GeCAD srl

The Software Company

User's Guide

RAV for Linux/FreeBSD/BeOS

version 8

GeCAD Software - Sos. Mihai Bravu, nr. 223, sector 3, Bucuresti

tel./fax 321 78 03, hotline: 321 78 59

Copyright © 2000 GeCAD Software® s.r.l.

GeCAD reserves itself the right to revise and modify its own products according to its own necessities. This material describes the product, as it was in the moment this material was written and may not correctly describe further developments. For this reason we recommend you to read the whatsnew.txt file located in the folder where you installed RAV.

GeCAD cannot be held responsible for any special, collateral or accidental damages, related in any way to the use of this manual.

GeCAD's entire liability, depending on the action, cannot go beyond the price paid for the product described in this material.

GeCAD does not guarantee either implicitly or explicitly the suitability of this material for specific needs. This material is provided on an "as-is" basis.

GeCAD Trademarks: GeCAD, GeCAD Fast Commander, GFC, RAV, Reliable AntiVirus, A.V.A.C., RAlert, RAVUtil, RAVeSpy, R.A.C.E., RAX, WisDOM.

The following are registered trademarks of their respective owners: Times New Roman, Courier, Arial, IBM, OS/2, Intel, Microsoft, MS-DOS, Windows, Windows95, Windows98, WindowsNT, QEMM, F-PROT, TBSCAN, Viruscan, TBAV, DSAV, DrWEB, AVP, MSAV, MS Office, MS Word, MS Access, MS Excel, MS Visual Basic, NetWare.

Date: 26.02.2001

Table of Contents

License Agreement

RAV AntiVirus Desktop is a registered trademark of GeCAD Software s.r.l.

All the products and the their licenses are accompanied by a License Agreement.

Before installing or using The Software, please read carefully The License Agreement. This is a legal agreement between you and GeCAD Software s.r.l ("GeCAD") for the software product you are installing, which includes computer software and related documentation. By installing or otherwise using the software, you accept all the terms and conditions of this agreement. If you don't accept the terms of this agreement, you don't have the rights to install or otherwise use The Software.

This Agreement represents the complete agreement concerning this license between the parties and supersedes all prior agreements and representations between them. This Agreement may be amended only in writing executed by both parties.

THE ACCEPTANCE OF ANY PURCHASE ORDER PLACED BY YOU IS EXPRESSLY MADE CONDITIONAL ON YOUR ASSENT TO THE TERMS SET FORTH HEREIN, AND NOT THOSE CONTAINED IN YOUR PURCHASE ORDER.

> ***! On your original CD for installing the product you may find other programs in addition to what you have bought. Those programs are offered for evaluation and they are making the object of the terms of The License Agreement for Evaluation Versions.***

Introduction

Congratulations!

You have just acquired one of the best Antivirus Software, among the first ten antivirus programs in the world.

RAV Antivirus, now at version 8, has been tested on a wide range of computer hardware, in order to check its compatibility and performance. The team that realized this product is doing antivirus research since 1989, the application itself being commercially available since 1993 and being constantly improved, both in terms of detection and cleaning rates and in terms of usability.

We suggest you take a moment to fill the Registration Form attached to The License Certificate. All personal data you fill in this form is strictly confidential and will only be recorded in our database of registered customers, to keep you informed of new developments, updates and activate your technical support account. All suggestions you wish to make will be taken into consideration for future versions. We care very much about your opinion, and we try to fulfill our customers' requests as soon as possible. Remember that it is you, the RAV user, who can make it better, the way you like.

The License Certificate is your guarantee that GeCAD Software legally licenses the program you have acquired, under the law 8/1996. It grants you the rights to use the product according to the terms of The License Agreement, to upgrade it to the new versions at preferential prices, and to receive free revisions of the current version.

> ***! Because of the attention we pay to delivering highly efficient antivirus software, the rapid evolution of viruses and implementation of features requested by our customers, the present documentation may not be up to date. The best source of information on RAV is our website, which you can find at http://www.gecadsoftware.com, http://www.ravantivirus.com.***

How to use this manual

This manual will describe RAV for Linux setup procedures, RAV functionality and configuration, as well as offer brief information on computer viruses, infection methods and several virus analysis reports written by or virus research team members.

To make sure you will be using RAV for Linux efficiently from the beginning, we recommend you to read carefully this guide, even if you are using a previous version of RAV AntiVirus.

Required hardware and software

Hardware requirements:

Processor: Intel compatible.

RAM: A minimum of 8 MB of RAM is required.

Free space on disk: RAV for Linux requires a minimum of 3 MB of free disk space. Additional free space is also required for log files (if logging to file is enabled), as well as for storing suspicious files in the Quarantine.

If you bought the complete package, you need a **CD-ROM unit**.

For update, you will an active **connection** to the Internet.

Software requirements:

For installing and running RAV for Linux on your system, you will need:

- glibc-2.1.2-11 (www.gnu.org)
- gtk+-1.2.8-1 (www.gtk.org)
- XFree86-libs-3.3.5-3 (www.xfree86.org)

Getting to know your friends and enemies

Generalities

Since you have already bought an antivirus software, there is no doubt that you know what a virus is. However, let's start with some basic virus theory…

What is a computer virus?

This question received different answers from the specialists – all having in common a basic definition of the virus:

The virus is a computer program that is able to replicate.

One who thinks that the virus is a malefic and genial creation of a programmer is wrong. Viruses are usually written by mediocre programmers. Due to the expansion of the Internet, it is very easy for viruses' authors to exchange opinions, discoveries, even sources. That is why, after one author makes public a virus's sources, many variants of that virus appear immediately. Let's take for example the virus WIN95/CIH. There are, at this moment, tens of variants for this virus and other viruses based on it, just because its author made public its sources for the "interested" programmers. More than that, other authors are using routines of old viruses; an example being the routine for destroying the Flash BIOS from WIN95/CIH, already integrated in many other viruses.

People are used to consider trojans and viruses as the same thing. However, these are distinct software types and we should pay attention to each of these categories.

Viruses are programs capable to replicate. For example, a virus for executables will try to infect other executables on disk when launched from an infected program.

Worms are programs that replicate through systems. For example, I_Worm/Happy replicates using electronic mail. When one user affected by this worm sends an e-mail, I_Worm/Happy will attach itself to that e-mail, spreading to other systems. There are several types of worms, classified by the way they replicate:

- *I_Worm* – they use the e-mail for replication;
- *mIRC_Worm*, *pIRC_Worm*, *vIRC_Worm* – use IRC clients for replication;

- *network worms* – search systems that they will infect by attacking the computers from the local network or by randomly searching computers connected to the Internet.

