Ransomeware project

Team Members:

Muvva Hima sai -- 11695369
Tagore Hari Prasad Chintamaneni -- 11702057
Ajay Eedara -- 11702053
Venkata Naga sai hemanth varma kunaparaju -- 11701764
Jaideep Tripurani -- 11709159

What is Ransomware

- Ransomware is a malicious software or we can it as code designed to block access to a computer system or files until ransom is paid.
- System may be Server or Client.
- They maintained a secure channel for communication and attackers mostly ask ransom through cryptocurrency.
- Its developed using cryptography.

Cryptography

- Why Cryptography?

Because Ransomware is implemented using Cryptography techniques.

- Types of Cryptography

  Symmetric and Asymmetric cryptography

Symmetric and Asymmetric

- Symmetric is implemented with one key for Encryption and Decryption of data.
- Asymmetric is implemented with two keys that is public and private key for encryption and decryption.
- In this Project We have implemented the Symmetric Key Encryption.

Our Implementation Plan

- We have developed a ransomware using python
- Converted the python to executable file
- Sended the exe file over link to victim
- Victim installed the exe because of phishing
- Implemented the Monitoring, Detection and Mitigation tools from stopping the Ransomware attack.

Action

- Encryption

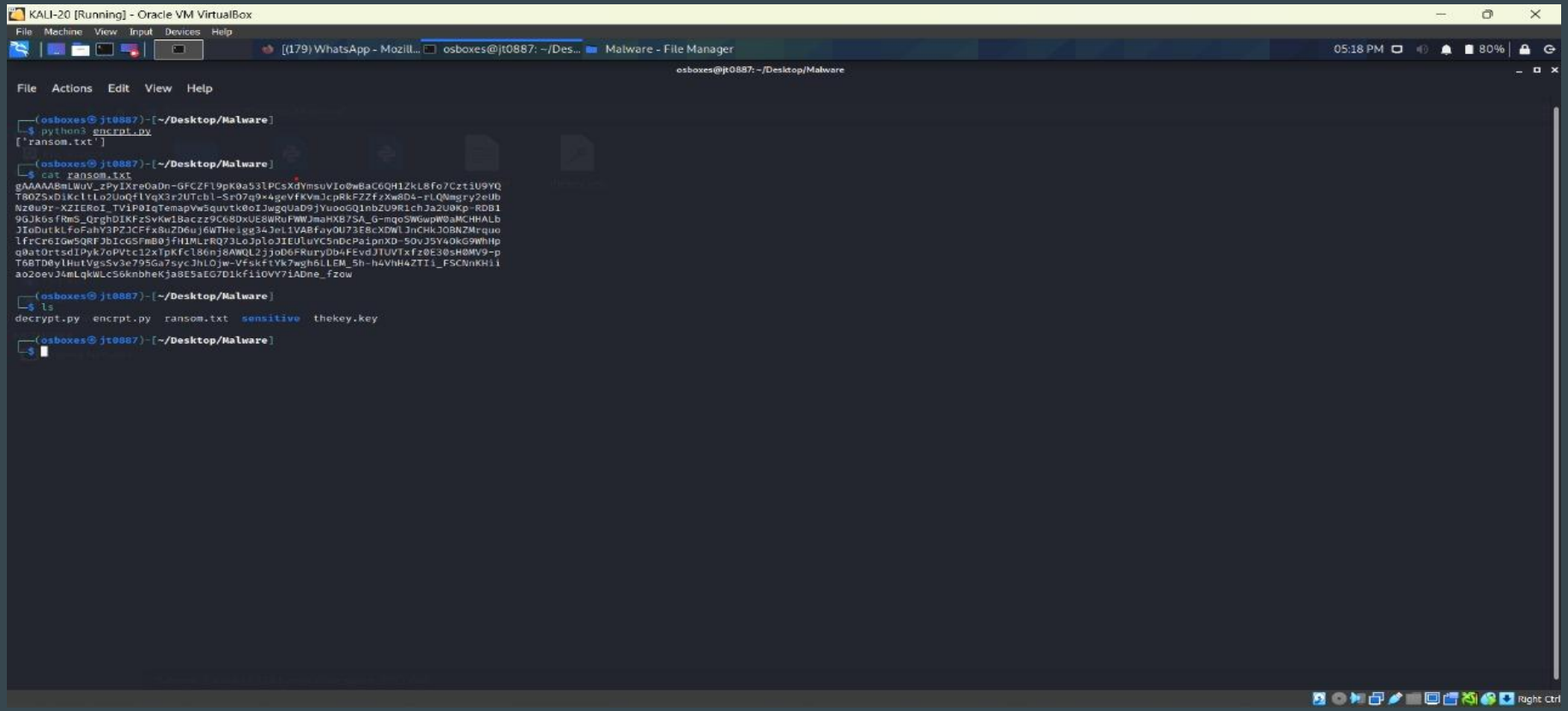
We have implemented the python code which works on symmetric method which encrypts the directory recursively.

