ENPM687 – Digital Forensics and Incidence Responses

Final Report

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

UID: 118428369

Email: iamibi@umd.edu

Brief Summary of Information

The goal of this document is to go over the Rebel malware hard drive recovered by the Imperial Army. This report will outline the findings and the steps involved in achieving them. The malware has reportedly been connecting with its command-and-control center to transmit information that might cause problems to the Imperial Army. The investigation performed as part of forensics found the plans for the Death Star which can help the Rebel army to initiate a counterattack on Imperial Army.

Tools Used in the investigation

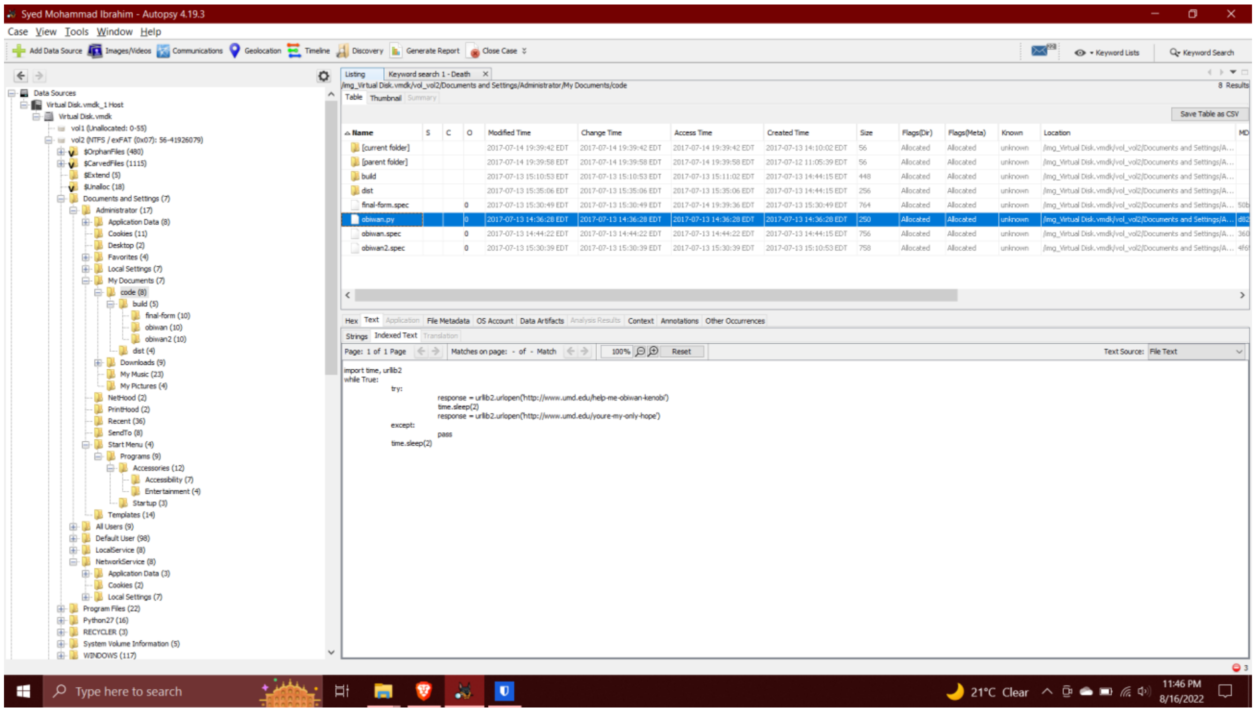
- Autopsy
- WireShark
- VeraCrypt

Repository

The following steps were involved in the forensics investigation which yielded the plans for the Death Star that were sent by the malware to C2:

1. The hard drive image provided was of windows XP. The image was loaded in the Autopsy, and it generated the file system hierarchy.
2. While traversing the directories in the “vol2”, I found that under “Documents and Settings/Administrator/Recent” there were a few interesting entries like “obiwan.lnk”, “obiwan2.lnk”. Also, there were a few files that said “plans” in their names like “the-official-rogue-one-death-star-plans-are-revealed.lnk”, etc.
3. Then I proceeded to traverse other folders and found the binaries named “obiwan.exe” and “obiwan2.exe” at the location “Documents and Settings/Administrator/My Documents/code/dist/”. These binaries were generated by the python package called pyinstaller as there were “spec” files present.
4. Along with the binaries, in a folder up, there was a source file called “obiwan.py” which contained the source code of the assumed obiwan.exe binary. However, there were two

different binaries found, which questioned the piece of code legitimacy. The only way to confirm is to run them in an isolated environment and track their network calls.



