

Summary.

At a great cost the Imperial Army has come into possession of an image of a hard drive for a rebel scum malware writer. Their codes have plagued our computers for the last time, infecting them but also using it to send messages across the galaxy. The mission is to analyze the image of the Rebel malware writer hard drive. Find out what their newest "malware" does, any messages it may send out, and review the image for other useful intelligence. Is it trying to corrupt different files? What kind of messages it is trying to send? Where it is located what is its behavior? By making use of forensics tools and intelligence we have to investigate the scenario.

Tools used in this forensics investigation.

1. Autopsy.
2. Wireshark.
3. VeraCrypt.

Repository.

In this scenario I am going to find the final form of the malware that has infected Imperial Force's system and also sending message across the galaxy. I went through the hard drive and found the below evidences which can be really helpful to catch the final form of the malware sent by rebels.

Aayushi Dubey ENPM687 - Autopsy 4.16.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

Recent Documents

Table Thumbnail

Source File S C O Path Date/Time Data Source

Death_star_blueprints_sw_card_trader.png.jpg M:\Death Star Plans\Death_star_blueprints_sw_card_trader.png.jpg 2017-07-13 11:02:59 PDT Virtual Disk.vmdk

Menuettos_1_2_from_41st_Symphony.Ink C:\Documents and Settings\Administrator\My Documents\My Music\Menuettos_1_2_from_41st_Symphony.Ink 2017-07-13 11:07:31 PDT Virtual Disk.vmdk

156a70b41b339278361bdc923d0327c.jpg.gif M:\Death Star Plans\156a70b41b339278361bdc923d0327c.jpg.gif 2017-07-13 11:02:38 PDT Virtual Disk.vmdk

21c2d524cd56625bc5b8f91e3df2a790.jpg M:\Death Star Plans\21c2d524cd56625bc5b8f91e3df2a790.jpg 2017-07-13 11:02:54 PDT Virtual Disk.vmdk

blah.Ink C:\Documents and Settings\Administrator\My Documents\code\blah.py 2017-07-14 16:39:27 PDT Virtual Disk.vmdk

Bournee_4th_Lute_Suite-Bach.Ink C:\Documents and Settings\Administrator\My Documents\My Music\Bournee_4th_Lute_Suite-Bach.Ink 2017-07-13 11:07:12 PDT Virtual Disk.vmdk

code.Ink C:\Documents and Settings\Administrator\My Documents\code 2017-07-13 11:36:28 PDT Virtual Disk.vmdk

Concerto-4-Violini-2_Telemann.Ink C:\Documents and Settings\Administrator\My Documents\My Music\Concerto-4-Violini-2_Telemann.Ink 2017-07-13 11:06:51 PDT Virtual Disk.vmdk

Courante_1st_Cello_Suite.Ink C:\Documents and Settings\Administrator\My Documents\My Music\Courante_1st_Cello_Suite.Ink 2017-07-13 11:07:46 PDT Virtual Disk.vmdk

Death Star Plans.Ink M:\Death Star Plans 2017-07-13 11:02:25 PDT Virtual Disk.vmdk

Death-star-1.Ink M:\Death Star Plans\Death-star-1.jpg 2017-07-13 11:02:47 PDT Virtual Disk.vmdk

death-star-plans-157613.Ink M:\Death Star Plans\death-star-plans-157613.jpg 2017-07-13 11:02:42 PDT Virtual Disk.vmdk

DeathStar1.Ink M:\Death Star Plans\DeathStar1.jpg 2017-07-13 11:02:32 PDT Virtual Disk.vmdk

DeathStar3.Ink M:\Death Star Plans\DeathStar3.jpg 2017-07-13 11:03:09 PDT Virtual Disk.vmdk

Deathstar_blueprint.Ink M:\Death Star Plans\Deathstar_blueprint.jpg 2017-07-13 11:03:03 PDT Virtual Disk.vmdk

layout.Ink M:\Death Star Plans\layout.jpg 2017-07-13 11:02:29 PDT Virtual Disk.vmdk

Local Disk (N).Ink M:\ 2017-07-13 11:03:46 PDT Virtual Disk.vmdk

Read-This.Ink M:\Read-This.txt 2017-07-13 11:03:46 PDT Virtual Disk.vmdk

the-official-rogue-one-death-star-plans-are-revealed.Ink M:\Death Star Plans\the-official-rogue-one-death-star-plans-are-revealed.jpg 2017-07-13 11:02:50 PDT Virtual Disk.vmdk

Downloads.Ink C:\Documents and Settings\Administrator\My Documents\Downloads 2017-07-13 10:56:01 PDT Virtual Disk.vmdk

DSOTM-1088x816-651507587451.Ink M:\Death Star Plans\DSOTM-1088x816-651507587451.jpg 2017-07-13 11:02:25 PDT Virtual Disk.vmdk

final-form.Ink C:\Documents and Settings\Administrator\My Documents\code\final-form.py 2017-07-13 11:40:46 PDT Virtual Disk.vmdk

get-pip.Ink C:\Documents and Settings\Administrator\My Documents\Downloads\get-pip.py 2017-07-13 10:56:01 PDT Virtual Disk.vmdk

Gigue_3rd_Cello_Suite-Bach.Ink C:\Documents and Settings\Administrator\My Documents\My Music\Gigue_3rd_Cello_Suite-Bach.Ink 2017-07-13 11:07:25 PDT Virtual Disk.vmdk

Ir2mf.Ink M:\Death Star Plans\Ir2mf.jpg 2017-07-13 11:03:19 PDT Virtual Disk.vmdk

Largo-from-Concerto-No5_JS_Bach.Ink C:\Documents and Settings\Administrator\My Documents\My Music\Largo-from-Concerto-No5_JS_Bach.Ink 2017-07-13 11:07:06 PDT Virtual Disk.vmdk

My Music.Ink C:\Documents and Settings\Administrator\My Documents\My Music 2017-07-13 11:06:05 PDT Virtual Disk.vmdk

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 1 of 1 Result: 1 of 1

Type Value Source(s)

Path M:\Death Star Plans\Death_star_blueprints_sw_card_trader.png.jpg RecentActivity

Path ID -1 RecentActivity

Date/Time 2017-07-13 11:02:59 RecentActivity

Source File Path /img_Virtual Disk.vmdk\vol_vol2\Documents and Settings\Administrator\Recent\Death_star_blueprints_sw_card_trader.png.jpg

Artifact ID -9223372036854775437

Analyzing files from Virtual Disk.vmdk 9% (1 more...)

9:06 AM 12/11/2020

In "Recent Documents" folder I have found some interesting items code.Ink, death star plans, blueprint and many more things related to death star and those were accessed recently. There may be possibility that the death star plans were already leaked to the rebels.

Aayushi Dubey ENPM687 - Autopsy 4.16.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

Recent Documents

Table Thumbnail

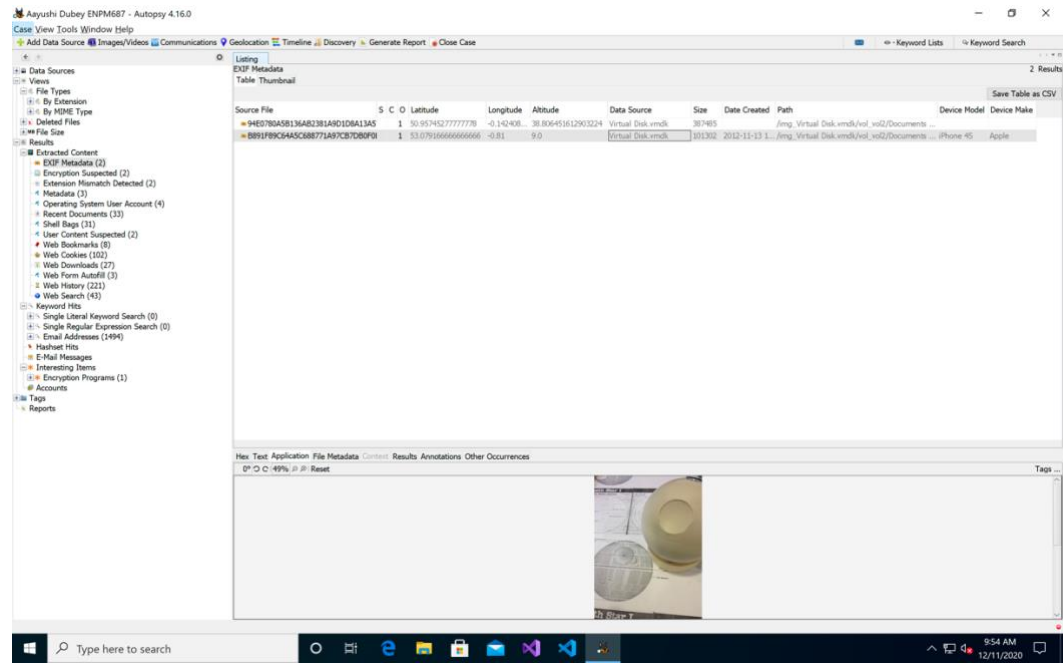
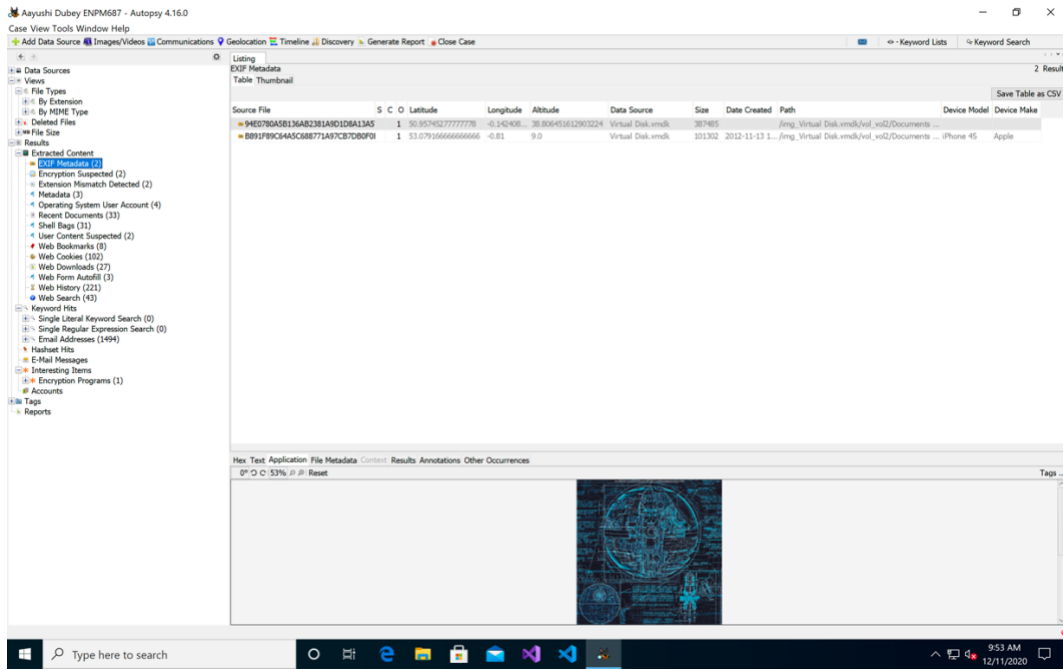
33 Results