- Decryption

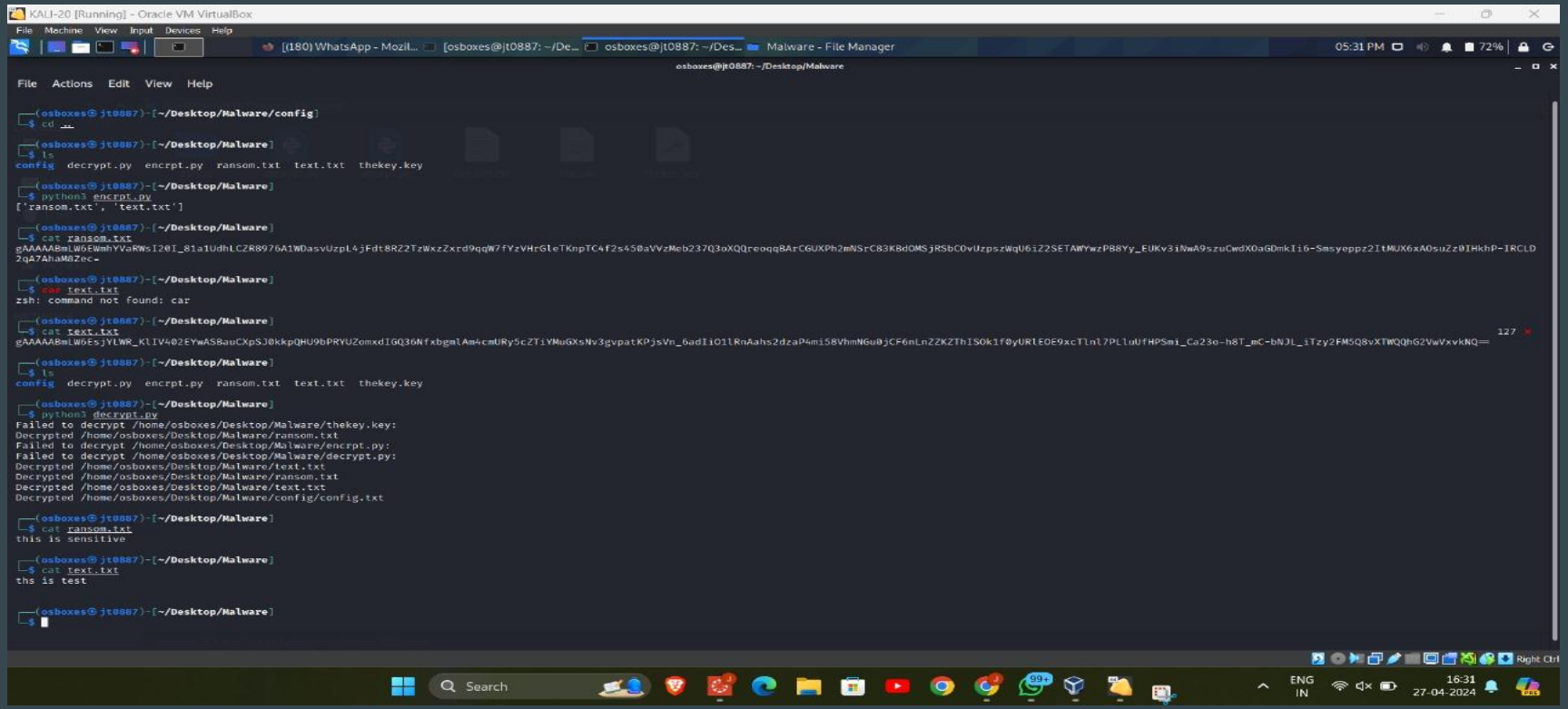
We have implemented the python code which works on symmetric method and decrypts the directory recursively.

