

Forum:[Hack Forums](#)

Thread: [\[Question\] Static call vs Dynamic call against AntiVirus](#)

Praet0rian - January 30, 2017, 12:12 pm

I've been curious and I can't seem to find an answer to this question, does it matter if you dynamically link the functions you want or statically link them when it comes to anti viruses detecting them? for example, if I wanted to use Qt's classes on a malware, would it be better to statically link or dynamically link?

first thread in this forum, after being here for 2 weeks and got a a lucky clover :)

Zyklon A - January 30, 2017, 1:28 pm

It doesn't matter! AVs have callbacks on certain functions and based on that they determine if your file is malicious. It doesn't matter if you call the function dynamically, well it does if you want to make your file undetected at scantime but you would need to encrypt/obfuscate/encode the function name/s.

Praet0rian - January 31, 2017, 6:16 am

(Jan 30, 2017 02:28 PM)Zyklon A Wrote: [\[CITE\]](#) It doesn't matter! AVs have callbacks on certain functions and based on that they determine if your file is malicious. It doesn't matter if you call the function dynamically, well it does if you want to make your file undetected at scantime but you would need to encrypt/obfuscate/encode the function name/s.interesting, but how would I use the libraries I want then? but surely they cannot thing that because I use a 3rd party lib called QT then it is most likely malware, tons of programs use QT, most of them are legitmate, what would you suggest? I would prefer the functions being statically linked because then it will be far less messier, all-in-one payload

Zyklon A - January 31, 2017, 8:00 am

(Jan 31, 2017 07:16 AM)Praet0rian Wrote: [\[CITE\]](#) interesting, but how would I use the libraries I want then? but surely they cannot thing that because I use a 3rd party lib called QT then it is most likely malware, tons of programs use QT, most of them are legitmate, what would you suggest? I would prefer the functions being statically linked because then it will be far less messier, all-in-one payload Why would you use QT to develop a malware? Dont use third party libs, they just make your malware bloated.

0xDEAD10CC - January 31, 2017, 9:27 pm

Furthermore, why would you need Qt? It's mainly a GUI framework... Are you intending to do give the end user a nice UI element for your malware that they most likely don't want on their PC? ???

Good luck with small filesize when linking Qt statically too, you'll be in the Mb range without a doubt.

maldev0 - February 1, 2017, 7:05 am

try to avoid standard c libs and implement the essential functions (memcpy/memset) on your own, which is not hard.

u can create a custom GetProcAddress function in order to dynamically call the api's, in a "stealth" way. You'll need to understand how the PE structure works, that's an easy task.

Praet0rian - February 1, 2017, 12:08 pm

(Jan 31, 2017 10:27 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Furthermore, why would you need Qt? It's mainly a GUI framework... Are you intending to do give the end user a nice UI element for your malware that they most likely don't want on their PC? ???

Good luck with small filesize when linking Qt statically too, you'll be in the Mb range without a doubt.

I'm mostly interested in crypto and networking, Qt was merely an example

morph - February 2, 2017, 9:25 am

I would statically link all libraries so it's just one file.

Praet0rian - February 2, 2017, 11:26 am

(Jan 31, 2017 10:27 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Furthermore, why would you need Qt? It's mainly a GUI framework... Are you intending to do give the end user a nice UI element for your malware that they most likely don't want on their PC? ???

Good luck with small filesize when linking Qt statically too, you'll be in the Mb range without a doubt.

Also, I don't think size will be a problem, UPX has compression rate of about 70% or so...

0xDEAD10CC - February 2, 2017, 11:31 am

(Feb 2, 2017 12:26 PM)Praet0rian Wrote: [\[CITE\]](#) Also, I don't think size will be a problem, UPX has compression rate of about 70% or so...

If size was always unimportant, then good luck with lots of code injection methods and UPX.

If you're unlucky enough to end up with a size like what this guy had:

<http://stackoverflow.com/q/25426895/6264524> 160MB.. 70% doesn't mean a whole lot anyways.

Praet0rian - February 2, 2017, 11:54 am

(Feb 2, 2017 12:31 PM)0xDEAD10CC Wrote: [\[CITE\]](#) If size was always unimportant, then good luck with lots of code injection methods and UPX.

If you're unlucky enough to end up with a size like what this guy had:

<http://stackoverflow.com/q/25426895/6264524> 160MB.. 70% doesn't mean a whole lot anyways.

ahaha holy shit, poor fella

but yeah I don't intend to use Qt anyway, like I posted above: it was merely an example.

I need to use networking and cryptography classes in C++ for a virus [educational purposes of course :)], so I was wondering if this was going to be a problem, the standard shit you get with windows with Winsock is annoying, especially if I want to make a server, plus encryption is a big deal, I tried using OpenSSL but after trying it it has tons of memory leaks and it's in C...

Zyklon A - February 2, 2017, 12:25 pm

(Feb 2, 2017 12:54 PM)Praet0rian Wrote: [\[CITE\]](#) ahaha holy shit, poor fella

but yeah I don't intend to use Qt anyway, like I posted above: it was merely an example.

I need to use networking and cryptography classes in C++ for a virus [educational purposes of course :)], so I was wondering if this was going to be a problem, the standard shit you get with windows with Winsock is annoying, especially if I want to make a server, plus encryption is a big deal, I tried using OpenSSL but after trying it it has tons of memory leaks and it's in C...

