

Forum:[Hack Forums](#)

Thread: [protect game application triggers AVs and WD](#)

valance1337 - July 14, 2024, 8:25 am

Hi all and sorry if this is not the right section.

As the title says, what I'm trying to achieve is to somehow protect my game application (.exe) against reverse engineers and cheaters.

Little context, I'm hosting an MMORPG private server, and many public cheats work on almost every server. If they get patched, cheat devs usually in a few days try to adjust that.

The most efficient way I managed to find to counter them is to use Themida or VMProtect (it's not 100% guaranteed, but it keeps a lot of cheaters away and makes devs life harder).

Using Themida is a great solution imho because you can use VM Macros to virtualize vital functions + use xbundle to embed other vital files which will be harder to dump and extract.

Here's the point, as you know, Themida triggers many false positives. I honestly don't care about them, but the most annoying is Windows Defender since 90% of the player base uses Windows Defender and probably don't even know how add that as exception.

Submitting each time the .exe for review is not a viable solution, because I'm planning to release updates almost each week, and these are the timings that Microsoft takes to review your submitted file.

PS: without Themida/VMProtect the file is clean (1/74 on VT), with Themida it's 17/74 (WD included).

Again, I'm not doing any blackhat/illegal activity, just trying to help my user base keeping away cheaters as best as i can, and at the same time not having to tell me to add everytime the application to the exceptions.

Some people told me the "best" solution is to buy a code signing certificate, but 300\$ for a certificate for 1 year is a cost I can't and don't want to afford.

Any help or suggestion is highly appreciated

Cheers
Valance

__Digital__ - July 14, 2024, 9:08 am

(Jul 14, 2024 08:25 AM)valance1337 Wrote: [\[CITE\]](#) Hi all and sorry if this is not the right section.

As the title says, what I'm trying to achieve is to somehow protect my game application (.exe) against reverse engineers and cheaters.

Little context, I'm hosting an MMORPG private server, and many public cheats work on almost every server. If they get patched, cheat devs usually in a few days try to adjust that.

The most efficient way I managed to find to counter them is to use Themida or VMProtect (it's not 100% guaranteed, but it keeps a lot of cheaters away and makes devs life harder).
Using Themida is a great solution imho because you can use VM Macros to virtualize vital functions + use xbundle to embed other vital files which will be harder to dump and extract.

Here's the point, as you know, Themida triggers many false positives. I honestly don't care about them, but the most annoying is Windows Defender since 90% of the player base uses Windows Defender and probably don't even know how to add that as an exception.

Submitting each time the .exe for review is not a viable solution, because I'm planning to release updates almost each week, and these are the timings that Microsoft takes to review your submitted file.

PS: without Themida/VMProtect the file is clean (1/74 on VT), with Themida it's 17/74 (WD included).

Again, I'm not doing any blackhat/illegal activity, just trying to help my user base keeping away cheaters as best as I can, and at the same time not having to tell me to add everytime the application to the exceptions.

Some people told me the "best" solution is to buy a code signing certificate, but 300\$ for a certificate for 1 year is a cost I can't and don't want to afford.

Any help or suggestion is highly appreciated

Cheers
Valance

Yes if your application is legit and not doing anything wrong why not spend the money on code signing ? It's going to be your best bet. Otherwise you will be wasting your time and effort on something in which will not give you 100% credibility.

valance1337 - July 14, 2024, 9:29 am

(Jul 14, 2024 09:08 AM) __Digital__ Wrote: [\[CITE\]](#) Yes if your application is legit and not doing anything wrong why not spend the money on code signing ? It's going to be your best bet. Otherwise you will be wasting your time and effort on something in which will not give you 100% credibility. the amount of money required probably won't be covered by donations.

One more question, is it possible to purchase "anonymously" these code signing certs?

notagh0st - July 14, 2024, 4:30 pm

Could you do your Themida/VMProtect, then take the resulting binary, encrypt it or XOR it or something, and then write a wrapper that unravels it and loads it into memory (a lot of malware works like this)? I'm not sure if this will still trigger MS Defender and the likes, but it might be worth a shot. I know a lot of defender alerts occur with static file analysis, but I haven't done much research into the dynamic file analysis. You could write a proof of concept that you could test with pretty easily.

valance1337 - August 18, 2024, 8:20 am

(Jul 14, 2024 04:30 PM) notagh0st Wrote: [\[CITE\]](#) Could you do your Themida/VMProtect, then take the resulting binary, encrypt it or XOR it or something, and then write a wrapper that unravels it and loads it into memory (a lot of malware works like this)? I'm not sure if this will still trigger MS Defender and the likes, but it might be worth a shot. I know a lot of defender alerts occur with static file analysis, but I haven't done much research into the dynamic file analysis. You could write a proof

of concept that you could test with pretty easily.

sorry for my late reply and thank you. it seems a very interesting combo, however I believe this is beyond my skills xD but I will definitely give it a try with some AI help