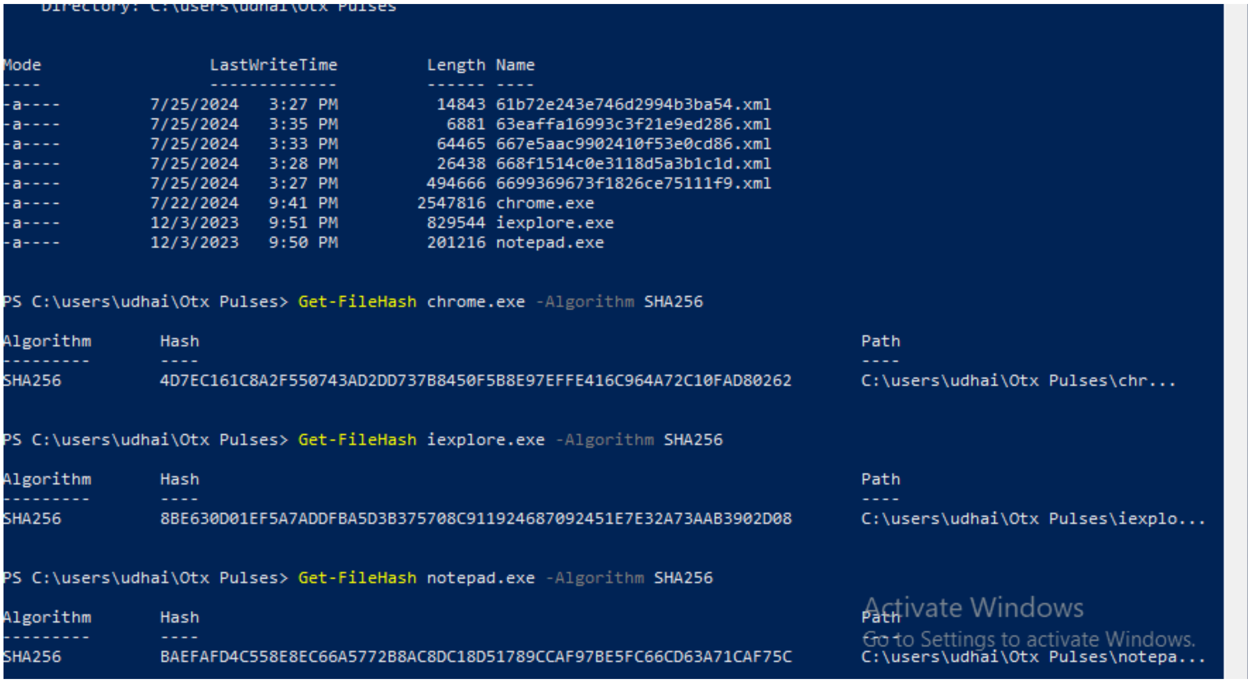
File Size-2,551,808 bytes

Process Name - chrome.exe

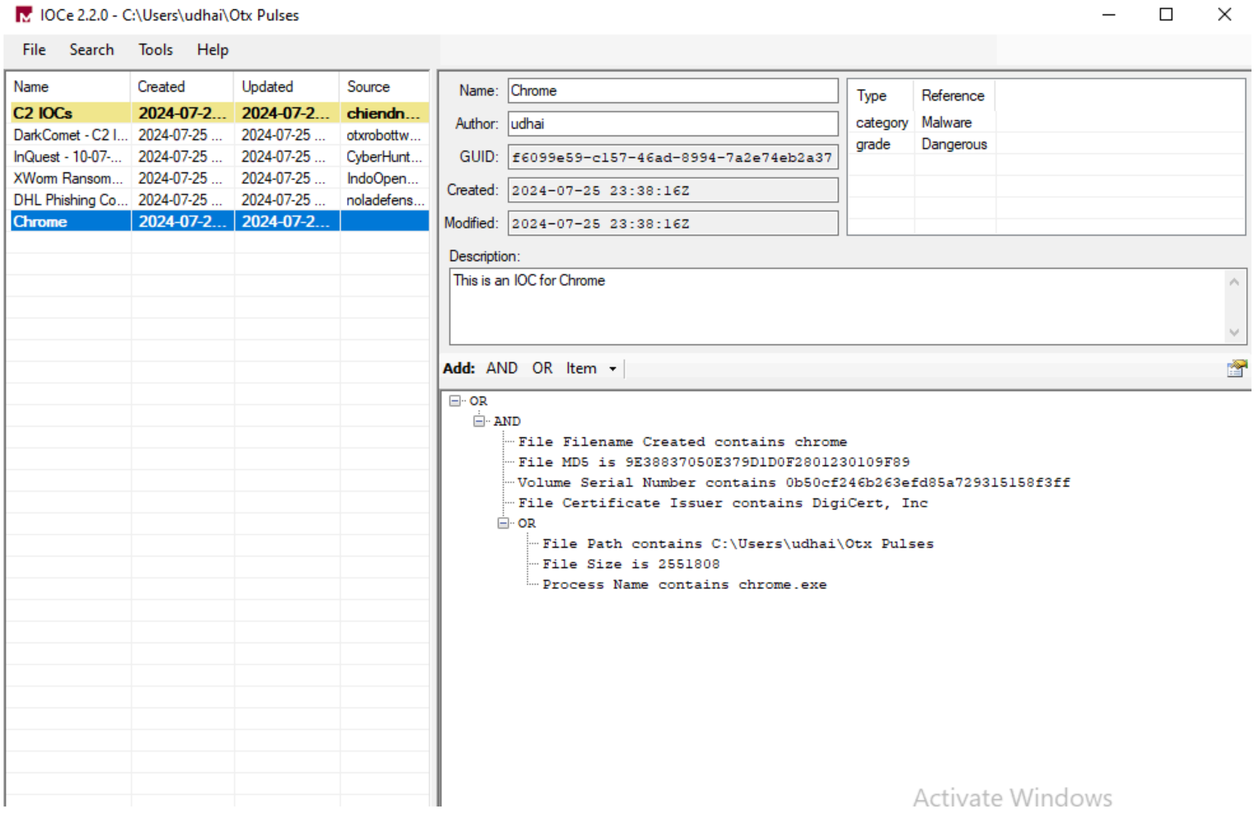
File Certificate Issuer -DigiCert, Inc

File path-C:\Users\udhai\Otx Pulses

serial ID -0b50cf246b263efd85a729315158f3ff



```
    Directory: C:\users\udhai\Otx Pulses


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/25/2024   3:27 PM          14843 61b72e243e746d2994b3ba54.xml
-a----         7/25/2024   3:35 PM           6881 63eaffa16993c3f21e9ed286.xml
-a----         7/25/2024   3:33 PM          64465 667e5aac9902410f53e0cd86.xml
-a----         7/25/2024   3:28 PM          26438 668f1514c0e3118d5a3b1c1d.xml
-a----         7/25/2024   3:27 PM         494666 6699369673f1826ce75111f9.xml
-a----         7/22/2024   9:41 PM        2547816 chrome.exe
-a----         12/3/2023   9:51 PM         829544 iexplore.exe
-a----         12/3/2023   9:50 PM         201216 notepad.exe


PS C:\users\udhai\Otx Pulses> Get-FileHash chrome.exe -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          4D7EC161C8A2F550743AD2DD737B8450F5B8E97EFFE416C964A72C10FAD80262       C:\users\udhai\Otx Pulses\chr...


PS C:\users\udhai\Otx Pulses> Get-FileHash iexplore.exe -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          8BE630D01EF5A7ADDFBA5D3B375708C911924687092451E7E32A73AAB3902D08       C:\users\udhai\Otx Pulses\iexplo...


PS C:\users\udhai\Otx Pulses> Get-FileHash notepad.exe -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          BAEFAFD4C558E8EC66A5772B8AC8DC18D51789CCAF97BE5FC66CD63A71CAF75C       C:\users\udhai\Otx Pulses\notepa...
```



Name	Created	Updated	Source
C2 IOCs	**2024-07-2...**	**2024-07-2...**	**chiendn...**
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobottw...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
XWorm Ransom...	2024-07-25 ...	2024-07-25 ...	IndoOpen...
DHL Phishing Co...	2024-07-25 ...	2024-07-25 ...	noladefens...
Chrome	2024-07-2...	2024-07-2...	

