TÀI LIỆU HƯỚNG DẪN RÀ SOÁT MÃ ĐỘC GIÁN ĐIỆP

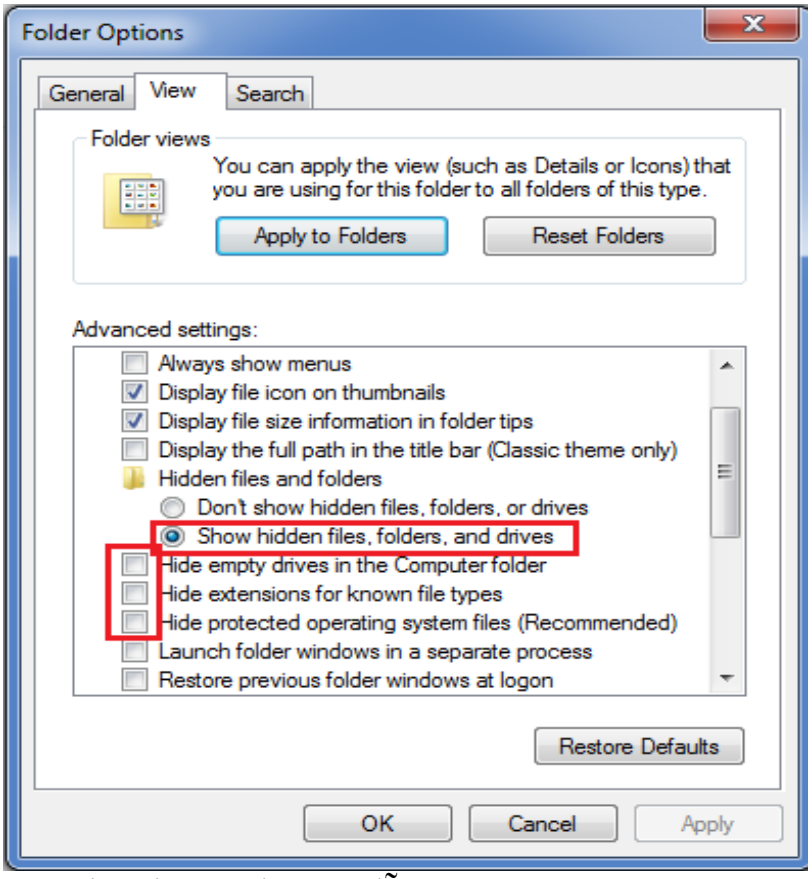
(Kèm theo Công văn số……/UBND-TH ngày……/…/2023)

1. Phương pháp phát hiện biến thể mã độc gián điệp mới trên máy tính

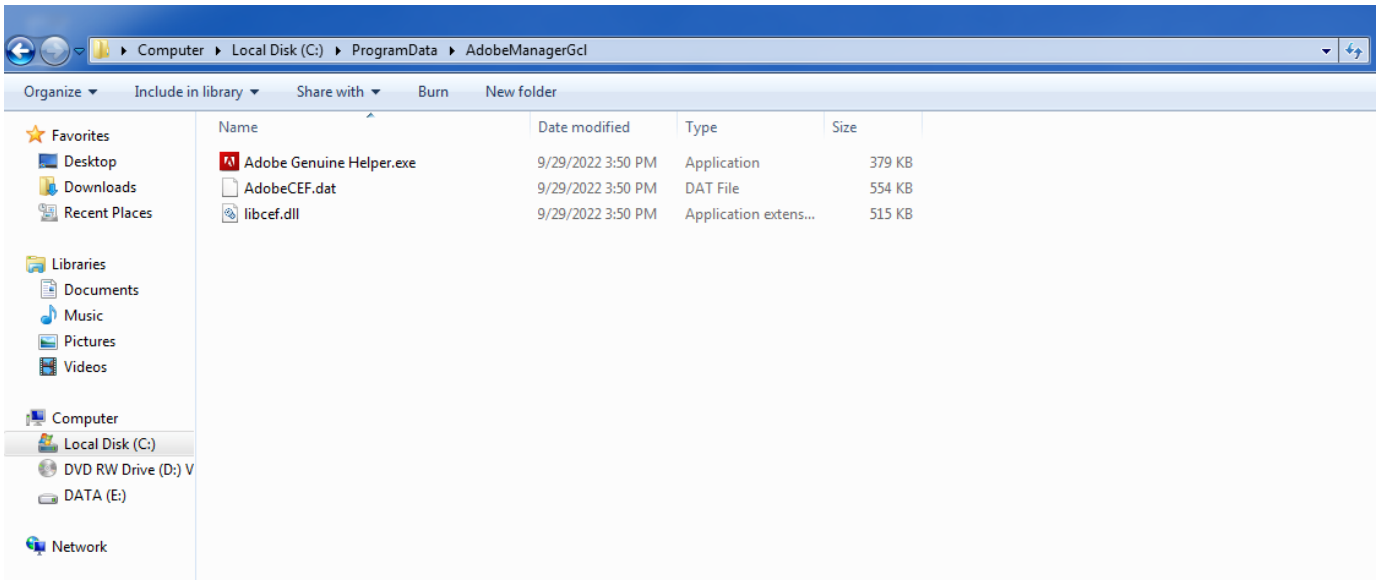
Để phát hiện biến thể mã độc gián điệp mới trên máy tính sử dụng các cách sau:

