

PE_LUDER virus removal procedures for computers and USB drives

Information Technology Services, Kansas State University
updated Oct. 30, 2007

In order to fully remove the PE_LUDER virus from computers, please follow the instructions below.

Note: Trend now recognizes a piece of the PE_LUDER.ch virus as **WORM_SMALL.JBC**. This malware is not a new infection. It is Trend cleaning up pieces of the malware it did not recognize previously.

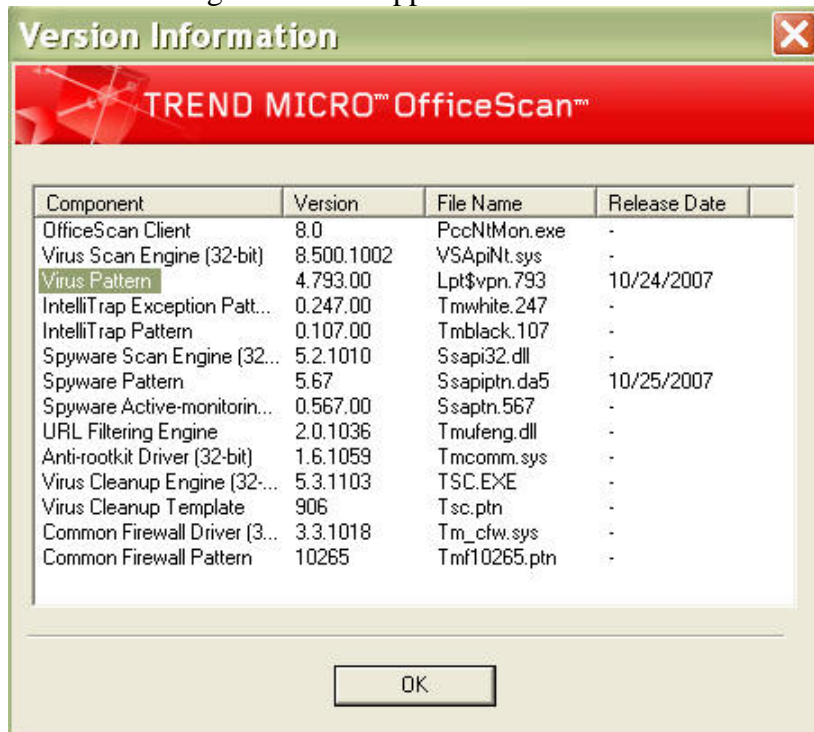
For Computers

1. Right-click **My Computer** and then click **Properties**.
 2. Click the **System Restore** tab.
 3. Click the **Turn off System Restore** check box and then click **Yes**.
 4. Click the **Start** button and then click **Run** to open the Registry Editor.
 5. In the **Run** box, type **REGEDIT** and then press **Enter**.
 6. In the left panel, double-click
HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>services>wuauserv
 7. In the right panel, locate **ImagePath = "%System%\drivers\svchost.exe"**
 8. Right-click the **value name** and then click **Modify**.
 9. Change the **value data** to **%System%\system32\svchost.exe -k wugroup**
 10. In the right panel, locate **Description = "{Chinese characters} Windows {Chinese characters} Windows Update {Chinese characters}"**
 11. Right-click the **value name** and then click **Modify**.
 12. Change the **value data** to **Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.**
 13. Close the Registry Editor.
 14. Perform an update on the Trend Micro client and then perform a complete system scan. Virus Pattern File 4.794.00 or higher is required.
- Note: If Trend cannot clean or quarantine the svchost.exe file, reboot the system then perform a manual scan again.

How to tell what virus pattern file you have

1. Right-click on the Trend Micro icon  in the system tray.
2. Click **Component Versions**.

3. The following screen will appear:



4. In the third line, you will see **Virus Pattern**. Confirm that the pattern file has been updated to version 4.794.00.

For USB Devices

Once Trend is updated to virus pattern file 4.794.00 or higher it will quarantine the setup.exe file on any external devices. Users will have to manually go in and delete the autorun.inf file.

1. Click **My Computer** to find the drive letter of the USB device. Drive 'E:' will be used in the instructions that follow.
2. Click **Start** and then click **Run**.
3. In the **Run** box, type **cmd** and then click **OK**
4. In the new window that appears, type the drive letter of the USB device (Example: F:) and then press the **Enter** key
5. Type **attrib** and then press **Enter**
6. Type **attrib -s -h E:*.*** and then press **Enter**.
7. Type **del E:autorun.inf** and then press **Enter**.