THE MAGIC OF BEING HACKER

VOLUME 1

The Magic of BEING HACKER
Volume 1

Priyank Dinesh Gada
Group Flexi Production
Team Kustom Company

Edition 3
Updated – 01–04–2016

Facebook Page : www.facebook.com/webmaster.pg
Facebook Page : www.facebook.com/groupflexi
Twitter : www.twitter.com/group_flexi
Youtube : www.youtube.com/c/priyankgada

Contents :

1.1 Introduction

This book or series of book wont encourages computer hacking (unethical) or infecting (in this volume) , but rather it focuses on computer security and disinfecting . Hacking and Ethical Hacking (infecting and disinfecting) are two concepts that goes hand–in–hand . Once you know how to hack (infect) you know how to stop infection which is the inertial phase of disinfecting .

Goo.gle – All links in this volume are shortened using the google url shortener at goo.gl . This link are not malicious at all.

1.1.1 Malware – Malicious Softwares are known as malwares (mal from malicious and ware from software) . It is a kind of software that is used to disrupt computer operating and to gather some sensitive information or to gain access to private or office computer systems.

1.1.2 Computer Viruses – Computer virus is a malware program that , when executed (opened) , replicates by copying itself into other computer programs , data files , or the boot sector of the hard disk.

1.1.3 Boot Sector Viruses – Boot sector viruses sepecifically target the boot sector/master boot record (MBR) of the target harddrive or removable storage media (pen drives , etc.).

1.1.4 Trojan horse – Trojan horse is generally non–self–replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the torjan.

1.1.5 Adware – Adware is a kind of advertising supported softwarew which will automatically renders advertisements in order to generate revenue for its author .

1.1.6 Keyloggers – Keyloggers are a kind of malware which can log all keystrokes which you type. This includes your usernames , passwords as well as credit and debit card details. Keyloggers upload their log file via ftp or send it via email. Keylogger can be in the form of software as well as hardware.

1.1.7 Botnet – A botnet is a collection of programs which will control your computer and will perform tasks . This is used by hackers to commit various crimes from your computer

1.1.8 Ransomware – Ransomware is a application which will lock your computer or lock your computer and ask for money. Fake FBI Ransomware virus is the most famous ransomware.

1.1.9 Rescue Disc or DVD – Most anti–virus companies provide Rescue dvd which are bootable and which can scan your computer before starting windows. This helps to delete viruses which are imposed with windows and rescue discs also fix windows.

1.1.10 Browser Hijackers – Browser Hijackers are a kind of adware which will change browser settings and will change the home page as well as search engine providers. This might be irritating as you dont need crap engines when you have google and yahoo.

1.1.11 Malicious Toolbars – You might also find some fake toolbars which promote third party deals. This are to be removed and are termed as malicious toolbars.

1.1.12 Security News Malwares – Some time you might find some fake security news and when you click it your computer will be infected . This can be related to famous social websites getting hacked or some fake news related to youtube.

1.2 Going through Statistics

So before starting with disinfecting and infecting , lets look into computer virus statistics. Computer viruses are known to compromise private information , destroy data and harm hardware for your system. So lets start with a home or personal user statistics .

1.2.1 Home Users Statistics

Accourding to the Microsoft Security Intelligence Report and Consume Repors the following home user statistics illustrate the impact of viruses.

- 24 million households experience heavy spam
- 16 million households have experienced a serious virus problem in past two years
- 8 million housholds have had spyware in the past six months
- 1 million households lost money or compromised accounts using phishing method
- Estimated cost of all households impacted by viruses , spyware and other malwares is $ 4.55 billion.
- 40% of households are affected by viruses.

And this is legal statistics whereas almost 50% to 60% of windows users use cracked windows . Now lets look into malware threats by types . A listing of types of malwares and percentages of those that impact users .

1.2.2 Impacts of malware threats

- Viruses – 57%
- Misc. Trojans – 21%
- Torjan Downloaders – 7%
- Unwanted Softwares – 4%
- Adware and Exploits – 6%
- Worms – 2%

- Password stealers and monitoring tools – 2%
- Backdoors and spywares – 1%

Now lets see into expensive computer viruses of all time . MyDoom is the most expensive computer virus of all time which caused $38 billion in damages . It was fast moving and infecting open networks. In 2004 , this virus was estimated to impact 25% of all emails . Lets check top 10 most costly virus programs is listed below and the total amount of damages that occurred.

1.2.3 Expensive computer viruses

1. MyDoom - $38 billion
2. So Big - $37.1 billion
3. ILOVEYOUE - $15 billion
4. Conficker - $9.1 billion
5. Code Red - $2 billion
6. Melissa - $1.2 billion
7. SirCam - $1 billion
8. SQL Slammer - $750 million
9. Nimda - $635 million
10. Sasser - $500 million

1.2.4 Top 10 Countries with Most Virus Threats

As according to Kaspersky Security Bulletin, here is a listing of the top 10 countries that experience the most online virus threats and percentage of unique users impacted.

1. Russian Federation – 55.9%
2. Oman – 54.8%
3. United States – 50.1%
4. Armenia – 49.6%

5. Belarus – 48.7%
6. Azerbaijan – 47.5%
7. Kazakhstan – 47%
8. Iraq – 45.4%
9. Ukraine – 45.1%
10. Guinea–Bissau – 45.1%

1.3 Understanding BAT virus files

So lets check into bat virus commands. Most newbie or computer geek use this tool because this tricks are shared on many social media websites . Your friend

might give you some bat files in Flash Drive . Bat viruses or cmd viruse are simple dos commands which are used for bad purpose . This bat files are mostly ignored by anti–virus. So do not open any bat file instead right click on the file and click on edit or open with notepad so you can see the codes behind the file. Lets create our own bat virus to learn how it works and how they are created .

Note : How to create bat virus is just for information purpose only. We are showing this trick just to learn how they are created , how they work and some countermeasures and fixes . We are not responsible if you use it on your friends or crash others and your computer.

1.3.1 Harmful Virus 1

How it is created :

Step 1 . Open Notepad and write the following command
del c:*.* | y
del d:*.* | y
Step 2 . Save it as virus.bat

How it works :

This virus will delete every file in c and d drive but some windows files wont be deleted. It will surely delete some personal files. The best way is do not open any file without knowledge .

1.3.2 Harmful Virus 2

How it is created :

Step 1. Open Notepad and write the following commands
del ″c:\windows\system32\bootok″
/Q/S >nul
del ″C:\WINDOWS\SYSTEM32\bootvid.dll″
/Q/S >nul
del ″C:\WINDOWS\SYSTEM32\bootvrfy″
/Q/S >nul
Step 2. Save it as anything.bat (You need to go to save as and then save it in .bat format not in .txt format)

How it works :

del command will delete file in the directory given next to del command. It will give you some kind of error because boot files are deleted . You might get error ″Operating System could not start because of a faulty file″ . To fix you need to reinstall windows.

1.3.3 Computer Crashing Virus

How it is created :

Step 1. Open Notpad and write the following commands
start virus.bat
virus.bat
Step 2. Save it as virus.bat
Step 3. Click on Start – all programs – startup and place the virus.bat in that folder.

How it works :

This will open cmd many times and this will hang your

computer and when you put it in the startup folder , it will automatically start when computer is turned on. To stop this press ctrl+c to stop the script of cmd and then delete the file in startup folder. Always check autostart folder because most viruses are in the startup program.

1.4 Backup your personal and business data.

You need a external harddisk (harddisk with USB) to backup all your files and data. Copy everything to

external harddisk and keep it in a safe place . You can also use flash drives to back up small files because in some case we might need to format computers. We will focus on non formatting methods but for safety we will backup everything. You can also use cloud storage to backup your data. I would prefer cloud storage because cloud storage usually have protection against viruses and malwares and they wont get backed up on cloud but it depends on your internet plan and internet speed.

1.4.1 USB Flash Drive Backup

You can buy some flash drives and External Harddisks as per your required size. Transcend provides best external harddisks that have one click backup button and some kind of inbuild application that can backup and copy fast as shown in the figure below.

Figure 1.4.1 – External USB Harddisk

Plug the USB flash drive or External Harddisk into your computer and backup or click the backup button.

1.4.2 Online Backup Service

You can use applications like I–cloud or free applications

like google drive. You can also choose paid services listed below .

- Backblaze – 5$/month
- CrashPlan – 6$/month
- Carbonite – 59.99$/year
- SOS Online Backup – 80$/year
- Livedrive – 25$/month
- Mozy – 10$/month
- Bitcasa – 10$/month
- SpiderOak – 10$/month

Note : This charges can change without notice. You can find more information from here .

1.5 Stopping virus and malware processes.

Stopping Malicious Processes is the first step because in windows open programs or files in use cant be deleted . Some malware and viruses will prevent programs and applications from opening and will try to or will change

file associations. To stop virus and malware processes we might need to use some tools or software created by their respective programmers or companies , we do not own or pretend to own these tools.

