

Forum:[Hack Forums](#)

Thread: [Is the process hollowing bad option for crypter FUD?](#)

pedrosegundo - February 17, 2022, 6:05 pm

I am making my crypter. I wanna use process hollowing, but my friends told me that process hollowing is not good for FUD.

He said AV can easily detect my stub if I use process hollowing

I am not clear. I know many crypters use process hollowing.

If the process hollowing is rly not good and old for FUD, then what process injection techniques are best for FUD?

jmark7 - February 18, 2022, 10:18 am

You should not believe on what other say,

You should try yourself and check if there is detection on it or not.

Crypters not have many methods to bypass AV, only a few handful methods and process hollowing is one of it.

YAK_CODER - February 18, 2022, 12:43 pm

process hollowing

is known very well by most av

to test ur runpe is good or not

kindly use this tool called RunPEDetectorV2

Aphosis - February 20, 2022, 2:13 pm

"RunPE" (Process Hollowing) "can" provide decent results if coded right paired with the right evasion implementations, I've personally got a RunPE implementation down to 2-3 detections at runtime. If I were you I'd personally look into developing a "LoadPE" over a "RunPE" though. You won't be disappointed and the implementation concept for "LoadPE" honestly isn't too much more complex to understand than "RunPE".

Aphosis - February 20, 2022, 2:53 pm

(Feb 20, 2022 03:47 PM)Incog Wrote: [\[CITE\]](#) The premise of a LoadPE is that instead of calling createprocess for then suspending and hollowing, it gets an already running process right?

I've seen the term LoadPE thrown around but haven't found a proper explanation for it, beyond that LoadPE can achieve better results

So LoadPE isn't "process injection" at all, A LoadPE will load the payload exactly like the Windows PE Loader would making it less noisy compared to something like "process injection". Where as for example process injection will spawn a new process often a trusted windows process to execute the context of the payload from. LoadPE is manually mapping the payload into the currently executing process and you will handle relocations and imports yourself. I can provide you some of my personal code examples (C++) and any information you'd like on LoadPE if you PM me I'll always show love to someone with an interest to learn. <3

Aphosis - February 20, 2022, 3:21 pm

(Feb 20, 2022 04:11 PM)Incog Wrote: [\[CITE\]](#) AHFFFH okay, so if I was to make a similar comparison to C# it would be Invoke() which allows for .NET files to be executed within the same space as itself

and yeah I'd love to look at sources if you are offering, shooting a pm now :)

No that isn't correct it wouldn't be like that, I just realized as well I don't have 10 posts so I can't have a conversation in HF messages. I'm a new account here but send me a PM with your XMPP and I will contact you on there and explain the concept to you. I have much experience in C# development as well so I can give you some insight in .Net specifically as well.

Aphosis - February 20, 2022, 3:25 pm

(Feb 20, 2022 04:23 PM)Incog Wrote: [CITE](#) I thought if a member sent a convo you could then reply, but XMPP is incog@thesecure.biz

and oh, guess I got a fair bit to learn about this whole memory shiz lol

I believe if it's a PM and not a conversation then you can but I haven't been on this forum in ages so I wouldn't be sure. Sending a request on XMPP now!