

# **V**ba32 Rescue **USER GUIDE**



VirusBlokAda

Copyright © 2010 «VirusBlokAda» Ltd.

Documentation version: 3.12.4.0 (January, 2010)

All rights reserved. All contents, graphics and texts, in this documentation are the property of VirusBlokAda Ltd. No part of this documentation may be reproduced in any form or by any means, including online and offline publications, without written permission from VirusBlokAda Ltd.

Microsoft® и Windows® are registered trademarks of Microsoft Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

**VirusBlokAda Ltd.**

Kalvarijskaja Str., 17, 611

220004 Minsk, Belarus

Tel.: (+375 17) 226-62-85 - Sales department

Tel.: (+375 17) 226-85-55 - Programming department

E-mail: [support-en@anti-virus.by](mailto:support-en@anti-virus.by)

VirusBlokAda may make improvements or changes in the product described in this documentation at any time. The latest version of the documentation is available on the developer's web-site:

<http://www.anti-virus.by/en/>

# Contents

<b>Introduction</b> .....	4
<b>Hardware requirements</b> .....	6
<b>Create bootable drive</b> .....	7
Create bootable CD/DVD .....	7
Create bootable USB-drive .....	7
Create bootable USB-drive in OS Windows .....	7
Create bootable USB-drive in OS Linux (without data lost) .....	7
Create bootable USB-drive in Vba32 Rescue environment (without data loss) .....	8
<b>Boot Vba32 Rescue image</b> .....	9
<b>Vba32 Rescue User Interface</b> .....	11
Midnight Commander .....	11
Shell .....	12
Dismount disks .....	13
Shutdown .....	13
About .....	13
<b>Computer scanning</b> .....	15
Scanner settings .....	16
Scanning objects settings .....	16
Interface settings .....	18
Action settings .....	18
Scanning process .....	20
Launching Vba32.CS.L in manual mode .....	20
<b>Vba32.CS.L update</b> .....	23
Network .....	23
Update scanner .....	24
Automatic update .....	24
Update via command shell .....	24
Saving updated scanner to USB-drive .....	25
<b>Appreciations</b> .....	26

# Introduction

**Vba32 Rescue** – allows to recover system functionality after malware impact.

This software allows to cure malware (and suspicious) on user's computer with maximum effect. Scanning and curing processes are produced independently from OS, installed on the computer. Due to this, malware won't be able to oppose to cure process.

**Attention!** This software doesn't protect system from appearance such situations in the future. To prevent infection of the computer, it's necessary to use the whole solution antivirus programs, given by «**VirusBlokAda**».

**Vba32 Rescue** is a bootable ISO-image, what can be written on CD/DVD-disk or USB-drive. In a basis of image there is kernel on the base OS **Linux**, loader **grub2**, console scanner **Vba32.CS.L** under **Linux** and other modules of working with file system, net environment, graphic user's interface and so on.

**Vba32 Rescue** works at the following modes:

- **vba32rescue** - standard mode;
- **vba32rescue2ram** – loading image into memory mode.

The first mode gives the standard possibilities Rescue Image and invoke by default. This mode is less exacting to computer's hardware resources.

Second mode, except standard opportunities, provides a feature of drive release from which this image was booted. This allows to perform parallel check of multiple computers, using the same bootable CD or USB-drive.

More detailed work of each of the modes considered in this guide.

Features of **Vba32 Rescue** Image:

- **high speed of loading image;**
- **drive release mode**, from which image was booted;
- **automatic configure of network environment** allows to customize the connection with update server;
- **ability to update antivirus scanner and bases** allows to maintain the image always up to date and doesn't require daily downloading the whole image;
- **saving updated image on USB-drive;**
- **ability to create bootable USB-drive in OS** Windows, Linux and in **Vba32 Rescue** environment;
- **using swap files on "weak" computers** allows to produce full service even on very old computers;
- **presence of mhdh и memtest utilites** gives the possibility to scan RAM and HDD on hardware error;
- **support of a great number of file system;**
- **using Vba32.CS.L scanner** allows to apply all the possibilities of **Vba32** antivirus kernel;
- **possibility of individual scanning configure settings;**
- **copy of infected and suspicious files to Quarantine** allows to avoid data loss due to false positives in antivirus;
- **keep report files** allows to analyze the results of system scan and maintain feedback with Technical Support.

**Note.** All products and utilities described in this guide are available for downloading from servers and also from sites «**VirusBlokAda**»:

<http://anti-virus.by/>

<ftp://anti-virus.by/>

<ftp://vba.ok.by/vba/>

# Hardware requirements

Necessary hardware requirements for different modes of work of **Vba32 Rescue** Image are specified below.

For loading:

- processor i686;
- 96МБ RAM;
- CD/DVD-ROM or USB-drive with a storage capacity of at least 128 MB.

For scanning:

- processor i686;
- 96МБ RAM;
- CD/DVD-ROM or USB-drive with a storage capacity of at least 128 MB;
- HDD with PATA or SATA interface and the corresponding controller.

For updating and scanning:

- processor i686;
- 192МБ RAM;
- CD/DVD-ROM or USB-drive with a storage capacity of at least 128 MB;
- HDD with PATA or SATA interface and the corresponding controller;
- Ethernet- interface.

