

Forum:[Hack Forums](#)

Thread: [\[AV, AM, AS\] Security Tools Ultimate Compilation \[with Rating\] \[Mega Thread\]](#)

Antigen - July 14, 2013, 6:53 am

Introduction

Anti-virusESET NOD

Kaspersky

Bitdefender

Avira

F-Secure

Avast

AVG

Norton

G-Data

McAfee

Symantec Norton

Anti-Malware and Anti-SpywareMalwarebytes' Anti-Malware

Spybot Search and Destroy

SUPERAntiSpyware

ComboFix

Virus/Malware Diagnosing Log EnumeratorsHijackThis

OTL

Portable/Standalone ToolsAnti-rootkit utility TDSSKiller

Welcome to my Security Tools Ultimate Compilations thread. In this thread we will be covering almost all Anti-virus, Anti-malware, Anti-spyware, Firewall. All the information, rating, price, statistics are referenced from reputed Antivirus testing lab's reports like av-comparatives.org. Prices of products and versions names are grabbed from respective official sites, there might have slight variations in the price. This thread will hopefully be an informative resource to the members, the motivation for this thread is the tons of questions posted here about best antivirus and other security tools. I'll keep update this thread and add as many as information I can. If you have any questions regarding anything listed in here, or need additional help, post here or PM me.

Antivirus or anti-virus software (usually written with the acronym of AV) is software used to prevent, detect and remove malware (of all descriptions), such as: computer viruses, malicious BHOs, hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware. Computer security, including protection from social engineering techniques, is commonly offered in products and services of antivirus software companies.(wiki)

[\[img\]http://chart.av-comparatives.org/scripts/css/images/logo/eset.jpg?0](http://chart.av-comparatives.org/scripts/css/images/logo/eset.jpg?0)[\[img\]](#)

ESET NOD32 Antivirus, commonly known as NOD32, is an antivirus software package made by the Slovak company ESET. ESET NOD32 Antivirus 6 is an award-winning antivirus with fast and powerful detection of malware. Recipient of the 2012 PCMag.com award for the "Most Consumer Recommended" product in the security category, ESET NOD32 Antivirus 6 features an all-new Anti-Phishing module that protects you from fake websites trying to acquire your personal information. The new Social Media Scanner extends your security to Facebook by checking your wall, news feed and private messages for malicious content.

Editions [ESET NOD 32 Antivirus 6](#) (\$20/Year)

[ESET Smart Security 6](#) (\$27/Year)

[ESET Endpoint Security \(Server\)](#)

Supported Platforms Windows XP/7/8

Mac

Linux

Android, Windows, Symbian

ESET NOD 32 Smart Antivirus 6 BenchmarksVirus/Malware Detection : Advanced +

Performance : Advanced +

Detection Rate : 97.5%

New FeaturesAnti-Theft: Locate and Retrieve Your Missing Laptop

Parental Control

Gamer Mode

Host-based Intrusion Prevention System (HIPS)

Screencaps ([Click to View](#))

[img]http://www.tsiakkas.com/modules/modProducts/uploadFiles/photos/1368777075-allindir.10f6abafa.jpg[/img]

[img]http://img.creativemark.co.uk/uploads/images/101/15101/img3File.png[/img]

Rating

[img]http://chart.av-comparatives.org/awards/logo_perf_adv+_may2013.png[/img]

Antigen - July 14, 2013, 6:54 am

[\[img\]http://chart.av-comparatives.org/scripts/css/images/logo/kaspersky.jpg?0\[/img\]](http://chart.av-comparatives.org/scripts/css/images/logo/kaspersky.jpg?0)

Kaspersky Anti-virus is one of the most powerful antivirus solutions currently on the market, providing an excellent detection rate, combined with real-time protection and definition updates delivered to every computer on a regular basis. The interface is pleasant and makes you believe you're using an application that's only focused on basic functions, although the powerhouse hidden under the hood is worth every single penny. Kaspersky Anti-Virus is capable not only to discover and remove threats on your computer, but also to protect your email client, instant messengers and web traffic, regardless of the browser you use.

