

# Novel Persistence Method in Windows

Examining a New Windows Persistence Technique Based on DLL Hijacking

**DarkBit**  
@MALCOREX

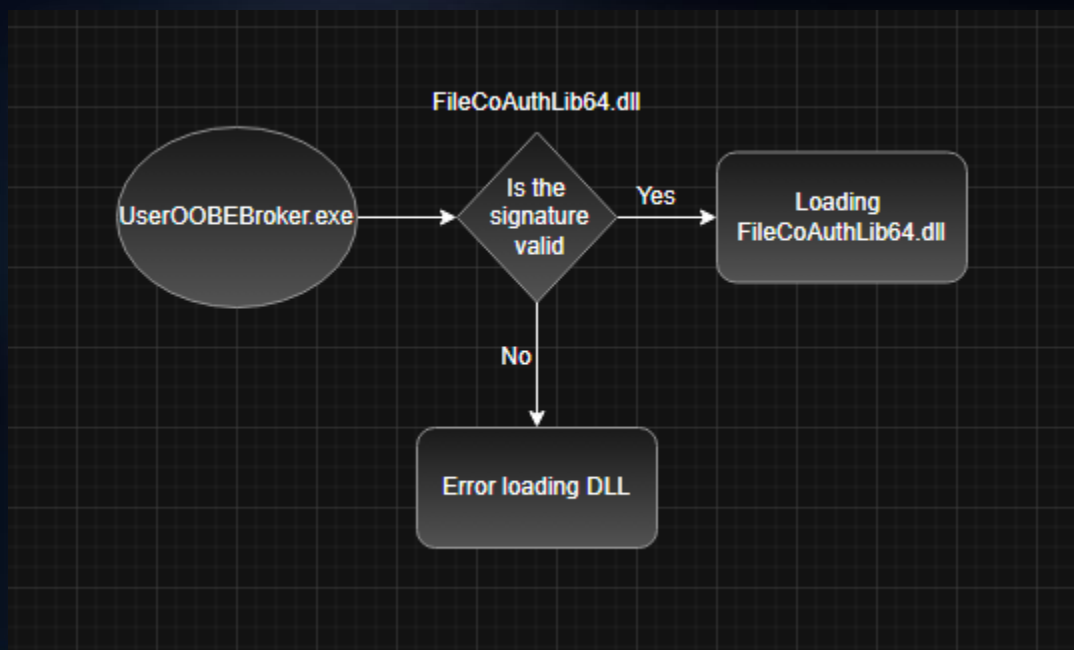
## مقدمه

---

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.

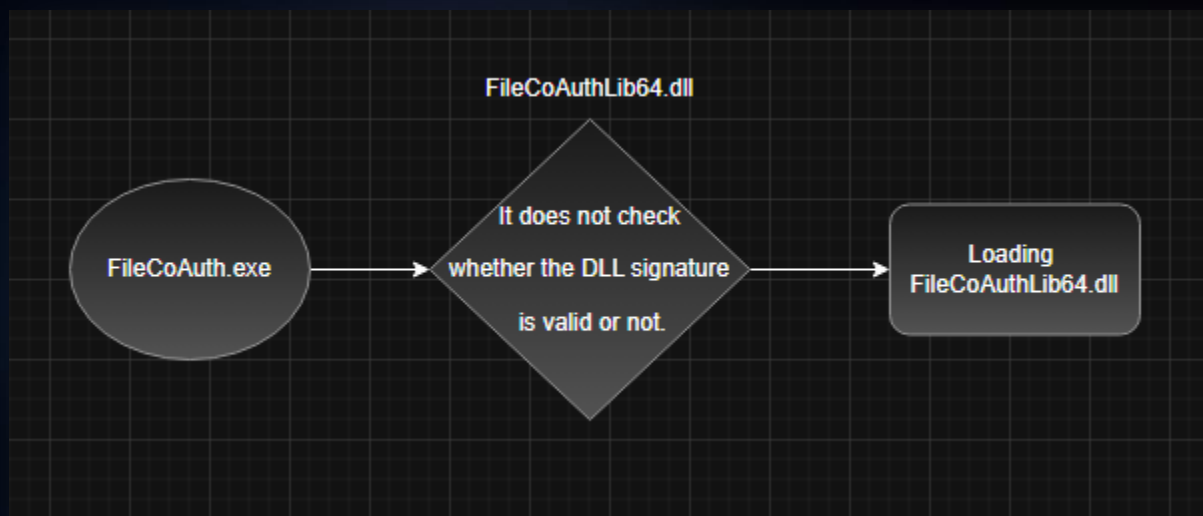
## ضعف های امنیتی



همان طور که در فلوجارت 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 :

