Step-By-Step PC Virus Repair/Removal Guide for the Home/Power User - Optional Sections are for Power Users.
Hopefully this Article is Both Educational and Useful for Both the Advanced Home and Power User.

Your Mind Set is Important When trying to Clean Infected Systems. Be Patient and Methodical.
Cleaning Infections can be very time consuming and frustrating at times, so you need to have a patient mind set before you start. Most Advanced Home Users can step through this guide and save themselves both time and money. A lot of the procedures outlined here are what your Local Tech guy might perform as well, so you can get a jump on the cleaning process and same some time. Below you will find some of the best tools around, as of this writing. So your chances for success are excellent. I've tried to be very thorough and include every reference/tool along the way to help clean your PC, as well as educate you. I've also tried to address the needs of the power user as well with some advanced tools/procedures you may not have known about before.

Also if you are a Power User helping out a family member or friend, this a good guide to direct them to just to get them started to help themselves, until your services are needed or until you can be available to help. All the initial time consuming basics are covered, which could save you some precious time.

Note: Here is a 30 minute instructional video on cleaning malware by Britec - Definitely Worth Watching!
Britec has a really badly infected PC and cleans the machine with all free tools.
Remove Malware For Free 2013 by Britec

Contents of the Guide

Some Preliminary Notes/Steps Before We Start:

a, Are You Really Infected or is Windows Just Damaged?
How Do I Know I am Infected? What are the signs? Click Here.

b. Understanding Virus Names
How can I find out the name of the virus I am infected with?

c. Backup Your Data Before You Do Anything Else!!!
Now is the time to think about transferring all those important docs, songs and pictures if you did not do it before.
Suggestion- Create a folder called backup on an external USB drive and transfer your files.
Once your system is clean you can then turn your attention to that folder and scan through the files to make sure they were not affected.
The best program I've seen for this is a piece of shareware call Fab's AutoBackup listed on my homepage. Used by all PC Tech's

Note: If you are unable to launch windows you can still save your data with a Rescue CD.
Boot from the CD and launch the built-In Navigator. Have you external USB drive connected. Navigate to your Data Folder and simply copy
the files to your external USB drive.
List of Rescue CDs or ***My Pick*** Hirens Boot CD.zip

Article - Emergency Kit - How to save your files from a dead OS

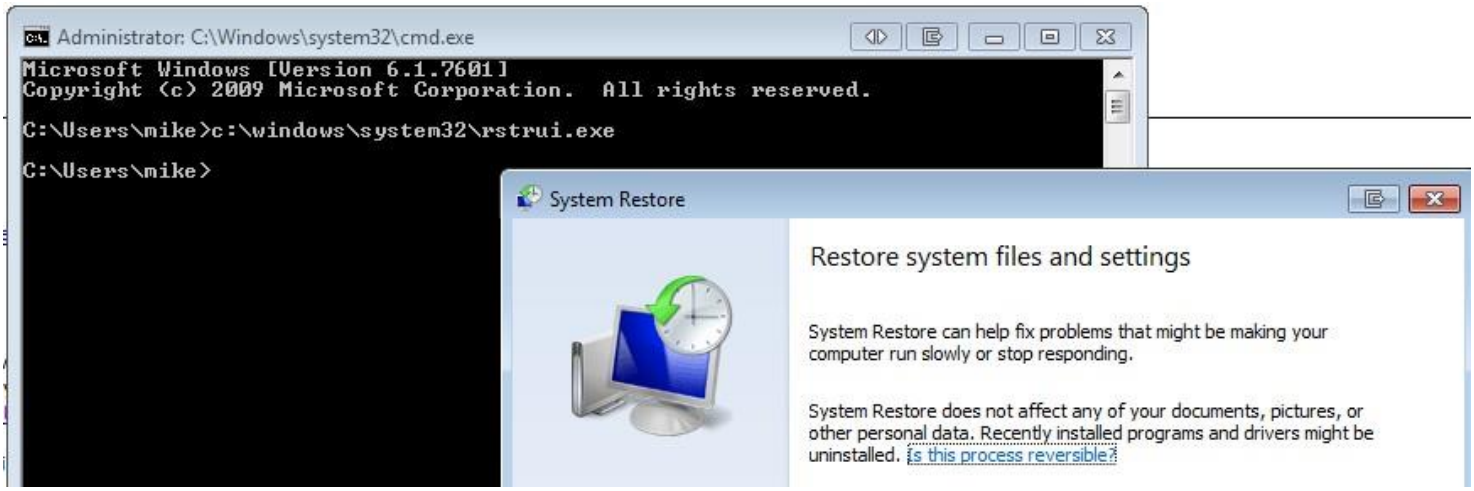
Step 1 - Everything is Backed Up, So let's Begin!