Detection :
While opening applications you might see some popups . For example :

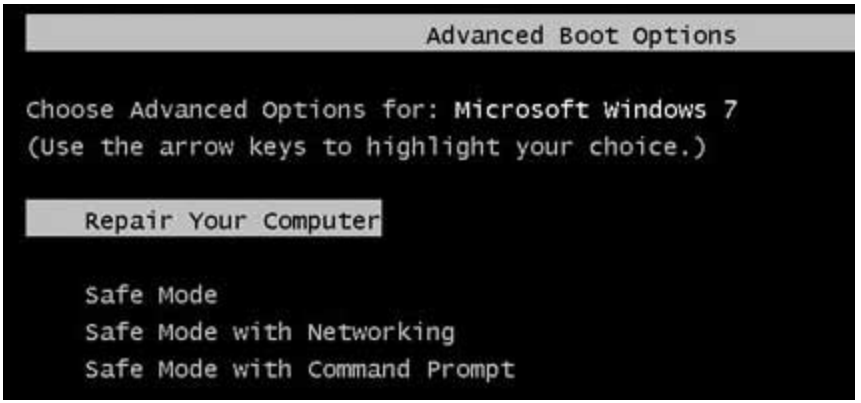
- Not a Valid Win32 Application
- The Specified Service does not exist as an installed service.

Prevention : You can use programs like **Rkill** and **RogueKiller** .

1.5.1 Entering Safe Mode : You need to first boot into safe mode . Now this might vary from windows to windows and which things and settings you are using. But i will show some common methods here.
Note : First download Roguekiller and Rkill application from the links given below because internet might not work in safe mode without networking.

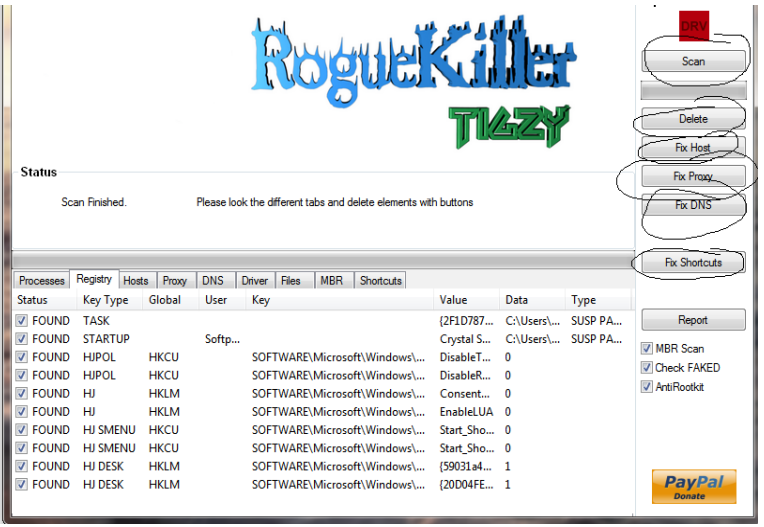
Restart your computer and keep on pressing F8 key till you get some options as shown in the picture. This is in windows 7 but it will be same in other windows also.

Figure 1.5.1 Advanced Boot Options



1.5.2 Using RogueKiller : It is a free anti–malware tool which can fix file associations.
Open and run roguekiller as admin. (Note : you might get some false positive and roguekiller might be detected as malicious tool but its not so run it as admin) Then click on scan on the top right corner as shown in picture. Once the scan is complete just delete malicious registry keys. You can click on all fixing buttons.

Figure 1.5.2 – RogueKiller

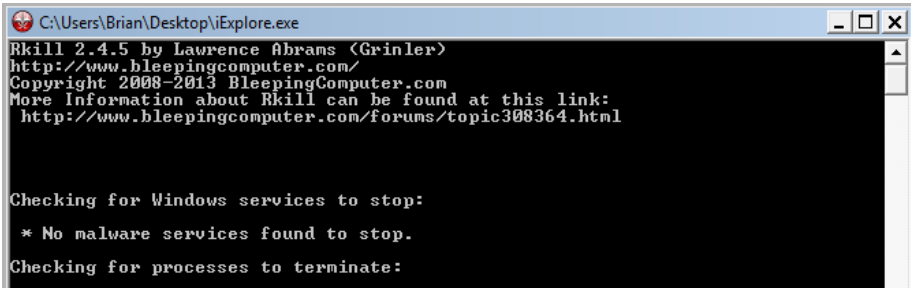


Download and open RogueKiller
RogueKiller.exe – http://goo.gl/hPtQAl
Homepage – http://goo.gl/vCyT52

1.5.3 Using Rkill : It is a free anti–virus kind of application that will detect and stop malware processes and fix file associations. Rkill is in two versions . Just run the application . Try both versions as one version might not work on some computers.

Download and open Rkill –
Iexplore.exe – http://goo.gl/zRZxaK
Rkill.com – http://goo.gl/vCFPid
Homepage – http://goo.gl/tN7jHq

Figure 1.5.3 – RKill



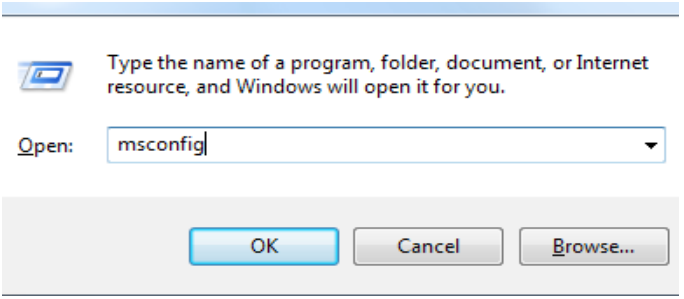
1.6 Managing Startup Applications

Managing Startup applications is necessary because even if you stop processes , there might be some applications which start when you turn your computer on. To stop this you need to manage startup applications. So lets start with it. Follow simple steps given below to manage startup application.

1.6.1 Selective Startup option.

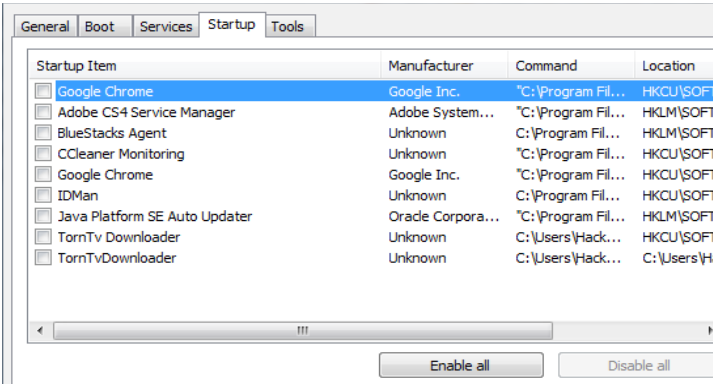
1. Turn your computer in safe mode
2. Press windows key + R or go to startmenu and lick on run

Figure 1.6.1 MSconfig



3. Type msconfig and press enter .

Figure 1.6.2 Selecting Startup Programs



Now select Startup and disable unknown programs . You can selete programs which you need to start . Deselect programs which you didnt installed or things which seems to be malicious.

4. You are now done , its time for a restart.

1.7 Dealing with Ransomware

1.7.1 Introduction

Ransomware – Ransomware are malicious software that restrict access to a computer until a ransom money is paid . This are sometime in form of FBI virus or some police blocking computer access. Below is the picture of FBI ransomware which stops you to access computer without paying money. Ransomware are usually downloaded from free porn websites . So if you have ransomware then you know what i mean :D. Ok lets start with removal. You need to perform backup and other steps shown in 1.2 and 1.3 chapter of this book. Ransomware is old and they dont happen now a days but still you need to know the removal method.

Figure 1.7.1 Fake FBI Ransomware

Some fake ransomeware are as follows :

- FBI Pornography Ransomware (as shown above)
- U.S. Cyber Security ransomware

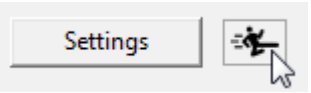
- EUROPOL virus
- Internet Complaint Center

1.7.2 Using Kickstart

Download HitmanPro Kickstart –
Kickstart.exe32.bit – http://goo.gl/y3Ufeh
Kickstart.exe64.bit – http://goo.gl/FPvphU
Homepage – http://goo.gl/dGQFm5

Note : You need to download this application from other computer and copy it into a flash drive. Then go to your computer and into safe mode (read 1.2 and 1.3 for safe mode) and run the applications and click on kick icon at the bottom of the screen.

Figure 1.6.4 Kickstart



Now follow the onscreen instructions and this will create a kickstart USB flash drive. Restart your computer now and make sure USB is plugged in. Go to the boot menu and boot from the pendrive.

