Group 7

Step 3: Infection

Team Members:-

1. **Vamshi Krishna Bukka - 11693102 - vamshikrishnabukka@my.unt.edu**
2. **Sivabhavana Nelluri - 11702191 - sivabhavananelluri@my.unt.edu**
3. **Nithish Kumar Boggula -** 11559328 - nithishKumarBoggula@my.unt.edu
4. **Revanth Boddupalli - 11718089 - revanthBoddupalli@my.unt.edu**
5. **Vikram Reddy Allam - 11697684 - vikramallam@my.unt.edu**

Memo: Infection Method Development

Step 1: Preparation of the executable file

AES encryption can be used to encrypt files in a designated directory by executing a prepared Python script called script.py This script is going to be transformed into an executable file (your gift is inside this) in order to mimic a typical file type that people could anticipate receiving by email.

Step 2: Email Distribution

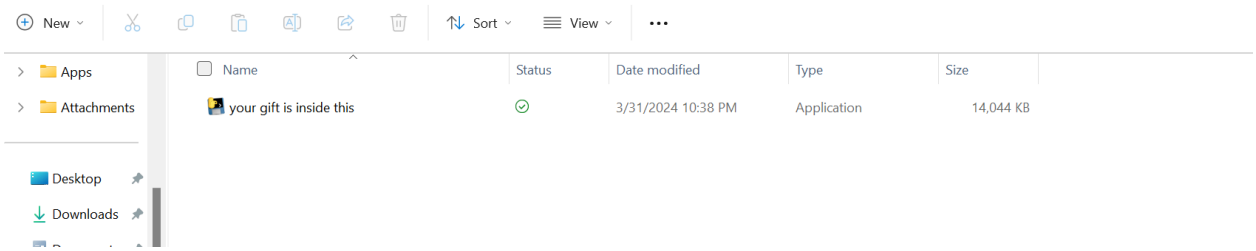
An email with the executable link will be sent, carefully designed to look real and tempt the recipient to open the attachment link.

Step 3: Execution and Encryption

The script simulates the impact of a ransomware infection by encrypting files in the preset directory after downloading and running the (your gift is inside this.exe) file.

Screenshots:-

Executable File Image: -



First, we converted the script file into an executable file in order to encrypt the file without giving commands.

After this, we will be sending an email to a targeted email which is called email phishing where we will lure the target user to click on the link and get infected. The target user will not know that this is malicious code.

https://drive.google.com/file/d/1Ij0U4cxOeuhhHXe0A3hd4quoJYsyjXFc/view?usp=drivesdk
This link contains the malicious code.

Free Gift!! Inbox ×

Hakuna Matata <dishaagarwal619@gmail.com>
to me

11:21 PM (3 minutes ago)

One attachment • Scanned by Gmail

your gift is inside ...

Congratulations you won the lottery Inbox ×

Hakuna Matata <dishaagarwal619@gmail.com>
to me

11:31 PM (0 minutes ago)

Hello,

Thank you for participating in our monthly lottery. We are delighted to share that you have won a lottery. Please find the attached gift to claim your gift. You will need to click on the link to access the gift.

https://drive.google.com/file/d/1Ij0U4cxOeuhhHXe0A3hd4quoJYsyjXFc/view?usp=drivesdk

