



# Defensive Security 1

(INFO70243)

## *Assignment 2*

by

Uthaya Krishnan  
Sheridan College

## Indicator of Compromise (IOC) creation

### 1. Account with AlienVault OTX platform

The screenshot shows the AlienVault OTX platform interface. The top navigation bar includes links for Blue/Labs, Dashboard, Browse, Scan Endpoints, and a search bar with the text "All Search OTX". The user's name "UDHAIKRISH" and a settings gear icon are visible on the right. Below the navigation bar, a message states "We've found 73M + results". A summary row displays various categories: Pulses (310K), Users (286K), Groups (944), Indicators (73M), Malware Families (27K), Industries (19), and Adversaries (346). Below this, a filter section shows "Show: All" and "Sort: Recently Modified". The main content area features a card for "ETIC Cybersecurity 2024-07-25 Por...". The card includes the ETIC logo, a "CREATED" status (19 HOURS AGO), a "MODIFIED" status (2 MINUTES AGO by EticCybersecurity), and a "Public" status with a "TLP: White" label. A blue "Subscribe (415)" button is located on the right side of the card.

### 2. Download 5 pulses

The screenshot shows a Windows File Explorer window titled "Otx Pulses". The address bar indicates the path: "This PC > Local Disk (C:) > Users > udhai > Otx Pulses". The left sidebar shows the "Quick access" menu with options for Desktop, Downloads, Documents, Pictures, Music, Otx Pulses, Videos, and OneDrive. The main pane displays a list of files with columns for Name, Date modified, Type, and Size. The files are listed as follows:

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

The screenshot displays the Mandiant IOC Editor (IOCe 2.2.0) interface. The main window shows a list of C2 IOCs with columns for Name, Created, Updated, and Source. The selected entry is 'C2 IOCs'.

Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobotw...
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...

The details pane on the right shows the following information for the selected 'C2 IOCs' pulse:

- 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

The 'Add: AND OR Item' section shows a list of indicators:

- 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 competdhuaafa.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

An 'Activate Windows' watermark is visible in the bottom right corner of the screenshot.

## 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

The screenshot displays the IOCe 2.2.0 application window. The title bar reads 'IOCe 2.2.0 - C:\Users\udhai\Otx Pulses'. The interface includes a menu bar with 'File', 'Search', 'Tools', and 'Help'. On the left, a table lists various IOCs, with 'DarkComet - C2 IP Addresses' selected. The right pane shows the details for this selected IOC, including its name, author, GUID, creation/modification dates, and a list of C2 IP addresses.

Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 IP...	2024-07-25 ...	2024-07-25 ...	otxrobottwo...
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...

**DarkComet - C2 IP Addresses Details:**

- 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
- Description: DarkComet - C2 IP Addresses
- Reference: 54 <https://otx.alienvault.com/pulse/61b72e243e746d2994b>

**Add: AND OR Item**

**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 103.47.52.121

Activate Windows  
Go to Settings to activate Windows.

## 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).

The screenshot shows the IOCe 2.2.0 application window. The title bar reads "IOCe 2.2.0 - C:\Users\udhai\Otx Pulses". The menu bar includes "File", "Search", "Tools", and "Help".

On the left, a table lists several IOCs:

Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobotw...
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...

The "InQuest - 10-07-2024" entry is selected. The right pane displays its details:

- 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:** <https://otx.alienvault.com/pulse/668f1514c0e3118d5a3b1c1>
- Description:** InQuest - 10-07-2024

Below the details, there is a section for "Add: AND OR Item" and a list of indicators under the "OR" operator:

- Port Remote IP is 193.161.193.99
- DNS Host contains waell111-32127.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

An "Activate Windows" watermark is visible in the bottom right corner of the application window.

## 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.

The screenshot displays the IOCe 2.2.0 application interface. On the left, a table lists various pulses, with 'xWorm Ransom...' selected. The main panel on the right shows the configuration for the 'xWorm Ransomware' pulse.

**IOCe 2.2.0 - C:\Users\udhai\Otr Pulses**

**File Search Tools Help**

Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobotw...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
<b>xWorm Ransom...</b>	<b>2024-07-25 ...</b>	<b>2024-07-25 ...</b>	<b>IndoOpen...</b>
DHL Phishing Co...	2024-07-25 ...	2024-07-25 ...	notadefens...

**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

**Add: AND OR Item**

**OR**

- File MD5 contains 012alc230dle84d83cabl4abf5cd219a
- File MD5 contains 030fe4503d2b266b73443a901b29ba03
- File MD5 contains 04c9852d75f4ed4e56393bf22360615c
- File MD5 contains 09703331e54090107567a22723152915
- File MD5 contains 11510279023a5399f5af0495d55eba28
- File MD5 contains 1180e6af8f0e7ffbcclb6e3ff0c17a00
- 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 4053f1c3a147c3180f5eeeee223e12c75
- File MD5 contains 41d98d1dc4e22bdb13444f2cdc80d080
- File MD5 contains 42cbb759c6261c54e06541d38ef19c2
- File MD5 contains 4b987250f542cc296a7f7f4f0c544756
- File MD5 contains 54846ba2f55540444b2f62d30ef9cdbc
- File MD5 contains 54d32550d7f7488629721686e9482c21

Activate Windows  
Go to Settings to activate Windows.

