Prevent Autorun.inf from infiltrating your computer via USB

USB is the inevitable result of the development of information technology, saving you time and cost to minimize the flow of information, but it also brings a lot of trouble for privacy. Your private via Autorun.inf Virus. The article will introduce a small trick to prevent Autorun.inf intrusion when connecting mobile devices to a computer.

USB is the inevitable result of the development of information technology, saving you time and cost to minimize the flow of information, but it also brings a lot of trouble for privacy. Your private via Autorun.inf Virus.The article will introduce a small trick to prevent Autorun.inf intrusion when connecting mobile devices to a computer.

Once you've installed Windows and the necessary applications, the first thing to do is to disable the **System Restore** function to avoid hiding the Virus on the system in the copies (Backup), you usually take one more step. with Windows **AutoPlay** function to avoid the intrusion of Autorun.inf when connecting the computer. After doing these 2 important steps, you think it is safe to Autorun.inf when accessing mobile devices to work with the data stored here.

But it is actually insecure because there is another important feature in Windows operating system that you have missed or have not learned about it or have never known its presence in the operating structure. of Windows, it is **MountPoints2** . This feature is responsible for creating mobile log registers to perform actions related to activating the menu window or running automatically. And this is the reason for the question " ***Why did I disable AutoPlay and click mouse while still being infected with Autorun.inf or Virus.exe?*** ", The reason is simply not disabled. of MountPoints2.

To disable the MountPoints2 feature, follow these steps:

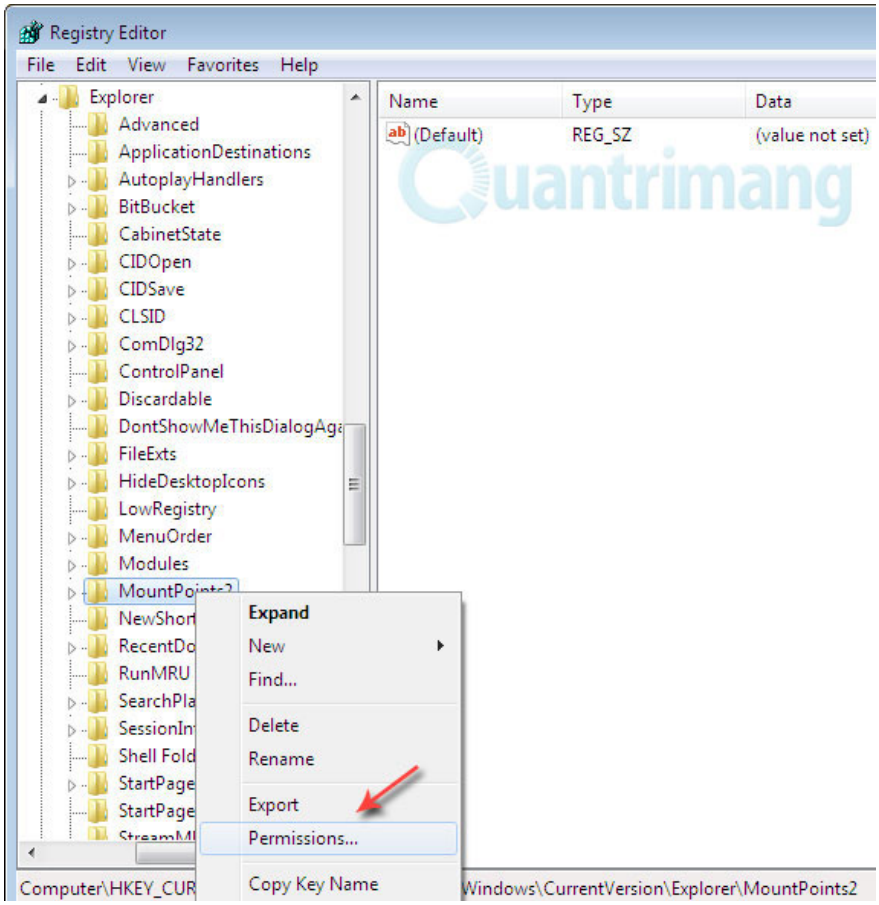
1. Start> **Run** or **Win + R**

2. Enter **Regedit** in the Run> **Enter box**

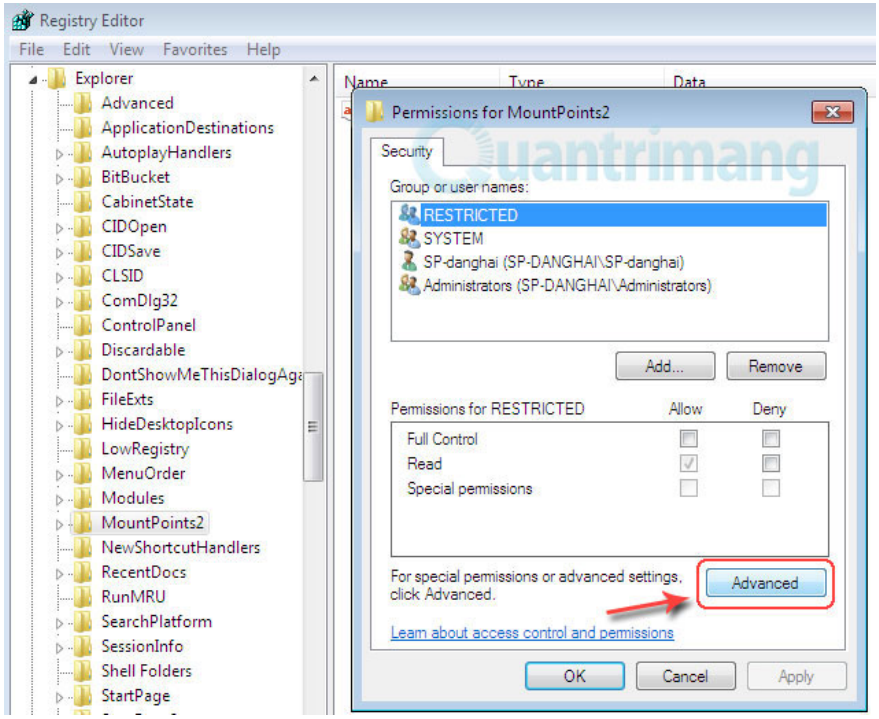
3. In the Registry Editor window, perform the key:

HKEY_CURENT_USERSoftwareMicrosoftWindowsCurentVersionExplorerMountPoints2

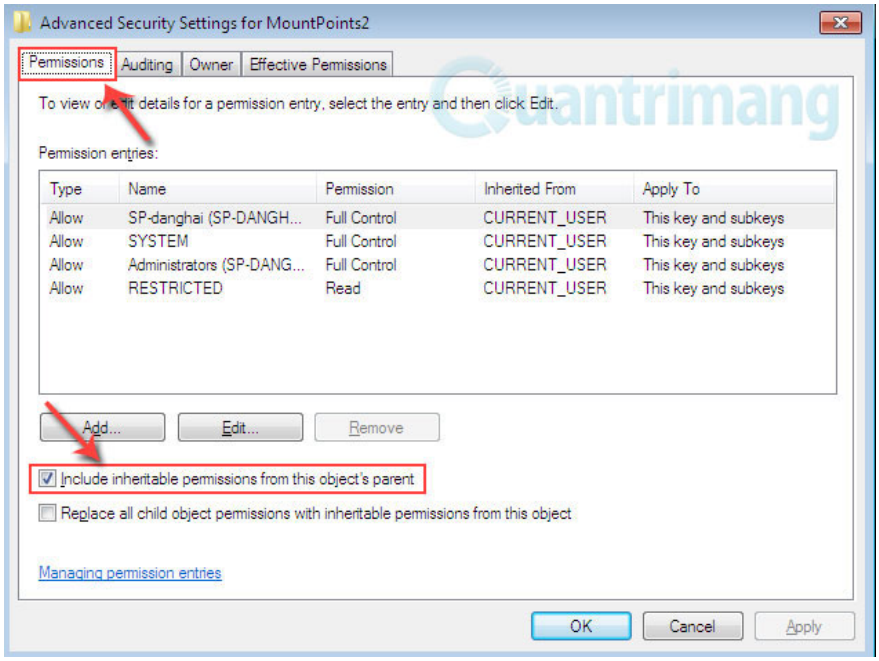
4. Right-click **MountPoints2** > **Permission .**