Save Table as CSV

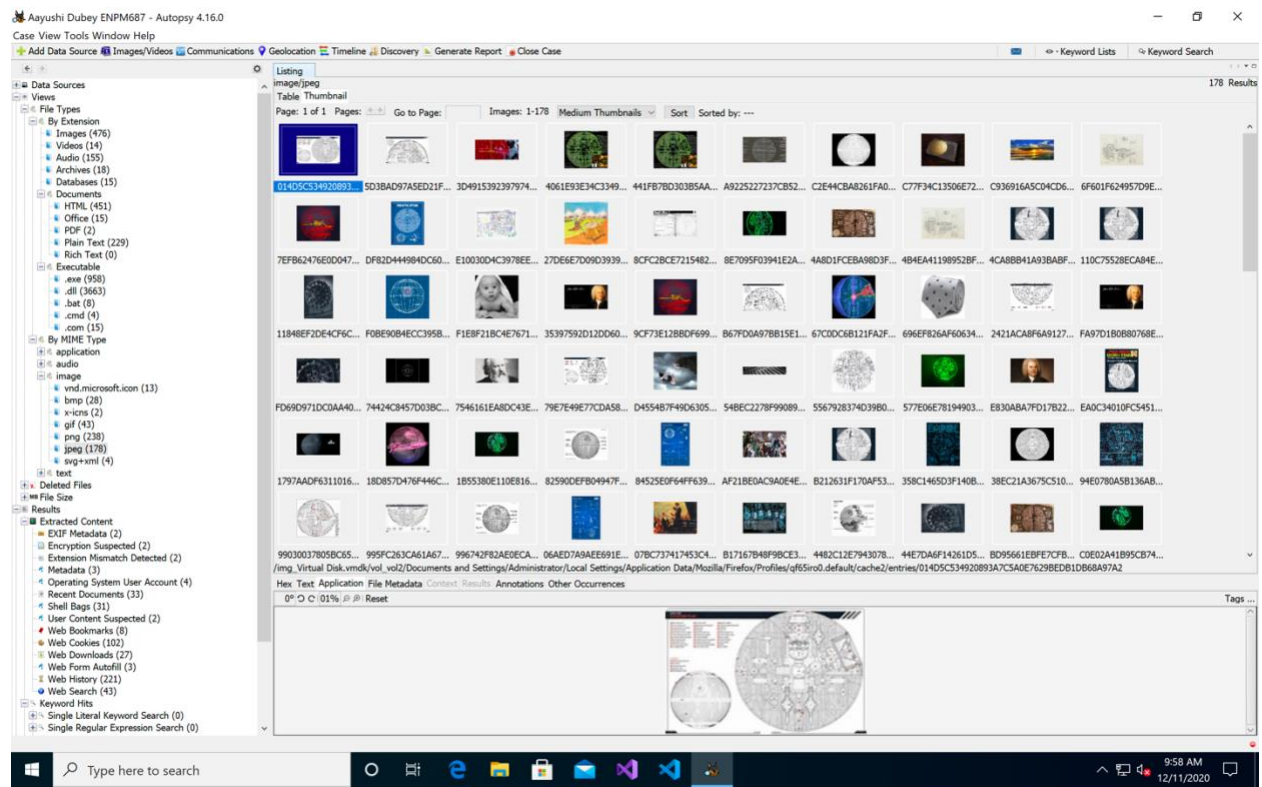
Source File	S	C	O	Path	Date/Time	Data Source
Concerto+4+Violin+Z. Jeleman.Ink				C:\Documents and Settings\Administrator\My Documents\My Music\Concerto+4+Violin+Z...	2017-07-13 11:06:31 PDT	Virtual Disk.vrm
Courante_1st_Cello_Suite.Ink				C:\Documents and Settings\Administrator\My Documents\My Music\Courante_1st_Cello...	2017-07-13 11:07:46 PDT	Virtual Disk.vrm
Death Star Plans.Ink				M:\Death Star Plans	2017-07-13 11:02:25 PDT	Virtual Disk.vrm
Death-star-1.Ink				M:\Death Star Plans\Death-star-1.jpg	2017-07-13 11:02:47 PDT	Virtual Disk.vrm
death-star-plans-157613.Ink				M:\Death Star Plans\death-star-plans-157613.jpg	2017-07-13 11:02:42 PDT	Virtual Disk.vrm
DeathStar1.Ink				M:\Death Star Plans\DeathStar1.jpg	2017-07-13 11:02:32 PDT	Virtual Disk.vrm
DeathStar3.Ink				M:\Death Star Plans\DeathStar3.jpg	2017-07-13 11:03:09 PDT	Virtual Disk.vrm
Deathstar_blueprint.Ink				M:\Death Star Plans\Deathstar_blueprint.jpg	2017-07-13 11:03:03 PDT	Virtual Disk.vrm
layout.Ink				M:\Death Star Plans\layout.jpg	2017-07-13 11:02:29 PDT	Virtual Disk.vrm
Local Disk (M).Ink				M:\	2017-07-13 11:03:46 PDT	Virtual Disk.vrm
Read-This.Ink				M:\Read-This.txt	2017-07-13 11:03:46 PDT	Virtual Disk.vrm
the-official-rogue-one-death-star-plans-are-revealed.Ink				M:\Death Star Plans\the-official-rogue-one-death-star-plans-are-revealed.jpg	2017-07-13 11:02:50 PDT	Virtual Disk.vrm
Downloads.Ink				C:\Documents and Settings\Administrator\My Documents\Downloads	2017-07-13 10:56:01 PDT	Virtual Disk.vrm
D507H-1088b616-651507587451.Ink				M:\Death Star Plans\D507H-1088b616-651507587451.jpg	2017-07-13 11:02:25 PDT	Virtual Disk.vrm
final-form.Ink				C:\Documents and Settings\Administrator\My Documents\code\final-form.py	2017-07-13 11:40:46 PDT	Virtual Disk.vrm
get-pip.Ink				C:\Documents and Settings\Administrator\My Documents\Downloads\get-pip.py	2017-07-13 10:56:01 PDT	Virtual Disk.vrm
Gigue_3rd_Cello_Suite-Bach.Ink				C:\Documents and Settings\Administrator\My Documents\My Music\Gigue_3rd_Cello_Su...	2017-07-13 11:07:25 PDT	Virtual Disk.vrm
IrZnF.Ink				M:\Death Star Plans\IrZnF.jpg	2017-07-13 11:03:19 PDT	Virtual Disk.vrm
Largo+from+Concerto-No5_35_Bach.Ink				C:\Documents and Settings\Administrator\My Documents\My Music\Largo+from+Conc...	2017-07-13 11:07:06 PDT	Virtual Disk.vrm
My Music.Ink				C:\Documents and Settings\Administrator\My Documents\My Music	2017-07-13 11:06:05 PDT	Virtual Disk.vrm
obiwan.Ink				C:\Documents and Settings\Administrator\My Documents\code\obiwan.py	2017-07-13 11:36:28 PDT	Virtual Disk.vrm
obiwan2.Ink				C:\Documents and Settings\Administrator\My Documents\code\obiwan2.py	2017-07-13 11:38:52 PDT	Virtual Disk.vrm
Rhapsody_No2_G-Minor_Brahms.Ink				C:\Documents and Settings\Administrator\My Documents\My Music\Rhapsody_No2_G-M...	2017-07-13 11:06:58 PDT	Virtual Disk.vrm
Scherzo+No1_+Chopin.Ink				C:\Documents and Settings\Administrator\My Documents\My Music\Scherzo+No1_+Cho...	2017-07-13 11:06:46 PDT	Virtual Disk.vrm
[tndeck.com]++3on+Sayles++Double+Violin+Concerto+1st+Movement++3.5.+Bach.Ink				C:\Documents and Settings\Administrator\My Documents\My Music[tndeck.com]++3o...	2017-07-13 11:06:05 PDT	Virtual Disk.vrm
ProcessExplorer.Ink				C:\Documents and Settings\Administrator\My Documents\Downloads\ProcessExplorer.zip	2017-07-13 11:42:16 PDT	Virtual Disk.vrm

Hex Text Application File Metadata Context Results Annotations Other Occurrences

I have also found obiwan.Ink and obiwan2.Ink and final-form.Ink files which are python scripts and located in “My Documents” folder of the Administrator which is highly suspicious. These files may be the malwares. I have investigated further to find these files and other important evidence.



In the EXIF Metadata I found this image in document folder which is the Death star plan. So, I can say that the blueprints/plans of the death star may have been compromised.



The death star plans are located in the cache section of Firefox.

Aayushi Dubey ENPM687 - Autopsy 4.16.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img_Virtual Disk.vmdk/vol_02/RECYCLER/S-1-S-21-57989941-1972579041-1801674531-500 6 Results

Table Thumbnail

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash
[current folder]				2017-07-14 16:39:58 PDT	2017-07-14 16:39:58 PDT	2017-07-14 16:39:58 PDT	2017-07-13 12:29:35 PDT	344	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	
[parent folder]				2017-07-13 12:29:35 PDT	2017-07-14 16:39:53 PDT	2017-07-14 16:39:05 PDT	2017-07-13 12:29:35 PDT	320	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	
DC2.exe				2017-07-13 10:43:49 PDT	2017-07-14 16:39:58 PDT	2017-07-14 16:39:55 PDT	2017-07-13 10:43:45 PDT	45319026	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	
DC2.exe:Zone.Identifier				2017-07-13 10:43:49 PDT	2017-07-14 16:39:58 PDT	2017-07-14 16:39:55 PDT	2017-07-13 10:43:45 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	
desktop.ini				2017-07-14 16:39:53 PDT	2017-07-14 16:39:53 PDT	2017-07-14 16:39:53 PDT	2017-07-13 12:29:35 PDT	65	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	
Info2				2017-07-14 16:40:04 PDT	2017-07-14 16:40:04 PDT	2017-07-14 16:40:04 PDT	2017-07-13 12:29:35 PDT	800	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	

Save Table as CSV

Views

- Extracted Content
 - EXIF Metadata (2)
 - Encryption Suspected (2)
 - Extension Mismatch Detected (2)
 - Metadata (3)
 - Operating System User Account (4)
 - Recent Documents (33)
 - Shell Bags (31)
 - User Content Suspected (2)
 - Web Bookmarks (8)
 - Web Cookies (102)
 - Web Downloads (27)
 - Web Form Autofill (3)
 - Web History (221)
 - Web Search (43)
- Keyword Hits
 - Single Literal Keyword Search (0)
 - Single Regular Expression Search (0)
 - Email Addresses (1494)
 - Hashtest Hits
 - E-Mail Messages
 - Interesting Items
 - Encryption Programs (1)
 - Accounts
- Tags
- Reports

