Final Project in NT230 course– Malware's Modus Operandi

Worm Malware: Simulating WannaCry propagation via SMB

*Members: Ngô Hồng Phúc (22521124), Nguyễn Việt Hoàng (22520471),
Nguyễn Tài Hiếu (22520442), Trần Hữu Hiếu (22520444)*
Group ID: G04, Project ID: S04

Introduction

WannaCry was a ransomware attack that affected over 300,000 computers across more than 150 countries by exploiting the EternalBlue vulnerability. This study aims to simulate the propagation and impact mechanisms of the WannaCry ransomware to provide a clear and visual understanding of its destructive capabilities and associated risks. Based on this simulation, the research proposes preventive measures and mitigation strategies to reduce the impact of future attacks involving worm-based ransomware.

Workflow

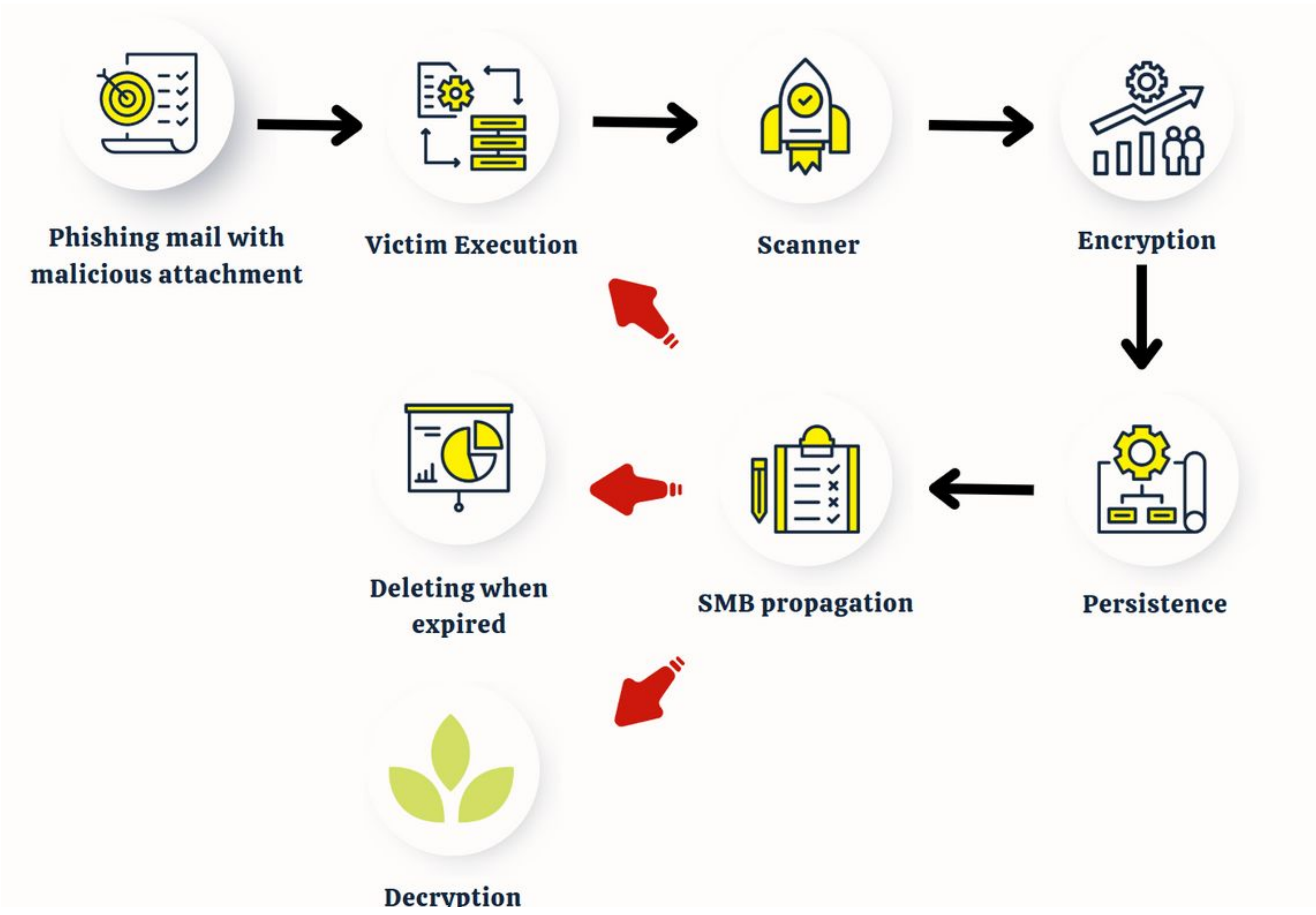


Fig.1 *How WannaCry.exe malware works*

Methodology

Step 1: Send a phishing email with a malicious attachment to the victim.

