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)

Đặt breakpoint tại ret 4 vì ta còn cần nó sau này.

Graphical user interface

Description automatically generated with medium confidence

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



Table

Description automatically generated

Disable thêm IsDebuggerPresent để luôn luôn return 0

Shape

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 thay đổi. Ta thấy tại lần hit thứ 2 tại BlockInput thì thấy .text thay đổi. Lúc này chính là lúc packer load code vào session.

Set breakpoint on access tại session. Và lần hit tiếp theo tại session chính là OEP

Graphical user interface, application, Word

Description automatically generated with medium confidence

Graphical user interface, application

Description automatically generated

Sau khi breakpoint tại BlockInput hit lần thứ 2 thì ta thấy .text đã có code

Text

Description automatically generated

Table

Description automatically generated

Breakpoint on access session .text và F9 cho tới khi gặp được OEP (tâm linh).

Dump bằng Scylla và fix import bằng cách trace tới địa chỉ hàm và xem hàm nào được gọi (basic trace).

Graphical user interface, text, application, email

Description automatically generated

Ta thu được file exe có thể chạy được.

Graphical user interface, application

Description automatically generated