Editions[Kaspersky Anti-Virus 2013](#) (\$39.95)

[Kaspersky Internet Security 2013](#) (\$59.95)

[Kaspersky PURE 3.0](#) (\$99.95)

[Kaspersky Small Office Security \(Network\)](#)

Supported Platforms Windows XP/7/8

Mac

Android

Kaspersky Anti-Virus 2013 Benchmarks Virus/Malware Detection : Advanced +

Performance : Advanced +

Detection Rate : 99.2%

New Features Safe Money – adds more protection for financial transactions

Secure Keyboard & improved Virtual Keyboard – help protect your identity

Automatic Exploit Prevention – defends against the exploitation of vulnerabilities

Secure vaults – protect your most precious data

Online backup – makes data backup even more convenient

Screencaps [\(Click to View\)](#)

[img]http://maxuninstaller.com/howtouninstallguides/wp-content/uploads/2012/08/Kaspersky_Internet_Security2013.png[/img]

Rating

[img]http://chart.av-comparatives.org/awards/logo_perf_adv+_may2013.png[/img]

[img]<http://chart.av-comparatives.org/scripts/css/images/logo/bitdefender.jpg>[/img]

Bitdefender has stepped up its game with the latest Antivirus Plus release, bringing forth new technologies and powerful features for ensuring the security of your system from viruses and other e-threats. After installation, the utility offers two configuration modes: Autopilot mode runs with default settings and doesn't interrupt user activity, while Automatic Game mode caters to users who wish to play video games and not worry about any interference. Bitdefender Antivirus Plus boasts a modern and clean interface, where you have a few scanning modes at your disposal: the Quick mode goes through key areas of your hard drive, while the System mode thoroughly looks for just about any suspicious activity.

Editions [Bitdefender Antivirus Plus 2013](#) (\$20)

[Bitdefender Internet Security 2013](#) (\$34)

[Bitdefender Total Security](#) (\$42)

[Endpoint Security \(Network\)](#)

Supported PlatformsWindows XP/7/8

Mac

Android, iOS

Bitdefender Anti-Virus 2013 BenchmarksVirus/Malware Detection : Advanced +

Performance : Advanced +

Detection Rate : 99.3%

New FeaturesRescue Mode -

Bitdefender Autopilot™

Enhanced! Bitdefender Safepay™

Two-way Firewall

Remote Management

Screencaps ([Click to View](#))

[img]http://www.bitdefender.com/themes/red/images/homepage_banner_boxes_image2.png[/img]

[img]http://www.ghacks.net/wp-content/uploads/2012/07/bitdefender-total-security-2013.jpg[/img]

Rating

[img]http://chart.av-comparatives.org/awards/logo_perf_adv+_may2013.png[/img]

Antigen - July 14, 2013, 6:58 am

[img]http://chart.av-comparatives.org/scripts/css/images/logo/avira.jpg[/img]

Avira AntiVir seems to be the right choice for all those who are searching for a solution with decent performance and regular updates, just to be sure infections stay away from their precious data. The

developers over at Avira have always offered a well-organized interface, and their latest antivirus solution makes no exception to this rule. Fortunately, although it's supposed to fight against viruses, the application comes with a handy user interface that lets you configure it with ease. Avira only offers a bunch of settings, so advanced users should have no problem to deal with them, although beginners should too find the whole application quite easy to use.

Editions [Avira Antivirus Free 2013](#) (Free !)

[Avira Premium 2013](#) (\$18)

[Avira Internet Security](#) (\$30)

[Avira Internet Security Plus](#) (\$42)

[Endpoint Security](#)

Supported Platforms Windows XP/7/8

Mac

Android

Avira Anti-Virus 2013 Benchmarks Virus/Malware Detection : Advanced +

Performance : Advanced

Detection Rate : 99.6%

New Features Browser Tracking Blocker

Protection Cloud

Disk Wiper

Enhanced Child Protection

File Encryption

File Shredder

Screenshots [\(Click to View\)](#)

[img]http://4.bp.blogspot.com/-QmTW5YnCIUQ/ULGtvvddJ-I/AAClc/kdQis0ceAEM/s400/2012-11-25_013518.png[/img]

Rating

[img]http://chart.av-comparatives.org/awards/logo_perf_adv+_may2013.png[/img]

[img]http://chart.av-comparatives.org/scripts/css/images/logo/f-secure.jpg?0[/img]

F-Secure Antivirus is a security system that assists you in removing viruses, spyware and other infections from your computer. After a long installation process, the software performs an automatic update, which takes a long time as well. Once you have initiated F-Secure Antivirus, you are acquainted with a user-friendly interface. There aren't many features available in the antivirus system, so beginners should not have a difficult time understanding how it works. In the main window you can access the current status of the virus and spyware scanning, of the scheduled tasks and DeepGuard, but you can also view general statistics.