Syed Mohammad Ibrahim - Autopsy 4.19.3

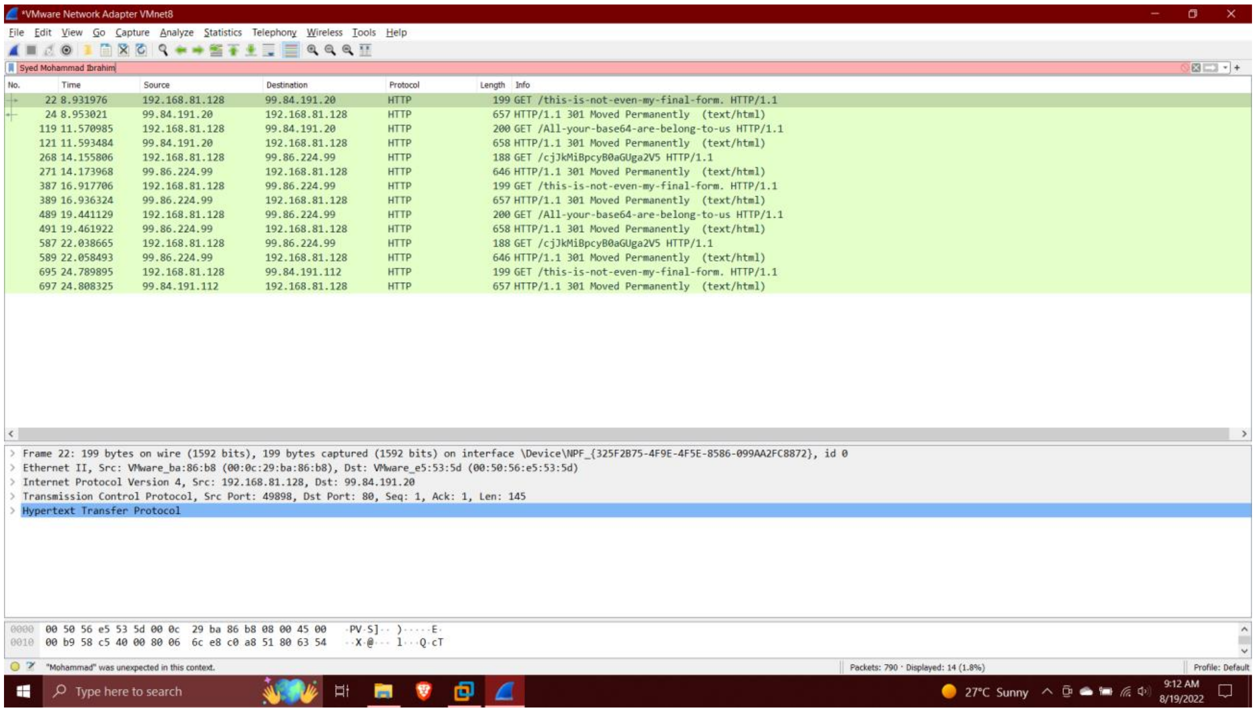
```
Data Sources
  Virtual Disk.vmdk_1 Host
    Virtual Disk.vmdk
      vol1 (Unallocated: 0-55)
      vol2 (NTFS / exFAT (0x07): 56-41926079)
        $OrphanFiles (480)
        $CarvedFiles (1115)
        $Extend (5)
        $Unalloc (18)
        Documents and Settings (7)
          Administrator (17)
            Application Data (8)
            Cookies (11)
            Desktop (2)
            Favorites (4)
            Local Settings (7)
            My Documents (7)
              code (8)
                build (5)
                  final-form (10)
                  obiwan (10)
                  obiwan2 (10)
                dist (4)
              Downloads (9)
              My Music (23)
              My Pictures (4)
            NetHood (2)
            PrintHood (2)
            Recent (36)
            SendTo (8)
            Start Menu (4)
              Programs (9)
                Accessories (12)
                  Accessibility (7)
                  Entertainment (4)
                Startup (3)
            Templates (14)
          All Users (9)
          Default User (98)
          LocalService (8)
          NetworkService (8)
            Application Data (3)
            Cookies (2)
            Local Settings (7)
        Program Files (22)
        Python27 (16)
        RECYCLER (3)
        System Volume Information (5)
        WINDOWS (117)
```