Note : Boot key might vary from computer to computer. Usually F12 and Esc key are used as boot menu. You can see the onscreen instruction when turning your computer on. You can see the boot menu key there. For example here boot menu key is F11

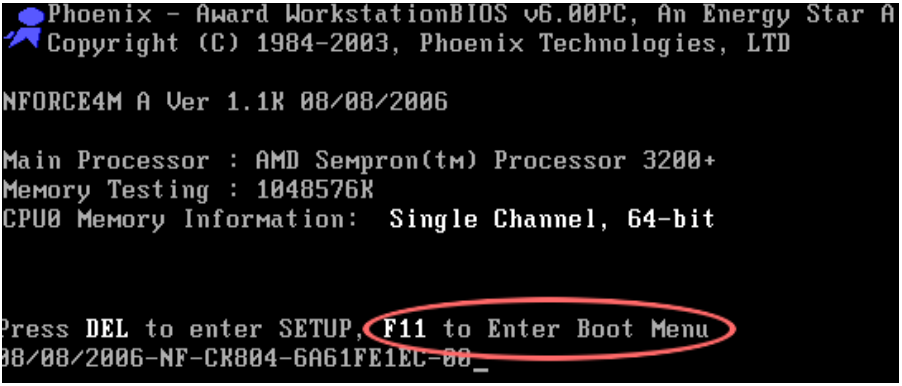
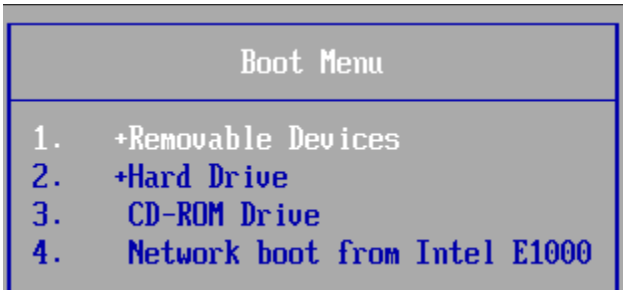


Figure 1.7.2 Entering Boot Menu

Press the key before windows start and select the pendrive or flash drive inserted (if you are late then note the key and restart your computer) . Select USB flash drive letter or Removable Devices and press enter.

Figure 1.7.3 Boot Menu

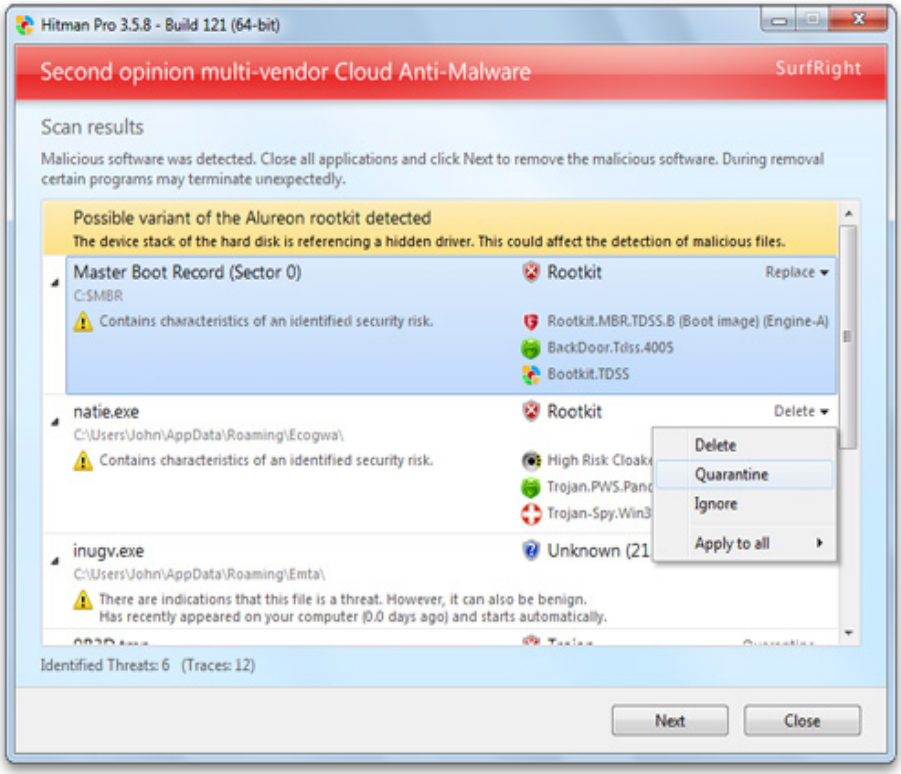


Now wait and follow the on–screen instructions. After some time you will be asked . Then click on next and again next then activate free license and click on next to remove the ransomware . Restart your computer and remove the USB drive . You are free form ransomware.

1.7.3 Using Hitman Pro

Hitman pro can be used to remove rootkits and other boot sector malwares . Best anti-malware tool.

Figure 1.7.4 Hitman Pro



1.8 Dealing with viruses

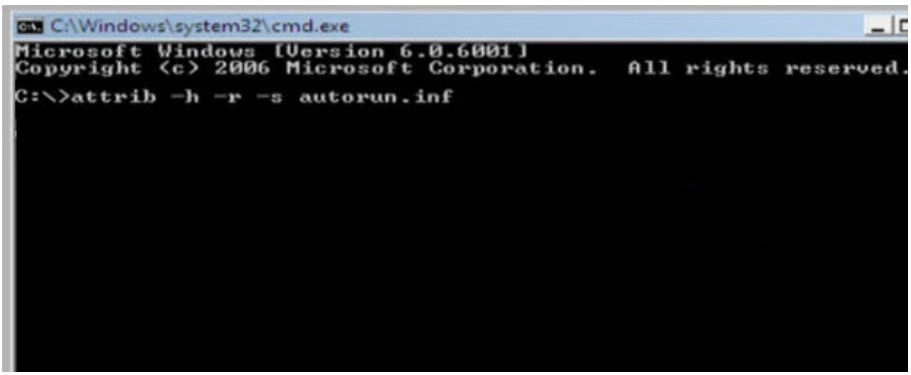
The first malware to deal with is a virus. So lets learn how to remove most common viruses .
Autorun.inf – Autorun.inf is a most famous virus which copies itself to various medias such as USB drives as well as external harddisk. You might see some unknown files on your Flash drives.

1.8.1 Removing autorun.inf

Autorun.inf Removal – Method 1

1. Click on start and run then type cmd and click ok.
2. Now a black window (command prompt) will start. You need to type the following commands.
3. Cd\ (press enter and type it again till you get to the root directory i.e. Till you see the c:\ )
4. attrib –h –r –s autorun.inf (type this and press enter as shown in the figure below.)

Figure 1.8.1 CMD commands



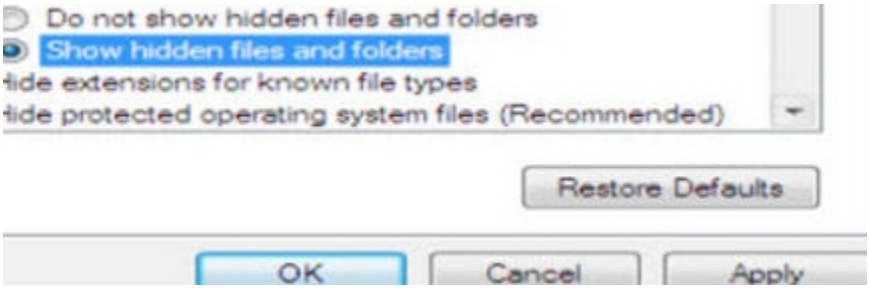
5. del autorun.inf (now type this and press enter. Here we are deleting autorun.inf)

6. d: (type d: and do the same process from step4 again)
7. e: (type e: and do the same process from step4 again)
8. Restart your computer.

Autorun.inf Removal – Method 2 – Registry edit method

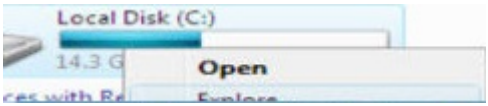
1. Open any folder and click on tools –> Folder options

Figure 1.8.2 Show hidden files and folders



2. Click on view tab and then select ″Show hidden files and folders″ and press ok.
3. Go to my computer and right click on c drive and press explore.

Figure 1.8.3 Explorer



4. Delete autorun.inf and MS32DLL.dll.vbs or MS32DLL.dll (press shift+delete and delete it forever)
5. Click on start and click run. Then type regedit and press enter.

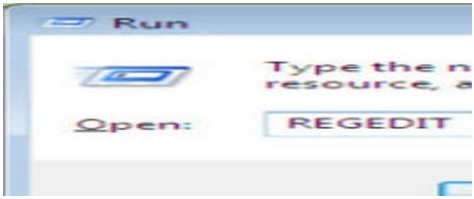


Figure 1.8.4 Regedit

6. Now navigate to HKEY_local_machine –> Software –> Microsoft –> Windows –> Current version –> Run.

Figure 1.8.5 Modify Regedit

7. Now delete the entry named MS32DLL (use delete key to delete it)
8. Now navigate to HKEY_current_user –> software –> microsoft –> Internet Explorer –> Main
9. Delete the entry named ″Hacked by godzilla″ (use delete key to delete it)
10. Close everything and head over to start menu and click on run . Type gpedit.msc and press enter.

