1. **Giới thiệu về Virus và Sâu (Worm): <Nhờ đồng chí>**
2. **Nói bla bla bla gì đó**

* Tóm lược, có nhiều loại virus cùng nhiều mục đích khác nhau khi được gây dựng. Ở phần này một virus mã hóa tập tin người bị hại đòi tiền chuộc được nhóm hiện thực.

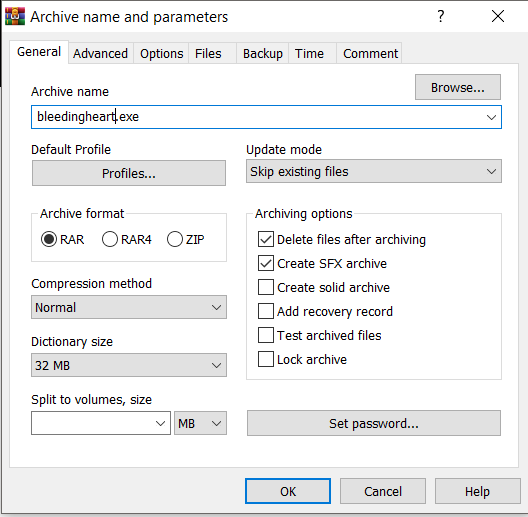
1. **Quá trình lên ý tưởng**

* Đặt dưới mục đích học tập, virus được sử dụng bằng cách chèn thủ công vào các tập tin có khả năng được sử dụng cao: Ảnh, PDF, Word, …. Các dạng tập tin như vậy sẽ mang đến sự bất cẩn cho người bị hại.
* Khi xâm nhậm được vào một người bị hại, virus tạo kết nối đến server để lấy key mã hóa và sử dụng nó cho việc mã hóa các tập tin của người dùng, tất cả các yêu cầu chạy đều sẽ được thực hiện ẩn, chỉ có thể tắt bằng “*kill process”*  hoặc *“task manager”*. Với những người dùng ít khả năng với bảo mật máy tính, họ sẽ không nhận ra máy tính đang bị tấn công cho đến khi virus đã tấn công xong.

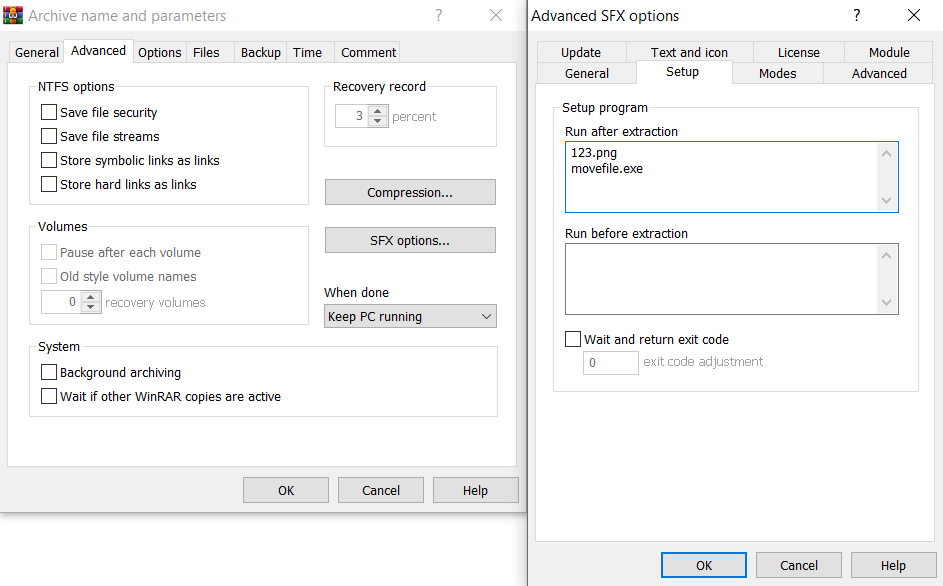
1. **Quá trình hiện thực:**
2. **Yêu cầu về vấn đề chèn tập tin.**

* Để chèn tập tin vào file ảnh, word, pdf,.. Ta có thể sử dụng SFX của winrar, một phần mềm đã được microsoft kiểm chứng.