/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/code — 8 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2017-07-14 19:39:42 EDT	2017-07-14 19:39:42 EDT	2017-07-14 19:39:42 EDT	2017-07-13 14:10:02 EDT	56	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/A...
[parent folder]				2017-07-14 19:39:58 EDT	2017-07-14 19:39:58 EDT	2017-07-14 19:39:58 EDT	2017-07-12 11:05:39 EDT	56	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/A...
build				2017-07-13 15:10:53 EDT	2017-07-13 15:10:53 EDT	2017-07-13 15:11:02 EDT	2017-07-13 14:44:15 EDT	448	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/A...
dist				2017-07-13 15:35:06 EDT	2017-07-13 15:35:06 EDT	2017-07-13 15:35:06 EDT	2017-07-13 14:44:15 EDT	256	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/A...
final-form.spec			0	2017-07-13 15:30:49 EDT	2017-07-13 15:30:49 EDT	2017-07-14 19:39:36 EDT	2017-07-13 15:30:49 EDT	764	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/A...
obiwan.py			0	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	250	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/A...
obiwan.spec			0	2017-07-13 14:44:22 EDT	2017-07-13 14:44:22 EDT	2017-07-13 14:44:22 EDT	2017-07-13 14:44:15 EDT	756	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/A...
obiwan2.spec			0	2017-07-13 15:30:39 EDT	2017-07-13 15:30:39 EDT	2017-07-13 15:30:39 EDT	2017-07-13 15:10:53 EDT	758	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/A...

```python
import time, urllib2
while True:
        try:
                response = urllib2.urlopen('http://www.umd.edu/help-me-obiwan-kenobi')
                time.sleep(2)
                response = urllib2.urlopen('http://www.umd.edu/youre-my-only-hope')
        except:
                pass
        time.sleep(2)
```

5. The binary "obiwan2.exe" was run in an isolated environment with WireShark monitoring the network traffic. It made the calls shown in the below picture:



*VMware Network Adapter VMnet8

Filter: Syed Mohammad Ibrahim

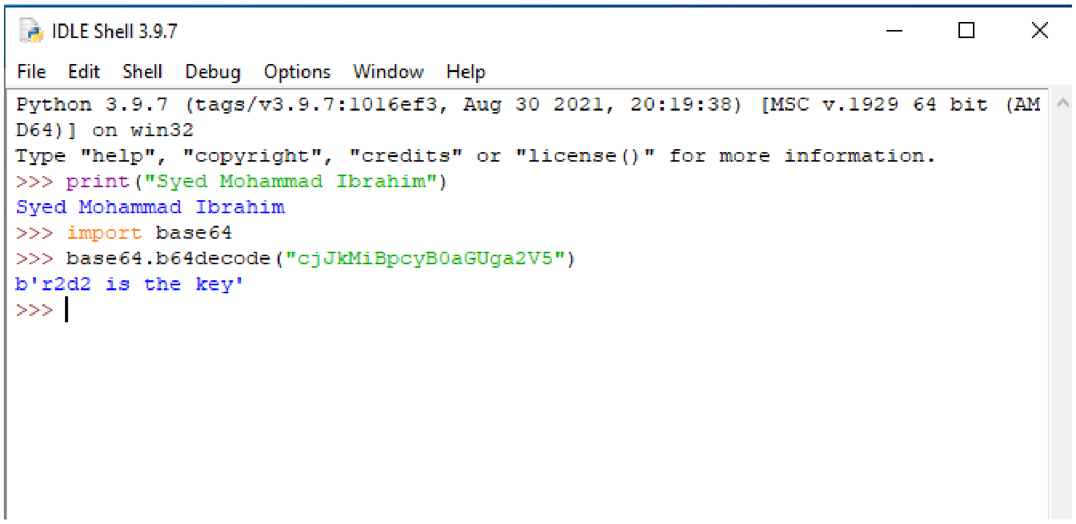
```
No.  Time       Source          Destination     Protocol  Length Info
  22 8.931976   192.168.81.128  99.84.191.20    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
  24 8.953021   99.84.191.20    192.168.81.128  HTTP      657 HTTP/1.1 301 Moved Permanently  (text/html)
 119 11.570985  192.168.81.128  99.84.191.20    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
 121 11.593484  99.84.191.20    192.168.81.128  HTTP      658 HTTP/1.1 301 Moved Permanently  (text/html)
 268 14.155806  192.168.81.128  99.86.224.99    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
 271 14.173968  99.86.224.99    192.168.81.128  HTTP      646 HTTP/1.1 301 Moved Permanently  (text/html)
 387 16.917706  192.168.81.128  99.86.224.99    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
 389 16.936324  99.86.224.99    192.168.81.128  HTTP      657 HTTP/1.1 301 Moved Permanently  (text/html)
 489 19.441129  192.168.81.128  99.86.224.99    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
 491 19.461922  99.86.224.99    192.168.81.128  HTTP      658 HTTP/1.1 301 Moved Permanently  (text/html)
 587 22.038665  192.168.81.128  99.86.224.99    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
 589 22.058493  99.86.224.99    192.168.81.128  HTTP      646 HTTP/1.1 301 Moved Permanently  (text/html)
 695 24.789895  192.168.81.128  99.84.191.112   HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
 697 24.808325  99.84.191.112   192.168.81.128  HTTP      657 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
> Frame 22: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface \Device\NPF_{325F2B75-4F9E-4F5E-8586-099AA2FC8872}, id 0
> Ethernet II, Src: VMware_ba:86:b8 (00:0c:29:ba:86:b8), Dst: VMware_e5:53:5d (00:50:56:e5:53:5d)
> Internet Protocol Version 4, Src: 192.168.81.128, Dst: 99.84.191.20
> Transmission Control Protocol, Src Port: 49898, Dst Port: 80, Seq: 1, Ack: 1, Len: 145
> Hypertext Transfer Protocol
```

```
0000  00 50 56 e5 53 5d 00 0c  29 ba 86 b8 08 00 45 00   ·PV·S]·· )·····E·
0010  00 b9 58 c5 40 00 80 06  6c e8 c0 a8 51 80 63 54   ··X·@··· l···Q·cT
```