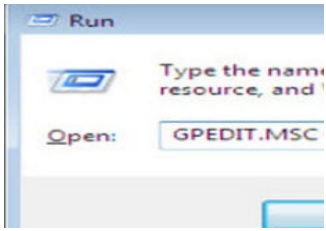


Figure 1.8.6 GPEDIT.MSC

11. Select User Configuration –> Administrative Templates –> System.
12. Double click on entry named Turn off autoplay and turn autoplay off.
13. Select Enable. Select All drives. Click ok.

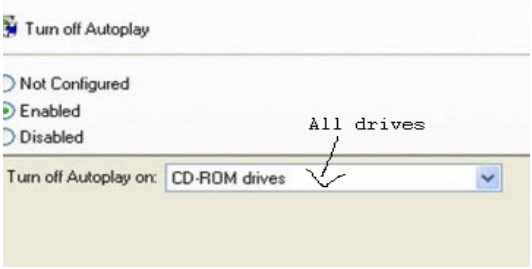


Figure 1.8.7 Selecting Drives

14. Restart and run post removal steps with ccleaner. You might need to clean recycle bin.

1.8.2 Removing Copy of Shortcut

The second most common type of virus is "copy of shortcut " which infects pendrive and keeps on infecting other computers that are connected with the infected computer. So its time to remove it.

Step 1. Download and Extract "Autorun–exterminator" – Download – http://goo.gl/WbsKhe
This will remove the autorun.inf files from USB drives . Now plug your USB Flash drives and click remove .
Step 2. Now its time to remove copy of shortcuts . Click on Start – Run – type cmd and click ok.
Step 3. Type the command given below and press enter.
Step 4. attrib –h –r –s /s /d g:*.* (here g is the Flash Drive.

You need change it with drive letter) .
Step 5. Use Malwarebytes to remove other malwares and dont forget to delete copy shortcut form your Flash Drives.

We are done with removing copy of shortcut. You can use same tools and technique to remove Recycler and System Volume Information Virus.

1.9 Dealing with Malwares

1.9.1 TornTV : TornTV is a adware application which will show you ads everywhere and it will also install unwanted programs or even malicious infected files. This adware can be downloaded from video streaming websites or even official website www.torntv.com .

1.9.2 Search App Askv2 : Search app askv2 is a famous adware which will change all your browser settings such as home page and search engine provider. It is very likely that you installed the application accidently.

1.9.3 Go.wvydeo.com : go.wvydeo.com is a advertising website which mostly have fake ads. If you get redirect to this page then you are infected by go.wvydeo.com adware. It might replace your homepage as well as your search engine.

1.9.4 Cyber Monday Deals : This is another adware to promote third parties . This adware shows ads which are usually quite bothersome and the users complain that they seriously impede their browsing.

1.9.5 GuardedWeb : This application will install potentially unwanted progras and it affects google chrome, mozilla firefox and IE. It claims to be for safer web browsing but its not a internetsecurity application or something like that.

1.9.6 Lampy Lighty : Adware created by superweb LLC. It is supposed to be very useful for shopping but you dont

need it because it will change all your major browser settings. It promotes third party products that will offer you good deals.

1.9.7 Deja Data : Another adware created by superweb LLC. It is classified as an ad–supported program because it displays commercial data in your web browser.

Other similar adwares are vebergreat Ads , Caramava Deals , Gate Snapper , SwizzleBiz ads as well as Browser good ads . So you know most adware programs its time to remove them.

1.9.8 How to remove adwares from Windows 8:

1. Tap the Windows key to access the Metro UI start screen.
2. Right-click on the background.
3. Select All apps.
4. Open Control Panel.
5. Click Uninstall a program.
6. Right-click the application you want to remove.
7. Select Uninstall.

1.9.9 How to remove adwares from Windows Vista/Windows 7:

1. Open the Start menu.
2. Click Control Panel.
3. Click Uninstall a program.
4. Right-click the unwanted application.
5. Select Uninstall to delete it.

1.9.10 How to remove adwares from Windows XP:

1. Click the Start menu icon.
2. Select Control Panel.
3. Double–click Add or Remove Programs.

4. Click the unwanted application.
5. Select Remove.

1.9.11 Removing adwares from Internet Explorer

- Click the Gear icon and pick Internet Options
- Move to the Advanced tab and click Reset
- Tick Delete personal settings and click Reset

1.9.12 Removing adwares from Mozilla Firefox

- Press Alt+H to open Help
- Click on Troubleshooting Information
- Click on the Reset Firefox button
- Confirm your action and then click Finish

1.9.13 Removing adwares from Google Chrome

- Click on the menu and choose Settings
- Select Show advanced settings
- Click on Reset Settings and then Reset

So you have removed unwanted programs . Its time for a last scan and to remove other adware applications may be hiddent. Here is a little tool which will do that for you.

1.9.14 Using AdwCleaner – AdwCleaner is another tool which will help you to remove adwares from your computer. It works with most adwares .

Download and open AdwCleaner –
Adwcleaner.exe – http://goo.gl/VgfrWn
Homepage – http://goo.gl/VsWxQ6

Now click on delete button and restart your computer again into safemode.

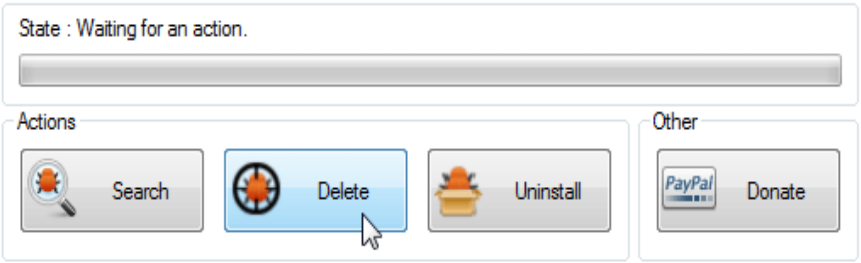


Figure 1.9.1 Adwclearner

1.10 Dealing with RootKits

Rootkit can be hard to remove but we will remove them using some simple tools .

1.10.1 Using Kaspersky TDSSKiller

Kaspersky TDSSkiller is an rootkit removal tool which is easy to use and free . It takes less than a minute to complete and remove rootkits. This tool is designed by a well known anti–virus company. They have also designed rescue discs and other tools.

Download and open TDSSkiller – TDSSkiller.exe1– http://goo.gl/qZcWE6

TDSSkiller.exe2 – http://goo.gl/bOMvM0
Homepage – http://goo.gl/jedaqW
After opening , click on Start scan . Once the scan is finished you need to click on continue . After it has complete removing rootkits just restart your computer .

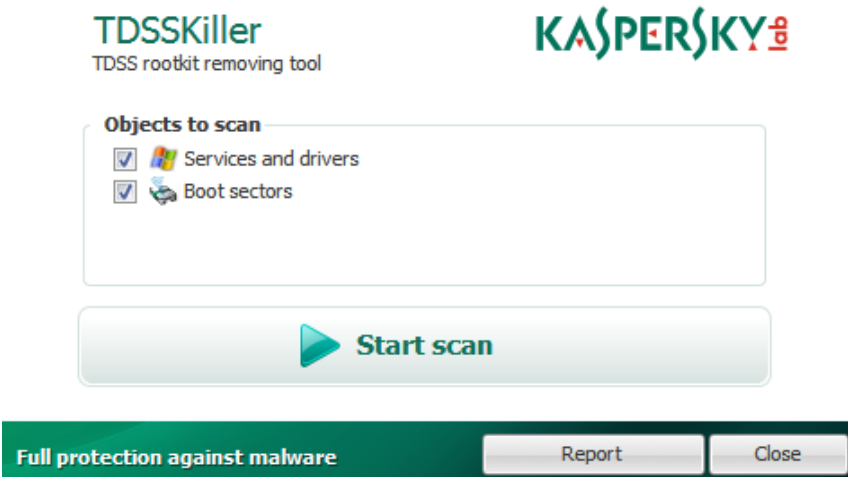


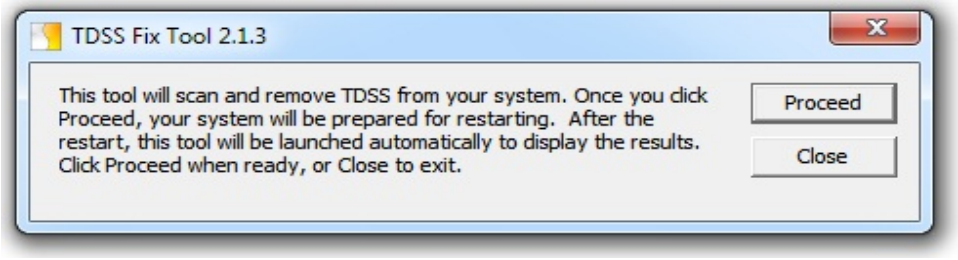
Figure 1.10.1 TDSSKiller

Note : Some time you wont be able to download TDSSkiller or you wont be able to open it. Try to run it as admin and still if you cant open it then make sure you have stopped malware processes .

