How to clean virus and malware infections Tips & Tricks

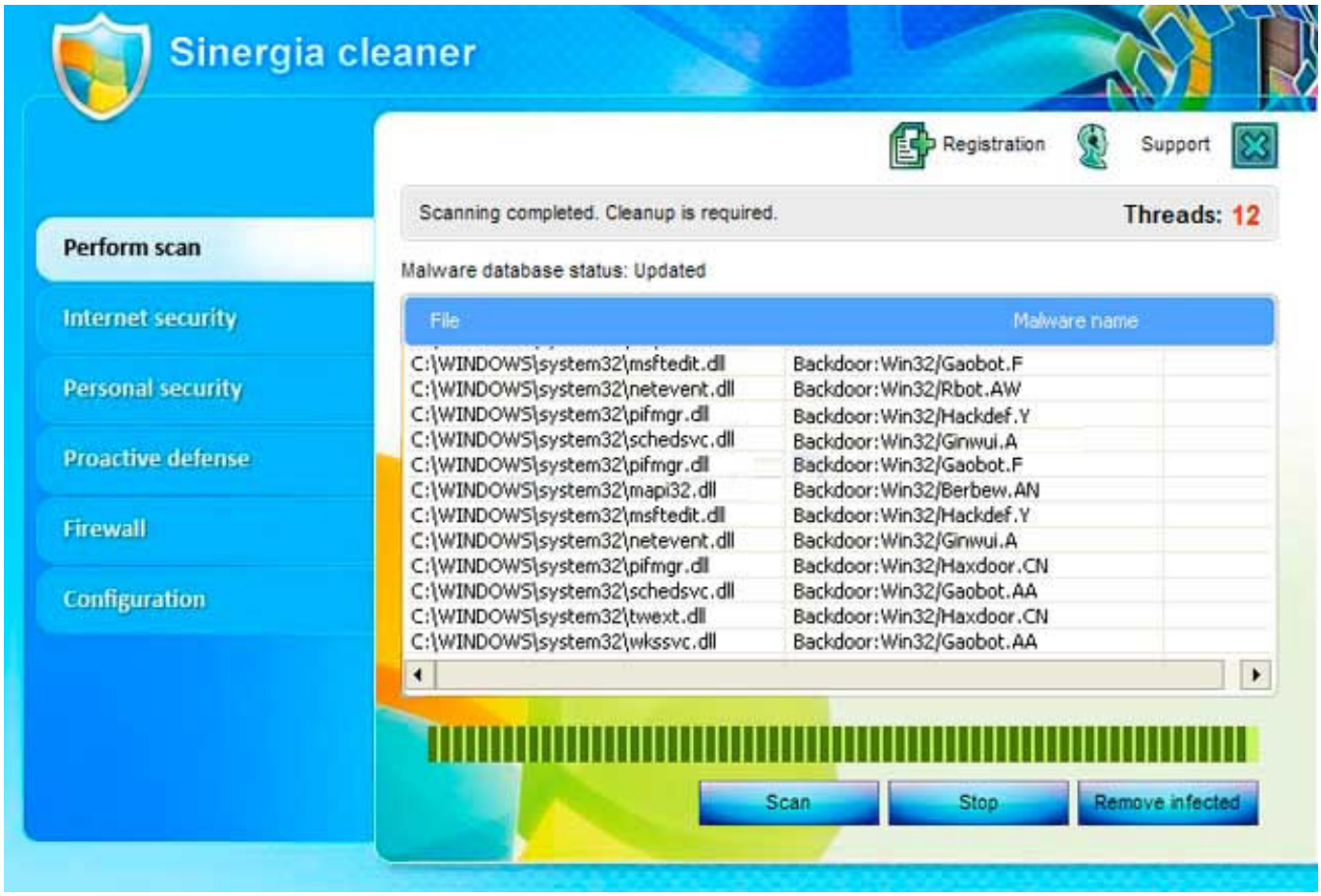
Let's get straight to the point.

Depending on the malware type, you may get away only by using the infected computer to perform self-cleaning.But if you suffer from a more sinister intrusion type, you will need another computer with an internet connection and a USB stick or any other type of removable storage to copy the needed files to infected pc.

