

Forum:[Hack Forums](#)

Thread: [Tips on Memory based application I can create](#)

passwords - May 9, 2017, 10:02 pm

So you know how game hacking uses offsets etc and pretty much lots of memory adress stuff..
I want to expand my knowledge on Memory mapping and anything with memory really, how a process works
Offsets, 0x values etc (Not even sure what the 0x values are called, adresses?)

What applications do you recommend me doing?

I could continue game hacking but I want to expand as I said.

Also if you have any sources of good information I would appriciate it alot, like PDF's, forums, anything really!

I would highly appriciate it! ?

Have a great day programmers!

Random Arab Girl - May 10, 2017, 12:48 am

gonna comment so i can come back later, also looking for something like this.

tomboy182 - May 10, 2017, 1:31 am

I suggest looking at the intel manuals for virtual addressing. This is a type of memory model that introduces using virtual addresses with your physical memory (page tables, page directories) This prevents memory segmentation, and more importantly allows each process to have its memory space.

Once you're done with the basics you can endeavor on your "Game hacking" with ollydbg & Cheat Engine & windbg & IDA

Most game hacking is done using CE, since CE has alot of features used to find objects in memory, of which includes base pointers.

IDA is more of a primitive disassembler used to find objects on an executable that's been dumped from memory.

atom0s - May 10, 2017, 11:36 pm

Some tools commonly used in game hacking:

- Cheat Engine / Artmoney / TSearch
- OllyDbg (or x64Dbg)
- IDA

A hex editor I recommend using:

- 010 Editor (Binary templates are a godsend.)

API to learn / reference:OpenProcess

ReadProcessMemory

WriteProcessMemory

VirtualAllocEx

VirtualProtectEx

CreateToolhelp32Snapshot (Or look into the PSAPI equivalents.)Process32First

Process32Next

Module32First

Module32Next

Thread32First

Thread32Next

CreateRemoteThread

The above are the most commonly used API in terms of game hacking from a remote standpoint (non-injected). Keep in mind usage of these depends on the target. In some cases you may need to use lower-level Nt calls or even a driver depending on the protection of the game, if any.

If you are injected, then you do not need most of this since you will instead have direct access to the process and its memory.

There are a lot of open source projects that cover memory related game hacking stuff that you can find on Github. Things like WhiteMagic/BlackMagic, Cheat Engines source code, and so on. There are a handful of open source injectors as well for both native and managed injection.

severos - May 11, 2017, 2:24 am

0x values are written in hexadecimal, people use them for easier reference to specific memory locations that writing in decimal system.

As for the hacking part I have no idea, so keeping an eye on this thread for later.