

Re: Licence and software protection

Source:

<http://coding.derkeiler.com/Archive/Delphi/borland.public.delphi.thirdpartytools.general/2005-03/0823.html>

From: Nick Rollas (*nickrollas_at_hotmail.com*)

Date: 03/17/05

Date: Fri, 18 Mar 2005 00:36:42 +0200

Since your software is running in user-mode (Ring3), any kernel-mode (Ring0) tool can spy, debug and crack your program. That's why everything can be cracked. Most of crackers tools are running in kernel mode making possible to watch your protection routines in low level, study them and therefore crack.

There is a new software protector (Themida), actually the first one, that runs in kernel mode (ring0), in the same level cracking tools are running. It's more more difficult (in some cases impossible) for cracking tools to fight against the protection routines because they are running in the same operation level. On the other hand, when protection runs on the higher operation level, it has all the privileges enabled and almost everything is possible. For example, regular software protections such as ASProtect, IonWorx, ACProtect, Armadillo, running in user mode (ring3) are unable to use global-scope registry hookers to protect specific registry keys used by protection routines. Themida, is running in kernel mode (ring0) and it is able to run any system hooking or protection is necessary to prevent from cracking.

The disadvantage is that kernel mode (ring0) protection requires a device driver (small one) to be installed in the user machine. Unfortunately, due to the plethora of cpus and hardwares around there are some stability issues. Some crashes on some old or very new machines. But, it's the only one it supports 64bit and dual xeon cpus. I can see that version by version the product is becoming more stable and in a few months I'm sure it will be very stable. Anyway, I recommend this product only in big projects or business applications. I don't recommend to use Themida in small utilities.

You can check it at www.oreans.com. I'm excited with it. I'm waiting for the upcoming WinLicense which will support licensing. According to the author, it will use revolutionary technologies, never seen before on the security market and it will be the first protector that will ensure a secure full functional trial distribution. The old traditional security gap of comparing BEFORE to AFTER, to detect the changes done in registry and/or files is already filled. As you understand, that is only possible when running in kernel mode (ring0).

PS: For your information, there is one more software protection that runs in ring0, but its not a regular software protector in the form ASprotect. Its the Starforce (www.star-force.com) that protects CDs (usually games). That means the everytime your application is running, the CD is required on the cd drive. That system puts in my mind the old days we were running software with a special 3,5" floppy disk on the drive. At last, CD/DVD protection makes the e-distribtion impossible, because the CD/DVD media is required to run the software.

Nick

"Steven Yates" <duel@telkomsa.net> wrote in message
news:42398534@newsgroups.borland.com...

> *Hi All*

>

> *Two questions:*

>

> 1.) *I have had a look at Turbopower's Onguard – how hard is this to crack
> for the average hacker?*

> 2.) *Can anyone reccomend near bullet proof software protection or the best
> there is ?*

>

> *Thanks*

>

>

>