

Re: Registry error warnings

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-06/0819.html>

From: Malke (invalid_at_not-real.com)

Date: 06/27/05

Date: Mon, 27 Jun 2005 12:20:44 -0700

PS wrote:

> *I was working on a Win 2000 pro machine today and kept getting pop-up
> "System Warning" windows saying the registry was corrupted, system is
> about to crash, etc. Each one said immediately go to a microsoft
> website and download registry repair tools. I became very suspicious
> because one of the website references was to a .info domain –
> somewhere I don't think a legit MS site would be. I checked the sys
> event log and the pop-ups said application warnings – but did not
> specify the app generating them – I think I may have a Trojan
> generating the pop-ups?? Or are they legit?? Thanks*

What does a scan with your current version antivirus (not earlier than 2004 and using updated definitions) show? Do you have a firewall in place? If you haven't done any malware removal work, I would definitely do so. Here are some general steps; it is crucial that you do everything with updated tools in Safe Mode:

First delete all Temporary and Temporary Internet Files. For IE's Temporary Files, go to Control Panel>Internet Options>General tab. You'll see where you can delete cookies and files. For Firefox, clear its cache by going to Tools>Options>Privacy>Cache> Clear. For Windows Temporary files, Start>Run cleanmgr [enter]. Then follow these detailed malware removal steps, doing everything with updated tools in Safe Mode. You can find all the links to referenced programs and sites on my website here:

http://www.elephantboycomputers.com/page2.html#Removing_Malware

1) Scan in Safe Mode with current version (not earlier than 2004) antivirus using updated definitions.

Before you remove malware, get LSPFix or WinSockFix for XP – see links below.

2) Remove spyware with Spybot Search & Destroy and Ad-aware. These programs are free, so use them both since they complement each other. There is a new version of CWShredder from Intermute. I would not

microsoft.public.security: Re: Registry error warnings

install the other Intermute programs, however. Alternately, there are CoolWebSearch malware removal steps at SilentRunners.

Be sure to update these programs before running, and it is a good idea to do virus/spyware scans in Safe Mode. Make sure you are able to see all hidden files and extensions (View tab in Folder Options).

If the malware remains even after you used Ad-aware and Spybot, you can scan with HijackThis. HijackThis is an excellent tool to discover and disable hijackers, but it requires expert skill. See the links on my website for a HijackThis tutorial and places where you can post your HJT log. Again, this is an expert tool and novices should get help with it.

3) If you are running Windows ME or XP, you should disable/enable System Restore after the system is clean because malware will be in the Restore Points. With ME, you must disable System Restore completely. With XP, you can delete all but the most recent (presumably clean) System Restore point from the More Options section of Disk Cleanup (Run>cleanmgr).

4) Make sure you've visited Windows Update and applied all security patches. Do not install driver updates from Windows Update.

5) Run a firewall.

Malke

--

Elephant Boy Computers
www.elephantboycomputers.com
"Don't Panic!"
MS-MVP Windows - Shell/User