JUNE 2021
SILICON INSTITUTE OF TECHNOLOGY, BHUBANESWAR

THE JIGSAW RANSOMWARE

A closer look into the spread...

PREPARED BY:

- Prabhudarshan Samal (180310180)
- Subhrajyoti Behera (190310158)
- Raoshnak Quadri (190310020)
- Sai Subramanyam (190310452)

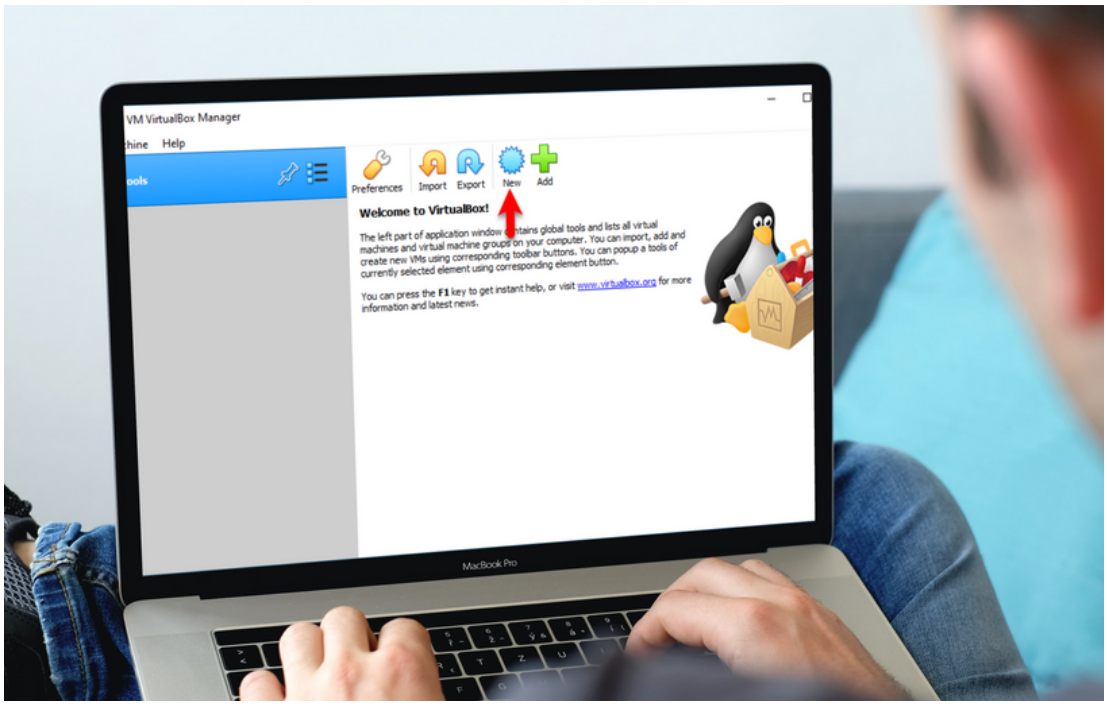
MENTORED BY:

- Mr. Venkatesh Mainani

STEP:1

Setting Up the Virtual Machine on Windows

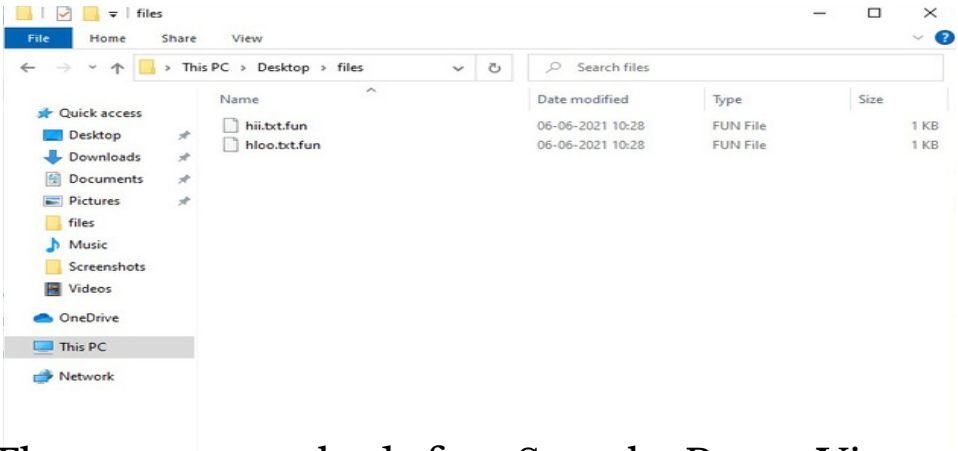
- We visited the official website of VirtualBox from where we downloaded the **Oracle VM VirtualBox** from **VirtualBox 6.1.18 platform packages**.
- After the download was complete we ran the Setup to install the latest version of Oracle VM VirtualBox on our **host Windows platform**.
- After the previous steps were successfully completed, we visited the official website of Microsoft to download the **Windows 10 Enterprise ISO**.
- Thereafter following all the necessary steps including memory allocation, mounting the windows ISO file, creating a virtual optical disc etc we finally installed the windows 10 as VM.