For releasing drive and scanning:

- processor i686;
- 192МБ RAM;
- CD/DVD-ROM or USB-drive with a storage capacity of at least 128 MB;
- HDD with PATA or SATA interface and the corresponding controller;
- Ethernet-интерфейс.

For releasing drive, updating and scanning:

- processor i686;
- 256МБ RAM;
- CD/DVD-ROM or USB-drive with a storage capacity of at least 128 MB;
- HDD with PATA or SATA interface and the corresponding controller;
- Ethernet- interface.

Supported file systems: NTFS, FAT, ext2/3/4, reiserfs, reiser4, btrfs.

## Create bootable drive

**Vba32 Rescue** Image supports the ability to boot from two types of drives: CD/DVD and USB-drive. Below the process of creating bootable CD/DVD/USB drive.

### Create bootable CD/DVD

For creating bootable CD/DVD it is necessary to record iso-image **vbarescue.iso** on CD/DVD with burning programs.

**Note.** Before creating CD/DVD make sure that your computer supports booting from them.

**Note.** As the burning program you can use **Nero** package. For burning CD/DVD it is necessary: to put matrix in CD/DVD-ROM drive, run **Nero Burning ROM**, select menu item **File/Open**. In the appeared window, select the file **vbarescue.iso** and follow the instructions.

### Create bootable USB-drive

**Vba32 Rescue** provides three ways to create bootable USB-drive. The first way is to create in **Vba32 Rescue** environment. The next two ways are to create with the help of special utilities in OS Windows and in OS Linux.

**Note.** Before creating bootable USB-drive make sure that your computer supports booting from USB-drive.

### Create bootable USB-drive in OS Windows

It is necessary to use package utilities **vbarescue\_wintools** for this:

1. It is necessary to unzip the archive **vbarescue\_wintools.zip** in a new folder;
2. Copy iso-image **vbarescue.iso** to the folder **vbarescue\_wintools**;
3. Launch bat-file **runme.bat** and follow the instructions.

**Attention!** During the creation of bootable USB-drive in Windows all data at this drive will be lost. It is recommended to save all files from USB-drive to another drive.

**Attention!** It is impossible to create bootable USB-drive with several partitions in OS Windows.

**Attention!** OS Windows does not properly recognize a bootable USB-drive, created with **vbarescue\_wintools**.

**Note.** **Vbarescue\_wintools** supports work in Windows 2000, Windows XP, Windows 2003.

### Create bootable USB-drive in OS Linux (without data lost)

It is required to use utilities **vbarescue\_linux** package:

1. It is necessary to unzip the archive **vbarescue\_linux.tar.gz** in a new folder;
2. Copy iso-image **vbarescue.iso** to the folder **vbarescue\_linux**;
3. Mount USB-drive with FAT32;
4. Run script **runme.sh** and **runme.sh** and transfer the path to the point of USB-drive mounting.

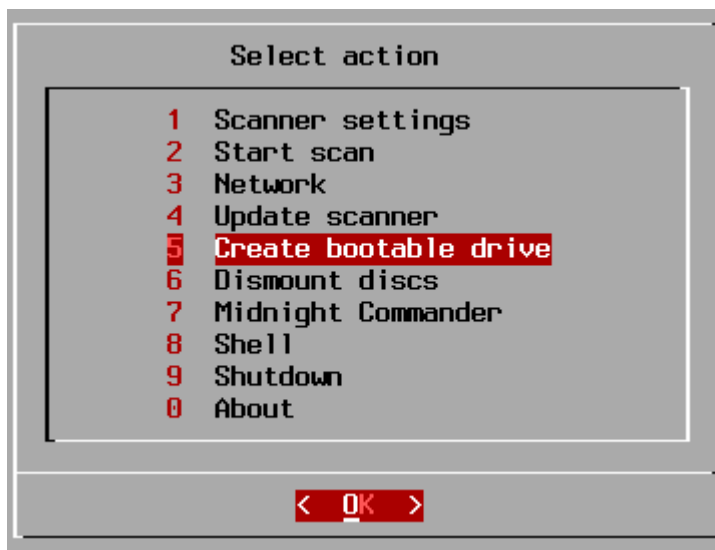
```
wget ftp://anti-virus.by/pub/vbarescue_linux.tar.gz
```

```
wget ftp://anti-virus.by/pub/vbarescue.iso  
  
tar -xzf vbarescue_linux.tar.gz  
  
mount /dev/sdb1 /mnt/flash -t vfat  
  
./runme.sh /mnt/flash
```

**Attention!** This command provides creating a bootable USB-drive without data loss. Though, it is recommended to save all files from USB-drive to another drive.

## Create bootable USB-drive in Vba32 Rescue environment (without data loss)

It is required to use the menu command **Create bootable drive**.



**Picture 1 – Menu item Create bootable drive**

Select this menu item and follow the instructions.

**Attention!** This command provides creating of bootable USB-drive without data loss. Though, it is recommended to save all files from USB-drive to another drive.

**Note.** In this mode it is possible to create bootable USB-drive with several partitions. Files will be created on the first partition. Also, if this partition isn't formatted in FAT32, it will be offered to do it.

