

Forum:[Hack Forums](#)

Thread: [ANTI KILL PROCESS HACKER \[SR\] VB.NET API](#)

xVipX - April 20, 2015, 12:13 pm

hello today i have coding simple class to bypass process hacker by found window visible & child & setwindowtext & enable button and use timer very easy !

image :)

[img]http://up.dev-point.com/uploads1/cda83ae148cf1.gif[/img]

class

<http://pastebin.com/wnZC5T2G>

use :

Code Dim x As New prote

x.pass()good luck

EagleEye - April 20, 2015, 12:15 pm

nice share good code btw , its good way ... i may use it in my future projects

Only3 - April 20, 2015, 12:19 pm

what normal person do when he see that his process hacker doesnt work

LethalNET - April 20, 2015, 12:21 pm

this could be done to task manager too, winapi is very useful.

good work op although the code could be improved its a unique release :)

xVipX - April 20, 2015, 12:54 pm

(Apr 20, 2015 12:19 PM)Only3 Wrote: [\[CITE\]](#) what normal person do when he see that his process hacker doesnt workyes i will put class to bypass taskmng + bsod

this gifte to y bro y the best in this :)

Ninja - April 20, 2015, 3:14 pm

(Apr 20, 2015 12:21 PM)LethalNET Wrote: [\[CITE\]](#) this could be done to task manager too, winapi is very useful.

good work op although the code could be improved its a unique release :)

Unique? I saw at least 5 other threads this month about anti process killers.

LethalNET - April 20, 2015, 4:24 pm

(Apr 20, 2015 03:14 PM)Tyranitar Wrote: [\[CITE\]](#) Unique? I saw at least 5 other threads this month about anti process killers.

The method its using is what I'm saying is a unique release, instead of setting the process as critical or admin only its uses a completely different approach.

I'm not so active in these subforums so I may have overlooked but I haven't seen this posted anywhere here.

I'm not saying the concept of process protection is unique only the method he is using.

Cecilia - April 20, 2015, 7:27 pm

(Apr 20, 2015 04:24 PM)LethalNET Wrote: [\[CITE\]](#) The method its using is what I'm saying is a unique release, instead of setting the process as critical or admin only its uses a completely different approach.

I'm not so active in these subforums so I may have overlooked but I haven't seen this posted

anywhere here.

I'm not saying the concept of process protection is unique only the method he is using.

Anyone remember that .net 'rootkit' that removed the process from taskmanager using winapi stuff?

Its not unique at all, its been done before with plenty of things.

nuk - April 20, 2015, 10:03 pm

(Apr 20, 2015 07:27 PM)LaPanthere Wrote: [\[CITE\]](#) Anyone remember that .net 'rootkit' that removed the process from taskmanager using winapi stuff?

Its not unique at all, its been done before with plenty of things.

Is there really such a thing as a TRUE .net ring-0 Rootkit? ...I'm just wondering because I didn't think that was possible? Would be interesting to take a look at the source to something like that.

Vigor - April 20, 2015, 10:47 pm

(Apr 20, 2015 07:27 PM)LaPanthere Wrote: [\[CITE\]](#) Anyone remember that .net 'rootkit' that removed the process from taskmanager using winapi stuff?

Its not unique at all, its been done before with plenty of things.

Yaaa I remember that. I was the one that originally posted, coded, and released that. The very first one. :)

Moon Rock - April 20, 2015, 10:49 pm

Hmm, code seems pretty long but if it does the job then I don't see a problem.

Ninja - April 21, 2015, 4:34 am

Who calls their PC "COBRAXx-PC", lol.

GhostCode - April 21, 2015, 4:51 am

(Apr 20, 2015 10:03 PM)nuk Wrote: [\[CITE\]](#) Is there really such a thing as a TRUE .net ring-0 Rootkit? ...I'm just wondering because I didn't think that was possible? Would be interesting to take a look at the source to something like that.

A ring0 rootkit is not possible in C#/VB.Net.

A ring3 rootkit is theoretically possible in .net, tho its tricky to code, but it is possible.

It requires knowledge about remote process hooking, code injection etc.

Many people called 'Darkfire' a rootkit in .net.

Its not a rootkit at all.. ;]

Cecilia - April 21, 2015, 4:59 am

(Apr 21, 2015 04:51 AM)GhostCode Wrote: [\[CITE\]](#) A ring0 rootkit is not possible in C#/VB.Net.

A ring3 rootkit is theoretically possible in .net, tho its tricky to code, but it is possible.

It requires knowledge about remote process hooking, code injection etc.

Many people called 'Darkfire' a rootkit in .net.

Its not a rootkit at all.. ;]

Thats the one I thought of when I saw this thread.

Exactly, its not a rootkit at all, just a trick or two.

(Apr 21, 2015 04:51 AM)GhostCode Wrote: [\[CITE\]](#) A ring0 rootkit is not possible in C#/VB.Net.

A ring3 rootkit is theoretically possible in .net, tho its tricky to code, but it is possible.

It requires knowledge about remote process hooking, code injection etc.

Many people called 'Darkfire' a rootkit in .net.

Its not a rootkit at all.. ;]

Thats the one I thought of when I saw this thread.

Exactly, its not a rootkit at all, just a trick or two.

He B TeMy - April 21, 2015, 7:06 am

This has nothing to do with a rootkit, it's just "tampering" with processhacker.

iLogic™ - April 21, 2015, 7:42 am

Nice code bro. I'm going to rewrite some of my projects ?

xeinebiu - April 24, 2015, 12:50 pm

It is not working on windows 7 ultimate 32bit ... V2 does not works too ...

Menalix - April 25, 2015, 3:46 pm

(Apr 20, 2015 10:03 PM)nuk Wrote: [CITE](#) Is there really such a thing as a TRUE .net ring-0 Rootkit? ...I'm just wondering because I didn't think that was possible? Would be interesting to take a look at the source to something like that.

He didn't say ring0.

It's easy to remove the process from taskmanager :)

nazist - August 20, 2015, 9:41 pm

imposter this code is not yours
this coded by njq8 coder of njrat
this code from 2012 man
sham on you ..

SIM-2303144 - August 20, 2015, 11:43 pm

You Not Coded this
Njq8 Coded this class

Raymond - August 21, 2015, 3:22 am

Can someone translate the code on C #?

N3w8i3H4ck3r - August 21, 2015, 11:25 am

Really?? This??

windows key + r
cmd
taskkill /f /im GitGud.exe
echo GitGudBro