Next We have the image of implementation.

Encryption Image

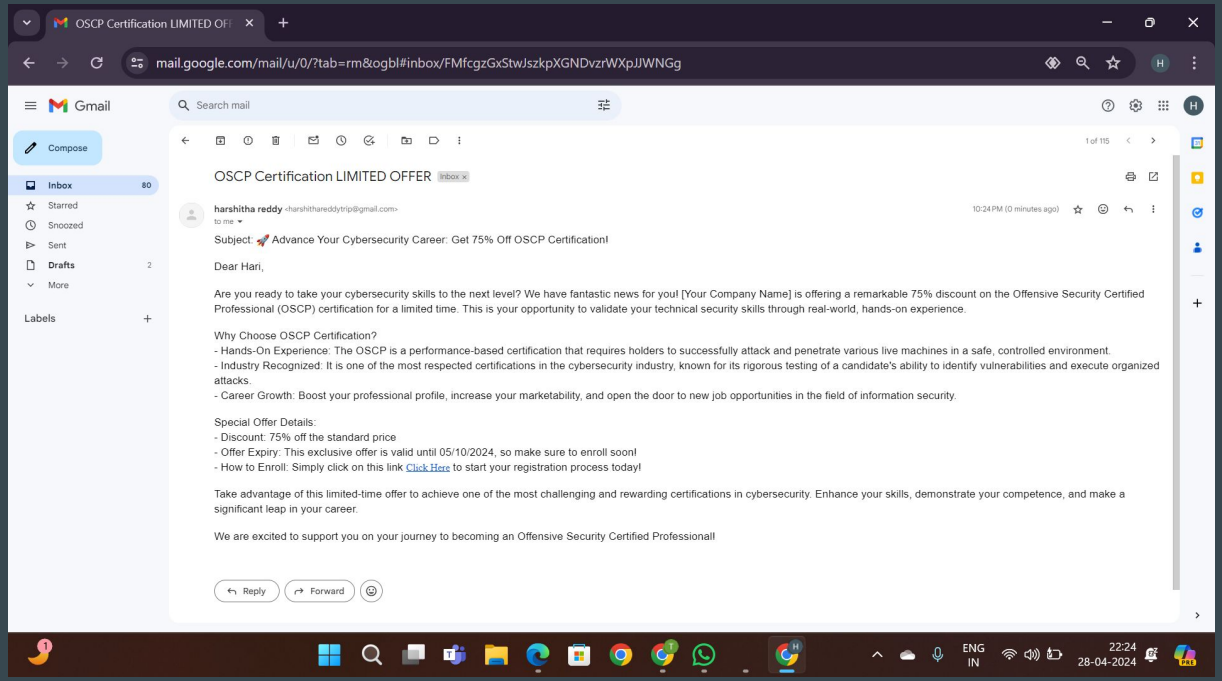


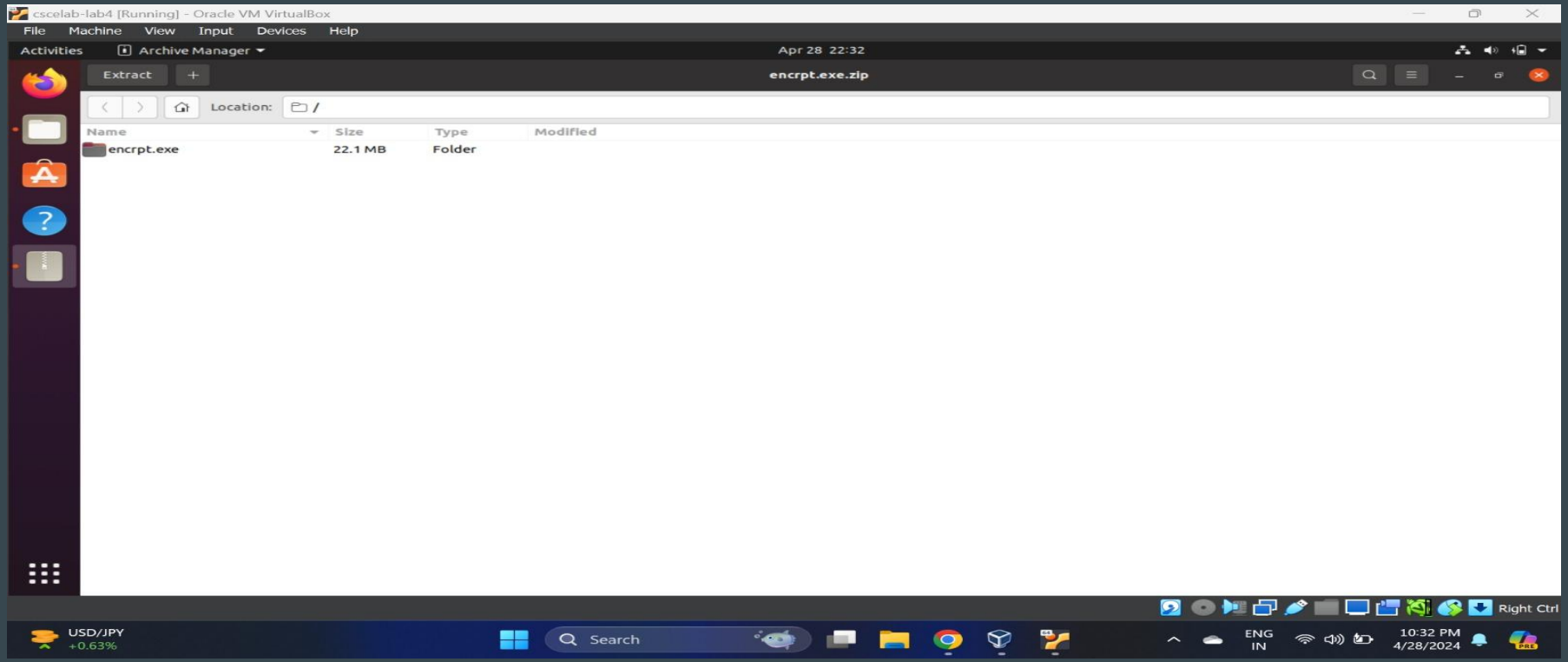
Decryption image



Infection

- We have generated the exe file from python file
- Sended the exe file as a link to the victim which is a phishing mail.