Editions [F-Secure Antivirus 2013](#) (\$39.99/3 Users)

[F-Secure Internet Security 2013](#) (\$59.99 /3 Users)

Supported Platforms Windows XP/7/8

Mac

Android, iOS

F-Secure Anti-Virus 2013 Benchmarks Virus/Malware Detection : Advanced +

Performance : Advanced +

Detection Rate : 99.5%

New Features Advanced real-time cloud-based technology

Advanced firewall protection

Personalized settings for each user

Screencaps ([Click to View](#))

[img]http://i1-news.softpedia-static.com/images/news-700/F-Secure-Improves-Internet-Security-2013-with-Banking-Protection.png?1352816730[/img]

[img]http://asset1.cbsistatic.com/cnwk.1d/i/tim/2012/09/13/F-Secure_Internet_Security_2013_610x448.png[/img]

Rating

[img]http://chart.av-comparatives.org/awards/logo_perf_adv+_may2013.png[/img]

[img]http://chart.av-comparatives.org/scripts/css/images/logo/avast!.jpg?0[/img]

Avast! Free Antivirus is a reliable antivirus software solution designed to provide computer users with effective protection against viruses and spyware. Avast comes with well-organized interface that targets beginners and professional users alike, with all features being clearly displayed right in the main window. Be careful during the installation though, because the setup kit also attempts to drop a separate browser on your computer, although Avast doesn't need this kind of app to work properly. However, once installed, Avast works simply great, with virus definitions updated even several times a day. The scanning process is very fast and is quite light on hardware resources, but it all depends on the computer and the files you're about to scan. We were pleased with its speed during our tests, even though sometimes we were a bit annoyed by the boot-time scanner.

Editions [Avast! Free Antivirus 2013](#) (Free)

[Avast! Pro Antivirus 2013](#) (\$39.99)

[Avast! Internet Security](#) (\$49.99)

[Avast! Premier](#) (\$69.99)

[Avast! File Server Security](#)

Supported Platforms Windows XP/7/8

Mac

Android, iOS

Avast! Anti-Virus 2013 Benchmarks Virus/Malware Detection : Advanced

Performance : Advanced +

Detection Rate : 97.8%

New Features Remote Assistance

SafeZone™

AccessAnywhere

Firewall

Screenscaps [\(Click to View\)](#)

[img]http://1.bp.blogspot.com/-9uOn4nRqfos/ULyjscezNpI/AAQU/90nfqYM0Rvo/s320/Avast+7.FunLoadz.Com_P.jpg[/img]

[img]http://4.bp.blogspot.com/-X6KJrpfMH8g/UOEytbx2gAI/AA_M/cZe10y24pVI/s320/Download+Avast!+Internet+Security+7.0.1474+++License+Valid+2050.png[/img]

Rating

[img]http://chart.av-comparatives.org/awards/logo_perf_adv_may2013.png[/img]

Antigen - July 14, 2013, 6:59 am

[img]http://chart.av-comparatives.org/scripts/css/images/logo/avg.jpg?0[/img]

AVG Free Edition is one of the freeware antivirus software that should be taken into consideration when thinking about a freeware solution to protect one's PC. It only provides basic protection, but this should be enough for those who are not avid computer users who download tons of files from the Internet. Extra attention should be paid when installing this application, since it offers to make some changes to your search engine and install a browser toolbar. Even if you refuse these offers, the software still functions properly. The interface of AVG Free Edition pleasant, and packed with features that users would only expect from paid solutions, including modules such as LinkScanner, E-mail Protection or Anti-Rootkit.

Editions [AVG Free Antivirus 2013](#) (Free)

[AVG Pro Antivirus 2013](#) (\$39.99)

[AVG Internet Security](#) (\$54.99)

[AVG Premium Security](#) (\$69.99)

Supported Platforms Windows XP/7/8

Mac

Android, iOS, Windows Mobile

Avast! Anti-Virus 2013 Benchmarks Virus/Malware Detection : Advanced

Performance : Advanced

Detection Rate : 98.4%

New Features AVG Do Not Track

AVG WiFi Guard

AVG Identity Protection™

AVG Enhanced Firewall

AVG Turbo Scan

Screencaps [\(Click to View\)](#)

[img]http://zapt1.staticworld.net/images/article/2013/01/avg-2013-main-windows-100023043-large.jpg[/img]

[img]http://www.avlabsoftware.com/antivirus_software/screens_avg_free/avg_2013_free.png[/img]

Rating

[img]http://wp.av-comparatives.org/wp-content/uploads/adv.jpg[/img]

[img]http://chart.av-comparatives.org/scripts/css/images/logo/g%20data.jpg?0[/img]

G DATA Internet Security is a suite of applications that work together in order to provide you with the best protection for your computer. The security features include an antivirus, a firewall, antispam filtering and child protection. In addition to its award-winning virus detection rates, G Data InternetSecurity has a new idle scan feature which scans the system when it is idle to utilize your system's uptime efficiently. Cloud-based analysis of suspicious files and the silent firewall give your system an effective all-round defense against viruses, worms, spam and hacking - without loss of performance and without tedious queries.

