Steps to remove W32.Sasser.Worm and W32.Sasser.A Viruses

The following steps are to be used to remove the W32.Sasser.Worm and W32.Sasser.A viruses. Please perform each of these steps as outlined below.

These viruses take advantage of a flaw in the LSASS.EXE file within Windows XP. Microsoft released a patch for this file on 4/13/04 to remove the flaw. eMachines also released a BigFix Fixlet to all eMachines customers advising them to download the patch.

Please note: If you have performed the steps outlined on our phone message, please start with Step #3.

Step #1: Enabling the Internet Connection Firewall

1.   Restart your Computer

2.   Once you are in Windows please click on Start, then click on Run.

3.   In the Run window, type **ncpa.cpl** in the Open Box.
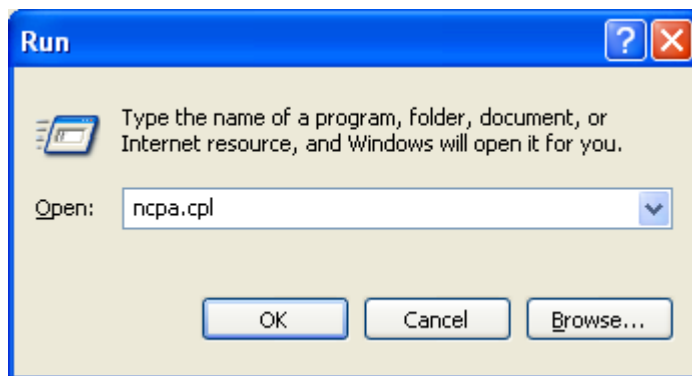

4.   Click on the OK button.

5.   In the Network Connections Window that appears you will see multiple items in the white area. We will be enabling the Windows Internet Connection Firewall on all of these items.
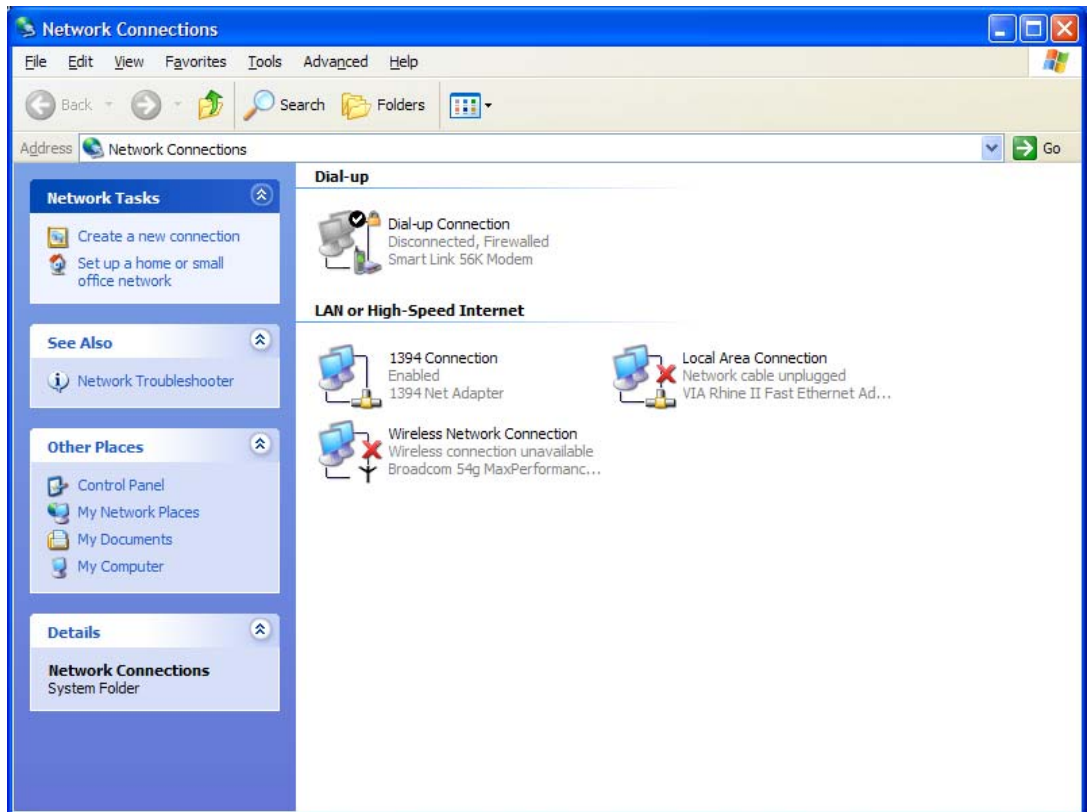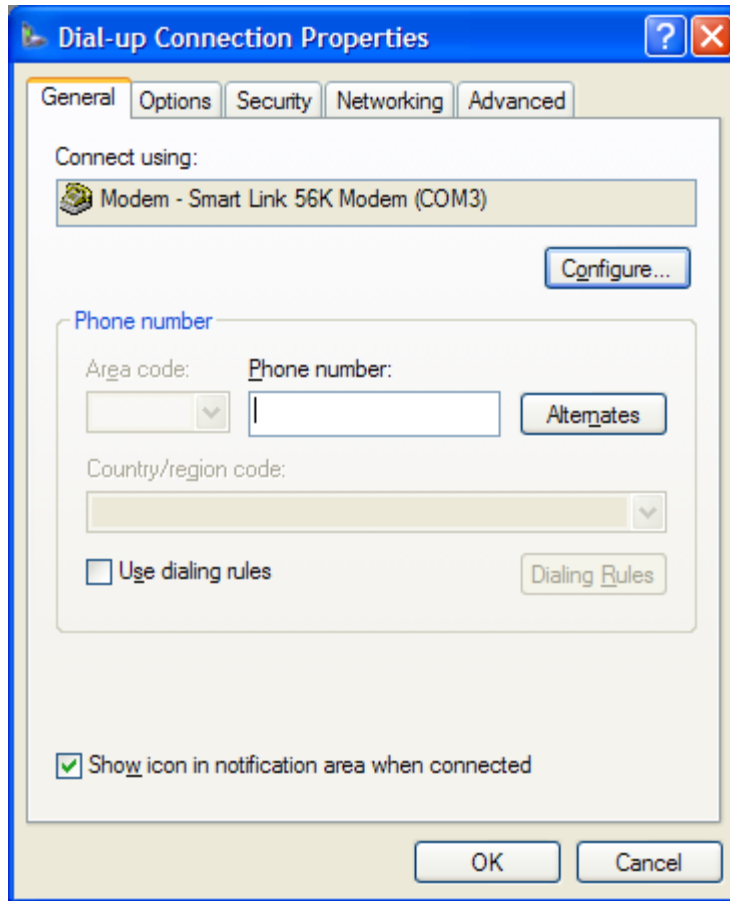
Please note that the icons on your screen may differ from those in this picture.
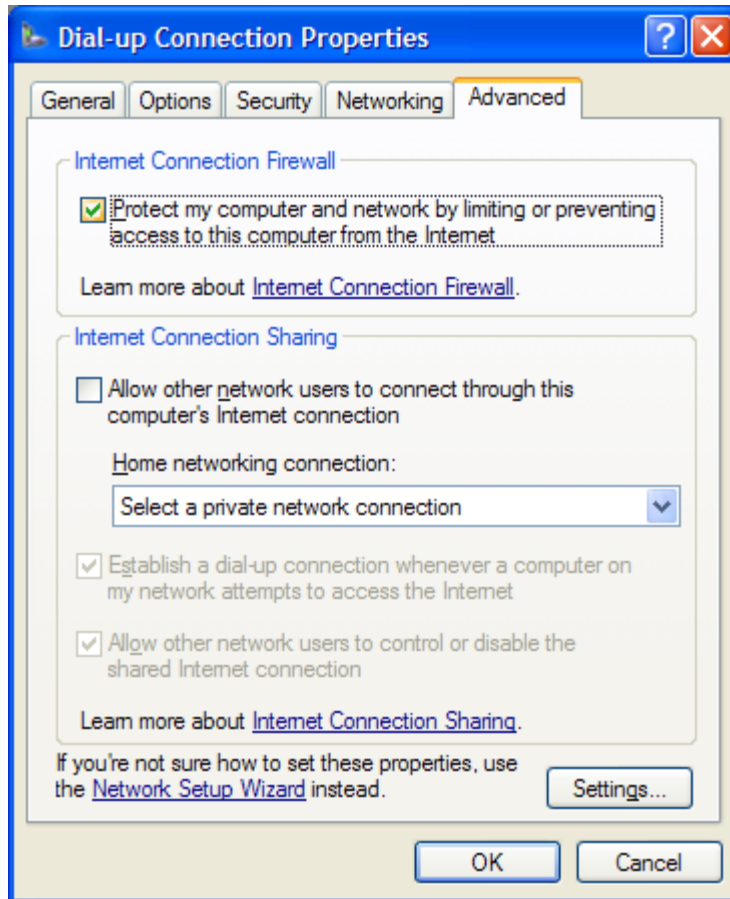
6. Place your mouse over the first icon and right-click on the icon. A box should appear. Please left-click on the PROPERTIES line.
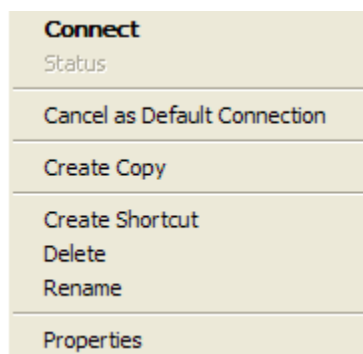
7. A new window will appear. Click on the tab labeled **Advanced**.