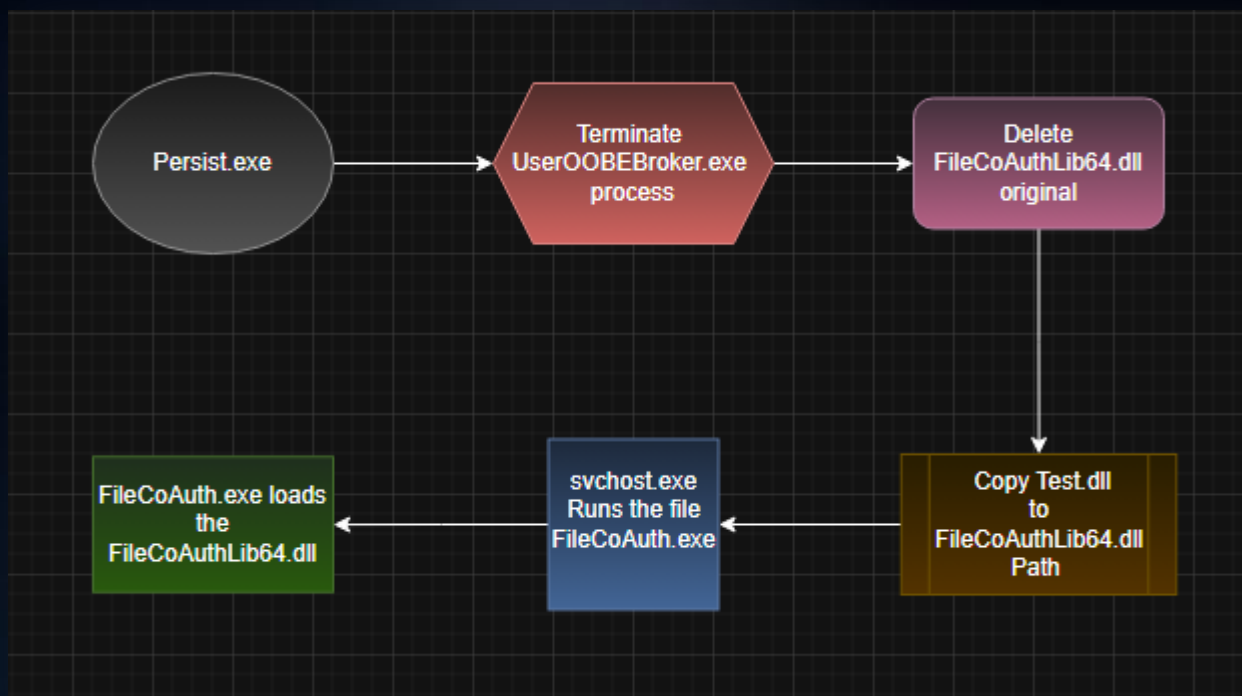
C:\Users\<<USER>\AppData\Local\Microsoft\OneDrive\X.X.X.X\  
FileCoAuthLib64.dll



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 جایگزین شده نیازی به تعریف توابع صادرشده (export) یا موارد مشابه ندارد و تنها کافی است نقطه شروع (Entry Point) آن مشخص باشد.