# Boot **Vba32 Rescue** image

During **Vba32 Rescue** Image loading, user is offered the next modes of work to choose from:

```
vba32rescue >
vba32rescue2ram >
memtest
mhdd
reboot
```

**Picture 2 – Window of select Rescue Image working mode**

- **vba32rescue** – standard mode of Rescue Image work;
- **vba32rescue2ram** – Rescue Image loading mode with the ability to release drive, from which this image was loaded;



**Picture 3 – Window of remove bootable drive**

- **memtest** – launching **memtest86+**. This utility allows to scan computer's RAM to presence of hardware errors.  
Project's home page: <http://www.memtest.org/>;
- **mhdd** – launching **mhdd**. This utility allows to scan computer's hard disks to errors presence.  
Project's home page: <http://www.ihdd.ru/>;
- **reboot** – computer rebooting.

Selection one of the modes or **vba32rescue** or **vba32rescue2ram** leads to loading user's interface. It is necessary to select screen resolution.

```
screen 80x25
screen 1280x1024
screen 1024x768
screen 800x600
screen 640x480
```

**Picture 4 – Window of screen resolution selecting**

Initialization of the program internal components will start after selecting of screen resolution.

**Note.** Initialization time depends on selected bootable mode, RAM capacity, amount of partitions on hard disks and free space. Initialization can take up several minutes.

Loading of Rescue image will be finished with the dialog of selecting language of user's interface.



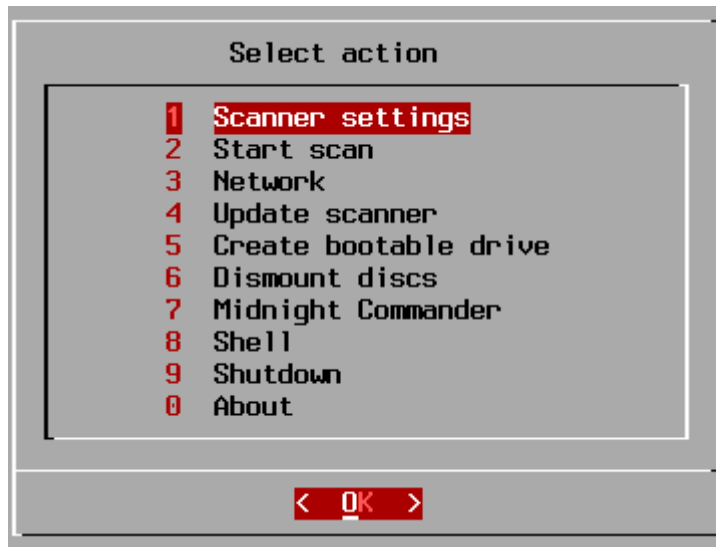
**Picture 5 – Window of selecting language of user’s interface**

**Vba32 Rescue** supports four localizations: English, Russian, German and Belarusian.

**Attention!** If the computer’s hard disks were not properly dismounted before the image downloading (for example, as a result of "cold" reboot), the computer was at Sleep or Hibernate, hard disks wouldn’t be mounted automatically to **Vba32 Rescue** Image. In such situation user will be offered to mount necessary disks in manual mode.

# Vba32 Rescue User Interface

This chapter will consider some menu settings of **Vba32 Rescue** Image user interface.



Picture 6 – Main menu

**Note.** Settings of the menu item **Create bootable drive** is considered in the chapter **Create bootable drive**.

**Note.** Settings of the menu item **Scanner settings** and **Start scan** are considered in the chapter **Computer scanning**.

**Note.** Settings of menu item **Network** and **Update scanner** are considered in the chapter **Vba32.CS.L update**.

Menu navigation is implemented using the following keys:

- **Up/down** – navigation on menu lists;
- **Left/right** – navigation on action buttons;
- **Space** – enable / disable the selected item;
- **Enter** – enter menu item or apply changes;
- **Escape** – exit menu or cancel changes;
- **Numbers** – quick selection of menu items.

Switching between entry fields and other elements of user's interface is possible using the Tab key.

