

Re: Re:How To Suspend Thread In Kernel?

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-03/msg00652.htm>

- *From:* "Scherbina Vladimir" <vladimir.scherbina@xxxxxxxxxxxxx>
 - *Date:* Wed, 29 Mar 2006 17:15:44 +0300
-

Anton,

Yes, I fully understand what you mean, and at the same time I understand those guys that are here against us :).

This newsgroup is not connected with security in the way you think about it; when someone asks "what is the best way to create secured system" everybody here will respond with "use well known algo, well know way that was checked and came through water, fire and the atom war", but this approach is applied to cryptography mostly.

Another side, if we will try to design approach to secure PC from viruses, malware and simular stuff, ways mentioned above are stupid.

VirMakers are creating polymorphing engines that uses sometimes unique techniques and cannot be detected by the signatures feature of AV;

Malware comes to kernel mode and begin hooking SDT, IDT to prevent been found by av's or SoftIce for example :);

How can one be protected from this stuff using well-known ways ? And here it goes – AV companies create "cleaners" that modify SDT using device PhysicalMemory or in the kernel mode, another AV companies creates "virtual machines" that emulates code, third companies create components that hooks API to protect themself from been terminated by malware, because malware uses *undocumented ways* !

The same with protectors – they use a lot of undocumented stuff. We again met the sentence "each task has it's own implementation".

—

Vladimir

<http://spaces.msn.com/vladimir-scherbina/>

"anton bassov" <xxx@xxxxxxx> wrote in message
<news:1d15ea4a320d49f3aab4093c4cf9802e@xxxxxxxxxxxxx>

Hi Vladimir

Re: Re:How To Suspend Thread In Kernel?

I am really glad that there is at least one person who understands what I mean. You seem to be the only one on this thread who understands that sometimes we come across problems that cannot be solved by any officially supported means – anyone in the right state of mind would not play such tricks just for the fun of doing it, don't you think???

Such trick is dangerous, and I can foresee quite a few problems using it (at least directly – probably, it may require quite a few additional modifications). This is definitely not a solution that wins you MS awards – I don't want to even argue about that. However, what is the alternative solution???

Everyone on this thread says that this is dangerous trick, but no one came up with any alternative proposal so far. You seem to be the only one who has a realistic view of the situation

Regards

Anton Bassov