## 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.

The screenshot shows the IOCe 2.2.0 application interface. The main window displays a list of pulses on the left and details for the selected 'DHL Phishing Collection' pulse on the right.

**Pulse List:**

Name	Created	Updated	Source
C2 IOCs	2024-07-25 ...	2024-07-25 ...	chiendn2k...
DarkComet - C2 1...	2024-07-25 ...	2024-07-25 ...	otxrobotw...
InQuest - 10-07-...	2024-07-25 ...	2024-07-25 ...	CyberHunt...
XWorm Ransom...	2024-07-25 ...	2024-07-25 ...	IndoOpen...
<b>DHL Phishing Co...</b>	<b>2024-07-25 ...</b>	<b>2024-07-25 ...</b>	<b>noladefens...</b>

**DHL Phishing Collection Details:**

- 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

**Add: AND OR Item**

**OR**

- DNS Host contains invoice-03067385925935843.ultimatgolffcoach.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.internationalshipping.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 wrd-gh.org

Activate Windows  
Go to Settings to activate Windows.

#### 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 63eafffa16993c3f21e9ed286.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
-----
SHA256         4D7EC161C8A2F550743AD2DD737B8450F588E97EFFE416C964A72C10FAD80262
C:\users\udhai\Otx Pulses\chr...

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

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

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

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

```

Activate Windows  
Go to Settings to activate Windows.  
C:\users\udhai\Otx Pulses\notepa...



IOCe 2.2.0 - C:\Users\udhai\Otx Pulses

Name	Created	Updated	Source
<b>C2 IOCs</b>	<b>2024-07-2...</b>	<b>2024-07-2...</b>	<b>chiendn...</b>
DarkComet - C2 I...	2024-07-25 ...	2024-07-25 ...	otxrobotw...
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...
<b>Chrome</b>	<b>2024-07-2...</b>	<b>2024-07-2...</b>	

Name: Chrome

Author: udhai

GUID: #6099e59-c157-46ad-8994-7a2e74eb2a37

Created: 2024-07-25 23:38:16Z

Modified: 2024-07-25 23:38:16Z

Type: Malware

Reference: Dangerous

category: Malware

grade: Dangerous

Description: This is an IOC for Chrome

Add: AND OR Item

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

Activate Windows

## 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            E60295D4D202496C1D689343B858C9E0      C:\users\udhai\Otx Pulses\notepe...

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

Algorithm      Hash                                     Path
-----
MD5            4D52DFE6452FF34F3577D3E622FC8ECD      C:\users\udhai\Otx Pulses\iexpl...

PS C:\users\udhai\Otx Pulses>

```

IOCe 2.2.0 - 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: 5ab18396-0bb4-4947-8706-465467eb55dc

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

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

Type: Suspicious

Reference: Beware ! Have a Eye on this

Description: This is an IOC for Notepad

Add: AND OR Item

AND

- File Sha256sum is BAEFAFD4C568E8EC66A5772B8AC8DC18D51789CCAF97BE5FC66CD63A71CAF75C
- 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

Activate Windows  
Go to Settings to activate Windows.

Save

## IOC - iExplore.exe

### File Attributes of iexplore

File size - 831,488

Process Name - iexplore.exe

File Certificate - Signing PCA 2010

SHA256-8BE630D01EF5A7ADDFBA5D3B375708C911924687092451E7E3  
2A73AAB3902D08

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

File Name - iexplore.exe

IOCe 2.2.0 - C:\Users\udhai\Otx Pulses

Name	Created	Updated	Source
C2 IOCs	2024-07-2...	2024-07-2...	chiendn...
DarkComet - C21...	2024-07-25 ...	2024-07-25 ...	otxrobotw...
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: threatgroup

Reference: Ransomware potential threat

Description: This is an IOC created for Internet Explorer

Add: AND OR Item

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

Activate Windows  
Go to Settings to activate Windows.

Save

Loaded IOCs: 8 | Unsaved IOCs: 4

## The Newly created IOCS

IOCe 2.2.0 - C:\Users\udhai\Otx Pulses

File Search Tools Help

Name	Created	Updated
explorer	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: explorer

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	Ransomware
comment	potential threat

Description:

This is an IOC created for Internet Explorer

Add: AND OR Item

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

Activate Windows  
Go to Settings to activate Windows.

Save

Loaded IOCs: 8