Unless otherwise stated, all procedures listed here should be performed from within Safe Mode if Possible.
If asked to reboot that return to Safe Mode immediately afterwards.

Note: If you cannot get into safe mode due to infection, then download safemodefixer and run that to fix Safe Mode.

First thing to try is System Restore.
Often overlooked or forgotten, which could possibly provide a very quick resolution to your problem, is System Restore.
Windows has a feature called System Restore that can restore your registry to a previously known good state.
It's worth a shot. You can also download the System Restore Mgr to aid you in the restoring process of a restore point.
Using Windows 7 or Vista System Restore
How to use System Restore to fix a Windows 8 PC

Note: If you are unable to launch the GUI for the System Restore utility due to the infection, then go to Start, type in Run, then Cmd.exe
At the DOS Prompt type in the following:
c:\windows\system32\rstrui.exe
This will launch the System Restore Utility shown below: Select the date that you know your computer was not infected.
Reboot normally and test. If still infected go back to safe mode and continue.



top

Step 2 - OK, Everything is backed up and System Restore Did Not Work. Some Basic Environment Pre-Work Preparation is Necessary.

Unless otherwise stated, all procedures listed here should be performed from within Safe Mode if Possible.
If asked to reboot that return to Safe Mode immediately afterwards.

Note: If you cannot get into safe mode due to infection, then download safemodefixer and run that to fix Safe Mode.
Note: It might also be a good idea to read ahead and download all the following programs ahead of time from a clean PC if possible.

a. Disable UAC in Vista/Windows 7 (Just to speed things along during our repair process. Turn it back on later)
goto Start menu--> in search box type UAC--> Drag it down to lowest level--> ok.

b. Unhide all Hidden files.
The How To Procedure for every version of Windows is located here.
For Windows 7 I've listed the steps here

Close all programs so that you are at your desktop.
Click on the Start button.
Click on the Control Panel menu option.
When the control panel opens click on the Appearance and Personalization link.
Under the Folder Options category, click on Show Hidden Files or Folders.
Under the Hidden files and folders section select the radio button labeled Show hidden files, folders, or drives.
Remove the check mark from the check box labeled Hide extensions for known file types.
Remove the check mark from the check box labeled Hide protected operating system files (Recommended).
Press the Apply button and then the OK button..
Now Windows 7 is configured to show all hidden files.
Make sure to Hide all Folders again when finished with this document!

c. Disable ALL currently installed Anti-Virus programs

or any other security product (Just to speed things along during our repair process)
The link below shows how to disable your security application if you are not sure.
http://www.techsupportforum.com/security-center/virus-trojan-spyware-help/490111-how-disable-your-security-applications.html
Use Control + F on that page to search for your Antivirus on how to disable it.
Turn it back when finished with this document.
It's ok to reboot if necessary, but return to safe mode.

d. Turn System Restore OFF and Delete All old restore points

It's assumed you tried system restore first. Since system restore did not work, we will not be needing any of these previous restore points
now since they might be infected anyway. Viruses have been known to make themselves resident in the Windows System Restore section,
which is a protected area, **Read Only!** How to turn System Restore Off
Turning System Restore off **deletes** all these possibly infected files.
Re-enable when your pc is clean!
It's ok to reboot if necessary, but return to safe mode.

e. Delete the Hibernate file - hiberfil.sys - I personally disable this on all desktop's anyway.

