

Re: Dynamically loading binaries in Kernel mode.

Re: Dynamically loading binaries in Kernel mode.

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2006-03/msg00836.html>

- *From:* "Doron Holan [MS]" <doronh@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 28 Mar 2006 22:21:42 -0800
-

All I would have to do to detect your dynamic load is to put a bp on nt!MmLoadSystemImage and then set up all the breakpoints I want. Loading a driver/logic on demand is not going to make your product any more secure, all it will do is make your product more complicated and error prone. Unlike user mode, there is very little support for loading/unloading modules in the kernel and all the associated ref count problems that arise from it...you don't want to go there.

d

Please do not send e-mail directly to this alias. this alias is for newsgroup purposes only.

This posting is provided "AS IS" with no warranties, and confers no rights.

"David J. Craig" <Dave@xxxxxxxxxxxxxx> wrote in message news:O7aelFvUGHA.5108@xxxxxxxxxxxxxxxxxxxxxxxx

Do you want to have something "debug" resistant or just the appearance of resistance? You can spend a lot of time writing anti-debug code and a lot more time and effort debugging it or you can just forget about it and go for quality instead of glitz. If you really want to keep your competitors from reverse engineering your design you can have their computer call yours to do the work. Then you have control over the more difficult pieces. You can easily write a driver that functions as a DLL, but keeping the logic intact and loading it when required and unloading it when it is not will be a lot of work. If the DLL is encrypted all someone needs to do is force a kernel dump and can grab the object code in plaintext form. A little editing of the dump will give them an easy way to reverse engineer your product.

Make the product work and work well. Support your users. Provide value for their money and you will succeed unless your target market is less than a thousand users.

"Luis Miguel Huapaya" <LuisMiguelHuapaya@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:574869DE-A063-41B1-84A7-F9CB6F94046E@xxxxxxxxxxxxxxxxxxxxxxxx

Re: Dynamically loading binaries in Kernel mode.

We have a component that needs to be "debug" resistant that will load specific code on demand and unload it as soon as the code runs. This way, it will be difficult for hackers to get a full picture of all the components binary.

Ok, I've answered your question, how about you answer mine :-) ?

cheers,
Luis Miguel Huapaya

"Mark Roddy" wrote:

On Tue, 28 Mar 2006 13:31:06 -0800, Luis Miguel Huapaya
<LuisMiguelHuapaya@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote:

I absolutely need to
figure out how to dynamically load code at
the kernel level (this code
will
be loaded by a file system minifilter).

Why is this a requirement?

=====
Mark Roddy DDK MVP
Windows Vista/2003/XP/2000 Consulting
Device and Filesystem Drivers
Hollis Technology Solutions 603-321-1032
www.hollistech.com