DLL: thư viện liên kết động

Là file thư viện chứa các export function c/c++.

Vd như:

**kernel32.dll** chứa các hàm quản lý memory,process,thread.

**User32.dll** chứa các hàm hiển thị giao diện cho người dùng như tạo cửa sổ hay thông báo đến

**GDI32.dll** chứa các hàm cho hiển thị hình ảnh đồ họa và hiển thị văn bản

Dll có thể được tải vào address space của process

Tránh đặt tên dll chứa space

Cách thức building file dll :

1.Tạo file header (.h) chứa tên các hàm, function prototypes, structure,symbol

2.Tạo file cpp include file header trên và code các hàm.

3. Compiler xử lý thành file .obj đối với mỗi file cpp

4.Linker kết hợp các file .obj thành file .dll

Các cách Inject dll:

**1**.**Dùng Registry:**

Truy cập đường dẫn này bằng Registry Editor:

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

Trong đường dẫn registry này có 1 Key là AppInit\_Dlls, Set giá trị trường Data của nó là đường dẫn tới file dll mình cần inject.(có thể inject nhiều DLL ngăn cách nhau bằng dấu cách)

Khi 1 process nào đó sử dụng User32.dll , nó sẽ nhận được thông báo DLL\_PROCESS\_ATTACH, xử lý thông báo này sẽ truy xuất giá trị của Key AppInit\_Dlls , gọi LoadLibrary cho mỗi dll (chứa cả dll mình cần inject)

*Nhược điểm* **:**

* Chỉ có thể tiêm vào process dùng User32.dll.
* Cách này sẽ không hoạt động nếu tiêm dll vào compiler hoặc linker.
* Nếu đưa vào nhiều process thì dễ xảy ra xung đột.

**2**.**Dùng Window hook:**

Do winapi cung cấp 1 hàm hỗ trợ tiêm dll vào adds-spc của 1 process, gọi là hook.

Hàm này là :SetWindowsHookEx

HHOOK hHook =

SetWindowsHookExA(int *idHook*, HOOKPROC *lpfunc*,HINSTANCE *hdll*,DWORD *dwThreadId*);

* *idHook*: kiểu (type ) hook. Vd: WH\_GETMESSAGE,…
* *lpfunc*: địa chỉ hàm function (trong file dll cần inject) mà mình muốn system gọi nó.
* *Hdll*: chính là file dll cần inject( được lấy bằng hàm loadLibrary).
* *dwThreadId*: Tid của luồng cần móc vào, nếu chọn 0 là móc tất cả các luồng.

**3**.**Dùng Remote Thread:**

(Đây là cách linh hoạt nhất)

Cách làm : Tạo 1 thread mới trong process mục tiêu, điều khiển thread đó gọi hàm Load-Library đến dll mà ta muốn inject.(đương nhiên trước đó phải tiêm dll vào không gian địa chỉ của target process trước đã)

Winapi cung cấp 1 hàm để tạo thread trong 1 process khác là CreateRemoteThread

1. xác định process cần tiêm
2. cấp phát bộ nhớ trong process đó cho đủ để ghi đường dẫn đến dll cần tiêm.
3. copy đường dẫn hoặc toàn bộ DLL đến vùng nhớ của process vừa cấp phát.
4. Thực thi dll đó bằng hàm CreateRemoteThread.

**4**.**Trojan DLL:**

Thay thế file dll mà ta biết là process load nó. (đổi tên file dll thật đi, thay thế nó bằng file dll giả với tên giống hệt tên file dll thật)

Bên trong file dll giả, phải export tất cả các symbols giống với bản dll gốc,

(sử dụng “function forwarders” techniques để làm việc này).

Nên tránh dùng cách này vì nếu bị update thì có khả năng dll gốc sẽ bị thay thế, hoặc dễ bị hỏng hóc nếu ko thạo về .exe và .dll file formats.

**5**. **Lợi dụng debugger:**

Mỗi process có 1 không gian địa chỉ dành riêng cho “debuggee”, sử dụng “debugger” để chèn đường dẫn file dll ta muốn tiêm , vào kg địa chỉ của “debugee” đó, sau đó khi thread của “debugee” thực thi , nó sẽ thực thi cả phần code chứa địa chỉ dll ta muốn tiêm vào .

Extra:

* Cách set dll vào trong process mình muốn của cách Registry Method:

Code trong hàm dll+main(): dùng hàm GetCurrentProcessId lấy Pid,

Sau đó lấy ProcessName, so sánh với process name mình mong muốn, nếu không đúng thì exit , unload

1 số hàm liên quan: RegOpen KeyEX,Create key, query value,set value

(Global mutex)

* Hook Method:

Vd:Unikey: gõ 2 chữ a thành â

Unikey.exe word.exe

Unikey.dll

Khi gõ trên word System gửi messenge( vd WM\_KEYPRESS) tới word.exe,

Có 1 queue WM lưu các mess này.(hookchain)

Dùng SetwindowHook , unikey.exe hook unikey.dll vào hookchain của word.exe và trong unikey.dll chứa các hàm( vd biến aa thành â).

* Remote Method:

VitualAlloc: cấp phát cho process hiện tại

VitualAllocEx: tương tự trên nhưng other process

Cách inject truyền thống:

1.alloc

2.chuẩn bị sẵn 1 đoạn shell code

3.write đoạn shell code vào phần alloc

4.createRemoteThread để chạy đoạn shell code

* Trojan method: dùng Proxy dll để ko bị hỏng hóc program khi đổi tên file.