The hiberfil.sys file is hidden and by default is not visible in Windows Explorer, or accessible by any application, including anti-virus programs.
Control Panel - Power Options, select the Hibernate tab in the Power Options Properties, Clear the Enable Hibernation check box.
Reboot Re-enable when your pc is clean!
It's ok to reboot if necessary, but return to safe mode.

f. Delete the Swap File - pagefile.sys - As a security option it Should be set to "Clear page file at Shutdown" Go here for that fix: AutoFix

Many viruses like to hide here as well. The only way to delete it is to set your swap file size to zero and reboot. Re-enable when done!
Go to the Control Panel, System, Advanced, Performance, Settings, Virtual Memory
Change the page file swap size to zero (No Paging File) and reboot.
Re-enable when your pc is clean!
It's ok to reboot if necessary, but return to safe mode.

g. Delete Temp Files

Go to Start, Run and type %temp% this will open a folder with all the temporary files on your computer.
Delete all these files. Use Ctrl + A and press the del key.
How To Delete Temporary Files in Windows XP
How To Delete Temporary Files in Windows 7
How To Delete Temporary Files in Windows 8
Download CCleaner and Run as Well

Note: Sometimes Viruses prevent or disable Internet Explorer/Network Connections from working so you can't download files.
Here's a program that you can use to repair your internet connection/ Internet Explorer Complete Internet Repair
Try and get a 2nd copy of Opera, Firefox or Chrome downloaded from your 2nd PC or from your friend and install that as well.

A portable browser might be a good alternative here as well. Portable Firefox

h. Check for a malicious proxy server - This will prevent internet access as well.
Some forms of Malware may add a proxy server which prevents the user from accessing the internet
Start IE, Tools, Internet Options, Go to the tab Connections. At the bottom, click on LAN settings.
Uncheck the option Use a proxy server for your LAN
MiniToolBox - http://www.bleepingcomputer.com/download/minitoolbox/ Can do this for you.

l. Make sure MSConfig is set to Normal Startup Mode
How to use MSConfig

k. Reboot and go back into safe mode immediately and
continue with Running Malware Removal Programs in Step 3..

top

Step 3 - Running Malware Removal Programs

Unless otherwise stated, all procedures listed here should be performed from within Safe Mode if Possible.
If asked to reboot that return to Safe Mode immediately afterwards.

Note: If you cannot get into safe mode due to infection, then download safemodefixer and run that to fix Safe Mode.
Note: It might also be a good idea to read ahead and download all the following programs ahead of time from a clean PC if possible.

Note Some viruses will block the execution of certain antivirus programs by their name. I have in the past been successful by simply renaming
the .exe file to a temp name and the antivirus program was then able to run no problem.
Ex: For MalwareBytes rename **mbam.exe** to **explorer.exe** and it should run.
OR if programs will not execute run the program below.
Run FixExec -
http://www.bleepingcomputer.com/download/fixexec/
FixExec is a program that is designed to fix executable file associations for the .bat, .exe, and .com file extensions.
Run this is you cannot execute any programs

Part 1 - General Infection Removal - Run all of these. Takes time so be patient!

a. Run RKILL
http://www.bleepingcomputer.com/download/rkill/
Attempts to terminate all known Malware processes so that your security software can then run and clean your computer of infections
Just double click the file you downloaded.
Don't reboot until the end of this section if possible.

b. Run AdwCleaner
www.bleepingcomputer.com/download/adwcleaner/
AdwCleaner is a program that searches for and deletes Adware, Toolbars, Potentially Unwanted Programs (PUP), and browser Hijackers.
Don't reboot until the end of this section if possible.