Trojans - are (as their name suggests), programs that gain access to a computer claiming a fake functionality, generating unwanted side effects. This category can be divided into the following subcategories:

- *Backdoors* – once launched, enable the host system to be controlled remotely. There are several commercial or non-commercial applications that do the same thing; the difference is that the backdoors run without the user awareness.
- *Passwords stealers* – decrypt the passwords from the Windows 9x PWS files or the Windows NT RAS files, and send them to the authors of the password stealers.
- *D.O.S. tools* – D.O.S. (Denial-of-Service) are a newer class. These programs try to block Internet sites by sending very large information packages or incorrect requests. A very well known case is that of the Trojan/D_O_S.Trinoo or Trojan/D_O_S.Tfn2k that tried to block the Internet access for some very well known Internet sites.
- *Simple Trojans* – they produce damages to the affected system upon launching or when a condition is activated. That is why this class is also known under the name of "*logic bomb*".

The three categories presented above (viruses, worms and trojans) can merge very well into a single program. Let's take for example Win32/Moridin; it contains all the three characteristics: virus – it infects Win32 executables and Word documents; worm – it replicates using MAPI-compliant e-mail clients and IRC programs; backdoor – it accepts remote commands.

All these categories can be included in a super-class, named "*malware*". Viruses, worms and trojans can be included in other programs – those programs are named "*droppers*".

Taking into account the target of infection, viruses can be classified in several categories. It is not necessary for a virus to have only one target for infection. Viruses having multiple targets are named "*multipartite*".

Boot viruses – they use for replication the boot sector of the floppies, MBR (master boot record) or the boot sectors of the fixed disks. The only way of replication for these viruses is booting from the infected disk. Accessing or copying the infected disks are not dangerous operations as long as the system is not started from the infected disk.

Tips against boot viruses:

> Change the boot sequence from BIOS, so the floppy won't be the first in that sequence. That way, you are protected when you accidentally forget an infected floppy in your floppy drive. Booting from the floppy drive could be necessary only when installing/reinstalling the Operating System or scanning for some special viruses. We recommend you to scan the floppy disk using an antivirus program

after formatting and copying system files on it; after that, activate the floppy write-protection.

Parasitic viruses – they infect executable files, so that when the infected file is launched, the virus code gains control. They usually execute prior to normal executable code. Then, the original code regains control and, in most cases, executes normally. There are viruses that gains control after the execution of the original code ends or when a routine from this code is called. These viruses are more difficult to detect, but they are less spread too, due to their complexity and the way they replicate.

Because these viruses infect executable files, they could spread through any data storage or transfer media: floppies, CDs, modems, networks. The virus spreads when the host file is executed.

Parasitic viruses may be memory resident (after the launching of an infected file, the virus stays in memory and infects other active files) and non-resident parasitic viruses. The non-resident parasitic viruses infect a number of files, then return control to the host program.

Parasitic viruses need to be able to distinguish between infected and non-infected files. If a virus is unable to do this (such as certain versions of the Jerusalem or Vienna viruses), they will repeatedly infect a file until this will become too large and the virus will be easily detected.

Tips against parasitic viruses:

- When you notice that the programs you usually work with became larger, use an antivirus program. Because the virus can hide itself in your system (stealth viruses), you must launch the antivirus from a bootable clean floppy disk.
- When an installing kit or a program that is capable to verify itself warns you that it is corrupted and you are sure about the functionality of that program, use an antivirus program. If you have a backup copy, we recommend you to use it, after you verify it too. Even if the antivirus cleans the viral code, many viruses change parts of the original program, leading to the impossibility of using that program. The best example is that of Win95/CIH, which overwrites parts of the file supposed to be unused; that is why the installing kits (which verify themselves) won't work properly after being infected with Win95/CIH.

Companion viruses create a file having the same name, but another executable extension; for example, if you have a file named PROGRAM.EXE and you notice that a file named PROGRAM.COM appears, this is a possible infection with a companion virus (when the operating system encounters two executable files, with the same name but different extensions, it will first launch the .COM file). If the effect is the same for more executable files, the infection is obvious.

Link viruses are extremely dangerous because they use an unusual infection method. Link viruses do not change the content of an executable file; they alter

the directory structure, redirecting the directory entry of an infected file to the area that contains the viral code. Once the virus has executed, it can load the executable file, knowing the correct directory entry of the file. Eliminating such a virus from the system is both difficult and risky.

Macro viruses are placed inside one or more of the macros inside the document. At this moment, the number of macro viruses is growing very fast (more than 6,000 in August 2000). Due to the powerful features of Visual Basic for Applications, it is very easy to use all the facilities offered by Microsoft in Windows. For example, to send an e-mail you need at most 10 code lines. That is probably why many macro viruses have worm capabilities (the best example is W97M/Melissa.A@MM).

System infector viruses, when infecting a drive, do not change the MBR content or the boot sector, but partially modify the FAT allocation of IO.SYS (or its equivalent, IBMBIO.COM) to allow inclusion of their own viral code sequence at the beginning of this file. Because, at boot time, DOS reads IO.SYS in a linear way, the virus will be read before the IO.SYS code. On the other hand, if the IO.SYS file is opened with a text viewer, it will appear perfectly normal, because the FAT allocation chain correctly includes the area overwritten by the virus, which has been saved to another area on the disk.

Multipartite viruses combine two or more basic types from those described above. There are viruses capable to infect executables and Word documents, or viruses capable to infect boot sectors and executables, etc.

Viruses' authors are trying to include as many "*facilities*" as possible in their creations. A perfect example is Esperanto, capable to infect files on different operating systems and to run on different hardware architectures (i386 and Mac).

How do viruses spread?

The most widely spread viruses are those having worm capabilities (VBS/Loveletter, W97M/Melissa.A@MM). The worms are spreading rapidly, too: VBS/Stages, I_Worm/Kak, I_Worm/ZipExplorer or I_Worm/Happy99. The expansion of the Internet put them on the first place regarding virus spreading.

The exchange of documents between users is a favorable way of spreading macro viruses.

In the last years, boot viruses lost their "popularity" because the floppy disks are more and more rarely used.

What can viruses do?

Some viruses are boring, while others are extremely dangerous. The least they can do is to increase the file size and slow down the computer. Many viruses only try to spread, not to damage your computer. There is, however, the

possibility for such benign viruses to occasionally interact with other software and damage your computer. That is why there are no viruses that do not produce any damage – even a simple change in an installing kit might be considered one.

Other viruses are far more dangerous, intentionally modifying or destroying data, or deleting files and / or formatting your drive. Till Win95/CIH it was said that viruses couldn't destroy or damage hardware components. CIH was the first virus (and unfortunately not the last) that was able to modify the Flash BIOS so that the computer would not work when subsequently booting the system.

Another virus capable of hardware damage (but in a strange way) is {Win32,W97M}/Beast. During the night, Beast opens and closes the door of the CD-ROM unit for two hours! This will damage that unit for sure!

How can we protect ourselves against viruses?

There are no "*recipes*" for making our applications and our computers to viral attacks.

