



Mission Name

Indicators of Compromise

History Context

EUPHEA - Principal & Chancellor's office at Shanghai. The investigation leads to The Principal and the Chancellor. Ethan must place the bug.

Technical High-Level Overview

Player must locate how he/she managed to download the bug using a LOLBIN (certutil) of the operating system itself. To do so, he/she must identify the download URL.

Short Description

In previous missions, you had to check Ethan's bug but this, you're going to investigate how Ethan downloaded the bug into the system. Your goal will be to identify de URL used to download the bug. Finally you must calculate hash MD5, including http and so on.

Mission Description

Previously was the first time that you go to connect to a live Windows machine to investigate how Ethan placed the bug into the system. This time, you will face an offline evidence to check your capabilities in terms of finding indicators of compromise. Your goal will be to identify the URL used to download the bug. Finally you must calculate hash MD5, including http and so on.

Location

EUPHEA FACULTY | THE PRINCIPAL'S QUARTERS



Tools

- <https://github.com/AbdulRhmanAlfaifi/CryptnetURLCacheParser>
- <https://github.com/markmckinnon/Autopsy-Plugins>

Questions

Which is the size of the file downloaded in bytes?

- 123392

Which name was used, once the file was downloaded?

- winoffice.exe

Hints

1. Use Autopsy to mount the evidence provided.
2. Analyse all execution artifacts, specially Prefetch.
3. Use the timeline option On Autopsy to locate the file downloaded.



Write Up

Player should use Autopsy 4.9.0 version to mount the image provided:

The screenshot shows the 'New Case Information' dialog box for Autopsy. On the left, a sidebar titled 'Steps' shows '1. Case Information' (which is selected) and '2. Optional Information'. The main area is titled 'Case Information' and contains the following fields:

- 'Case Name:' input field containing 'C3-M4'
- 'Base Directory:' input field containing 'C:\THREATIA\Autopsy\' with a 'Browse' button to its right
- 'Case Type:' radio buttons for 'Single-User' (selected) and 'Multi-User'
- A note below the radio buttons stating 'Case data will be stored in the following directory:' followed by an input field containing 'C:\THREATIA\Autopsy\C3-M4'

Figure 1



Fill all the necessary information to create the case:

The screenshot shows a software interface titled "New Case Information". On the left, a sidebar lists "Steps": 1. Case Information and 2. Optional Information. The main area is titled "Optional Information". It contains sections for "Case" (Number: C3-M4), "Examiner" (Name, Phone, Email, Notes), and "Organization" (Organization analysis is being done for: Not Specified, Manage Organizations). The background features a stylized blue and white graphic.

Figure 2

Select the source of the information to analyse:

The screenshot shows a software interface titled "Add Data Source". On the left, a sidebar lists "Steps": 1. Select Type of Data Source To Add, 2. Select Data Source, 3. Configure Ingest Modules, and 4. Add Data Source. The main area is titled "Select Type of Data Source To Add". A red box highlights the first option, "Disk Image or VM File", which has a checked checkbox icon next to it. Other options listed are Local Disk, Logical Files, Unallocated Space Image File, Autopsy Logical Imager Results, and XRY Text Export. The background features a stylized blue and white graphic.

Figure 3

Once Autopsy requires you, to select ingest modules, player must select Windows Internals (Prefetch and ShimCache) and "All files and Directories":