**Vba32 Rescue** user interface is built on the basis of the project **Dialog**.

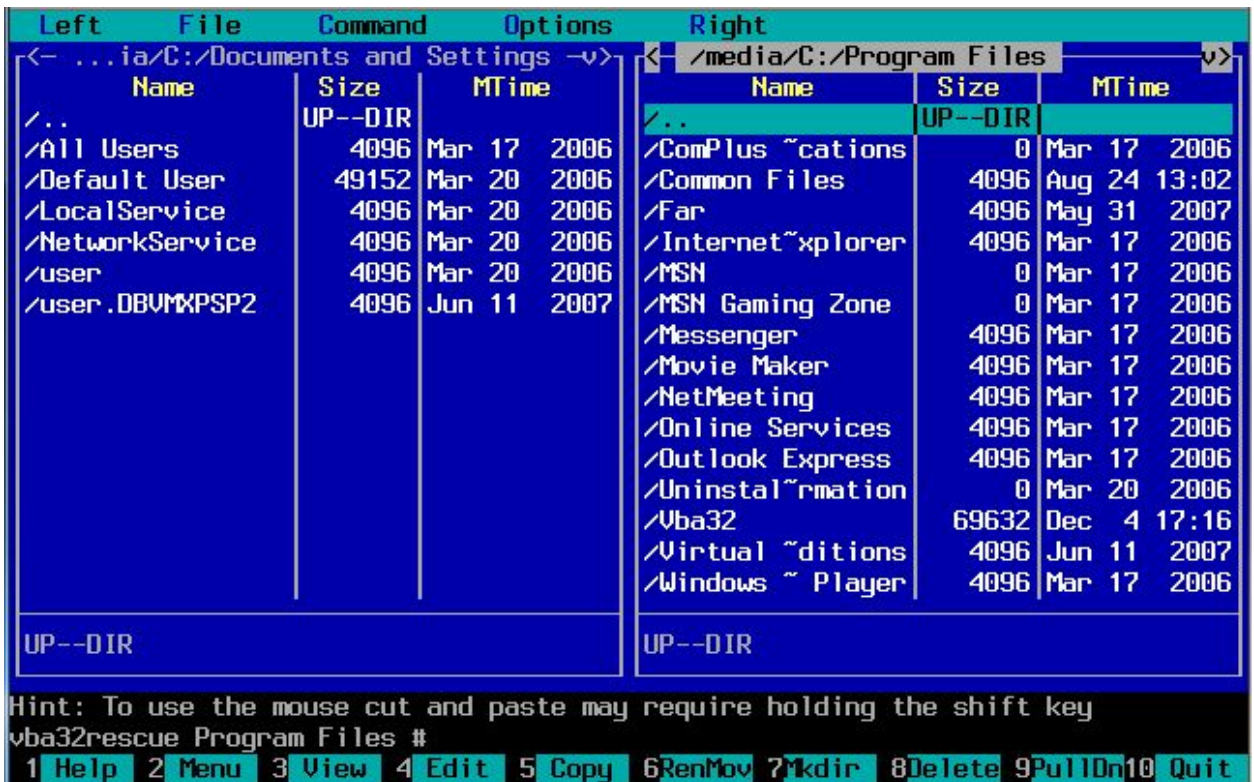
Project's home page: <http://www.invisible-island.net/dialog/dialog.html>.

## Midnight Commander

This allows to run **Midnight Commander**.

**Midnight Commander** is a file manager with text interface like Norton Commander for OS UNIX. File Manager provides an intuitive user interface and allows you to perform most common operations on files — create, view, edit, move, rename, copy, delete, etc..

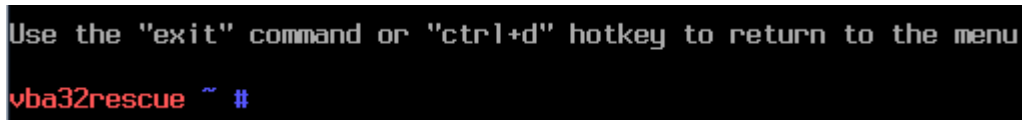
Project's home page: <http://www.midnight-commander.org>.



Picture 7 –Midnight Commander

## Shell

Menu item **Shell** is intended to enter the command shell **Vba32 Rescue**. After choosing this menu item the screen prompts to enter the **vba32rescue**.



Picture 8 – Shell

Using this mode, all the actions available through the user's menu are able to perform.

So, for example, call **Midnight Commander** is available from the following command:

```
mc
```

Rescue Image supports the ability to work in four command shells. Each of them is appropriated keys combination from **Alt + F1** to **Alt + F4**. The report about the work of Rescue Image is available in the fifth command shell. User Interface is available in the sixth command shell (**Alt + F6**).

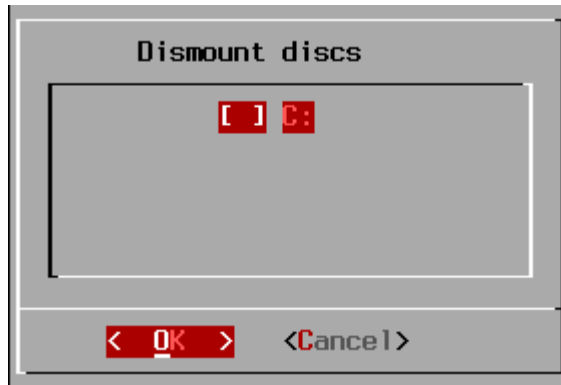
The work with console scanner **Vba32.CS.L** via command shell will be described in the chapter **Computer scanning**.

**Vba32.CS.L** console scanner update via command shell will be described in the chapter **Vba32.CS.L update**.

**Attention!** Working mode via command shell is designed for users confident in their knowledge. Using this mode is not recommended for unskilled users. For more stable and reliable work of software is recommended to work through the user interface menu.

## Dismount disks

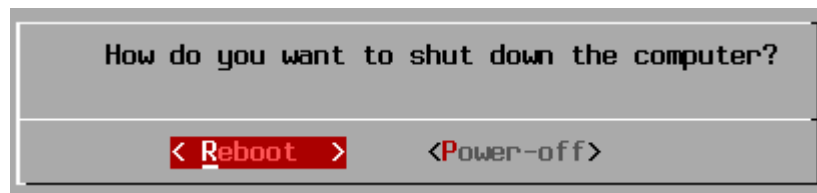
This item allows to dismount disks, mounted through **Vba32 Rescue** initialization, as well as USB-drive mounted to the system.



