

Re: undestroyable process

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-10/msg00620.htm>

- *From:* "anton bassov" <soviet_bloke@xxxxxxxxxxx>
 - *Date:* 30 Oct 2006 22:47:49 -0800
-

James,

What about referencing application's main thread (i.e. opening its handle with `OpenThread()`) from some process that cannot be killed without terminating a session (say, `smss.exe`)??? As long as reference count is non-zero, the thread cannot get removed from the thread list.

If you do something like that to the process itself, you will get Windows version of "zombie process" – even if all threads in it are terminated, it is still on the process list.

I just wonder what happens if you do the same thing to the thread.....

Anton Bassov

James Brown wrote:

"azsx" <radu_plugaru@xxxxxxxxxxx> wrote in message
<news:1162245761.096262.307420@xx>

run the process under the administrator account

an administrator could stop a process, right? that's not good.

make it a system service

a system service can't be shutdown? If positive then how can I make it a system service?

An administrator can do *anything* to his machine. It is impossible to stop him killing/shutting down processes. You can think up the best 'trick' you can to stop him doing it – but you will still fail. If you want to stop

Re: undestroyable process

people shutting down your process, then do **not** give them administrative rights to your computer system. There is **no other way** to make this work. So, my answer again:

Run the process under the administrator account. It can be a regular process, or a system-service (which only admin can start/stop). Do **NOT** give administrator rights to anyone that you don't trust with your system's security.

You started this topic on another forum and got the exact same response – people's answers aren't going to change no matter how many times you ask.

--

James Brown
Microsoft MVP – Windows SDK
www.catch22.net
Free Win32 Tutorials and Sourcecode