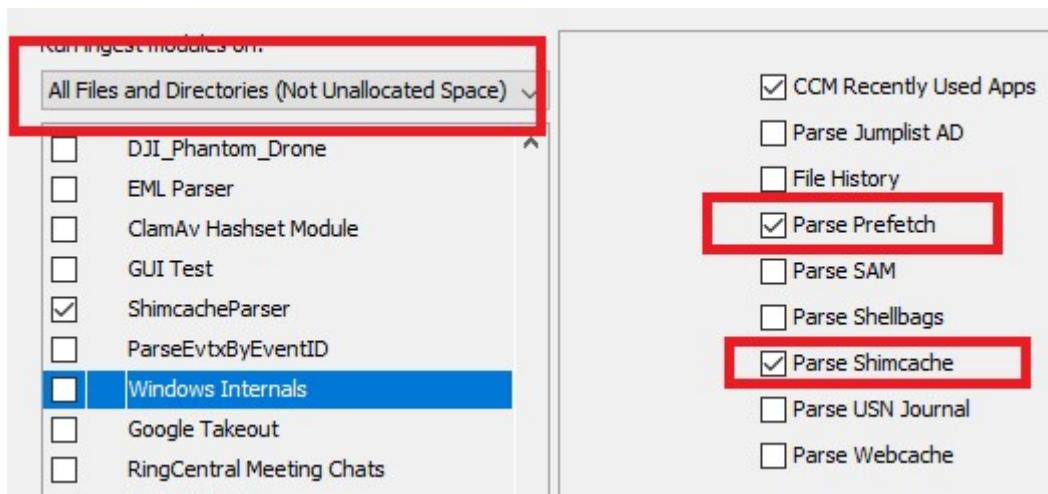


Figure 4

When Autopsy finishes, there will be two option on extracted content:

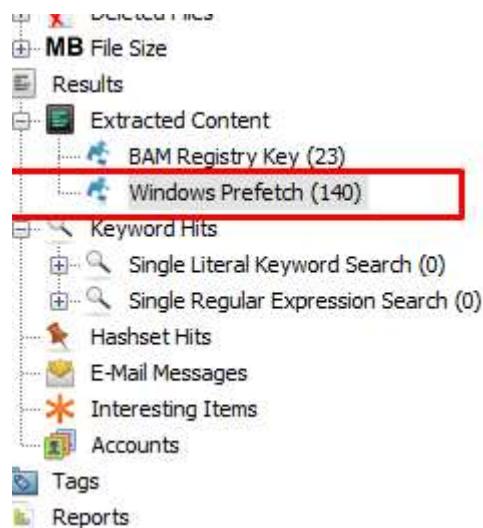


Figure 5

Select Prefetch folder and sort columns by first execution:



As you can see below, there is the typical processes tree when you executes something on command prompt:

1. CMD.exe
2. CONHOST.exe
3. CERTUTIL.exe

Source File	S	C	O	PF Execution DTTM 1
TASKHOSTW.EXE-2E5D4B75.pf				2021-06-20 22:44:33 CEST
RUNTIMEBROKER.EXE-318BAC70.pf				2021-06-20 22:44:34 CEST
SVCHOST.EXE-9F82877C.pf				2021-06-20 22:44:35 CEST
VSSVC.EXE-6C8F0C66.pf				2021-06-20 22:44:41 CEST
SVCHOST.EXE-BFF367D9.pf				2021-06-20 22:44:51 CEST
SVCHOST.EXE-FF256082.pf				2021-06-20 22:44:51 CEST
BACKGROUNDTRANSFERHOST.EXE-30A6F22E.pf				2021-06-20 22:45:06 CEST
RUNDLL32.EXE-BF72C764.pf				2021-06-20 22:45:11 CEST
RUNDLL32.EXE-FDCBB5A1.pf				2021-06-20 22:45:12 CEST
MPCMDRUN.EXE-2C9109F9.pf				2021-06-20 22:45:30 CEST
BACKGROUNDTASKHOST.EXE-4EED4AF4.pf				2021-06-20 22:45:32 CEST
WMIADAP.EXE-BB21CD77.pf				2021-06-20 22:45:33 CEST
WMIPRVSE.EXE-E8B8DD29.pf				2021-06-20 22:45:33 CEST
CMD.EXE-0BD30981.pf				2021-06-20 22:45:36 CEST
CONHOST.EXE-0C6456FB.pf				2021-06-20 22:45:36 CEST
CERTUTIL.EXE-28F1E0C1.pf				2021-06-20 22:45:48 CEST
DLLHOST.EXE-92F548BD.pf				2021-06-20 22:46:14 CEST
RUNTIMEBROKER.EXE-640D902C.pf				2021-06-20 22:46:14 CEST
SECHEALTHUI.EXE-B8DB14A2.pf				2021-06-20 22:46:14 CEST
SECURITYHEALTHHOST.EXE-06344EE9.pf				2021-06-20 22:46:14 CEST
CONSENT.EXE-40419367.pf				2021-06-20 22:46:16 CEST
BACKGROUNDTASKHOST.EXE-4A9935D7.pf				2021-06-20 22:46:17 CEST
NISSRV.EXE-09946424.pf				2021-06-20 22:46:17 CEST