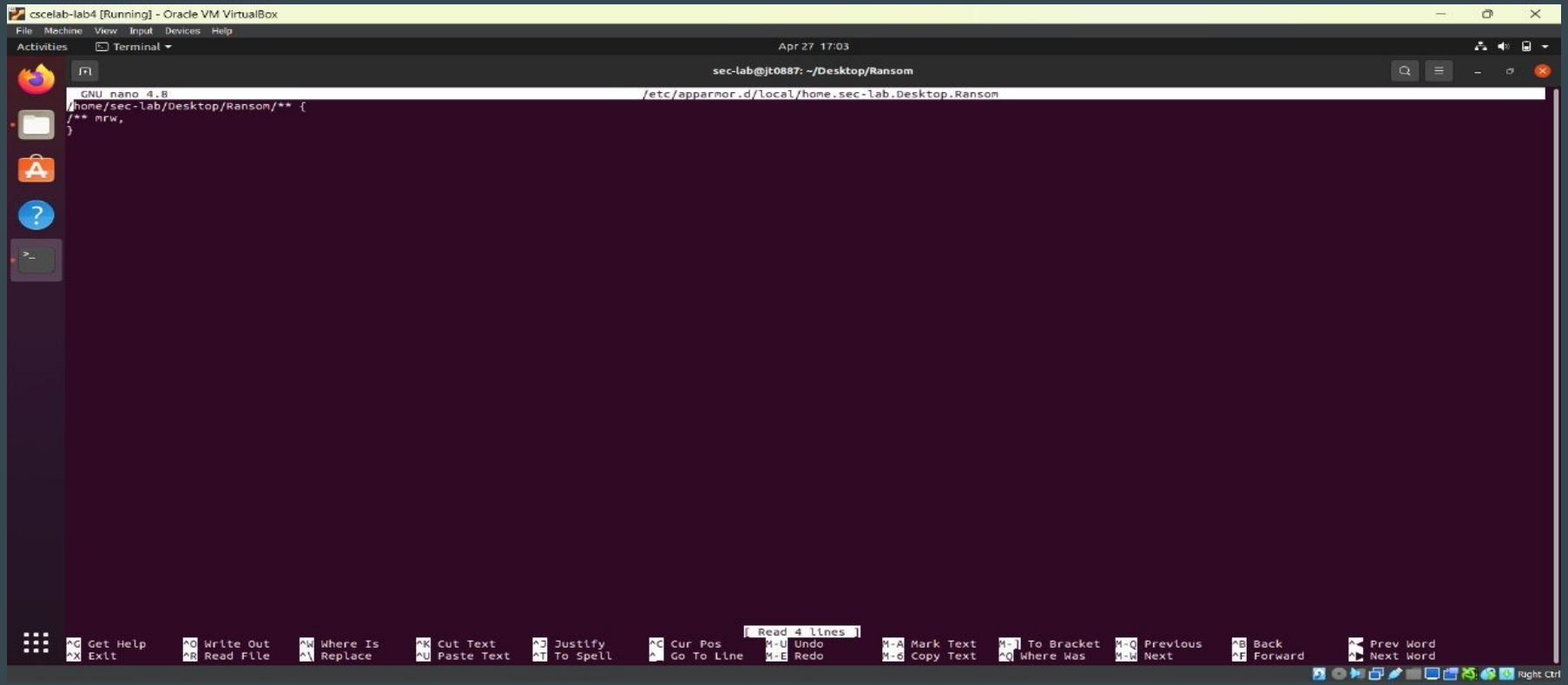


As you can see the file has been downloaded into victim’s system after victim click on the link which we have sent through mail.