1.10.2 Using Symantec FixTDSS

Symantec FixTDSS is another TDSS fixer or rootkit removal tool. You can use both applications one by one. Make sure you run both as admin .

Figure 1.10.2 Symantec FixTDSS



Download Symantec –
Symantec.exe – http://goo.gl/MUbA3l
Homepage – http://goo.gl/ux9Hfx

1.10.3 Windows Defender Offline – If you are still infected then you can use windows defender offline . Its a standalone tool made by microsoft which has latest antimalware software . You just need to download and run it on your computer .

Download and open Windows Defender Offline –
Windowsdefender.exe – http://goo.gl/VpTzVg
Homepage – http://goo.gl/RbKr9i

Create a DVD or USB flash drive . Boot from the USB or DVD and remove any malware that is found on your computer. You can find more information on microsoft website – HERE – http://goo.gl/RbKr9i

With growing Internet accessibility a new trend of malicious software has rapidly evolving. So called Web–based malware typically consists of multiple components and combines elements written mostly in script language also known as exploit kit or exploit packs.

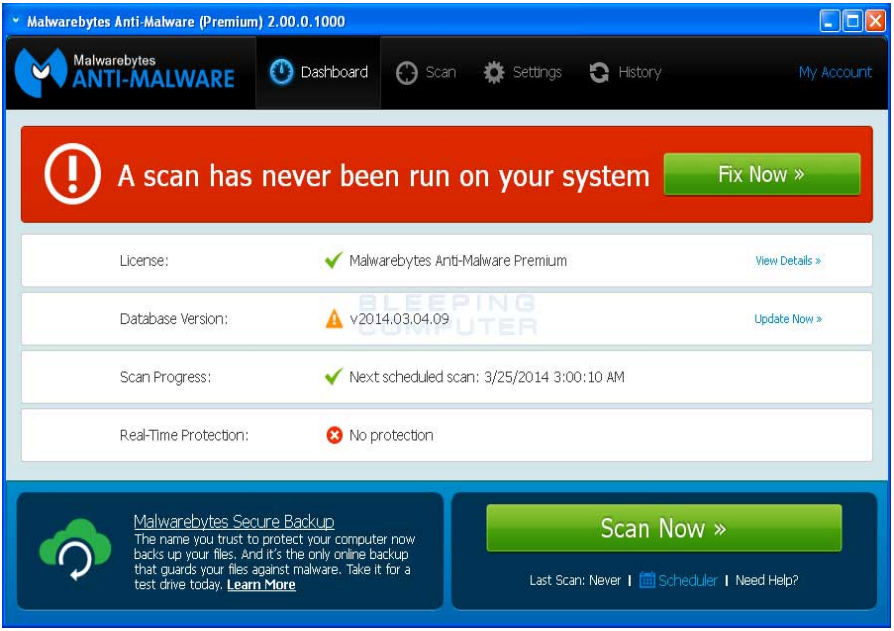
1.10.4 Using Malwarebytes – AntiMalware

Malwarebytes – As the name suggests , it is a tool which will find and remove various known malware or malicious programs.

Download and install Malwarebytes Anti–Malware
Anti–malware.exe1 – http://goo.gl/vtyk30
Anti–malware.exe2 – http://goo.gl/2c8VZg
Homepage – http://goo.gl/nQ2DKp

Unselect free trail option and click on finish. Perform a scan and click on remove selected to remove the malware from your computer . This application needs internet you can also try offline database installer (which you can find here http://goo.gl/PFvFZy) if you do not have internet. You can fix other problems using the same application.

Figure 1.10.3 Malwarebytes – AntiMalware



1.11 Web-based Malware Threat

Google itself claimed that 10% of its indexed pages contain malware , did the public become widely of this threat ? The answer is no . In 2008 , a follow up research report by the author of HITB magazine demonstrated that as of February 2008 , Google has indexed over 3 million URLs that initiate drive–by–downloads , and over 1.3% of queries submited to google returned malicious URLs in the search result . This means that even google is not safe .

1.11.1 Internet Affecting Viruses :

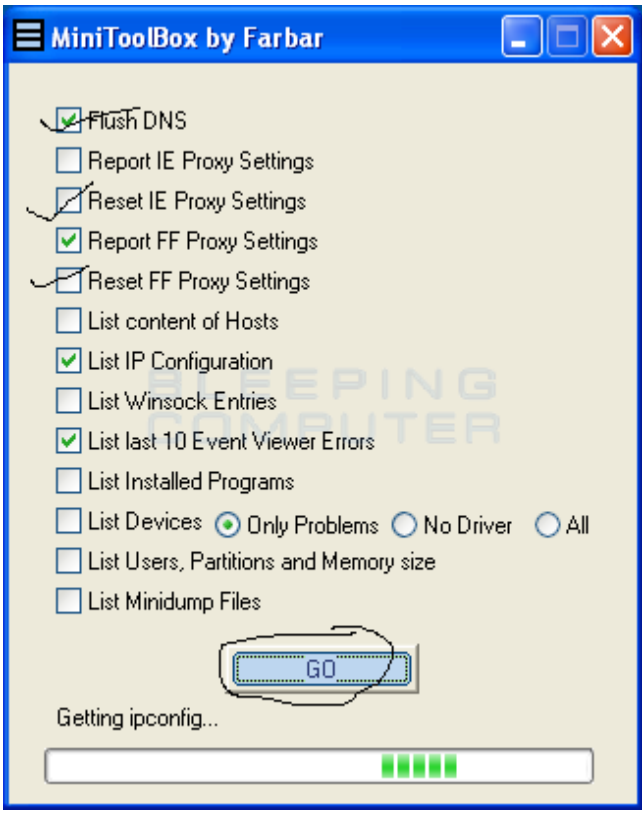
Some viruses will disconnect your computer or turn on proxy server and hijack windows DNS cache , and this will lead to data loss or slow internet and also can disconnect internet. So here is a tool called MiniToolBox which will help you to reset your internet proxy settings and cookies .

1.11.2 Using MiniToolBox

Download and open MiniToolBox –
Minitoolbox.exe – http://goo.gl/RzgS42
Homepage – http://goo.gl/5BGmXF

Now select the following checklists : Flush DNS , Reset IE proxy settings , Reset FF Proxy settings (firefox settings) and now click on go. Close everything and you are done.

Figure 1.11.1 MiniToolBox



1.12 Browser Hijackers and Malicious toolbars

1.12.1 Browser Hijackers
Hopefully browser hijackers are not that rare. They promote third party deals.

1.12.2 7searches.org – It is categorized as browser hijacker because it will actually hijack browser search engine providers as well as home page without permissions. It promotes third party deals to earn money.

1.12.3 Qozmo.net – Another browser hijacker which will change settings without permission or even a notice. It is compatible with IE , Google Chrome as well as Mozilla Firefox.

Some other browser hijacker tools are veqzz.updateinstall.toesbait.xyz , Websearch.searchoholic.info , Websearch.searchrocket.info as well as isearch.omiga–plus.com. Veqzz.updateinstall.toesbait.xyz is a browser hijacker which will tell you to update some plugins such as adobe flash . This is a fake popup .

1.12.4 Toolbar Removal
Toolbars are always malicious .

1.12.5 Nvstech – Nvstech Toolbar is a browser extension that is available on all popular web browsers . This application is promoted as a tool that will help you to search but it actually promote internet scam and ads.

Some other fake adware related toolbars are

AplusGamerToolbar , DailyImageBoard Toolbar , Tube Dimmer , Widgi Toolbar , ButterflyField , Torntv toolbar , Plus–HD toolbar as well as wizline Toolbar.

So you knwn about browser hijackers as well as fake toolbars. Its time to remove them .

1.12.6 How to remove Browser Hijackers and toolbars from Windows 8:

1. Tap the Windows key to access the Metro UI start screen.
2. Right-click on the background.
3. Select All apps.
4. Open Control Panel.
5. Click Uninstall a program.
6. Right-click the application you want to remove.
7. Select Uninstall.

1.12.7 How to remove Browser Hijackers and toolbars from Windows XP:

1. Click the Start menu icon.
2. Select Control Panel.
3. Double–click Add or Remove Programs.
4. Click the unwanted application.
5. Select Remove.