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

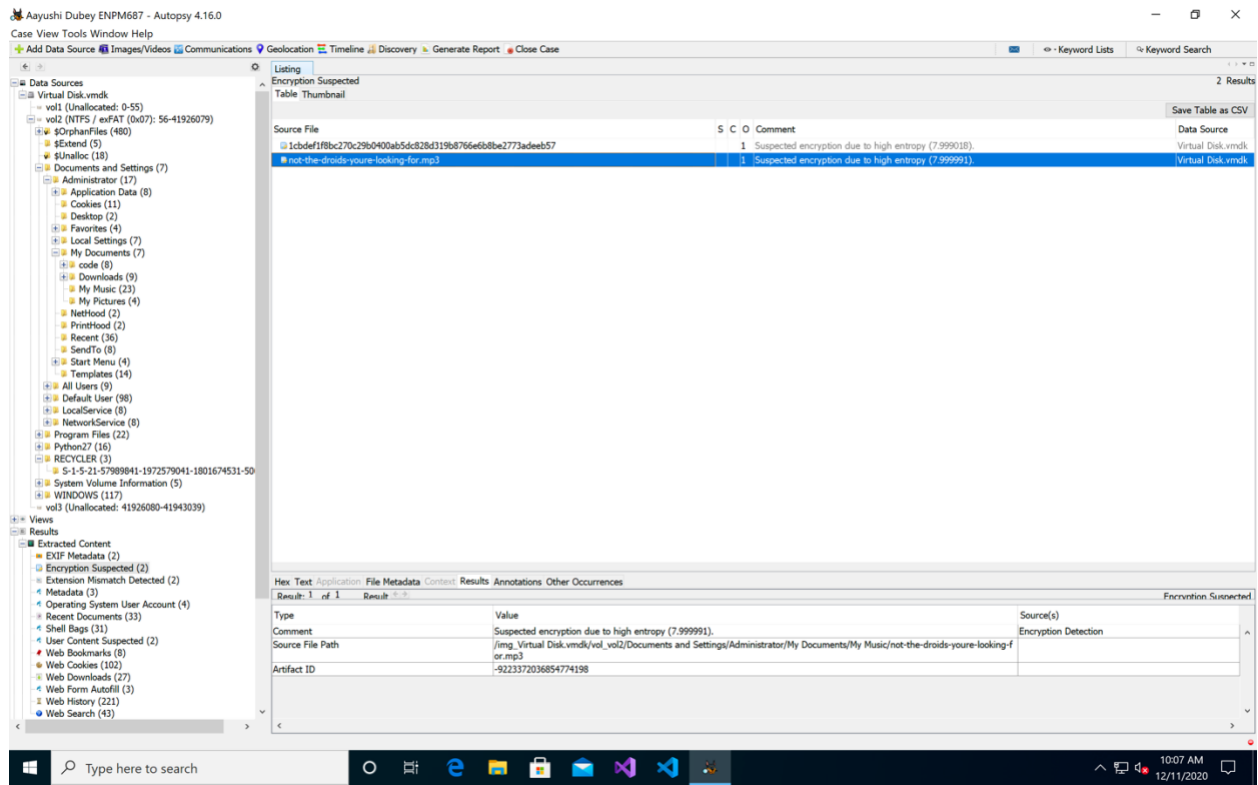
P... 1 ... Go to Page: Script: Latin - Basic

C:\Documents and Settings\Administrator\My Documents\Firefox Setup 52.2.1esr.exe
C:\Documents and Settings\Administrator\My Documents\Firefox Setup 52.2.1esr.exe

Type here to search

10:05 AM 12/11/2020

I have also checked the recycler folder if that can give me some useful evidence but found only a deleted installer executable of Firefox. Which was deleted from “My Documents:” folder of Administrator.



I went through “Encryption suspected” folder which is located under result and found 2 files in which one file named is not-the-droids-you-are-looking-for which is a mp3 file this is encrypted as suspected by autopsy. The other file is system’s file.

Aayushi Dubey ENPM687 - Autopsy 4.16.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing

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

9 Results

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
[current folder]				2017-07-13 12:29:36 PDT	2017-07-13 12:29:36 PDT	2017-07-14 16:39:22 PDT	2017-07-13 10:45:13 PDT	56	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	
[parent folder]				2017-07-14 16:39:58 PDT	2017-07-14 16:39:58 PDT	2017-07-14 16:39:58 PDT	2017-07-12 08:05:39 PDT	56	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	
ProcessExplorer				2017-07-13 12:17:07 PDT	2017-07-13 12:17:07 PDT	2017-07-13 12:17:07 PDT	2017-07-13 11:42:33 PDT	56	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	
ProcessExplorer.zip	1			2017-07-13 11:42:16 PDT	2017-07-13 11:42:16 PDT	2017-07-13 11:42:16 PDT	2017-07-13 11:42:10 PDT	1931969	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	4e084be484f5
ProcessExplorer.zip:Zone.Identifier	2			2017-07-13 11:42:16 PDT	2017-07-13 11:42:16 PDT	2017-07-13 11:42:16 PDT	2017-07-13 11:42:10 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	fbccf14d504b
python-2.7.13.msi	1			2017-07-13 10:46:40 PDT	2017-07-13 10:46:40 PDT	2017-07-13 10:47:11 PDT	2017-07-13 10:46:36 PDT	19161088	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	0f057ab4400e
python-2.7.13.msi:Zone.Identifier	2			2017-07-13 10:46:40 PDT	2017-07-13 10:46:40 PDT	2017-07-13 10:47:11 PDT	2017-07-13 10:46:36 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	fbccf14d504b
VeraCrypt Setup 1.21.exe	1			2017-07-13 10:45:25 PDT	2017-07-13 10:45:50 PDT	2017-07-13 11:56:37 PDT	2017-07-13 10:45:10 PDT	29625696	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	8f601a03f84f5
VeraCrypt Setup 1.21.exe:Zone.I...	2			2017-07-13 10:45:25 PDT	2017-07-13 10:45:50 PDT	2017-07-13 11:56:37 PDT	2017-07-13 10:45:10 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_v...	fbccf14d504b

Hex Text Application File Metadata Context Results Annotations Other Occurrences

When I checked the Downloads item on the disk and found that VeraCrypt was installed in the system so there may be a possibility that the mp3 file that was found above was encrypted by VeraCrypt.



Found VeraCrypt in cookies.

Aayushi Dubey ENPM687 - Autopsy 4.16.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

27 Results

Save Table as CSV

Source File	S	C	O	URL	Path	Date Accessed	Program Name	Domain
places.sqlite	1			https://launchpadlibrarian.net/728012...	C:\Documents and Settings\Administrator\My Documents\Downloads\VeraCrypt ...	2017-07-13 10:45:13 PDT	Firefox	launchpadlibrarian.net
places.sqlite	1			https://www.python.org/ftp/python/2.7...	C:\Documents and Settings\Administrator\My Documents\Downloads\python-2.7...	2017-07-13 10:46:38 PDT	Firefox	www.python.org
places.sqlite	1			https://bootstrap.pypa.io/get-pip.py	C:\Documents and Settings\Administrator\My Documents\Downloads\python-2.7...	2017-07-13 10:56:01 PDT	Firefox	bootstrap.pypa.io
places.sqlite	1			http://a.dlcdn.com/bl/wp-content/upl...	W:\Death Star Plans\DSOTM-308b636-651507587451.jpg	2017-07-13 11:02:25 PDT	Firefox	a.dlcdn.com
places.sqlite	1			http://en.space.mayachts.ru/ships/2/la...	W:\Death Star Plans\layout.jpg	2017-07-13 11:02:29 PDT	Firefox	en.space.mayachts.ru
places.sqlite	1			https://www.wired.com/wp-content/ul...	W:\Death Star Plans\DeathStar1.jpg	2017-07-13 11:02:32 PDT	Firefox	www.wired.com
places.sqlite	1			http://media-cache-ak0.pinimg.com/fo...	W:\Death Star Plans\156a70b41b339278b361b8c923d0327c.jpg.gif	2017-07-13 11:02:38 PDT	Firefox	media-cache-ak0.pinimg.com
places.sqlite	1			http://media.comicbook.com/2015/11/...	W:\Death Star Plans\death-star-plans-157613.jpg	2017-07-13 11:02:40 PDT	Firefox	media.comicbook.com
places.sqlite	1			https://1k953baqia3baqia3baqia3baqia...	W:\Death Star Plans\DeathStar-1.jpg	2017-07-13 11:02:47 PDT	Firefox	1k953baqia3baqia3baqia3baqia-wpe
places.sqlite	1			https://milnersblog.files.wordpress.c...	W:\Death Star Plans\the-official-rogue-one-death-star-plans-are-revealed.jpg	2017-07-13 11:02:50 PDT	Firefox	milnersblog.files.wordpress.com
places.sqlite	1			https://s-media-cache-ak0.pinimg.com/...	W:\Death Star Plans\21c2d524c056625bc58691e3d7a790.jpg	2017-07-13 11:02:54 PDT	Firefox	s-media-cache-ak0.pinimg.com
places.sqlite	1			http://wimages.vr-zone.net/2016/11/D...	W:\Death Star Plans\Death_star_blueprint_sw_card_trader.png.jpeg	2017-07-13 11:02:59 PDT	Firefox	wimages.vr-zone.net
places.sqlite	1			http://vignette2.wikia.nocookie.net/sta...	W:\Death Star Plans\Deathstar_blueprint.jpg	2017-07-13 11:03:03 PDT	Firefox	vignette2.wikia.nocookie.net
places.sqlite	1			https://www.wired.com/wp-content/ul...	W:\Death Star Plans\DeathStar3.jpg	2017-07-13 11:03:09 PDT	Firefox	www.wired.com
places.sqlite	1			https://i.stack.imgur.com/Tr2nF.jpg	W:\Death Star Plans\Tr2nF.jpg	2017-07-13 11:03:19 PDT	Firefox	i.stack.imgur.com
places.sqlite	1			http://tindeck.com/download/projphnt...	C:\Documents and Settings\Administrator\My Documents\My Music\tindeck.com...	2017-07-13 11:06:05 PDT	Firefox	tindeck.com
places.sqlite	1			http://tindeck.com/download/projphnt...	C:\Documents and Settings\Administrator\My Documents\My Music\Scherzo_Rel...	2017-07-13 11:06:45 PDT	Firefox	tindeck.com
places.sqlite	1			http://tindeck.com/download/projshu...	C:\Documents and Settings\Administrator\My Documents\My Music\Concerto-4...	2017-07-13 11:06:51 PDT	Firefox	tindeck.com
places.sqlite	1			http://tindeck.com/download/projshu...	C:\Documents and Settings\Administrator\My Documents\My Music\Rhapsody_R...	2017-07-13 11:06:58 PDT	Firefox	tindeck.com
places.sqlite	1			http://tindeck.com/download/projshu...	C:\Documents and Settings\Administrator\My Documents\My Music\Large from ...	2017-07-13 11:07:06 PDT	Firefox	tindeck.com
places.sqlite	1			http://tindeck.com/download/projshu...	C:\Documents and Settings\Administrator\My Documents\My Music\Bournee_4th...	2017-07-13 11:07:12 PDT	Firefox	tindeck.com
places.sqlite	1			http://tindeck.com/download/projshu...	C:\Documents and Settings\Administrator\My Documents\My Music\Gigue_3rd_C...	2017-07-13 11:07:25 PDT	Firefox	tindeck.com
places.sqlite	1			http://tindeck.com/download/projshu...	C:\Documents and Settings\Administrator\My Documents\My Music\Menuetto_1...	2017-07-13 11:07:31 PDT	Firefox	tindeck.com
places.sqlite	1			http://tindeck.com/download/projshu...	C:\Documents and Settings\Administrator\My Documents\My Music\Courante_1a...	2017-07-13 11:07:48 PDT	Firefox	tindeck.com
places.sqlite	1			https://download.sysinternals.com/file...	C:\Documents and Settings\Administrator\My Documents\Downloads\ProcessExp...	2017-07-13 11:42:16 PDT	Firefox	download.sysinternals.com