Editions [G Data AntiVirus 2013](#) (\$ 29.95)

[G Data Internet Security 2013](#) (\$34.95)

[G Data Total Security 2013](#) (\$39.95)

Supported Platforms Windows 7/8

Android

G Data Anti-Virus™ 2013 Benchmarks Virus/Malware Detection : Advanced (Due to high number of False positives can't have Advance + even though it've highest detection rate.)

Performance : Standard

Detection Rate : 99.9%

New Features Device control controls use of USB devices or DVDs

New BankGuard technology for secure banking and online shopping

Integrated backup function for automatic data backup in the background

Behavior monitoring protects against unknown viruses

System tuning for a fast PC

Screenscaps ([Click to View](#))

[img]http://3.bp.blogspot.com/-9ihBP7SZ0ZY/UFVmw2nbDpl/AABPs/O_1uS7HoAsk/s1600/Gdata-2013+products+logo.jpg[/img]

[img]http://cdn4.pcadvisor.co.uk/cmsdata/reviews/3374180/G_Data_Total_Protection_2013.jpg[/img]

Rating

[img]http://chart.av-comparatives.org/awards/logo_od_adv_mar2013.png[/img]

Antigen - July 14, 2013, 7:00 am

[img]http://chart.av-comparatives.org/scripts/css/images/logo/mcafee.jpg?0[/img]

McAfee initially aimed at home and home-office users, McAfee VirusScan was designed for virus detection and removal. The integrated technologies would fend-off network attacks, spyware and adware threats. However, McAfee VirusScan is not available anymore as a standalone product. Instead, you can find it integrated in McAfee Internet Security Suite and McAfee Total Protection. There is an Enterprise edition of McAfee VirusScan available for download and it also aims to keep malware off your desktop and server systems. This version is meant to be used on larger networks and has two complementary components: a server application and a client application.

Editions[McAfee AntiVirus Plus 2013](#) (\$34.99)

[McAfee Internet Security 2013](#) (\$55.99)

[McAfee Total Protection 2013](#) (\$62.99)

Supported PlatformsWindows 7/8

Mac

Android, Blackberry

McAfee Anti-Virus™ 2013 BenchmarksVirus/Malware Detection : Advanced

Performance : Standard

Detection Rate : 98.0%

New FeaturesNEW McAfee® SafeKey

Centralized Visibility into Protection

Two-way Firewall

Wireless Network Protection

ENHANCED Digital Data Shredder

Screenscaps ([Click to View](#))

[img]http://home.mcafee.com/SupportPages/ImageLoader.aspx?imgtype=boxshots&imgname=pd_maa_new_1user_med.png[/img]

[img]http://zapt5.staticworld.net/images/article/2013/01/mcafee_internet_security_2013_main-100023070-large.jpg[/img]

Rating

[img]http://chart.av-comparatives.org/awards/logo_od_adv_mar2013.png[/img]

[img]http://chart.av-comparatives.org/scripts/css/images/logo/symantec.jpg?0[/img]

Norton 360 can be considered a computer security suite that has everything required to protect your PC. This compact package includes an antivirus tool, firewall, anti-malware, a backup system and a PC tune up utility, all the necessary elements needed to protect you against any threat. The interface of Norton 360 is intuitive enough to enable not only experts, but also novices to operate it successfully. Each function is neatly organized and every button brings up additional features. For instance, one of the sections is dedicated to the actual scanning of the PC, while also enabling you to choose the drive, folder or file you want to scan, as well any Facebook link from your wall. The Identity section allows you to take all the necessary measures for protecting your online usernames, passwords or other sensitive data. So as to prevent phishing, you can even rely on Norton 360 to display full details about the current website or block malicious sites.

Editions[Norton Anti-Virus™](#) (\$39.99)

[Norton Internet Security™](#) (\$49.99)

[Norton 360™](#) (\$59.99)

[Norton 360™ Premier Edition](#) (\$66)

Supported PlatformsWindows XP/7/8

Mac

Android, iOS

Norton Anti-Virus™ 2013 BenchmarksVirus/Malware Detection : Standard

Performance : Advanced

Detection Rate : 91.2%

New FeaturesSONAR Behavioral Protection

Intelligent detection and quiet background operation

Automatic backup

exclusive clean up and tuneup feature

Network Defense Layer Protection

Screenscaps [\(Click to View\)](#)

[img]http://now.symassets.com/now/en/pu/images/Product_Family/N360/N360_2013/Boxes/BX_N360_Y13_r_r_EN_342.png[/img]

[img]http://www.o2worldnews.com/wp-content/uploads/2013/04/9.gif[/img]

Rating

[img]http://chart.av-comparatives.org/awards/logo_od_ttd_mar2013.png[/img]

Antigen - July 14, 2013, 7:00 am

Malware, short for malicious software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. Anti-Malware software is a form of antivirus that is concentrated against Malwares.(wiki)