8. On the **Advanced** tab put a check into box next to "Protect my computer and network by limiting or preventing access to this computer from the internet."

9.   Then click on OK.

10.   Repeat Steps 6-9 on all the icons in the Network Connections Window.

11.   Once you have completed the steps for all icons within the Network Connections Window you should see a small lock symbol next to each of the icons.
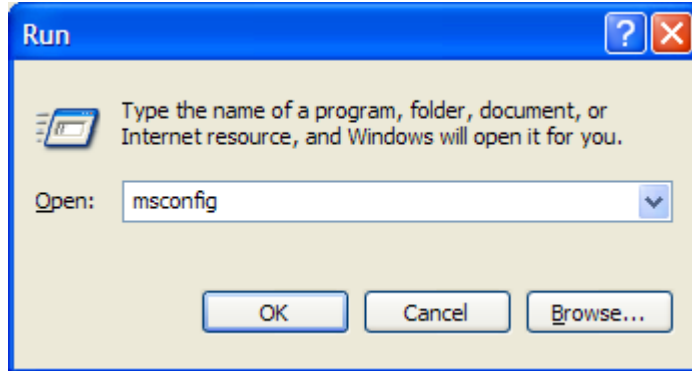

12.   You have now enabled the Internet Connection Firewall on all of your connection devices.

13.   Please close the Network Connections window.
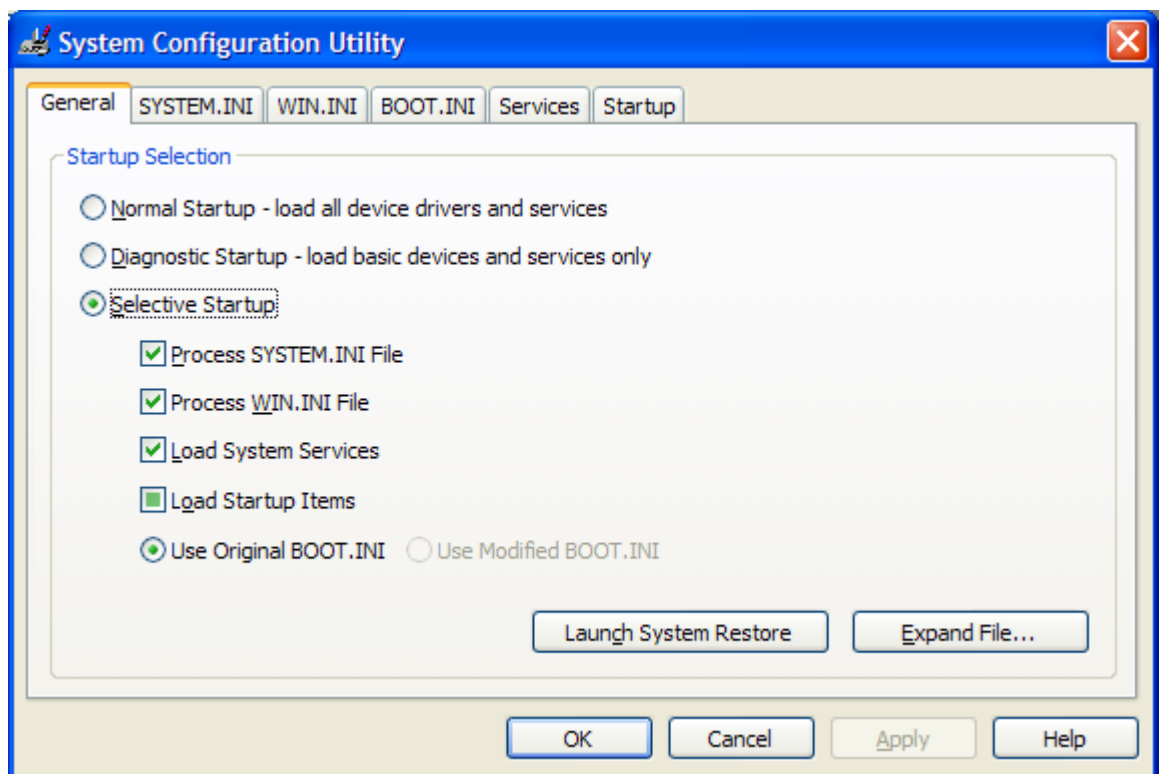
Step #2: Disabling the Virus from Loading

