

Forum:[Hack Forums](#)

Thread: [hide, protect, kill process in windows task manager](#)

nikau6 - January 10, 2015, 6:26 am

Hi everybody. English is not my first language so sorry for the errors I could make. Don't know too if I'm in the good rubric. My question is about windows API.

I have three questions :

- 1 : How to hide a process in the task manager ?
- 2 : How to protect a process in the task manager, as the anti-virus do ?
- 3 : How to kill a protected process in the task manager ?

I'm not asking you to tell me exactly how to do but to give me indices, to tell me where to start, where to search.

Thanks

Sakuto - January 11, 2015, 12:31 pm

You should probably post in the hacking section, you will get more answer.

nikau6 - January 11, 2015, 5:46 pm

Ok, I'll do that. Thanks for your answer.

Mr. Dr. Prof. Patrick - January 11, 2015, 5:50 pm

Google rootkit, read a few of the sources and you will realize that the topic is much more complicated than you thought, especially if you want anti-virus level persistence

nikau6 - January 12, 2015, 8:30 am

Thanks. I'm going to start by simply hide a process in task manager. After a search on google, It seems that it can be done by hooking the partially unreferenced 'NtQuerySystemInformation' function.

It seems too that you can hide a process with 'PsLookupProcessByProcessId' by deleting your process struct from the linked list it retrieves. Doesn't seem really hard. Going to try like that first.