5. The P *emission for MountPoints2* window opens> **Advanced**



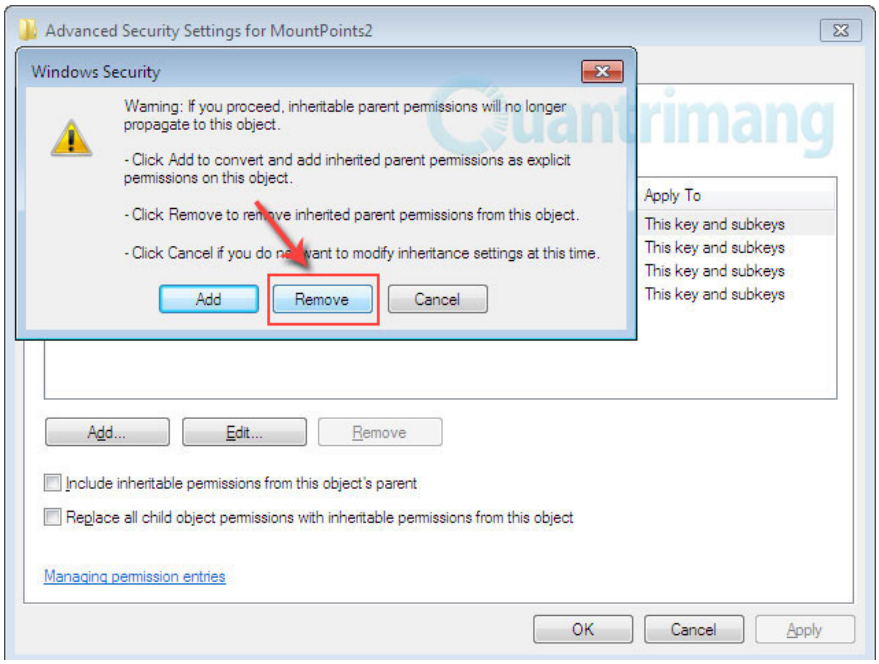
6. In the settings window *Advanced Security Settings for MountPoints2* select the **Permissions** tab



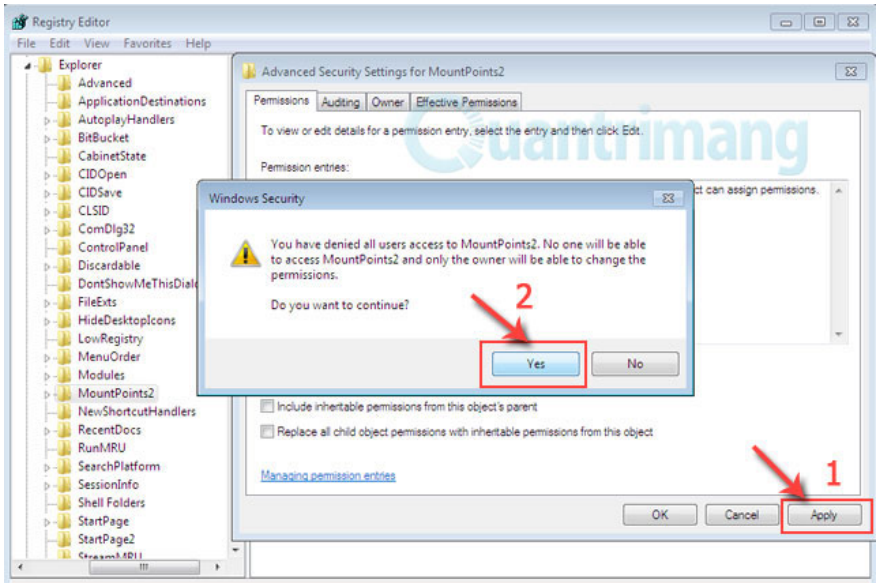
*** Win 7:** Uncheck ***Include inheritable pemssions from this object's parrent feature*** and currently there are 4 registration keys displayed in the Pemission entries frame.

*** Win XP:** Uncheck the ***Inherit*** feature ***from parent pemission entries that apply to child objects. Include này v?i m?c nh?p xác ??nh ?ã xác ??nh*** .

7. The *Windows Security* dialog box appears> **Remove**



8. At the *Advanced Security Settings for MountPoints2* window> **Apply**



9. The Windows Security dialog box appears again with the content " *You have denied all users access MountPoints2. No one can access MountPoints2 and only you can change the permission. Do you want to continue* "> **Yes** > **OK** 2 times> close the Registry Editor> restart the system.

And now, you can safely connect the USB to the computer even though it is infected with Autorun.inf because you have completely disabled the registration of the mobile device information on MountPoints2 and the devices. Automatic setting up of these devices.

Note: The article only shows how to disable the operation of MountPoints2 to prevent Autorun.inf's intrusion but does not encourage you to delete it even though you can still do this without doing affect the operation structure of Windows. ***Good luck!***

You finished reading the article "**Prevent Autorun.inf from infiltrating your computer via USB**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.