Incident Handling Report

Simulated Ransomware Attack

Scenario: Ransomware Simulation in Controlled Environment

Type: Crypto ransomware

Date/Time of Incident: August 09, 2025 – 11;00 PM

Location: `C:\Users\USER 1\testfiles`

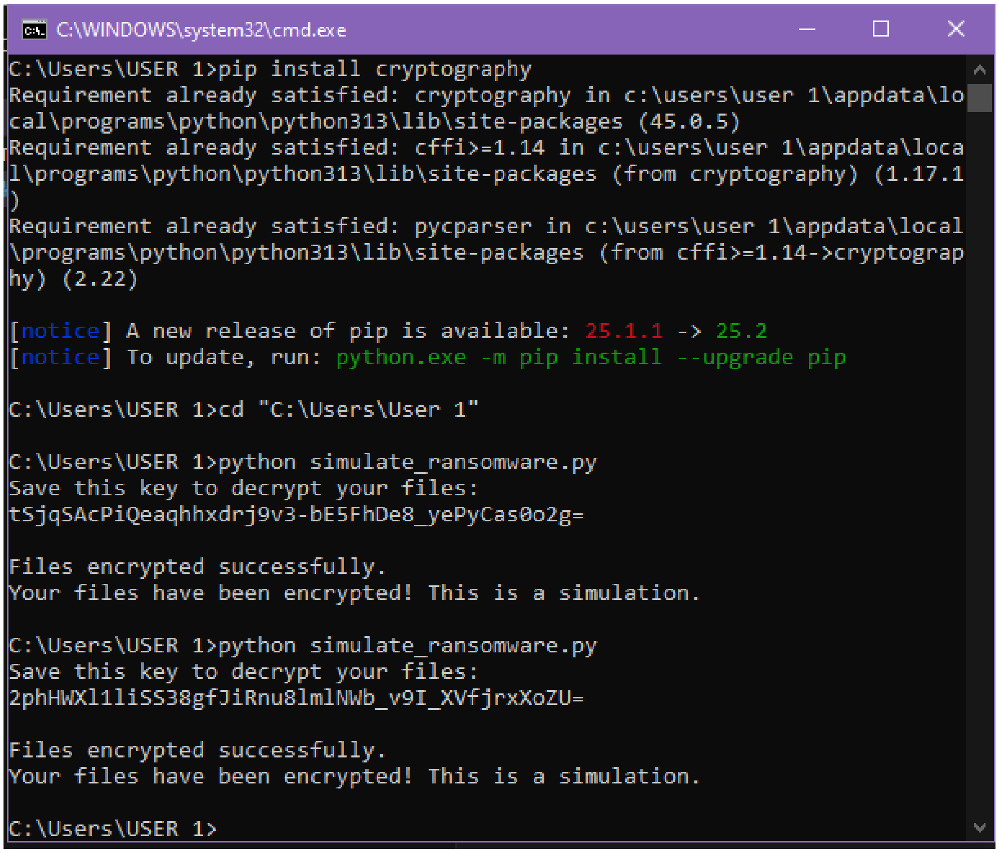
Incident Owner: Ammarah Taj – Cybersecurity Intern

Impact Scope: Only targeted folder/files in the simulation

Behavior: Encrypts files using symmetric encryption (Fernet, which is AES-128 in CBC mode with HMAC for authentication) and replaces originals with `.locked` versions.

Summary

A controlled ransomware simulation was conducted to evaluate detection, containment, eradication, and recovery procedures. The simulation used a Python script leveraging the Fernet encryption library to encrypt dummy `.txt` files. A custom decryption script was later executed with the correct key to restore the files.



```
C:\Users\USER 1>pip install cryptography
Requirement already satisfied: cryptography in c:\users\user 1\appdata\lo
cal\programs\python\python313\lib\site-packages (45.0.5)
Requirement already satisfied: cffi>=1.14 in c:\users\user 1\appdata\loca
l\programs\python\python313\lib\site-packages (from cryptography) (1.17.1
)
Requirement already satisfied: pycparser in c:\users\user 1\appdata\local
\programs\python\python313\lib\site-packages (from cffi>=1.14->cryptograp
hy) (2.22)

[notice] A new release of pip is available: 25.1.1 -> 25.2
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\USER 1>cd "C:\Users\User 1"

C:\Users\USER 1>python simulate_ransomware.py
Save this key to decrypt your files:
tSjqSAcPiQeaqhhxdrj9v3-bE5FhDe8_yePyCas0o2g=

Files encrypted successfully.
Your files have been encrypted! This is a simulation.

C:\Users\USER 1>python simulate_ransomware.py
Save this key to decrypt your files:
2phHWXl1liSS38gfJiRnu8lmlNWb_v9I_XVfjrxXoZU=

Files encrypted successfully.
Your files have been encrypted! This is a simulation.

C:\Users\USER 1>
```