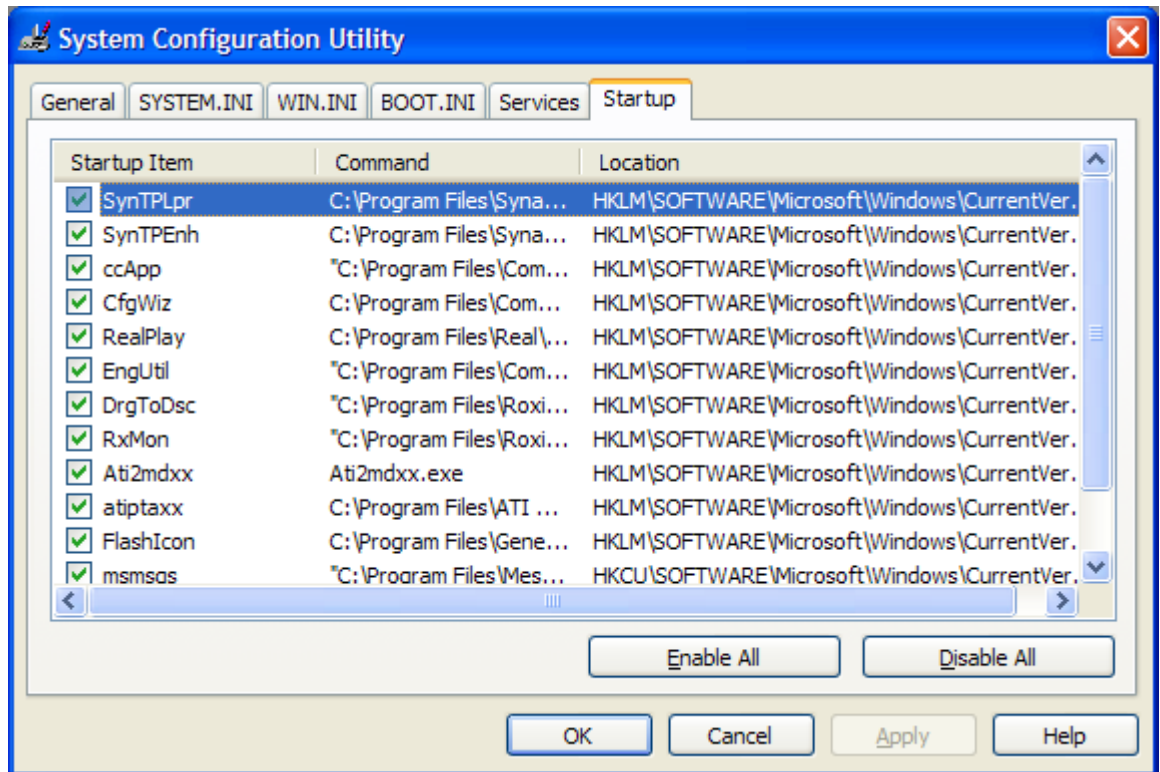1.   Click on Start and then click on Run.

2.   In the Run Window type MSCONFIG.


3.   Click on the OK Button.

4.   In the System Configuration Utility Window that appears, click on the
        Startup tab at the top.

5.   On the Startup Tab, look for the Startup Item named AVSERVE or
        AVSERVE2.

6. Remove the check in the box if you locate any items that say AVSERVE or AVSERVE2. Please scroll down also if there are more items listed than can be displayed in the window.
   a. If you cannot locate AVSERVE or AVSERVE2 on the Startup tab it is likely that you do not have the W32.Sasser.Worm or S32.Sasser.A virus.

