Hàm ở 0000000140004730 sẽ kiểm tra đầu vào là flag

Có 2 hàm chạy trc main là 0000000140001020 và 0000000140001000

Hàm 0000000140001020 sẽ hook ntreadfile

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

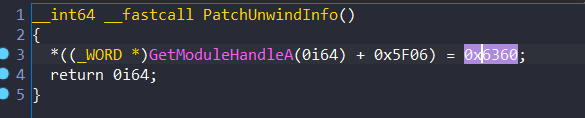
0000000140001000 sẽ vá là thông tin liên quan tới xử lý exception

Và vào section .ldata

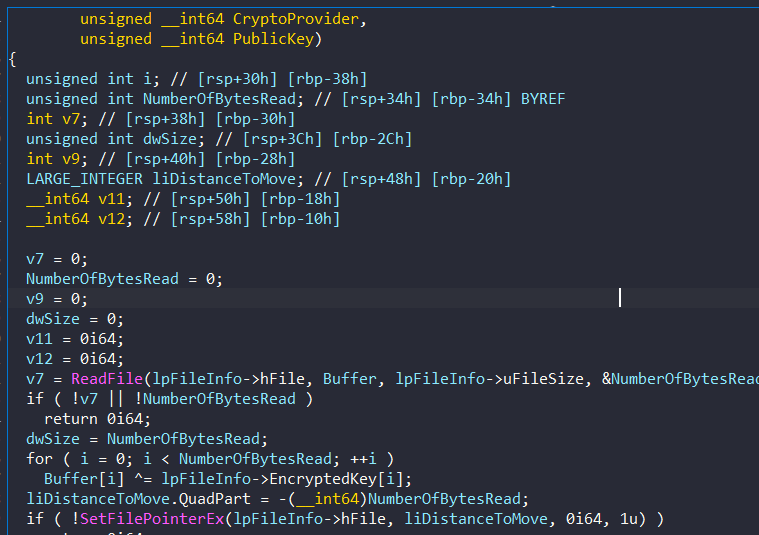
A screenshot of a computer

Description automatically generated

Section này gốc phải là rdata nhưng đã bị tác giả sửa thành ldata và có quyền ghi



Như ta tháy hàm exception handler thực sự được gọi là 0000000140006360



Exception xảy ra khi ở hàm kiểm tra flag, nó sẽ nhảy tới hàm rác gây exception

A screen shot of a computer

Description automatically generated

Đọc hiểu 2 hàm ẩn kia ta có dc cách tính flag

A screenshot of a computer code

Description automatically generated

Những bytes cuối chứa thông tin của file bị mã hoá, trong đó 0x28 là kích thước file.

Do đó 28 bytes đầu là flag bị mã hoá

Những bytes phía sau là key.

Hàm detour ntreadfile sẽ xor input của flag với 0xdd

Còn hàm exception handkler ẩn sẽ xor key, tức là các bytes phía sau offset 0x28.

Ví dụ

Flag là MSEC{}

Thì kết quả mã hoá là ord(‘M’) ^ 0xDD ^ 0x4b = cipher

Trong đó 0x4b là bắt đầu ở offset 0x28

A number on a white background

Description automatically generated

Cứ tiếp tục như vậy ta sẽ tìm dc flag

ASCIS{G00d\_j0b!Y0u\_f1nd\_all\_h1dden\_tr4p}