Regards,
Lottery Team

One attachment • Scanned by Gmail

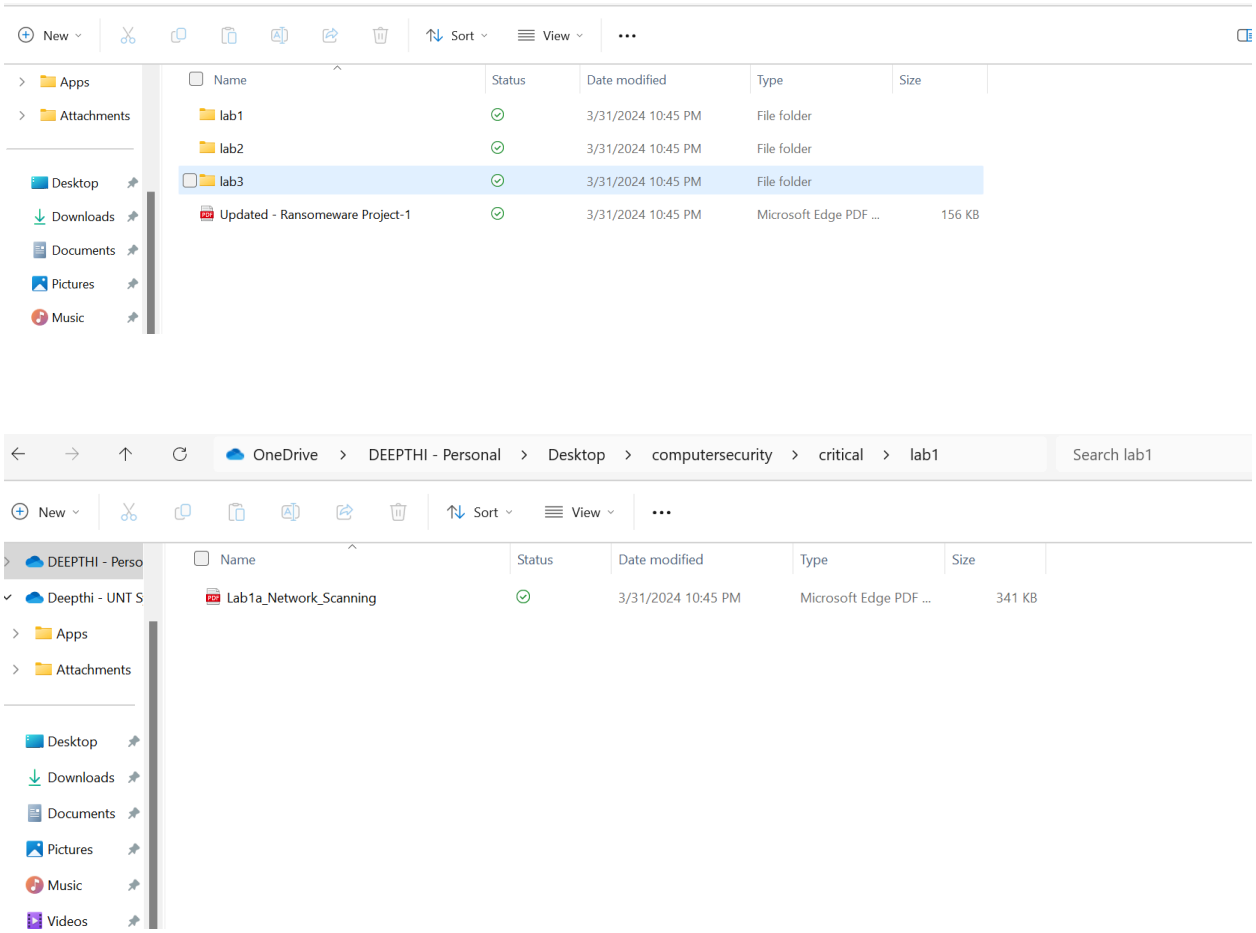
your gift is inside ...

