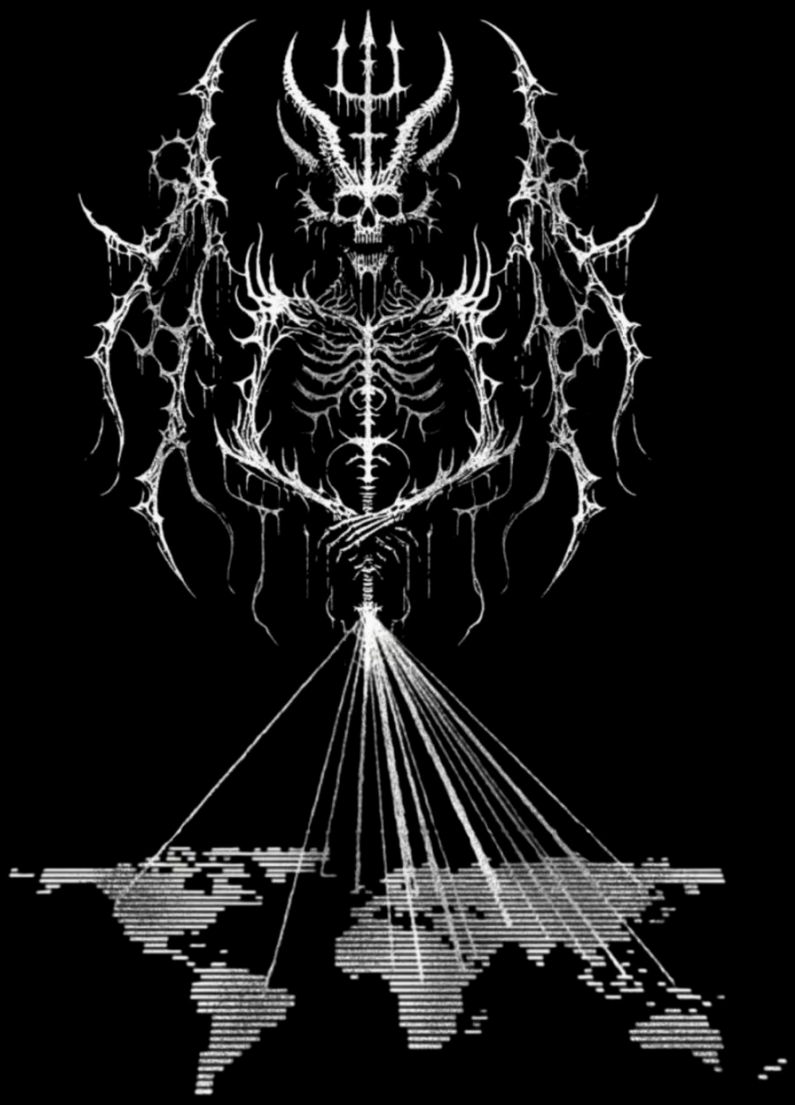


Novel Persistence Method in Windows

Examining a New Windows Persistence Technique Based on DLL Hijacking

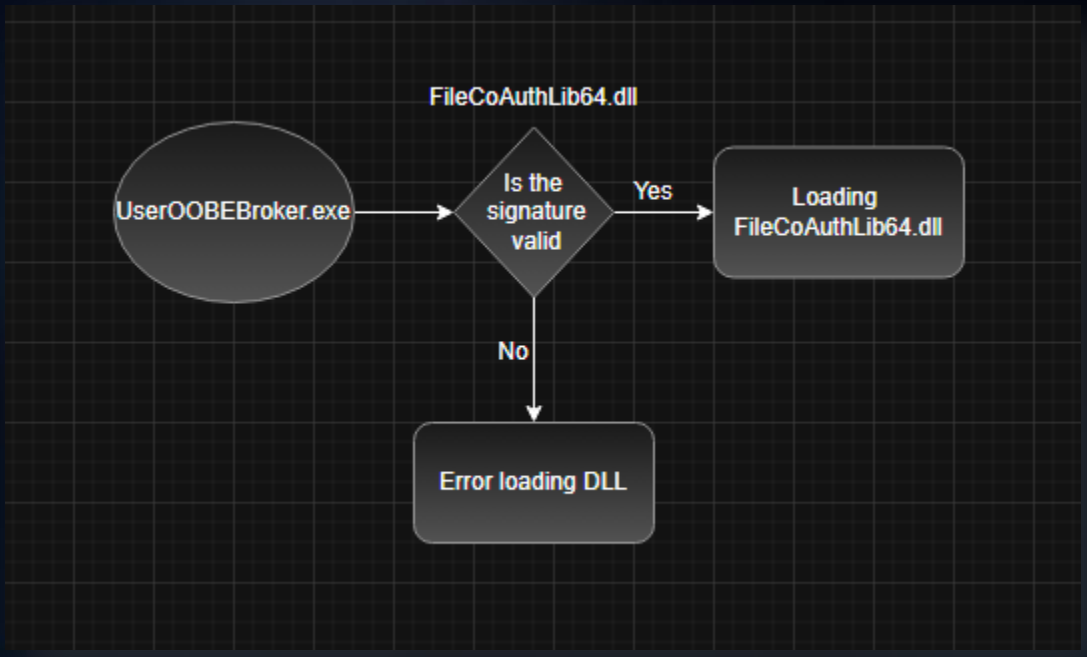
DarkBit
@MALCOREX

مقدمه

در این مقاله تکنیکی را معرفی می کنیم که در زمینه پایداری (Persistence) در سیستم عامل ویندوز کاربرد دارد. این تکنیک با استفاده از تزریق و جایگزینی DLL (با دسترسی یوزر) پیاده سازی شده و فایل DLL ما توسط svchost.exe اجرا میشود که باعث ماندگاری و اجرای مخفیانه کد در سیستم هدف خواهد شد. در ادامه راجب این تکنیک و نوع عملکرد آن به طور کامل صحبت خواهیم کرد.