[img]http://cdn.windows7themes.net/pics/malwarebytes-update-faster-scan.jpg[/img]

Malwarebytes' Anti-Malware is a very effective application especially designed to keep malware away from your computer. It can fight off trojans, rootkits, worms, spyware, rogues and more. The program sports a tabbed interface that provides a simple way to browse among the main features. Malwarebytes' Anti-Malware enables you to perform three types of scan, 'Quick', 'Full' and 'Flash', with the last one specifically designed to analyze memory and autorun objects. The scanning process is pretty fast, regardless if there's something wrong with your computer or not. When the

operation is complete, the application automatically generates a report in which you're informed about the files affected by malware, so that you can safely take the most appropriate action. Cleaning the threats found by Malwarebytes' Anti-Malware is again a straightforward process that takes only a few seconds and has an efficiency rate close to perfection, as we found out during our tests.

Editions [Malwarebytes Anti-Malware Free](#) (free)

[Malwarebytes Anti-Malware Pro](#) (\$26.6)

Supported Platforms Windows XP/7/8

Malware Bytes Anti-Malware™ 2013 Benchmarks

No benchmarks available from official sites. But MBAM is considered as the The best anti-malware tool for ordinary users, MBAM is highly recommended by HF's MRT members.

New Features Flash - Lightning fast scan speeds

Puts YOU first! - Priority database updates

Puts Malware in the Slammer - Quarantine function holds threats and lets you restore at your convenience

Chameleon - Gets Malwarebytes running when blocked

Nitty Gritty - Command line support for quick scanning

RPP, Yeah You Know Me - Realtime Proactive Protection Module

Toolbox - Extra utilities to help remove malware manually

Screenaps [\(Click to View\)](#)

[img]http://3.bp.blogspot.com/-VeerExwfgY/Tbr1tsjE70I/AAOts/eKQTNsUkfz8/s320/Malwarebytes_Anti-Malware_v1.46.jpg[/img]

[img]http://images.cdn.static.malwarebytes.org/site_resources/20130709-042f2b55a1/images/screenshots/1.70/Scanner.png[/img]

[img]http://download.cnet.com/i/bto/20080305/spybot_logo_270x66.bmp[/img]

SpyBot - Search & Destroy is a full featured security solution designed to keep this kind of malware away from you, while also providing a suite of tools for system repair, file shredding and managing autostart items. The interface has a clean and professional look, with all the modules in plain view. It

provides direct access to the scanning modes, namely: a full system scan that thoroughly analyzes your computer for threats and a custom file/folder scan that allows you to manually select the locations to be processed. The scanning speed is decent and a full-system scan took about twenty minutes in our case, which is acceptable, but the amount of resources it requires is impressive (the CPU usage exceeded 50% at times). A system immunization feature is also available, aimed to apply preventive measures against spyware in order to block malware from infecting your computer.

Editions [Spybot Free](#)

[Spybot Home](#) (\$13.99)

[Spybot Professional](#) (\$25.99)

Supported Platforms Windows XP/7/8

New Features Immunizes System

System (Registry) Repair

Secure Shredder

Protected Repair Environment

Boot CD Creator

Supports multi core processors

Screenscaps [\(Click to View\)](#)

[img]http://1.bp.blogspot.com/-tPsfadpEJPY/Tjxljh0P6qI/AAIU/Vk0SHcydT_Q/s200/Spybot+Search+%2526+Destroy+2.0+Beta+3.jpg[/img]

[img]http://www.2-spyware.com/images/data_images/spybot-search-and-destroy1.jpg[/img]

SUPERAntiSpyware is a one of the software solutions currently available on the market that join the effort to keep malicious files, be them Trojan horses, keyloggers, dialers, worms or hijackers off our computers. This application has the power to scan and remove the threats and even provide real time protection. Once you run the utility, you can choose between four different scan types, quick, complete, critical point and custom. Each of them detects and removes threats in the most efficient way, but it's recommended to choose the complete one to obtain the best results. It's also important to make sure you close all the other programs before starting the scan so the application can search for malicious files without having to deal with too many running processes. The scanning operation went pretty smoothly and quickly during our tests and the system resources were not at all stressed. What's more, SUPERAntiSpyware includes several repair utilities, mostly supposed to fix the issues

caused by spyware. These include tools to reset URL prefixes, reset Windows clock time display, repair broken Network Connection, remove or reset Windows desktop wallpaper and many others.

Editions [Super Anti-Spyware Free](#)

[Super Anti-Spyware Portable](#) (Free)

[Super Anti-Spyware Pro](#) (\$29.95)

Supported Platforms Windows XP/7/8

New Features Spyware, Adware and Remove Malware, Trojans, Dialers, Worms, KeyLoggers, HiJackers, Parasites, Rootkits, Rogue Security Products and many other types of threats.

