

## Binary Instrumentation 2



Medium Reverse Engineering picoCTF 2025

AUTHOR: VENAX

### Description

I've been learning more Windows API functions to do my bidding. Hmm... I swear this program was supposed to create a file and write the flag directly to the file. Can you try and intercept the file writing function to see what went wrong?

Download the exe [here](#). Unzip the archive with the password `picoctf`

### Hints

1 2 3

Frida is an easy-to-install, lightweight binary instrumentation toolkit

865 users solved









 84% Liked 

 picoCTF{FLAG}

Submit Flag

Frida 툴을 사용하는 문제다.

### 오늘

 flag.txt	2025-08-21 오후 12:04	텍스트 문서	0KB
 bininst2.exe.id0	2025-08-21 오전 8:08	ID0 파일	296KB
 bininst2.exe.id1	2025-08-21 오전 7:51	ID1 파일	120KB
 bininst2.exe.id2	2025-08-21 오전 6:51	ID2 파일	3KB
 bininst2.exe.nam	2025-08-21 오전 6:51	NAM 파일	16KB
 bininst2.exe.til	2025-08-21 오전 6:51	TIL 파일	1KB
 bininst2.exe	2025-08-21 오전 6:50	응용 프로그램	29KB
 __handlers__	2025-08-21 오후 12:04	파일 폴더	

프로그램을 실행시키면 어떤 것도 뜨지 않고 바로 종료된다.

```
$ frida-trace -i *File* -f bininst2.exe -X KERNEL32
```

-X KERNEL32 옵션을 통해 해당 동적라이브러리를 제외하고 계측을 시도한다.

```

Warning: Skipping FileEncryptionData : unable to intercept function at 000077D1
Started tracing 576 functions. Web UI available at http://localhost:54627/
/* TID 0x8a6c */
1965 ms NtDeviceIoControlFile()
1966 ms RtlDosApplyFileIsolationRedirection_Ustr()
1966 ms RtlDosApplyFileIsolationRedirection_Ustr()
1966 ms RtlDosApplyFileIsolationRedirection_Ustr()
1966 ms NtQueryAttributesFile()
1966 ms NtQueryAttributesFile()
1966 ms NtOpenFile()
1966 ms RtlDosApplyFileIsolationRedirection_Ustr()
1973 ms GetSystemTimeAsFileTime()
1973 ms | GetSystemTimeAsFileTime()
1973 ms GetModuleFileNameW()
1973 ms | GetModuleFileNameW()
1973 ms AreFileApisANSI()
1973 ms | AreFileApisANSI()
1973 ms CreateFileA()
1973 ms CreateFileA entering in module: KERNELBASE.dll
1973 ms lpFileName = <Insert path here>
1973 ms | CreateFileA()
1973 ms | | CreateFileW()
1973 ms | | | CreateFileW()
Process terminated

```

해당 프로세스에서는 CreatFile API를 사용한다. 또한 lpFileName에 <Insert path here>라는 문자열을 파일 경로로 넘기고 있는데, 파일이 없어서 강제종료된 것이었다.

그래서 매개변수에 flag.txt를 전달하고 파일 이름을 넘긴다.

```

8   defineHandler({
9       onEnter(log, args, state) {
10          log('CreateFileA()');
11          const newPath = "flag.txt";
12          const buf = Memory.allocUtf8String(newPath);
13          this.buf = buf;
14          args[0] = buf;
15          log('lpFileName = ' + args[0].readUtf8String());
16      },
17
18      onLeave(log, retval, state) {
19      }
20  });
21

```

KERNEL32/CreateFileA 에 flag.txt를 생성하는 코드를 작성한다.

그리고 실행했는데 flag.txt에 아무 값도 채워지지 않았다.

```

Started tracing 2 functions. Web UI available at http://localhost:58014/
/* TID 0x84b4 */
8 ms CreateFileA()
8 ms lpFileName = flag.txt
8 ms | CreateFileA()
Process terminated

```

WriteFile 로그를 보면 0바이트를 채우는 것을 알 수 있다.

```

8   defineHandler({
9       onEnter(log, args, state) {
10          log('WriteFile() - hFile = ' + args[0]);
11          log('WriteFile() - nNumberOfBytesToWrite = ' + args[2]);
12      },
13
14      onLeave(log, retval, state) {
15      }
16  });

```

```

CreateFileA: Loaded handler at "C:\Users\hkh\Downloads\bininst2\__handlers__\KERNEL32.DLL\CreateFileA.js"
WriteFile: Loaded handler at "C:\Users\hkh\Downloads\bininst2\__handlers__\KERNEL32.DLL\WriteFile.js"
CreateFileA: Loaded handler at "C:\Users\hkh\Downloads\bininst2\__handlers__\KERNELBASE.dll\CreateFileA.js"
WriteFile: Loaded handler at "C:\Users\hkh\Downloads\bininst2\__handlers__\KERNELBASE.dll\WriteFile.js"
Started tracing 4 functions. Web UI available at http://localhost:58314/
/* TID 0x3f58 */
8 ms CreateFileA()
8 ms lpFileName = flag.txt
8 ms | CreateFileA()
8 ms WriteFile() - hFile = 0x294
8 ms WriteFile() - nNumberOfBytesToWrite = 0x0
9 ms | WriteFile()
Process terminated

```

그리고 WriteFile 두 번째 매개변수에는 어떤 값으로 세팅 되어있는지 보기 위해 log를 하나 더 추가했다.

```

defineHandler({
    onEnter(log, args, state) {
        log('WriteFile() - hFile = ', args[0]);
        log('WriteFile() - lpbuffer = ', hexdump(args[1]));
        log('WriteFile() - nNumberOfBytesToWrite = ', args[2]);
    },

    onLeave(log, retval, state) {
    }
});

```

```

15 ms WriteFile() - lpbuffer = 0 1 2 3 4 5 6 7 8 9 A B C D E F
140002270 63 47 6c 6a 62 30 4e 55 52 6e 74 6d 63 6a 46 6b cGljb0NURntmcjFk
140002280 59 56 39 6d 4d 48 4a 66 59 6a 46 75 58 32 6c 75 YV9mMHJfYjFuX2lu
140002290 4e 58 52 79 64 57 30 7a 62 6e 51 30 64 47 6c 76 NXRydW0zbnQ0dGlv
1400022a0 62 69 46 66 59 6a 49 78 59 57 56 6d 4d 7a 6c 39 biFfYjIxYWVmMzl9
1400022b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1400022c0 40 01 00 00 00 00 00 00 00 00 00 00 00 00 00 @.....
1400022d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1400022e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1400022f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
140002300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
140002310 00 00 00 00 00 00 00 00 00 00 30 00 40 01 00 00 .....0.@....
140002320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
140002330 a0 21 00 40 01 00 00 00 b0 21 00 40 01 00 00 00 .!.@.....!.@....
140002340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
140002350 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
140002360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
15 ms WriteFile() - nNumberOfBytesToWrite = 0x0
15 ms | WriteFile()
Process terminated

```

임의의 값이 나왔고, base64로 디코딩 했더니 flag가 출력됐다.

```
cGljb0NURntmcjFkYV9mMHJfYjFuX2luNXRydW0zbnQ0dGlvbiFfYjIxYWVmMzl9
```

ABC 64 1 64

## Output

```
picoCTF{fr1da_f0r_b1n_in5trum3nt4tion!_b21aef39}
```