7. Click on OK to make the necessary changes.

8. A new window will appear named System Configuration.
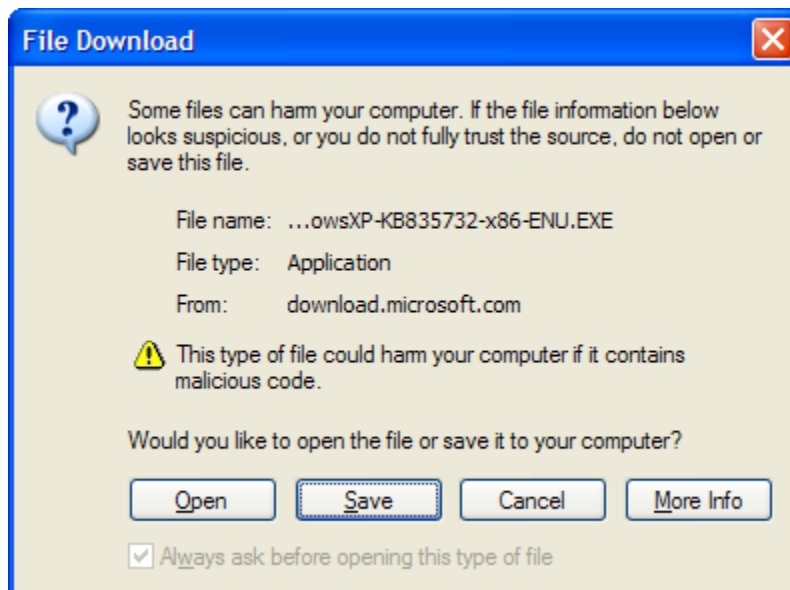
9. Click on the **Restart** button.
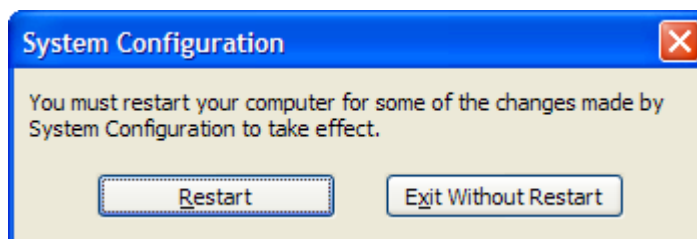
10. Your system will now shut down and restart.

11. You have now disabled the virus on your computer from loading.

12.   When the system reboots a window will appear stating that your settings
        have changed. This is due to us disabling the virus. Put a check in the
        box that states "Don't show this message or launch the System
        Configuration Utility when windows starts." Then click on OK.

Step 3: Downloading the Microsoft Update

1.   Connect to the Internet.

2.   Click on this link:
        http://download.microsoft.com/download/6/1/5/615a50e9-a508-4d67-
        b53c-3a43455761bf/WindowsXP-KB835732-x86-ENU.EXE

3.   The following window will appear. Click on the OPEN button.

4.   Your computer will now download the patch from Microsoft and install it.
        The file is 2.58 MB in size. Depending on your Internet Connection this
        can take a few minutes.

5.   Once the patch has been downloaded, Windows will start the installation
        Procedure.

Windows XP KB835732 Setup Wizard

Welcome to the Windows XP KB835732 Setup Wizard

Before you install this update, we recommend that you:

- Back up your system

- Close all open programs

To complete this installation, Windows might require restarting after you finish this wizard.

To continue, click Next.