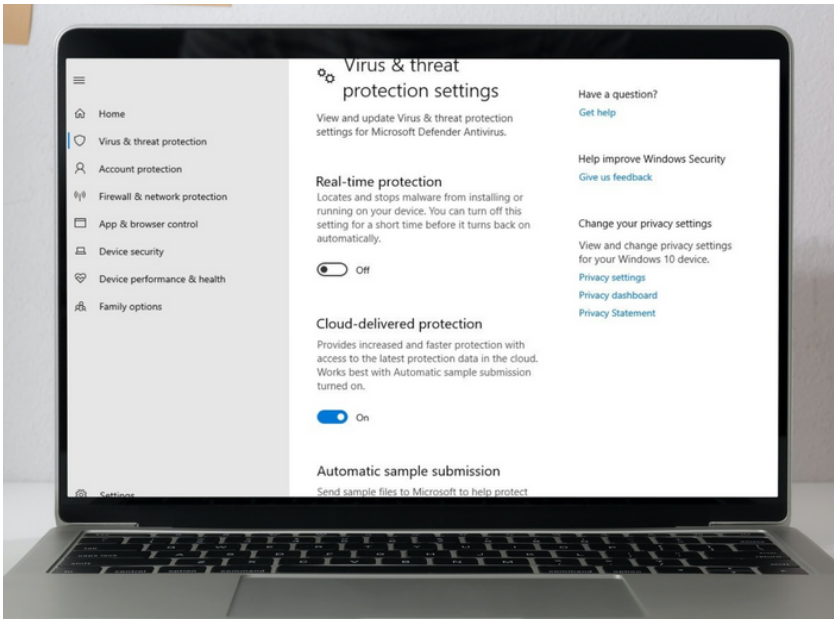
STEP:2

Testing JIGSAW RANSOMWARE

- After finishing the installation successfully we booted into the new **Virtual Machine.**
- Then we searched for Control Panel-->Programs-->Programs and Features-->Turn Windows Feature ON or OFF and verified that the **.NET Framework 3.5** is turned ON.
- Then after we created some random files and placed them on the desktop.



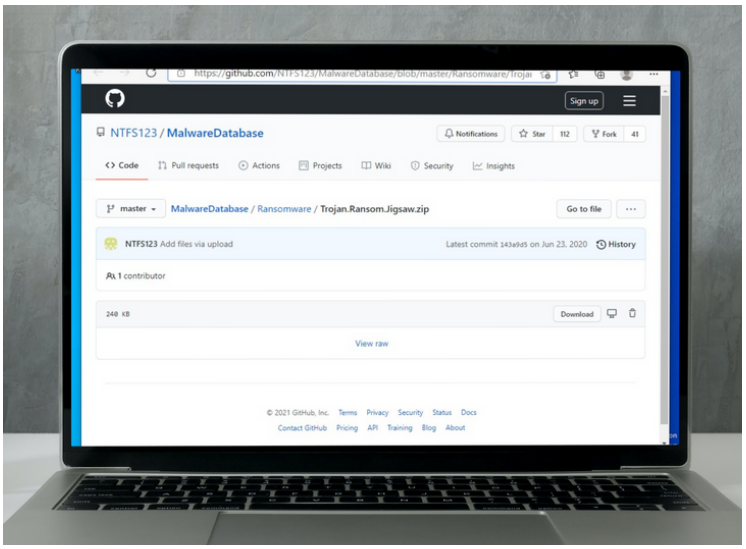
- Then we searched for Search Bar-->Virus and threat protection-->Manage Settings-->Virus and Threat Protection Settings and then we turned off **Real Time Threat Protection** which allowed us to test the Ransomware without the interference of windows security.



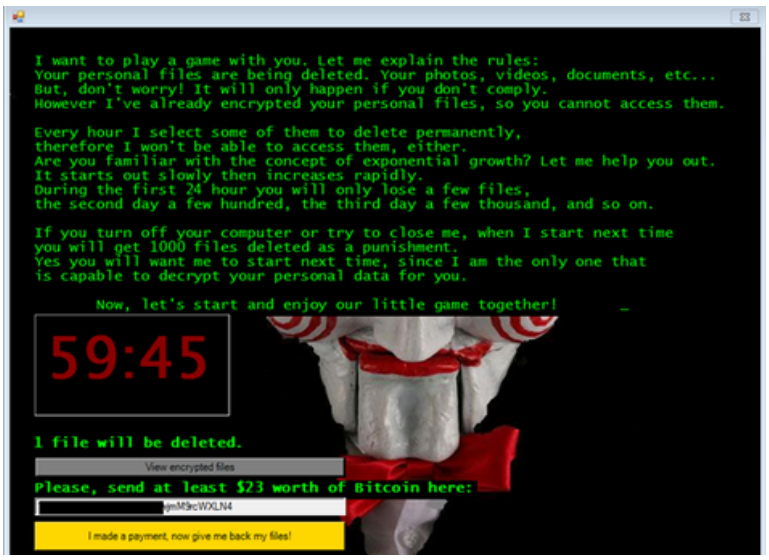
TO BE CONTINUED...