این روش کاملا اختصاصی بوده و توسط یکی از اعضای تیم ما (@malcorex) کشف و توسعه داده شده است.

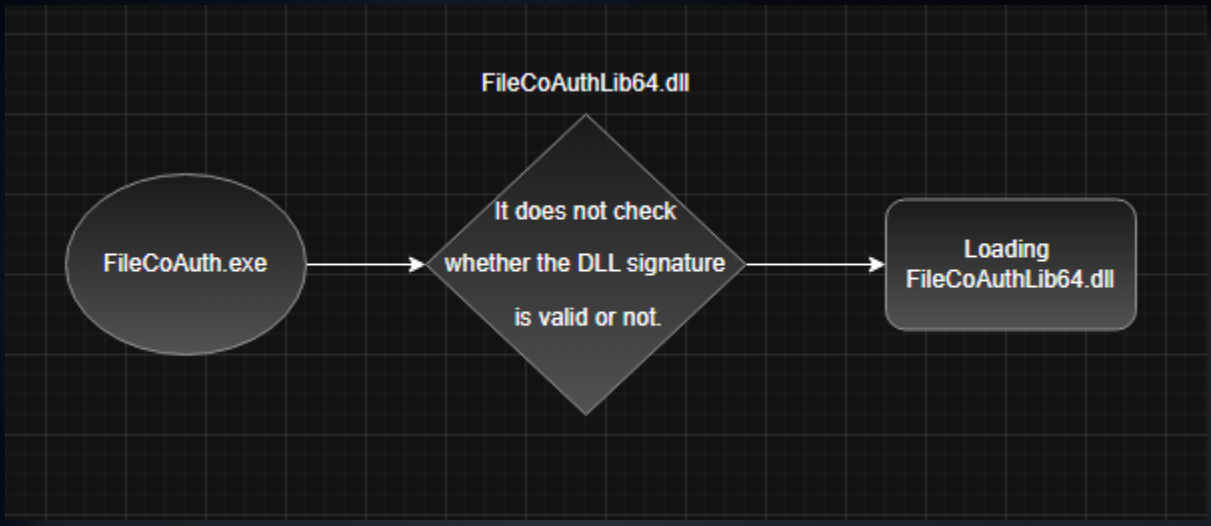
ضعف های امنیتی



همان طور که در فلوچارت مشاهده می کنید برنامه UserOOBEBroker.exe امضای DLL مورد نظر یعنی FileCoAuthLib64.dll را بررسی می کند و اگر امضا نامعتبر باشد آن را اجرا نمی کند. اما جالب هست بدانید که میتوان با دسترسی یوزر این DLL را تغییر داد که ما در این تکنیک از همین آسیب پذیری بهره می بریم.