< Back   Next >   Cancel
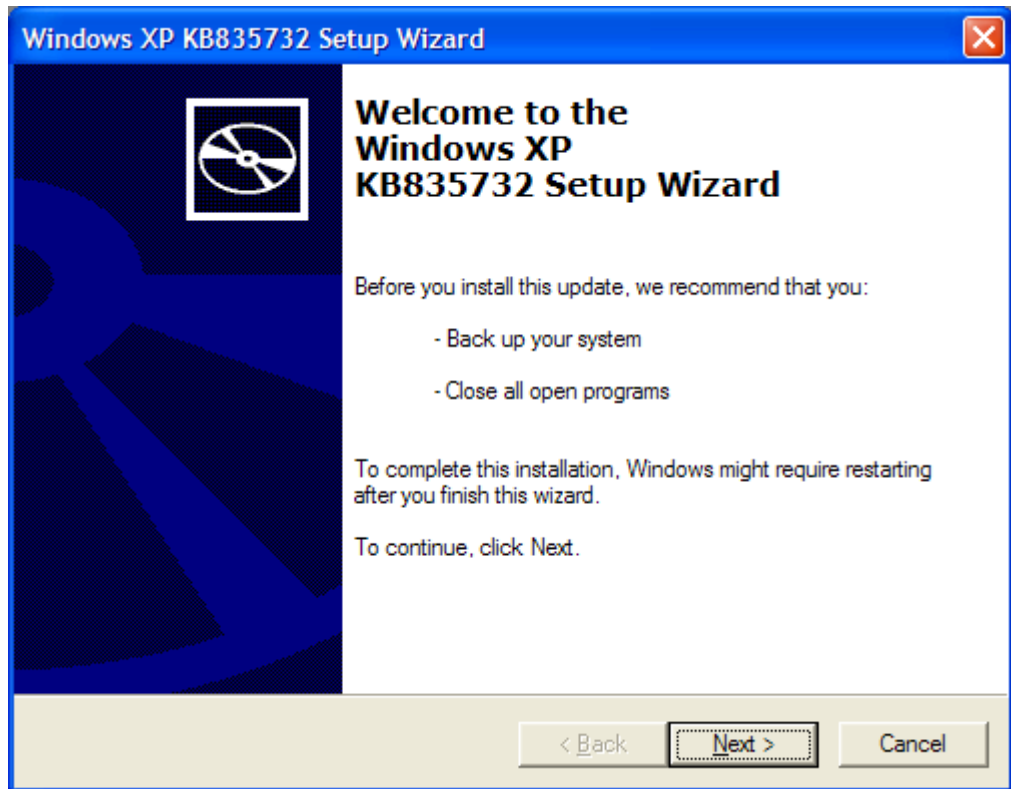
6.   Click on Next to start the Installation.

7.   Windows will then ask you to agree to the License Agreement. Please read the document carefully. To continue, you must put a dot in " I Agree". Click on Next to continue.

Windows XP KB835732 Setup Wizard

License Agreement

Please read the following license agreement. To continue with setup, you must accept the agreement.

> SUPPLEMENTAL END USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE ("Supplemental EULA")
>
> IMPORTANT: READ CAREFULLY - The Microsoft operating system components accompanying this Supplemental EULA, including any "online" or electronic documentation ("OS Components") are subject to the terms and conditions of the agreement under which you have licensed the applicable Microsoft operating system product described below (each an

I Do Not Agree   I Agree   Print

< Back   Next >   Cancel

8. The patch will now be installed on your computer. When it is complete you will see the final screen and can click on the check box labeled "Do not restart now" and then click on **Finish**.

9. You have now successfully installed the patch to prevent infection from this virus.

**Step 4: Downloading the Symantec Sasser Removal Tool**

1. The final step is to clean up any left over pieces of the virus on your computer. We will download a removal tool provided by Symantec to clean your computer of the virus.

