

Forum:[Hack Forums](#)

Thread: [How to implement an anti-debugger on my crypter?](#)

invisible_hack2 - August 4, 2020, 3:31 pm

I mean, do I have to patch the binary? , I really haven't found any example about this, my crypter is pretty basic encrypts and decrypts using XOR

thank you anyways????

spiderfruit - August 5, 2020, 1:38 am

(Aug 4, 2020 03:31 PM)invisible_hack2 Wrote: [\[CITE\]](#) I mean, do I have to patch the binary? , I really haven't found any example about this, my crypter is pretty basic encrypts and decrypts using XOR

thank you anyways????

so many techniques on anti-debugging (google alkhaseer irc) regarding the 'how' is up to you- generally speaking those checks (anti XX) should be implement in your stub before it decrypt and executes the binary

Freak_OG - August 5, 2020, 3:22 am

use a call to kernel32.dll and isdebuggerpresent and checkremotedebuggerpresent, these are the best methods I use them, you shouldnt have anyone debugging your crypter after that my friend!

unless they open x64dbg and edit the return values of those functions but its pretty hard and takes some skill.

Pernat1y - August 5, 2020, 8:08 am

(Aug 5, 2020 03:22 AM)Freak_OG Wrote: [\[CITE\]](#) you shouldnt have anyone debugging your crypter after that my friend!Cool story.

<https://github.com/x64dbg/ScyllaHide>

invisible_hack2 - August 5, 2020, 9:50 am

(Aug 4, 2020 03:31 PM)invisible_hack2 Wrote: [\[CITE\]](#) I mean, do I have to patch the binary? , I really haven't found any example about this, my crypter is pretty basic encrypts and decrypts using XOR

thank you anyways????

(Aug 5, 2020 01:38 AM)spiderfruit Wrote: [\[CITE\]](#) so many techniques on anti-debugging (google alkhaseer irc) regarding the 'how' is up to you- generally speaking those checks (anti XX) should be implement in your stub before it decrypt and executes the binary

thanks so i just have to add some anti-debugging technique to my stub? no need to patch the binary.

Freak_OG - August 5, 2020, 7:32 pm

(Aug 5, 2020 09:50 AM)invisible_hack2 Wrote: [\[CITE\]](#) thanks so i just have to add some anti-debugging technique to my stub? no need to patch the binary.

No need to patch the binary bro. ?

3DES - August 5, 2020, 11:21 pm

(Aug 5, 2020 03:22 AM)Freak_OG Wrote: [\[CITE\]](#) use a call to kernel32.dll and isdebuggerpresent and checkremotedebuggerpresent, these are the best methods I use them, you shouldnt have

anyone debugging your crypter after that my friend!

unless they open x64dbg and edit the return values of those functions but its pretty hard and takes some skill.

"Prettt hard" lmao. Easiest thing ever, theres even plugins to automate this.

HRRHHRRH - August 6, 2020, 12:44 am

If you have to ask this you probably should not yet be attempting to make a "Crypter".

There's tens to hundreds of public methods you can use, and probably tens more that are not public. All of them are created based on the knowledge of how a debugger works, how the operating system works, etc. You need real knowledge of your computer's internals.

Even then, if you just have a couple of debug checks in your software and that's it, someone could very easily stop them from executing at all trough 10 different hook methods or 10 different patch methods.

invisible_hack2 - August 7, 2020, 11:14 am

(Aug 5, 2020 11:21 PM)3DES Wrote: [\[CITE\]](#) "Prettt hard" lmao. Easiest thing ever, theres even plugins to automate this.

I know , i thought i needed to patch the binary

4Txe4y33C9zvNhMj - August 7, 2020, 12:30 pm

Just implement this, take a look at what malware does and what malware analysts do to bypass those checks

https://anti-reversing.com/Downloads/Anti-Reversing/The_Ultimate_Anti-Reversing_Reference.pdf

H4x10r - August 15, 2020, 7:40 am

Best way to get into this is

<https://github.com/LordNoteworthy/al-khaser>

<https://github.com/cetfor/AntiDBG>