**Phân tích chi tiết về quy trình tiếp tục (Work Flow Sequence Continued) và bộ lọc ProcMon (ProcMon Filters)**

**1. Lọc dữ liệu trong ProcMon**

Trong quy trình phân tích malware, sử dụng ProcMon để giám sát các hoạt động hệ thống cụ thể. Các bộ lọc giúp tập trung vào những sự kiện quan trọng liên quan đến hành vi của malware.

**Áp dụng các bộ lọc sau trong ProcMon:**

* **ProcessName:**
  + Thiết lập tên process là tên của malware cần phân tích (ví dụ: malware-name).
* **Operation:**
  + Chỉ quan tâm đến các hoạt động sau:
    - **WriteFile:** Malware ghi dữ liệu vào tệp tin.
    - **SetDispositionInformationFile:** Malware sửa đổi hoặc xóa tệp tin.
    - **RegSetValue:** Malware thay đổi giá trị registry.
    - **ProcessCreate:** Malware tạo tiến trình mới.
    - **TCP/UDP:** Malware thực hiện kết nối mạng qua giao thức TCP hoặc UDP.

A white background with black text

Description automatically generated

**2. Các loại hoạt động trong ProcMon**

ProcMon phân chia các hoạt động thành các danh mục chính như sau:

* **File Operations:**
  + **CreateFile:** Tạo tệp mới hoặc mở tệp hiện có.
  + **ReadFile:** Đọc dữ liệu từ tệp.
  + **WriteFile:** Ghi dữ liệu vào tệp.
  + **SetDispositionInformationFile:** Xóa hoặc thay đổi thuộc tính tệp.
* **Registry Operations:**
  + **RegCreateKey:** Tạo khóa registry mới.
  + **RegQueryValue:** Đọc giá trị từ registry.
  + **RegSetValue:** Ghi giá trị mới vào registry.
  + **RegDeleteKey:** Xóa khóa registry.
* **Process Operations:**
  + **ProcessStart:** Bắt đầu một tiến trình.
  + **ProcessCreate:** Tạo tiến trình mới.
* **Network Operations:**
  + **TCP:** Gửi hoặc nhận dữ liệu qua giao thức TCP.
  + **UDP:** Gửi hoặc nhận dữ liệu qua giao thức UDP.

A screenshot of a computer screen

Description automatically generated

**3. Hình minh họa về bộ lọc ProcMon**

Hình ảnh minh họa quy trình:

* Bảng phân loại các hoạt động ProcMon (File, Registry, Process, Network).
* Giao diện bộ lọc của ProcMon:
  + Hiển thị các sự kiện phù hợp với tiêu chí lọc.
  + Dễ dàng phát hiện các hành vi bất thường của malware.

A screenshot of a computer

Description automatically generated

**4. Ví dụ thực tế**

Giả sử bạn đang phân tích một malware thực hiện hành vi:

* Tạo tiến trình mới tên là malicious.exe.
* Ghi dữ liệu vào tệp C:\temp\malicious.txt.
* Thay đổi giá trị registry tại HKCU\Software\TestKey.
* Kết nối đến địa chỉ IP qua cổng 443 bằng giao thức TCP.

**Cách thực hiện:**

1. Trong ProcMon, đặt **ProcessName** là malware-name.
2. Thêm các bộ lọc **Operation** như: WriteFile, RegSetValue, ProcessCreate, và TCP.
3. Chạy malware và giám sát các sự kiện trong thời gian thực.
4. Xác định các hành vi cụ thể và đối chiếu với thông tin từ Fakenet và Regshot (nếu có).

**5. Lợi ích của việc lọc chính xác**

* Giảm nhiễu từ các sự kiện không liên quan.
* Tập trung vào các hành vi nguy hiểm.
* Tiết kiệm thời gian phân tích.
* Hỗ trợ việc so sánh dữ liệu từ các công cụ khác như Fakenet và Regshot