Detect it easy: Yoda’s Protector 1.03.2

Bài này chỉ chạy được trên window xp (do tâm linh mà biết, đánh đổi 3 ngày chạy mãi không được trên window 10).

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, application

Description automatically generated

Yoda’s Protector sẽ sử dụng 2 kĩ thuật anti-debug:

GetCurrentProcessId để check PID của mình và PID của calling process. Nếu không trùng thì sẽ kill calling process (ở đây là debugger).

Gọi BlockInput để chặn các thao tác input rồi thực hiện check các thứ các thứ. Nếu phát hiện có vấn đề hoặc bị exception hoặc vân vân thì hệ điều hành sẽ bị hang (hdh đợi user action nhưng lại bị BlockInput)

Như vậy ta cần debug cho tới khi user32.dll được nạp, disasembly và patch để disable BlockInput.

Đầu tiên, ta breakpoint tại cuối các hàm LoadLibraryA của kernel32.dll. Sau đó vừa F9 vừa kiểm tra Tab symbol, khi user32.dll được xuất hiện thì dừng lại.

Graphical user interface

Description automatically generated with medium confidence

Sau đó jump tới BlockInput và nop hết từ đầu hàm tới ret 4 (Ez bypass)

Graphical user interface

Description automatically generated with medium confidence

Tiếp tới là GetCurrentProcessId, cũng nop hết từ đầu tới cuối, và edit lại 1 instruction để return ra PID của x32dgb



Table

Description automatically generated

Sau khi sửa xong 2 API, trở lại với EIP hiện tại và show segment .text tại dump hex để xem khi nào .text được sinh ra