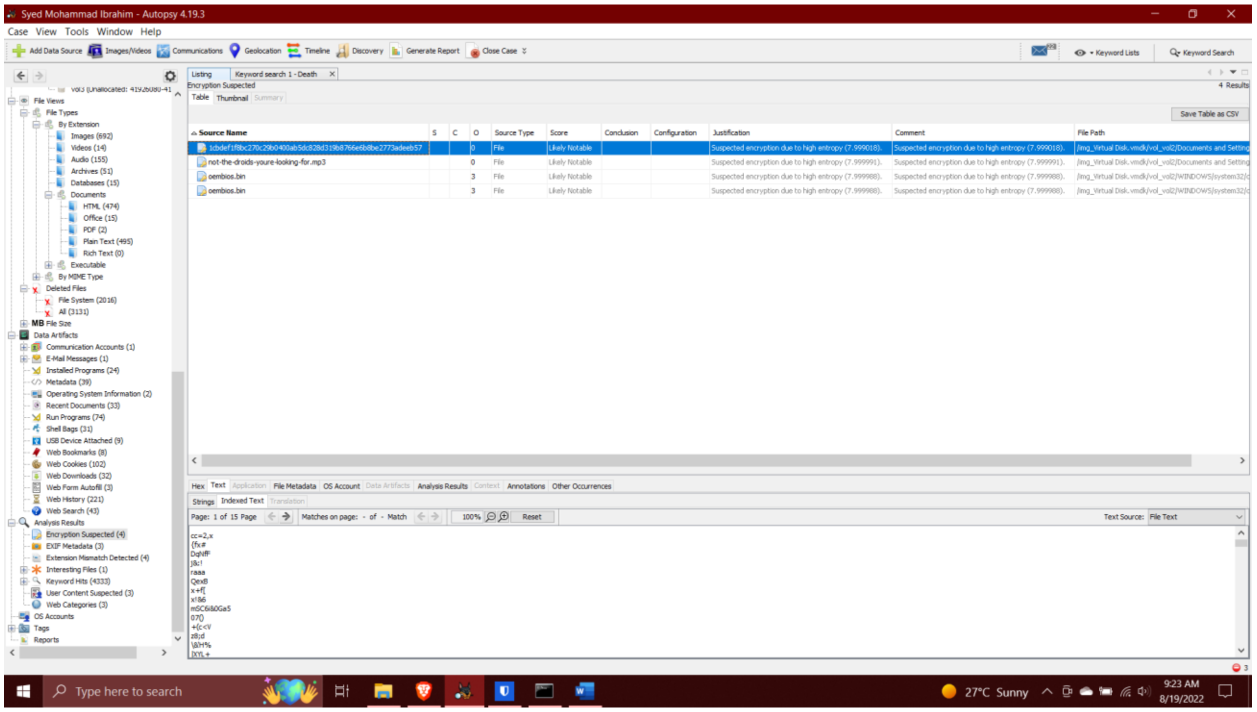
"Mohammad" was unexpected in this context. | Packets: 790 · Displayed: 14 (1.8%) | Profile: Default