(1) Always **do your best to find out the malware name or intrusion type.** 60-70% of times if you find the virus name or type, you will easily find a tool to get rid of it. Many antivirus companies make small applications free for download that remove certain types of viruses. To find a virus name, look at your **desktop** for any unknown new icons, check your **antivirus log** (it has possibly detected it but unable to remove, it will display the name or type), look for obvious things like suddenly you have a program called "Registry Cleaner" or "Microsoft Antivirus" or "Speed optimiser" etc. Very often **malware will pretend to be helping you**, in a very nice looking application layout it will be showing you all these problems with your machine etc. , but instead its all fake. So **"Google" the name and you will find out instructions or tools to get it out.**

EXAMPLES OF VIRUSES PRETENDING TO BE ANTIVIRUS:


Antivirus 2010
Antivirus 2010
Stay protected from the latest threats
Registration
Help
System Scan
Security
Privacy
Update
Settings
Get full real-time protection with Antivirus 2010
Antivirus 2010: Status
Protection level: low
Low
Medium
High
Recommendation:
Update antivirus
Virus Protection
NOT FOUND
Spyware Protection
NOT FOUND
General Security
NOT FOUND
Automatic Updating
NOT FOUND
Scan Now
Check your computer for viruses and other threats
Update Now
Download the latest protection to help keep your PC safe
Last scan: 10/7/2008 8:56:28 PM
Total scans: 3
Registration e-mail: Unregstered
Registration code: Unregstered


Sinergia cleaner
Registration
Support
Perform scan
Internet security
Personal security
Proactive defense
Firewall
Configuration
Scanning completed. Cleanup is required.
Threads: 12
Malware database status: Updated
File
Malware name
C:\WINDOWS\system32\msftedit.dll
Backdoor:Win32/Gaobot.F
C:\WINDOWS\system32\netevent.dll
Backdoor:Win32/Rbot.AW
C:\WINDOWS\system32\pifmgr.dll
Backdoor:Win32/Hackdef.Y
C:\WINDOWS\system32\schedsvc.dll
Backdoor:Win32/Ginwui.A
C:\WINDOWS\system32\pifmgr.dll
Backdoor:Win32/Gaobot.F
C:\WINDOWS\system32\mapi32.dll
Backdoor:Win32/Berbew.AN
C:\WINDOWS\system32\msftedit.dll
Backdoor:Win32/Hackdef.Y
C:\WINDOWS\system32\netevent.dll
Backdoor:Win32/Ginwui.A
C:\WINDOWS\system32\pifmgr.dll
Backdoor:Win32/Haxdoor.CN
C:\WINDOWS\system32\schedsvc.dll
Backdoor:Win32/Gaobot.AA
C:\WINDOWS\system32\twext.dll
Backdoor:Win32/Haxdoor.CN
C:\WINDOWS\system32\wkssvc.dll
Backdoor:Win32/Gaobot.AA
Scan
Stop
Remove infected

(2) Most everyday viruses can be removed by running you antivirus scan (deep/full scan). Unfortunately there is still a lot of malware out there for which you will need some more advanced tools to heal your system.

- 

RKill and **ComboFix** from Bleeping Computers, my absolute favourites. **Combinaton**

of these tools can remove 98% of viruses today.

http://www.bleepingcomputer.com/download/combofix/

http://www.bleepingcomputer.com/download/rkill/

HOW TO USE THEM:

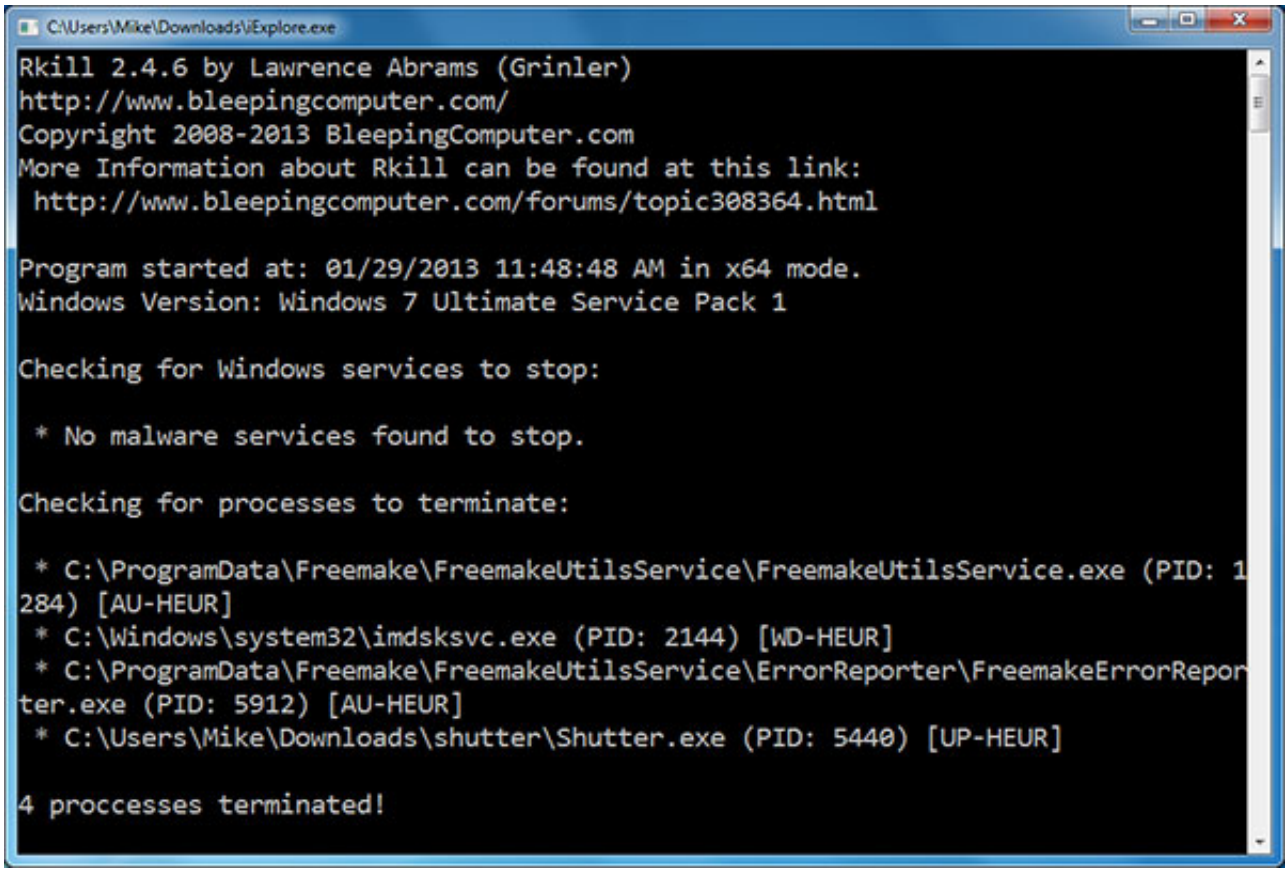
!!! IMPORTANT !!! **Only use these tools when necessary, ComboFix can damage your system in some cases, do not use if there is no intrusion. ComboFix is not an antivirus and can not be installed. It is only a tool for malware removal. DISABLE ANY INSTALLED ANTIVIRUS BEFORE RUNNING COMBOFIX. Combofix needs to be re-downloaded every time because it doesn't update the definitions like a normal antivirus, therefore make sure to grab the latest version from the link above.**

1. Once downloaded put both files (RKill and ComboFix) on your C: drive (Windows OS Drive usually C:)

2. Run RKill first with Administrator rights (right click>Run as administrator or just double click if you already have admin rights)

Rkill will open a Command Prompt (black DOS) window and start checking the system for anything out of the ordinary. It looks at the executables file association, it looks at registry, running services/processes etc. Many viruses will hook up to your system before OS boots so your Antivirus is unable to detect them and stop. RKill sees these intrusions and stops them from being in "Work in progress mode" to "Inactive" mode. It does not remove them, it only gives your antivirus some chance against them.