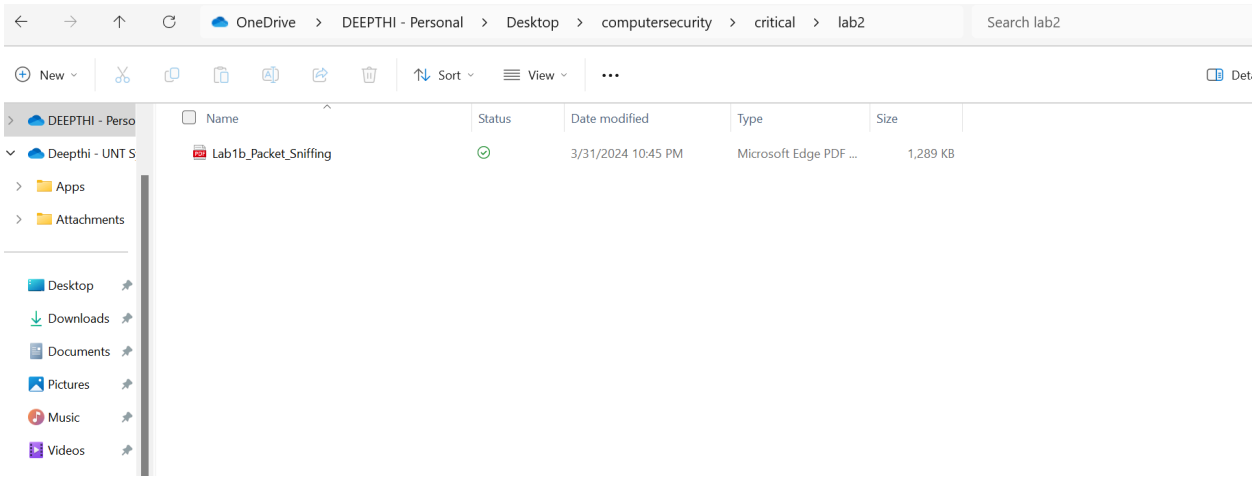
Reply Forward

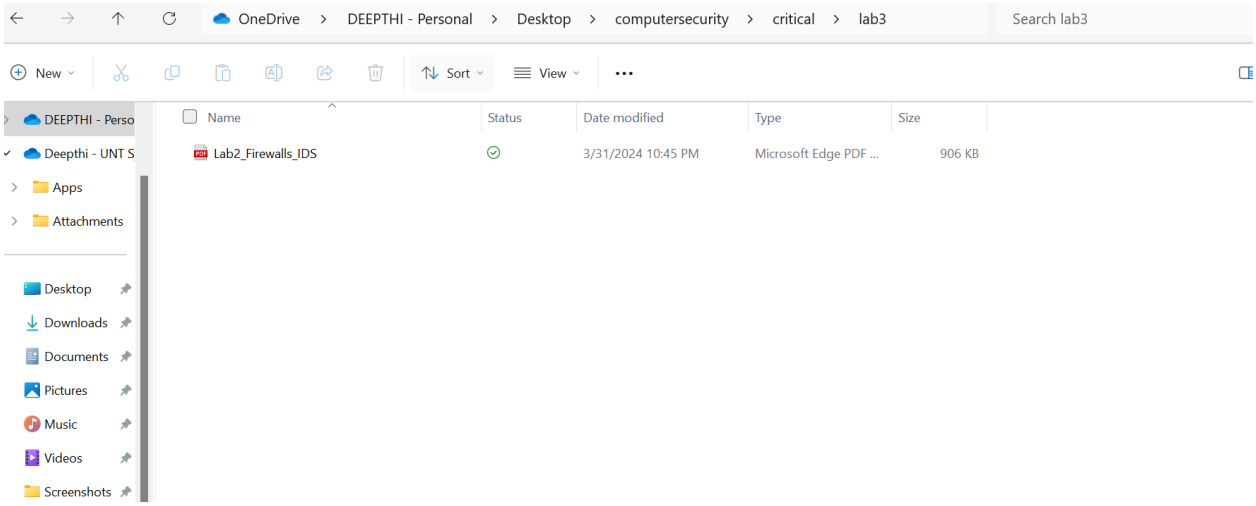
This is the image the recipient will get.