6. The GET request "/All-your-base64-are-belong-to-us" pointed out that there is a presence of base64 type string. Looking at another GET request "/cjJkMiBpcyB0aGUga2V5", it seemed that this is a base64 string. So, I decoded it with python's base64 decoder.



```
Python 3.9.7 (tags/v3.9.7:1016ef3, Aug 30 2021, 20:19:38) [MSC v.1929 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> print("Syed Mohammad Ibrahim")
Syed Mohammad Ibrahim
>>> import base64
>>> base64.b64decode("cjJkMiBpcyB0aGUga2V5")
b'r2d2 is the key'
>>>
```

7. This indicated that there is potential an encrypted text or file which will require this key to be used. I searched the image in autopsy again and found few files which autopsy indicated as encrypted. However, I didn't know what kind of tool or encryption algorithm was used to encrypt them. I searched other folders and found a VeraCrypt tool binary. After googling, I found that it is an encryption utility tool which I believed was used to encrypt these files.



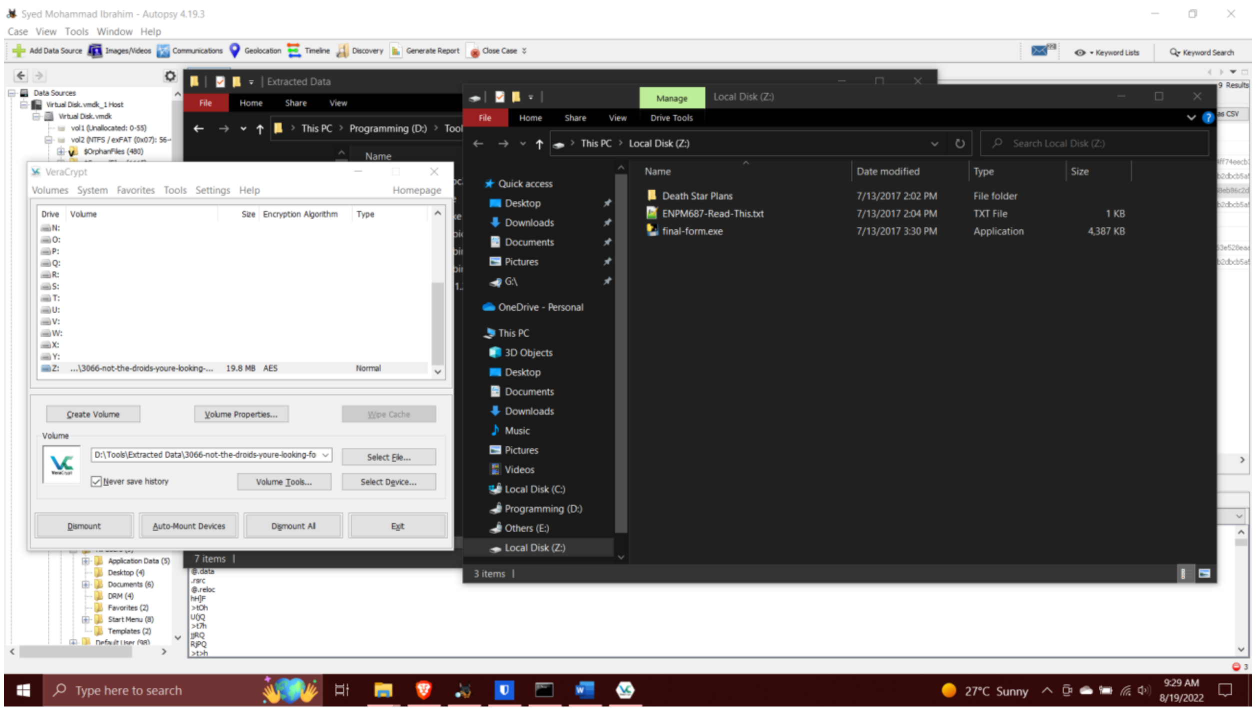
Encryption Suspected — 4 Results

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment	File Path
1cbdef1f8bc270c29b0400ab5dc828d319b8766e6b8be2773adeeb57			0	File	Likely Notable			Suspected encryption due to high entropy (7.999018).	Suspected encryption due to high entropy (7.999018).	/img_Virtual Disk.vmdk/vol_vol2/Documents and Setting