Step 2: Find target files.

Step 3: Encrypt files with AES and rename them with a new extension.

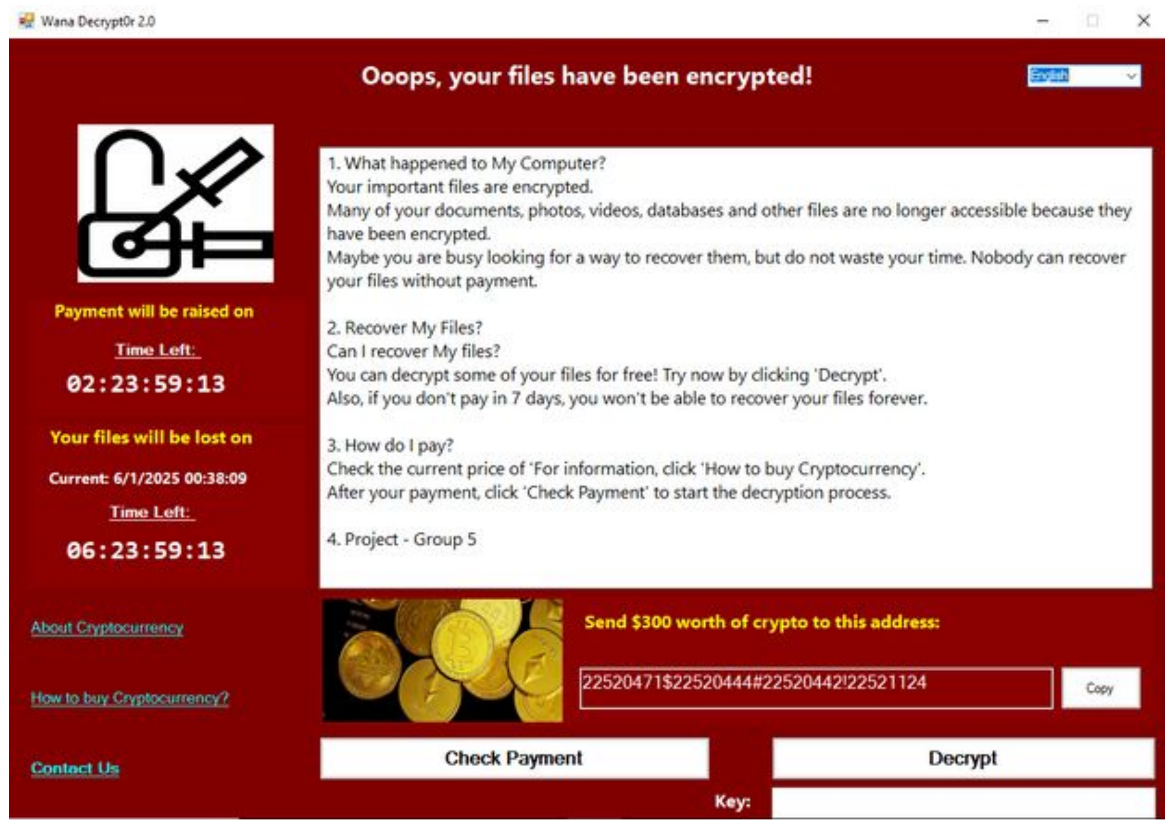
Step 4: Add itself to Windows startup (registry).

Step 5: Spread via SMB (port 445) to shared folders.

Step 6: Save infection time; delete files after expiry.

Step 7: Decrypt files if correct key provided.

Experiments - Attacks on Victim



Ooops, your files have been encrypted!

Payment will be raised on
Time Left:
02:23:59:13

Your files will be lost on
Current: 6/1/2025 00:38:09
Time Left:
06:23:59:13

1. What happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted.
Maybe you are busy looking for a way to recover them, but do not waste your time. Nobody can recover your files without payment.