The data security expert team from GeCAD recommends you to use an Antivirus Software. You will have to apply the following rules in order for such a program to be effective:

- *Rule #1: Protect your data – use an Antivirus Software!*
- *Rule #2: Use the proper AntivIrus for your necessities!*
- *Rule #3: Keep your AntiVirus up to date!*
- *Rule #4: Use a complete AntiVirus protection!*
- *Rule #5: If you find a virus, don't panic; your AntiVirus will solve the problem (contact the technical support of the producer)!*
- *Rule #6: Keep informing on the latest viruses and other threats to data security!*
- *Rule #7: Always apply the first six rules!*

We also recommend:

- Install ONLY original software, obtained through legal distribution channels.
- SCAN for viruses all the CDs that you run programs or open documents from, even if the source of those CDs is "secure". There are many cases of CDs containing viruses without the intention of the producer (CDs from magazines, presentations of famous software producers, etc.).
- DON'T open e-mail attachments, even if they are presented as text files or they came from known persons. Let's take for example

VBS/Loveletter: when run on a system, it sends a file (presented by the mail client as a text file) to all contacts from the address book.

- DON'T launch programs obtained from insecure sources. When you receive a text file or an executable through a discussion list, for example, don't launch it until you verify it with an up to date AntiVirus.
- Even your best friends can try to play tricks on you (innocent ones at the beginning). There are several backdoor programs distributed on the Internet and very well documented. When a friend sends you an executable file, we recommend you to scan it for viruses. The most dangerous thing is that even the backdoors can act like droppers and can spread viruses. In the second half of the year 2000, due to the large number of backdoor programs (Netbus is the best example), some worms capable of finding computers for infection using these programs appeared.
- DON'T use backdoor programs as tools for remote administration. There are many commercial or free programs that do the same thing in a safer way than backdoor programs.
- UPDATE your operating system. The new versions of Windows 2000 and Windows 98/ME give the possibility of updating through Internet. Using these updates, you will have a safer system – many viruses are based on errors in the operating system project.

RAV AntiVirus offers daily updates. This means that, no later than one day from the discovery of a new virus, you will have the solution for detecting and cleaning it. That is why we recommend the update to be done as frequently as possible.

RAV, a friend you can't live without?

If you are familiar with antivirus software, RAV will appear extremely easy to use.

The main purpose of efficient antivirus software is virus infection prevention. RAV is able to detect a large number of viruses, including all Romanian viruses, and that is why we consider it the best Romanian antivirus software. This may become very important, as the following case demonstrates. Starting 1995, on December 17, many users had the unpleasant surprise to see that their systems were no longer working. The cause was the virus known as RP.Dec_17, which either was not detected, or erroneously detected as Rhubarb. When trying to clean, the result was disk damage. Users of RAV Antivirus had no problems because, long before, the virus was isolated and analyzed by our team. RAV 3.2 was already able to successfully eliminate it (this because of permanent user feedback and the product's ability to isolate new viruses).

Using new heuristic methods, RAV can detect all the potentially dangerous actions, specific to viruses, so that new/unknown viruses are also detected.

The daily updates and the free access to our virus databases give you the possibility to use a permanently updated product. The update is done for all installed components.

Because we consider all your suggestions and due to a permanent user feedback from the entire world, RAV proves it has a new quality: flexibility.

The power and development speed of RAV are recognized worldwide by its placement in *the first ten anti-virus products* as a result of tests run by the Virus Bulletin and Virus Test Center in Hamburg. Read the ***About RAV AntiVirus*** chapter for details.

What to do when you find a new virus?

Even if RAV will detect almost any virus you will be confronted with, there may be exceptions, which should be considered, such as viruses specially created not to be detected by RAV. More than that, taking into account the actual rate of virus creation, we could say that there is no program able to eliminate, nor to detect all the existing viruses.

If you think your system is infected with a new virus, or if RAV reports a suspicious file, we recommend sending the file(s) to GeCAD for analysis. For details on sending files, read the chapter ***Technical Support***.

> ***! Visit the GeCAD Internet sites, www.ravantivirus.com and www.gecadsoftware.com for latest information and free updates of the virus databases.***

About RAV AntiVirus

RAV AntiVirus Desktop v.8

RAV AntiVirus v.8 Product Family

The RAV family had, at version 7, the following members:

- RAV 7 Desktop – contained a DOS version and a Win9x/NT Workstation version, as well as another components and utilities (Monitor, Scheduler, Live Update, etc.).
- RAV 7 MailGuard – for MS Outlook.
- RAV 7 WebWatcher – for Internet Explorer and Netscape.

Now at version 8, RAV AntiVirus integrates all the Desktop components in a single product:

- RAV for DOS *(freeware for home users)*
- RAV for Windows
- RAV Monitor for Win9x/2000/NT
- RAV for Office 2000
- RAV for Outlook
- RAV for Internet browsers
  - RAV for Internet Explorer
  - RAV for Netscape Communicator
  - RAV for Netscape Messenger
  - RAV for Opera
- RAV for Linux *(freeware for home users)*
- Utilities:
  - RAV Configuration Center
  - RAV Tray
  - RAV Scheduler
  - Virus Info
  - RAV Quarantine
  - RAV Update
  - Rescue Disk
- **Auxiliary utilities:**
  - RAV_ONE
  - RAV_D17

Version 8 presents a better integration between its components.

RAV Enterprise Server is now a distinct product, based on client-server technologies. You can find more details on *RAV Enterprise Server* at ***www.ravantivirus.com***.

Technology

Based on a multi-layer and multi-platform technology for antivirus protection, RAV AntiVirus v.8 includes the latest specifications and technologies of the antivirus industry, some of them worldwide unique .

- **TPI** (Total Platform Independent) technology – a worldwide premiere (the same engine for detection and cleaning, and a single signatures database for all components and programs, no matter what platform or operating system they are used on);
- **MLES** technology (Multi Layer Embedded Scaning). Scans "embedded objects" on multiple layers – a top technology;
- **IC** technology (Integrity Check) – a new technology that increases the scanning speed with 50%;
- **UCP** technology (Updates Cumulative Plugins). Cumulative Updates (contain only the latest available signatures => very small files). There are two layers for these updates: weekly and daily;
- **HMETH** technology – Heuristic METHods for all existent types of viruses (including BAT, VBS, JS, etc.) – unique in the world. A new code emulator, capable of interpreting executables no matter what platform they run on (DOS, Win32, Linux, etc.), using speed optimized algorithms (~40% quicker than RACE from RAV v.7);
- **RELO** (RAV Engine LOader). Micro-kernel architecture, using operating systems' technology (the kernel is booted by RELO – RAV Engine Loader) – unique in the world;
- **Behavior Blocker** technology. "On Access" modules (Monitor, Outlook and Office) use Behavior Blocker technology (they report dangerous actions and wait for user confirmation – depending on configuration) – they eliminate the possibility of destructive actions performed by some viruses or trojans;
- **Virtual File Systems**. Working with Virtual File Systems, RAV scans the processes in memory and IFS chains (for detecting and cleaning resident viruses like CIH).