این DLL در مسیر زیر وجود دارد :

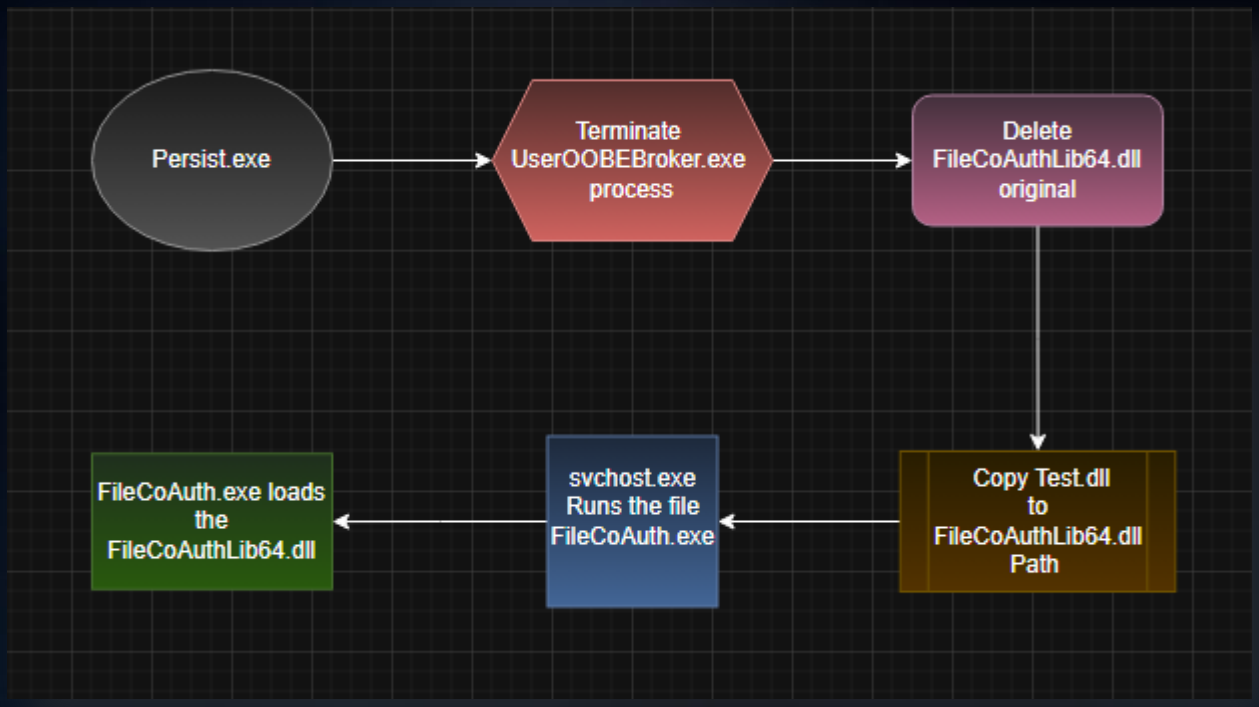
C:\Users\<USER>\AppData\Local\Microsoft\OneDrive\X.X.X.X\FileCoAuthLib64.dll



همان طور که مشاهده می کنید برنامه FileCoAuth.exe نیز از FileCoAuthLib64.dll استفاده می کند و آن را لود می کند. اما این برنامه بررسی نمی کند که امضای DLL معتبر است یا نه که همین یک آسیب پذیری در ویندوز هست که باعث می شود هر DLL دلخواهی را جایگزین DLL اصلی کنیم.

توجه داشته باشید که ساختار DLL جایگزین‌شده نیازی به تعریف توابع صادرشده (export)یا موارد مشابه ندارد و تنها کافی است نقطه شروع (Entry Point) آن مشخص باشد.

عملکرد



این فلوچارت عملکرد تکنیک را نشان می دهد. در ابتدا وقتی ما فایل Persist.exe را با دسترسی یوزر اجرا می کنیم سعی می کند فرایند UserOOBEBroker.exe را متوقف کند زیرا این فرایند FileCoAuthLib64.dll را درون خود لود کرده است و برای اینکه ما بتوانیم این DLL را حذف کنیم ابتدا فرایند مربوطه را متوقف می کنیم.

