**Quy Trình Phân Tích Malware Bằng Procmon, Fakenet, và Regshot**

**Mô Tả Tổng Quan**

Quy trình phân tích malware dùng ba công cụ chính: **Procmon**, **Fakenet**, và **Regshot**. Đây là quy trình cơ bản để xác định hành vi của malware trong môi trường an toàn (sandbox).

**Chi Tiết Các Bước**

**1. Start Procmon, then pause and clear**

* **Giải thích**:
  + Procmon (Process Monitor) giúp giám sát hoạt động hệ thống như tệp tin, registry, và tiến trình.
  + Sau khi khởi động, tạm dừng để xóa lịch sử log cũ, đảm bảo kết quả phân tích không bị nhầm lẫn.
* **Lưu ý**: Tạo môi trường an toàn (sandbox) trước khi bắt đầu.
* **Ví dụ**: Mở Procmon, nhấn "Ctrl+X" để tạm dừng và "Ctrl+E" để xóa log hiện tại.

**2. Start Fakenet**

* **Giải thích**:
  + Fakenet giả lập một môi trường mạng để giám sát các kết nối mạng do malware thực hiện.
  + Dùng để phát hiện hành vi giao tiếp với server điều khiển (C2).
* **Lưu ý**: Đảm bảo Fakenet đã được cấu hình chính xác.
* **Ví dụ**: Chạy Fakenet trong terminal và quan sát các kết nối HTTP, DNS, v.v.

**3. Start Regshot, then take 1st shot**

* **Giải thích**:
  + Regshot tạo snapshot (bản sao) của registry để lưu trữ trạng thái hệ thống ban đầu.
  + Giúp so sánh thay đổi trong registry sau khi malware chạy.
* **Lưu ý**: Nên lưu snapshot vào một thư mục an toàn.
* **Ví dụ**: Mở Regshot, nhập thư mục lưu kết quả và nhấn "1st Shot".

**4. Once 1st shot completes, Resume Procmon**

* **Giải thích**:
  + Sau khi tạo snapshot đầu tiên, tiếp tục giám sát hoạt động hệ thống với Procmon.
* **Ví dụ**: Nhấn "Ctrl+X" để tiếp tục ghi log trên Procmon.

**5. Run Malware for about 1–3 mins and study Fakenet output**

* **Giải thích**:
  + Chạy mẫu malware trong môi trường kiểm tra (sandbox).
  + Quan sát các hành vi mạng do malware thực hiện.
* **Lưu ý**: Cần dò tìm các domain, IP, hoặc giao thức mạng bất thường.
* **Ví dụ**: Malware cố gắng kết nối tới domain: malicious-example.com.

**6. After about 3 mins, pause Procmon**

* **Giải thích**:
  + Tạm dừng Procmon sau khi malware đã chạy đủ thời gian, đảm bảo ghi nhận đủ log.
* **Ví dụ**: Nhấn "Ctrl+X" để dừng ghi log.

**7. Use Regshot to take 2nd shot**

* **Giải thích**:
  + Tạo snapshot thứ hai sau khi chạy malware, sẽ so sánh với snapshot đầu tiên.
* **Lưu ý**: Để cần thận lưu snapshot vào đúng thư mục.
* **Ví dụ**: Trong Regshot, nhấn "2nd Shot" và lưu kết quả.

**8. Once 2nd shot completes, click Compare -> Compare and show output**

* **Giải thích**:
  + So sánh hai snapshot để tìm ra thay đổi trong registry do malware gây ra.
* **Lưu ý**: Kiểm tra kỹ lưỡng dữ liệu lớn khi so sánh.
* **Ví dụ**: Trong Regshot, chọn “Compare” và lưu log kết quả ra file.

**9. Study Regshot output**

* **Giải thích**:
  + Phân tích kết quả so sánh để tìm ra thay đổi trong registry, file, hoặc các thiết lập khắc.
  + Xác định các vùng registry quan trọng như:
    - **HKEY\_LOCAL\_MACHINE** (HKLM): Đường dẫn hệ thống.
    - **HKEY\_CURRENT\_USER** (HKCU): Thay đổi cho user hiện tại.
* **Ví dụ**: Malware chỉnh sửa registry để tự khởi động cùng Windows:
  + HKCU\Software\Microsoft\Windows\CurrentVersion\Run để thêm file: malware.exe

**Đánh Giá Kết Quả**

* **Procmon**: Phát hiện hành vi ghi/ghi đọc file và thay đổi các tiến trình.
* **Fakenet**: Quan sát kết nối mạng để phát hiện C2 server.
* **Regshot**: Xác định thay đổi registry do malware gây ra.

**Kết Luận**