Light on System Resources and designed not to slow down your computer like many other anti-spyware products. Designed not to conflict with your existing anti-spyware or anti-virus solution!

Repair broken Internet Connections, Desktops, Registry Editing and more with our unique Repair System!

First Chance Prevention examines over 50 critical points of your system each time your system starts up and shuts down to eliminate threats before they have a chance to infect and infiltrate your system.

Screenshots [\(Click to View\)](#)

[img]http://www.superantispyware.com/images/SAS50/IMGsAS50_Main_Large.jpg[/img]

Combofix is a smart spyware and malware removal application known for its speed and effectiveness. It performs in-depth scans that in addition to being short, always result in a complex cleaning process or a detailed report of the analysis. Combofix is designed for advanced users, system administrators and computer technicians; it is not to be used by beginners, because it can cause serious damage to your computer, to the point where the system can become unbootable. In other words, Combofix can return the best and furthermore, the safest results only if in the right hands. Although it performs such a complex task and should be handled with the utmost care, it isn't difficult to accommodate it on the system. In addition, it creates a backup of the registry, as well as a system restore point, in case crashes occur. Please note that during the scan / cleaning process, Combofix deletes files from three locations, namely Recycle Bin, Temporary Internet Files and the Temp Folder; a wise move would be to backup this type of data before you run the application. One of the greatest advantages of Combofix is its ability to detect combinations of common spyware and malware threats, leaving your computer clean from the first run.

Editions [ComboFix](#) 13.7.13.1 (Free)

Supported PlatformsWindows XP/7

WARNING: This program can have adverse effects and cause significant damages to machines if not used properly. It is recommended to not run this program without guidance from an experienced technician, such as the members of the MRT team on HackForums.

Tutorial ([Click to View](#))

[Video: https://www.youtube.com/watch?v=7PRWXVD_8-8]

Antigen - July 14, 2013, 7:01 am

Log Generators, is a tool that is used to diagnose a computer for a possible malware presence and to provide system diagnostics information that can be used by someone working on a computer. When run, these tools will scan your computer for a variety of information and then generate a report with a tremendous amount of information about your computer's hardware, programs, files, and running environment. In a case of infection HF MRT team often asks to generate logs with these tools.

OTL by OldTimer runs out-of-the-box as it does not require any installation and it can identify the modifications spyware or malware might have caused on the computer. Once the PC has been scanned, the application generates a detailed report of all the files and registry entries that have been affected, allowing users to determine which of the items need to be removed.

Editions[OTL by OldTimer 3.2.70.2](#) (Free)

Supported PlatformsWindows XP/Vista/7

Screenshots ([Click to View](#))

[img]<http://www.bleepstatic.com/download/screenshots/o/otl/otl.jpg>[/img]

[img]<http://www.bleepstatic.com/download/screenshots/o/otl/otl-log.jpg>[/img]

Tutorial ([Click to View](#))

[Video: <https://www.youtube.com/watch?v=2KsVWmHKCT8>]

HijackThis is a cleanup utility that detects browser hijacking issues and attempts to solve them by deleting the registry entry that holds the malware. Unlike similar software, Hijack This does not rely on a database of the latest malware out there, but instead it tracks the modifications performed in

your browser and allows you to undo it. Utmost care is required when removing the adjacent registry entries, since the adjustments are sometimes irreversible. The user interface does not sport any visual incentives, but it's straight-forward and intuitive. From the main menu you can perform a system scan and optionally to save the results to a logfile, view the list of backups, open the miscellaneous tools section or open the online HiJackThis QuickStart.

Editions [HijackThis 2.0.4](#) (Free)

Supported Platforms Windows XP/Vista/7

Screenshots [\(Click to View\)](#)

[img]http://i1-win.softpedia-static.com/screenshots/HijackThis_1.png[/img]

Tutorial [\(Click to View\)](#)

[Video: <https://www.youtube.com/watch?v=FDWD9mhgeno>]

These portable tools can help users detect and remove the threats of specific categories before it does any damage. The benefit in using portable tools is that users need to simply run the program and press a single button in order for the scanning process to launch. Otherwise, one would need to search the registry for entries affected by the rootkit and erase them manually.

Kaspersky Lab has developed the TDSSKiller utility that allows removing rootkits.