Facilities

General Facilities:

- RAV AntiVirus Desktop is an integrated suite. It contains all the necessary components in one single installation!
- Everyone can use it efficiently: professionals – Advanced Mode; home users – Quick Mode.
- The Quick Panel is an optimized variant: you can scan for viruses every resource of your computer by one single click! More than that, the interface could take whatever shape and look you want it to!
- You can configure all the components in one single window – RAV Configuration Center!

- In a world where new threats appear every day (viruses/trojans), The RAV Antivirus Research Team ensures a daily update of virus database;
- RAV AntiVirus Desktop components detect not only viruses, but also all the existent malware: viruses, backdoors, trojans, worms, etc.
- RAV itself is protected against trojan attacks, all modules being signed and verified.

Engine:

- RAV Engine accurately detects more than 55,000 viruses (on the date this guide was written) and the RAV Antivirus Research Team adds all the new viruses daily.
- Based on the new technologies used, the scanning speed is superior to any other antivirus engine.
- Heuristic methods for all conventional viruses, including boot viruses.
- Detection (including heuristic methods) and precise identification for all macro viruses (Word, Excel, Access, etc.).
- Modules for scanning inside archives that can detect infected files in all most known types of archives (zip, arj, rar, ace, lha, lhz, gzip, tar, cab, etc.); it scans archives inside archives no matter how deep they go.
- The new engine scans inside packed executables (lzexe, pklite, cryptcom, wwpack, aspack, pepack, vgcrypt, upx).
- Mail files can be scanned not only from the mail client, but also from the command line (uuencode, base64, mime, quoted printable).
- Working with Virtual File Systems, RAV can scan the processes in memory, IFS chains (for detecting and cleaning resident viruses like CIH).
- The multi-platform native language for viruses' detection and cleaning guarantees a minimal response time for new viruses, on all platforms and processors supported.

Specifics:

- GeCAD Software offers free protection: the components for MS-DOS and Linux are free for home users. These components have all the capabilities found in all the other components and can detect all the known viruses.
- For exigent users, the scanning from the command line can be used, including from MS-DOS prompt and from Linux.
- RAV monitors every action of opening/copying files from your computer.
- MS Office 2000 documents (Word, Excel, Project, etc.) are scanned before opening, for a complete protection against the most spread viruses: macro viruses.
- Triple protection against e-mail infections (Outlook and Netscape Messenger): RAV scans and cleans all the incoming messages,

prevents sending accidentally infected e-mails and warns the sender of an infected file.

- RAV protects the files downloaded from the Internet using Internet Explorer, Netscape or Opera, scanning them before they are copied on the local disk.
- Additional utilities for data recovery (OneHalf, RP.Dec_17th).
- "Year 2000 " Compliant.

Others about RAV:

- RAV AntiVirus received the following awards:
- UK Virus Bulletin 100% Award September 1999;
- UK Virus Bulletin 100% Award November 1999;
- ZDNet Editor's Pick/June 1999;
- Virus Test Center Hamburg - TOP 5 for high level of stability during installation and usage - March 1999;
- Binary 1999 – the award for the best software program in Romania.

Updating RAV

For an efficient protection, RAV must be periodically updated.

Considering the present rate of appearance of new viruses, an antivirus program becomes obsolete in a few months (sometimes even weeks or days) if it is not updated.

RAV AntiVirus includes an utility that let you update RAV from Internet or from the local area network. See the chapter *RAV Update* for details.

! Until the new version comes out (version 9) all updates are free for all users!

Generalities

RAV for Linux is a product offered by GeCAD for your protection against viruses. The program detects and cleans both viruses in Linux and viruses in Windows or Dos (all RAV AntiVirus products use the same virus database and detection and cleaning engines).

RAV for FreeBSD/BeOS is similar to RAV for Linux – the command line version.

Installing

RAV for Linux is distributed in rpm. format. Use the following command from an account having root privileges and from the directory where the file “ravlin8.8.0-1.i386.rpm” is placed:

```
rpm –ivh ravlin8.8.0-1.i386.rpm
```

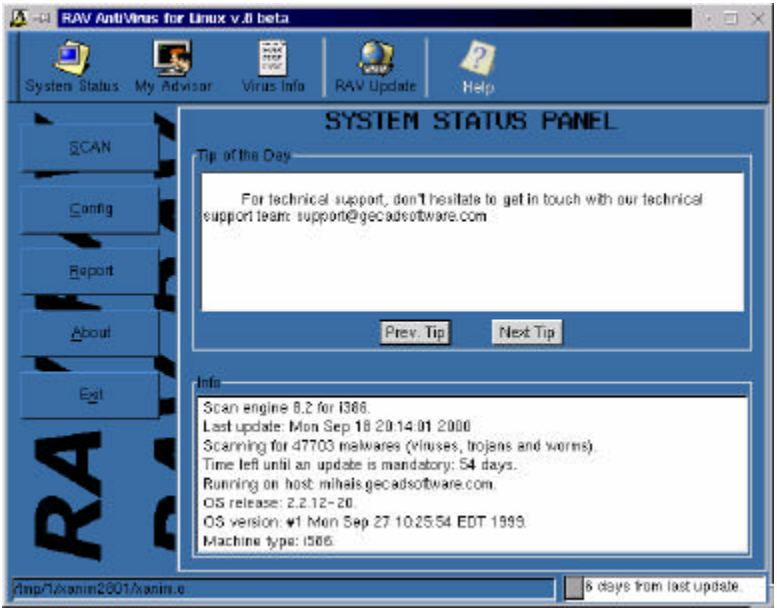
Writing “ravlin8” at a command prom pt can launch the program.

Subdirectory rav8 was created in directory /usr/local, and a link to the executable file in /usr/bin. At the first launching of the program in graphic mode, a subdirectory “.rav8” will be created in the user’s home directory, in which the report files, the configuration file and the Quarantine files will be stored.

RAV for Linux Description

In the panel below you can distinguish four components, each of them having different functionalities:

- Title bar
- Toolbar
- Sidebar
- Main window
- Status bar



Title bar

The title bar contains the name of the application, the version and the system menu, which allows you to maximize, minimize or close the window/application.

Toolbar

This area contains the following buttons:

- System Status – Pressing this button displays the System Status window.
- My Advisor – If you have an active link to the Internet, the Internet browser will open a WEB page on RAV AntiVirus site, which contains the latest news on RAV Antivirus and the world of antiviruses.
- Virus List – Displays the list of the viruses in RAV AntiVirus database.
- RAV Update – Launches the automatic update utility of RAV for Linux.
- Help

Sidebar

The sidebar of the application contains buttons that activate the main configuration and visualization instruments of RAV for Linux. These buttons are:

- **SCAN** – changes the content of the main Window to Scan Panel, allowing the user to choose the targets of a scanning job.
- **Config** – changes the content of the main Window to Config Panel, which gives you the opportunity to configure the entire RAV for Linux.
- **Report** – changes the content of the main Window to Report Panel, which offers a statistics and details on the latest scan or the current scan.
- **About** – changes the content of the main Window to About Panel, which contains information on the product.
- **Exit** – closes the application.