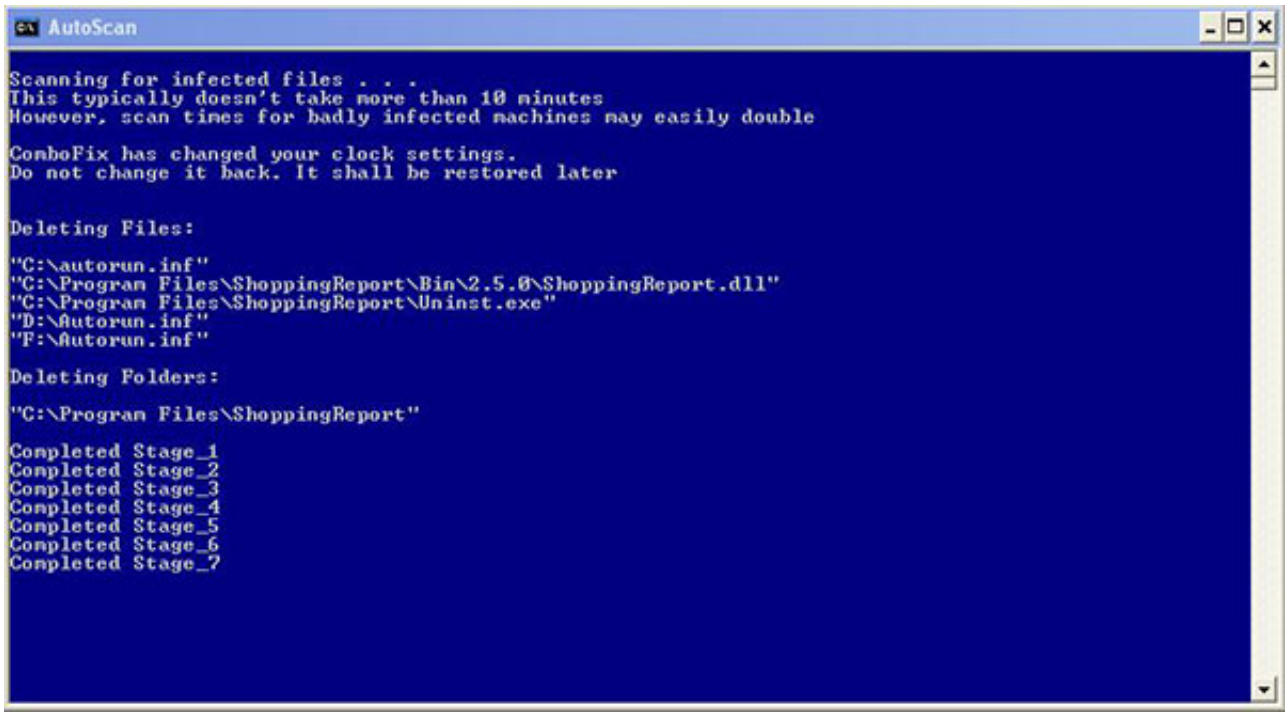
RKILL

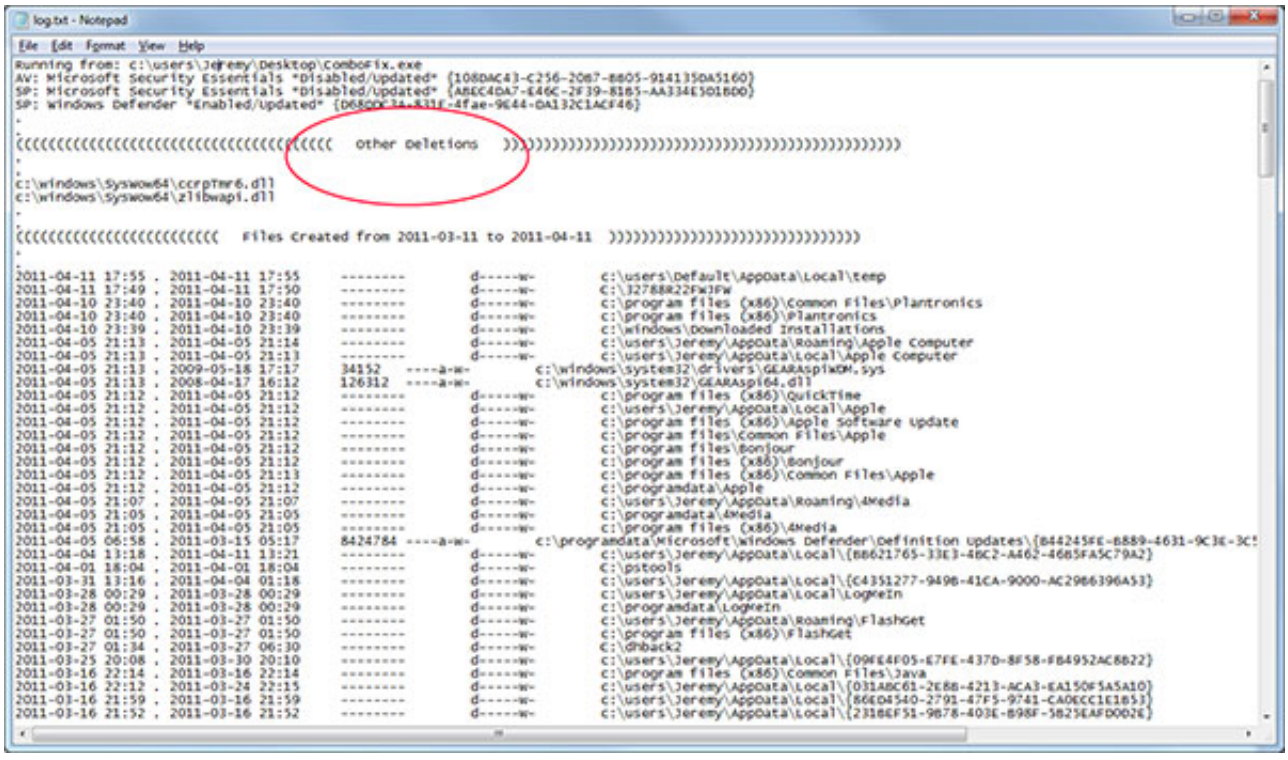


After RKill you can try and run your ordinary Antivirus software, but i recommend to run ComboFix instead. From personal experience regular antivirus programs even after RKill are unable to take the virus down.

Run ComboFix with administrator rights and follow its instructions. It is very straight forward, make sure not to interrupt ComboFix in any stage. Depending on the infection size, it may take from 5min to 1hour (yes thats right 1 hour!). Do not restart the pc on your own unless instructed. Once ComboFix is done it will show you a log file in notepad.

ComboFix





Now, to be on the safe side, reboot your PC and run the process again. RKill then ComboFix.

Rest coming soon.