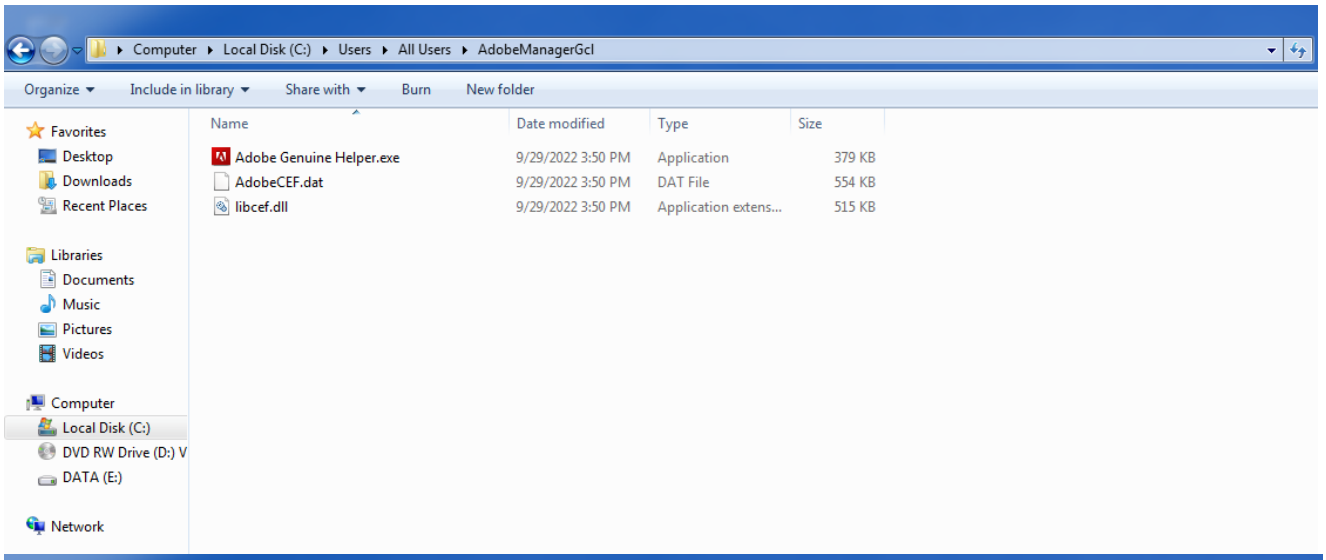
(1) Tìm kiếm trực tiếp các tệp tin của mã độc gián điệp trên máy tính