1.12.8 How to remove browser hijackers and toolbars from Internet Explorer

- Click the Gear icon and pick Internet Options
- Move to the Advanced tab and click Reset
- Tick Delete personal settings and click Reset

1.12.9 How to remove browser hijackers and toolbars from Mozilla Firefox

- Press Alt+H to open Help
- Click on Troubleshooting Information
- Click on the Reset Firefox button
- Confirm your action and then click Finish

1.12.10 How to remove browser hijackers and toolbars from Google Chrome

- Click on the menu and choose Settings
- Select Show advanced settings
- Click on Reset Settings and then Reset

Note : To remove toolbars you might need to remove them from the browser adons page and then again reset your browser.+

1.13 Security News Malwares Threat

1.13.1 Facebook Virus "WTF – Youtube" – Facebook virus is a fake virus this type of news are used to catche attention and when you click on it. You might find that something is being downloaded or even browser restarting or adons . This might result in installation of malicious softwares , adwares and even viruses while in some cases your pc might get compromised or might

crash.

1.13.2 Top Cybercrime countries – Another eye catching news which can be fake (sometimes its a real news but most times its a malware news) which will promote some adwares or malicious applications.

1.13.3 Shellshock – It is a kind of bug which will close all open applications and will make your system go crazy or unstable. You might also lose your data and files. Shellshock is in security news malware list because it is been published and promoted via security news.

1.13.4 Conclusion – Do not believe or click on any fake security news or even some eye catching news which is shared on social media via post or via message. You can browse or view trusted contents or content shared via official pages such as google news or thehackernews.com

1.14 Manual Disinfection

So its time for a manual disinfection . Here is a little trick which will help you to manually remove any rootkit or malware program running on your computer . Instructions are very simple . Just follow them.

1.14.1 Enable Boot Log

1. Click on the "Start" menu and select "Run" Type "msconfig" and press ok.

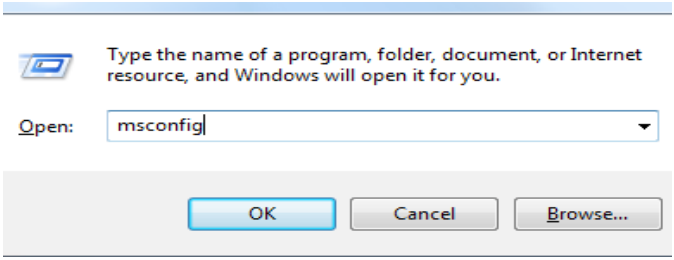


Figure 1.14.1 Msconfig

2. Click on the "Boot" tab and check the box next to Bootlog . Click on apply and restart your computer.

1.14.2 Locate Infected Files

Now we are going to search for infected files.

1. Click on the Start menu and Search files and folders (in windows 7 and above you can directly go to my computer and search for file name given below)
2. Search for file name which start from the following names : Once you find files that start with this name you need to note down the name and where the file is located .
    - rot
    - Gas
    - Gaopdx
    - seneka
    - win32k.sys
    - uacd
    - tdss
    - kungsf
    - gxvxc
    - ovsfth

1.14.3 How to disable File Permissions

1. Click on the Start menu and click on run. Type "cmd" and press ok. Command Prompt windows will be opened
2. Now type the following command
3. cacls c:\WINDOWS\system32\drivers\(filename) /d everyone

Note : Here filename stands for which file you had found in the step above for example if you find a file with rot then the command will be ″cacls c:\WINDOWS\system32\drivers\rot /d everyone ″

4. You are half done now restart computer .

1.14.4 Deleting Infected Files

1. Click on start and search the files again which you found in step 2. This time you need to delete the files by right clicking on it. You can also press Shift+delete to permanently delete the file.

1.15 Microsoft Utilities

Most of us dont use any inbuild application pre installed in microsoft windows. Windows defender is one of the application preinstalled . This tool wont be installed in some outdated windows . You can install it from the link given below .After trying all methods you can still be infected by some unknow virus so you need to run malicious software removal tool designed by microsoft.

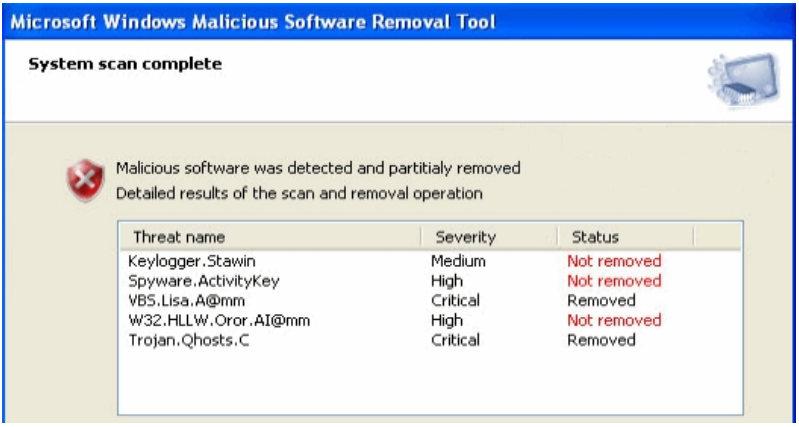
1.15.1 Mircosoft Malicious Software Removal Tool

Mircosoft Malicious Software Removal Tool is an anti–malware utility that checks computers and removes any malicious software .

Download and open Malicious Software Removal Tool –
Download – http://goo.gl/VZjihM
Homepage – http://goo.gl/pZ8FJ1

Follow onscreen instructions and with few simple clicks you are disinfected .

Figure 1.15.1 Microsoft Windows Malicious Software

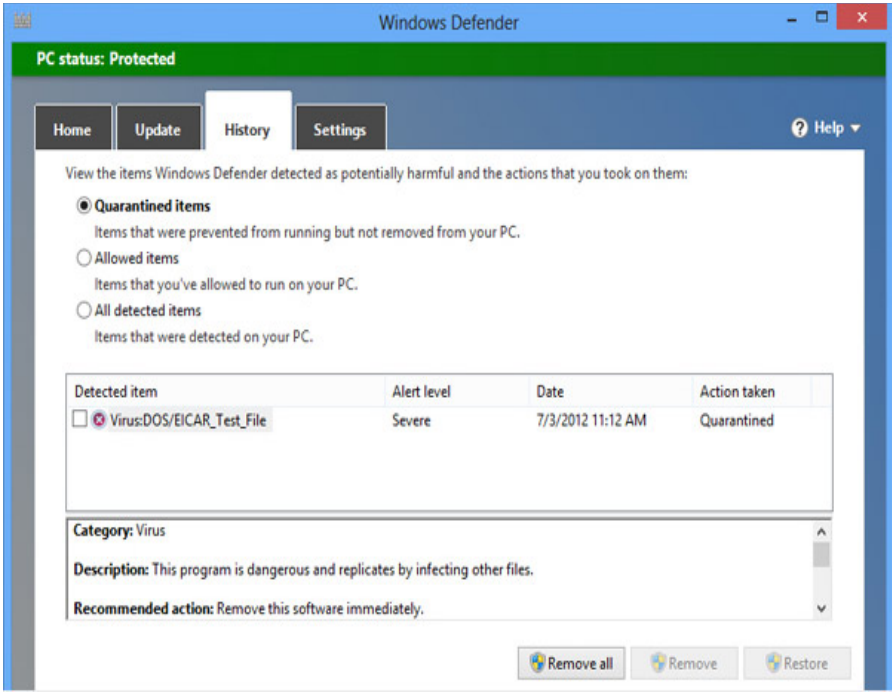


1.15.2 Microsoft Windows Defender

Download and install windows defender –
Download – http://goo.gl/vWNpKL
Homepage – http://goo.gl/64pHkZ

Windows defender is malware protection that is included with windows . This software helps identify and remov viruses , spyware and other malicious software.

Figure 1.15.2 Windows Defender

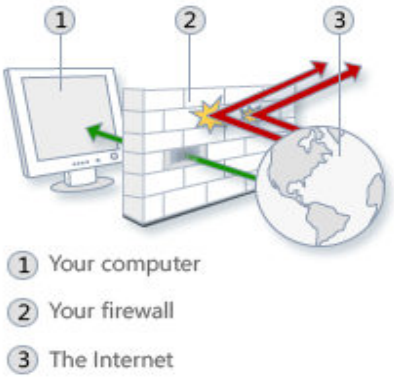


Download and install windows firewall –
Download – http://goo.gl/HaQ4z8
Homepage – http://goo.gl/qT2GIY

1.15.3 Windows Firewall

A firewall is a software program or piece of hardware that helps screen out hackers , viruses , and worms that try to reach your computer over the Internet . If you cant start windows firewall or you are getting an error then you can try free tool to diagnose and fix problems.

Figure 1.15.3 Windows Firewall



1.15.4 Windows Diagnose and fix it.

Sometimes you wont be able to open applications . So to fix this and other problems you need to use fix it mircrosoft diagnose tools.

What it fixes :

- Windows Firewall is not the default firewall
- Windows Firewall does not start
- Windows could not start windows firewall
- Other Problems.