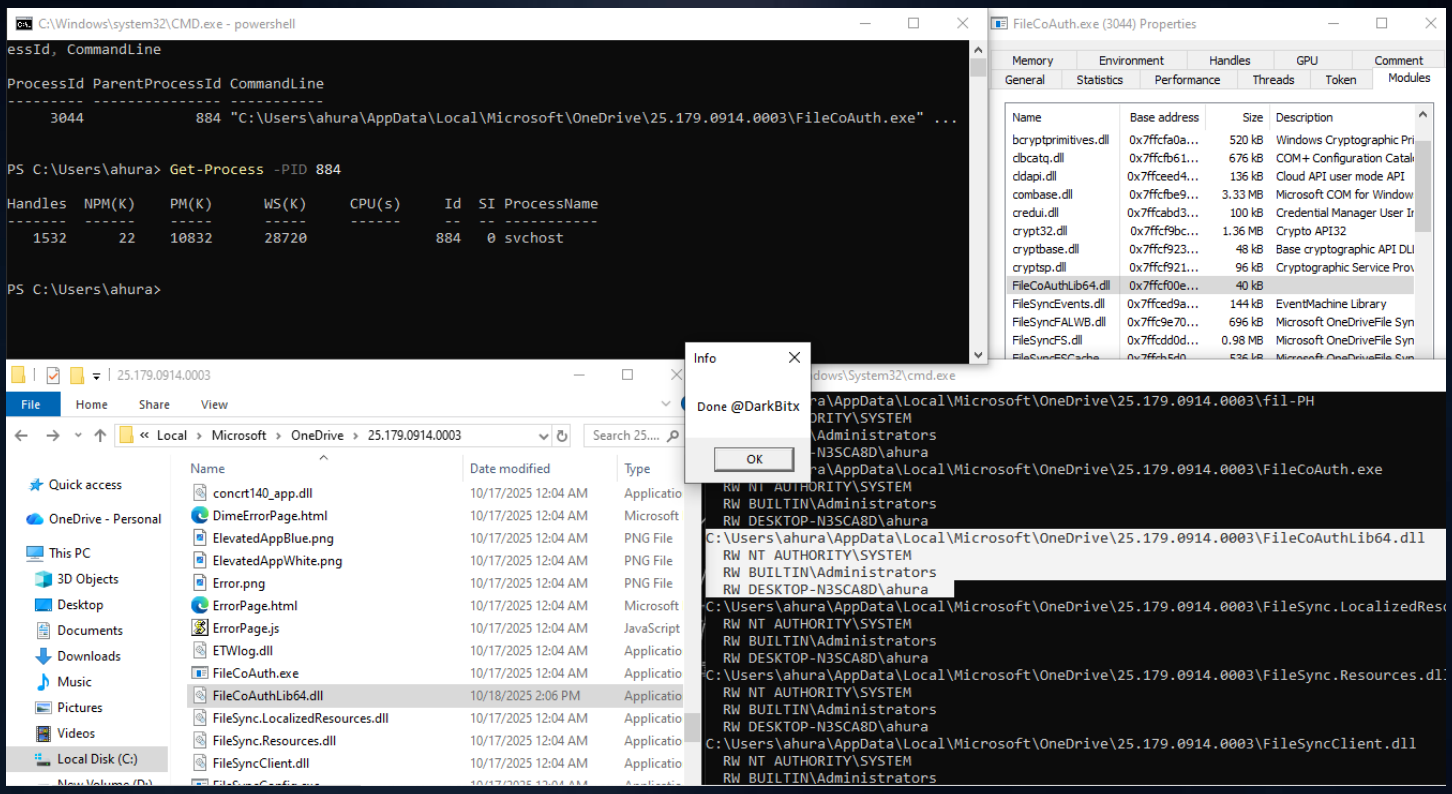
زمانی که DLL را حذف کردیم DLL خودمان را در مسیری که بالا ذکر شد با همان اسم کپی می کنیم.

بعد از چند دقیقه svchost.exe به صورت خودکار برنامه FileCoAuth.exe را اجرا می کند و در نتیجه DLL ما اجرا خواهد شد.

نکته : ممکن هست DLL ما هر چند دقیقه یکبار توسط برنامه FileCoAuth.exe اجرا شود.

جمع بندی

در این مقاله به بررسی یک تکنیک جدید Persist در ویندوز بر پایه DLL Hijacking پرداختیم. برنامه FileCoAuth.exe فایل DLL ما را با دسترسی یوزر اجرا می کند و همچنین در DLL ما از Mutex استفاده کردیم تا همزمان چند بار اجرا نشود.



این تکنیک در ویندوز 10 و 11 تست شده و به خوبی کار می کند

برای دیافت سورس کد فایل Persist.exe و DLL به چنل @DarkBitx مراجعه نمایید.

```
; Created by DarkBit ★ 2025
; Follow for more: https://t.me/Darkbitx
```