Final Project

Dadhija Patel

119186367

ENPM687 0101

***“I pledge on my honor that I have not given or received any unauthorized assistance on this assignment.”***

**Summary of Information:**

The forensic investigation of the image obtained from the malware writer has led to interesting discoveries relating to the rebbelion. The most important piece of information found was a malware that would soon affect our system and a secret message communication between the rebel forces that they have intel on how to Defeat Darth vader.

**Tools Used:**

Autopsy: Autopsy is an open-sourced digital forensics platform that can be used to analyze files and recover data from damaged electronics like cell phones, hard drives, and computers.

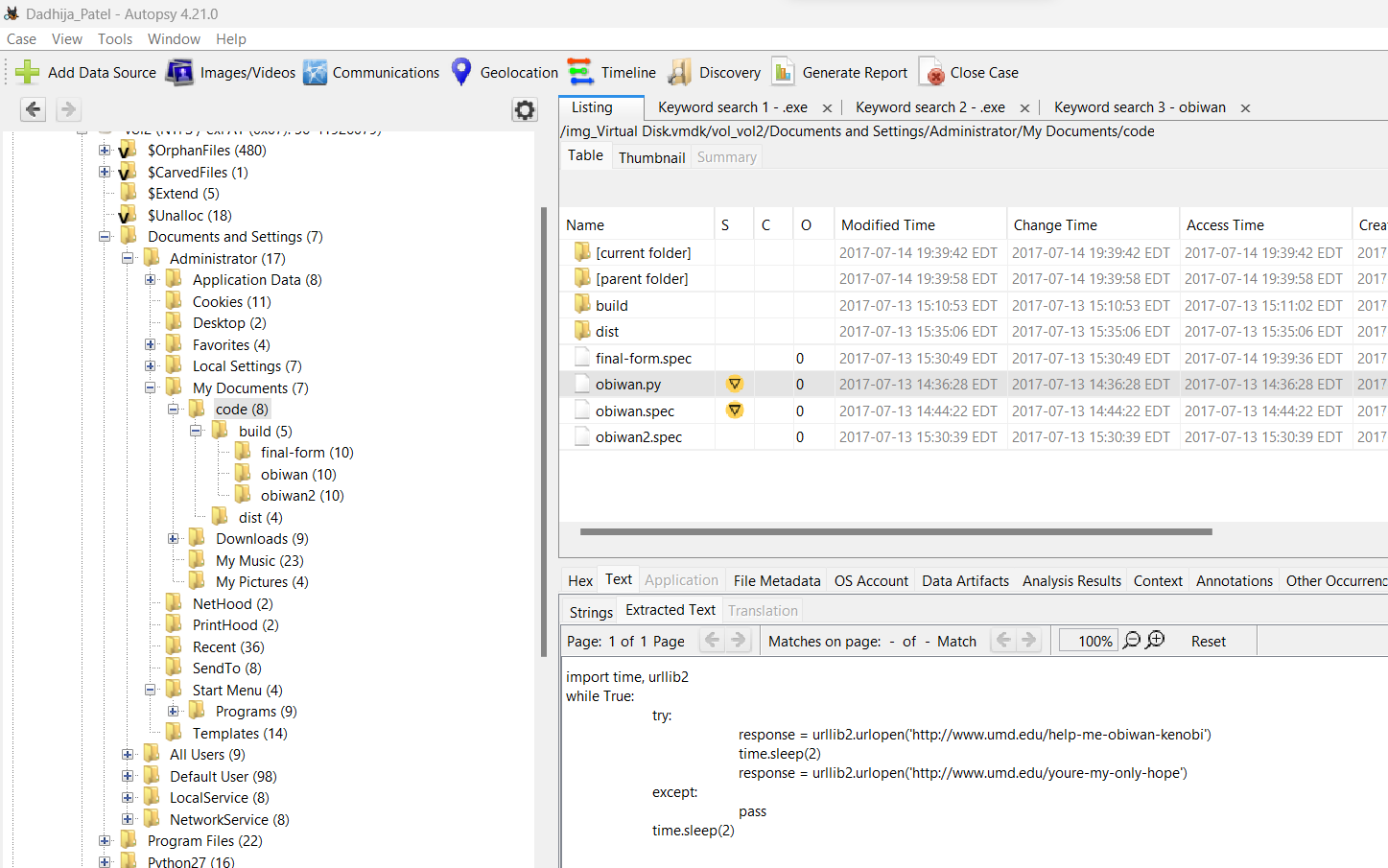
Wireshark: Wireshark is a free and open-source tool used to analyze network traffic. It captures packets and provides information contained in those packets.