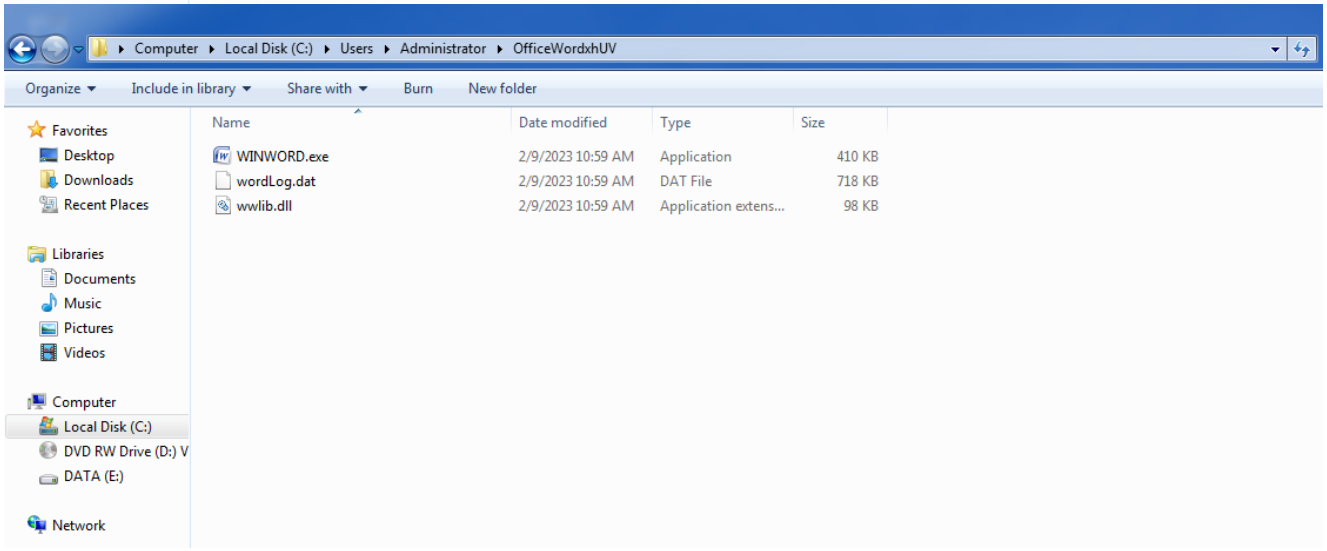
Cấu hình cho phép hiển thị tệp tin ẩn và tệp tin hệ thống để tìm kiếm tệp tin mã độc như hình sau:



Kiểm tra trên máy tính tại các đường dẫn: **"*C:\ProgramData\ AdobeManagerGcl ****"; **"*C:\Users\All Users\ AdobeManagerGcl ****"** và **"C:\Users\%username%\OfficeWordxhUV",** biến thể mã độc mới bao gồm các tệp tin sau:





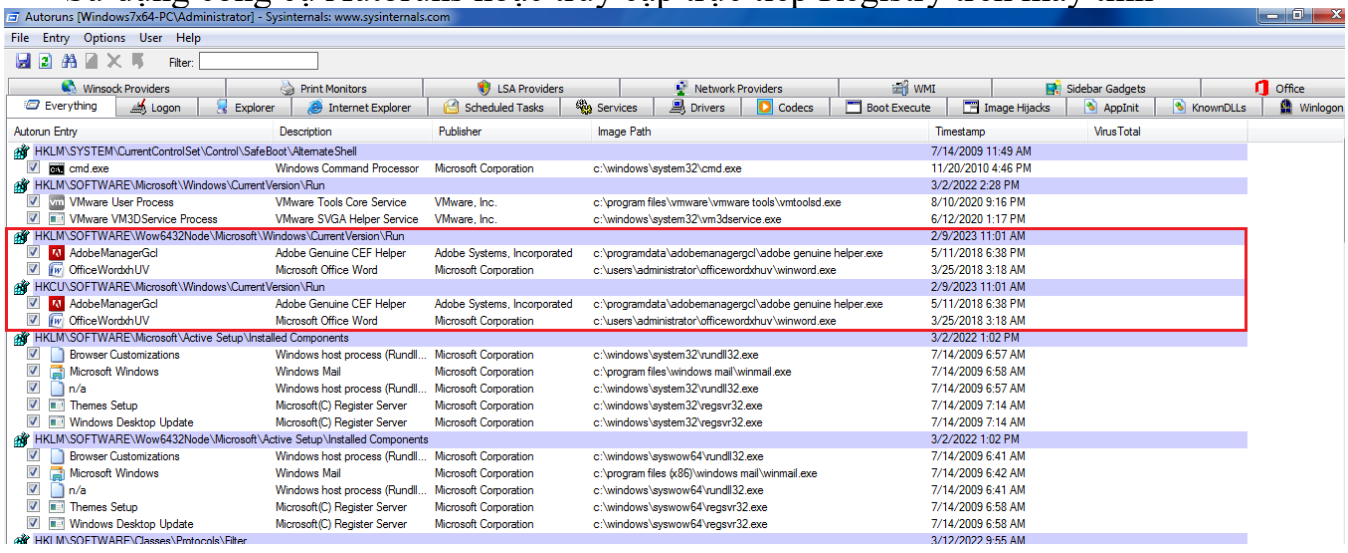


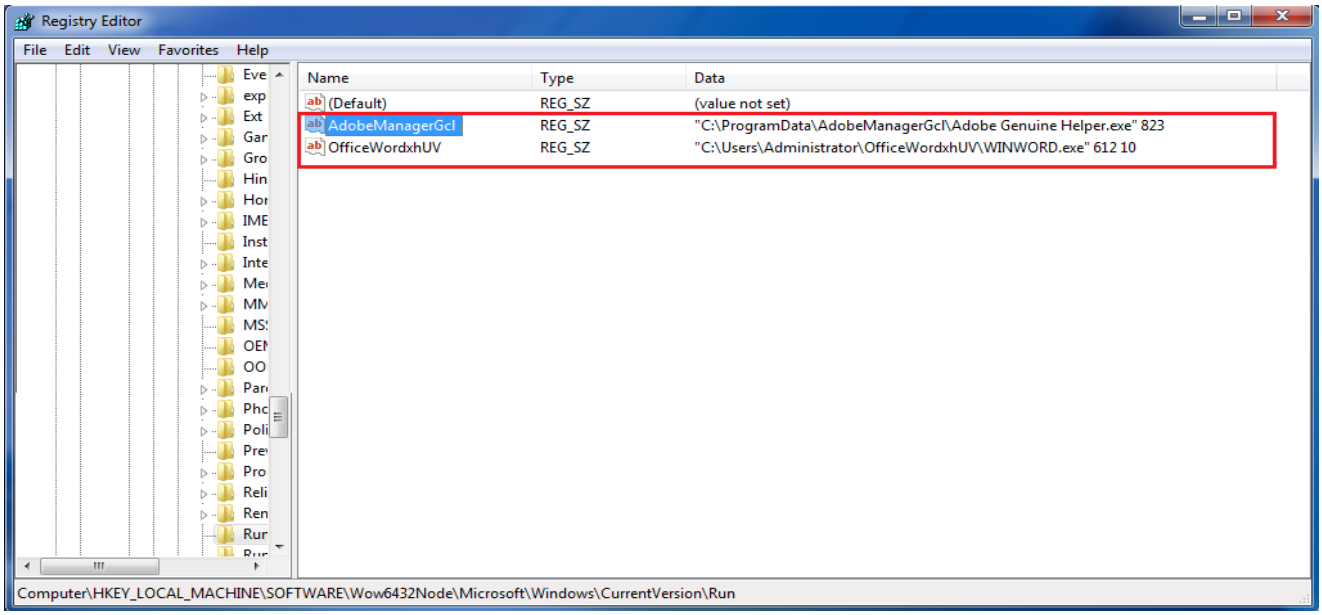
Các tệp tin của mã độc

Lưu ý: Phân biệt tệp tin của mã độc với tệp tin ứng dụng hợp pháp dựa vào đường dẫn và các tệp tin đính kèm. Tệp tin ứng dụng thường trong thư mục **"*C:\Program Files*"** hoặc **"*C:\Program Files (x86)*"**. Trong khi đó, mã độc nhiễm vào máy tính thường ghi các tệp tin tại các thư mục ẩn như hình trên.

