

Forum:[Hack Forums](#)

Thread: [Protecting by hooking ZwOpenProcess | Rootkit](#)

GenesisDatabase - January 31, 2011, 3:50 am

Want to know how Antivirus and rootkits protect themselves from being terminated? You might have tried running Windows Task Manager and find it impossible to kill avp.exe by Kaspersky. This is because the process is being protected by a higher privilege, the kernel. Visit my blog to learn more about how to do so and download the source code!

Source: <http://genesisdatabase.wordpress.com/2011/01/27/protecting-by-hooking-zwopenprocess/>

Sia - January 31, 2011, 12:00 pm

No thank you... To be honest i already knew that... Not anything new, and this IS called hackforums so don't expect people to be surprised.

frazdaz - January 31, 2011, 4:05 pm

(Jan 31, 2011 01:00 PM)VirtualDUDE Wrote: [\[CITE\]](#) No thank you... To be honest i already knew that... Not anything new, and this IS called hackforums so don't expect people to be surprised. You may have already known they were ring0 protected but I doubt you knew how. Now you do. So what if you did? It will help others.

And I honestly don't see where he's expecting people to be surprised?

stdio - January 31, 2011, 6:55 pm

(Jan 31, 2011 05:05 PM)frazdaz Wrote: [\[CITE\]](#) You may have already known they were ring0 protected but I doubt you knew how. Now you do. So what if you did? It will help others.

And I honestly don't see where he's expecting people to be surprised?

It may help others, and I hope it does and my next statement is completely wrong (I doubt it though). Its HFs, people here cant seem to compile hello world, let alone install the WDK and make a KMD that correctly installs (Especially in win vista/7 where unsigned drivers are a big no no, and need further steps to get working).

All and all though its not a terrible piece of code. Though I guess for the sake of brevity they hard coded the pid but thats a really lame way out.

GenesisDatabase - January 31, 2011, 8:36 pm

The article i found basically (yeah hard coded the PID) doesn't point out how you could possibly get the PID from a process name as well as the user but generally this is one of the concept and a simple source code to show how it is done. As VirtualDUDE mentioned, "and this IS called hackforums so don't expect people to be surprised," i feel that your statement is entirely wrong. Even if this is a forum where people learn to hack (if it is), it isn't a forum of coders in mass and most of the coders you can find are generally learners.

And i thank frazdaz and stdio for their generous comment.

Sri Krishna - January 31, 2011, 9:02 pm

I know Hooking and stuff but I don't understand those ring0, ring3 and what not.

Would anyone mind explaining them?

Navigator - January 31, 2011, 9:12 pm

(Jan 31, 2011 10:02 PM)Sri Krishna Wrote: [\[CITE\]](#) I know Hooking and stuff but I don't understand those ring0, ring3 and what not.

Would anyone mind explaining them?

Ring0 - kernel level. Ring3 - application level. Ring1-2 is for device drivers.

stdio - January 31, 2011, 9:20 pm

(Jan 31, 2011 10:12 PM)Navigator Wrote: [\[CITE\]](#) Ring0 - kernel level. Ring3 - application level. Ring1-2 is for device drivers.
...misleading...kinda

Intel designed 4 layers of security in memory access... ring 0 - 3. Microsoft Windows only actually uses 2, 0 and 3. 1&2 are not used for anything currently.

wikipedia Wrote:For example, the reason Windows uses only two levels (ring 0 and ring 3) is that some hardware architectures that were supported in the past (such as PowerPC or MIPS) implemented only two privilege levels.[3]

This isnt including the special areas that arent allowed even to the OS. (ex SMRAM)

CYSER - February 1, 2011, 10:33 am

old but gold.

[img]http://upload.wikimedia.org/wikipedia/commons/thumb/0/03/Computer_abstraction_layers.svg/200px-Computer_abstraction_layers.svg.png[/img]