Status bar

The status bar has a contextual content. In this area, you can find suggestions for using the interface of RAV for Linux and details on the running action, such as the name of the file being scanned, the scan status, etc. Also, you can find, on the right side, the date of the latest update of viruses database.

Main Window

This area changes its content and functionality depending on:

- The button pressed in the Sidebar;
- The icon pressed in the Toolbar.

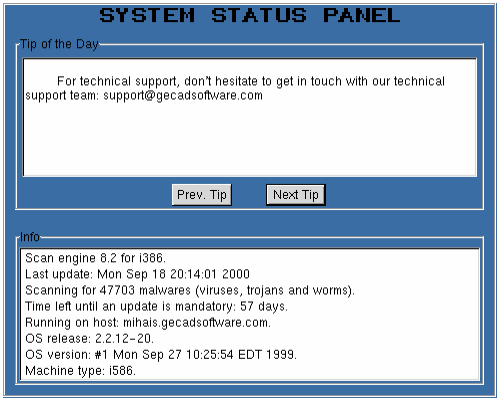
Depending on the context, the functionalities of the Main Window are:

- System Status
- Scan
- Config
- Report
- About
- Virus Info
- RAV Update

System Status Window:

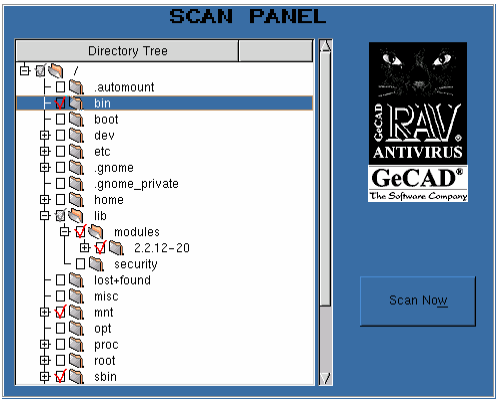
This window is displayed:

- When starting RAV for Linux;
- When pressing the icon System Status from the Toolbar;



This window contains general information on RAV for Linux and the system status: product version, the number of viruses recognized by the product, the moment of the latest update. You can also find here suggestions for a better use of the product; you can read these suggestions using ***Prev. tip*** and ***Next tip*** buttons.

Scan Panel

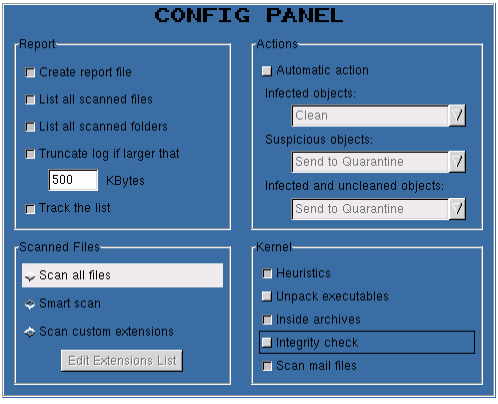


It displays a tree having as entries all the mounted disk devices. The directories you want to scan are chosen from this tree by checking the box on the left side of the directory name. After having created a list with the directories to be scanned, you can start the scanning operation by pressing **Scan Now** button.

! During the scanning this window cannot be accessed.

Config Panel

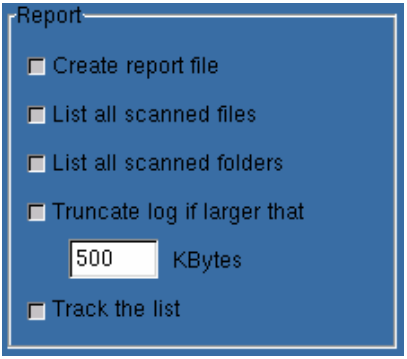
It can be accessed by using the ***Config*** button from the Sidebar.



It contains four areas for configuring the program.

Report

The available options are the following:



- **Create report file** – select this option if you want RAV for Linux to generate a report file.
- **List all scanned files** – select this option if you want RAV for Linux to write all the names of the scanned files in the report displayed in Report Window.
- **List all scanned folders** – select this option if you want RAV for Linux to write all the names of the scanned directories in the report.
- **Truncate log if larger than** - select this option if you don't want the report file to exceed a certain dimension, which you can specify in the box below (the value represents the kilobytes number, and the default value is 500 Kb).
- **Track the list** – if you select this option, you will always see in the report window the latest scanned file.

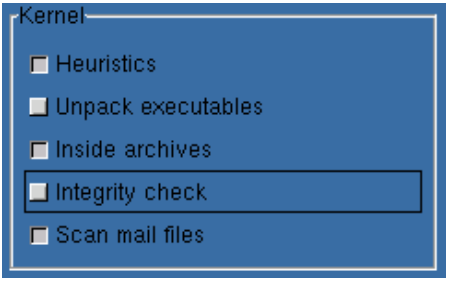
! If you don't limit the dimension of the report file, especially when you choose the listing of all files or the adding to the existent report, the dimension of this file can become dangerous for you space on the disk.

Kernel

In this area the configurations for the scanning engine of RAV for Linux can be set.

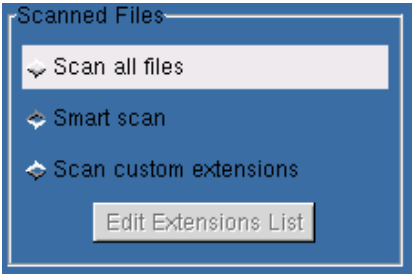
- **Heuristics** – selecting this option activates the heuristic scanning methods for detecting new, unknown viruses.
- **Unpack executables** – selecting this option activates the scan inside the executables packed with utilities such as: VVPACK, UCEXE, PEPACK, etc.
- **Inside archives** – selecting this option activates the scan inside the archives such as ZIP, ARJ, RAR, CAB, etc.
- **Integrity check** – selecting this option increases the scanning speed, using the data integrity check.

- **Scan mail files** – selecting this option activates the scan inside the mail clients files such as Outlook Express, Netscape Messenger, Eudora, etc.



Scanned Files

It specifies what kind of files will be scanned:



- **Smart scan** - **RAV** will decide what files will be scanned (as recommended)
- **Scan all files** – all files will be scanned;
- **Scan custom extensions** – only those files that have extensions in the customized extensions list will be scanned; this list can be edited after having pressed the ***Edit Extensions List*** button.