(2) Kiểm tra các tiến trình khởi động cùng máy tính

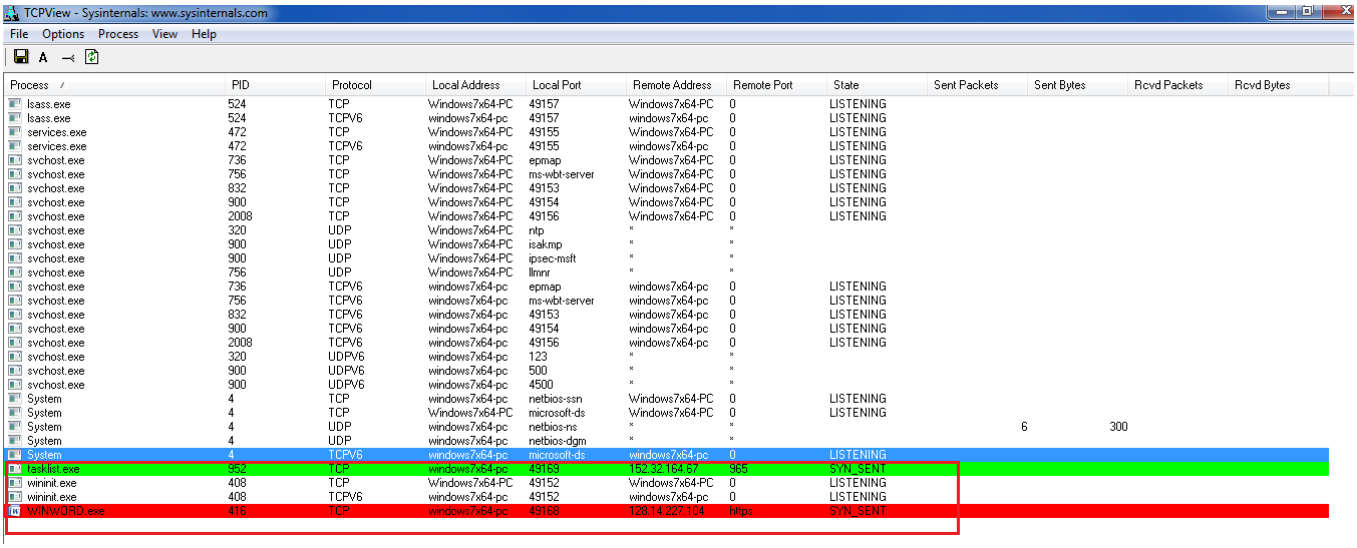
Sử dụng công cụ Autoruns hoặc truy cập trực tiếp Registry trên máy tính





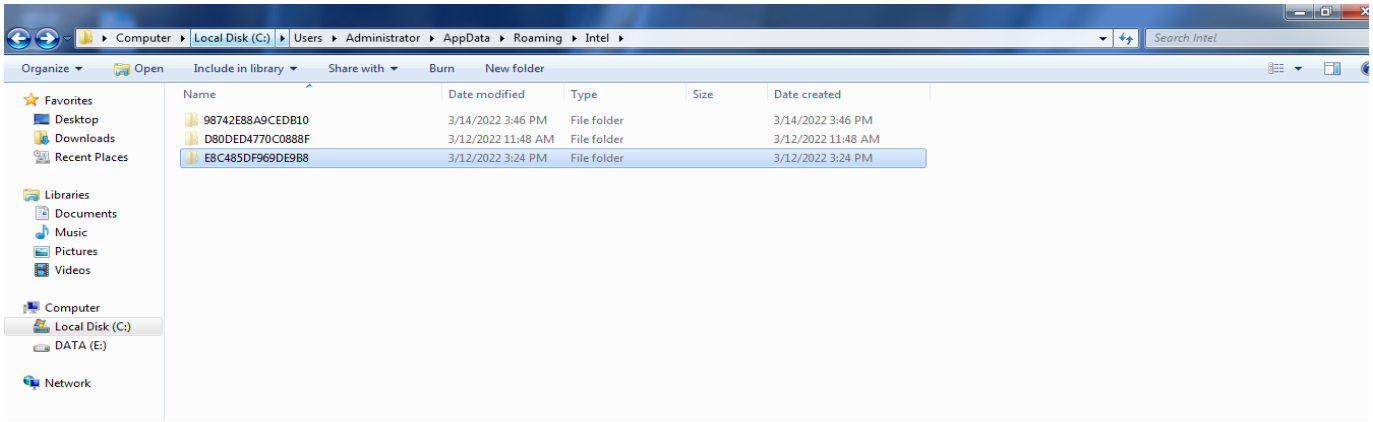
*Mã độc có các bản ghi khởi động cùng máy tính là: "**AdobeManagerGcl**" và "**OfficeWordxhUV**"*