Figure 6



This is the key for players. Next step would be to select the exact moment when certutil.exe was executed, right click on it and "View Source in Timeline"

The screenshot shows a table of file metadata. A context menu is open over the first row, which contains the file name 'CERTUTIL.EXE-28F1E0C1.pf' and its creation date '2021-06-20'. The menu options include:

- Properties
- View Result in Timeline...
- View Source File in Timeline...** (highlighted)
- View Source File in Directory
- View in New Window
- Open in External Viewer Ctrl+E
- Extract File(s)
- Export selected rows to CSV
- Add File Tag
- Add Result Tag

Figure 7

Select file created:

The dialog box title is 'View /img_C3-M4-cl1.vmdk/vol ... RTUTIL.EXE-28F1E0C1.pf in timeline.' It contains the following sections:

- Choose an event to show in timeline:** A table with columns 'Event Type' and 'Date/Time'. The 'File Created' row is selected and highlighted with a red box. The other rows are: 'File Accessed' (2021-06-20 22:45:49), 'File Changed' (2021-06-20 22:45:49), and 'File Modified' (2021-06-20 22:45:49).
- Choose the amount of time to show before and after the selected event:** A numeric input field set to '1' and a dropdown menu set to 'minuto'.
- Show Timeline** (highlighted with a red box) and **Cancelar** buttons at the bottom.

Figure 8

Finally, you will be able to identify:

- **DEL%20full.exe:** the previous name, it means, when certutil download the file before renaming. We will check in the following steps.
- **Winoffice.exe:** the name of the same file but renamed. To reach this conclusion, Winoffice has the same creation time as prefetch, and obviously the same hash.

EVERY	EVERYTHING	/Windows/Offline Web Pages/winoffice.exe
2021-06-20 22:45:48	MA_C	/Users/user/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData
2021-06-20 22:45:48	_B_	/Users/user/AppData/Local/Microsoft/Windows/INetCache/IE/YO59KXG1/DEL%20full[1].exe
2021-06-20 22:45:48	_A_	/Windows/WinSxS/amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.18362.30_none_e685621eb27f4d6a/comctl32.d
2021-06-20 22:45:48	_A_	/Windows/System32/dhcpcsvc.dll
2021-06-20 22:45:48	_A_	/Windows/WinSxS/amd64_microsoft-windows-lsa-secur32_31bf3856ad364e35_10.0.18362.1_none_bb7d0d66e96047be/secur32.dll
2021-06-20 22:45:48	_A_	/Windows/System32/ntdsapi.dll
2021-06-20 22:45:49	_A_	/Windows/System32/en-US/certutil.exe.mui
2021-06-20 22:45:49	MABC	/Windows/Offline Web Pages/winoffice.exe
2021-06-20 22:45:49	MABC	/Windows/Prefetch/CERTUTIL.EXE-28F1E0C1.pf

Figure 9

The new key to follow by players would be this folder:

- Users/user/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData

This folder is used by Certutil.exe to store information about downloads. If player performs a little search, he/she will be able to locate the necessary tool to parse it:

Figure 10

Player should download the tool and install it from:

- <https://github.com/AbdulRhmanAlfaifi/CryptnetURLCacheParser>

CryptnetURLCacheParser

CryptnetURLCacheParser is a tool to parse CryptAPI cache files located on the following paths:

```
C:\Windows\System32\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache
C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache
C:\Users\<USERNAME>\AppData\LocalLow\Microsoft\CryptnetUrlCache
```

The `metadata` folder contains metadata about the downloaded files. Each file contain the following data:

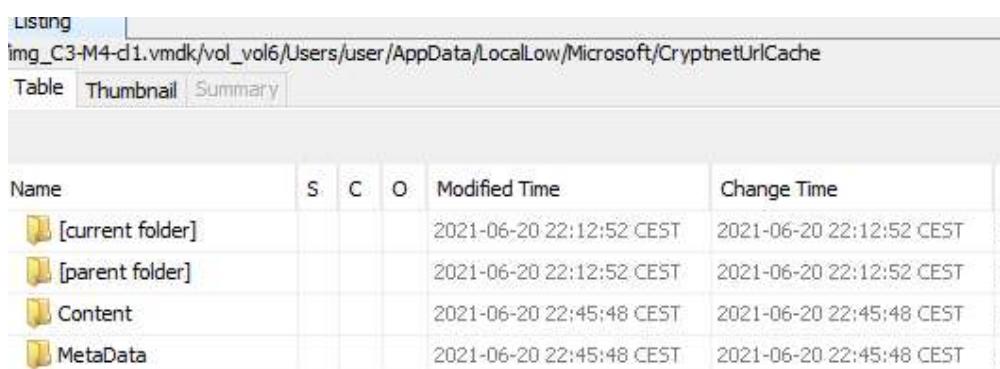
1. `Timestamp` : This is the last time the file was downloaded.
2. `URL` : The URL form where the file was downloaded.
3. `FileSize` : The downloaded file size in bytes.
4. `MetadataHash` : The hash for the downloaded file. The following is some of the hashing algorithms absorbed:
 - o SHA1
 - o SHA256
 - o MD5
5. `FullPath` : The full path for the parsed file.
6. `MD5 (Optional)` : The calculated MD5 hash for the actual file in the `content` folder. This field is only available if you used the `--useContent` option.

• **Figure 11**

First of all, we should extract from Autopsy, the following folder:

- C:\Users\<USERNAME>\AppData\LocalLow\Microsoft\CryptnetUrlCache

To achieve this, right click on the necessary folder and select "Export"



The screenshot shows the Autopsy interface with the following details:

- The title bar says "Listing" and the path is "img_C3-M4-d1.vmdk/vol_vol6/Users/user/AppData/LocalLow/Microsoft/CryptnetUrlCache".
- The top navigation bar has tabs: Listing, Table, Thumbnail, and Summary. The "Table" tab is selected.
- The main area displays a table with the following data:

Name	S	C	O	Modified Time	Change Time
[current folder]				2021-06-20 22:12:52 CEST	2021-06-20 22:12:52 CEST
[parent folder]				2021-06-20 22:12:52 CEST	2021-06-20 22:12:52 CEST
Content				2021-06-20 22:45:48 CEST	2021-06-20 22:45:48 CEST
MetaData				2021-06-20 22:45:48 CEST	2021-06-20 22:45:48 CEST

Figure 12



Eventually, player must launch **CryptnetUrlCacheParser.py** over Metadata extracted folder:

- python3 CryptnetUrlCacheParser.py -d ./CryptnetUrlCache/MetaData/ -o file_output.csv --outputFormat csv

And then open file_output.csv to identify the file downloaded:

```
ATLACIUS/140 / -C:\Windows\system32\cmd.exe\Windows7\102724\7AFA3111E00000000000000000000000\2_EEE4E23000  
"2021-06-20T20:45:48.860943", "http://karajjavad.ir/file/DEL%20full.exe", 123392, "", "  
"2021-06-20T20:16:21.763540", "http://ctldl.windowsupdate.com/msdownload/update/v3/s  
ata/FB0D848F74F70BB2EAA93746D24D9749"
```

Figure 13

The key is the timestamp, is the same as Prefetch timestamp. The URL for DEL%20full.exe is

- http://karajjavad.ir/file/DEL%20full.exe

Player must provide MD5 hash of the URL:

- 11DCCEE68815BC20DBBF06AC0C415439

Flag Information

flag{11DCCEE68815BC20DBBF06AC0C415439}