Name: Chrome
Author: udhai
GUID: f6099e59-c157-46ad-8994-7a2e74eb2a37
Created: 2024-07-25 23:38:16Z
Modified: 2024-07-25 23:38:16Z

Type	Reference
category	Malware
grade	Dangerous

Description:
This is an IOC for Chrome

```
OR
  AND
    File Filename Created contains chrome
    File MD5 is 9E38837050E379D1D0F2801230109F89
    Volume Serial Number contains 0b50cf246b263efd85a729315158f3ff
    File Certificate Issuer contains DigiCert, Inc
    OR
      File Path contains C:\Users\udhai\Otx Pulses
      File Size is 2551808
      Process Name contains chrome.exe
```

IOC - Notepad.exe

File Attributes of Notepad

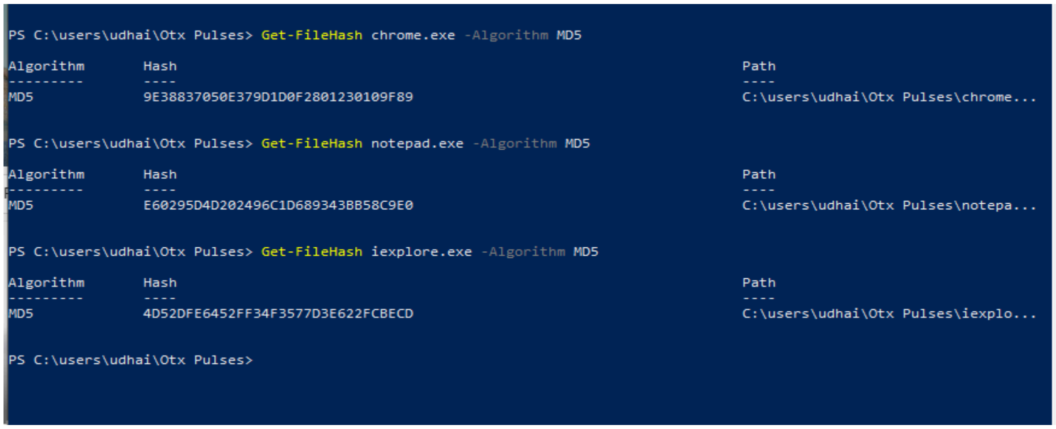
SHA256-BAEFAFD4C558E8EC66A5772B8AC8DC18D51789CCAF97BE5FC66CD63A71CAF75C