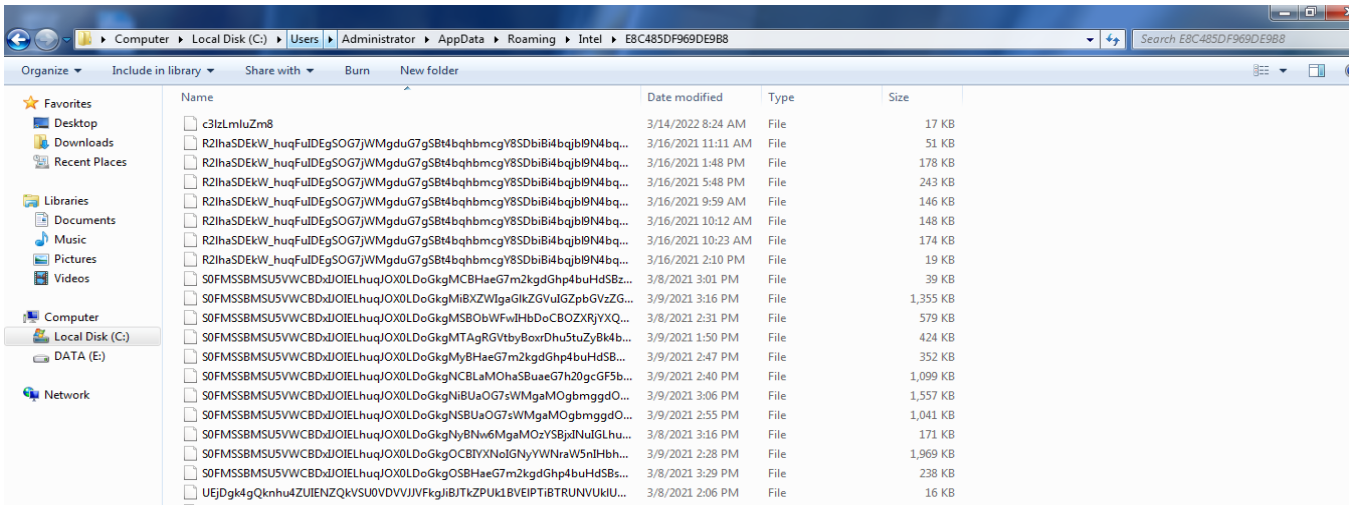
Quan sát kết nối mạng của mã độc, sử dụng công cụ TCPView



*Hình ảnh ghi nhận hành vi của biến thể mã độc gián điệp mới thực hiện gửi truy vấn ra máy chủ điều khiển của hacker bên ngoài (C&C Server) tại các địa chỉ IP: **152.32.164.67** và **128.14.227.104 (Đài Loan)***

Chú ý: Máy tính kết nối Internet nhiễm mã độc gián điệp, dữ liệu thu thập được lưu trữ tại đường dẫn ẩn sau: ***C:\Users\%username%\AppData\Roaming\Intel***. Sau đó, mã độc thực hiện gửi dữ liệu thu thập ra máy chủ điều khiển bên ngoài





