

Re: IE is allowing virii/trojans/spyware etc. to install without help

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-07/1796.html

From: Carey Frisch [MVP] (mrxp2004_at_nospamyahoo.com)

Date: 07/12/04

Date: Mon, 12 Jul 2004 13:09:02 -0500

Security enhancements in Microsoft Windows XP Service Pack 2

<http://support.microsoft.com/default.aspx?scid=kb:en-us:832490&Product=winxp>

Windows XP Service Pack 2: A Developer's View

<http://msdn.microsoft.com/security/default.aspx?pull=/library/en-us/dnwxp/html/securityinxpsp2.asp>

Note: The information provided about Windows XP SP2 is subject to change without notice because SP2 is not yet been released.

--

Carey Frisch
Microsoft MVP
Windows XP - Shell/User
Be Smart! Protect your PC!
<http://www.microsoft.com/security/protect/>

"Morbius" Morbius@discussions.microsoft.com wrote in message:

news:D5278A7C-DA28-47C3-AA28-FD3D117E2235@microsoft.com...

| Just my personal experience...

| I'm certainly no PC or internet newbie. And I've been online before there was even a well-known using CompuServ in it's earliest days, and BBS's before that. I know how to avoid email virii, scams, and can spot a virus "hoax" a mile away. I have a home network, behind a firewall/router, routinely run ZoneAlarm, Norton AV, AdAware, SpyBot S&D, and have used various pop-up blockers, relying on the one built into the Google Toolbar.

| In spite of all this, twice within the last month my system has been compromised by my doing no than clicking a web link on what appeared to be trustworthy sites. Just a couple days prior to t scare, I was surfing around looking for info on digital cameras. After clicking some link, sudden screen began filling with popups (in spite of the Google popup blocker), and then the system froze. rebooting, I found my desktop wallpaper had been replaced by an active desktop page to a "security site, and the CPU was pegged at near 100%. After about 9 hours, and multiple passes with various found I that along with the desktop hijack, I had been infected with Backdoor.Jeem, several adware and the nefarious CoolWebSearch. I lost a whole day tracking down and removing all traces of this

| This Sunday, an identical episode occurred...searching Google for info on injector razors. One I clicked on took me to another site that had some "consolidated" links regarding my search. About link I clicked on there suddenly put a couple of popups on the screen, and one looked like a normal permissions screen, asking if I wanted to install something-or-other from "Slotch.Com". Of course didn't...but I paused for a minute to look over that window, as it didn't look quite right. The "Yes" and "No" buttons, and a couple other things, didn't appear genuine. I actually felt that c

microsoft.public.windowsxp.security_admin: Re: IE is allowing virii/trojans/spyware etc. to install without help

anywhere on that window was a bad idea, so I just closed down all browser windows. I also shut down the system, and then I decided that considering my experience from a couple weeks earlier, I better check out thoroughly.

|
| I unplugged the network cable, and booted to safe mode. First I ran CWSshredder, which found 4 programs installed. I then ran Spybot S&D, which found 40 suspicious files/entries, and deleted those. Then I ran Norton AV, which found 57 bad hits. It was only able to delete 37 of them, so I had to manually check the name and location of each file/registry entry and attempt to get rid of them. After working on this, I reconnected to the network and booted up normally. During the course of this, I also discovered two programs called PowerScan and Sidebar T-Search, or something like that, had been installed, and when I had to uninstall or entry in Add/Remove programs, I had to manually get rid of those.

|
| I wanted to go to the Symantic site and see what other info might be available for some of the programs found. After booting up, I decided to use Mozilla Firefox to go to the site, as I had installed Firefox the previous problem, and thought I might be a little safer till I was sure the machine was clean. I clicked on the Firefox desktop icon, it couldn't find the program...sure enough, the entire Firefox install was gone. Sneaky move on the spyware's part! I still had the Firefox install package on my hard drive so I reinstalled, and went out to the Symantec site. I went to a couple more site with Firefox and the system down.

|
| I started it up a little later, and once again, clicking on the Firefox icon said it couldn't launch the program...and again, the entire folder and install was gone. So something was still on the system deleting Firefox apparently at will. I ran HiJack This! and noticed a new BHO listing that point I hadn't seen before, something like bvm202.dll. I went and looked at the properties of that DLL, and it had been created that day, at the same time all the problems started. So I booted to safe mode again, deleted the DLL, and deleted all references to it in from the Registry. Reinstalled Firefox again, and now it's staying, so I'm not sure if that was the problem or not.

|
| In any event, I probably lost almost 20 hours of time over the two incidents. I'm still not 100% sure of the machine's status at this point. Numerous bad things got installed in each instance, and with no more than clicking a web link...in both cases, I did not attempt to download or install anything that would give permission for installation, and I had firewalls and AV products active at the time, along with "supposed" popup blockers, and I was not doing or visiting anything "shady" that I shouldn't have. All of this did nothing to stop these incidents from occurring.

|
| Point is, IE is simply allowing way to much damage to occur with little or no action on the end user's part. It should never allow something to be installed on my system without my explicit permission. I don't understand how this has happened, as I didn't think it was even possible for things like this to happen without me doing SOMETHING to initiate it. If clicking on a web link is all it takes, then quite frankly IE browser is useless.

|
| So now I'm back to using Firefox. We'll see how this goes. In any event, MS needs to complete and improve it's security model for this thing, as right now I wouldn't trust it to go to MS's own website.