How Text Application File Metadata Context Results Annotations Other Occurrences

10:20 AM 12/11/2020

I found some suspicious things under web downloads like the death star plans are located in some M drive.

Autopsy 4.16.0 - Case View Tools Window Help

Web History

Source File	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name
index.dat				file:///Read-This.txt	2017-07-13 18:03:48 PDT			Internet Explorer
index.dat				file:///Documents%20and%20Settings/Administrator/My%20Documents/My%20Music/Scheroz+No1_+Chopin.mp3	2017-07-13 18:07:25 PDT			Internet Explorer
index.dat	2			https://www.mozilla.org/en-US/firefox/new/?con=tabs	2017-07-13 17:43:34 PDT			Internet Explorer
index.dat				file:///Death%20Star%20Plans/Death-star-1.jpg	2017-07-13 18:02:47 PDT			Internet Explorer
index.dat				file:///Death%20Star%20Plans/the-official-rogue-one-death-star-plans-are-revealed.jpg	2017-07-13 18:02:50 PDT			Internet Explorer
index.dat				file:///Death%20Star%20Plans/Deathstar_blueprint.jpg	2017-07-13 18:03:03 PDT			Internet Explorer
index.dat				about:Home	2017-07-12 15:05:47 PDT			Internet Explorer
index.dat				file:///Documents%20and%20Settings/Administrator/My%20Documents/My%20Music/Scheroz+No1_+Chopin.mp3	2017-07-13 18:06:54 PDT			Internet Explorer
index.dat				file:///Documents%20and%20Settings/Administrator/My%20Documents/My%20Music/Remuettos_1.2_from_Alist_5...	2017-07-13 18:07:31 PDT			Internet Explorer
index.dat	1			http://www.msn.com/en-us/news/india/india-nagpur-bomb-attack-timeline	2017-07-13 17:42:48 PDT			Internet Explorer
index.dat	2			http://www.bing.com/search?q=mozilla+firefox&ag=5C&ag=mozilla+firefox+8&cid=9CA4933887A543CA14608...	2017-07-13 17:43:21 PDT			Internet Explorer
index.dat	1			https://www.bing.com/search?q=mozilla+firefox&ag=5C&ag=mozilla+firefox+8&cid=9CA4933887A543CA14608...	2017-07-13 17:43:24 PDT			Internet Explorer
index.dat				file:///Documents%20and%20Settings/Administrator/My%20Documents/Downloads/ProcessExplorer.zip	2017-07-13 18:42:18 PDT			Internet Explorer
index.dat				file:///Documents%20and%20Settings/Administrator/My%20Documents/Downloads/ProcessExplorer.zip	2017-07-13 18:03:19 PDT			Internet Explorer
index.dat				file:///Documents%20and%20Settings/Administrator/My%20Documents/code/final-form.py	2017-07-13 19:32:18 PDT			Internet Explorer
index.dat				file:///Documents%20and%20Settings/Administrator/My%20Documents/code/final-form.py	2017-07-14 23:39:27 PDT			Internet Explorer
index.dat				file:///Death%20Star%20Plans/21c2d524c056625bc5d8f91a3d2a790.jpg	2017-07-13 18:02:25 PDT			Internet Explorer
index.dat				file:///Death%20Star%20Plans/21c2d524c056625bc5d8f91a3d2a790.jpg	2017-07-13 18:02:38 PDT			Internet Explorer
index.dat				file:///Documents%20and%20Settings/Administrator/My%20Documents/code/ibwand.py	2017-07-13 18:38:52 PDT			Internet Explorer
index.dat				file:///Documents%20and%20Settings/Administrator/My%20Documents/code/ibwand.py	2017-07-13 17:56:03 PDT			Internet Explorer

Web History

Type	Value	Source(s)
URL	file:///Death%20Star%20Plans/DeathStar3.jpg	Recent Activity
Date Accessed	2017-07-13 18:03:09	Recent Activity
Referrer URL		Recent Activity
Program Name	Internet Explorer	Recent Activity
Username	Administrator	Recent Activity
Source File Path	\\jing_virtual_disk_vmdk\\vol_vo2\\Documents and Settings\\Administrator\\Local Settings\\History\\History.IES5\\index.dat	Recent Activity
Artifact ID	-9223720385477952	

Found some useful files related to the plans of Death Star in the history section of internet explorer.

Aayushi Dubey ENPM687 - Autopsy 4.16.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing

/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/code/dist

Table Thumbnail

4 Results

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash
[current folder]				2017-07-13 12:35:06 PDT	2017-07-13 12:35:06 PDT	2017-07-13 12:35:06 PDT	2017-07-13 11:44:15 PDT	236	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_x...	
[recent folder]				2017-07-14 16:39:42 PDT	2017-07-14 16:39:42 PDT	2017-07-14 16:39:42 PDT	2017-07-13 11:40:02 PDT	56	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_x...	
obiwan.exe	1			2017-07-13 11:44:27 PDT	2017-07-13 12:31:21 PDT	2017-07-13 11:44:27 PDT	2017-07-13 11:44:27 PDT	4206347	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_x... 97c90c038e2b060ac	
obiwan2.exe	1			2017-07-13 12:30:44 PDT	2017-07-13 12:31:21 PDT	2017-07-13 12:30:44 PDT	2017-07-13 12:10:58 PDT	4491789	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_x... cb183dc18d180e6dc	

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Views

- File Types
- Deleted Files
- File Size

Results

- Extracted Content
 - EXIF Metadata (2)
 - Encryption Suspected (2)
 - Extension Mismatch Detected (2)

I found some interesting things in Administrator's "My Documents" folder which was obiwan.exe and obiwan2.exe under dist. folder.

Aayushi Dubey ENPM687 - Autopsy 4.16.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing

/img_Virtual Disk.vmdk/vol_02/Documents and Settings/Administrator/My Documents/code/build/final-form

Table Thumbnail

10 Results

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
[current folder]				2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	2017-07-13 12:30:49 PDT	56	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	
[parent folder]				2017-07-13 12:10:53 PDT	2017-07-13 12:10:53 PDT	2017-07-13 12:11:02 PDT	2017-07-13 11:44:15 PDT	448	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	
final-form.exe.manifest	1			2017-07-13 12:30:49 PDT	2017-07-13 12:30:49 PDT	2017-07-13 12:30:49 PDT	2017-07-13 12:30:49 PDT	1011	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	51fa0e1b22a
out00-Analysis.toc	1			2017-07-13 12:30:51 PDT	2017-07-13 12:30:51 PDT	2017-07-13 12:30:51 PDT	2017-07-13 12:30:51 PDT	21965	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	037ccf9a2d0
out00-EXE.toc	1			2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	3554	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	a131340cd89
out00-PKG.pkg	1			2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	2017-07-13 12:30:52 PDT	4364786	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	f496c636bcff
out00-PKG.toc	1			2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	2017-07-13 12:30:53 PDT	2594	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	2f2fb79a93e
out00-PYZ.pyz	1			2017-07-13 12:30:52 PDT	2017-07-13 12:30:52 PDT	2017-07-13 12:30:52 PDT	2017-07-13 12:30:52 PDT	1039720	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	9a7eb65994f
out00-PYZ.toc	1			2017-07-13 12:30:52 PDT	2017-07-13 12:30:52 PDT	2017-07-13 12:30:52 PDT	2017-07-13 12:30:52 PDT	20216	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	e4755dc262d
warnfinal-form.txt	1			2017-07-13 12:30:51 PDT	2017-07-13 12:30:51 PDT	2017-07-13 12:30:51 PDT	2017-07-13 12:30:51 PDT	1841	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol_...	80b162c8b51

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Views

- File Types
- Deleted Files
- File Size
- Results
- Extracted Content

Type here to search

11:19 AM 12/11/2020

In the same location I have also found 3 folders under the folder named “build” and those 3 folder names are final form, obiwan and obiwan2. They were only the part of code. This is highly likely that obiwan.exe, obiwan2.exe files are malwares also I was only able to find the package of the application named final form which may have used to build the malware.