Before Encryption: -

These are before encryption

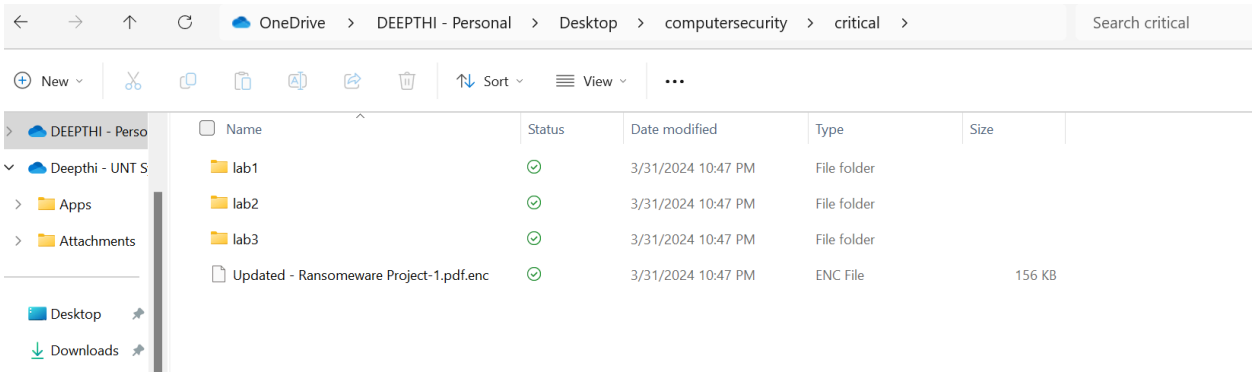


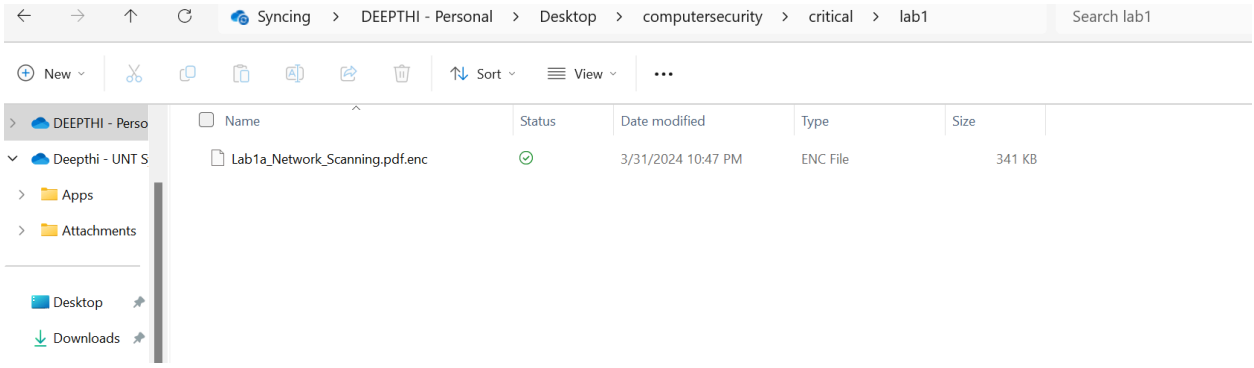


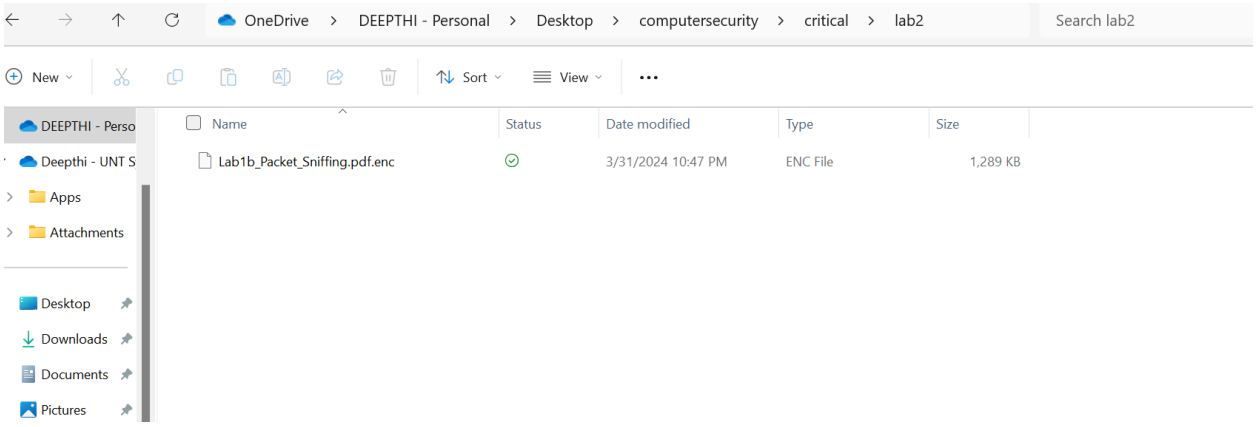


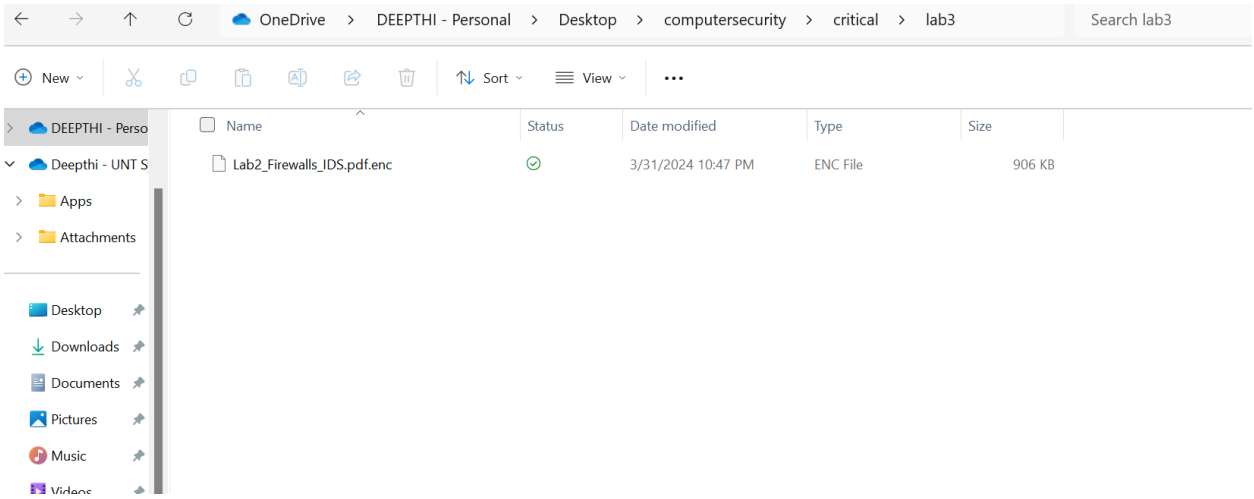
After Encryption: -

This is after encryption.


OneDrive › DEEPTHI - Personal › Desktop › computersecurity › critical ›
Search critical
New
Sort
View
DEEPTHI - Perso
Deepthi - UNT S
Apps
Attachments
Desktop
Downloads
Name
Status
Date modified
Type
Size
lab1
3/31/2024 10:47 PM
File folder
lab2
3/31/2024 10:47 PM
File folder
lab3
3/31/2024 10:47 PM
File folder
Updated - Ransomeware Project-1.pdf.enc
3/31/2024 10:47 PM
ENC File
156 KB


Syncing › DEEPTHI - Personal › Desktop › computersecurity › critical › lab1
Search lab1
New
Sort
View
DEEPTHI - Perso
Deepthi - UNT S
Apps
Attachments
Desktop
Downloads
Name
Status
Date modified
Type
Size
Lab1a_Network_Scanning.pdf.enc
3/31/2024 10:47 PM
ENC File
341 KB


OneDrive › DEEPTHI - Personal › Desktop › computersecurity › critical › lab2
Search lab2
New
Sort
View
DEEPTHI - Perso
Deepthi - UNT S
Apps
Attachments
Desktop
Downloads
Documents
Pictures
Name
Status
Date modified
Type
Size
Lab1b_Packet_Sniffing.pdf.enc
3/31/2024 10:47 PM
ENC File
1,289 KB


OneDrive
DEEPTHI - Personal
Desktop
computersecurity
critical
lab3
Search lab3
New
Sort
View
DEEPTHI - Perso
Deepthi - UNT S
Apps
Attachments
Desktop
Downloads
Documents
Pictures
Music
Videos
Name
Status
Date modified
Type
Size
Lab2_Firewalls_IDS.pdf.enc
3/31/2024 10:47 PM
ENC File
906 KB