Picture 9 –Dismount disks window

## Shutdown

Using this menu item the computer can be powered off or reboot.



Picture 10 – Shutdown the computer

## About

This menu item displays the current version of **Vba32.CS.L** console scanner.



Picture 11 – Current version window

Information about the navigation keys, company contact information and thanks to those projects that have been used to create software.

VBA32 Rescue is supported by VirusBlokAda Ltd.

WWW: <http://www.anti-virus.by>

E-Mail: [support@anti-virus.by](mailto:support@anti-virus.by)

Tel.:

(+375 17) 226-85-55 - programming department

(+375 17) 226-62-85 - sales department

(+375 29) 623-63-23 - chief commercial officer

Thanks ...

Aufs <http://aufs.sourceforge.net/>

Bash <http://tiswww.case.edu/php/chet/bash/>

Bzip2 <http://www.bzip.org/>

55%



Picture 12 – About window

## Computer scanning

In this chapter will be considered the main task of **Vba32 Rescue** – scanning by **Vba32.CS.L** antivirus scanner. This scanner is a powerful facility, allows to detect and curing infected objects on the user's computer. The undoubted advantages of this scanner are:

- **powerful heuristic analyzer** – allows to detect unknown patterns of malware. Ability to select different working mode (from optimal to excessive) allows to aski required balance between quality of detection and quantity of false positives;
- **file viruses curing function** – gives the ability to deal qualitatively with the consequences of viral infections. Analysis of cure of such large-scale infections as **Sality (Sector)** and **Virut** proved the validity of this method;
- **Vba32 software code emulator** – allows to detect malware, processed as already known such as unknown difficulty analysis program of malicious code (cryptors, packers, obfuscators). This is achieved through continuous improvements of emulator, rather than the addition, became known, algorithms for static extraction;
- **just-in-time technology** – allows to speed up emulation of processed files;
- **daily updates of antivirus bases** - allows to reduce the threats impact on the user's computer;
- **supports of all common archive formats**, mail databases and other data formats.

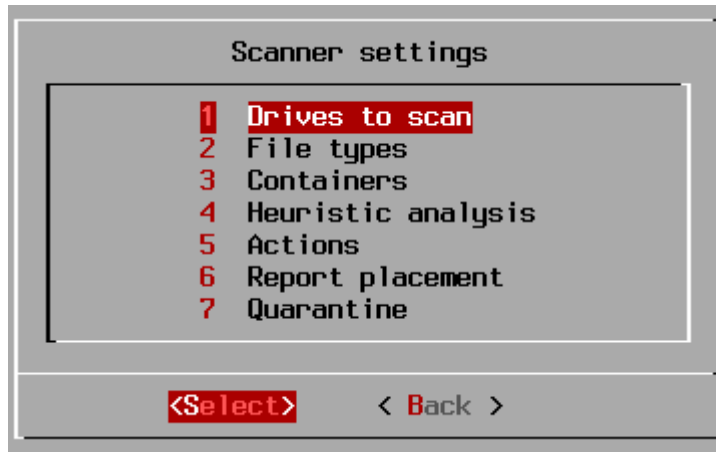
Then scanner settings are described, scanning process and console scanner keys to run via command shell.

**Attention!** Before running the scanner make sure that current version of the product is used. If Rescue Image is used with outdated databases, it is recommended to update or download new one.

**Attention!** Optimal settings for scan / cure are set in the product by default. It isn't recommended to modify them by unskilled users.

## Scanner settings

Menu item **Scanner settings** allows to configure the scanner settings used by **Vba32.CS.L** scanner.



Picture 13 –Scanner settings

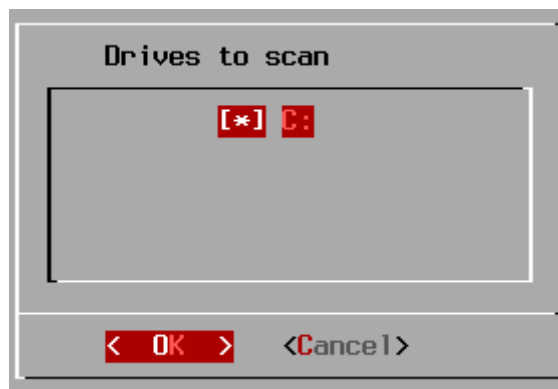
Conditionally, settings can be divided into three groups:

- **scanning objects settings;**
- **interface settings;**
- **action settings.**

### Scanning objects settings

Scanning objects setting is produced via following menu items:

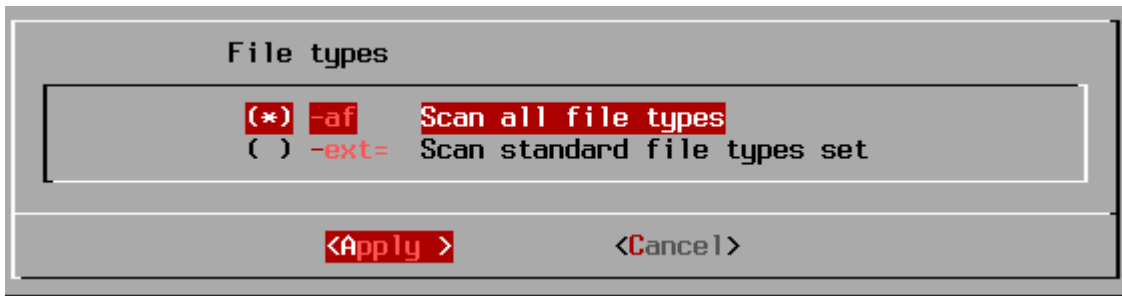
- **Drives to scan** – sets disks, which will be checked by antivirus scanner.