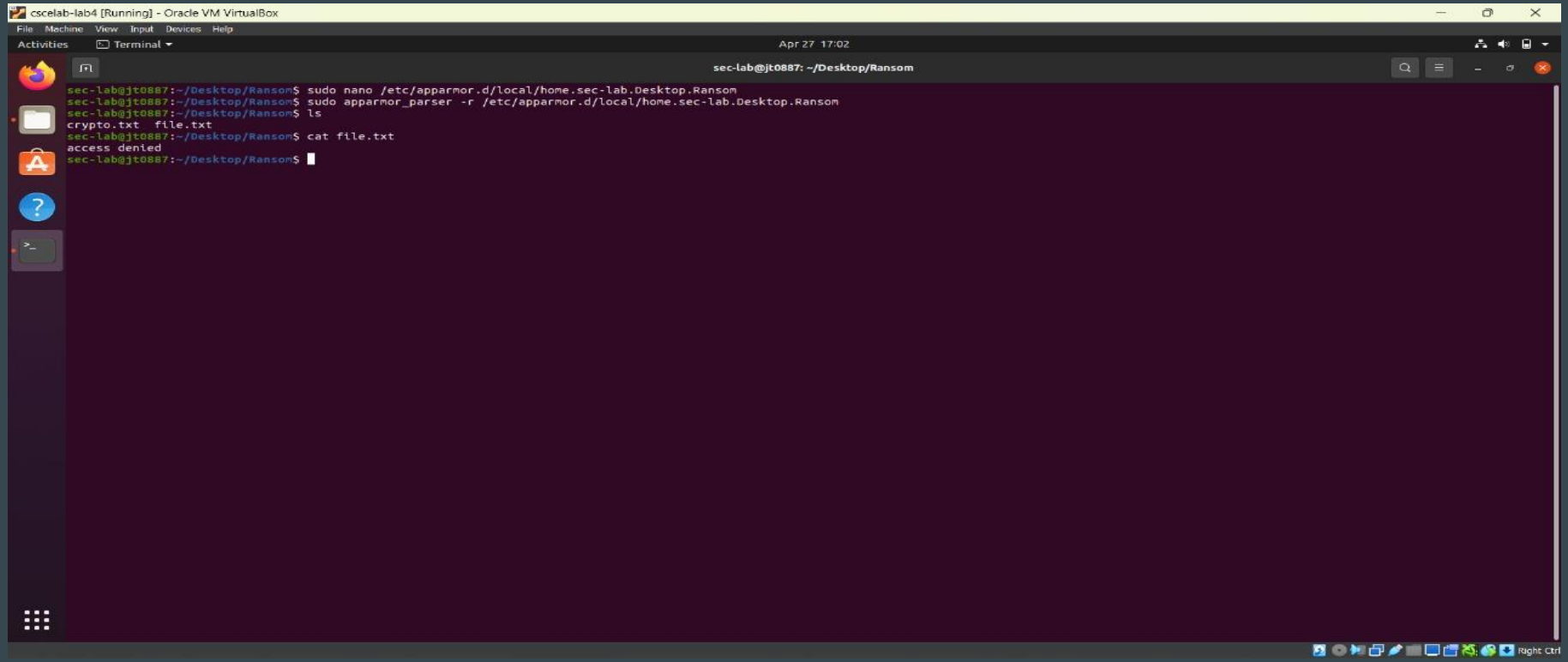
Monitoring

- We have used tools like apparmor for monitoring the system for file changes and configured the file permissions based on the policy.
- We have used the windows defender for monitoring the system for malware monitoring .

Monitoring Policy Apparmor



Monitoring apparmor



Monitoring using File Integrity Check

fileintegriy.py

```python
import os
import hashlib
import json

def calculate_file_hash(file_path):
    hasher = hashlib.sha256()
    with open(file_path, 'rb') as file:
        for chunk in iter(lambda: file.read(4096), b''):
            hasher.update(chunk)
    return hasher.hexdigest()

def create_or_load_hash_database(database_path):
    if os.path.exists(database_path):
        with open(database_path, 'r') as db_file:
            return json.load(db_file)
    else:
        return {}

def update_hash_database(database_path, file_path, file_hash):
    database = create_or_load_hash_database(database_path)
    database[file_path] = file_hash
    with open(database_path, 'w') as db_file:
        json.dump(database, db_file, indent=2)

def check_integrity(directory_to_monitor, database_path):
```

LightEdit mode. Access full IDE

Autosave: off 1:1

items 1 item selected 1.59 KB

Search

1:59 PM
4/28/2024

Detection

- We have used the Windows Defender and Windows Firewall for detection of malware
- In windows we have the real time malware detection and its the best approach for the detection of malware

Detection

Windows Defender Firewall

Control Panel › System and Security › Windows Defender Firewall

Search Control Panel

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	babycalmdown
Notification state:	Notify me when Windows Defender Firewall blocks a new app

See also

Security and Maintenance

Network and Sharing Center

Search

ENG IN

16:25 28-04-2024

Windows Security

- Home
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control
- Device security
- Device performance & health
- Family options
- Protection history

CrowdStrike Falcon Sensor

CrowdStrike Falcon Sensor is turned on.

Current threats

No actions needed.

Protection settings

No actions needed.

Protection updates

No actions needed.

Open app

Microsoft Defender Antivirus options

You can keep using your current provider, and have Microsoft Defender Antivirus periodically check for threats.

Periodic scanning

Off

Code for services check

- We have a idea of python code which check the suspicious long running services check in the system.
- It gives the names of the services which is one of the way of detection.