FileVersion - 10.0.19041.3636

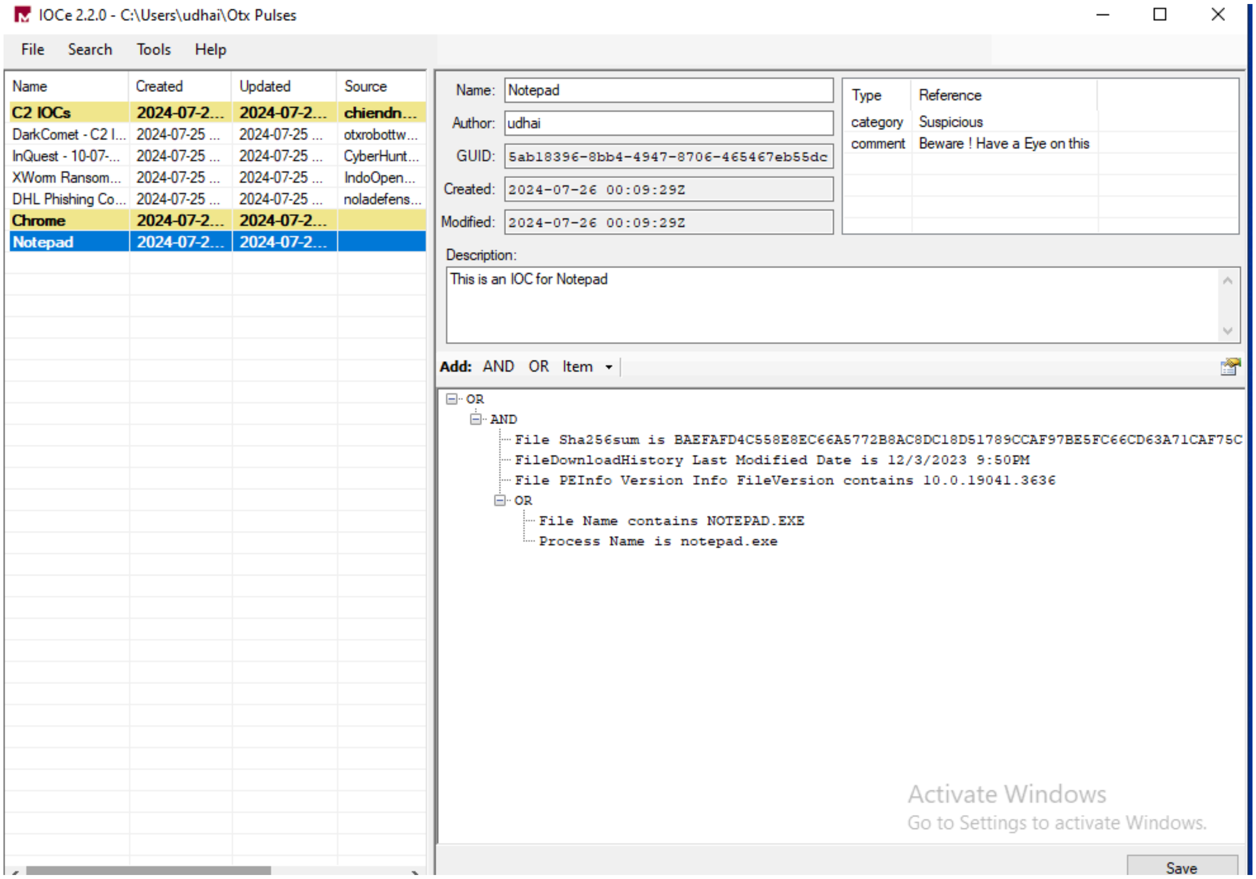
Process Name -notepad.exe

Original filename-NOTEPAD.EXE

Date Modified -12/3/2023 9:50PM



```
PS C:\users\udhai\Otx Pulses> Get-FileHash chrome.exe -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             9E38837050E379D1D0F2801230109F89                                       C:\users\udhai\Otx Pulses\chrome...

PS C:\users\udhai\Otx Pulses> Get-FileHash notepad.exe -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             E60295D4D202496C1D689343BB58C9E0                                       C:\users\udhai\Otx Pulses\notepa...

PS C:\users\udhai\Otx Pulses> Get-FileHash iexplore.exe -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             4D52DFE6452FF34F3577D3E622FCBECD                                       C:\users\udhai\Otx Pulses\iexplo...

PS C:\users\udhai\Otx Pulses>
```



Name	Created	Updated	Source
C2 IOCs	**2024-07-2...**	**2024-07-2...**	**chiendn...**
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobottw...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
XWorm Ransom...	2024-07-25 ...	2024-07-25 ...	IndoOpen...
DHL Phishing Co...	2024-07-25 ...	2024-07-25 ...	noladefens...
Chrome	**2024-07-2...**	**2024-07-2...**	
Notepad	**2024-07-2...**	**2024-07-2...**	