Picture 14 – Drives to scan window

By default, all logical drives, which could be detect and mount, are scanned;

- **Files types** – sets lists of file extensions, which will be checked by antivirus scanner.

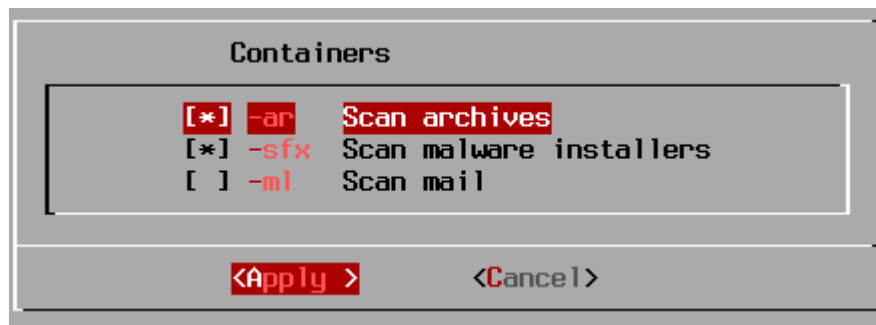


Picture 15 – File types window

All the file types (**Scan all file types**) are scanned by default. The setting **Scan standard file types** can be used to reduce the scan time. This operation checks only files with following extensions:

*.COM.EXE.DLL.DRV.SYS.OV?.VXD.SCR.CPL.OCX.BPL.AX.PIF.DO?.XL?.HLP.RTF.WI?.WZ?  
 .MSI.MSC.HT\*.VB\*.JS.JSE.ASP\*.CGI.PHP\*.\*HTML.BAT.CMD.EML.MSG.NWS.XML.MSO  
 .WPS.PPT.PUB.JPG.JPEG.INF.PDF.SWF.ARJ.AO?.RAR.RO?.ZIP.HA.GZ.TGZ.TAR.BZ2.CHM  
 .DBX.TBB.MBX.PST*

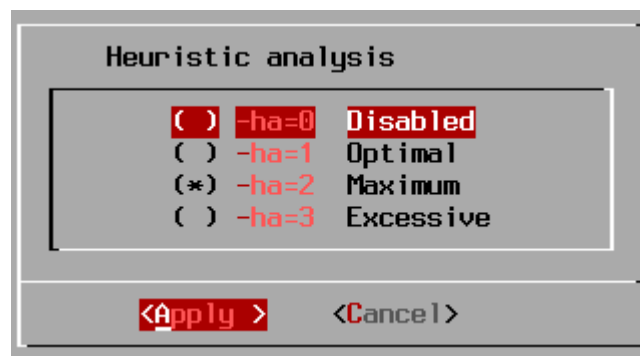
- **Containers** - specifies the need to scan the archives (**Scan archives**), mail databases (**Scan mail**), malware installers (**Scan malware installers**).



Picture 16 – Containers window

**Scan archives** and **Scan malware installers** are enabled by default.

- **Heuristic analysis** – specifies the mode of heuristic analysis (**Disabled**, **Optimal**, **Maximum**, **Excessive**).



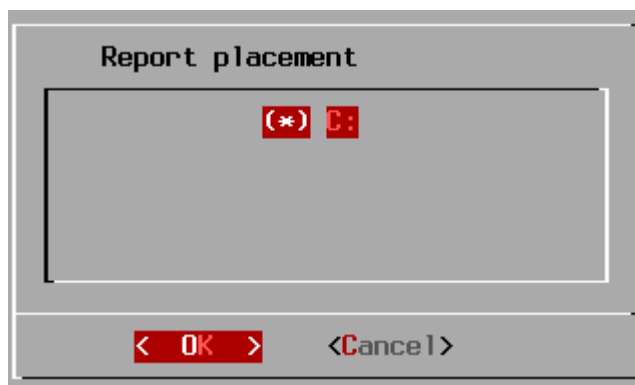
Picture 17 – Heuristic analysis window

**Maximum** mode is specified by default.

## Interface settings

Interface setting is produced through the next menu item:

- **Report placement** – specifies disk, on which would be created folder VBARESCUE. In this folder will be kept report file vba32.rpt and Quarantine. The first partition is specified as a default disk.



Picture 18 – Report placement window

## Action settings

Setting of actions upon objects is produced via menu item:

- **Actions**– specifies actions upon infected and suspected objects.



