

Forum:[Hack Forums](#)

Thread: [x86 RunPE Shellcode Wrapper](#)

Wardow - April 2, 2016, 7:57 pm

Hello!

As posted here: <https://hackforums.net/showthread.php?tid=5224701>

I have recently released a x86 RunPE Shellcode, I have made an AutoIT Wrapper for it.

Enjoy ;)

EDIT: Updated and fixed memory leak of the shellcode page

French Products - April 3, 2016, 12:22 am

Good job my friend, it's the best public RunPE of moment.

?

DuguWudi - April 3, 2016, 12:30 am

Bro, you change the code, the previous one run in endless loop. Cozing me to shutdown and reboot my computer a few times until I change some code.

Wardow - April 3, 2016, 12:40 am

(Apr 3, 2016 12:30 AM)DuguWudi Wrote: [\[CITE\]](#) Bro, you change the code, the previous one run in endless loop. Cozing me to shutdown and reboot my computer a few times until I change some code.

It displays an MsgBox between each tries, I've changed that, it was just for testing and i forgot to remove it

?????? - April 3, 2016, 11:15 pm

Wardow cheers mate :)

Wardow - April 12, 2016, 1:17 am

Updated with newest version!

N3oNight - April 12, 2016, 1:49 am

(Apr 12, 2016 01:17 AM)Wardow Wrote: [\[CITE\]](#) Updated with newest version!

What improvement you made and when you releasing the .net version ?

TERRORISST--- - April 12, 2016, 1:52 am

Lol, all of the morons who don't even understand this code are complimenting the true basis of garbage.

ShellCode should never be compiled. The point of PIC is for reliability on local relative addressing. You're completely missing the point. You should invest time in learning Assembly, then release proper shellcode with a proper size. (That doesn't invoke memory leaks, and is capable of injecting into memory without screaming HIPS)

Wardow - April 12, 2016, 1:55 am

(Apr 12, 2016 01:52 AM)TERRORISST--- Wrote: [\[CITE\]](#) Lol, all of the morons who don't even understand this code are complimenting the true basis of garbage.

ShellCode should never be compiled. The point of PIC is for reliability on local relative addressing. You're completely missing the point. You should invest time in learning Assembly, then release proper shellcode with a proper size. (That doesn't invoke memory leaks, and is capable of injecting into memory without screaming HIPS)

Get a life, troll.

TERRORISST--- - April 12, 2016, 1:55 am

(Apr 12, 2016 01:55 AM)Wardow Wrote: [\[CITE\]](#) Get a life, troll.

Troll ? I'm merely evaluating your shitty code.

Wardow - April 12, 2016, 1:57 am

(Apr 12, 2016 01:55 AM)TERRORISST--- Wrote: [\[CITE\]](#) Troll ? I'm merely evaluating your shitty code.

yes, get a life :)

TERRORISST--- - April 12, 2016, 1:57 am

(Apr 12, 2016 01:57 AM)Wardow Wrote: [\[CITE\]](#) yes, get a life :)

how about you release something that isn't garbage

Wardow - April 12, 2016, 2:01 am

(Apr 12, 2016 01:57 AM)TERRORISST--- Wrote: [\[CITE\]](#) how about you release something that isn't garbage

how about you even release something :')

TERRORISST--- - April 12, 2016, 2:01 am

(Apr 12, 2016 02:01 AM)Wardow Wrote: [\[CITE\]](#) how about you even release something :')

My codes too precious for HF.

Wardow - April 12, 2016, 2:02 am

(Apr 12, 2016 02:01 AM)TERRORISST--- Wrote: [\[CITE\]](#) My codes too precious for HF.

Get over it, troll.

TERRORISST--- - April 12, 2016, 2:06 am

(Apr 12, 2016 02:02 AM)Wardow Wrote: [\[CITE\]](#) Get over it, troll.

Keep telling yourself that i'm a troll, your code is really shit.

Wardow - April 12, 2016, 2:06 am

(Apr 12, 2016 02:06 AM)TERRORISST--- Wrote: [\[CITE\]](#) Keep telling yourself that i'm a troll, your code is really shit.

yet you did not even test anything :)

Get over HF.

TERRORISST--- - April 12, 2016, 2:07 am

(Apr 12, 2016 02:06 AM)Wardow Wrote: [\[CITE\]](#) yet you did not even test anything :)

Get over HF.

It's already been settled that your previous code produced memory leaks, and further more, showed the ability to copy & paste public code.

French Products - April 12, 2016, 2:07 am

(Apr 12, 2016 01:55 AM)TERRORISST--- Wrote: [\[CITE\]](#) Troll ? I'm merely evaluating your shitty code.

If it's " shitty code" why you don't pm for help him ????

Have you already test this ?....

Please if you post, make a post with something usefull/helpfull not shit ...

Wardow - April 12, 2016, 2:08 am

(Apr 12, 2016 02:07 AM)TERRORISST--- Wrote: [\[CITE\]](#) It's already been settled that your previous code produced memory leaks, and further more, showed the ability to copy & paste public code. proof of that please? thank you :)

If you have anything more to say, just stop the useless and not helpful posts, people wont ever learn from insults :p

TERRORISST--- - April 12, 2016, 2:09 am

(Apr 12, 2016 02:07 AM)French Crypter Wrote: [\[CITE\]](#) If it's " shitty code" why you don't pm for help him ????

