

### עבודה 3:

CreateFileW

**יצירת הDLL: (DLL-CreateFileW-microsoft-detours)**

השתמשנו ב[microsoft-detours](https://github.com/microsoft/microsoft-detours) על מנת לבצע את hooking.

הכנו קובץ DLL, שכאשר הוא נטען לראשונה, הוא יוצר קובץ עם מספר התהליך בתקייה c:\temp.

ולאחר מכן הוא מבצע DetourAttach לפונקציה שהכנו.

הפונקציה שהכנו נקראת:

newCreateFile, והיא נקראת כאשר מנסים לקרוא לפונקציה CreateFile המקורית. פעולת הפונקציה מאוד פשוטה, כאשר היא נקראת, היא כותבת לקובץ הלוג את הקובץ שנפתח, ולאחר מכן קוראת לפונקציה המקורית (originalCreateFile).

**הזרקת הDLL: ( process )**

עברנו על כל רשימת התהליכים, ונסינו לפתוח אליהם handler עם ההרשאות

- PROCESS\_QUERY\_INFORMATION
- PROCESS\_VM\_OPERATION
- PROCESS\_CREATE\_THREAD
- PROCESS\_VM\_READ
- PROCESS\_VM\_WRITE

אם הצלחנו, אנחנו טוענים לזיכרון התהליך את הpath המלא לDLL (מניחים שהוא בתקייה הנוכחית)

לאחר שטענו את הpath לזיכרון, אנחנו פותחים thread חדש, שירץ ישירות לפונקציה LoadLibraryA, וישתמש כארגומנט בכתובת הpath הנ"ל.

ובעצם כאשר הdll נטען, הוא יבצע את hook.

גילוי הhook:

- אם הhook בוצע על ידי Microsoft-detour, ניתן לזהות אותו על ידי התבוננות בתחילת הפונקציה (5-byte prolog)

88 FF – mov, edi, edi

55 – push ebp

8B EC – mov ebp, esp

כאשר מתבצע hooking על ידי Microsoft detour, הוא מחליף את ה5 בתים בפונקציה .jump.

- לכן ניתן לעבור על כל הפונקציות, ולבדוק אם הprologue השתנה.  
אם הHOOK בוצע על ידי שינוי Import Address table (IAT), ניתן פשוט לבדוק אם כל הכתובות שנמצאות שם הם בטווח הDLL של הIAT המתאים.

#### בנוסף:

- **גילוי של hooking (checkIfHookOrDetour)**  
רעיון הוא שהוא עובר על טבלת הIAT של כל DLL, והוא בודק האם הפונקציה שאנחנו עוברים אליה היא מתחילה עם הפרולוג המתאים (*88ff558bec*), ובנוסף היא אמורה לבדוק אם הפונקציה מוגדרת בתחום של הDLL המתאים.
- **WriteFile - (DLL-WriteFile-microsoft-detours)**  
מימשנו בנוסף hooking לפונקציה WriteFile בדיוק באותה צורה כמו שמימשנו CreateFileW.  
והכנו injector מתאים שמזריק את dll שמבצע hook לWriteFile לכל התהליכים שניתן (injector-writeFile).

#### קבצים:

- checkIfHookOrDetour – בודק איזה פונקציות חשודות לhooking
- DLL-CreateFileW-microsoft-detours - dll שמחליף את הפונקציה CreateFileW
- DLL-WriteFile-microsoft-detours - dll שמחליף את הפונקציה WriteFile
- proccess - מזריק את הdll של CreateFileW (הוא מחפש אותו בתקליה הנוכחית)
- injector-writeFile – מזריק את הDLL של WriteFile

צילומי מסך:

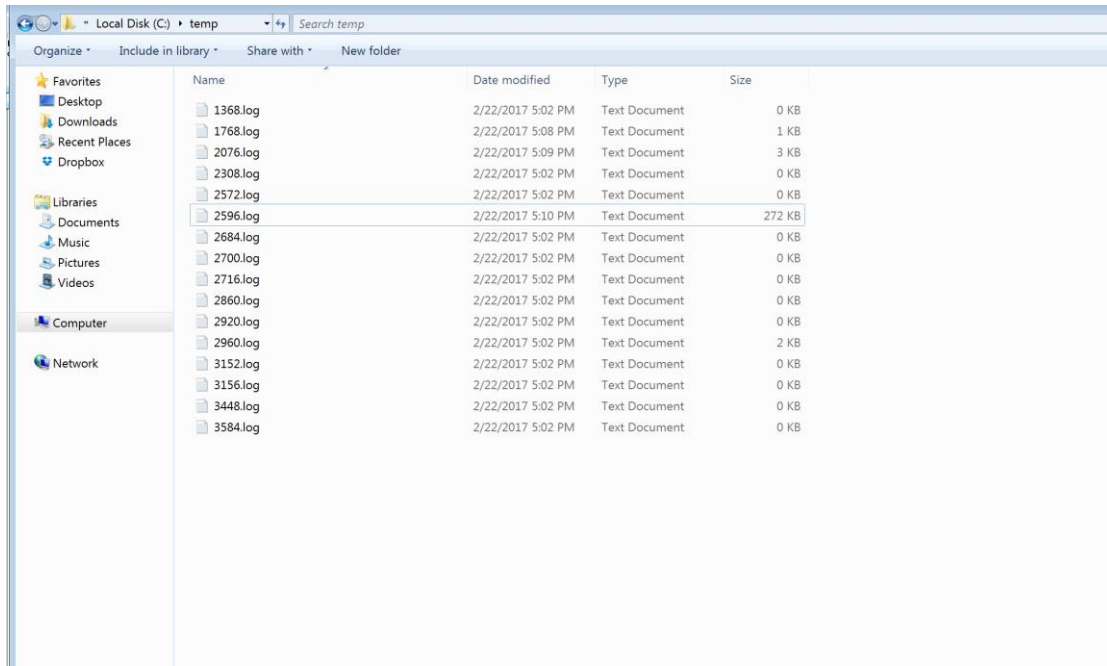
```
:_CreateFileW
```

The screenshot shows a Windows File Explorer window. The address bar indicates the current location is 'Local Disk (C:) > temp'. The search bar contains the text 'Search temp'. The left sidebar shows the 'Computer' section selected, with 'temp' highlighted. The main pane displays a table of files in the 'temp' directory.

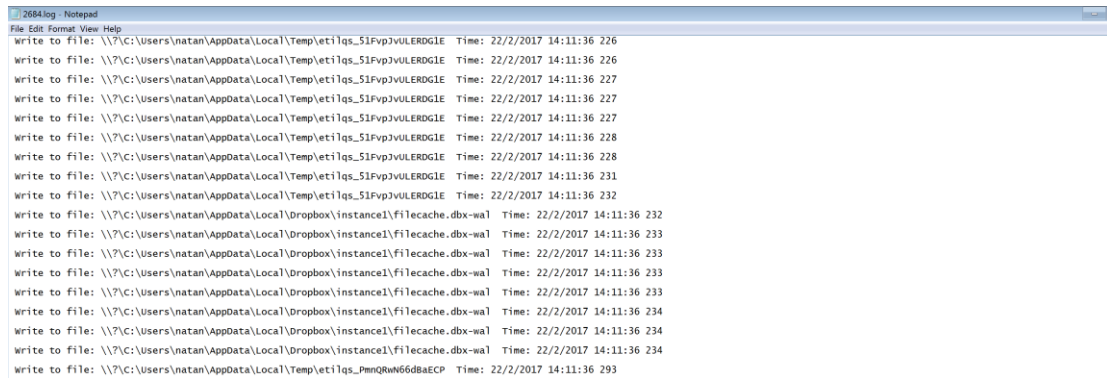
Name	Date modified	Type	Size
1368.log	2/22/2017 5:02 PM	Text Document	0 KB
1768.log	2/22/2017 5:02 PM	Text Document	1 KB
2076.log	2/22/2017 5:02 PM	Text Document	1 KB
2308.log	2/22/2017 5:02 PM	Text Document	0 KB
2572.log	2/22/2017 5:02 PM	Text Document	0 KB
2596.log	2/22/2017 5:02 PM	Text Document	0 KB
2684.log	2/22/2017 5:02 PM	Text Document	0 KB
2700.log	2/22/2017 5:02 PM	Text Document	0 KB
2716.log	2/22/2017 5:02 PM	Text Document	0 KB
2860.log	2/22/2017 5:02 PM	Text Document	0 KB
2920.log	2/22/2017 5:02 PM	Text Document	0 KB
2960.log	2/22/2017 5:02 PM	Text Document	2 KB
3152.log	2/22/2017 5:02 PM	Text Document	0 KB
3156.log	2/22/2017 5:02 PM	Text Document	0 KB
3448.log	2/22/2017 5:02 PM	Text Document	0 KB
3584.log	2/22/2017 5:02 PM	Text Document	0 KB