Aayushi Dubey ENPM687 - Autopsy 4.16.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Data Sources

- Virtual Disk.vmdk
 - vol1 (Unallocated: 0-55)
 - vol2 (NTFS / exFAT (0x07): 56-41926079)
 - orphansFiles (460)
 - 1 (2)
 - pywin32-219.dif-info (8)
 - pywin32_system32 (5)
 - tools (14)
 - win32 (46)
 - win32com (23)
 - win32comet (15)
 - xlntend (5)
 - xlntallic (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)
 - obivian (10)
 - obivian2 (10)
 - dist (4)
 - Downloads (9)
 - My Music (23)
 - My Pictures (4)
 - NetHood (2)
 - PrintHood (2)
 - Recent (36)
 - SendTo (8)
 - Start Menu (4)
 - Programs (9)
 - Templates (14)
 - All Users (9)
 - Default User (98)
 - LocalService (8)
 - NetworkService (8)
 - Program Files (22)
 - Python27 (16)
 - RECYCLER (3)
 - System Volume Information (5)
 - WINDOWS (117)
 - vol3 (Unallocated: 41926080-41943039)

Listing

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

Table Thumbnail

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2017-07-13 12:34:01 PDT	2017-07-13 12:34:01 PDT	2017-07-14 16:38:51 PDT	2017-07-12 08:05:44 PDT	56	Allocated	Allocated	unknown	/img_Virtual Disk
[parent folder]				2017-07-14 16:39:58 PDT	2017-07-14 16:39:58 PDT	2017-07-14 16:39:58 PDT	2017-07-12 08:05:39 PDT	56	Allocated	Allocated	unknown	/img_Virtual Disk
[index.com]++Jon+Sayles++Double+Violin+Concert	1			2017-07-13 11:06:05 PDT	2017-07-13 11:06:05 PDT	2017-07-13 11:06:10 PDT	2017-07-13 11:06:05 PDT	6158525	Allocated	Allocated	unknown	/img_Virtual Disk
[index.com]++Jon+Sayles++Double+Violin+Concert	2			2017-07-13 11:06:05 PDT	2017-07-13 11:06:05 PDT	2017-07-13 11:06:10 PDT	2017-07-13 11:06:05 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk
Bourree_4th_Lute_Suite-Bach.mp3	1			2017-07-13 11:07:13 PDT	2017-07-13 11:07:13 PDT	2017-07-13 11:07:13 PDT	2017-07-13 11:07:12 PDT	3003101	Allocated	Allocated	unknown	/img_Virtual Disk
Bourree_4th_Lute_Suite-Bach.mp3.Zone.Identifier	2			2017-07-13 11:07:13 PDT	2017-07-13 11:07:13 PDT	2017-07-13 11:07:13 PDT	2017-07-13 11:07:12 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk
Concerto-4-Violini-2_Telemann.mp3	1			2017-07-13 11:06:54 PDT	2017-07-13 11:06:54 PDT	2017-07-13 11:06:54 PDT	2017-07-13 11:06:53 PDT	5072418	Allocated	Allocated	unknown	/img_Virtual Disk
Concerto-4-Violini-2_Telemann.mp3.Zone.Identifier	2			2017-07-13 11:06:54 PDT	2017-07-13 11:06:54 PDT	2017-07-13 11:06:54 PDT	2017-07-13 11:06:53 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk
Courante_1st_Cello_Suite.mp3	1			2017-07-13 11:07:50 PDT	2017-07-13 11:07:50 PDT	2017-07-13 11:07:50 PDT	2017-07-13 11:07:48 PDT	3631311	Allocated	Allocated	unknown	/img_Virtual Disk
Courante_1st_Cello_Suite.mp3.Zone.Identifier	2			2017-07-13 11:07:50 PDT	2017-07-13 11:07:50 PDT	2017-07-13 11:07:50 PDT	2017-07-13 11:07:48 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk
Gigue_3rd_Cello_Suite-Bach.mp3	1			2017-07-12 08:05:54 PDT	2017-07-12 08:05:54 PDT	2017-07-14 16:39:01 PDT	2017-07-12 08:05:44 PDT	189	Allocated	Allocated	unknown	/img_Virtual Disk
Gigue_3rd_Cello_Suite-Bach.mp3.Zone.Identifier	2			2017-07-13 11:07:26 PDT	2017-07-13 11:07:26 PDT	2017-07-13 11:07:26 PDT	2017-07-13 11:07:25 PDT	4028773	Allocated	Allocated	unknown	/img_Virtual Disk
Largo+from+Concerto-No5_JS_Bach.mp3	1			2017-07-13 11:07:26 PDT	2017-07-13 11:07:26 PDT	2017-07-13 11:07:26 PDT	2017-07-13 11:07:25 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk
Largo+from+Concerto-No5_JS_Bach.mp3.Zone.Identifier	2			2017-07-13 11:07:07 PDT	2017-07-13 11:07:07 PDT	2017-07-13 11:07:07 PDT	2017-07-13 11:07:06 PDT	3914670	Allocated	Allocated	unknown	/img_Virtual Disk
Menuettos_1_2_from_41st_Symphony.mp3	1			2017-07-13 11:07:07 PDT	2017-07-13 11:07:07 PDT	2017-07-13 11:07:07 PDT	2017-07-13 11:07:06 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk
Menuettos_1_2_from_41st_Symphony.mp3.Zone.Identifier	2			2017-07-13 11:07:34 PDT	2017-07-13 11:07:34 PDT	2017-07-13 11:07:34 PDT	2017-07-13 11:07:31 PDT	5903930	Allocated	Allocated	unknown	/img_Virtual Disk
not-the-droids-you-are-looking-for.mp3	1			2017-07-13 10:59:36 PDT	2017-07-13 12:34:01 PDT	2017-07-13 12:34:07 PDT	2017-07-13 10:59:33 PDT	20971520	Allocated	Allocated	unknown	/img_Virtual Disk
Rhapsody_No2_G-Minor_Brahms.mp3	1			2017-07-13 11:07:06 PDT	2017-07-13 11:07:06 PDT	2017-07-13 11:07:06 PDT	2017-07-13 11:06:58 PDT	12124200	Allocated	Allocated	unknown	/img_Virtual Disk
Rhapsody_No2_G-Minor_Brahms.mp3.Zone.Identifier	2			2017-07-13 11:07:06 PDT	2017-07-13 11:07:06 PDT	2017-07-13 11:07:06 PDT	2017-07-13 11:06:58 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk
Sample Music Link	1			2017-07-12 08:05:44 PDT	2017-07-12 08:05:44 PDT	2017-07-13 12:34:06 PDT	2017-07-12 08:05:44 PDT	638	Allocated	Allocated	unknown	/img_Virtual Disk
Scherzo+No1_+Chopin.mp3	1			2017-07-13 11:06:54 PDT	2017-07-13 11:06:54 PDT	2017-07-13 11:06:54 PDT	2017-07-13 11:06:45 PDT	16756780	Allocated	Allocated	unknown	/img_Virtual Disk
Scherzo+No1_+Chopin.mp3.Zone.Identifier	2			2017-07-13 11:06:54 PDT	2017-07-13 11:06:54 PDT	2017-07-13 11:06:54 PDT	2017-07-13 11:06:45 PDT	26	Allocated	Allocated	unknown	/img_Virtual Disk

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 48 Page Matches on page: of - Match 100% Reset

Text Source: File Text

8q9+

-t\k

0iwc3

8KIQ

w122

a0q5

lwaq

x_94

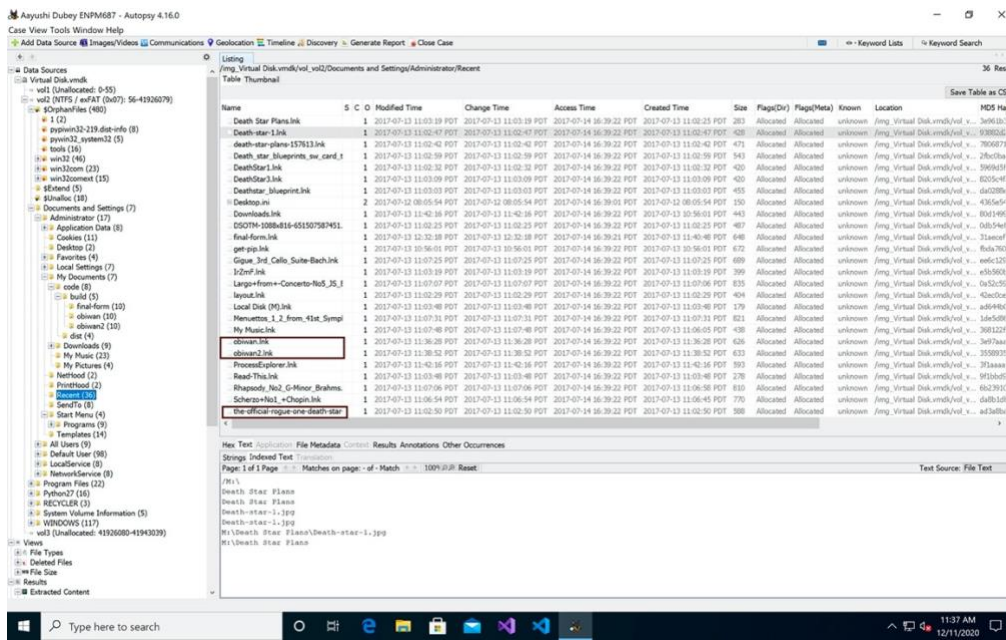
7:vy

Ck1j*

8b+e

1.2c

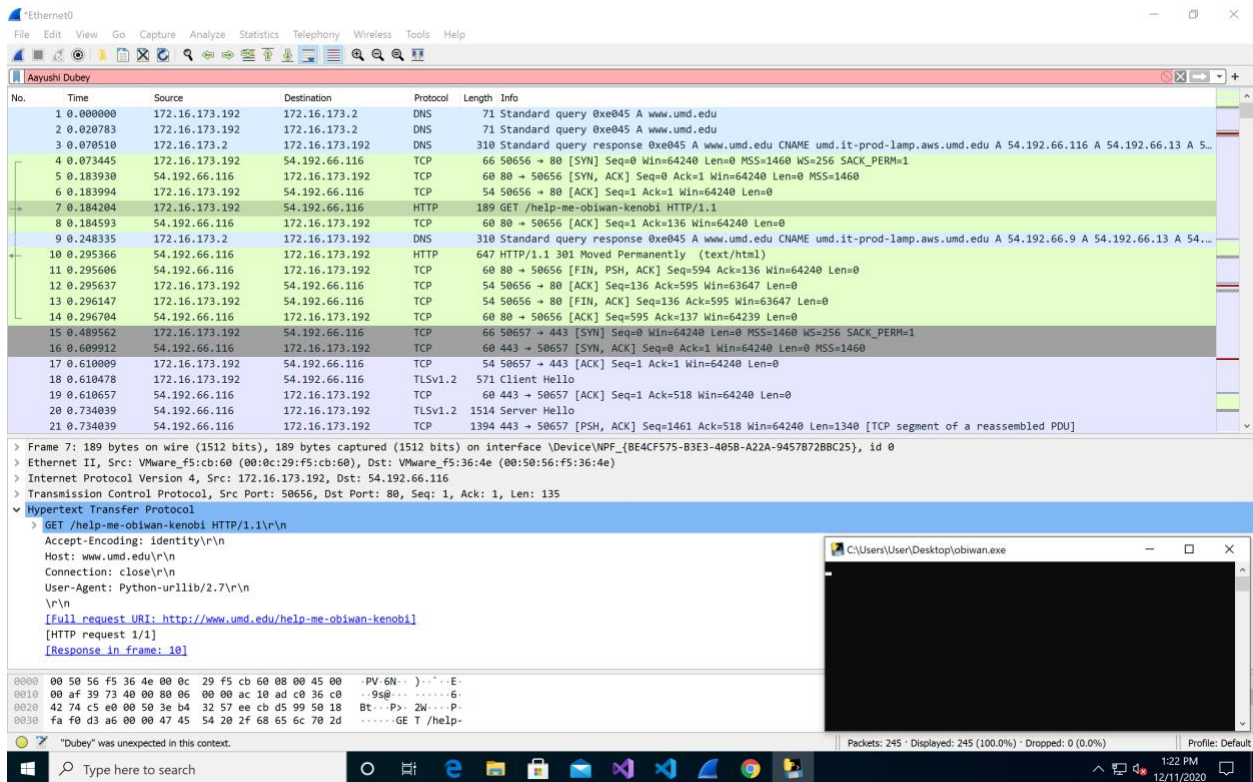
After analyzing “My Music” folder and extract the mp3 file named not-the-droids-you-are-looking-for. Which was suspected an encrypted file by autopsy. This can be a helpful evidence in future.

