

Forum:[Hack Forums](#)

Thread: [Explorer.exe imports CreateProcessW, but doesnt use IAT address to access it?](#)

Tr0jandog - September 9, 2019, 9:49 pm

Hello guys, I'm a student trying to learn hooking, right now trying to hook explorer to get notified when a new process gets created (please let me know if there is any better method in userland)

i successfully hooked the task manager in win 10 and 7, 64 bit, to hide a process

now the thing is, that worked because NtQuerySystemInformation was inside the IAT of task manager in both 7 and 10, so it did import it (this also meant windows own binaries do link up against ntdll.lib so they can use its functions directly without getProcAddress)

now there is no NtCreateProcess or CreateProcessInternalW in the explorer.exe's IAT! (right now trying with windows 7) and only CreateProcessW, and this means it has to be using it, otherwise why would the compiler put it in the IAT? why doesnt explorer have NtCreateProcess inside its IAT unlike task manager which does have NtQuery, and still doesn't use one that it does import (CreateProcessW)

but the problem is, it doesn't get used from IAT, it does gets called but it doesnt get the address from IAT and doing xref in xdbg didnt give any valid info

so why is this happening? why is explorer.exe importing it but not using it via IAT?

thanks in advance!

YouthInAsia - September 10, 2019, 2:57 am

NtCreateProcess is an undocumented function. It doesn't need to be in the IAT.

Tr0jandog - September 10, 2019, 5:46 am

(Sep 10, 2019 02:57 AM)YouthInAsia Wrote: [\[CITE\]](#) NtCreateProcess is an undocumented function. It doesn't need to be in the IAT.

That makes sense, so another question : generally when i can do a IAT hooking, it is preferred compared to inline hooking, right? in terms of AV evasion, which of them is better?

__arkr - September 10, 2019, 8:36 am

<http://www.catch22.net/tuts/undocumented-createprocess>

Here's this dudes blog regarding CreateProcess and some undocumented bits

Tr0jandog - September 10, 2019, 11:47 am

(Sep 10, 2019 08:36 AM)__arkr Wrote: [\[CITE\]](#) [Undocumented CreateProcess - Catch22](#)

Here's this dudes blog regarding CreateProcess and some undocumented bits

thanks that was a good read.