

Re: U3 TEchnology was RE: strange new virus

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2006-12/msg00039.html>

- *From:* "Thor (Hammer of God)" <thor@xxxxxxxxxxxxxxxx>
 - *Date:* Mon, 18 Dec 2006 09:10:40 -0800
-

Hey James... inline:

On 12/15/06 5:07 PM, "James D. Stallard" <james@xxxxxxxxxxxxxxxx> spoketh to all:

Thor, et al

Question regarding autorun on USB flash disks (I never like the term "thumbdrive"):

If you have a file in the root called "autorun.inf" and it contains a valid syntax for an icon file, the icon will appear as the drive icon in Windows Explorer. This most certainly works with XPSP2+patches.

Actually, you'll get a drive icon whether it has an autorun.inf or not... That's just Windows identifying the device as a mountable drive. The autorun doesn't do anything... Even with it present (on my systems) it doesn't even ask you to run it.

The OS is clearly executing something, just not your arbitrary code.

The question is, would it be possible to take advantage of the icon functionality (presumably within explorer.exe) to hijack the process and run your own code? I'm thinking buffer overflow as the most likely scenario, but I'm also thinking that following MS "trustworthy computing initiative" and XPSP2, the existence of buffer overflow possibilities in the OS is pretty minimal these days.

Well, that's the trick... Explorer.exe is just saying "This device mounted as a drive letter, and here it is." Yes, it's "running code" (Actually, I would guess that the code is already running and that it just renums available drives by type) but as you said, it's not running any code on the device itself.

Re: U3 TEchnology was RE: strange new virus

Sure you could hijack the process, but that would mean that the OS was already compromised in some way, or that you've already got code on the box to do that (a rootkit could easily do this. Well, "easily" if you know how ;). But at that point, it's moot. I don't see how you could do that with any data that requires it be loaded from the device to then exploit some vector, even if such vector exists. But even if you could, and you really wanted to go down that path, I think it would be easier to just get yourself a U3 drive so that stuff like autorun would work by design.

t