c. Run Junkware Removal Tool
http://thisisudax.blogspot.com/2012/09/junkware-removal-tool-jrt-by-thisisu.html
Many of the infections we see on the forums and in the work environment nowadays involve a user that has an unwanted program,
toolbar, or browser helper object (BHO) on their computer. The tool is designed to remove all traces of these types of programs which

includes services, registry values, registry keys, files, and folders. The tool will also restore some default settings for Internet Explorer
and Mozilla FireFox. Google Chrome is not supported (perhaps in future).

d. Run Malwarebytes anti-Malware
http://www.malwarebytes.org/products/malwarebytes_free
It's ok to reboot if necessary, but return to safe mode.

e. Run HitManPro
http://www.surfright.nl/en/hitmanpro/
It's ok to reboot if necessary, but return to safe mode.

f. Run SpybotSD __ Optional
http://www.safer-networking.org/en/download/
It's ok to reboot if necessary, but return to safe mode.

g. Run Emsisoft Emergency kit scanner __ Optional
http://www.emsisoft.com/en/software/eek/
It's ok to reboot if necessary, but return to safe mode.

h. Run SuperAntiSpyware __ Optional
http://www.superantispyware.com/
It's ok to reboot if necessary, but return to safe mode.

Part 2 - RootKit Removal - Run the First Two at a minimum.

a. Run TDSS-Killer
http://support.kaspersky.com/faq/?qid=208283363
Note: If TDSSKiller will not open, download and run FixTDSS from Symantec.
It's ok to reboot if necessary, but return to safe mode.

b. Run Trend Micro RootkitBuster
http://www.bleepingcomputer.com/download/trend-micro-rootkitbuster/
It's ok to reboot if necessary, but return to safe mode.

c. Run Combofix - Optional
http://www.bleepingcomputer.com/download/anti-virus/combofix
(very useful for trojans and root kit removal.which not caught by major AV tools)
Read the instructions carefully!

d. Run GMER (ONLY FOR EXPERTS) Optional
http://www.gmer.net/
(best for manual removal of rootkits,includes cmd shell,registry,process)
-double click file-->select rootkit/Malware'-->remove detection-->close

Part 3 - Fake Security programs - Run only if they apply! Optional

a. Run remove fake-antivirus
http://freeofvirus.blogspot.com/2009/05/remove-fake-antivirus-10.html
If you know the name of the Ransomware you are infected with you can search here for a specific fix.
OR Search here for a Ransomware program with the name that matches your Infection.

Part 4 - At this Point Your System Should be Clean. Perform a Normal Reboot and Verify all System Operations.

Re-enable the Following Items You Disabled
Turn UAC Prompts back to where it was last set.
Check to Hide all files again
Re-Enable ALL currently installed Anti-Virus programs
Turn System Restore back on
Turn Hibernation back up
Set your paging file to Let Windows Manage it
Make sure MSConfig is set to Normal Startup Mode Always

Reboot and test your system for functionality.

top

Step 4 - System Cleanup and Optimization

Note: I always perform this step as a added precaution just in case anything was left behind/damaged after the cleanup.

a. Run Advanced System Care Free __ Optional
http://www.iobit.com/advancedsystemcarepro.html
This is a complete maintenance suite utility program that I typically have running on my system everyday.
At this point in time, if we assume your PC is clean, it's a very good idea to have this program scan your entire system for errors and optimize your system. It even has a Malware scanner included as part of its scan.
I would also recommend that you leave this program installed and periodically scan your system with it to maintain system health. I use it myself and have never had an issues with its repairs.

Reboot and test your system for functionality.