## عملکرد



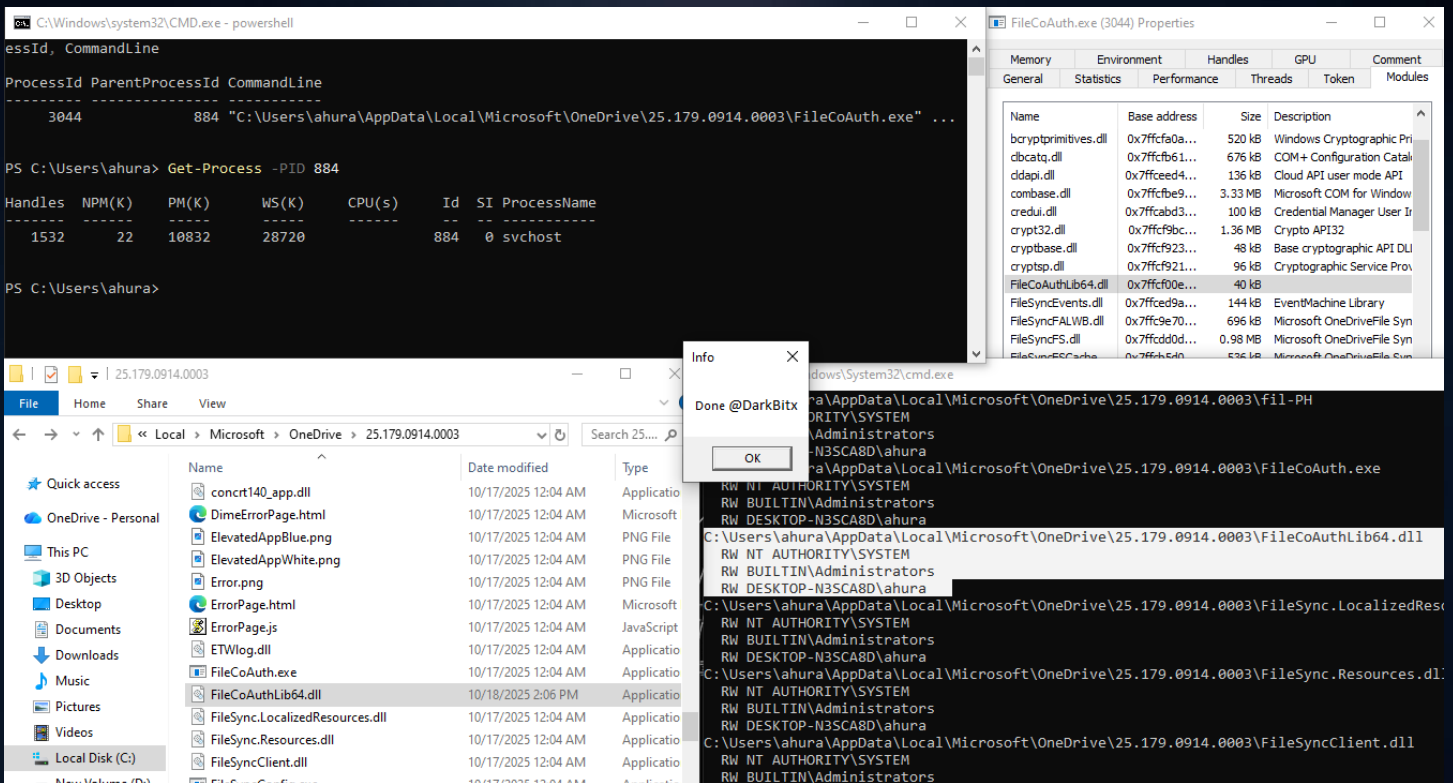
این فلوجارت عملکرد تکنیک را نشان می دهد. در ابتدا وقتی ما فایل Persist.exe را با دسترسی یوزر اجرا می کنیم سعی می کند فرایند UserOOBEBroker.exe را متوقف کند زیرا این فرایند FileCoAuthLib64.dll را درون خود لود کرده است و برای اینکه ما بتوانیم این DLL را حذف کنیم ابتدا فرایند مربوطه را متوقف می کنیم. زمانی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



The screenshot displays a Windows environment with three main windows:

- PowerShell Window:** Shows the command `Get-Process -PID 884` and its output:
 

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
1532	22	10832	28720		884	0	svchost
- File Explorer Window:** Shows the directory `C:\Users\ahura\AppData\Local\Microsoft\OneDrive\25.179.0914.0003` containing files like `FileCoAuth.exe` and `FileCoAuthLib64.dll`.
- FileCoAuth.exe Properties Dialog:** Shows the 'Modules' tab with a list of loaded DLLs:
 

Name	Base address	Size	Description
bcryptprimitives.dll	0x77cfa0a...	520 kB	Windows Cryptographic Pri...
cbcatq.dll	0x77cfa61...	676 kB	COM+ Configuration Catal...
ddapi.dll	0x77fced4...	136 kB	Cloud API user mode API
combase.dll	0x77fcb9e...	3.33 MB	Microsoft COM for Window...
credui.dll	0x77fcb9d3...	100 kB	Credential Manager User In...
crypt32.dll	0x77cf9bc...	1.36 MB	Crypto API32
cryptbase.dll	0x77cf923...	48 kB	Base cryptographic API DLU
cryptsp.dll	0x77cf921...	96 kB	Cryptographic Service Prov...
FileCoAuthLib64.dll	0x77cf00e...	40 kB	
FileSyncEvents.dll	0x77fcd9a...	144 kB	EventMachine Library
FileSyncFALWB.dll	0x77cf9e7...	696 kB	Microsoft OneDriveFile Syn...
FileSyncFS.dll	0x77fcd0d...	0.98 MB	Microsoft OneDriveFile Syn...
FileSyncFSCache...	0x77cf9e5...	536 kB	Microsoft OneDriveFile Syn...

این تکنیک در ویندوز 10 و 11 تست شده و به خوبی کار می کند  
برای دریافت سورس کد فایل Persist.exe و DLL به چنل @DarkBitx مراجعه نمایید.

*; Created by DarkBit ★ 2025*

*; Follow for more: <https://t.me/Darkbitx>*