[illegible]

## WriteFile



Name	Date modified	Type	Size
1368.log	2/22/2017 5:02 PM	Text Document	0 KB
1768.log	2/22/2017 5:08 PM	Text Document	1 KB
2076.log	2/22/2017 5:09 PM	Text Document	3 KB
2308.log	2/22/2017 5:02 PM	Text Document	0 KB
2572.log	2/22/2017 5:02 PM	Text Document	0 KB
2596.log	2/22/2017 5:10 PM	Text Document	272 KB
2684.log	2/22/2017 5:02 PM	Text Document	0 KB
2700.log	2/22/2017 5:02 PM	Text Document	0 KB
2716.log	2/22/2017 5:02 PM	Text Document	0 KB
2860.log	2/22/2017 5:02 PM	Text Document	0 KB
2920.log	2/22/2017 5:02 PM	Text Document	0 KB
2960.log	2/22/2017 5:02 PM	Text Document	2 KB
3152.log	2/22/2017 5:02 PM	Text Document	0 KB
3156.log	2/22/2017 5:02 PM	Text Document	0 KB
3448.log	2/22/2017 5:02 PM	Text Document	0 KB
3584.log	2/22/2017 5:02 PM	Text Document	0 KB



```
File Edit Format View Help
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_51Fvp3vULERDGE Time: 22/2/2017 14:11:36 226
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_51Fvp3vULERDGE Time: 22/2/2017 14:11:36 226
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_51Fvp3vULERDGE Time: 22/2/2017 14:11:36 227
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_51Fvp3vULERDGE Time: 22/2/2017 14:11:36 227
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_51Fvp3vULERDGE Time: 22/2/2017 14:11:36 227
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_51Fvp3vULERDGE Time: 22/2/2017 14:11:36 228
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_51Fvp3vULERDGE Time: 22/2/2017 14:11:36 228
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_51Fvp3vULERDGE Time: 22/2/2017 14:11:36 231
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_51Fvp3vULERDGE Time: 22/2/2017 14:11:36 232
Write to file: \\?C:\Users\natan\AppData\Local\Dropbox\instance1\filecache.dbx-wal Time: 22/2/2017 14:11:36 232
Write to file: \\?C:\Users\natan\AppData\Local\Dropbox\instance1\filecache.dbx-wal Time: 22/2/2017 14:11:36 233
Write to file: \\?C:\Users\natan\AppData\Local\Dropbox\instance1\filecache.dbx-wal Time: 22/2/2017 14:11:36 233
Write to file: \\?C:\Users\natan\AppData\Local\Dropbox\instance1\filecache.dbx-wal Time: 22/2/2017 14:11:36 233
Write to file: \\?C:\Users\natan\AppData\Local\Dropbox\instance1\filecache.dbx-wal Time: 22/2/2017 14:11:36 233
Write to file: \\?C:\Users\natan\AppData\Local\Dropbox\instance1\filecache.dbx-wal Time: 22/2/2017 14:11:36 234
Write to file: \\?C:\Users\natan\AppData\Local\Dropbox\instance1\filecache.dbx-wal Time: 22/2/2017 14:11:36 234
Write to file: \\?C:\Users\natan\AppData\Local\Dropbox\instance1\filecache.dbx-wal Time: 22/2/2017 14:11:36 234
Write to file: \\?C:\Users\natan\AppData\Local\Temp\etilqs_PmnQRwN56d8aECP Time: 22/2/2017 14:11:36 293
```