

Re: What are these "Impersonate" keys about?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2007-04/msg00379.html

- *From:* SueInCincy <SueInCincy@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 30 Apr 2007 10:16:01 -0700
-

"Harry Johnston" wrote:

If you install your computer from the Microsoft-provided CD, without connecting it to any network or plugging any devices into it (the mouse and keyboard are OK) does it show signs of infection?

The short answer is a qualified no. Qualified, because as you know I have been doing the same thing (reformatting the hard drive and hooking up to the Internet to get updates) and expecting a different result for a long time. So you know I am crazy.

The longer answer may be more interesting to you, I hope. I have had two HP printers, one a 1012, I believe (it died a few months ago, and is gone...) which I replaced with a 1020. Both of them seem to be keystones in closing the whole system, and I had even contacted HP about the possible security issue with the 1012.

After I get the expired security certificate for the Microsoft Update ActiveX control, and the first three updates (WGA, Installer 3.1 v2, and some other Installer-related update I can't recall at this moment) the 13 "subscriber" accounts don't appear until after I hook up these printers.

At one point, in desperation, I even bought a Mac, and as soon as I would hook up the printer after a reformat, I would see the creation of 13 subscriber accounts and certain other inexplicably similar behaviors to my PC experience—ON A MAC!. Yes, you are reading correctly — I reformatted a Mac hard drive multiple times, many under telephone supervision from Cupertino. The guys at the store where I bought it saw exactly what I was talking about when I brought it back to the store. When *they* reformatted and hooked up to their Net connection, the signs were gone.

The installation of the printer driver is one of the things that is particularly suspicious. According to HP, that printer should be 100% plug-and-play on any XP machine with SP2, and when I first got the 1012, it was. After my problem manifested in late 2005, it would take three runs to get the installation done. 1) A "found new hardware" balloon would pop up, and the usual plug and play routine would run. Just as the "Your new printer

Re: What are these "Impersonate" keys about?

is installed balloon appeared, 2) a whole new "Detected new printer" balloon would pop up, and I would be prompted to install the printer using a driver. The machine couldn't find a suitable driver in its own files (although it had just done so, apparently) AND it couldn't find one online, either. So I would be forced to use the manufacturer-provided disk. After that installation ran, I could print any document I wanted, but, after restart, 3) I would get a prompt that some file was missing (the exact file is in my notes somewhere) and the only place I was ever able to find that was by browsing my manufacturer disk. I explained all this to HP, via e-mail, and they responded that no one had ever heard of such a thing, thanks for your business.

I tried bypassing all this by going to HP's website and downloading the latest driver on disk, but I had basically the same experience when I did that.

As this "system" has evolved, I don't have the 3-step process, I just have no choice but to install from the manufacturer disk. Even if I download the HP driver on disk, I am still prompted to insert the manufacturer's disk in order to get a successful installation.

Here is my hypothesis about what goes on there: HP has on its disks a horrible "order reminder" function that I believe is a helpful pathway for this invader. The invader has a "rock in the door" with its three bogus XP updates and this order reminder thing helps it along. That's why I have to have the manufacturers' disk to proceed, and I can't just use the downloaded driver. The downloaded driver doesn't include that "value add."

Last but not least, I have this old Windows 98 Dell Inspiron laptop that I have been limping along with while I try to figure out what to do about connecting my Averatec with its new motherboard and hard drive to the net safely. I use Firefox, and Avast and firewall software. I learned the other day that if I tried to use that 1020 printer offline, that is, while I wasn't connected to the Internet, the jobs would simply queue up, with the status of "Waiting for operator approval" or something like that. As soon as I got on the Net, the jobs printed.

As I have said before, I may not have all the right language for describing what is happening, but I have observed and documented it in a lot of detail. It is great to have your insight, Harry.

Cheers, Sue

.

Re: What are these "Impersonate" keys about?