VeraCrypt: VeraCrypt is an open-source encryption software that uses encryption protocols like AES (strong encryption properties) to encrypt and decrypt files, folders, and even entire devices.

**Repository: Hard Drive Image**

Summary: The interesting evidence found in the hard drive includes two malware files that show some communication and give key to open a suspicious audio file. The audio file, when decrypted in veracrypt, opens a folder containing death star plans and a malware that sends messages about defeating Darth Vader.

1. In Documents and Settings 🡪 Administrator 🡪 Code, there are two obiwan files. The obiwan.py file shows that it is trying to reach umd.edu/help-me-obiwan-kenobi and umd.edu/youre-my-only-hope. The requests are send repeatedly over specific time intervals.



A screenshot of a computer

Description automatically generated

The wireshark traffic captured for obiwan.exe shows the malware trying to to reach the above two sites. The response is that the site is moved permanantly. The analysis into such a request leads me to believe that obiwan.exe is trying to send a message for help.

A close up of a screen

Description automatically generated

A screenshot of a computer

Description automatically generated

1. The obiwan2.exe file also shows some interesting URL requests. As deduced from the previous obiwan.exe file, I believe that these files are being used to communicate among the rebels rather than as malware. So, the code found in the URL request of obiwan2.exe could be some secret code of communication.

A close-up of a computer screen

Description automatically generated

The series of messages sent by the obiwan2.exe files reveal that the code is base64 encoded. Moreover, this is not the end of the malware writer’s malicious code. There seems to be a final-form that contains more information about the malware writer’s mission and role with the rebels.

A screenshot of a computer

Description automatically generated

1. I found a VeraCrypt folder in the image. I suspected that the malware writer might be using the VeraCrypt software, so I went into the software folder of the hard disk and found VeraCrypt version v.1.21 installed. Therefore, the malware writer must have used it to encrypt files.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. After realizing that the malware file might be encrypted, I opened the encryption suspected folder and found a few interesting files.

A screenshot of a computer

Description automatically generated

1. In the My Music folder, I found an audio “not-the-droids-youre-looking-for.mp3” that was marked suspicious and sticking with the Star Wars theme, decided that it was worth the investigation.

Upon extraction, I realized that it was not an audio file, but an encrypted file made to look like audio.

A screenshot of a computer

Description automatically generated

1. The code from obiwan2.exe revealed the key as “r2d2” when decoded.

A screenshot of a computer

Description automatically generated

1. Using the key, I decrypted the above audio and a folder containing death star plans was revealed.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

1. The final-form.exe file was another communication file that sent the message about defeating Darth Vader with the blueprints of Death Star.

A close-up of a screen

Description automatically generated

A close-up of a screen

Description automatically generated

A screenshot of a computer

Description automatically generated

**Recommendations for next steps:**

My recommendation would be to continue the investigation as a lot of files still seem unrecovered. These files may contain data that could prevent future malware attacks and help the organization realize some of the flaws in their system.

**Challenges I faced in the project:**

1. Finding that the code obtained in obiwan2.exe was base64 encoded.

I captured a lot of traffic in the obiwan2.exe file. I saw the code and tried to think of ways to decode it, but nothing was working well. After capturing the data twice, I decided to just go through the http requests to make the number of packets smaller and succeeded in finding the right decoding method.

1. Finding other interesting files in the hard disk image.

After going through the folders, I realized that many files were marked suspicious by the autopsy software. I went through 5 or 6 files which revealed nothing to me until I found the emails folder and realized that these could be something that would help with the investigation. Going through recent files was also an afterthought. Understanding what the malware writer was using before I went through all the encoding would have made this investigation a lot easier.

**Other interesting files I found:**

1. Emails

A screenshot of a computer

Description automatically generated

1. Email attachments

The email attachment shows SMTP request overload. This could mean that the attacker was trying to overload the server into stopping the service (DDoS attack).

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Death Star plans in recent files

A screenshot of a computer

Description automatically generated

**References:**

<https://www.sleuthkit.org/autopsy/>

<https://en.wikipedia.org/wiki/Wireshark>

<https://en.wikipedia.org/wiki/VeraCrypt>