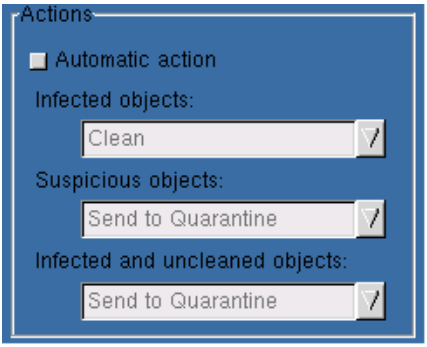
Edit Extensions List – press this button if you want to specify the extensions that will be scanned when the **Scan custom extensions** option is checked**.** The extensions that will be added to the list have to contain '.' as the first character. For instance „.exe", „.vbs".

Actions

This area offers the possibility of choosing the actions that RAV for Linux will perform when it finds infected or suspicious objects.

If the **Automatic action** option is selected (which is not recommended for inexperienced users), RAV for Linux will perform the selected actions without asking for user's confirmation. Uncheck the option to force the scanning

module to let the user decide on what has to be done when finding an infected or suspicious object.



The settings can be done for three types of objects:

- **Infected objects** – contain the body of a known virus;
- **Suspicious objects** – contain a suspicious code, which could be the body of an unknown virus or just a false alarm (contact our technical support when RAV AntiVirus finds such objects)
- **Infected and uncleaned objects** – are infected objects that failed to be cleaned.

The actions associated to these types are:

For ***Infected files***:

- **Clean** – the virus will be cleaned;
- **Ignore** – the infected file will be ignored;
- **Rename** – the file will be renamed – the first letter of its extension will be changed with character '_', so that, for instance, .doc will become ._oc and .xls, ._ls .;
- **Delete** – the file will be deleted from the hard disk;
- **Send to Quarantine** – the file will be copied in a special place on the hard disk, named Quarantine.

For ***Suspicious objects***:

- **Send to Quarantine** - the file will be copied in a special place on the hard disk, named Quarantine.
- **Ignore** – the suspicious code will be ignored;
- **Rename** – the file will be renamed – the first letter of its extension will be changed with character '_', so that, for instance, .doc will become ._oc and .xls, ._ls .;
- **Delete** – the file will be deleted from the hard disk;
- **Validate** – from now on, the suspicious code will be ignored whenever the file is scanned.

For ***Infected and uncleaned objects***:

- **Send to Quarantine** - the file will be copied in a special place on the hard disk, named Quarantine.
- **Ignore** – the virus will be ignored;

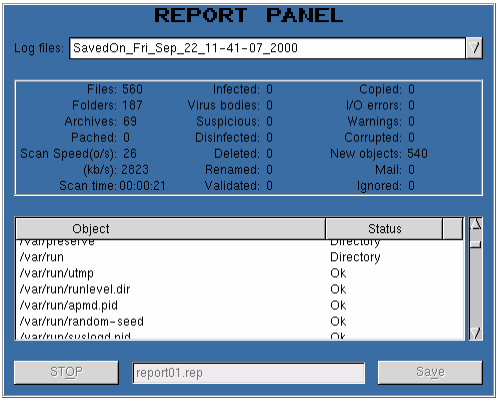
- **Rename** – the file will be renamed – the first letter of its extension will be changed with character '_', so that, for instance, .doc will become ._oc and .xls, ._ls .;
- **Delete** – the file will be deleted from the hard disk.

Report Panel

It appears in the following situations:

- When the Report button in the Sidebar is pressed;
- Automatically, after starting scanning.

The Report Panel presents statistics and details on a scanning session.



Statistics

This panel section presents general information about scanning:

- **Files** – the number of scanned files;
- **Folders** – the number of scanned directories;
- **Archives** – the number of scanned archives;
- **Packed** – the number of scanned packed executables;
- **Scan speed (o/s) (Kb/sec)** – the average number of objects scanned in one second, respectively the average number of Kilobytes scanned in one second; an object can be a normal file or a file placed in an archive;
- **Scan time** – total time of scanning;
- **Infected** – the number of files detected as infected;
- **Virus bodies** – the number of viruses found during the scan;
- **Suspicious** – the number of files detected as suspicious;
- **Disinfected** – the number of files that where disinfected;
- **Deleted** – the number of deleted files;
- **Renamed** – the number of files that were renamed;
- **Validated** – the number of files for which the validation option was chosen;

- **Copied** – the number of files copied to Quarantine; see RAV Quarantine for details;
- **I/O errors** – the number of Input/Output errors appeared during the scan;
- **Warnings** – the number of warnings;
- **Corrupted** – the number of corrupted files (files invalid for their format);
- **New** – the number of new files relatively to the previous scan;
- **Mail** – the number of scanned e-mail files;
- **Ignored** – the number of objects detected as infected or suspicious that were ignored.

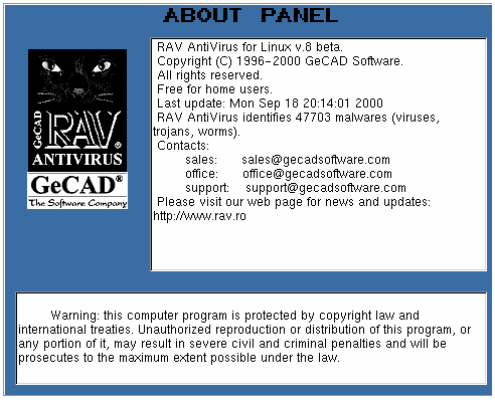
Details

The second section of this panel displays in a window a list containing the names and the status of the scanned objects. The display mode can be set in the Config Panel.

If the Report Panel is active during a scan, it updates with every scanned object.

You can save the content of the panel by pressing the ***Save*** button after the normal end of the scan or after the scan was stopped using the ***Stop*** button. On the upper side of the panel there is a list from which you can select a previously saved report to consult it; you can specify a name for the report file or the default one can be used.

About Panel

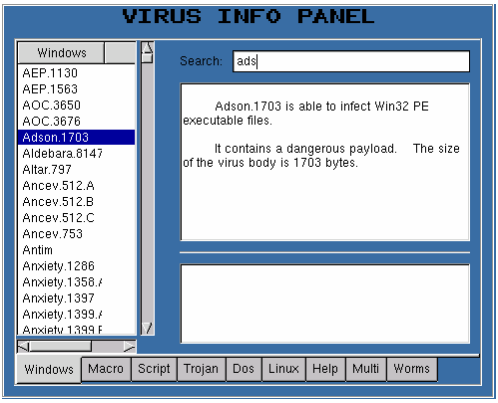


This panel presents information on the name of the product, version, time of the latest update and the addresses for the technical support.

Virus Info Panel

For a better informing of the users, RAV for Linux includes a utility that allows the display of brief information on viruses that are detected and cleaned by RAV.

This utility can also be accessed by pressing the ***Virus List*** button on the Toolbar.



The virus list is dynamic and is extracted from the viruses database. On every update of RAV, the new viruses will appear on this list.

The Virus Info Panel includes the following areas:

- The type of the virus;
- The virus list;
- The information area;
- The quick search dialog.