**Bước 1:** Chọn định dạng SFX và các tập tin đóng gói.



**Bước 2:** Cấu hình định quá trình mở tập tin SFX

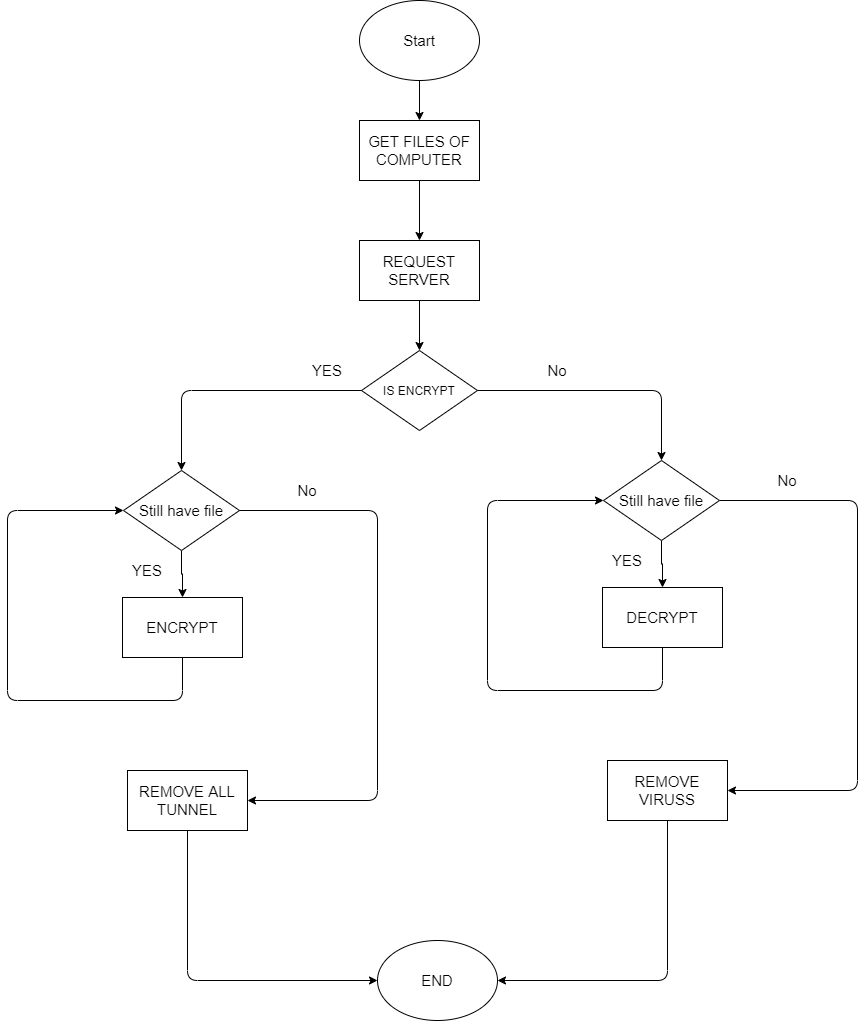


**Bước 3:** Kết quả đóng gói.



Tập tin mylove thứ hai đang giả mạo tập tin ảnh mylove thứ 3.

1. **Yêu cầu về quá trình mã hóa tập tin.**

* Mã hóa tập tin phải đảm bảo làm ẩn dạng dưới máy tính của người bị tấn công. Các tập tin được mã hóa lần lượt nhằm tránh tốn tài nguyên gây nghi ngờ cho người bị tấn công, kết quả sẽ được thông báo lên màn hình.
* Sơ đồ hoạt động của virus như sau:

1. **Yêu cầu về hệ thống**

* Kết nối giữa client-server là sử dụng request HTTP.
* Các khóa được tạo ngẫu nhiên, dạng bytes.

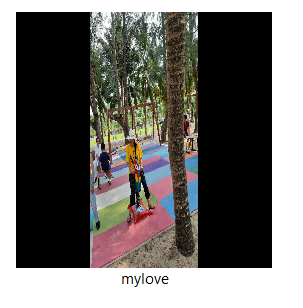
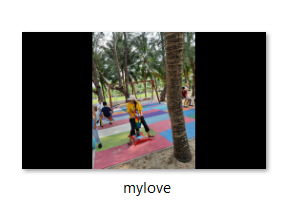
1. **Yêu cầu sinh tồn cho virus.**

* Sau khi tấn công người bị hại, virus tạo một bản sao chép đặt tại một thư mục ẩn trong hệ thống người dùng, đồng thời chuyển sang chế độ khởi động cùng windows. Do đó mỗi khi người dùng khởi động virus cũng sẽ khởi động theo, và tồn tại cùng người dùng trong mỗi phiên làm việc. Sau cùng người dùng không thể xóa tập tin đang hoạt động (trường hợp người dùng tìm thấy tập tin) nếu không có kĩ năng về kill process.

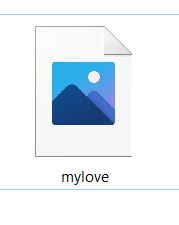
1. **Kết quả hiện thực**
2. **Kết quả phân tích.**

* Về cơ bản, virus đã chạy được hoàn thiện quá trình: Kết nối server -> Xin hành động -> Hành động -> Thông báo -> Xóa bỏ.
* Các di chứng về quá trình tấn công bị xóa bỏ hoàn thiện. không tạo tồn tại dấu vết.

Trước Sau

1. **Kết quả hoạt động.**

* Thời gian kết nối của virus đến server và nhận được sự phản hồi là tương đối nhanh, không chiếm dụng quá nhiều tài nguyên của máy bị tấn công dẫn đến khó phát hiện.
* Các tập tin bị tấn công đạt yêu cầu cho vấn đề phá giải trong tương lai, tất cả chỉ số đều được lưu trữ ổn định trong tập tin.
* Một ổ cứng có giá trị 1TB, có thể bị mã hóa hoàn toàn sau 1 giờ đồng hồ, tức là với mỗi phiên làm việc của người bị tấn công, hoàn toàn có thể mất sạch dữ liệu.
* 

1. **Kết quả sinh tồn của virus.**

* Virus sinh tồn tốt trong máy tính người dùng, các request sẽ được virus gửi mỗi khi người bị hại khởi động hệ điều hành mục đích xin hành động cần thực hiện từ phía server. Trường hợp người bị hại sửa mã nguồn của virus cũng yêu cầu nhận được request từ phía server.

1. **Vấn đề và cách khắc phục.**

* **Virus chỉ hoạt động trên windows:** Hiện nay các hệ điều hành linux, macOS đều có sẵn trình biên dịch của python, virus có thể chuyển dạng gửi cả tập tin .exe (cho windows) và các tập tin .py (cho linux và macOS). Tuy nhiên vấn đề tường minh đoạn code của virus sẽ làm mất tính tấn công.
* **Lộ địa chỉ của server cấp khóa**: Server cấp khóa được để lộ trong hệ thống người dùng, trong tương lai server sẽ bị tạo một mã hash, và từ chính server đó sẽ được kết nối tới server khác. Server thứ hai mới là server cấp khóa thực sự.