[img]<http://support.kaspersky.com/images/5350-113-187993.png>[/img]

Rootkits [\(Click to View\)](#) Backdoor.Win32.Phanta.a,b,

Backdoor.Win32.Sinowal.knf,kmy,

Backdoor.Win32.Trup.a,b,

Rootkit.Boot.Mebusta.a,

Rootkit.Boot.Backboot.c,

Rootkit.Boot.Aeon.a,

Rootkit.Boot.Backboot.a,

Rootkit.Boot.Batan.a,

Rootkit.Boot.Bootkor.a,

Rootkit.Boot.Clones.a,
Rootkit.Boot.CPD.a,b,
Rootkit.Boot.Fisp.a,
Rootkit.Boot.Geth.a,
Rootkit.Boot.Goodkit.a,
Rootkit.Boot.Harbinger.a,
Rootkit.Boot.Krogan.a,
Rootkit.Boot.Lapka.a,
Rootkit.Boot.MyBios.b,
Rootkit.Boot.Nimnul.a,
Rootkit.Boot.Pihar.a,b,c,
Rootkit.Boot.Plite.a,
Rootkit.Boot.Prothean.a,
Rootkit.Boot.Qvod.a,
Rootkit.Boot.Smitnyl.a,
Rootkit.Boot.SST.a,b,
Rootkit.Boot.SST.b,
Rootkit.Boot.Wistler.a,
Rootkit.Boot.Xpaj.a,
Rootkit.Boot.Yurn.a,
Rootkit.Win32.PMax.gen,
Rootkit.Win32.Stoned.d,
Rootkit.Win32.TDSS,
Rootkit.Win32.TDSS.mbr,
Rootkit.Win32.ZAccess.aml,c,e,f,g,h,i,j,k,
Trojan-Clicker.Win32.Wistler.a,b,c,
Trojan-Dropper.Boot.Niwa.a,

Trojan-Ransom.Boot.Mbro.d,e,

Trojan-Ransom.Boot.Mbro.f,

Trojan-Ransom.Boot.Siob.a,

Virus.Win32.Cmoser.a,

Virus.Win32.Rloader.a,

Virus.Win32.TDSS.a,b,c,d,e,

Virus.Win32.Volus.a,

Virus.Win32.ZAccess.k,

Virus.Win32.Zhaba.a,b,c.

Download TDSSKiller [Windows 8](#)

[Windows 7](#)

[Windows Vista](#)

Thank You for reading this thread.

Important Notes

This thread is NOT complete, I'll be adding more entries soon .

All the information including price is grabbed from official webpages.

All ratings (Advanced +, Advanced etc.) are concluded from reputed security software reviewers such as av-comparatives.org & VB100.

I'm a human and I do make mistakes so if you find one feel free to let me know.

[Google](#)

[Av- Comparatives](#)

[Virus Bulletin](#)

[Wikipedia](#)

[Hackforums WHH](#)

[img]http://i1.minus.com/iLbdJjhOluAEW.png[/img]

[Corso](#) - Thanks for place holding and tip.

[Shinkirou](#) - For your opinions.

[LighterFluid](#) - Thanks for the GFX.

Corso - *July 14, 2013, 7:02 am*

Glad I don't have to placeholder anymore... lol. Nice guide, again!

LighterFluid - *July 14, 2013, 7:03 am*

This is one of the most useful threads I've seen about this subject personally glad to know my Anti-virus is one of the bests. Thanks for spending the time to write this.

Antigen - *July 14, 2013, 7:10 am*

Thanks Corso and LighterFluid, means a lot.

1nf4m0us - *July 14, 2013, 7:14 am*

Don't forget to mention that you need 4GB of ram to run all those programs at once (jk).

You can use all those or simply switch to a free *nix distribution and keep the headache away, plus you save some pocket money.

Thanks for your effort writing this guide.

Antigen - *July 14, 2013, 7:19 am*

(Jul 14, 2013 07:14 AM)tokivena Wrote: [\[CITE\]](#) Don't forget to mention that you need 4GB of ram to run all those programs at once (jk).

You can use all those or simply switch to a free *nix distribution and keep the headache away, plus you save some pocket money.

Thanks for your effort writing this guide.

*nix distributions are good but last time I heard there can be virus in linux too ! ?

I'll add requirements soon.

Thanks

im abcd - *July 14, 2013, 8:00 am*

Nicely laid out and very informative! Good work. :)

Wires - *July 14, 2013, 8:39 am*

Very nice and detailed guide. I may refer back to these in future.

Antigen - July 14, 2013, 1:17 pm

Thanks for the appreciation.

I'm adding more sections like Online Scanners and stuff.

Hepic - July 15, 2013, 12:50 pm

Great thread, conclusive information, bookmarked it for future reference and this should be stickied.

Antigen - July 15, 2013, 8:38 pm

(Jul 15, 2013 12:50 PM)Hepic Wrote: [\[CITE\]](#) Great thread, conclusive information, bookmarked it for future reference and this should be stickied.

