

Forum:[Hack Forums](#)

Thread: [Need resources for learning about injections](#)

Abducted - February 19, 2020, 5:48 am

Hey,

Do any of you have any experience with or know any good references to resources where I could learn more about C++ injections to running processes? Or malware development resources in general?

Shisho - February 19, 2020, 9:34 am

At the moment I think process hollowing and process doppelganging are the de-facto injection methods involving trusted process hijacks. The latter also introduces a locking system in the form of NTFS transactions which makes the memory unreadable until the transaction is complete which will roll itself back and make it look like nothing ever happened in the first place.

A quick Google search can find you numerous PE loaders written to load arbitrary code into 32-bit or 64-bit processes. rohitab seems to have a lot of capable malware programmers that release their code for free and is a good place to find some examples to analyze.

ModernJS - February 19, 2020, 10:11 am

Is this process injection also possible on linux with elf binaries?

Shisho - February 19, 2020, 10:42 am

(Feb 19, 2020 11:11 AM)ModernJS Wrote: [\[CITE\]](#) Is this process injection also possible on linux with elf binaries?

On Linux you could likely just fork, exec, SIGSTOP and then replace the memory of the new process and then inject your shellcode or ELF file and then rebuild the import tables and addresses to mimic process hollowing.

ModernJS - February 20, 2020, 10:11 pm

(Feb 19, 2020 11:42 AM)Shisho Wrote: [\[CITE\]](#) On Linux you could likely just fork, exec, SIGSTOP and then replace the memory of the new process and then inject your shellcode or ELF file and then rebuild the import tables and addresses to mimic process hollowing.

Yup you're right

<https://security.stackexchange.com/questions/153829/equivalent-of-windows-process-hollowing-on-linux-unix-macos>

3DES - February 21, 2020, 2:01 am

Google has all the information in the world.