If Malware was removed but functionality is now compromised then continue on to Step 5.

top

Step 5 - Post Virus Removal Repair

We may have been successful in removing the virus but very often damage was left in its wake. Some functions may not work!
Verify all your system's functionality and then address the issues remaining with the programs listed below.
Note: I actually created a whole page just for Port Virus issues here since this is a very common issue with cleaning systems.

a. Run Windows Repair (All In One) if functions are not fully restored.
http://www.tweaking.com/content/page/windows_repair_all_in_one.
With Tweaking.com - Windows Repair you can restore Windows original settings.
For Windows XP, 2003, Vista, 2008 & 7 (32 & 64 Bit)

b. Run Security-Restore
http://www.softpedia.com/get/Security/Security-Related/Security-Restore.shtml

d. **Run complete internet repair**
http://www.petrichorpost.com/2013/09/complete-internet-repair/
Bonus Program - if needed - **Repair Internet Explore**r - http://www.tweaking.com/content/page/repair_internet_explorer.html

e. **Run Renable**

http://www.tangosoft.co.uk/index.html
Re-Enable was designed to repair the left over damage caused by Viruses,Malware,Trojans

f. Disk Heal
It allows you to fix common errors which are caused by certain viruses.
http://www.computer-realm.net/diskheal

g. Repair all damage left by the Malware - Read this article for more details
http://www.techsupportalert.com/content/how-fix-malware-infected-computer.htm

top

Step 6 - Protection Going Forward

Obviously you need better protection for your system going forward. I also have a Security page here as well.

a. Disable Autorun of Any Programs - Recommended Setting.
http://www.disableautorun.com/

b. Add MVPS Hosts File updates
http://winhelp2002.mvps.org/hosts.htm
Simple program that adds almost 10,000 known bad sites to your hosts file and blocks these sites from loading.
Probably the single most important and simple fix you can take to protect yourself online.

c. Use WOT (Web of Trust)
http://www.pcworld.com/downloads/file/fid,73058/description.html
Warns You / Ranks sites as you surf.

d. Here is a Complete List of all Windows Security Settings/Measures you can take to protect yourself in the future.
A complete listing of all security settings on your PC and an explanation of how it protects you.
Highly recommended to at least acknowledge their existence/understand how all these work.

e. Install a Different Antivirus - Many of these are free.
http://www.filehippo.com/software/antimalware/antivirus
http://www.pcmag.com/article2/0,2817,2400355,00.asp

f. Latest Report of How All the Antivirus Programs Were Ranked as to Their Effectiveness - Report is from Nov 2013

Antivirus-Comparatives Report as of Nov 2013: **Kaspersky was ranked best Antivirus/Anti-Malware program.**

	Sample											Points
	1	2	3	4	5	6	7	8	9	10	11	∅
AhnLab	DD	AA	AA	AA	BA	BA	AA	AA	AA	AB	DD	75
Avast	AA	AA	AA	AA	AA	AA	BA	AA	CA	AA	BC	87
AVIRA	AA	AA	AA	AA	AA	AA	AA	AA	BA	BB	AC	92
Bitdefender	AA	AA	AA	AA	AA	AA	AA	AA	AA	AB	AC	97
BullGuard	AA	BA	BA	BA	BA	AA	AA	BA	AA	BC	DD	73
Emsisoft	AA	AA	AA	AA	BA	AA	AA	AA	CA	BB	DD	79
eScan	AA	AA	AA	AA	BA	BA	AA	AA	AA	AB	DD	85
ESET	AA	AA	AA	AA	AA	AA	BA	AA	AA	BC	BC	88
F-Secure	AA	DD	AA	AA	AA	AA	AA	AA	AA	BC	BC	82
Fortinet	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	DD	91
G DATA	AA	AA	AA	BA	BA	BA	AA	AA	CA	DD	BC	73
Kaspersky Lab	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AC	98
Microsoft	AA	AA	BA	AA	AA	AA	AA	BA	AA	BA	DD	83
Panda	AA	AA	AA	AA	AA	AA	BA	AA	AA	AB	DD	87
Sophos	AA	AA	AA	AA	BA	AA	AA	AA	BA	BC	BC	85
ThreatTrack Vipre	BA	BA	BA	AA	BA	BA	BA	BA	CA	AB	DD	65