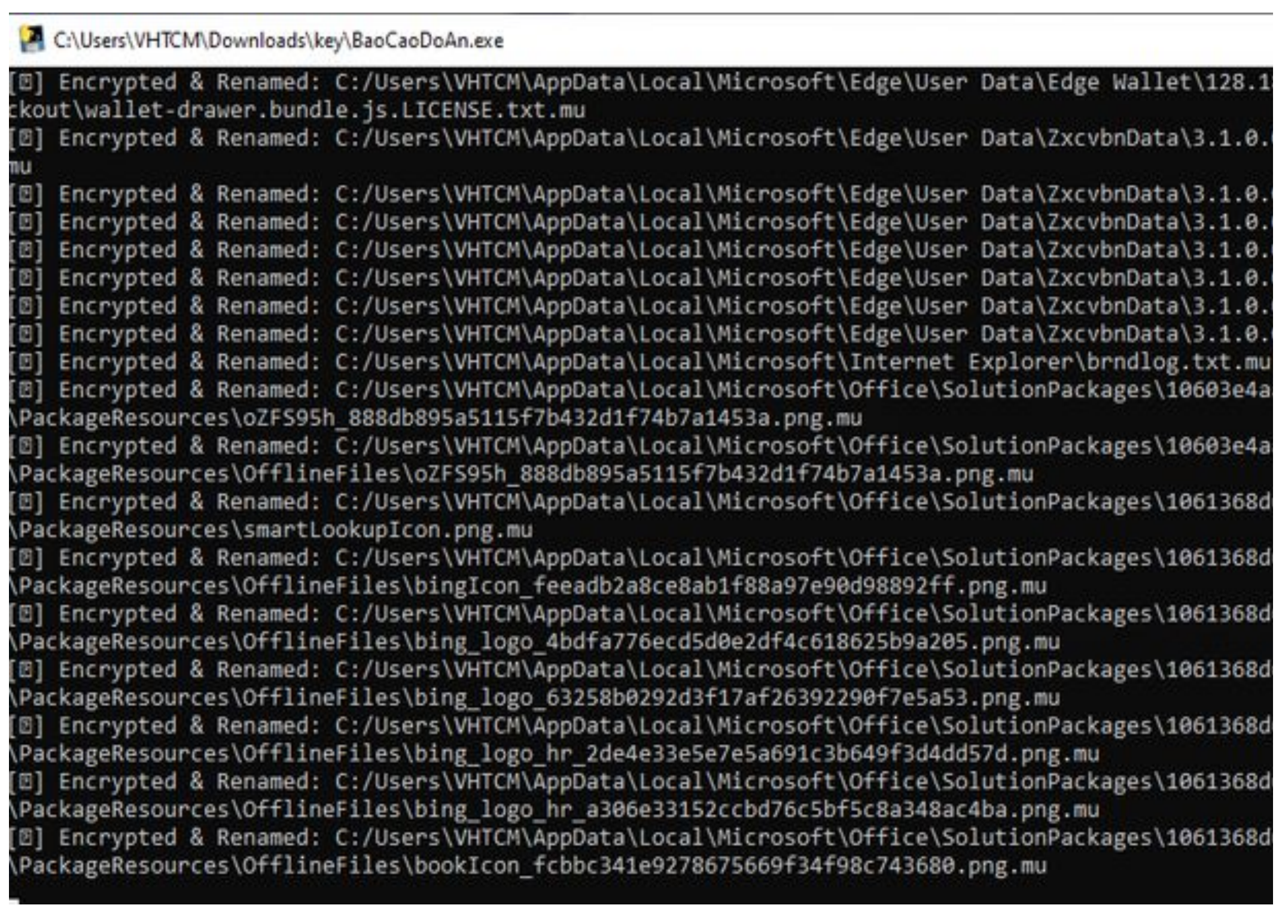
2. Recover My Files?
Can I recover My files?
You can decrypt some of your files for free! Try now by clicking 'Decrypt'.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

3. How do I pay?
Check the current price of 'For information, click 'How to buy Cryptocurrency'.
After your payment, click 'Check Payment' to start the decryption process.