Thanks for your appreciation, I hope so but the very purpose of this thread is to help people and everyone can find this thread with my Signature so I don't care about being stickied.

Ynne - July 16, 2013, 6:09 am

Really nice thread indeed, looks like you've worked hard for this.

Antigen - July 16, 2013, 7:31 am

(Jul 16, 2013 06:09 AM)Ynne Wrote: [\[CITE\]](#) Really nice thread indeed, looks like you've worked hard for this.

Thanks for your appreciation, Yea I dedicated whole 2 days :)

Annoited - July 16, 2013, 10:44 am

Very informative and many users should read this first before posting any threads relating to WHH! Good job Anti, nicely written guide, once again. ?

Antigen - July 16, 2013, 12:21 pm

(Jul 16, 2013 10:44 AM)Annoited Wrote: [\[CITE\]](#) Very informative and many users should read this first before posting any threads relating to WHH! Good job Anti, nicely written guide, once again. ?

I hope so, I saw many members asking for which Antivirus is good, what should be better to remove malware etc, that's why I wrote this up.

Thanks for your kind words.

Altera - July 18, 2013, 5:53 am

Damn, so many words :s

I'll try to read it all xD

Anyway nice thread bro.

efinitix - July 19, 2013, 4:18 am

Very nice guide, I've actually been thinking about picking up bitdefender.

BlackHatBrony - July 19, 2013, 7:59 am

Nice lot of information and it seems to be all trues atleast for the A/V I have used

HOLY SHIET RYMEZ - July 19, 2013, 3:18 pm

You sure that norton is so bad i havent problems with it yet and THE NortonPowerEraser is a really gerat tool from norton.

Alex© - July 20, 2013, 5:04 am

Really good thread thanks for the upload, this will help out lots of users.

Antigen - July 20, 2013, 8:23 am

(Jul 19, 2013 03:18 PM)HOLY SHIET RYMEZ Wrote: [\[CITE\]](#) You sure that norton is so bad i havent problems with it yet and THE NortonPowerEraser is a really gerat tool from norton.
Norton is a known resource hog and that makes Norton NOT a good AV.

(Jul 19, 2013 04:18 AM)R00TZer0 Wrote: [\[CITE\]](#) Very nice guide, I've actually been thinking about picking up bitdefender.
Bitdefender is a good choice, in fact many other AV is using Bitdefender's engine.

Deep Web - July 29, 2013, 9:29 am

thanks a lot antigen helped me a lot

Artisanal - July 30, 2013, 9:05 am

Great thread, really usefull ! ?

Mind adding [Comodo Internet Security](#) ? ?

Antigen - July 30, 2013, 9:07 am

(Jul 30, 2013 09:05 AM)Zombay Wrote: [\[CITE\]](#) Great thread, really usefull ! ?

Mind adding [Comodo Internet Security](#) ? ?

Thanks for your words, I'll add it soon.

But can't add Ratings about comodo since I grab that kind of info from other reputed AV researchers.

x534n - July 31, 2013, 5:22 pm

A very good, informative guide. Thanks for taking the time posting this.

Another AV I am liking is Vipre, it isn't as well known but I've been using it and I like it. I'd like to hear what you think of Vipre.

Antigen - August 2, 2013, 11:43 am

(Jul 31, 2013 05:22 PM)x534n Wrote: [\[CITE\]](#) A very good, informative guide. Thanks for taking the time posting this.

Another AV I am liking is Vipre, it isn't as well known but I've been using it and I like it. I'd like to hear what you think of Vipre.

Thanks for your appreciation, I'll add it soon.

But can't add Ratings about Vipre because I grab AV Ratings from other reputed AV researchers and they don't provide data about Vipre.

Infinity_ - November 19, 2013, 12:47 pm

Hey I'm trying to decide between eset, and kepersky. Which one would you recommend and is esets slightly lower detection rate a big deal? Thanks!

Corso - November 19, 2013, 4:16 pm

Infinity_ Wrote:Hey I'm trying to decide between eset, and kepersky. Which one would you recommend and is esets slightly lower detection rate a big deal? Thanks!If you have a good system, 4GB of RAM and a Dual or Quad (or above) core system - You may consider Kaspersky. If you are already on a slow or weak system, go with Eset. Eset uses less system resources, hence that choice.

Either way, install and run weekly or bi-weekly scans with [Malwarebytes](#) free edition (or pay for Pro if you so choose). This is more for a secondary scan and opinion. Example, when a doctor says you are terminally ill but feel fine/seem fine, you'll want a second opinion or tests to be run - Hence where [Malwarebytes](#) comes into play.

NOTE: Do NOT install two antiviruses at the same time and do not mistake [Malwarebytes](#) as a anti virus!