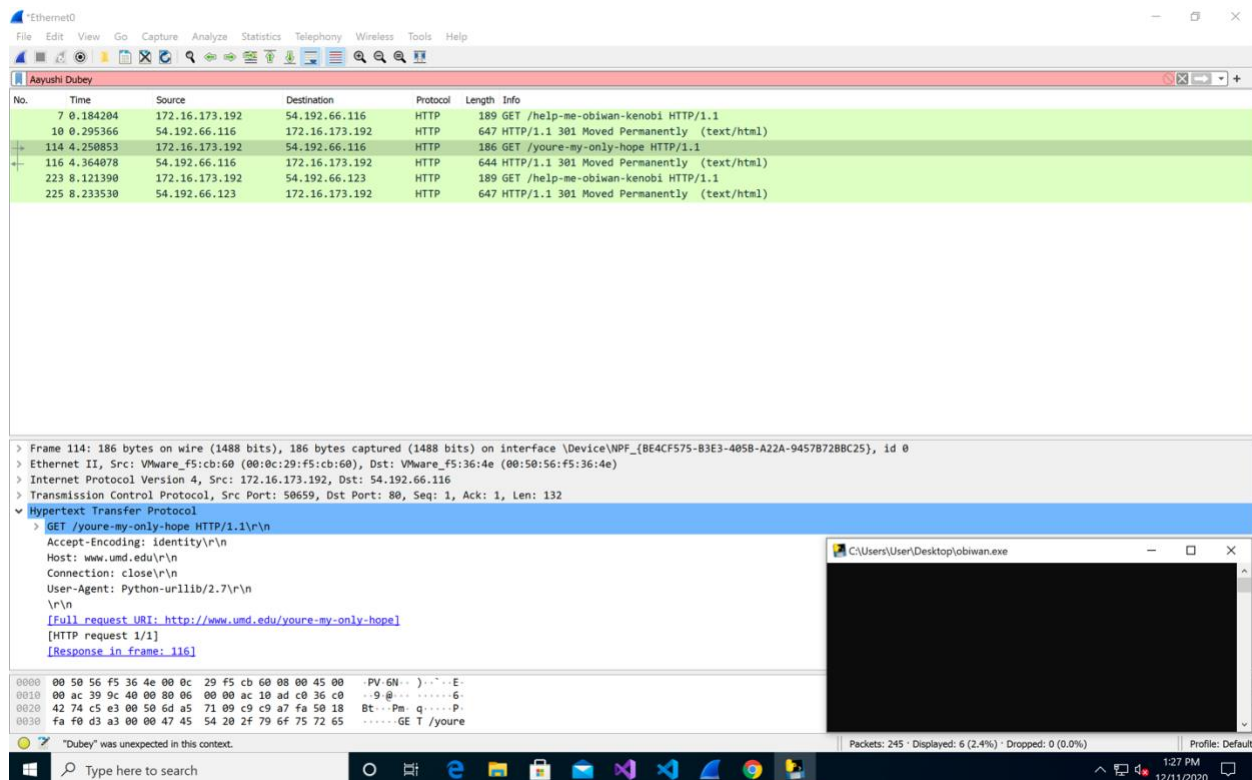


Analysis of Evidence found: - Three important files which I have extracted from the rebel's malware writer's disk.

1. Obiwan.exe
2. Obiwan2.exe
3. Not-the-droids-you-are-looking-for.mp3

The first 2 files are executable files which have higher chances that these are the malwares. I analyzed obiwan.exe file and checked the behavior of this file to check if it was sending any messages across the galaxy. I used Wireshark for this analysis.





I have found that when this exe file running it is trying to connect to two URL's:

<http://www.umd.edu/youre-my-only-hope>
<http://www.umd.edu/help-me-obiwan-kenobi>

These websites are giving http code 301 moved permanently means these websites doesn't host on www.umd.edu server anymore. This message must have sent by Rebels to the Jedi obiwan asking for help.

Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Aayushi Dubey

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000282	172.16.173.192	54.192.66.9	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
5	0.111071	54.192.66.9	172.16.173.192	HTTP	657	HTTP/1.1 301 Moved Permanently (text/html)
110	3.826912	172.16.173.192	54.192.66.9	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
112	3.938418	54.192.66.9	172.16.173.192	HTTP	658	HTTP/1.1 301 Moved Permanently (text/html)
217	8.000944	172.16.173.192	54.192.66.13	HTTP	188	GET /cjkMi8pcyB0aGuga2V5 HTTP/1.1
219	8.113059	54.192.66.13	172.16.173.192	HTTP	646	HTTP/1.1 301 Moved Permanently (text/html)

> Frame 3: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface \Device\NPF_{BE4CF575-B3E3-405B-A22A-9457B72BBC25}, id 0

> Ethernet II, Src: VMware_f5:cb:60 (00:0c:29:f5:cb:60), Dst: VMware_f5:36:4e (00:50:56:f5:36:4e)

> Internet Protocol Version 4, Src: 172.16.173.192, Dst: 54.192.66.9

> Transmission Control Protocol, Src Port: 49949, Dst Port: 80, Seq: 1, Ack: 1, Len: 145

> Hypertext Transfer Protocol

> GET /this-is-not-even-my-final-form. HTTP/1.1\r\n

Accept-Encoding: identity\r\n

Host: www.umd.edu\r\n

Connection: close\r\n

User-Agent: Python-urllib/2.7\r\n

\r\n

[Full request URI: http://www.umd.edu/this-is-not-even-my-final-form.]

[HTTP request 1/1]

[Response in frame: 5]

0030 fa f0 d3 45 00 00 47 45 54 20 2f 74 68 69 73 2d ...E-GE T /this-

0040 69 73 2d 6e 6f 74 2d 65 76 65 6e 2d 6d 79 2d 66 is-not-e ven-my-f

0050 69 6e 61 6c 2d 66 6f 72 6d 2e 20 48 54 50 2f inal-for m. HTTP/

0060 31 2e 31 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 1.1--Acc ept-Enco

0070 64 69 6e 67 3a 20 69 64 65 6e 74 69 74 79 0d 0a ding: id entity--

"Dubey" was unexpected in this context.

Type here to search

1:55 PM 12/11/2020

Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Aayushi Dubey

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000282	172.16.173.192	54.192.66.9	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
5	0.111071	54.192.66.9	172.16.173.192	HTTP	657	HTTP/1.1 301 Moved Permanently (text/html)
110	3.826912	172.16.173.192	54.192.66.9	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
112	3.938418	54.192.66.9	172.16.173.192	HTTP	658	HTTP/1.1 301 Moved Permanently (text/html)
217	8.000944	172.16.173.192	54.192.66.13	HTTP	188	GET /cjkMi8pcyB0aGuga2V5 HTTP/1.1
219	8.113059	54.192.66.13	172.16.173.192	HTTP	646	HTTP/1.1 301 Moved Permanently (text/html)

> Frame 217: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits) on interface \Device\NPF_{BE4CF575-B3E3-405B-A22A-9457B72BBC25}, id 0

> Ethernet II, Src: VMware_f5:cb:60 (00:0c:29:f5:cb:60), Dst: VMware_f5:36:4e (00:50:56:f5:36:4e)

> Internet Protocol Version 4, Src: 172.16.173.192, Dst: 54.192.66.13

> Transmission Control Protocol, Src Port: 49955, Dst Port: 80, Seq: 1, Ack: 1, Len: 134

> Hypertext Transfer Protocol

> GET /cjkMi8pcyB0aGuga2V5 HTTP/1.1\r\n

Accept-Encoding: identity\r\n

Host: www.umd.edu\r\n

Connection: close\r\n

User-Agent: Python-urllib/2.7\r\n

\r\n

[Full request URI: http://www.umd.edu/cjkMi8pcyB0aGuga2V5]

[HTTP request 1/1]

[Response in frame: 219]

0030 fa f0 d3 3e 00 00 47 45 54 20 2f 63 6a 4a 6b 4d ...-GE T /cjkM

0040 69 42 70 63 79 42 30 61 47 55 67 61 32 56 35 20 i8pcyB0a Uga2V5

0050 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 HTTP/1.1 --Accept

0060 2d 45 6e 63 6f 64 69 6e 67 3a 20 69 64 65 6e 74 -Encodin g: ident

0070 69 74 79 0d 0a 48 6f 73 74 3a 20 77 77 2e 75 Ity--Mos t: www.u

The full requested URI (including host name) (http.request.full_uri)

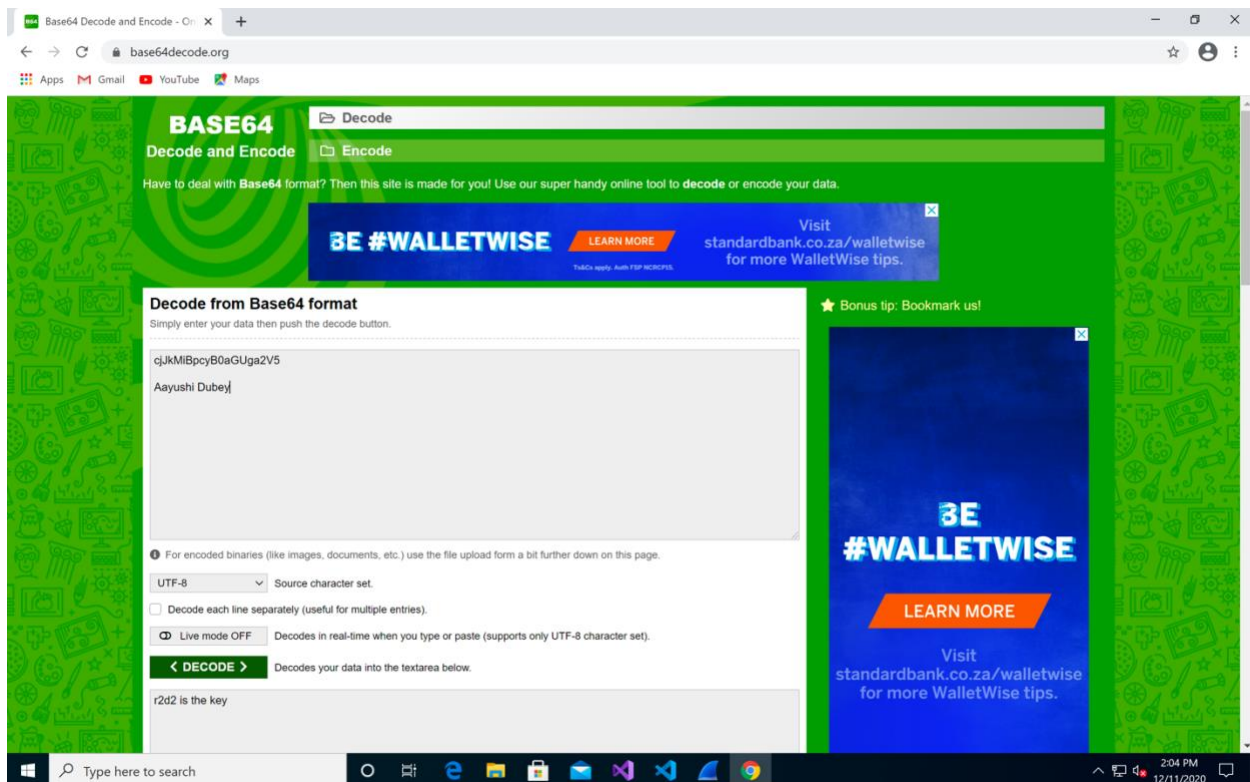
Type here to search

1:55 PM 12/11/2020

From the captured network data analysis sent by obiwan2.exe I have found that this file is trying to connect to 3 websites.

