

Forum:[Hack Forums](#)

Thread: [How can hiding process .exe from task manager win10?](#)

hoangdatcm89 - November 24, 2018, 11:42 am

i have a question, how i can hide process .exe running from task manager? ? ? ?

PurpleMongoose - November 24, 2018, 3:14 pm

(Nov 24, 2018 12:42 PM)hoangdatcm89 Wrote: [\[CITE\]](#) i have a question, how i can hide process .exe running from task manager? ? ? ?

Hello hoangdatcm89,

My name is PurpleMongoose, I hope I can help you solve this problem.

One solution is to subvert your program into running as a Window's service rather than an independently compiled .exe program. This will assure that during run-time the "program" is not showing up under task manager other than in the services tab where most people aren't familiar with what is what anyway. Another solution would be to rewrite your code and use Windows against itself, by this I mean using hooks into the kernel.

Why would I change it to run as a service? This would be the easiest and most reliable option as you may not be able to fully hide it from a diligent user but you can take away local admin privileges in services. Doing so would mean that the user infected would not be able to close the program normally and would have to work harder to get rid of it. If you are fully serious on creating some type of rootkit or mining software, I suggest learning subclassing and hooking as they will get you much farther.

I hope I was able to nudge you closer to doing some personal research and overcoming your obstacle. Remember, hiding is harder than seeking. You must put in the work to get the result you desire, don't give up and keep learning!

~PurpleMongoose

Mr. Kim - November 25, 2018, 1:04 pm

Try hooking NtQuerySystemInformation in NTDLL.DLL. In theory you should be able to filter our your process from the list that way, though I've never tried this personally.

spiderfruit - November 26, 2018, 12:27 pm

(Nov 24, 2018 12:42 PM)hoangdatcm89 Wrote: [\[CITE\]](#) i have a question, how i can hide process .exe running from task manager? ? ? ?

you can use dkom- hiding your process by manipulating activeprocesslink in eprocess structure (on win10 you should disable patchguard)

qtkite - December 4, 2018, 3:33 am

Another idea is allocating memory in another program - that isn't protected and running your code there using injection.

jammy47 - December 6, 2018, 10:37 am

process hollowing! start process in suspended state and inject code. check rohitab.

Mr. Kim - December 6, 2018, 10:43 am

(Dec 6, 2018 11:37 AM)jammy47 Wrote: [\[CITE\]](#) process hollowing! start process in suspended state and inject code. check rohitab.

I could be wrong, but I don't think that's what OP is looking for. Process hollowing doesn't really hide a process, it just makes it appear as though it's a different process. I think OP wants to remove a process from the list of processes task manager shows.

jammy47 - December 6, 2018, 10:59 am

(Dec 6, 2018 11:43 AM)Mr. Kim Wrote: [\[CITE\]](#) I could be wrong, but I don't think that's what OP is looking for. Process hollowing doesn't really hide a process, it just makes it appear as though it's a different process. I think OP wants to remove a process from the list of processes task manager shows.

Ya you are right on this. It doesn't hide the process, just difficult to detect and may be hooking ntquerysysteminformation is what he wants to go for or a kernel mode hook.

F1r3w - December 9, 2018, 3:07 am

So many ways/alternatives:

- hijacking the task manager process
- user mode hooking
- kernel mode hooking
- DKOM
- hypervisor technology

Mr. Kim - December 9, 2018, 1:17 pm

(Dec 9, 2018 04:07 AM)F1r3w Wrote: [\[CITE\]](#) So many ways/alternatives:

- hijacking the task manager process
- user mode hooking
- kernel mode hooking
- DKOM
- hypervisor technology

I'm not an expert on the NT kernel by any stretch of the imagination, but doesn't hooking kernel functions on x64 cause a kernel panic?