not-the-droids-youre-looking-for.mp3			0	File	Likely Notable			Suspected encryption due to high entropy (7.999991).	Suspected encryption due to high entropy (7.999991).	/img_Virtual Disk.vmdk/vol_vol2/Documents and Setting
oembios.bin			3	File	Likely Notable			Suspected encryption due to high entropy (7.999988).	Suspected encryption due to high entropy (7.999988).	/img_Virtual Disk.vmdk/vol_vol2/WINDOWS/system32/
oembios.bin			3	File	Likely Notable			Suspected encryption due to high entropy (7.999988).	Suspected encryption due to high entropy (7.999988).	/img_Virtual Disk.vmdk/vol_vol2/WINDOWS/system32/

```
cc=2,x
{fx#
DqNfF
j8:!
raaa
QexB
x+f[
x!&6
mSC6i&0Ga5
07()
+(c<V
z8;d
\8H%
|XYL+
```

Syed Mohammad Ibrahim - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing Keyword search 1 - Death
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Indexed Text Translation
Page: 1 of 15 Page
Text Source: File Text
Type here to search
27°C Sunny
9:23 AM
8/19/2022

8. I downloaded the tool, installed, and ran it on the files that I extracted with the "r2d2" key. Only one file was successfully decrypted named "3066-not-the-droids-youre-looking-for.mp3". I mounted it on virtual drive "Z".



Drive	Volume	Size	Encryption Algorithm	Type
Z:	...\3066-not-the-droids-youre-looking-...	19.8 MB	AES	Normal

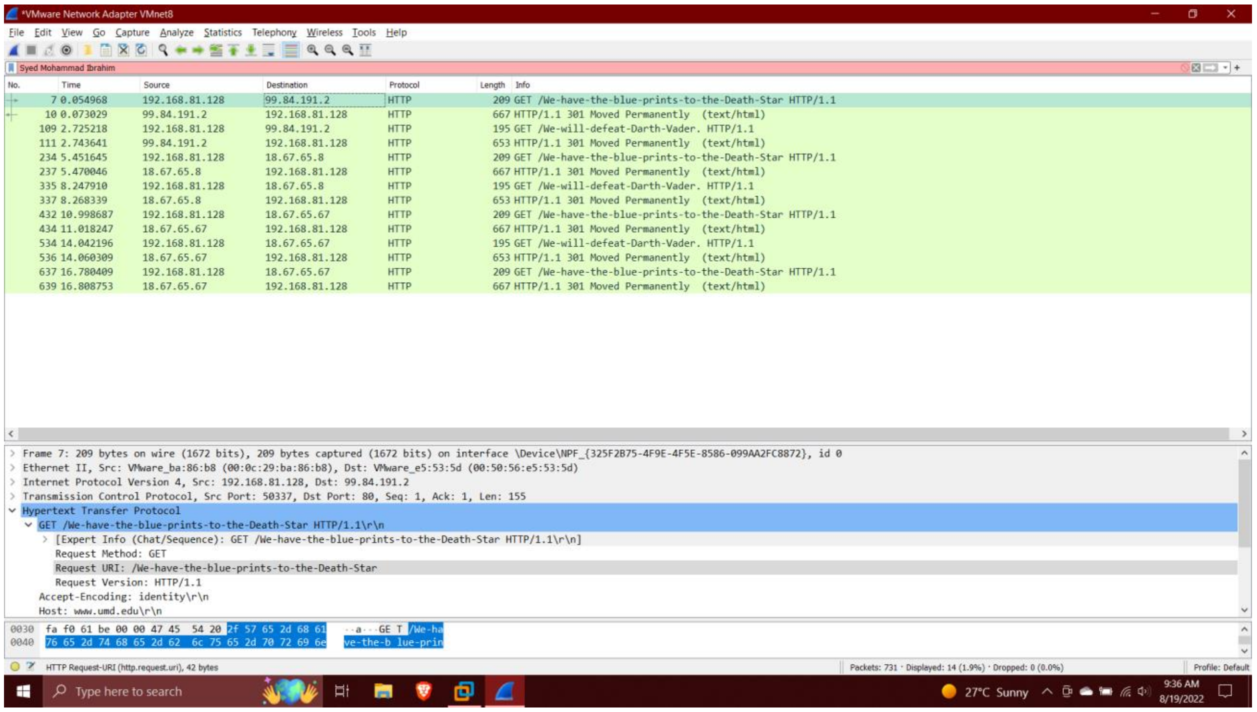
Volume: D:\Tools\Extracted Data\3066-not-the-droids-youre-looking-fo