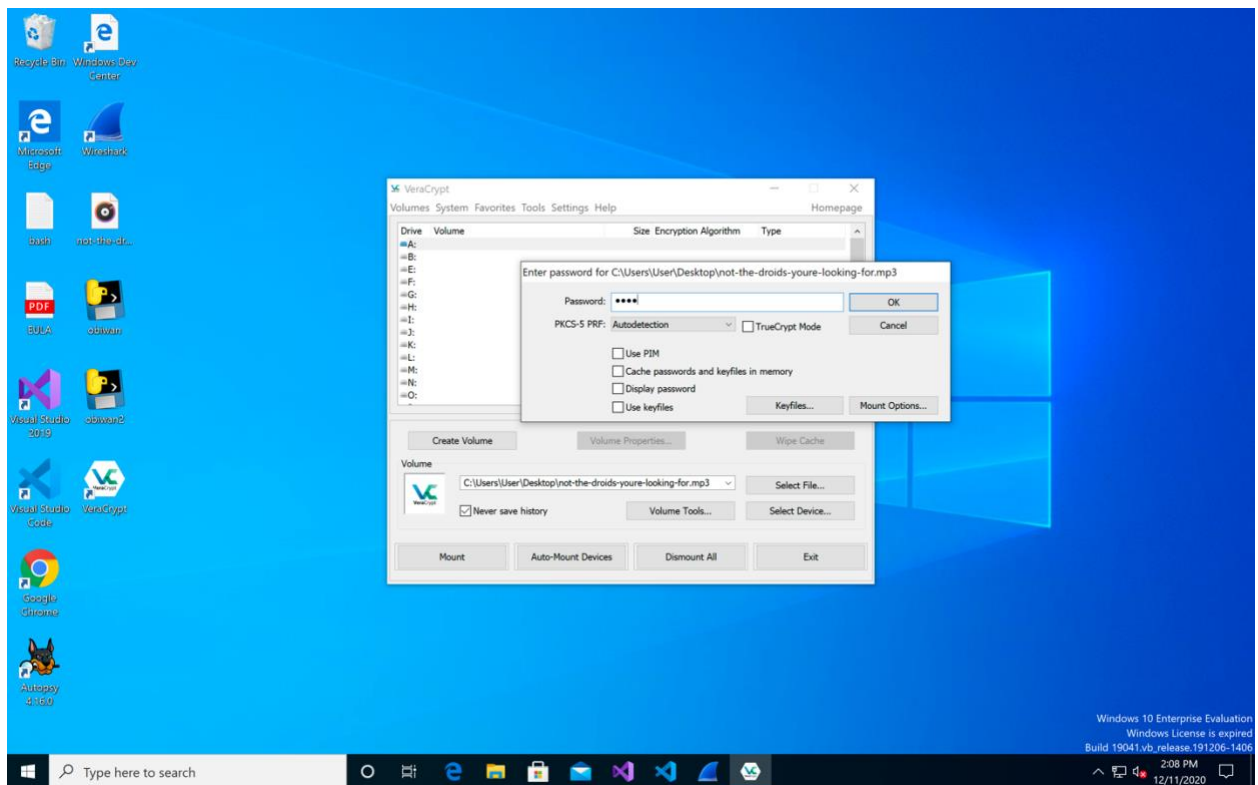
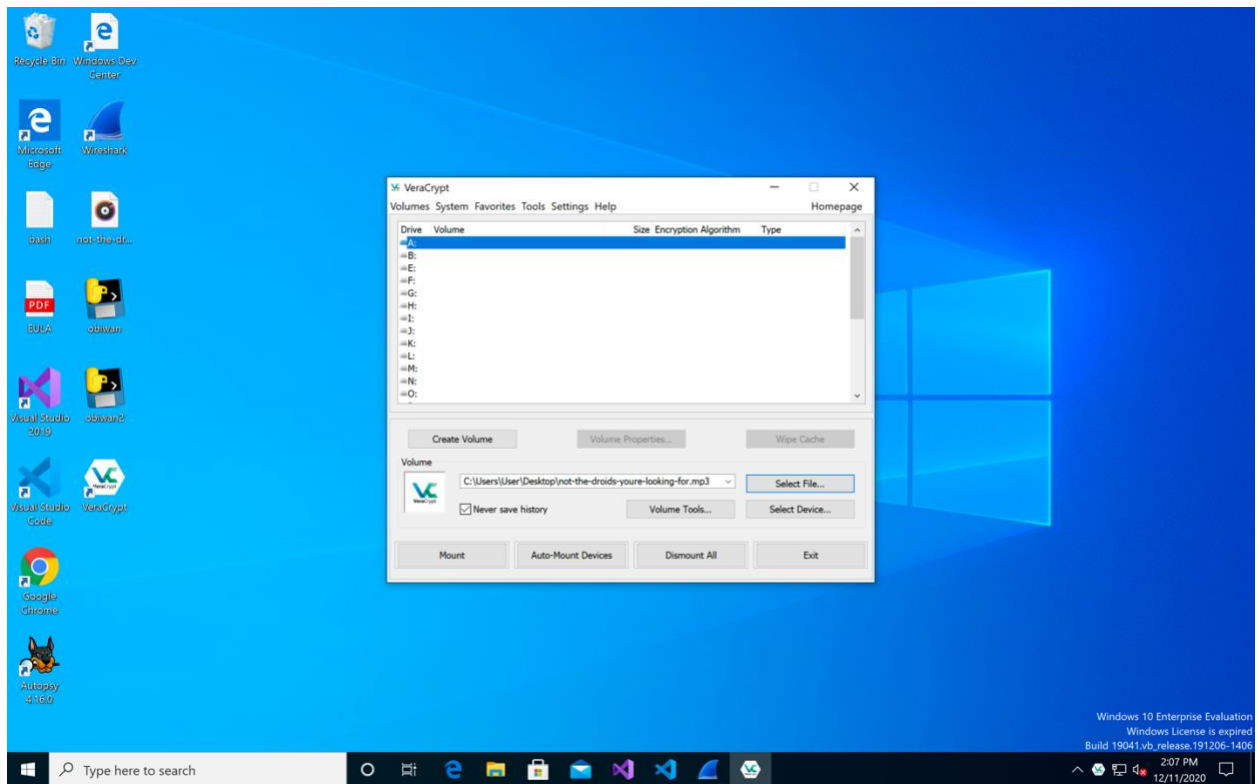
[http://www.umd.edu/this-is-not-even-my-final-form.](http://www.umd.edu/this-is-not-even-my-final-form)
<http://www.umd.edu/All-your-base64-are-belong-to-us>
<http://www.umd.edu/cjJkMiBpcyB0aGUga2V5>

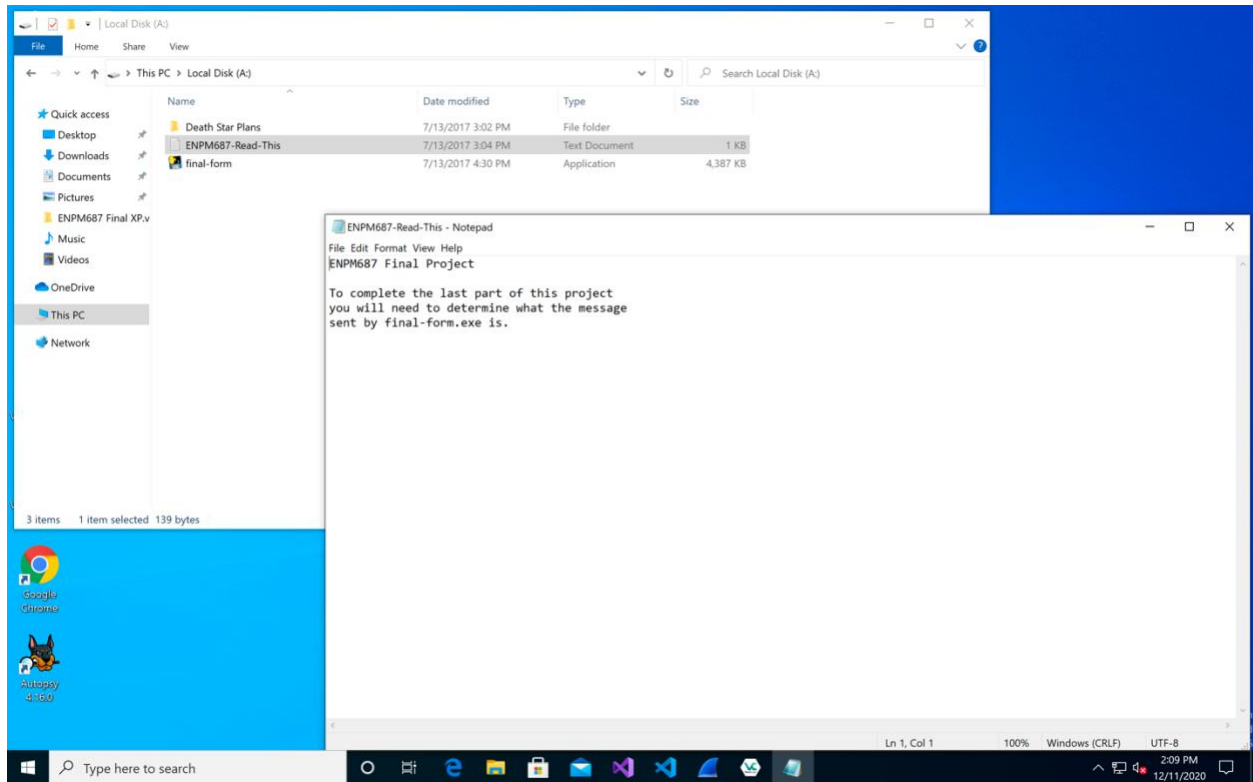
All the 3 websites which are trying to connect are showing http 301 moved permanently message. So, these sites are no longer hosted on umd.edu domain anymore. Also, these can be interpreted as the messages to the imperial army. From these URL's I have concluded that this is not the final form of the virus there may be a malware exist somewhere which is the final form of the malware written by the rebel's malware writer. Also, I have also interpreted as the 3rd no. URL we found is kind of hidden message and may be encoded in base64 as interpreted from the 2nd URL's message above.



