

Re: Pop ups

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-06/0559.html

From: Malke (*invalid_at_not-real.com*)

Date: 06/12/05

Date: Sat, 11 Jun 2005 15:38:11 -0700

pxriet wrote:

> *I have been getting popups the last few days. My default homepage is*
> *Yahoo,*
> *and as soon as it logs on I get at least one popup. I get them at*
> *various*
> *times throughout the day. I also am getting shortcuts from these*
> *popups save on my desktop.*
>
> *I have Norton Internet Security & Yahoo Popup blocker, but neither has*
> *helped. I need to find where these are coming from or loading*

Go through these malware removal steps systematically, doing 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 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