Windows Diagnose –
Fixit.exe – http://goo.gl/CsePB0
Homepage – http://goo.gl/JkR1Ax

1.16 Using Dr. Web Live DVD

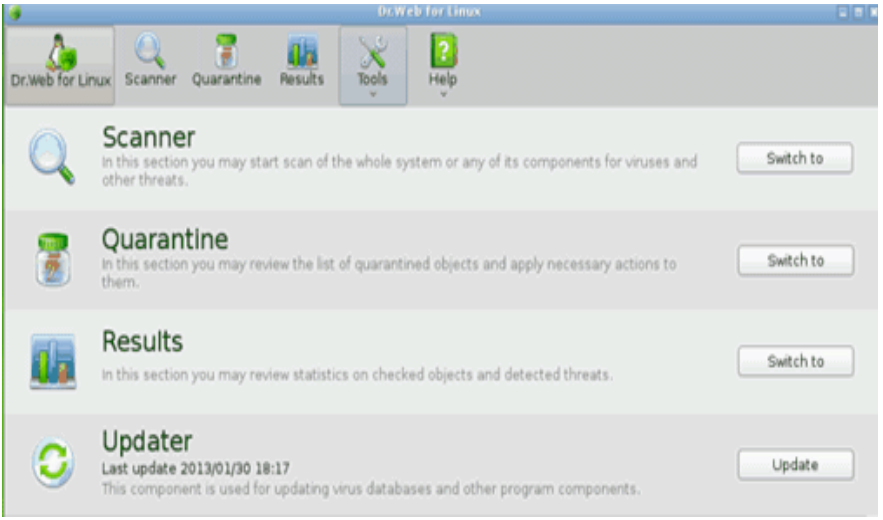
If the activities of malicious programs have made it impossible for you to boot a computer running windows , you can recover the affected system for free using Dr.

Web Livedisk. You can use DVD or USB tool . Which ever you like. USB can be usefull when you dont have dvd drive.

Download Dr. Web –
Livedisk DVD – http://goo.gl/LMX8KB
Livedisk USB – http://goo.gl/fQYjjp

1. After downloading you are ready to start by creating live DVD or USB.
2. Create a Bootable DVD or USB and boot from it.
3. Now after booting into live disk click on switch to and do a full scan.

Figure 1.16.1 Dr. Web DVD



4. You can use other options such as Quaratine files.
5. After completeting you can restart your computer.

Web Live can be useful when you cant boot your computer and you have send some mails or use the

internet . Then weblivedisk has firefox browser as well as mail client. This can be handy.

1.17 Avira utilities.

1.17.1 Avira Rescue System

Download – http://goo.gl/F1fhks
Homepage – http://goo.gl/L4Zpv0

This tool will help you to repair your infected computer . This is a handy tool which can recover files as well as remove malwares. If you still cant fix your problem then it has a free remote rescue system where you will help you to fix things.

1.17.2 Avira Command Line Scanner

Download – http://goo.gl/DVRSsR
Homepage – http://goo.gl/zpBfU6
This is a command line based scanner with no user interface .

1.17.3 Avira DNS repair Tool

Download – http://goo.gl/SfYfmk
Homepage – http://goo.gl/xckwMz
This tool will help you fix your DNS settings and damages made by internet disableing virus.

1.17.4 Avira PC– Cleaner

Download – http://goo.gl/mm3oMn
Hompage – http://goo.gl/xckwMz
This is a free malware scanner that works alongside other antivirus softwares. It will protect your computer from viruses and malwares.

1.18 Kaspersky Rescue Disk

Kaspersky rescue disk is a tool which can help you to recover your computer form malware. If your computer is not booting because of windows malfunction or other

problems. This tool will help you to create Live DVD or Live USB and fix the problems. So lets start making a bootable USB device for our infected computer.

1.18.1 Preparing USB Device

To create a USB device with Kaspersky resuce disk . You will need the following things :

- USB of more than 300 MB.

Format by right clicking on it and then select FAT16 or FAT32 file system.

Note : NTFS wont work you need FAT16 and FAT32.

1.18.2 Downloading

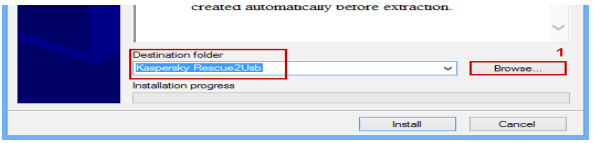
Kaspersky Rescue Disk IOS –> (~375 MB)
http://goo.gl/LL3tkx

Kaspersky Rescue Disk to USB tool –> (~379 KB)
http://goo.gl/Apsp36

1.18.3 Starting

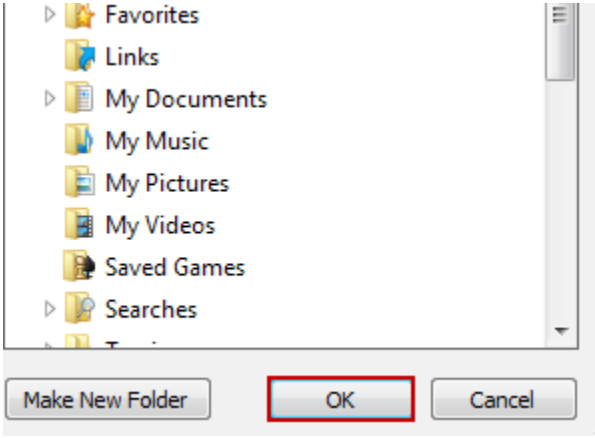
- Click Browse.

Figure 1.18.1 Installation



- Select the downloaded file and click OK.

Figure 1.18.2 Installation



- Click Install.

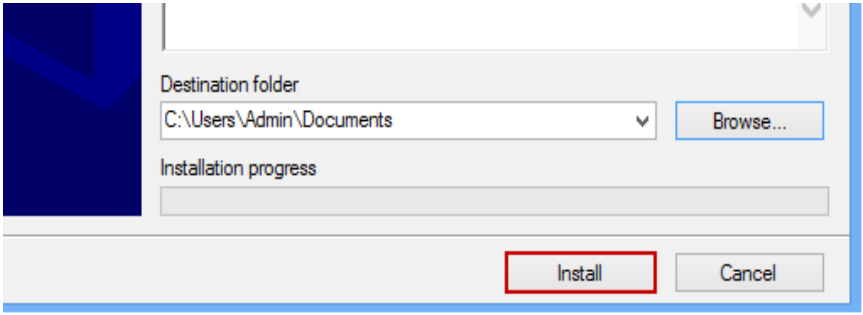
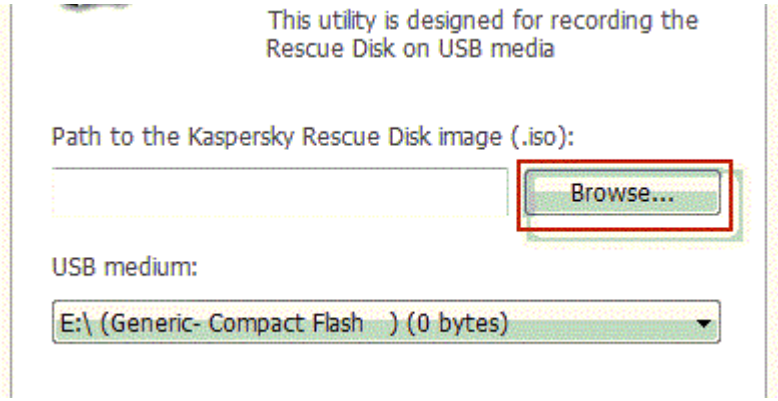


Figure 1.18.3 Installation

1. After extraction , Kaspersky USB rescue Disk Manager will open. Select the downloaded ISO image using browse button. Run the Downloaded file rescue2usb.exe

Figure 1.18.4 Kaspersky Usb rescue Disk Maker



2. Select USB device
3. Click START.
4. Wait and then click ok

s

Figure 1.18.5 Starting

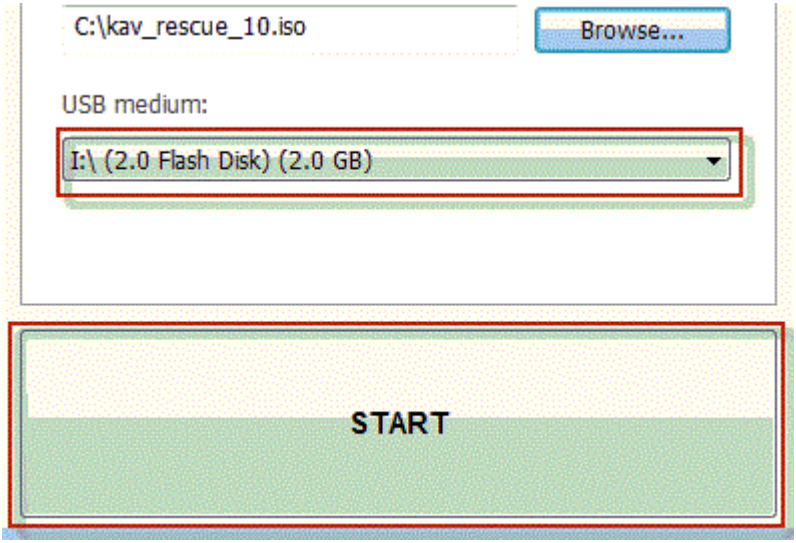
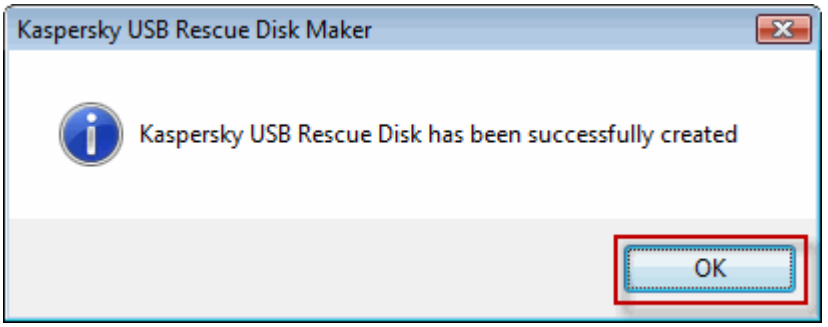