Local Disk (Z:)

Name	Date modified	Type	Size
Death Star Plans	7/13/2017 2:02 PM	File folder	
ENPM687-Read-This.txt	7/13/2017 2:04 PM	TXT File	1 KB
final-form.exe	7/13/2017 3:30 PM	Application	4,387 KB

3 items

9. I read the ENPM687-Read-This.txt file which stated that the final version of the malware "final-form.exe" has sent few messages. I ran the binary in an isolated environment with WireShark tracking the network calls and found the following



*VMware Network Adapter VMnet8

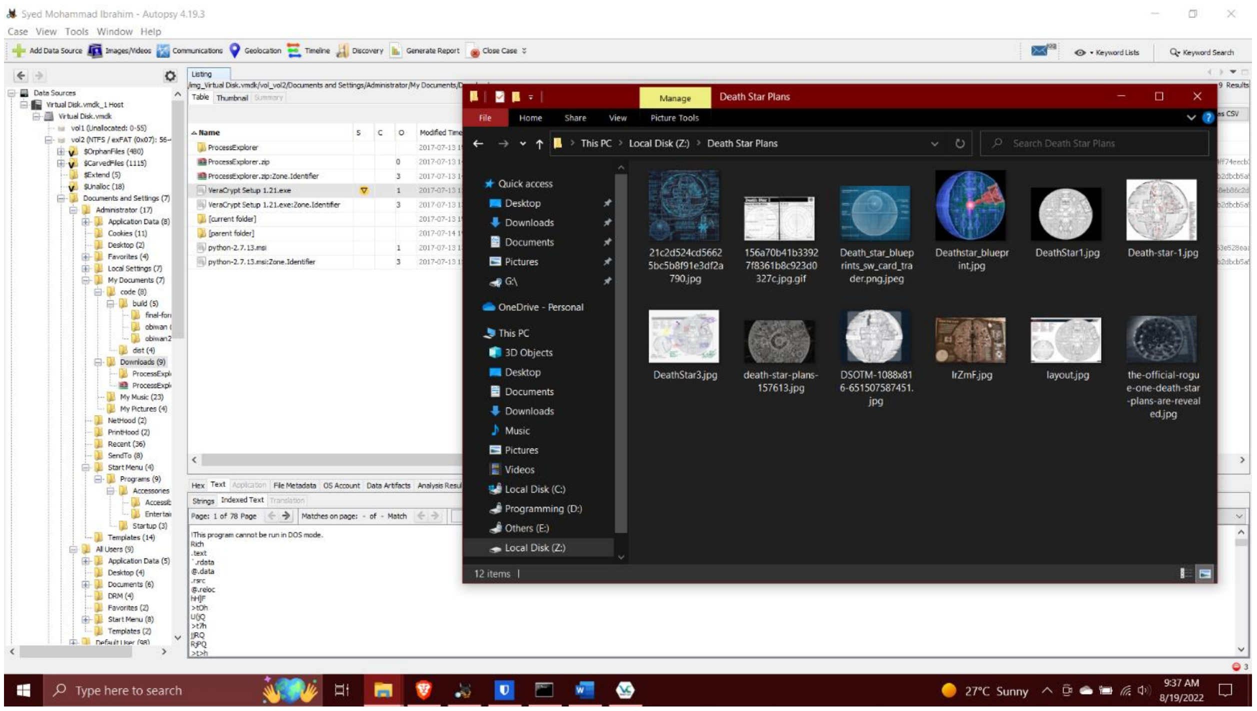
```
No.   Time       Source          Destination     Protocol  Length Info
    7 0.054968   192.168.81.128  99.84.191.2     HTTP      209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
   10 0.073029   99.84.191.2     192.168.81.128  HTTP      667 HTTP/1.1 301 Moved Permanently  (text/html)
  109 2.725218   192.168.81.128  99.84.191.2     HTTP      195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  111 2.743641   99.84.191.2     192.168.81.128  HTTP      653 HTTP/1.1 301 Moved Permanently  (text/html)
  234 5.451645   192.168.81.128  18.67.65.8      HTTP      209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  237 5.470046   18.67.65.8      192.168.81.128  HTTP      667 HTTP/1.1 301 Moved Permanently  (text/html)
  335 8.247910   192.168.81.128  18.67.65.8      HTTP      195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  337 8.268339   18.67.65.8      192.168.81.128  HTTP      653 HTTP/1.1 301 Moved Permanently  (text/html)
  432 10.998687  192.168.81.128  18.67.65.67     HTTP      209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  434 11.018247  18.67.65.67     192.168.81.128  HTTP      667 HTTP/1.1 301 Moved Permanently  (text/html)
  534 14.042196  192.168.81.128  18.67.65.67     HTTP      195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  536 14.060309  18.67.65.67     192.168.81.128  HTTP      653 HTTP/1.1 301 Moved Permanently  (text/html)
  637 16.780409  192.168.81.128  18.67.65.67     HTTP      209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  639 16.808753  18.67.65.67     192.168.81.128  HTTP      667 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
> Frame 7: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF_{325F2B75-4F9E-4F5E-8586-099AA2FC8872}, id 0
> Ethernet II, Src: VMware_ba:86:b8 (00:0c:29:ba:86:b8), Dst: VMware_e5:53:5d (00:50:56:e5:53:5d)
> Internet Protocol Version 4, Src: 192.168.81.128, Dst: 99.84.191.2
> Transmission Control Protocol, Src Port: 50337, Dst Port: 80, Seq: 1, Ack: 1, Len: 155
v Hypertext Transfer Protocol
  v GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /We-have-the-blue-prints-to-the-Death-Star
      Request Version: HTTP/1.1
    Accept-Encoding: identity\r\n
    Host: www.umd.edu\r\n

0030  fa f0 61 be 00 00 47 45  54 20 2f 57 65 2d 68 61   ··a···GE T /We-ha
0040  76 65 2d 74 68 65 2d 62  6c 75 65 2d 70 72 69 6e   ve-the-b lue-prin

HTTP Request-URI (http.request.uri), 42 bytes    Packets: 731 · Displayed: 14 (1.9%) · Dropped: 0 (0.0%)    Profile: Default
```