The type of the virus

This is an area on the lower part of the window and contains (for now) 9 sections with the types of viruses. These types are:

- **Win** – it infects Windows executables;
- **Macro** – it infects Office documents;
- **Script** – it infects script files: VBScript, JavaScript, JScript, MIRC, BAT, etc.
- **Trojan** – program that performs harmful operations instead of what it pretends to do;
- **Dos** – it infects DOS programs;
- **Linux** – it infects Linux executables;
- **Help** – it infects HLP files;
- **Worm** – it does not locally replicate but it sends itself through the Internet to other users;
- **Multi** – it theoretically belongs to more than one category among the ones already mentioned.

The virus list

It is an area on the left side of the window – a list of names (viruses names).

The information area

It is situated on the right side of the window and contains information on the selected virus in the virus list.

The quick search dialog

It is situated on the upper-right side of the panel.

To find out information on a certain virus, you will have to select the section corresponding to the type of the searched virus than to find it in the virus list or to write its name in the quick search dialog. The details on the virus will appear in the information area.

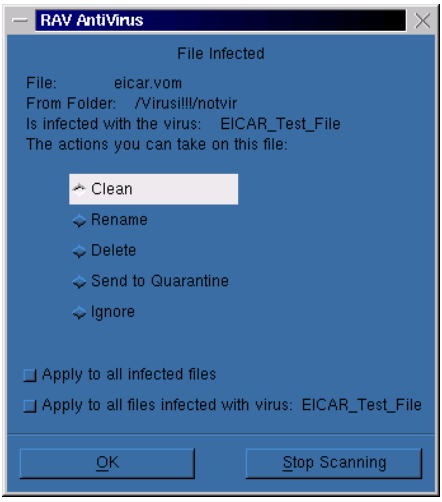
The quick search dialog immediately locates the first name that corresponds to the typed character. This way, you can also find viruses for which you don't have the exact names.

> ***! RAV AntiVirus names the viruses following the CARO international standard. Some antivirus products use other names than those imposed by this standard and that's why you might not find some nonstandard names of viruses that exist in our database.***

Operational dialogs

File Infected Dialog

This dialog appears when a file that contains the body of a known virus is detected and no automatic actions are set (see the paragraph Config Panel).



The dialog offers details on the name (***File Name***) and the path (***From folder***) of the infected file. You can also find here the name of the virus (***Is infected with virus***).

The user's choice about the action to be performed on the file is expected. The available options are:

- **Clean** - the virus will be cleaned;
- **Rename** - the file will be renamed – the first letter of its extension will be changed to '_', so .doc will become ._oc and .xls will become ._ls;
- **Delete** - the file will be deleted;
- **Send to Quarantine** - the file will be copied to the directory ~/.rav8/quarantine;
- **Ignore** - the virus will be ignored.

If you want the selected action to be automatically performed on the infected files found from now on, you can:

- **Apply to all files infected with virus** – the selected action will be applied for all the files infected with the same virus;
- **Apply to all infected files** - the selected action will be applied for all the infected files.

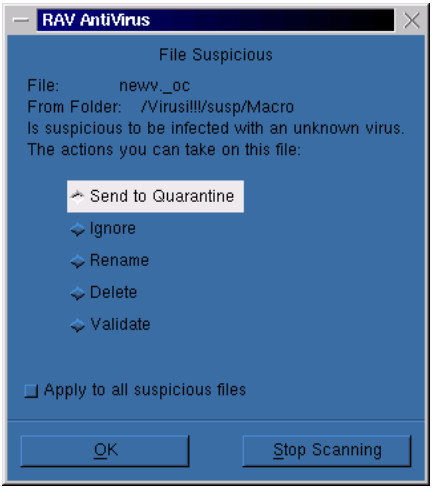
If you check one of the options described above the program will no longer ask for confirmation when finding an infected file – the selected action will be automatically performed.

After selecting the desired options, click ***OK*** to continue or click ***Stop Scanning*** to stop the scanning process.

If the selected action fails, the dialog reappears, but the previously selected action is no longer available (grayed).

File Suspicious Dialog

This dialog appears when a file that contains suspicious code is detected and no automatic actions are set. That suspicious code might be the body of an unknown virus or just a false alarm. We recommend you to contact our technical support.



The dialog offers details on the name (***File***) and the path (***From folder***) of the suspicious file.

The user's choice about the action to be performed on the file is expected. The available options are:

- **Send to Quarantine** - the file will be copied to the directory ~/.rav8/quarantine;
- **Ignore** - the file will be ignored**;**
- **Rename** - the file will be renamed – the first letter of its extension will be changed to '_', so .doc will become ._oc and .xls will become ._ls;
- **Delete** - the file will be deleted;
- **Validate** - the suspicious code will be ignored from now on, whenever the file will be scanned by RAV.

If you want the selected action to be automatically performed on the suspicious files found from now on, you can check the option ***Apply to all suspicious files***.
If you check this option program will no longer ask for confirmation when finding a suspicious file – the selected action will be automatically performed.

After selecting the desired options, click ***OK*** to continue or click ***Stop Scanning*** to stop the scanning process.

If the selected action fails, the dialog reappears, but the previously selected action is no longer available (grayed).

RAV Update

The routine for updating the viruses database through Internet was included to help you maintain an efficient protection, even against the newest viruses. To use it, you need an active connection to the Internet.

You can launch the RAV Update utility using the ***RAV Update*** button from the Toolbar.

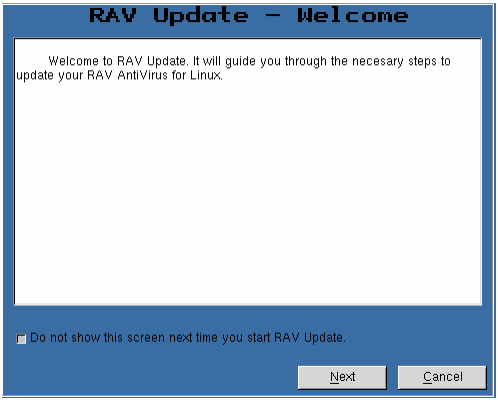
> ***! You can execute this utility only if you are running RAV for Linux from an account having superuser privileges.***

This utility assists you during the update process. All the panels contain three buttons:

- "**Next**" – go to the next step;
- "**Back**" – go back to the previous step;
- "**Cancel**" – close the Internet connection and the utility.

Step 1

Immediately after launching the utility, the window below is displayed.

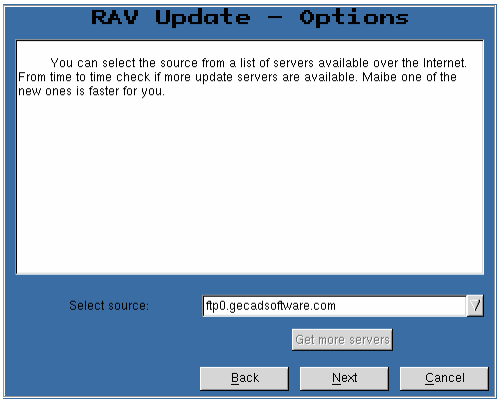


This is an introductory screen, which contains brief information on the functionality of the utility.

