

Forum:[Hack Forums](#)

Thread: [Need help/ideas on this detecting. Working on Runtime.](#)

Curs3d - August 11, 2025, 7:04 am

Hello So I working on my personal encryption method. My scan time is almost flawless (0/24 metadefender). However, runtime is a pain in the ass. I keep being detected for "Behavior:Win32/AMSI_Patch_T.B12" by windows 11 defender. The thing is, I have no asmi patch in my code. I do have obfuscation with delays and random code generation. Do you think this could be stopping me? Its also a staged payload. So my custom injection is compiled to a dll. Then that dll is placed in another "Staged loader." This loader runs the .dll which contains the shellcode and the injection methods. I do not know why I keep getting this detection. Any ideas?

Below is the metadefender scan. Im trying to trouble shoot to see why this asmi patch keeps getting me!.

Spoiler ([Click to View](#))

https://metadefender.com/results/file/bzl1MDgxMW1Jb3Q5X3RKdkhLX3JkTkJ2RUxq_mdaas

I think i found the bastard bitch Details
Found string artifact "dotnet" (AWL bypass Execute)
Found string artifact "timeout"
Found string artifact "reset"
Found string artifact "find"
Found string artifact "help"
Source
INPUT_FILE
ATT&CK ID
System Binary Proxy Execution (T1218)

The problem is how i am compiling dotnet publish -c Release -r win-x64 /p:PublishSingleFile=true --self-contained false i need the dll in one file.

I can build it self contained which would make file almost native in a sense. However the file ends up being 60mb.... which is huge however, this removes that asmi flag because i do not call for dotnet.exe this also brought me 2/71 on virustotal