Have you already test this ?....

Please if you post, make a post with something usefull/helpfull not shit ...

Why would i PM him for help?

Throw this shell code into IDA and decompile into C.. See for yourself, as shown in the C++ Thread. Seeing as you dont understand this code i wouldn't expect a skid like you to analyze it.

But yeah, go ahead and use it.

Wardow - April 12, 2016, 2:11 am

(Apr 12, 2016 02:09 AM)TERRORISST--- Wrote: [\[CITE\]](#) Why would i PM him for help?

Throw this shell code into IDA and decompile into C.. See for yourself, as shown in the C++ Thread.

Seeing as you dont understand this code i wouldn't expect a skid like you to analyze it.

But yeah, go ahead and use it.

He does and it's working perfectly fine!

TERRORISST--- - April 12, 2016, 2:14 am

(Apr 12, 2016 02:11 AM)Wardow Wrote: [\[CITE\]](#) He does and it's working perfectly fine!

The fact that it works is not the point you moron.

French Products - April 12, 2016, 2:16 am

(Apr 12, 2016 02:09 AM)TERRORISST--- Wrote: [\[CITE\]](#) Why would i PM him for help?

Throw this shell code into IDA and decompile into C.. See for yourself, as shown in the C++ Thread.

Seeing as you dont understand this code i wouldn't expect a skid like you to analyze it.

But yeah, go ahead and use it.

Always usefull post...

Please, your mental look to the mental of kid, you are multi accounter and you post shit ?

I think it's better for you start be helpfull with guy's and stop trash with immature reply.

I just want tell this RunPE is the better public in AutoIT, if you are more competent for make RunPE, I'll wait your release.

TERRORISST--- - April 12, 2016, 2:18 am

(Apr 12, 2016 02:16 AM)French Crypter Wrote: [\[CITE\]](#) Always usefull post...

Please, your mental look to the mental of kid, you are multi accounter and you post shit ?

I think it's better for you start be helpfull with guy's and stop trash with immature reply.

I just want tell this RunPE is the better public in AutoIT, if you are more competent for make RunPE, I'll wait your release.

You keep asking me to help this moron, trust me I've tried.

I'm definitely more competent, and by far more competent than you and this moron will ever be.

You clearly don't know me. "french crypter" Fucking skid.

1. You're using public code for your theme
2. Your shitty crypter is written in .NET
3. You don't understand how AntiViruses operate in the kernel.
4. You don't understand what a runpe is
5. You can't code for shit
6. You're not good at math.

So why am I arguing with you? Why should I even bother trying to teach you morons the basics of programming when you can't accurately define what INVALID_HANDLE_VALUE is? (Even though the compiler specifically tells you what it is, regardless of the environment nature you still defy the laws of logic and assume ! Refers to ≤ 0)

Wardow - April 12, 2016, 2:22 am

(Apr 12, 2016 02:18 AM)TERRORISST--- Wrote: [\[CITE\]](#) You keep asking me to help this moron, trust me I've tried.

I'm definitely more competent, and by far more competent than you and this moron will ever be.

You clearly don't know me. "french crypter" Fucking skid.

1. You're using public code for your theme
2. Your shitty crypter is written in .NET
3. You don't understand how AntiViruses operate in the kernel.
4. You don't understand what a runpe is
5. You can't code for shit
6. You're not good at math.

So why am I arguing with you? Why should I even bother trying to teach you morons the basics of programming when you can't accurately define what INVALID_HANDLE_VALUE is?

You shit on other's code, but yet did not post anything of yours, go ahead, skid.

French Products - April 12, 2016, 2:23 am

(Apr 12, 2016 02:18 AM)TERRORISST--- Wrote: [\[CITE\]](#) You keep asking me to help this moron, trust me I've tried.

I'm definitely more competent, and by far more competent than you and this moron will ever be.

You clearly don't know me. "french crypter" Fucking skid.

1. You're using public code for your theme
2. Your shitty crypter is written in .NET
3. You don't understand how AntiViruses operate in the kernel.
4. You don't understand what a runpe is
5. You can't code for shit
6. You're not good at math.

So why am I arguing with you? Why should I even bother trying to teach you morons the basics of programming when you can't accurately define what INVALID_HANDLE_VALUE is? Can I have a proof about about your claiming ? INVALID_HANDLE_VALUE = -1 .

Wardow - April 12, 2016, 10:29 am

Updated the shellcode with latest!

labbepierre - April 14, 2016, 9:03 am

Thank's for sharing your job Wardow

labbepierre - May 9, 2016, 2:44 pm

Hello Wardow , one question , it work with 64 bits or only 32 bits .

Thank's for your reply

Wardow - May 9, 2016, 7:40 pm

(May 9, 2016 02:44 PM)labbepierre Wrote: [\[CITE\]](#) Hello Wardow , one question , it work with 64 bits or only 32 bits .

Thank's for your reply

The shellcode will only run PE32 Executables and will only run under x32 Process.

labbepierre - May 10, 2016, 8:17 am

Ok thank you Wardow for information