2. Click on: http://securityresponse.symantec.com/avcenter/FxSasser.exe to download the tool.

3. You will be presented with the File Download window. Click on Open to download and run the application.
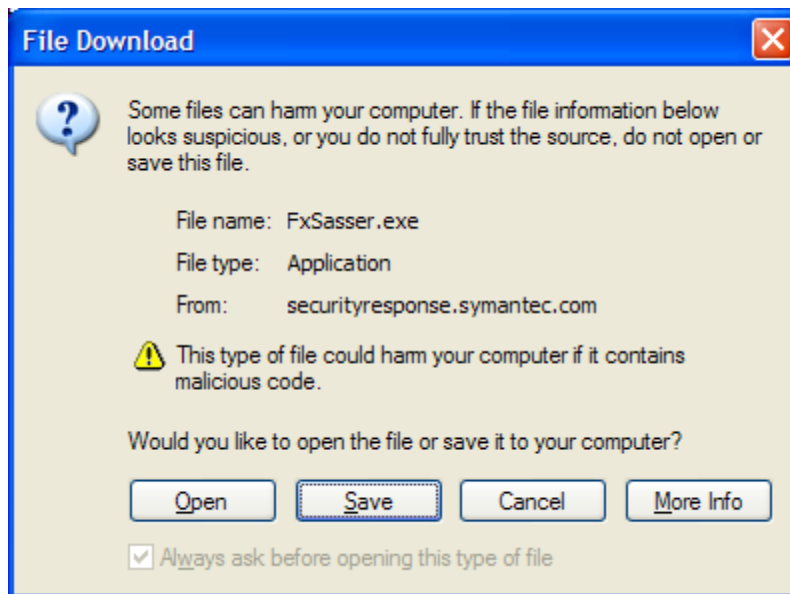
4.   Windows will now download the file and launch the removal tool.
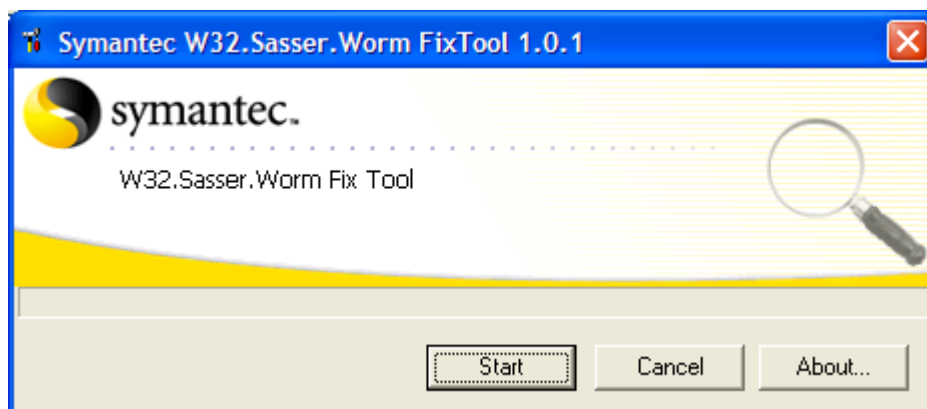
5.   Click on Start to launch the program.

6.   The program will now scan your computer for the virus and remove it, if it is found.
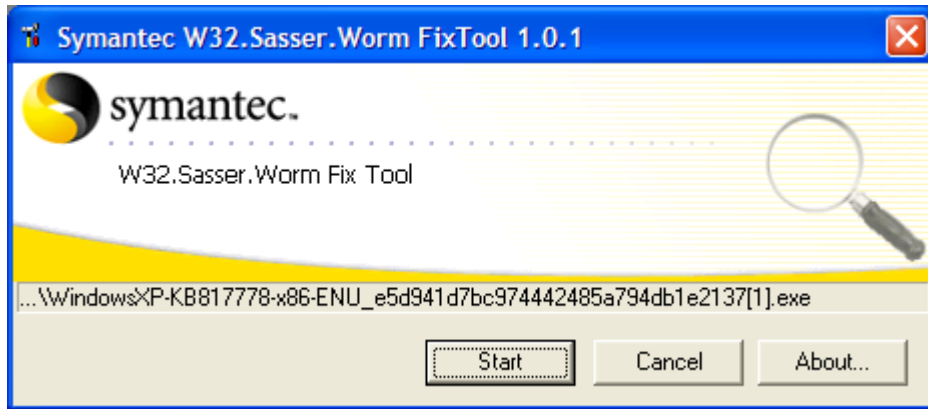
7. The scan can take awhile since it does check your entire Hard Drive for the virus. Please be patient.

8. When the scan is complete the tool will notify you if the virus was located and deleted or was not found on the computer.

9. You have removed the virus from your computer if it was to be found.

10. Furthermore you should also be safe from future W32.Sasser.Worm and W32.Sasser.A virus attacks.

11. Please restart your computer to finalize all changes.

In the future eMachines recommends to all of our customers that you check for updates to Windows on a weekly basis. Go to http://windowsupdate.microsoft.com and scan for updates. eMachines also recommends that you check your BigFix updates weekly for items that eMachines feels are critical to your computer's security.

Microsoft released the patch you downloaded on April 13, 2004. Whoever downloaded the patch at this time was safe from the attack that was released on May 1, 2004. eMachines also released a BigFix Fixlet informing all of our customers of this update and recommended that the update be downloaded and installed immediately.

eMachines Customer Support

If you would like to talk to a technician who can walk you through these steps, you can call our fee based support lines at: 1-800-229-1103 (Billed to a Credit Card) or 1-900-263-4899 (Billed to your phone bill)