

Forum:[Hack Forums](#)

Thread: [Process Hollowing and ShellCode](#)

Smoky - May 26, 2023, 6:52 pm

Hi guys,

I'm currently working on Process Hollowing.

I use among others, NtCreateSection, NtMapViewOfSection, WriteProcessMemory and ResumeThread for this.

The code seems ok because I get a connection on my Meterpreter payload, so far, so good.

My problem occurs as soon as I try with a RAT, Loader or Miner instead of Metasploit, from then on, impossible to inject in the created process, I can see the exe launching in ProcessHacker but it fails systematically.

I think my problem comes either from the injected process, but I've tried with several user processes and it's always the same, it fails, or, what I think is more likely, from the shellcode.

To recover the shellcode, I push my binary into HexEditor(HxD) and import it into C, then recover the Hexadecimal values.

Is my way of retrieving the shellcode is ok, please?

Do you think it could be something other than shellcode?

I can post the code if needed

Thanks in advance ?

SIM-5063966 - May 27, 2023, 6:10 am

You can use something like [donut](#) to generate shellcode from .NET assemblies & [pe2shc](#) to generate shellcode from native executables

If you want to learn more about shellcode loading, you can checkout [my \[censored\] pack!](#)

Smoky - May 27, 2023, 8:23 am

(May 27, 2023 06:10 AM)WtflsThis Wrote: [\[CITE\]](#) You can use something like [donut](#) to generate shellcode from .NET assemblies & [pe2shc](#) to generate shellcode from native executables

If you want to learn more about shellcode loading, you can checkout [my \[censored\] pack!](#)

Thanks for your answer man :)

Ok, i'll look into Donut.

After solving this problem, I'd also have questions about AV evasion in the runtime, although I also have the Sektor7 courses, maybe one of your e-books could be of interest to me if you treat this with examples in C# as I don't have much knowledge of C or ASM.

I'll be in touch soon in DM

PegasoUni - April 19, 2024, 7:25 am

Hi, can you send me a private message, I would like to ask you something

COCKBOT - May 4, 2024, 7:40 am

(May 27, 2023 06:10 AM)WtfIsThis Wrote: [\[CITE\]](#) You can use something like [donut](#) to generate shellcode from .NET assemblies & [pe2shc](#) to generate shellcode from native executables

If you want to learn more about shellcode loading, you can checkout [my \[censored\] pack!](#)
The second link, pe to shellcode, is what I used a year or so back when implementing runtime monitoring for a bot client I was selling.

15-20 shellcode variations, randomly sent over the wire on session init and mid-session re-negotiations.

I never had any problems with it. It's very useful.