Forum:Hack Forums

Thread: WinAPI Hooking with CodeCave (Video)

Menalix - *October 14, 2014, 10:15 pm*

[Video: https://www.youtube.com/watch?v=tiiI4_2psmc]

Got inspirated to do this as I saw this thread: https://hackforums.net/showthread.php?tid=4486586 and thought why not do that with a native api hook.
Hooking native API's with VB is quite a mess compared to how easy it is in C++, but is still possible with not so many lines of code, but you'll need some ASM knownledge or atleast know some C++ to make this any useful.
And sorry for my bad english ^^

The concept of hooking with a codecave is quite simple.
We replace the start of the original function to hook, with a call or jump to an offset to our codecave where we have written our own hookcode.
We do this in order to make it execute our code whenever the original function is called within the remote process.

stefsot - *October 15, 2014, 12:56 am*

I think you should have explained the concept, once you understand how and why it works it's very easy to make it yourself

Menalix - *October 15, 2014, 1:18 am*

(Oct 15, 2014 12:56 AM)stefsot Wrote: *[CITE]* I think you should have explained the concept, once you understand how and why it works it's very easy to make it yourself
I think I explained it quite well, but i guess maybe not then. I tryed a lot to hurry myself, do to the length of the video, first when I made the tutorial it was 40 minutes..... xD
I'll leave an explanation under the video then.

BerryP - *October 15, 2014, 10:12 am*

will this just work for this program ? Because as I know CodeCaves we need free space in the program, so we would have to do this for every taskmanager out there ? Or could we just simply loop trough all processes ?

Peace

Menalix - *October 15, 2014, 1:35 pm*

(Oct 15, 2014 10:12 AM)Maember Wrote: *[CITE]* will this just work for this program ? Because as I know CodeCaves we need free space in the program, so we would have to do this for every taskmanager out there ? Or could we just simply loop trough all processes ?

Peace
All taskmanagers out there, if you want something global you should look into SSDT Hooking (Not something achieveable in vb).
But well you could just run a loop and hook all programs in the syste, but then it would be best to make some hookcode which check PID and such.

(Oct 15, 2014 10:53 AM)Cornflower Blue ???-?— Wrote: *[CITE]* Hahah 'houk', soo funny, it's 'hook',

with a 'o'.

Am sorry.
Do you also think this is copy-pasted? I think AeonHack used OpenProcess in a project..... ?

NETExplorer - *October 15, 2014, 4:38 pm*
What switches are in your keyboard?
Those can't be blue, they are too quiet :P
Im thinking they are either brown or red

Menalix - *October 15, 2014, 6:51 pm*
(Oct 15, 2014 04:38 PM)PatPositron Wrote: *[CITE]* What switches are in your keyboard?
Those can't be blue, they are too quiet :P
Im thinking they are either brown or red
Hahaha, I love that you notice I have mechanical :D
And good guess, it's the CM Storm Rapid-I with brownies :D (I love its back-lighting and small size without numpad: http://hexui.com/mypc.jpg)

NETExplorer - *October 15, 2014, 6:57 pm*
(Oct 15, 2014 06:51 PM)Menalix Wrote: *[CITE]* Hahaha, I love that you notice I have mechanical :D
And good guess, it's the CM Storm Rapid-I with brownies :D (I love its back-lighting and small size without numpad: http://hexui.com/mypc.jpg)
?
I also noticed that your vs window was pretty big, what is your main res?

Menalix - *October 15, 2014, 7:29 pm*
(Oct 15, 2014 06:57 PM)PatPositron Wrote: *[CITE]* ?
I also noticed that your vs window was pretty big, what is your main res?
2560x1440 is my main res, and then I have secondary screen with 1920x1080 is quite nice to have for msdn stuff while coding and such :D

NETExplorer - *October 15, 2014, 7:30 pm*
(Oct 15, 2014 07:29 PM)Menalix Wrote: *[CITE]* 2560x1440 is my main res, and then I have secondary screen with 1920x1080 is quite nice to have for msdn stuff while coding and such :D
Very noice, I am looking to add a 3rd monitor to my current setup :P

Menalix - *October 15, 2014, 7:30 pm*
(Oct 15, 2014 07:30 PM)PatPositron Wrote: *[CITE]* Very noice, I am looking to add a 3rd monitor to my current setup :P
Nice what monitors are you having atm?

NETExplorer - *October 15, 2014, 7:37 pm*
(Oct 15, 2014 07:30 PM)Menalix Wrote: *[CITE]* Nice what monitors are you having atm?
1x 1680x1050
1x 1920x1080

I have an identical 1920x1080 downstairs, I've yet to put it in.
Im looking to have all 3 1920x1080s

Also, I really want that keyboard of yours. My blues are just too loud during the night ?

Ok
Back to ontopic discussion, tuppeh iz gunna g3t mad at uz

CodeAssassin - *October 15, 2014, 7:47 pm*
I really liked your tutorial, Thanks.

It's giving me a great need to go play with asm, so i will!! Looking forward to more tuts like this from you mate ^^

Kudos :3