Thư mục chứa các tệp tin mã hóa mã độc thu thập được gửi ra bên ngoài

2. Phương pháp phát hiện, loại bỏ mã độc trên thiết bị lưu trữ ngoài

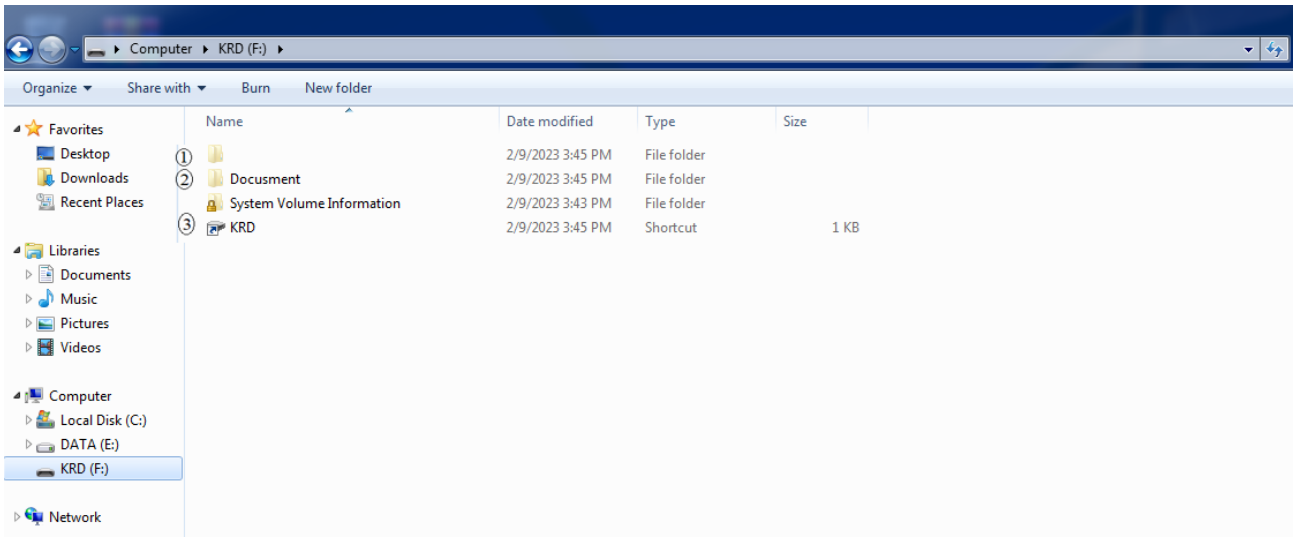
Để phát hiện mã độc trên thiết bị lưu trữ ngoài, thực hiện theo các bước sau:

- Bật cấu hình hiển thị tệp tin ẩn và tệp tin hệ thống trên máy tính.

- Trên cửa sổ explorer kích chuột vào ổ đĩa lưu trữ ngoài ở dọc thanh menu bên trái, không kích đúp trực tiếp vào thiết bị lưu trữ ngoài.

Chỉ sử dụng cây thư mục (bên trái) để xem tệp tin, thư mục

Nếu thiết bị lưu trữ ngoài bị nhiễm mã độc gián điệp, thì trong thiết bị lưu trữ ngoài có các tệp tin, thư mục sau:



Trong đó:

(1) Thư mục **không có tên** là thư mục chứa dữ liệu thật sự của người dùng trên thiết bị lưu trữ ngoài (*Mã độc sẽ tự động mở thư mục này để đánh lừa người dùng nếu người dùng kích hoạt tệp tin shortcut*).

(2) Thư mục tên **Docusment** là thư mục chứa các tệp tin của mã độc, dữ liệu mã hóa do mã độc sao chép từ máy tính vào thiết bị lưu trữ ngoài và thông tin card mạng wifi trên máy tính nhiễm mã độc.

(3) Tệp tin **shortcut** sử dụng để đánh lừa người dùng kích vào, sẽ kích hoạt mã độc lây nhiễm vào máy tính khi kết nối thiết bị lưu trữ bị nhiễm mã độc.

Cách xử lý mã độc: Tiến hành định dạng (format) lại thiết bị lưu trữ ngoài.