

Forum:[Hack Forums](#)

Thread: [C++ Making Program Protected \(Protected Mode\)](#)

Meterpreter - March 7, 2016, 3:41 am

Hi guys I've been searching Google for help with this but am coming up short. Could anyone assist me by either giving me some knowledge to doing this, or share a few relevant links?

I don't want to create a dll and inject it into a protected process. Rather, I want to make my program protected itself. To avoid script reading.

Any help will be appreciated. Thank you

morph - March 7, 2016, 3:43 am

(Mar 7, 2016 04:41 AM)Dafty™ Wrote: [\[CITE\]](#) Hi guys I've been searching Google for help with this but am coming up short. Could anyone assist me by either giving me some knowledge to doing this, or share a few relevant links?

I don't want to create a dll and inject it into a protected process. Rather, I want to make my program protected itself. To avoid script reading.

Any help will be appreciated. Thank you

What do you mean by script reading?

Meterpreter - March 7, 2016, 4:12 am

(Mar 7, 2016 04:43 AM)Zymbiotic Wrote: [\[CITE\]](#) What do you mean by script reading?

I mean the algorithms reading my program

?????? - March 7, 2016, 4:53 am

He wants to make his program non decompilable

Meterpreter - March 7, 2016, 4:58 am

(Mar 7, 2016 05:53 AM)Night-fox Wrote: [\[CITE\]](#) He wants to make his program non decompilable Affirmative. Would this mean I would need a MS Certificate? Or would a private certificate work?

Not entirely sure what BE has the right to read. I know they cannot read MS Signed Processes but you cannot sign processes with MS Certs obviously, and you cannot inject into processes signed by MS. -_-

Idk. If I were to self code a game trainer that farms a particular Item using offsets; whose game is backed up BE, would it be undetected? Or detected instantly. If it was momentarily undetected, for say 3 months, I could easily re-write/structure the code, to secure it for another 3 months? Especially if it was 99% private?

Hoodie+ - March 7, 2016, 5:00 am

You need to pack it.

It's simmilar to crypting.

EDIT: I didn't read correctly what OP said.

NTTITON378 - March 7, 2016, 1:21 pm

Acquire UAC Access, Enable test signing, Remove water mark, Load driver, use documented methods (obcallback) to protect your process by intercepting any requests to open a handle for your process OR disable PG timer, which in my opinion isn't a good idea, and demonstrates the inability to work around patch guard (incompetence)

otherwise have fun with system wide injections :) Which still won't protect your process against me.

Rule 1: Code obscurity isn't protection.

(Mar 7, 2016 05:53 AM)Night-fox Wrote: [\[CITE\]](#) He wants to make his program non decompilable
No, he does not.

(Mar 7, 2016 05:58 AM)Dafty™ Wrote: [\[CITE\]](#) Affirmative. Would this mean I would need a MS Certificate? Or would a private certificate work?

Not entirely sure what BE has the right to read. I know they cannot read MS Signed Processes but you cannot sign processes with MS Certs obviously, and you cannot inject into processes signed by MS. --

Idk. If I were to self code a game trainer that farms a particular Item using offsets; whose game is backed up BE, would it be undetected? Or detected instantly. If it was momentarily undetected, for say 3 months, I could easily re-write/structure the code, to secure it for another 3 months? Especially if it was 99% private?

you cannot inject into processes signed by MS. --
?