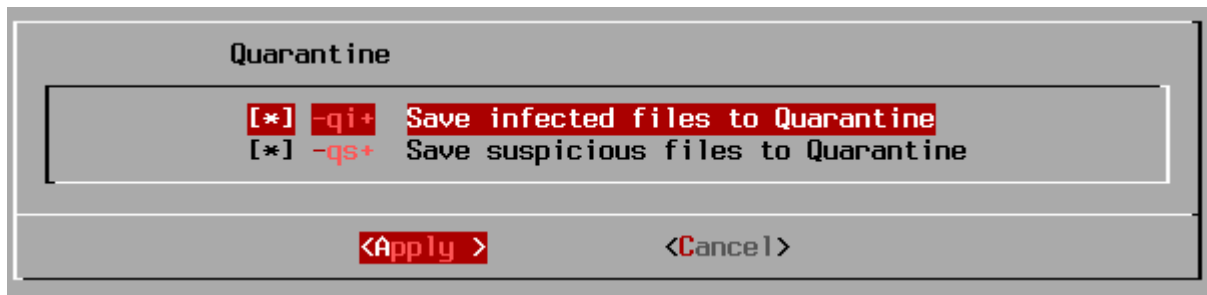
Picture 19 – Actions window

Keys **Cure infected files** and **Delete infected files** are specified by default.

**Note.** When settings **Cure infected files** and **Delete infected files** are combined, deletion of infected files will occur only if it is impossible to cure them. Thus, the file viruses will be cured, and trojans will be deleted.

The following options can be also controlled: **Delete suspicious files**, **Delete archives containing viruses**, **Delete messages containing viruses**;

- **Quarantine** - control the ability to save infected (**Save infected files to Quarantine**) and suspicious objects (**Save suspicious files to Quarantine**). Both options are specified by default.



**Picture 20 – Quarantine window**

Infected and suspicious files will be copied to Quarantine with saving way to the source file.

**Note.** The folder VBARESCUE is named Quarantine. This folder is created according to settings of menu item **Report placement**.

**Attention!** Files in **Vba32 Rescue** Quarantine don't modify. Launching Quarantine files could lead to further infection of computer.

## Scanning process

Scanning process starts at option of menu item **Start scan**.

```
/mnt/sda1/Awork/20080920/Virus.Sality...EXE : infected Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...virus is cured Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...nfo/OFFPRV10.EXE : backup copy created
/mnt/sda1/Awork/20080920/Virus.Sality...exe : infected Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...virus is cured Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...n/SrchAdmStp.exe : backup copy created
/mnt/sda1/Awork/20080920/Virus.Sality...EXE : infected Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...virus is cured Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality.../Office10/DW.EXE : backup copy created
/mnt/sda1/Awork/20080920/Virus.Sality...exe : infected Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...virus is cured Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...a/DeviceInst.exe : backup copy created
/mnt/sda1/Awork/20080920/Virus.Sality...exe : infected Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...virus is cured Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...F9730}/setup.exe : backup copy created
/mnt/sda1/Awork/20080920/Virus.Sality...exe : infected Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...virus is cured Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...gent/klmover.exe : backup copy created
/mnt/sda1/Awork/20080920/Virus.Sality...exe : infected Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...virus is cured Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...ent/klmagchk.exe : backup copy created
/mnt/sda1/Awork/20080920/Virus.Sality...exe : infected Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...virus is cured Virus.Win32.Sality.baka
/mnt/sda1/Awork/20080920/Virus.Sality...iveSync/astu.exe : backup copy created
/mnt/sda1/Awork/20080920/Virus.Sality...iles/Microsoft ActiveSync/CEAPPMGR.EXE :
```

Picture 21 –Scanning results

## Launching Vba32.CS.L in manual mode

**Vba32 Rescue** Image is the ability to work with **Vba32.CS.L** console scanner via command shell. There is a command for this:

```
/opt/vba/vba32l [path] ... [path] [-key] ... [-key]
```

Full keys list is provided upon commands:

```
/opt/vba/vba32l -?
```

```
/opt/vba/vba32l -H
```

```
/opt/vba/vba32l -HELP
```

Keys should be separated from each other by space symbol and premised by hyphen symbol «-». Keys can be written as in upper case such as in lower case. Paths are separated from keys by space symbol.

Below there is a keys list available to console scanner:

@filename	- scan files from filelist;
key	- specify program options;
-?[+ -]	- show help screen;
-H[+ -]	- show help screen;
-HELP[+ -]	- show help screen;
-M=1	- fast scanning mode;
-M=2	- optimal scanning mode (/AF+);
-M=3	- excessive scanning mode (/AF+ /PM+);