Name: Notepad

Author: udhai

GUID: 5ab18396-8bb4-4947-8706-465467eb55dc

Created: 2024-07-26 00:09:29Z

Modified: 2024-07-26 00:09:29Z

Type	Reference
category	Suspicious
comment	Beware ! Have a Eye on this

Description:

This is an IOC for Notepad

```
OR
  AND
    File Sha256sum is BAEFAFD4C558E8EC66A5772B8AC8DC18D51789CCAF97BE5FC66CD63A71CAF75C
    FileDownloadHistory Last Modified Date is 12/3/2023 9:50PM
    File PEInfo Version Info FileVersion contains 10.0.19041.3636
    OR
      File Name contains NOTEPAD.EXE
      Process Name is notepad.exe
```

IOC - iExplore.exe

File Attributes of iexplore

File size - 831,488

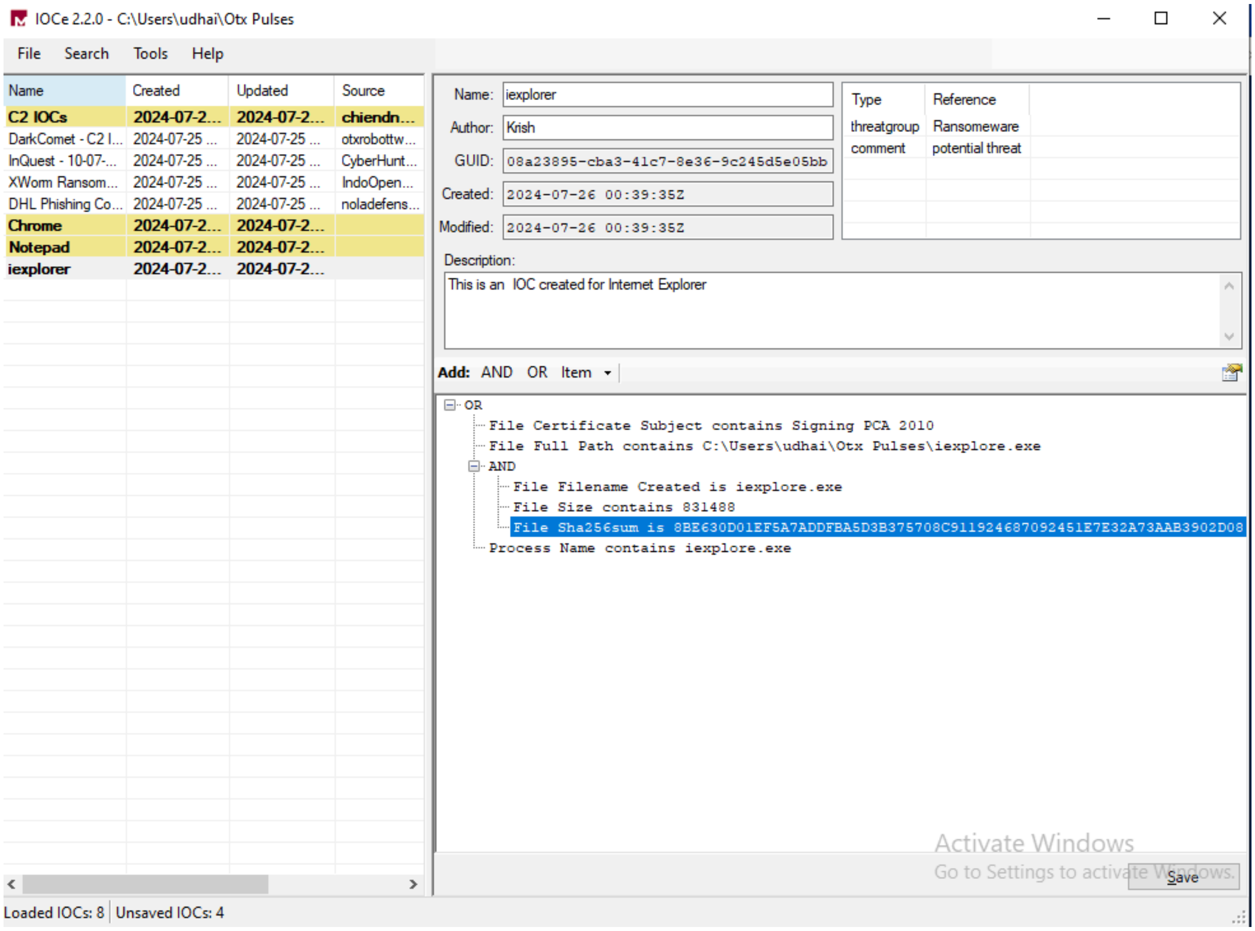
Process Name - iexplore.exe

File Certificate - Signing PCA 2010

SHA256-8BE630D01EF5A7ADDFBA5D3B375708C911924687092451E7E32A73AAB3902D08

File Path - C:\Users\udhai\Otx Pulses\iexplore.exe

File Name - iexplore.exe


IOCe 2.2.0 - C:\Users\udhai\Otx Pulses
File
Search
Tools
Help
Add: AND OR Item
Save
Activate Windows
Go to Settings to activate Windows.

Name	Created	Updated	Source
C2 IOCs	**2024-07-2...**	**2024-07-2...**	**chiendn...**
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobottw...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
XWorm Ransom...	2024-07-25 ...	2024-07-25 ...	IndoOpen...
DHL Phishing Co...	2024-07-25 ...	2024-07-25 ...	noladefens...
Chrome	**2024-07-2...**	**2024-07-2...**	
Notepad	**2024-07-2...**	**2024-07-2...**	
iexplorer	**2024-07-2...**	**2024-07-2...**	

