Internet Explorer always accesses strange websites

Annoying every time I access the Internet, Internet Explorer (IE) automatically accesses a web address even though you have reset the default website address in the Home Page section of Internet Options.

Annoying every time I access the Internet, Internet Explorer (IE) automatically accesses a web address even though you have reset the default website address in the Home Page section of Internet Options.

Some commercial, service and advertising websites have "promoted" viruses, spyware (spyware), adware (adware) when users download free gadgets, music files, images. . to collect user personal information or simply to advertise, send spam like spyware vnn.com originated from Vietnam and some of this spyware variants. Some viruses and spyware are too much, after entering the system, they change the homepage settings (homepage) of the web browser, prevent access to Group Policy, Registry, Folder Options and run the Run command. .

This will create a closed circle, preventing you from displaying files with hidden attributes (Folder Options), homepage resetting (in Group Policy) and not deleting the keys of viruses and spyware (in the Registry). . To "root the grass", please refer to the following information.

1. Locate viruses, spyware, adware

Figure 1

Due to its origins in Vietnam, foreign anti-virus and anti-spyware software does not detect this spyware. However, these software are still able to warn users when spyware files attempt to start when Windows boots (Figure 1). Based on this warning you can go to the archive folder and delete them (*Note:* remember this file name to use in the next steps).

If using BKAV (download at http://www.bkav.com.vn/frmDownload.aspx), you can easily determine the file of the spyware to be installed and delete them.

2. Handle changes made by spyware

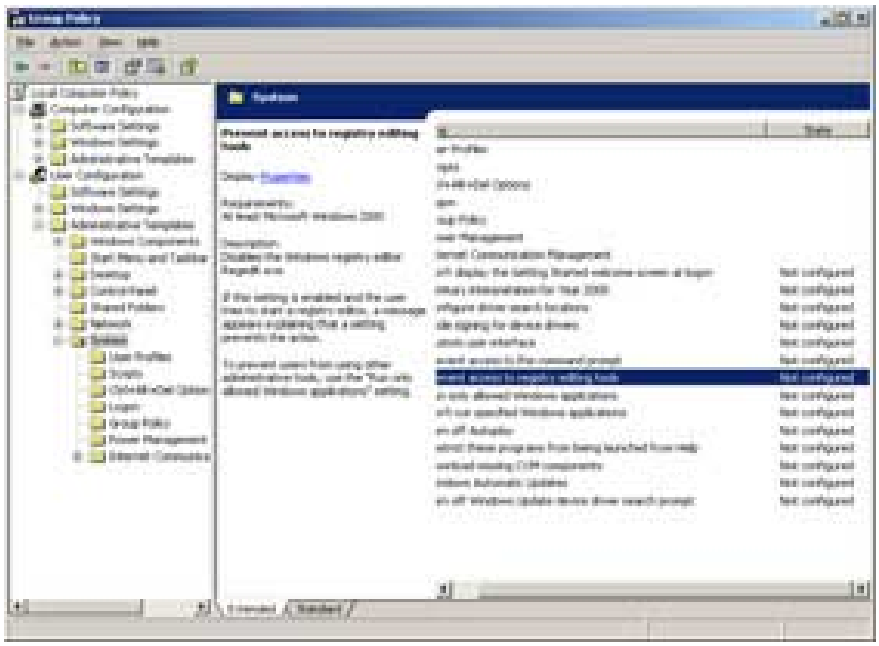

Figure 2
Delete the keys in the Registry. Select Start. Run to open DOS Prompt window; type "regedit" to open the Registry Editor window. Find and delete keys related to spyware file names in the following branches.

HKEY_CURRENT_USER. Software. Microsoft. Windows. CurrentVersion. Run

HKEY_CURRENT_USER. Software. Microsoft. Windows. CurrentVersion. RunOnce

HKEY_LOCAL_MACHINE. Software. Microsoft. Windows. CurrentVersion. Run

HKEY_LOCAL_MACHINE. Software. Microsoft. Windows. CurrentVersion. RunOnce

Note:

- If "regedit" doesn't work, refer to the information below to fix it.

- Using the search feature (Find) with keywords is the file name to make sure not to "lock" the spyware related keys.

" *Registry editing has been disabled by your administrator* ". Use *Group Policy Editor* to fix this and do the following: in the *DOS Prompt* window; Type " ***gpedit.msc*** " command and click OK to open the *Group Policy Editor* window, select the *User Configuration* branch . *Administrative Templates> System* . In the right window, select *Prevent access to registry editing tools* and change the properties to *Disable* or *Not Configured* (Figure 2).

Figure 3
Alternatively, you can restart *Registry Editor* (Regedit) by creating a **.vbs** (Visual Basic Script) file to correct the keys in the Registry or if the HijackThis (http://www.download utility) is available. com / HijackThis / 3000-8022-10307556.html), just run this utility, mark the key to delete in the *Registry* and select *Fix checked* (Figure 3).

The web browser home page is disabled. In the *Group Policy Editor* window, select the *User Configuration* branch > *Administrative Templates> Windows Components> Internet Explorer* . In the right window, select *Disable changing home page settings* , change *Not configured* properties. Launch IE and reset home page in *Tools> Internet Options* , *General* tab.