Image of services check

services.py - ...\ransom (1)\ransom

fileintegriy.py | services.py

```python
import win32service
import win32serviceutil
import win32con
from datetime import datetime, timedelta

def report_long_running_services(max_runtime_hours=24):
    scmanager = win32service.OpenSCManager(None, None, win32service.SC_MANAGER_ALL_ACCESS)

    status = 1
    services = win32service.EnumServicesStatus(scmanager, win32service.SERVICE_WIN32, win32service.SERVICE_STATE_ALL)

    for service in services:
        name, display_name, service_status = service[:3]
        if service_status[1] == win32service.SERVICE_RUNNING:
            # Service is running
            runtime = datetime.now() - win32serviceutil.GetServiceStartDate(name)
            if runtime > timedelta(hours=max_runtime_hours):
                print(f"Long-running service: {display_name} (Running time: {runtime})")
        else:
            print(f"{display_name} is not running currently.")

    win32service.CloseServiceHandle(scmanager)
```

mitigation

- Maintaining the backup is the best approach for mitigation.
- Maintaining the data at different availability zones and locations.
- We have a Python Script which automatically updates the data for every 4 hours and maintains the redundancy.
- Removing the services which are suspicious other way of mitigation.

Image of backup

fileintegriy.py | services.py | backup.py

```python
import os
import shutil
from datetime import datetime

def backup_files(source_dir, backup_dir):

    now = datetime.now().strftime('%Y-%m-%d_%H-%M-%S')
    backup_subdir = os.path.join(backup_dir, f'backup_{now}')


    os.makedirs(backup_subdir, exist_ok=True)

    for root, dirs, files in os.walk(source_dir):

        dest_dir = os.path.join(backup_subdir, os.path.relpath(root, source_dir))
        os.makedirs(dest_dir, exist_ok=True)
        for file in files:
            src_file = os.path.join(root, file)
            dest_file = os.path.join(dest_dir, file)
            shutil.copy2(src_file, dest_file)
            print(f'Copied {src_file} to {dest_file}')

    print(f'Backup completed successfully to {backup_subdir}')

# Set the source and backup directories
```

LightEdit mode. Access full IDE

Autosave: off 16:45

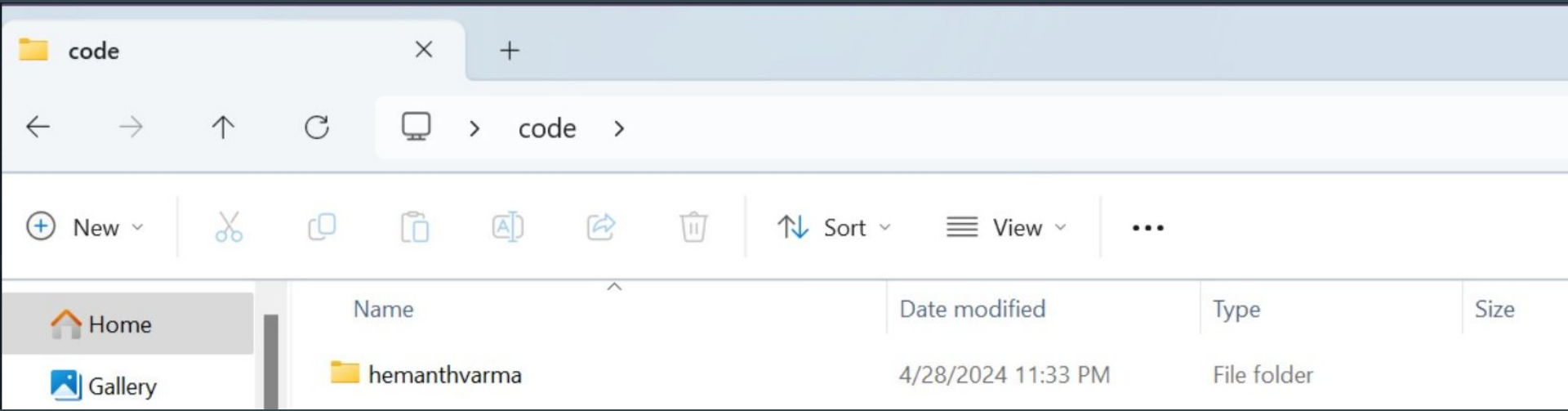
Windows PowerShell

```
PS C:\hemanthvarma> ls


    Directory: C:\hemanthvarma


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/28/2024  11:35 PM           1476 backup.py


PS C:\hemanthvarma> python3 backup.py
Copied C:\Users\dp1492\Desktop\data\3.py to C:\Users\dp1492\Desktop\crypto\backup_2024-04-28_23-37-32\.\3.py
Copied C:\Users\dp1492\Desktop\data\ciphertext.txt to C:\Users\dp1492\Desktop\crypto\backup_2024-04-28_23-37-32\.\ciphertext.txt
Backup completed successfully to C:\Users\dp1492\Desktop\crypto\backup_2024-04-28_23-37-32
PS C:\hemanthvarma> python3 backup.py
Copied C:\Users\dp1492\Desktop\data\3.py to C:\Users\dp1492\Desktop\crypto\backup_2024-04-28_23-37-36\.\3.py
Copied C:\Users\dp1492\Desktop\data\ciphertext.txt to C:\Users\dp1492\Desktop\crypto\backup_2024-04-28_23-37-36\.\ciphertext.txt
Backup completed successfully to C:\Users\dp1492\Desktop\crypto\backup_2024-04-28_23-37-36
PS C:\hemanthvarma>
```