Name: iexplorer

Author: Krish

GUID: 08a23895-cba3-41c7-8e36-9c245d5e05bb

Created: 2024-07-26 00:39:35Z

Modified: 2024-07-26 00:39:35Z

Type	Reference
threatgroup	Ransomeware
comment	potential threat

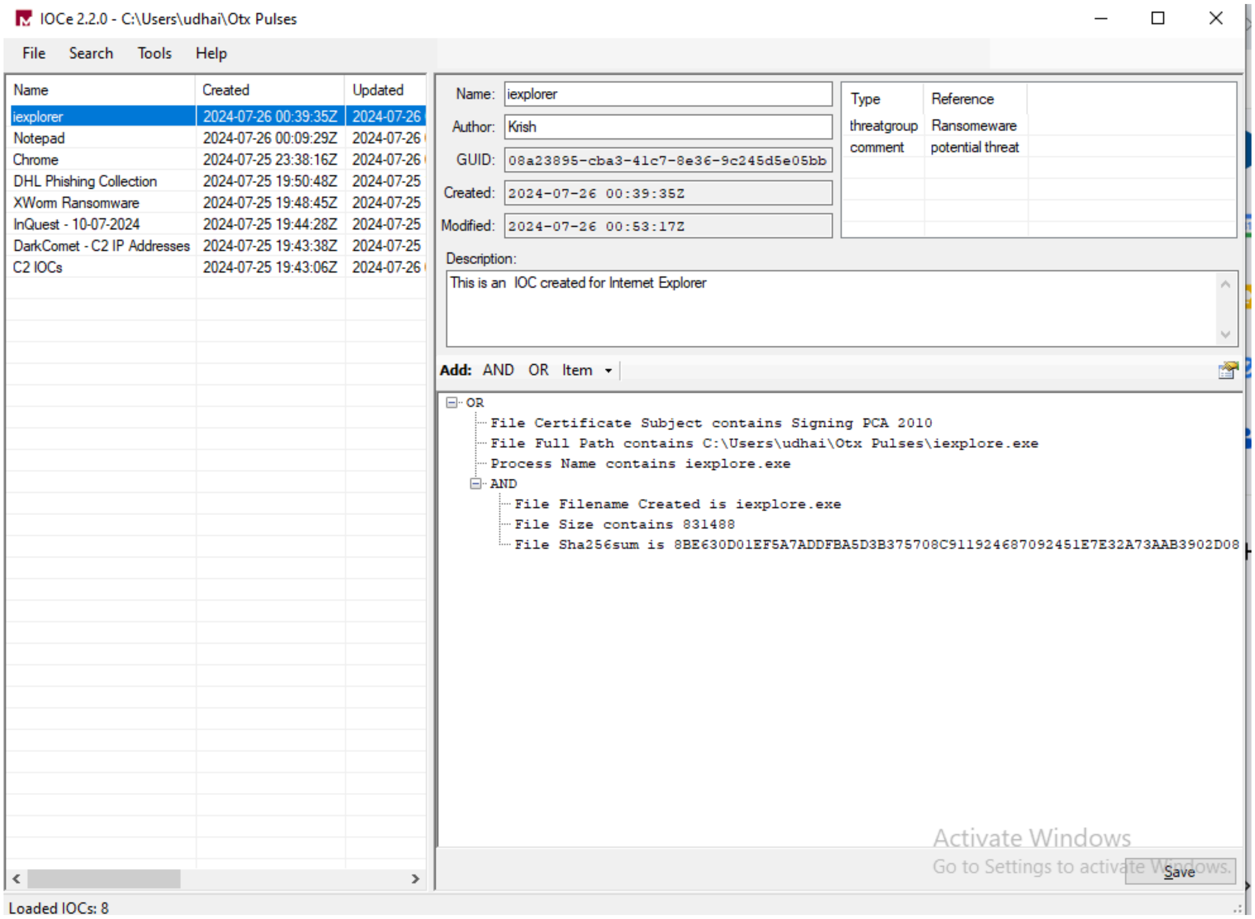
Description:

This is an IOC created for Internet Explorer

```
OR
  File Certificate Subject contains Signing PCA 2010
  File Full Path contains C:\Users\udhai\Otx Pulses\iexplore.exe
  AND
    File Filename Created is iexplore.exe
    File Size contains 831488
    File Sha256sum is 8BE630D01EF5A7ADDFBA5D3B375708C911924687092451E7E32A73AAB3902D08
  Process Name contains iexplore.exe
```

Loaded IOCs: 8 | Unsaved IOCs: 4

The Newly created IOCS



Name	Created	Updated
iexplorer	2024-07-26 00:39:35Z	2024-07-26
Notepad	2024-07-26 00:09:29Z	2024-07-26
Chrome	2024-07-25 23:38:16Z	2024-07-26
DHL Phishing Collection	2024-07-25 19:50:48Z	2024-07-25
XWorm Ransomware	2024-07-25 19:48:45Z	2024-07-25
InQuest - 10-07-2024	2024-07-25 19:44:28Z	2024-07-25
DarkComet - C2 IP Addresses	2024-07-25 19:43:38Z	2024-07-25
C2 IOCs	2024-07-25 19:43:06Z	2024-07-26

Name: iexplorer

Author: Krish

GUID: 08a23895-cba3-41c7-8e36-9c245d5e05bb

Created: 2024-07-26 00:39:35Z

Modified: 2024-07-26 00:53:17Z

Type	Reference
threatgroup	Ransomeware
comment	potential threat

Description:

This is an IOC created for Internet Explorer

```
OR
    File Certificate Subject contains Signing PCA 2010
    File Full Path contains C:\Users\udhai\Otx Pulses\iexplore.exe
    Process Name contains iexplore.exe
    AND
        File Filename Created is iexplore.exe
        File Size contains 831488
        File Sha256sum is 8BE630D01EF5A7ADDFBA5D3B375708C911924687092451E7E32A73AAB3902D08
```

Loaded IOCs: 8