SaadAhla / AMSI_patch Public

Notifications Fork 28 Star 143

Code Issues Pull requests Actions Projects Security Insights

main Go to file Code

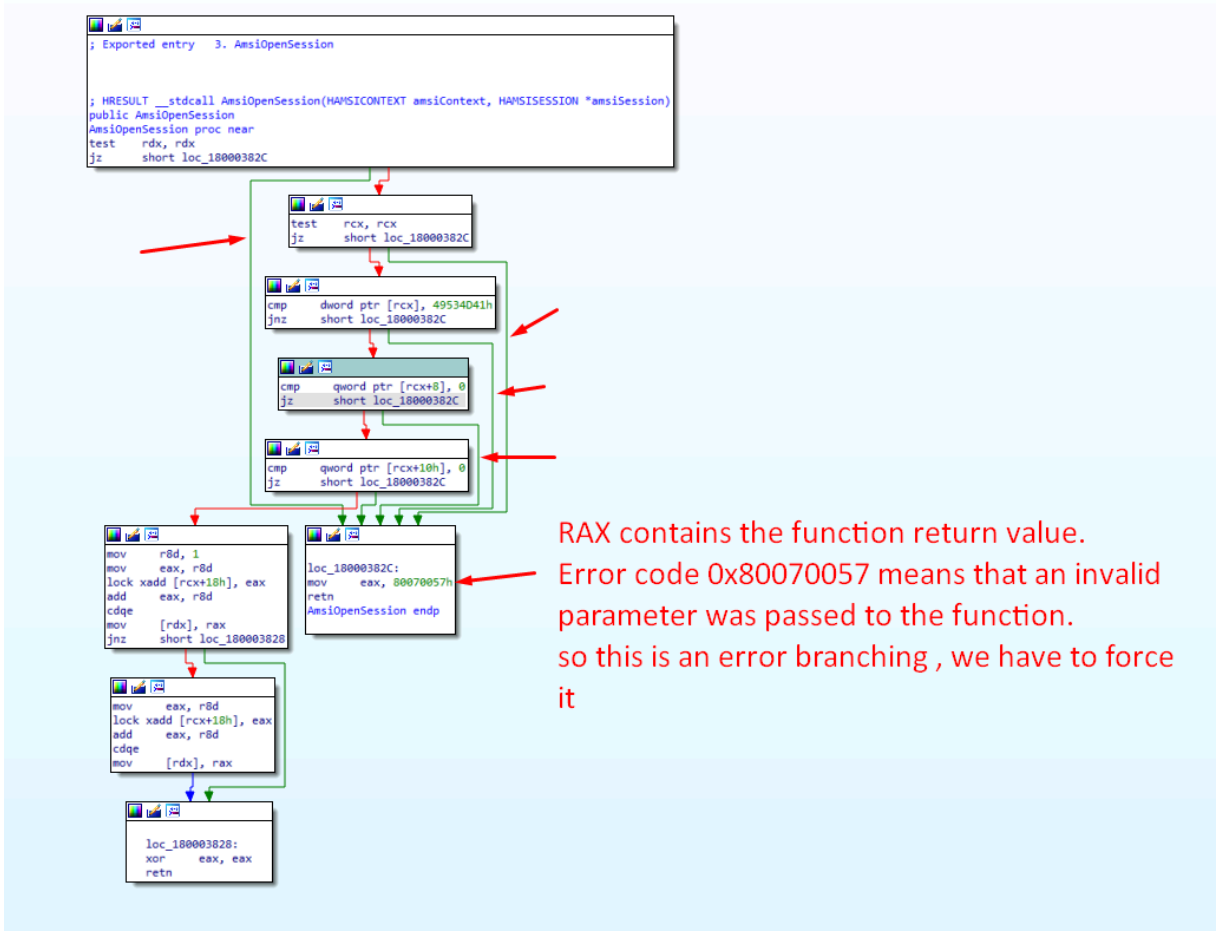
SaadAhla Create LICENSE 10f69da · last year 4 Commits

AmsiOpenSession	Add files via upload	last year
LICENSE	Create LICENSE	last year
README.md	Update README.md	last year

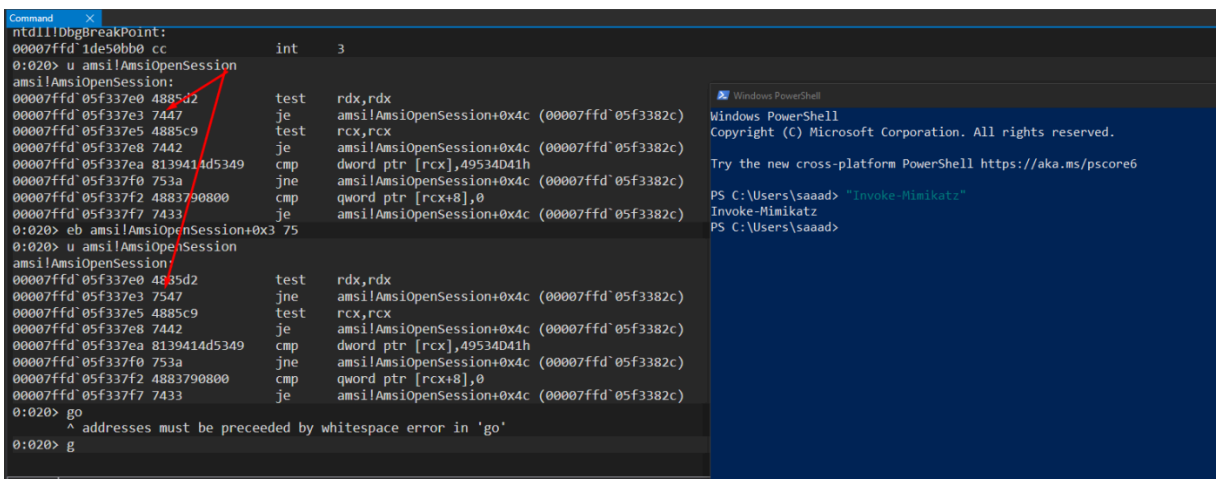
README MIT license

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` :



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



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%