Impact Assessment

- **Systems Affected:** Test Windows 10 workstation only
- **Data Affected:** Dummy `.txt` files in `testfiles` directory
- **Operational Impact:** None — simulation was conducted in a safe, isolated environment

Detection

Planned simulation. Encrypted `.locked` files appeared in place of original `.txt` files.

Containment

Not applicable — simulation was isolated from production network.

Eradication

Simulation scripts were removed after encryption and decryption phases. No persistent ransomware code remained.

Recovery - Decryption Proof

The following steps were taken to recover encrypted data:

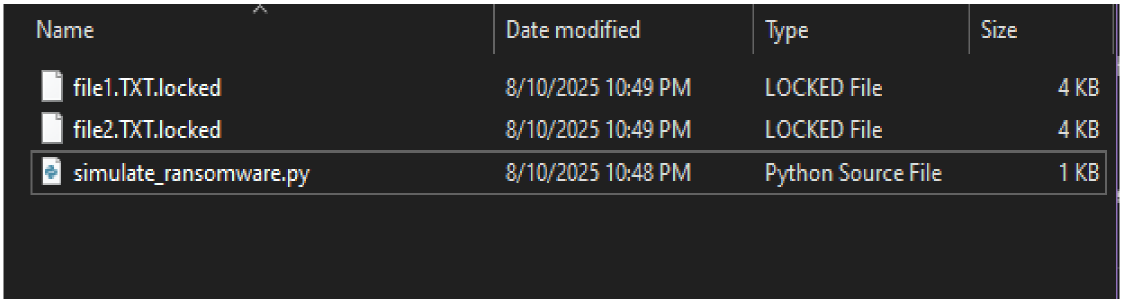
- Ran **simulate_decrypt.py** from the same directory:

```
cd "C:\Users\USER 1\testfiles"
python simulate_decrypt.py
```

- Entered the **saved encryption key** from the simulation:

```
IkgiLcCSiciOXzj3mx6GFhzn_mFbfPgEXZXY6ZA3tzU=
```

- Verified that `.locked` files were replaced by the original `.txt` files with intact content.



Name	Date modified	Type	Size
file1.TXT.locked	8/10/2025 10:49 PM	LOCKED File	4 KB
file2.TXT.locked	8/10/2025 10:49 PM	LOCKED File	4 KB
simulate_ransomware.py	8/10/2025 10:48 PM	Python Source File	1 KB

Verification

- File content matched pre-encryption state
- No corrupted or missing files detected

Incident Response Plan (IRP) – Ransomware

This plan follows **NIST SP 800-61** guidelines for cybersecurity incident handling.

1. Preparation

- Maintain offline backups and test them regularly
- Train all users on phishing and suspicious link avoidance
- Apply timely system patches and updates
- Maintain a ready Incident Response Team with defined roles

2. Identification

- Detect abnormal file changes (e.g., `.locked` or unknown extensions)
- Monitor CPU spikes, network anomalies, and ransom note creation
- Confirm infection via forensic tools or hash comparison

3. Containment

- Disconnect infected devices from the network immediately
- Disable SMB file sharing to prevent lateral spread
- Block malicious IPs/domains identified during threat intel analysis

4. Eradication

- Remove encryption scripts, binaries, and registry persistence entries
- Apply patches for vulnerabilities exploited
- Update endpoint protection signatures

5. Recovery

- Restore clean backups
- Run integrity checks and file hash verification
- Monitor endpoints for at least 72 hours for recurrence