Just use WINAPI. Windows has the cryptoapi that you can use and ditch the OpenSSL.

Also C++ is an overkill for malware, just stick with C. All WINAPI is made for C.

This is if you are targeting windows.

0xDEAD10CC - February 2, 2017, 2:41 pm

^ Not necessarily if you want cross-platform. WinAPI isn't. If you're on Windows though you can use WinInet or WinHTTP, in addition to the Crypto API. You can reduce binary size by avoiding CRT and using Windows functions.

<https://support.microsoft.com/en-us/help/99456/win32-equivalents-for-c-run-time-functions>

Praet0rian - February 3, 2017, 1:21 am

(Feb 2, 2017 03:41 PM)0xDEAD10CC Wrote: [\[CITE\]](#) ^ Not necessarily if you want cross-platform. WinAPI isn't. If you're on Windows though you can use WinInet or WinHTTP, in addition to the Crypto API. You can reduce binary size by avoiding CRT and using Windows functions.

<https://support.microsoft.com/en-us/help/99456/win32-equivalents-for-c-run-time-functions>

Yes I know of that CRT trick, did it once and got down to a few kilobytes most of the program was just filled with 0 bytes padding and I couldn't manage to remove it, now I don't know much about this part, but won't removing CRT also remove some features that protect the program from attacks like cookies? talking about Visual Studio, I know to "ignore default library" and use the other entrypoint that's called winCRTmain or something like that.

(Feb 2, 2017 01:25 PM)Zyklon A Wrote: [\[CITE\]](#) Just use WINAPI. Windows has the cryptoapi that you can use and ditch the OpenSSL.

Also C++ is an overkill for malware, just stick with C. All WINAPI is made for C.

This is if you are targeting windows.

I would like to stick with C++ because of the OOP, maintaining a large project, for me at least, is much easier in OOP than in C.

I know that there are some networking libraries that make communication much simpler and some even come with encryption, so I can focus on the other aspects of the program rather than re-inventing the wheel, which is why I am asking this question.

Qmz_ - February 3, 2017, 12:16 pm

Try both and test on a VM, runtime and scantime. That's the way to test it, if you don't know, or find the answers.

When done, post here the results. :)

caiveman - February 3, 2017, 9:06 pm

(Jan 30, 2017 02:28 PM)Zyklon A Wrote: [\[CITE\]](#) It doesn't matter! AVs have callbacks on certain functions and based on that they determine if your file is malicious. It doesn't matter if you call the function dynamically, well it does if you want to make your file undetected at scantime but you would need to encrypt/obfuscate/encode the function name/s.

encrypting function names does absolutely nothing unless you are compiling in debug mode (why the fuck)

Praet0rian - February 4, 2017, 12:24 am

(Feb 3, 2017 10:06 PM)caiveman Wrote: [\[CITE\]](#) encrypting function names does absolutely nothing unless you are compiling in debug mode (why the fuck)

what do you mean? I think he means to encrypt the strings that are sent to GetModuleHandle

and GetProcAddress so that an AV cannot tell in scantime what functions are being called.

Zyklon A - February 4, 2017, 4:18 am

(Feb 3, 2017 10:06 PM)caiveman Wrote: [\[CITE\]](#) encrypting function names does absolutely nothing unless you are compiling in debug mode (why the fuck)

Dont try to be a smartass and read my post again. They will still be shown in plain text.

Praet0rian - February 4, 2017, 4:53 am

(Feb 4, 2017 05:18 AM)Zyklon A Wrote: [\[CITE\]](#) Dont try to be a smartass and read my post again. They will still be shown in plain text.

I hve read that you can implement your own version of GetProcAddress, is that possible and is it a good idea?

Deadbyte - February 4, 2017, 9:31 am

I do not think the choice is relevant in this case.

Russ. - February 4, 2017, 9:13 pm

You wanna create ransomware for educational pruposes only *WINK WINK*. Honestly not that hard to do if you want ti very simple (ex: encrypt x files -> store keys on web side -> generate hwid of computer (like customer databse) -> send all to your website -> pop up cmd(doin this very simple) -> message (say blah blah heres my btc) -> countdown timer -> ... wait nvm this is to complicated I can shorten this

excrypt -> data to panel -> pop up cmd -> "email 1337ransom@lolz.com to get your files back, fee is x btc" -> once paid either decrypt files or be a dick and don't

kinda drunk so bare with me for stupid post.

Praet0rian - February 5, 2017, 7:34 am

(Feb 4, 2017 10:13 PM)Russ. Wrote: [\[CITE\]](#) You wanna create ransomware for educational pruposes only *WINK WINK*. Honestly not that hard to do if you want ti very simple (ex: encrypt x files -> store keys on web side -> generate hwid of computer (like customer databse) -> send all to your website -> pop up cmd(doin this very simple) -> message (say blah blah heres my btc) -> countdown timer -> ... wait nvm this is to complicated I can shorten this

excrypt -> data to panel -> pop up cmd -> "email 1337ransom@lolz.com to get your files back, fee is x btc" -> once paid either decrypt files or be a dick and don't

kinda drunk so bare with me for stupid post.

fbi plz...

Imao, how is this relevant

Russ. - February 5, 2017, 10:33 am

(Feb 5, 2017 08:34 AM)Praet0rian Wrote: [\[CITE\]](#) fbi plz...

Imao, how is this relevant

Fuck if I knew at the time?