Malware Persistant:

**Modifying registry keys:**

Vào Run của HKCU hoặc HKLM trong registry editor để tạo mới (path) tới target muốn khởi động.

HKEY\_CURRENT\_USER, SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE, SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Thêm trong HKCU dễ hơn vì HKLM cần quyền cao.

**Special Folder:**

Thêm shortcut vào thư mục này thì sau này nó sẽ tự khởi động.

C:\Documents and Settings\[user\_name]\Start Menu\Programs\Startup

**Task Scheduler: ( đăng ký vào lập lịch của window)**

1. Khởi tạo thư viện COM để sử dụng.
2. Tạo ITaskService object( sử dụng cái này để tạo task vào 1 folder chỉ định).
3. Sử dụng ITaskService vừa tạo để vào folder của task scheduler xong tạo task trong folder đó .
4. Xác định thông tin về task vừa tạo.
5. Tạo trigger đăng nhập cho task.
6. Tạo hành động tùy ý cho task.
7. Đăng ký task vào task cheduler.

**DLL Search oder hijacking: (kĩ thuật lợi dụng cách DLL đc load)**

Nếu OS ko tìm thấy dll, thì tìm theo thứ tự:

* Thư mục của chương trình
* System Directory(C:\Windows\System32)
* C:\Windows\System
* Windows Directory (C:\Windows)
* Thư mục hiện tại.
* Những directory trong biến môi trường PATH.

Do đó nếu chèn 1 **dll độc** cùng tên với **dll thật** vào thứ tự này và **dll độc** được tìm sớm hơn thì là chèn thành công. (sau đó **dll độc** sẽ gọi **dll thật** để đảm bảo chương trình chạy bình thường)

Yêu cầu dll độc phải giống với các hàm của dll thật,

Nếu mục tiêu là những application thường được khởi động cùng với máy thì có thể lợi dụng điều này để persistent.

**WMI event subscription: (đăng ký sự kiện Win Manage Intrument)**

WMI là 1 bộ công cụ quản lý dữ liệu và hoạt động trên hệ điều hành window.

Tất cả các đối tượng WMI được truy vấn bằng ngôn ngữ giống SQL được gọi là Ngôn ngữ truy vấn WMI (WQL).

Có 2 loại class: dynamic và persistent.

Đối tượng class persistent được lưu tại:

%SystemRoot%\System32\wbem\Repository\OBJECTS.DATA.

Persistent bằng cách che dấu dữ liệu lưu trữ , lợi dụng kho lưu trữ WMI để tạo các lớp WMI động và lưu trữ dữ liệu tùy ý.