

Forum:[Hack Forums](#)

Thread: [Is it possible to use a virtual CPU to emulate an internal cheat?](#)

SIM-4828712 - December 14, 2020, 7:40 pm

Hi, today I thought of something special. Anticheats, such as BE/EAC/Vanguard/VAC all commonly look through memory to find executable pages outside of known modules, to detect internal cheats. This can be done with NtQueryVirtualMemory, or reading dribase and walking paging tables. What if I could allocate read/write only memory, and use a virtual CPU to emulate the instructions in the mapped image. The code would be executing without executing, "ghost executing". This would bypass almost all internal detection vectors, including executable pages detection and stack walking. If this is actually possible, It would be an internal cheat that bypasses every single anticheat in existence.

I know that the main problem with this idea is the speed, instruction emulation has TERRIBLE speed, but if you look at code virtualizers such as vmprotect/thermida and interpreted languages such as python, maybe a virtual code emulator might have reasonable speed with optimization. (I have no knowledge of how to optimize a full instruction emulator)

If anyone else knows about emulation/virtualization or anticheat bypassing that's great. let's discuss, I think emulation/virtual execution is a fascinating concept.

TLDR I wonder if it's possible to fully emulate a read/write only internal cheat image

HFDone - December 15, 2020, 4:03 am

you can look into game hacking forums theres many good tuts that explains how to pass anti cheat search google "Anti Cheat Bypassing" cant post forums link in hf

cghhhhasd - December 16, 2020, 2:33 am

That's not how CPU emulators work.

You either execute the instructions or you don't If you don't, nothing will happen, if you do, it can be picked up on.

DeadCode - December 28, 2020, 12:17 pm

Even if a virtual CPU were to emulate your cheat (see VMProtect/Themida), the memory of the original game process will still be changed, and anti-cheats such as EAC will still detect the memory change.