Check "Do not show this screen next time you start RAV Update" if you want to skip this step next time you start the utility.

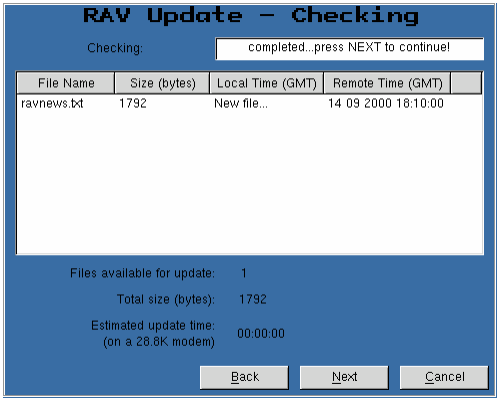
Step 2

You can choose here the source for updating RAV for Linux.



Step 3

If you have a slower connection to the Internet, the connection to the update server may take a while. If an error occurs, an appropriate message will be displayed.



After connecting to the server, all the installed files will be checked; if their version is the most recent one for all of them, an appropriate message will be displayed and the program will continue its execution – the System Status window will be displayed.

If there are more recent files on the server, their names will be dis played in the window.

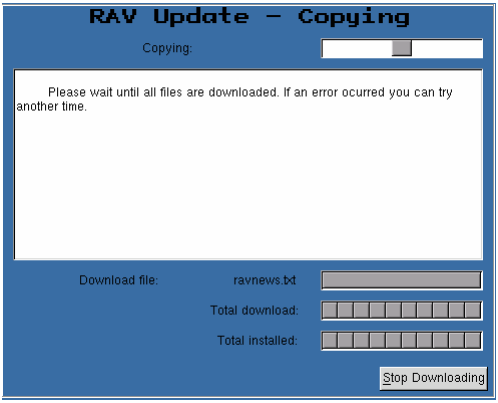
Step 4

RAV Update begins to download the files; it displays two progress bars: one for the entire operation and one for the file that is currently downloading.

There are also displayed the names of the files being downloaded.

When the downloading process ends, the window will display a message and the scanning engine will be reloaded with the new viruses databases.

One single button is available during this step – **Stop Downloading** – it stops the downloading and the update function.



You do **NOT** need to reboot your system. You will only need to restart RAV for Linux if some key elements were updated.

NOTE: One update may include one or more files. If, for some reasons, the connection with the server is lost, you can restart the update and it will continue from where it was stopped.

Using RAV for Linux

Operating modes

RAV for Linux can run both as a command line application and as X-Windows application. It will automatically start in the appropriate mode. If you want to use the command line from a graphical terminal, you will have to use “ravlin8 –h”. This will display the syntax and the options for the command line.

Command Line

Use “ravlin8 –h” to see the syntax and options for running RAV from the command line.

Graphical mode

One session of RAV for Linux as a X-Windows application can look like this:

- Execute “ravlin8” from a X terminal;
- Start the update utility for RAV;
- You can obtain information on viruses from the databases by clicking the “Virus List” button;
- From the Config Panel, choose the options for the scanning engine, the report file, the actions to be performed on infected and suspicious files, the files that will be scanned.
- In the Scan Panel, choose the directories to be scanned by checking the boxes beside them. Press the “Scan Now” button to start scanning;
- During the scanning process you can modify any option in the Config Panel; the changes apply immediately;
- When the scanning process ends you can save the report file (if the corresponding option was set in the Config Panel).

When an infected or suspicious object is found, the File Infected/Suspicious Dialog appears if you haven’t set any automatic actions.

> ***! If the Automatic Action option is checked and infected or suspicious objects are found, RAV for Linux will perform the selected actions without asking for confirmation.***

Press “Exit” for ending the session.

Technical Support

The Technical Support, regarding the installation and the functionality of the product RAV Antivirus, the latest version, is free.

If you experience any problems with RAV AntiVirus v.8:

- visit GeCAD's site, www.gecadsoftware.com , www.ravantivirus.com for the list of known and solved problems;
- send an e-mail to support@gecadsoftware.com ; our technical support team is ready to help you. For a quick and efficient response, please send us the Bug Report Form.
- phone to GeCAD Technical Support Department:
  - ⇒ +4 01 321 78 03
  - ⇒ +4 01 321 78 59

For the registered users of RAV AntiVirus the technical support is free at GeCAD's headquarters.

For a full technical support (24 hours/day, 7 days/week, 365 days/year), please contact the GeCAD Technical Support Department.

Bug Report Form

Although we have extensively tested RAV for Linux v.8, some bugs may get by us, or you may have incompatible hardware or software that we did not test. If you experience any problems with RAV, please print out this form and mail it to GeCAD S.R.L, Sos. Mihai Bravu, nr. 223, sector 3, Bucharest, Romania, or fax it to us on +40 1 321 78 03. Alternatively, copy it to your word processor, fill in the blanks and email the text file to ***support@gecadsoftware.com.*** Thank you!

Today's Date: ___/___/___ (MM/DD/YY)
Title: [ ] Mrs. [ ] Miss [ ] Ms [ ] Mr. [ ] Other:_____
Name:
Company (if applicable):
E-mail:
Address:
City:
State/Province:
ZIP/Postal Code:
Country:
Telephone (with Area & Country Codes):
Fax (with Area & Country Codes):

Program Name: RAV for Linux version:_____ Serial Number#:_____

Bugs, Wishes, Suggestions & Comments:

(Please be as specific as possible about bugs. If we cannot duplicate your problem, we cannot help get it fixed. Please read the program's documentation carefully first.)

SYSTEM CONFIGURATION
Computer:
Amount of memory:
Video Card**:** Mono/CGA/EGA/VGA/Herc/Other:
Type of Monitor**:** Mono/Color/Other:
Hard disk:
Number of floppies:
Windows Version:
Other:

How to contact RAV's producer

For details regarding the installation and the functionality of the product, please contact the dealer that you have bought the product from; if it does not offer you the adequate technical support, contact the producer.

For any problems regarding the copyright, the guarantee, suggestions and other problems related to RAV AntiVirus or data recovery from a destructive viral attack, please contact the producer.

GeCAD Software srl

Address: **Sos. Mihai Bravu, nr. 223, sector 3**
Bucharest, ROMANIA

Phone: **+40-1-3217803, 3217859**

Fax: **+40-1-3217803**

Email:

Office: **office@gecadsoftware.com**

***Sales*:** **sales@gecadsoftware.com**

***Technical support*:** **support@gecadsoftware.com**

Internet: **http://www.gecadsoftware.com**
http://www.ravantivirus.com