

Things to Check to Fix Your Internet Connection After Malware Infection

Tools Reference: to be kept on your flash drive

Farbar Scanner, DNSFix, MicrosoftFixIt50199.msi, MicrosoftFixIt50267.msi, Avira DNS Repair, Complete Internet Repair, LSPFix, Winsock Repair, ICRTTool
You can download all of them here:

<http://www.gegeek.com/documents/Downloads/Repairs/InternetRepairKit.zip>

- 1> Run a cleaner
- 1> Run Farbar Scanner
- 2> Read resulting log file for issues at take appropriate action.
- 3> Run Regedit
- 4> Go to HKEY-LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES
These registry keys typical get infected by malware
You can copy these from a non-infected machine and import them here
TYPICALLY THESE REG KEYS ARE HIT: AFD, DHCP, TDX, NETBT, NDSWAN, NDIS, TCPIP, TCPIPREG AND A FEW MORE.
- 5> It's a good idea to get copies of these from non-infected machines for an emergency repair and save them by Windows version.
- 6> There are Some files you should save as well from a clean system or refer to the article here on extracting files from Windows OS disks
- 7> This is all in preparation for what FarBar finds.
- 8> Make sure the following services are running:
DHCP CLIENT, DNS CLIENT, NETWORK SERVICES, TCPIP NETBIOS HELPER
- 9> Next tool to use is called MiniToolBox
Select Reset DNS, Reset IE/FF Proxy (Firefox settings), THEN HIT GO
- 10> Next tool to use is DNSFix - Avira DNS Repair
- 11> Next tool is to repair the TCP/IP Stack - MicrosoftFixIt50199.msi
- 12> Next thing is to reset the hosts file. - MicrosoftFixIt50267.msi
- 13> Here's a batch file you can create that does the same thing as 10-12

@echo on

```
pushd\windows\system32\drivers\etc
```

```
attrib -h -s -r hosts
```

```
echo 127.0.0.1 localhost>HOSTS
```

```
attrib +r +h +s hosts
```

```
popd
```

```
ipconfig /release
```

```
ipconfig /renew
```

```
ipconfig /flushdns
```

```
netsh winsock reset all
```

```
netsh int ip reset all
```

```
shutdown -r -t 1
```

- 14> And finally there's a tool called Complete internet repair which covers all the above tools mentioned above and more. Check it out!
- 15> IE - Tools - Internet Options - Check home page
- 16> Goto Advanced Options and reset all options to default
- 17> Go to the security tab and check the Trusted and Restricted sites entries
- 18> Now check all your Add-Ons for IE under tools
- 19> Now Firefox - same things to check here. Add-Ons, Plugins, Extensions
In the address bar type in: about:config and PRESS ENTER
- 20> Type In: "keyword.url" just as it is here.
Check to see if it has been changed
- 21> Check all of FF's security options under Options - Privacy, Security
- 22> Try your portable Firefox Browser you always carry with you. ;)
- 23> Two more tools we can use is LSPFix and Winsock Repair
- 24> Another great tool is ICRTTool