Note: Keep in mind that even though Kapersky ranked the highest, it usually comes with a performace hit on your machine, in my experience. Good security usually requires greater resources and stolen cpu time. So compare different security suites and note the performace of each.

g. Run the Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)

http://www.microsoft.com/en-us/download/details.aspx?id=7558

This program can identify missing security updates and common security misconfigurations.

h. Run All of the following Windows Microsoft Auto Fix-It Solutions

Fix security issues to protect and secure Windows automatically

Diagnose/Repair Windows security problems by turning on UAC, DEP protection, Windows Firewall and other Windows security options and features.

Automatically fix Windows security settings to keep your PC safe

Diagnose/Fix Windows security settings for IE, Windows firewall, group policy, Registry, UAC; check Windows Update and antivirus software status.

Fix Windows system performance problems on slow Windows computers

Automatically troubleshoot and repair performance problems. Improve, optimize and speed up Windows computers and make slow running PCs faster.

i. Good article to read as well.

Prevent Ransomware: Steps to take to stay protected & secure

top

Home User Final Thoughts

NOTE: At this point your system should be clean if indeed you found some viruses/spyware and successfully cleaned them from your system. Try booting up normally and test the system once again. If the virus/spyware persists then it's time to think about a reload or seeking professional help.

If at this point you need to ask for help, then these sites below are excellent in providing free repairs.
Simply log your problem and follow instructions to the letter. More often than not they are successful.

Recommended Malware Forums
BleepingComputer *My Pick*
GeeksToGo Forum
MalWareTips Forum

If you do decide to seek out help from a forum, The site might ask for either an OTL Log or HiJackThis log.
These programs scan your system for every pertinent Windows location. It would be nice to have these ready.

OTL Log Generation:
Download OTL to your desktop or other convenient location.
Download OTL
OTL is does not need to be installed, simply click OTL.exe to run.
Click the Quick Scan button.
A log will open in notepad, and OTL.txt will be saved to the same location as OTL.exe (i.e.: desktop)
Copy and paste this text into the Forum post for expert analysis.

HiJackThis Log Generation
Download HiJackThis
How to Run a Scan with HiJackThis

Programs/Tools/References Mostly for Power User's

Step 7 - From This Point on is My Recommended List of Tools/Procedures for the Power User if you are Still Infected. Optional

Note: Here are a couple of tools I would also recommend worth learning for the more advanced/adventurous users are:
Using these tools below I have removed some viruses in literally a matter of minutes. Sometimes you get lucky, but you need to have some
experience/knowledge about these programs and where viruses/spyware typically hide in order to be successful with them.

Advanced Programs List:
Autoruns - Great tool to peek into all the Window's hidden locations where virus/spyware can hide. How To Use Autoruns or Here
Adwcleaner - Searches for and deletes Adware, Toolbars, Potentially Unwanted Programs (PUP), and browser Hijackers.
ComboFix - Scans your computer for known Malware. Cleans systems where others have failed.
Comodo Cleaning Essentials - Combo of tools - Analyzer and Scanner
Comodo Killswitch - Runs like process explorer but scans and compare files to online database.
Comodo Autoruns - Runs like Autoruns but scans and compare files to online database.
D7 - My new favorite tool. Still learning all the In's and Outs of it but it is quickly becoming my go to tool.
HiJackThis - Scans startup / hidden locations and generates a log file which you can submit to the url below or a forum for help.
Junkware Removal Tool - Searches for and removes common adware, toolbars, and potentially unwanted programs (PUPs)
Kaspersky TDSKiller - A Rootkit scanner.
OTL - Diagnostic scanner for all pertinent windows locations.
Process Explorer - Process Explorer shows you information about which handles and DLLs processes have opened or loaded.
Process Monitor -Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.
RegScanner - Viewing the list of Registry keys modified in the last hours/days.
Registry Locations Where Malware Hide - Nice article by BleepingComputer.com noting locations in the registry to check.
RKill - Attempts to terminate known Malware processes so that your normal security software can then run and clean your computer of infections.
Services - How Malware hides and is installed as a Service

