

Forum:[Hack Forums](#)

Thread: [Metasploit-FrameWork *Important Update*](#)

CyberStrike - May 5, 2018, 10:20 pm

Not sure if everyone here has paid attention but metasploit-framework now has encryption for payloads.

<https://github.com/rapid7/metasploit-framework/pull/9869>

<https://blog.rapid7.com/2018/05/03/hiding-metasploit-shellcode-to-evade-windows-defender/>

This is definitely a major and long needed improvement.

SysAdmin - May 6, 2018, 4:56 am

Oh that is awesome! I bet this will help out in many occasions!

Nomad.Null - May 6, 2018, 11:36 pm

Very cool blog post. Glad to see this has finally been implemented. It was long overdue.

r0biba - May 7, 2018, 4:47 am

It's time... Would be really useful

Hooded Robin - May 7, 2018, 5:33 am

Still need to code yourself a custom loader to use it, but cool! Time to get coding...

InvictusLatinus - May 7, 2018, 11:48 am

That's actually really cool!

CyberStrike - May 7, 2018, 1:10 pm

(May 7, 2018 05:33 AM)Hooded Robin Wrote: [\[CITE\]](#) Still need to code yourself a custom loader to use it, but cool! Time to get coding...

That's the best way to evade AV's using custom shellcode loaders or other custom solutions.

hempuk - May 8, 2018, 7:53 am

very cool i guess its time to start learning how to create a custom loader...

Originalkillit - May 19, 2018, 7:39 am

Eagerly looking for posts like this thank you op helped me a lot ?

Big Fan Of MSF ?

Toxic Legend - May 21, 2018, 11:33 am

Very good information indeed.

shadowkk2 - December 12, 2018, 6:26 am

(May 7, 2018 01:10 PM)SilentWatch Wrote: [\[CITE\]](#) That's the best way to evade AV's using custom shellcode loaders or other custom solutions.

Having seen your detailed and informative replies on some posts here on HF, I wanted if you would mind sharing your thoughts towards any reliable seller or coder for silent exploit for exe files? Kindly PM me.

CyberStrike - December 12, 2018, 12:21 pm

(Dec 12, 2018 07:26 AM)shadowkk2 Wrote: [\[CITE\]](#) Having seen your detailed and informative replies on some posts here on HF, I wanted if you would mind sharing your thoughts towards any reliable seller or coder for silent exploit for exe files? Kindly PM me.

I don't use any tools from HF, I have sold my signature once I am not familiar with the market place here nor any of the products. Of course I will suggest using the contract feature of the forum for any deals and always check out the "Deals Disputes" section in the Market section.

jammy47 - December 12, 2018, 7:28 pm

how hard can coding a customer loader possibly be?

CyberStrike - December 12, 2018, 8:03 pm

(Dec 12, 2018 08:28 PM)jammy47 Wrote: [\[CITE\]](#) how hard can coding a customer loader possibly be?

Loader as in exploit which it now loads a payload or are you talking about a PE loader such as RunPE?

CarbonBasedHax - December 12, 2018, 9:41 pm

Cann we encode then encrypt, or encrypt then encode? to further variate the signature?

CyberStrike - December 12, 2018, 11:10 pm

(Dec 12, 2018 10:41 PM)CarbonBasedHax Wrote: [\[CITE\]](#) Cann we encode then encrypt, or encrypt then encode? to further variate the signature?

I would say obfuscate first then encrypt the payload the whole file can be encrypted as well. I always add to my payloads like for me domain name has to match and dates have to match then it queries the local machine (target) for the decryption key for the file from there another query something again I expect on the target to decrypt the payload.

jammy47 - December 13, 2018, 10:40 am

(Dec 12, 2018 09:03 PM)SilentWatch Wrote: [\[CITE\]](#) Loader as in exploit which it now loads a payload or are you talking about a PE loader such as RunPE?

taking about an exploit whose payload downloads a file and executes it. So ya im talking about run pe.

ANT. - December 13, 2018, 10:44 am

Thank you for the share, this was needed for many PL's in the past

CyberStrike - December 13, 2018, 6:30 pm

(Dec 13, 2018 11:40 AM)jammy47 Wrote: [\[CITE\]](#) taking about an exploit whose payload downloads a file and executes it. So ya im talking about run pe.

Basically a RunPE is creating a process, then getting the base address from there you will write your PE into said process, suspend the process and continue. It's process hollowing pretty much. If you want check out the following they have an example.

<https://www.andreafortuna.org/technology/runpe-a-practical-example-of-process-hollowing-technique/>

Process hollowing having done DFIR I know it's not impossible to detect, actually it's very common to run across it in memory forensics.