Folder Options are lost. In the *Registry Editor* , go to ***HKEY_CURRENT_USER*** > *Software> Microsoft> Windows> CurrentVersion> Policies> Explorer* . Right-click in the right window select *New> DWORLD Value* , name *NoFolderOptions* and assign a value of 0; If you want to hide the options folder, assign this value to 1.

Do the same in ***HKEY_LOCAL_MACHINE*** > *Software> Microsoft> Windows> CurrentVersion> Policies> Explorer* .

3. A few notes

Some readers believe that installing anti-virus and spyware software will slow down the system. In fact, you will encounter a lot of troubles, occupied resources, operating system sluggish without a powerful tool to protect the system against the attacks of viruses and spyware.

Each software has its own advantages and disadvantages and the results obtained depend on the level of users. Additional antispyware software if your antivirus software works ineffectively or uses "full package" solutions

like Norton Internet Security 2006 (http://www.symantec.com/home_homeoffice/products/internet_security/nis2006 / index.html), Internet Security Suite 2006 (http://us.mcafee.com/root/promo.asp?id=mistax06&cid=18322).

PREVENTING HORIZONTAL COPYING WITH DEFINITION THROUGH USB COMMUNICATION

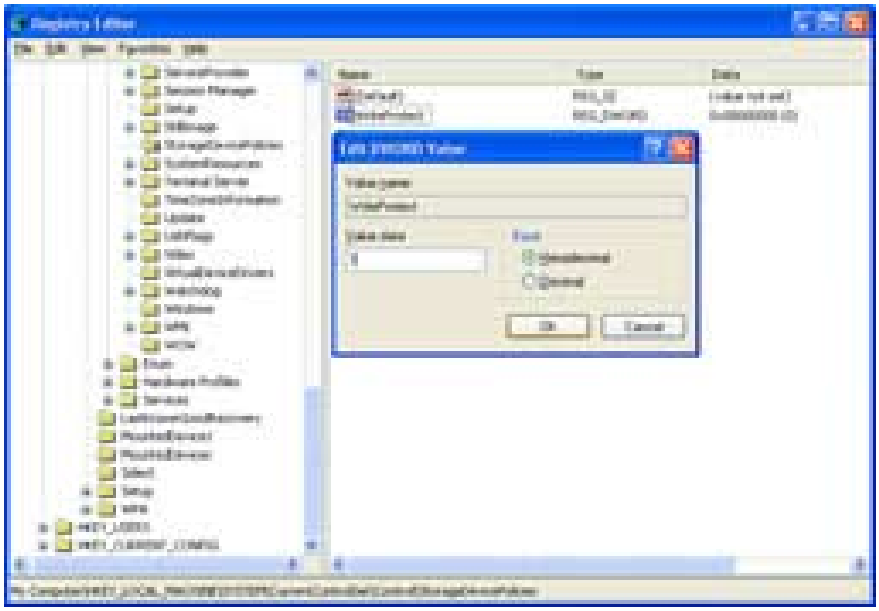

Figure 4

External storage devices use USB communication (external hard drives, flashdrive, media card .) to grow and gradually replace floppy disks because there are many advantages. But besides the positive side, external storage devices become a concern because it is easy to "slip" out personal data. To limit this, you can use feature software such as SecureWave (http://www.securewave.com/home.jsp) or edit the Registry. Do as follows:

- In *Registry Editor* , locate ***HKEY_LOCAL_MACHINE*** *> System> CurrentControlSet> Control*

- Right-click on the Control key and create a *StorageDevicePolicies* key in *Control*

- In the right pane of *StorageDevicePolicies* , right-click and choose *New> DWORLD Value* , name it ***WriteProtect*** (Figure 4) and assign value 1

- Select OK. Restart the computer for the change to take effect

Note:

This solution is only applicable if your computer uses Windows XP sp2 and it only restricts users from copying data to an external storage device. This does not completely prevent "leakage" of personal data if your device is connected to the network, using sharing tools like Kazza . So, in addition to preventing by "prohibition" Technically, enterprises need to further tighten the policy of copying and sharing data in their networks.

SCREEN CANNOT SHOW

Normal displays are only capable of displaying images at a certain resolution and scan frequency range (usually 85Hz, except for certain types of monitors that are capable of reaching 100 or 120Hz). Some readers who like to "poke" have pushed the screen resolution or the scan frequency beyond the display, resulting in a dark screen, if you want to correct it, you won't see the line to adjust.

In this case, you just wait about 15 seconds, the screen will automatically return to the old settings. If you miss your phone or press the reset button to restart the computer, you will only hear the sound when you enter Windows without seeing the image. To return the old settings, do the following:

- Restart the computer, press F8 when the system transfers control to Windows to start.

- Select Enable VGA Mode in the options and press Enter to start Windows in the basic graphic state.

- In Windows, right-click on the Desktop screen, select Properties to enter the Display Properties window.

- Select the Settings tab and adjust the settings back to the old location.

- Click OK and restart the computer (if necessary) for the settings to take effect.

Dong Quan