Startup Database - This database will allow you to search for programs that you find starting automatically on your computer
Trojan Killer - A Rootkit scanner
Unlocker - For times when you cannot delete a file/folder
Ultra Virus Killer - UVK - A suite of tools to aid in the exploration of your infected system.
Virus Removal Guide - *Latest* virus threats and their removal instructions

Manually Remving Malware - List of All Loading Points
Manually Remving Malware.pdf

Note: Here's a Reference of All Windows Startup Locations to Search Manually where Malware typically hides.
Bleeping Computer Windows Startup Locations
System Lookup Database
Services to Watch for and Their Locations

Note: These Sites Maintain Exact Removal Procedures for Specific Viruses by Name
Updated List of Viruses from BleepingComputer.com
Latest Viruses Listed Here
Kaspersky List of Tools
AVG List of Tools
Symantec List of Tools
Malware Tips List
BriTec Malware
Remove Specific Malware by Name
FBI or Police Theme Ransomware

You can also search this database of known Malware Startup programs for help determining whether or not suspicious files/programs are dangerous.

Windows Startup Database

Computer running Slow?
Take back control of your PC!

Filename to search for:

Search

Powered By:
BleepingComputer.com
Add this search to your site!

top

HiJackThis - This program scans all typical Malware locations and creates a log file for you to upload to professionals for analysis .
Or you can submit the logs to these automated log analysis engines and they can pick the more common Malware for yourself.
Download HiJackThis

For help with HiJackThis Logs

Analyzes your HiJackThis log file and the dB recommends deletions for possible infections. Be Careful if you are not sure what you are doing.
HiJackThis Analysis 1
HiJackThis Analysis 2
HiJackThis Analysis 3
HiJackThis Tutorial - Very detailed tutorial about all locations within the HiJackThis program.
HiJackThis Help

OTL Reference - Scans Your System for All Pertinent Windows Locations and reports its findings.
Download OTL
OTL Tutorial 1
OTL Tutorial 2
OTL Video by BriTec

Note: Bootable Malware Rescue/Antivirus Rescue CDs

Anvi Rescue Disk
Avira Rescue System
Avira USB
AVG Rescue CD
AVG Rescue USB
BitDefender Rescue CD
Bitdefender USB
Comodo Rescue CD
Dr Web LiveCD
ESET SysRescue
ESET Rescue USB
FixMeStick-USB
F-Secure Boot CD
G Data Boot-CD
HitManPro Kickstart USB
Kaspersky Rescue CD
Kaspersky USB
Kaspersky DiskUpdater
Norton Recovery Tool
PC Tools CD
Panda SafeCD
Sophos CD
Spybot Rescue CD
Trend Micro
Trinity Rescue Kit
Vba32Rescue
Vipre Rescue
Vipre Rescue USB

Excellent Tutorials on the Use of Autoruns and Process Explorer.

Fighting Malware Mark Russinovich
Process Explorer - SysInternals
Process Monitor - SysInternals
Autoruns - SysInternals
Fighting Malware: Viruses, Spyware 1/8
Fighting Malware: Viruses, Spyware 2/8
Fighting Malware: Viruses, Spyware 3/8
Fighting Malware: Viruses, Spyware 4/8
Fighting Malware: Viruses, Spyware 5/8
Fighting Malware: Viruses, Spyware 6/8
Fighting Malware: Viruses, Spyware 7/8
Fighting Malware: Viruses, Spyware 8/8

Note: How to Create a Clean PE Environment for Testing:

Creating a Clean Environment For Testing of your PC

top

GE Geek