4. Project - Group 5

Send $300 worth of crypto to this address:
22520471$22520444#22520442!22521124

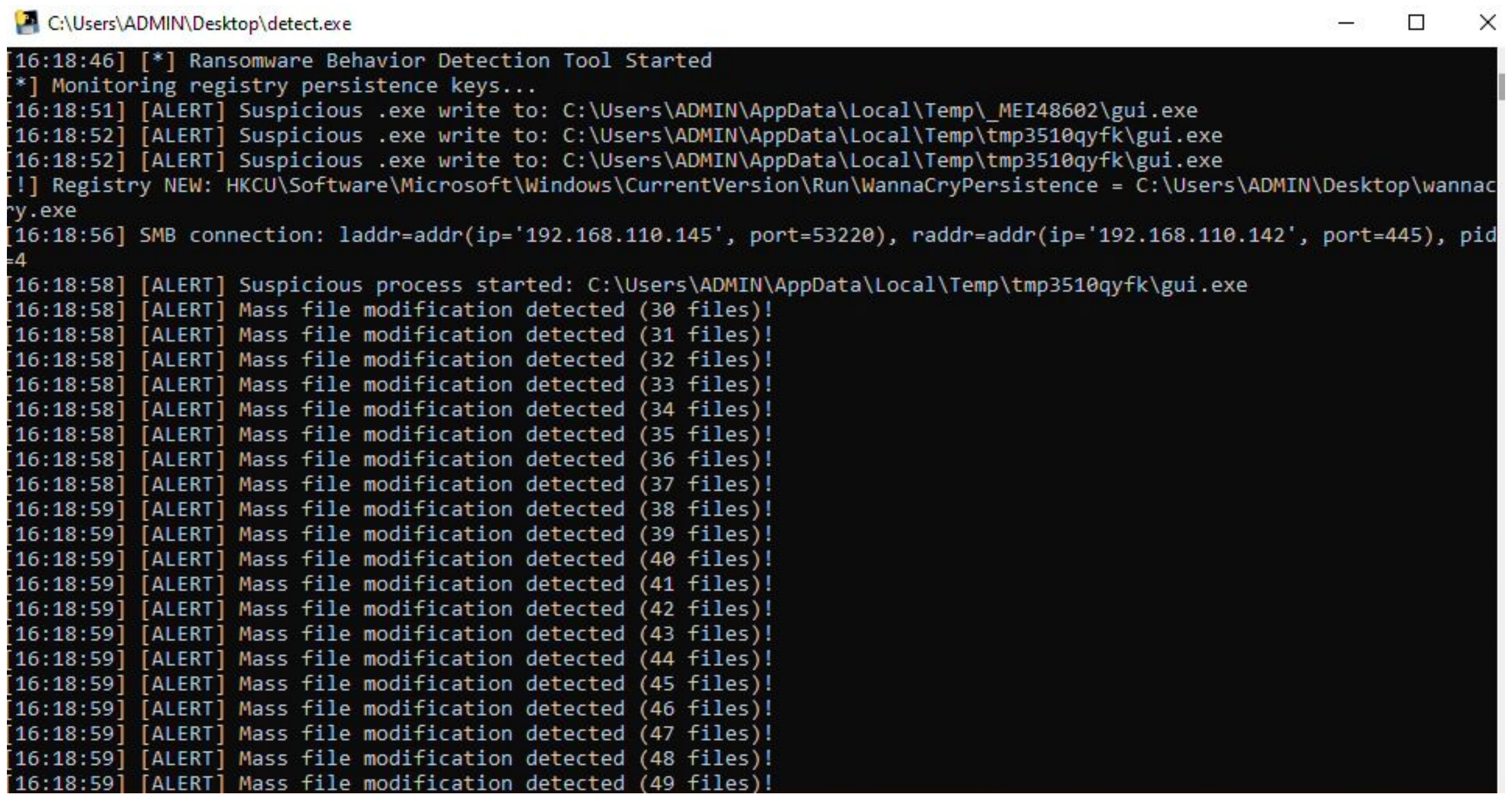
Fig.2 *WannaCry GUI*



```
C:\Users\VHTCM\Downloads\key\BaoCaoDoAn.exe
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Edge\User Data\Edge Wallet\128.1
ckout\wallet-drawer.bundle.js.LICENSE.txt.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Edge\User Data\ZxcvbnData\3.1.0.
mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Edge\User Data\ZxcvbnData\3.1.0.
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Edge\User Data\ZxcvbnData\3.1.0.
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Edge\User Data\ZxcvbnData\3.1.0.
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Edge\User Data\ZxcvbnData\3.1.0.
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Edge\User Data\ZxcvbnData\3.1.0.
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Edge\User Data\ZxcvbnData\3.1.0.
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Office\SolutionPackages\10603e4a
\PackageResources\oZFS95h_888db895a5115f7b432d1f74b7a1453a.png.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Office\SolutionPackages\10603e4a
\PackageResources\OfflineFiles\oZFS95h_888db895a5115f7b432d1f74b7a1453a.png.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Office\SolutionPackages\1061368d
\PackageResources\smartLookupIcon.png.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Office\SolutionPackages\1061368d
\PackageResources\OfflineFiles\bingIcon_feeadb2a8ce8ab1f88a97e90d98892ff.png.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Office\SolutionPackages\1061368d
\PackageResources\OfflineFiles\bing_logo_4bdfa776ecd5d0e2df4c618625b9a205.png.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Office\SolutionPackages\1061368d
\PackageResources\OfflineFiles\bing_logo_63258b0292d3f17af26392290f7e5a53.png.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Office\SolutionPackages\1061368d
\PackageResources\OfflineFiles\bing_logo_hr_2de4e33e5e7e5a691c3b649f3d4dd57d.png.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Office\SolutionPackages\1061368d
\PackageResources\OfflineFiles\bing_logo_hr_a306e33152ccbd76c5bf5c8a348ac4ba.png.mu
[⊠] Encrypted & Renamed: C:/Users\VHTCM\AppData\Local\Microsoft\Office\SolutionPackages\1061368d
\PackageResources\OfflineFiles\bookIcon_fcbbc341e9278675669f34f98c743680.png.mu
```