code
code
New
Sort
View
Home
Gallery
Name
Date modified
Type
Size
hemanthvarma
4/28/2024 11:33 PM
File folder

Conclusion

In conclusion, our study on attacks using ransomware provides a thorough examination of the details of their deployment, the vulnerabilities they exploit, and the direct effects they cause. We demonstrated the ease with which these assaults may be carried out by creating a proof-of-concept ransomware utilizing the AES encryption standard and Python's Fernet library, notably through social engineering approaches like as phishing. Our research highlights the critical need for strong cybersecurity measures and user attention. The use of strong encryption practices and the simulation of ransomware attacks in a controlled setting highlight the vital role of security awareness and proactive defenses in reducing the disastrous impacts of such cyber threats. Furthermore, our findings provide insight into effective monitoring, detection, and mitigation options for protecting against ransomware.

In Final as a team we have implemented the Ransomware from Development, Infection, Monitoring, detection and till the mitigation of malware Ransomware.

References

1)J. Hurtuk, M. Chovanec, M. Kičina and R. Billík, "Case Study of Ransomware Malware Hiding Using Obfuscation Methods," 2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA), Stary Smokovec, Slovakia, 2018, pp. 215-220, doi: 10.1109/ICETA.2018.8572218. keywords: {Ransomware;Encryption;Computers;Conferences;Electronic learning},
https://ieeexplore.ieee.org/document/8572218

2)Ekta and U. Bansal, "A Review on Ransomware Attack," 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCC), Jalandhar, India, 2021, pp. 221-226, doi: 10.1109/ICSCCC51823.2021.9478148. keywords: {Ransomware;Cryptography;Surges;Cyberattack;Ransomware;Locky;Malware;Classification;DNS;Cyber Attack},
https://ieeexplore.ieee.org/document/9478148

3) R. Wilson and I. Iftimie, "Emerging ransomware threats: An anticipatory ethical analysis," 2021 IEEE International Symposium on Technology and Society (ISTAS), Waterloo, ON, Canada, 2021, pp. 1-1, doi: 10.1109/ISTAS52410.2021.9629211. keywords: {Ethics;Government;Medical services;Games;Market research;Software;Ransomware},
https://ieeexplore.ieee.org/document/9629211

4)P. K, B. Nataraj and P. Duraisamy, "An Investigation on Attacks in Application Layer Protocols and Ransomware Threats in Internet of Things," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 668-672, doi: 10.1109/ICACCS57279.2023.10112669. keywords: {Protocols;Taxonomy;Computer architecture;Agriculture;Internet of Things;Ransomware;Security;Internet of Things;Architecture layers;Application layer;Security threats;Ransomware Attacks;RFID Attacks;Application Layer Protocols},
https://ieeexplore.ieee.org/document/10112669

5)Lena Yuryna Connolly, David S Wall, Michael Lang, Bruce Oddson, An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability, Journal of Cybersecurity, Volume 6, Issue 1, 2020, tyaa023, https://doi.org/10.1093/cybsec/tyaa023
https://academic.oup.com/cybersecurity/article/6/1/tyaa023/6047253

6)Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. *Sustainability, 14*(1), 8. https://doi.org/10.3390/su14010008
https://www.mdpi.com/2071-1050/14/1/8

Thank You