
Please help with my FreeFixer log [an example]

Posted by freefixer - 2007/11/13 15:08

Hello,

I'm having some problems with one of my computers. I suspect it is infected with malware. Please help analyze this log:

FreeFixer v0.25 log
http://www.freefixer.com/
Operating system: Windows NT 5.1
Log dated 2007-11-13 10:09

UserInits (1 whitelisted)
C:\WINDOWS\System32\ntos.exe

Winlogon Notify (9 whitelisted)
winhld32 - C:\WINDOWS\System32\winhld32.dll

TCP/IP settings
HKLM\..\Interfaces\{BC24B697-4C1E-4D3C-89B7-B171BA2A583F}, NameServer = 85.255.116.147,85.255.112.6
HKLM\..\Parameters, NameServer = 85.255.116.147 85.255.112.6

Registry Startups
HKCU\..\Run, MSMSGSGS = "C:\Program\Messenger\msmsgs.exe" /background
HKCU\..\Run, userinit = C:\WINDOWS\System32\ntos.exe

Autostart shortcuts
MSWin-2068753958.exe, , C:\Documents and Settings\Roger\Start-meny\Program\Autostart\MSWin-2068753958.exe

Processes (13 whitelisted)
C:\Program\FreeFixer\freefixer.exe

=====

Re:Please help with my FreeFixer log [an example]

Posted by securitywonks - 2007/11/26 12:22

Dear freefixer,

Go through the following instructions and do accordingly,

STEP 1:

If you are using Windows ME or Windows XP, you need to disable System Restore to make sure that the malicious files and registry entries that you will remove, donot get restored when you restart your computer back in Normal Mode.

For clear instructions,

- a) Right Click "My Computer"
- b) Select "Properties" in the drop down menu
- c) Select "System Restore" tab
- d) Check "Turn Off System Restore on all drives".
- e) Click "ok".

STEP 2:

Now Turn Off Your Computer and Start your computer up in safe mode.

For clear instructions,

- a) Print these instructions before you begin as you will not have access to them while your computer is off.
- b) Click "Start", then click "Turn Off Computer" and then in the opened dialog box, Select "Restart" button" and click OK.
- c) Allow your computer to power down completely. When it begins to reboot, press F8 repeatedly until a boot menu appears.
- d) Use the arrow keys to select the "Safe Mode with Networking" option and press "Enter" key.
- e) Select the operating system you would like to load (Windows 2000 or XP or whichever Windows version you use) and press "Enter" key.

STEP 3:

- a) Open FreeFixer
- b) Please select the following entries and (after closing all other windows), just Click "FIX"

C:\WINDOWS\System32\ntos.exe

C:\WINDOWS\System32\winhld32.dll

HKCU..Run, userinit = C:\WINDOWS\System32\ntos.exe

MSWin-2068753958.exe, , C:\Documents and Settings\Roger\Start-menu\Program\Autostart\MSWin-2068753958.exe

- c) After fixing them, restart your computer and take a new FreeFixer log in the Normal Mode and post it here.

=====

Re:Please help with my FreeFixer log [an example]

Posted by freefixer - 2007/11/27 22:26

Thank you very much! I've pasted the new log below. Please help me find the bad items.

FreeFixer v0.25 log

<http://www.freefixer.com/>

Operating system: Windows NT 5.1

Log dated 2007-11-27 21:19

UserInits (1 whitelisted)

C:\WINDOWS\System32\ntos.exe (file is missing)

Winlogon Notify (9 whitelisted)

winhld32 - (file is missing)

TCP/IP settings

HKLM\..Interfaces\{BC24B697-4C1E-4D3C-89B7-B171BA2A583F}, NameServer = 85.255.116.147,85.255.112.6

HKLM\..Parameters, NameServer = 85.255.116.147 85.255.112.6

Registry Startups

HKCU\..Run, MSMSGs = "C:\Program\Messenger\msmsgs.exe" /background

Processes (12 whitelisted)

C:\Program\FreeFixer\freefixer.exe

=====

Re:Please help with my FreeFixer log [an example]

Posted by securitywonks - 2007/12/03 13:19

Hello

select and remove the following nameserver entries,

HKLM..Interfaces{BC24B697-4C1E-4D3C-89B7-B171BA2A583F}, NameServer = 85.255.116.147,85.255.112.6

HKLM..Parameters, NameServer = 85.255.116.147 85.255.112.6

your log looks improved,

All the best with your system

=====