10. The final message sent by the Rebel malware was captured and there were plans present in the mounted drive with title "Death Star Plans".



/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/D

Name	S	C	O	Modified Time
ProcessExplorer				2017-07-13 1
ProcessExplorer.zip			0	2017-07-13 1
ProcessExplorer.zip:Zone.Identifier			3	2017-07-13 1
VeraCrypt Setup 1.21.exe	▽		1	2017-07-13 1
VeraCrypt Setup 1.21.exe:Zone.Identifier			3	2017-07-13 1
[current folder]				2017-07-13 1
[parent folder]				2017-07-14 1
python-2.7.13.msi			1	2017-07-13 1
python-2.7.13.msi:Zone.Identifier			3	2017-07-13 1

```
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
@.reloc
```

21c2d524cd56625bc5b8f91e3df2a790.jpg
156a70b41b33927f8361b8c923d0327c.jpg.gif
Death_star_blueprints_sw_card_trader.png.jpeg
Deathstar_blueprint.jpg
DeathStar1.jpg
Death-star-1.jpg
DeathStar3.jpg
death-star-plans-157613.jpg
DSOTM-1088x816-651507587451.jpg
IrZmF.jpg
layout.jpg
the-official-rogue-one-death-star-plans-are-revealed.jpg

Recommendations

The final message recovered has made the Rebel army aware of the Death Star plans. It is recommended that the Imperial Army add security to their communication channels and make sure that such detail plans are encrypted with a better key length (minimum 15 characters). The key should also be stored in a secure fashion as Base64 is a weak scrambling algorithm. One can always use a Password Manager for storing such sensitive passwords.

Challenges during investigation

1. It took a lot of time to figure out what kind of tool or utility was used to encrypt the files. Googling a lot of things that can potentially be a tool or using a python script to encrypt was a big blocker for me. Eventually, I landed on veracrypt binary and its details.
2. The veracrypt is not an easy-to-use tool. I had to search and read documentations on how to use it to finally figure it out.