**1. Registry Persistence (Sử dụng Registry để duy trì hoạt động)**

Hình ảnh đầu tiên minh họa các đường dẫn registry phổ biến trong Windows, thường được sử dụng để thiết lập chương trình chạy tự động khi hệ thống khởi động. Đây là cách mà phần mềm hợp pháp (hoặc mã độc) có thể duy trì hoạt động liên tục trên máy tính.

**Các đường dẫn registry chính:**

* **HKLM (HKEY\_LOCAL\_MACHINE):**
  + \Software\Microsoft\Windows\CurrentVersion\Run:  
    Chạy chương trình cho **tất cả người dùng** khi máy tính khởi động.
  + \Software\Microsoft\Windows\CurrentVersion\RunOnce:  
    Chạy chương trình **một lần duy nhất** trong lần khởi động tiếp theo.
  + \Software\Microsoft\Windows\CurrentVersion\RunServices:  
    Khởi chạy các **dịch vụ nền** khi hệ thống khởi động.
* **HKCU (HKEY\_CURRENT\_USER):**
  + Chỉ áp dụng cho người dùng đang đăng nhập. Ví dụ:
    - \Run và \RunOnce: Chạy chương trình dành riêng cho tài khoản người dùng đó.
* **Explorer Policies trong HKCU:**
  + Các chính sách này kiểm soát giao diện và hành vi của hệ thống. Ví dụ: chặn người dùng truy cập một số cài đặt hệ thống.
* **AppInit\_DLLs:**
  + Tải các DLL (thư viện liên kết động) vào mọi quá trình sử dụng user32.dll. Đây là một lỗ hổng thường bị khai thác để tiêm mã độc hoặc gắn các đoạn mã độc vào các chương trình hợp pháp.

**Ví dụ thực tế:**

* **Ứng dụng hợp pháp:** Một ứng dụng nhắn tin có thể thêm chính nó vào khóa Run để khởi động cùng hệ thống.
* **Mã độc:** Malware thường sử dụng các khóa như Run hoặc AppInit\_DLLs để duy trì hoạt động và chạy ẩn trong nền mà người dùng không nhận ra.

**2. Chương trình 32-bit trên Windows 64-bit**

Hình ảnh thứ hai giải thích cách Windows hỗ trợ các chương trình 32-bit trên hệ điều hành 64-bit thông qua cơ chế **WoW64** (Windows-on-Windows 64-bit).

**Các thành phần chính:**

* **SysWOW64:**
  + Thư mục chứa các file hệ thống 32-bit để hỗ trợ các chương trình 32-bit chạy trên Windows 64-bit.
* **System32:**
  + Mặc dù tên gọi là "32", thư mục này thực tế chứa các file hệ thống **64-bit** trên hệ điều hành 64-bit.
* **kernel32.dll:**
  + Thư viện đóng vai trò cầu nối, giúp các chương trình thực hiện các lệnh gọi hệ thống (system call). Nó đảm bảo rằng cả ứng dụng 32-bit và 64-bit đều hoạt động trơn tru.

**Cách hoạt động:**

Khi một chương trình 32-bit chạy trên Windows 64-bit:

* Chương trình sẽ sử dụng các thư viện từ thư mục **SysWOW64** (thay vì System32).
* Mọi lệnh gọi hệ thống từ chương trình sẽ được kernel32.dll chuyển đổi để tương thích với nhân (kernel) 64-bit.

**Ví dụ thực tế:**

Một trình phát video 32-bit chạy trên Windows 64-bit sẽ tự động gọi các thư viện cần thiết từ **SysWOW64**, giúp nó hoạt động bình thường mà không cần sửa đổi mã nguồn.

A screenshot of a computer

Description automatically generated