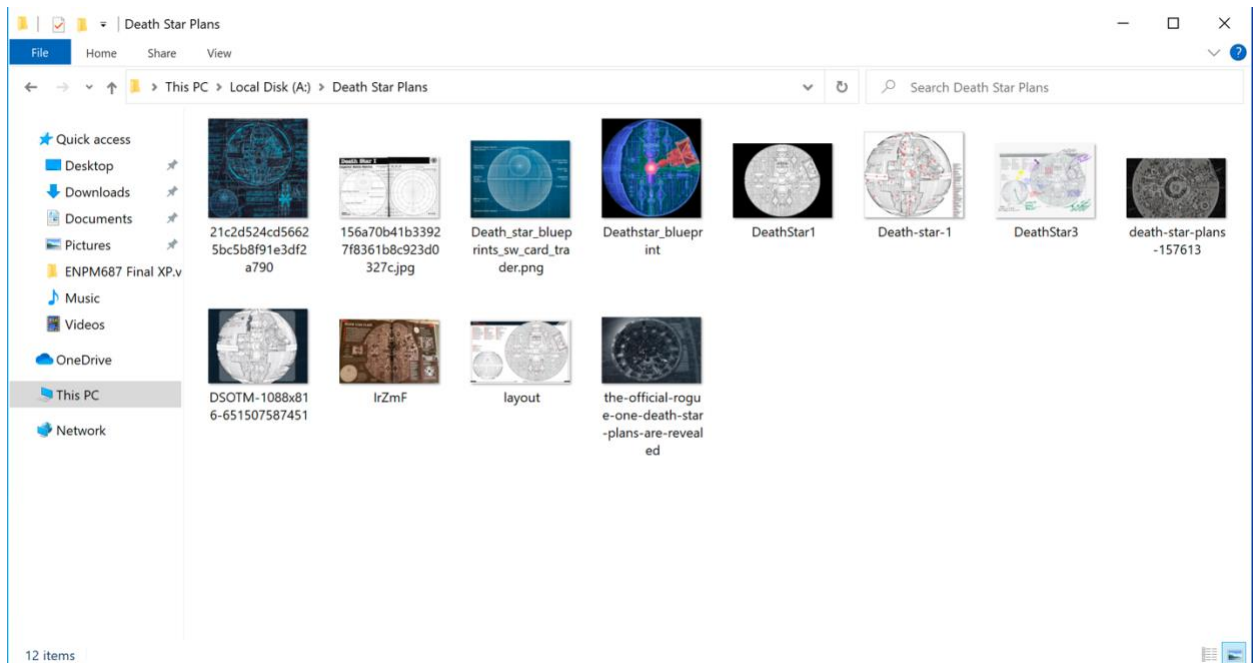
After decoding the hidden message online, the message was r2d2 is the key.

VeraCrypt was installed in the rebel's malware writer's computer also I have found one mp3 file which was suspected by an encrypted file. To unencrypt this mp3 file I need a key and I already got the key. Maybe this mp3 file contains all the secrets and final form of the malware. For that I have analyzed further and used VeraCrypt to mount my mp3 file to my computer's new drive.





The original content of the mp3 file.



It has the blueprints/design of Death star, a text file and the malware named final-form.exe
This is the final form of the malware written by rebel's malware writer.

Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Ayushi Dubey

No.	Time	Source	Destination	Protocol	Length	Info
65	2.065937	172.16.173.192	54.192.66.123	HTTP	209	GET /we-have-the-blue-prints-to-the-Death-Star HTTP/1.1
67	2.208350	54.192.66.123	172.16.173.192	HTTP	667	HTTP/1.1 301 Moved Permanently (text/html)
170	6.442822	172.16.173.192	54.192.66.123	HTTP	195	GET /we-will-defeat-Darth-Vader. HTTP/1.1
172	6.576332	54.192.66.123	172.16.173.192	HTTP	653	HTTP/1.1 301 Moved Permanently (text/html)
281	10.232167	172.16.173.192	54.192.66.13	HTTP	209	GET /we-have-the-blue-prints-to-the-Death-Star HTTP/1.1
283	10.344433	54.192.66.13	172.16.173.192	HTTP	667	HTTP/1.1 301 Moved Permanently (text/html)
388	14.191831	172.16.173.192	54.192.66.116	HTTP	195	GET /we-will-defeat-Darth-Vader. HTTP/1.1
390	14.302361	54.192.66.116	172.16.173.192	HTTP	653	HTTP/1.1 301 Moved Permanently (text/html)

> Frame 65: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF_{BE4CF575-B3E3-405B-A22A-9457B72B8C25}, id 0
> Ethernet II, Src: VMware_f5:cb:60 (00:0c:29:f5:cb:60), Dst: VMware_f5:36:4e (00:50:56:f5:36:4e)
> Internet Protocol Version 4, Src: 172.16.173.192, Dst: 54.192.66.123
> Transmission Control Protocol, Src Port: 50446, Dst Port: 80, Seq: 1, Ack: 1, Len: 155
▼ Hypertext Transfer Protocol
 > GET /we-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n
 Accept-Encoding: identity\r\n
 Host: www.umd.edu\r\n
 Connection: close\r\n
 User-Agent: Python-urllib/2.7\r\n
 \r\n
 [Full request URI: http://www.umd.edu/we-have-the-blue-prints-to-the-Death-Star]
 [HTTP request 1/1]
 [Response in frame: 67]

0030 fa f0 d3 c1 00 00 47 45 54 20 2f 57 65 2d 68 61GE 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
0050 74 73 2d 74 6f 2d 74 68 65 2d 44 65 61 74 68 2d ts-to-th e-Death-
0060 53 74 61 72 20 48 54 54 50 2f 31 2e 31 0d 0a 41 Star HT P/1.1-A
0070 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 ccept-En coding:

"Dubey" was unexpected in this context.

A:\final-form.exe

Type here to search

2:14 PM 12/11/2020

Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Ayushi Dubey

No.	Time	Source	Destination	Protocol	Length	Info
65	2.065937	172.16.173.192	54.192.66.123	HTTP	209	GET /we-have-the-blue-prints-to-the-Death-Star HTTP/1.1
67	2.208350	54.192.66.123	172.16.173.192	HTTP	667	HTTP/1.1 301 Moved Permanently (text/html)
170	6.442822	172.16.173.192	54.192.66.123	HTTP	195	GET /we-will-defeat-Darth-Vader. HTTP/1.1
172	6.576332	54.192.66.123	172.16.173.192	HTTP	653	HTTP/1.1 301 Moved Permanently (text/html)
281	10.232167	172.16.173.192	54.192.66.13	HTTP	209	GET /we-have-the-blue-prints-to-the-Death-Star HTTP/1.1
283	10.344433	54.192.66.13	172.16.173.192	HTTP	667	HTTP/1.1 301 Moved Permanently (text/html)
388	14.191831	172.16.173.192	54.192.66.116	HTTP	195	GET /we-will-defeat-Darth-Vader. HTTP/1.1
390	14.302361	54.192.66.116	172.16.173.192	HTTP	653	HTTP/1.1 301 Moved Permanently (text/html)

> Frame 170: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface \Device\NPF_{BE4CF575-B3E3-405B-A22A-9457B72B8C25}, id 0
> Ethernet II, Src: VMware_f5:cb:60 (00:0c:29:f5:cb:60), Dst: VMware_f5:36:4e (00:50:56:f5:36:4e)
> Internet Protocol Version 4, Src: 172.16.173.192, Dst: 54.192.66.123
> Transmission Control Protocol, Src Port: 50449, Dst Port: 80, Seq: 1, Ack: 1, Len: 141
▼ Hypertext Transfer Protocol
 > GET /we-will-defeat-Darth-Vader. HTTP/1.1\r\n
 Accept-Encoding: identity\r\n
 Host: www.umd.edu\r\n
 Connection: close\r\n
 User-Agent: Python-urllib/2.7\r\n
 \r\n
 [Full request URI: http://www.umd.edu/we-will-defeat-Darth-Vader.]
 [HTTP request 1/1]
 [Response in frame: 172]

0030 fa f0 d3 b3 00 00 47 45 54 20 2f 57 65 2d 77 69GE T /we-wi
0040 6c 6c 2d 64 65 66 65 61 74 2d 44 61 72 74 68 2d ll-defea t-Darth-
0050 56 61 64 65 72 2e 20 48 54 54 50 2f 31 2e 31 0d Vader. H TTP/1.1
0060 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 -Accept- Encoding
0070 3a 20 69 64 65 6e 74 69 74 79 0d 0a 48 6f 73 74 : identi ty--Host

The full requested URI (including host name) (http.request.full_uri)

A:\final-form.exe

Type here to search

2:14 PM 12/11/2020

After further analyzing what messages does the malware final-form.exe file is sending, and I have found messages/Http connections.

The final-form.exe is trying to connect to the 2 websites.

<http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star>

<http://www.umd.edu/We-will-defeat-Darth-Vader>.

Conclusion: -

From the evidence collected above we can conclude that: -

1. The Blueprints of the Death star are leaked, and they are with the rebels now.
2. Also, final-form.exe is the final form of the malware.

Suggestions to the Imperial Army: -

I would suggest to the imperial army that they should take the hash value of this malware and make an IOC also submit to AV solutions so it can be quarantine from the infected system. Then those systems should be scanned and If needed should be re-imaged and block the websites/domain in the firewall.

Also, I would suggest having good EDR solution and a proper SOC team which can work 24*7. This will be helpful to prevent further breaches and immediately start finding the loopholes in death star if any present to prevent further damage.

Difficulties faced: -

1. I was not able to relate the URL message that was originally in base64. But soon I have realized it and converted it to ASCII.
2. The other difficulty was with VeraCrypt. But after going through anti forensics slide again and doing exercise. I was able to successfully decrypt the content of mp3 file.

Most enjoyed things: -

I learned deeply about Autopsy and Wireshark. These tools are useful and used in everyday life of forensics investigator. I have learned a lot of things and I liked the lectures and the slides which will be really be helpful at the time of interviews. The lectures were in so many details which really helped me in understanding the world of DFIR deeply.