Figure 1.18.6 Done



1.18.4 Configuring BIOS

Restart your computer and plug the USB. Before computer starts keep pressing Delete or F2 keys, to load the BIOS menu. The keys F1, F8, F10, F11, F12 might be used for some motherboards, as well as the following key combinations for old computers with old motherboards.

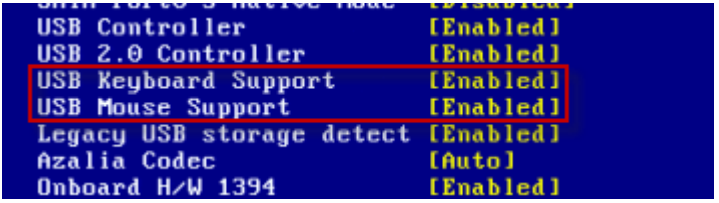
- Ctrl+Esc
- Ctrl+Ins
- Ctrl+Alt
- Ctrl+Alt+Esc
- Ctrl+Alt+Enter
- Ctrl+Alt+Del
- Ctrl+Alt+Ins
- Ctrl+Alt+S

Sometimes you can see the key to enter bios. You need to press the key. If you are late then you can restart computer again and then press the key to enter bios.

Figure 1.15.7 Selecting boot from USB

1. In BIOS enter Boot tab, select loading from a Removable Drive.
2. Make sure USB keyboard and mouse support is enabled in BIOS.

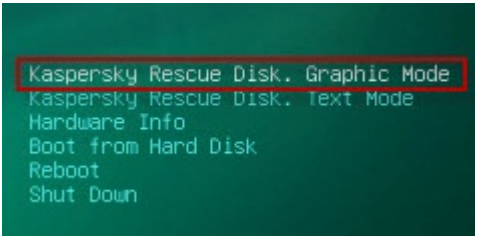
Figure 1.18.8 Live USB



You are done just restart your computer again and USB should be plugged .

1.18.5 Booting from USB

1. Restart your computer and boot from USB.
2. Press any key.
3. If you forget to press any key restart again and start again.
4. Press 1 and accept agreement.



5. Select Graphical Interface.

Figure 1.18.11 Graphical Mode

Press the ENTER key on the keyboard. Scan your computer and follow onscreen instructions. Remove USB and restart.

1.19 Finishing Disinfection

So now you have removed all adwares , viruses ,

malwares , trojan houses as well as rootkits and other malicious software. Its time to finish everything .

1.19.1 Using Ccleaner

Ccleaner – This application is used to speed your computer but it has handy tools that will help you to reset all settings and clean all registries that were created by unwanted applications which we uninstalled.

Ccleaner –
Download – http://goo.gl/cvIb5E
Hompage – http://goo.gl/5Niu1U

Download and install trial version of professional plus ccleaner.

1. Install the application and start with trail .
2. Open ccleaner and start scan and clean.
3. Now head over to the registry tab and start scanning
4. After scanning clean all registry errors and click on fix.
5. Now restart your computer and uninstall ccleaner if you dont need it.

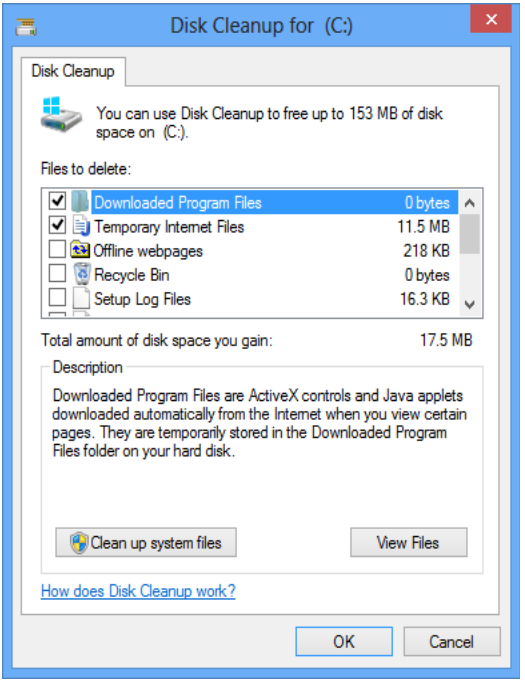
1.19.2 Defragmentation

Defragmentation – This is a tool which is build in windows. This will help you to defragment files so your computer becomes fast. As we have used many utilities and tools. We need to defragmentate files.

1.19.3 Disk Cleanup

Disk Cleanup – Other tool which is build in windows. This will help you to clean temp files in windows. Just open the tool , select drive , select all options and click on ok.

Figure 1.19.1 Disk Cleanup



1.20 Analyzing Anti-virus

We are going to analyze which is the best antivirus ever with various ratings system and tests .

1.20.1 Tested Anti–virus

The following products were tested in Dec 2014 . This are some most popular antivirus companies in India . During the test , the product were fully updated with up–to–date database and with settings recommeded by the antivirus companies . We do not abuse or advertise any of this product . This is just a educational test .

- Avas ! Free Antivirus
- AVG Internet Security
- eScan Internet Security
- Kaspersky Internet Security
- ESET Smart Security
- Indian NPAV

1.20.2 Malware Removal Analysis

This analysis only focuses on the malware removal . The test result is aimed not only on detection but also on removal of malware from the infected computer. All anti–viruses were purchased during the test and no crack was used . Windows 7 – ultimate was used during the test with a clean install. We infected computer and then made sure that it works well . Then we used some common antivirus and tried to remove the malware . If the malware was removed then we infected the computer again for the second antivirus . Even if most antivirus removed the malwares , they were rated on speed of scanning and removal .

1.20.3 Malware Removal Analysis Test Result

Antivirus	Mean Score
Avast ! Free Antivirus	B
AVG	A
Escan Internet Security	C

Kaspersky Internet Security	B
ESET Smart Security	B
Indian NPAV	A

Final Result : As you can see , AVG and Indian NPAV won the test with A.

1.20.4 Virus Removal Analysis

This analysis only focuses on the virus removal. The test result is aimed not only on detection but also on removal of virus from the infected computer . All antiviruses were purchased during the test and no crack was used. Windows 7 – Ultimate was used during the test with a clean install. Most popular anti–virus in india were selected for this test.

1.20.5 Virus Removal Analysis Test Result :

Antivirus	Mean Score
Avast ! Free Antivirus	A
AVG	A
Escan Internet Security	B
Kaspersky Internet Security	A
ESET Smart Security	B
Indian NPAV	A

Result : As the test result shows most anti–viruses are programed to detect and remove viruses so all worked well in the test .

1.20.6 Antivirus Features and Utilities

Anti–	Firew	Adwa	Malw	Rescu	Intern	Rootki	Price

virus progr ams	all Prote ction	re Remo val	are Remo val	e Disc	et Securi ty	t Remo val	
Avast	No	Yes	No	Yes	No	Yes	1799
AVG	No	No	Yes	Yes	Yes	Yes	799
NPAV	Yes	Yes	Yes	No	Yes	Yes	1400
Kaspe rsky	Yes	No	No	Yes	Yes	Yes	599

Prices – Prices of the antivirus are subject to change without any notice . This priceses are of subscription for 1 year for single user . In case of NPAV we tested Ultra Edition.

1.20.7 Final Results :

Final Resulats : You can buy any antivirus you want . If you are focused on Price then Kaspersky is the best where as if you are focused on security then NPAV is recommended . If you want low price and good security then AVG is the best for you.

Note : We do not offend or abuse any antivirus but as a security expert we are conducting this test . We are not paid to select any particular antivirus. We recommend to research more before buying any antivirus .

Tip : Do not download anything from torrent as most malicious software are spread via torrents or peer to peer connections such as DC++ . If you download any application or file , first scan it on free scanning website – HERE – http://goo.gl/JdQkJL. It will scan your file or website URL and analyze suspicious files and URLs.