Fig.3 *Encrypt files*

Detection Tool



```
C:\Users\ADMIN\Desktop\detect.exe
[16:18:46] [*] Ransomware Behavior Detection Tool Started
[*] Monitoring registry persistence keys...
[16:18:51] [ALERT] Suspicious .exe write to: C:\Users\ADMIN\AppData\Local\Temp\_MEI48602\gui.exe
[16:18:52] [ALERT] Suspicious .exe write to: C:\Users\ADMIN\AppData\Local\Temp\tmp3510qyfk\gui.exe
[16:18:52] [ALERT] Suspicious .exe write to: C:\Users\ADMIN\AppData\Local\Temp\tmp3510qyfk\gui.exe
[!] Registry NEW: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WannaCryPersistence = C:\Users\ADMIN\Desktop\wannac
ry.exe
[16:18:56] SMB connection: laddr=addr(ip='192.168.110.145', port=53220), raddr=addr(ip='192.168.110.142', port=445), pid
=4
[16:18:58] [ALERT] Suspicious process started: C:\Users\ADMIN\AppData\Local\Temp\tmp3510qyfk\gui.exe
[16:18:58] [ALERT] Mass file modification detected (30 files)!
[16:18:58] [ALERT] Mass file modification detected (31 files)!
[16:18:58] [ALERT] Mass file modification detected (32 files)!
[16:18:58] [ALERT] Mass file modification detected (33 files)!
[16:18:58] [ALERT] Mass file modification detected (34 files)!
[16:18:58] [ALERT] Mass file modification detected (35 files)!
[16:18:58] [ALERT] Mass file modification detected (36 files)!
[16:18:58] [ALERT] Mass file modification detected (37 files)!
[16:18:59] [ALERT] Mass file modification detected (38 files)!
[16:18:59] [ALERT] Mass file modification detected (39 files)!
[16:18:59] [ALERT] Mass file modification detected (40 files)!
[16:18:59] [ALERT] Mass file modification detected (41 files)!
[16:18:59] [ALERT] Mass file modification detected (42 files)!
[16:18:59] [ALERT] Mass file modification detected (43 files)!
[16:18:59] [ALERT] Mass file modification detected (44 files)!
[16:18:59] [ALERT] Mass file modification detected (45 files)!
[16:18:59] [ALERT] Mass file modification detected (46 files)!
[16:18:59] [ALERT] Mass file modification detected (47 files)!
[16:18:59] [ALERT] Mass file modification detected (48 files)!
[16:18:59] [ALERT] Mass file modification detected (49 files)!
```

Fig.4 *Detect ransomware techniques*

- Monitor for mass file modifications (potential ransomware activity).
- Detect suspicious .exe file writes and executions.
- Monitor abnormal SMB (port 445) connections.
- Watch for any registry changes in common persistence keys under HKCU and HKLM (such as Run, RunOnce, Services, etc.).
- Alerts are printed to the console. Modified files are logged to suspicious_modified_files.log.

A project at NT230 course– Semester 2 – School Year of 2024-2025, UIT-VNUHCM– Copyright: UIT InSecLab