

## Forum:[Hack Forums](#)

Thread: [Intercepting explorer.exe processes before they run](#)

**Fack you in particular** - May 3, 2015, 4:55 am

So when a user goes to explorer.exe (documents, pictures, etc.) and hits an item there, my program should intercept that and decide whatever happens.

I'm not totally helpless. I have a solution setup, but I reckon it's really shitty, and there must be a better way using hooking or something.

Anyways, here's my current solution:

I have a very broad WMI query: `SELECT * FROM __InstanceOperationEvent WITHIN 1 WHERE TargetInstance ISA 'Win32_Process'`

This is fed into an event listener, and then an event is fired everytime something fits that query.

Then, I'd close whatever process down that is (considering it's not owned by system or a well known process such as `dllhost.exe`), and then I'd do whatever I want.

Problem is WMI is horribly CPU expensive, and slow. Which in turn means the user will see their program flash for a second, then close.

Has anyone dealt with this before, and if so, what was your solution?

**Zettabit** - May 3, 2015, 11:03 am

If you're trying to program a so called "rootkit" in .NET, this is not the way to go about it.

**N3w8i3H4ck3r** - May 3, 2015, 11:09 am

Yeah, Malwarebytes Anti-Exploit or any other behavioural analysis type antivirus-antimalware would just block it, you're better off with a ring3 rootkit (ring3 because thats the lowest u can go with VB (i think))

**Fack you in particular** - May 4, 2015, 8:59 am

Right. I'm not looking for a rootkit. As far as I understand (from reading), rootkits have the effect of hiding your process in any task list, and from the registry.

I can't see how anybody reached the conclusion that is what I'm trying to achieve. I never even mentioned anything remotely in that gray sort of area.

But, what we're getting at is: It's impossible for .NETs hooks to do?

**N3w8i3H4ck3r** - May 4, 2015, 1:21 pm

Some people would categorize intercepting kernel level stuff as the gray area.

We all understand what you want to do but obobviously u don't.

This is deeper than VB (VB Is categorized as a "high level" language)

U need to go to C++ or Assembly level

(i may be completley wrong because i never went that deep, i only know c# and abit of IL/Assembly.)

From what i know u need to intercept windows api calls

(Something like this: <http://www.codeproject.com/Articles/2082/API-hooking-revealed> )