Testing JIGSAW RANSOMWARE

- After following all the above mentioned steps we downloaded the **Jigsaw Ransomware** with this link from the given link.



- After downloading we unzip the folder and renamed it by adding **.exe** at the end of the filename to make it executable.
- Then we double clicked on the file to run and clicked on run anyway.
- After a few minutes all the files of the system got encrypted, a pop-up windows appeared on the screen stating that we have to pay **0.4 Bitcoins** to get the decryption key.
- The pop-up window also contained a live countdown starting from 59:59 within which one file will be deleted if the Ransom was not paid.



STEP:3

Detection and Verification

- Although the files were encrypted but still we could able to access the web browser and visited the official website of ID Ransomware.
- There we uploaded a sample encrypted file to verify it is Jigsaw Ransomware and whether it is decryptable or not. And fortunately we found it decryptable!

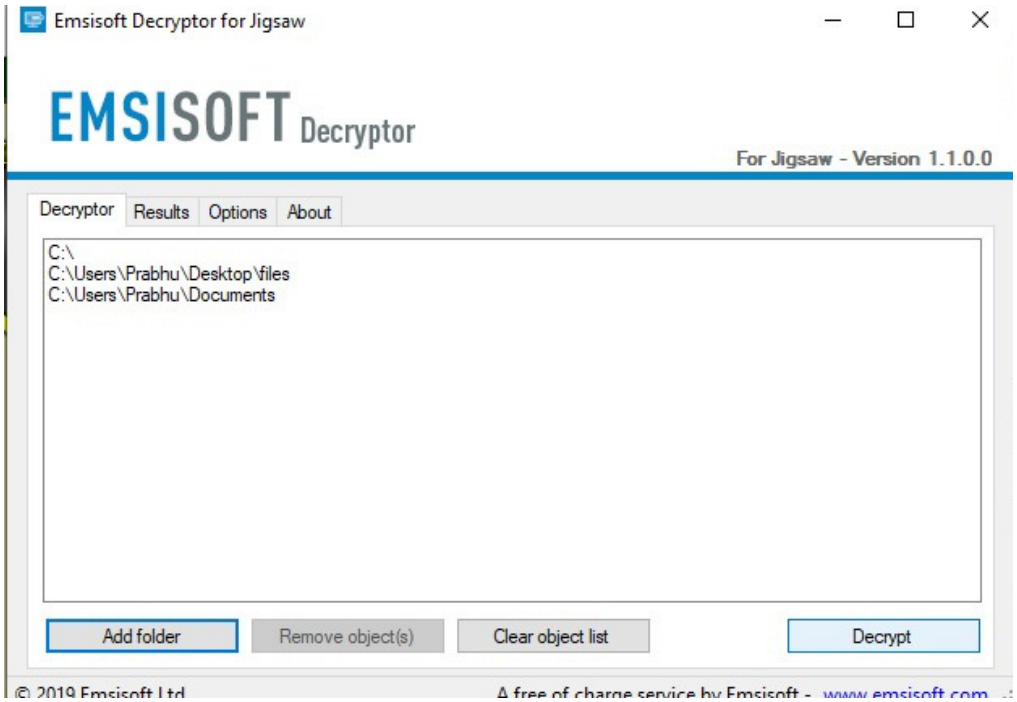
STEP:4

Removal and Decryption

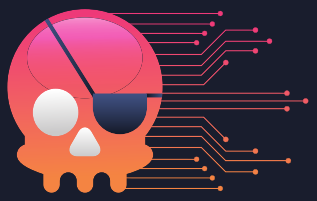
- We visited the **emsisoft** official website to download our ransomware decryption tool.
- There we searched for the Jigsaw **Decrypter** Tool and downloaded it.
- After the download was complete we ran the set-up to install the tool.
- After successful installation we ran the software where we added a folder in which all the ransomware encrypted drives were selected.
- Finally the decryption process started and as soon as it completed all the files in the system was back!

TO BE CONTINUDE...

Removal and Decryption

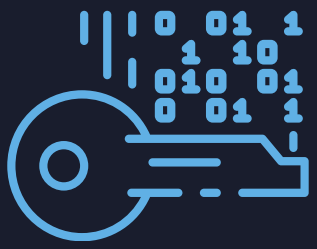


FINAL STEPS...



The Steps are as followed:

- Delete the residue/unnecessary files left over after the decryption process.
- Go to Task Manager and end all the unnecessary background processes.
- Restart the Virtual Machine to get rid of the Jigsaw Ransomware pop-up window.
- After the reboot is done, the system will back to its previous state.



******