

Forum:[Hack Forums](#)

Thread: [User mode hook bypass](#)

d3c0mpil3r - December 16, 2012, 9:56 am

Hey guys, visiting HF after a long time.. so thought I might share something.

Anyways, so this is a simple method to bypass user mode hooks.

You know how Hot-patching works? Yeah, a JMP instruction at the start of a function. So, it then executes your custom function.

Now, what it does is, replaces the function prologue i.e.

```
Code MOV EDI, EDI
PUSH EBP
MOV EBP, ESP
```

..more code..

with..

```
Code JMP <some_address>
```

..more code..

The bypass:

Execute the prologue on your own, and THEN jump to your function address + 5. This won't bypass every user mode hook!

Download:

<http://www.mediafire.com/?im28s6fye232zpy>

Usage: [\(Click to View\)](#)

Enjoy!

tweety - December 16, 2012, 10:07 am

This can calculate my mood!?!? OP fix the title lol, also this looks like ASM. This is the .NET section or am I missing something?

d3c0mpil3r - December 16, 2012, 10:18 am

(Dec 16, 2012 11:07 AM)Tweety. Wrote: [\[CITE\]](#) This can calculate my mood!?!? OP fix the title lol, also this looks like ASM. This is the .NET section or am I missing something?

LOL, thanks.

I'm so freaking tired right now.

Yeah, everything is being done in ASM but I made it so you could implement it in a managed language too.

Occulta - December 16, 2012, 10:22 am

A lot of members aren't going to understand this. When you get the chance comment it out.

<http://www.youtube.com/watch?v=lxIufJ650iY>

simonbenyo - December 16, 2012, 11:04 am

i use SYSENTER with my shellcode and fu*k for every ring3 hooks ,,, but nice code thanks ?

d3c0mpil3r - August 10, 2013, 2:04 pm

Wow, I'm so quick to respond I guess.

(Dec 16, 2012 11:59 AM)Salmoneus Wrote: [\[CITE\]](#) Can't you just use system call instruction to bypass user mode hooks?

Yes, but not all APIs have their respective native versions (Zw or Nt). Also, tbh, not everyone would love to use system call.. well.. atleast not like some lazy programmer like me! lol

aCrypt - August 10, 2013, 3:55 pm

So you're basically exporting a basic relative JMP hook from a native dll and expecting .net kids to use it?

get real.

d3c0mpil3r - August 11, 2013, 1:16 am

(Aug 10, 2013 03:55 PM)aCrypt Wrote: [\[CITE\]](#) So you're basically exporting a basic relative JMP hook from a native dll and expecting .net kids to use it?

get real.

It's basically executing the function prologue, then jumping to the function. Hence, any inline function hook is bypassed.

IF the hook is placed somewhere "deep" inside the function, this won't work. But, I've hardly seen anyone doing that. Anyways, it's just something simple one could use to bypass some of the common hooking techniques (IAT, hot-patching, etc).