

Forum:[Hack Forums](#)

Thread: [Process Manipulation: A Technique for Stealthy Malware Evasion](#)

Aeon - September 4, 2023, 8:03 am

"Process Manipulation: A Technique for Stealthy Malware Evasion"

Process manipulation, a favored technique employed by malware to skirt detection, hinges on the injection of malevolent code into a genuine process. This artful stratagem entails the inception of a fresh instance of a legitimate process, eventually superseding its authentic code with the nefarious payload.

The process unfolds as follows:

CreateProcess: Launches the process in a suspended state, with the CreationFlag parameter set at 0x0000 0004.

GetThreadContext: Retrieves the context of the designated thread within the process.

ZwUnmapViewOfSection: Effectively unmaps a designated section's view from the virtual address space of the target process.

VirtualAllocEx: Allocates memory within the suspended process's address space.

WriteProcessMemory: Transfers data from the Portable Executable (PE) file into the newly allocated memory space within the suspended process.

SetThreadContext: Adjusts the EAX register to point to the entry point of the written executable.

ResumeThread: Resumes execution of the suspended process's thread, thereby initiating the malicious payload.

If you could please give me a quick love it would mean everything to me :) will also give one back if you comment on my other post "Quick love for quick love"!