<i>-AF[+ -]</i>	<i>- all files;</i>
<i>-SL[+ -]</i>	<i>- follow symbol links;</i>
<i>-PM[+ -]</i>	<i>- excessive search;</i>
<i>-CH[+ -]</i>	<i>- enable cache while scanning objects;</i>
<i>-FC[+ -]</i>	<i>- cure infected files;</i>
<i>-FD[+ -]</i>	<i>- delete infected files;</i>
<i>-FR[+ -]</i>	<i>- rename infected files;</i>
<i>-FM+[directory]</i>	<i>- move infected files to specified directory (by default /var/virus);</i>
<i>-SD[+ -]</i>	<i>- delete suspicious files;</i>
<i>-SR[+ -]</i>	<i>- rename suspicious files;</i>
<i>-SM+[ directory]</i>	<i>- move infected files to specified directory (by default /var/virus);</i>
<i>-HA=[0 1 2 3]</i>	<i>- heuristic analysis level (0 - disable, 2 - maximum);</i>
<i>-D=[N,][filename]</i>	<i>- launch program once in N days (by default 1);</i>
<i>-QI+[directory] -]</i>	<i>- move to Quarantine infected objects;</i>
<i>-QS+[directory] -]</i>	<i>- move to Quarantine suspicious objects;</i>
<i>-R=[ filename]</i>	<i>- save report to file (by default VBA32.RPT);</i>
<i>-R+[ filename]</i>	<i>- append report to file (by default VBA32.RPT);</i>
<i>-L=[ filename]</i>	<i>- save list of infected files to file (VBA32.LST);</i>
<i>-L+[ filename]</i>	<i>- append list of infected files to file (VBA32.LST);</i>
<i>-QU[+ -]</i>	<i>- interrupt launching program (by default disabled);</i>
<i>-OK[+ -]</i>	<i>- include "clean" filenames in report;</i>
<i>-AR[+ -]</i>	<i>- include scanning files in archives;</i>
<i>-AL=[ file_size,kB]</i>	<i>- don't scan archives larger than specified;</i>
<i>-AD[+ -]</i>	<i>- delete archives containing infected files;</i>
<i>-SFX[+ -]</i>	<i>- detect malware installers;</i>
<i>-ML[+ -]</i>	<i>- mail scanning;</i>
<i>-MD[+ -]</i>	<i>- delete messages containing infected files;</i>
<i>-VL[+ -]</i>	<i>- view list of viruses known to program;</i>
<i>-VM[+ -]</i>	<i>- show macros information in documents;</i>
<i>-SI[+ -]</i>	<i>- additional information about program support;</i>
<i>-LNG= suffix</i>	<i>- select language file VBA32&lt;suffix&gt;.LNG;</i>
<i>-KF={ directory path }</i>	<i>- specify path to key file;</i>
<i>-EXT=</i>	<i>- specify list of scanning file extensions;</i>
<i>-EXT+</i>	<i>- add file extensions to default list;</i>
<i>-EXT-</i>	<i>- remove file extensions from default list;</i>
<i>-WK[+ -]</i>	<i>- wait for pressing any key for finishing;</i>

*The following settings are active by default: -QU -RW*

By default, the console scanner launches via user's interface with the following keys:

*-WK+ -FC+ -FD+ -AF+ -AR+ -CH- -RW+ -SFX+ -HA=2 -LNG="ru"*

*-R+"/media/C:/VBARESCUE/vba32.rpt" -QI+"/media/C:/VBARESCUE"*

*-QS+"/media/C:/VBARESCUE"*

If it is necessary for user to scan, for example, directory C:\Windows with the same settings, with which it is done in the user interface by default, enter the following command in a single line:

```
/opt/vba/vba32l "/media/C:/Windows" -WK+ -FC+ -FD+ -AF+ -AR+ -CH- -RW+ -SFX+  
-HA=2 -LNG="ru" -R+"/media/C:/VBARESCUE/vba32.rpt" -QI+"/media/C:/VBARESCUE"  
-QS+"/media/C:/VBARESCUE"
```

**Attention!** To avoid errors, use the scanner via menu of user interface is priority.

## Vba32.CS.L update

Update antivirus scanner allows to support **Vba32 Rescue** Image in actual state. This ability is available in both modes (**vba32rescue** and **vba32rescue2ram**) of software.

Updating antivirus scanner is able over Ethernet via FTP, HTTP using a proxy authorization and without it. The path <http://anti-virus.by/update/> is showed as updating source by default. But there is ability to change updating path by specifying another source in Internet or in local net work.

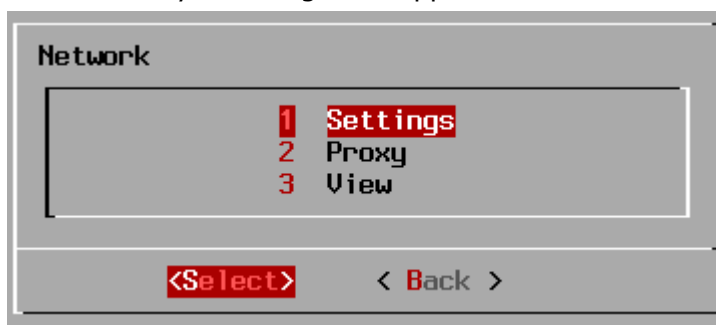
**Note.** «**VirusBlokAda**» give an opportunity of unwinding internal update server in local network. For this it is necessary to take advantage of free software **Vba32 Update Center**. To have the opportunity to update **Vba32 Rescue** from local network, on the tab **Complectation** in **Update Center** setting, it is necessary to flag **Vba32 Command-Line Scanner for Linux**.

**Vba32 Rescue** also allows to save updated Image on USB-drive. Settings of menu item **Network** are described below, menu item **Update scanner**, update process in manual and automatic modes and process of saving updated image to the USB-drive.

### Network

Menu item **Network** is design to get access to network settings.

The first time of the selection of this menu item working modules are initialized with network environment. The ability to configure it appears after this.



Picture 22 – Network window

Menu item **Settings** is design for this. The network setting is available via DHCP (if there is its support in the network) in automatic mode, or in manual mode.

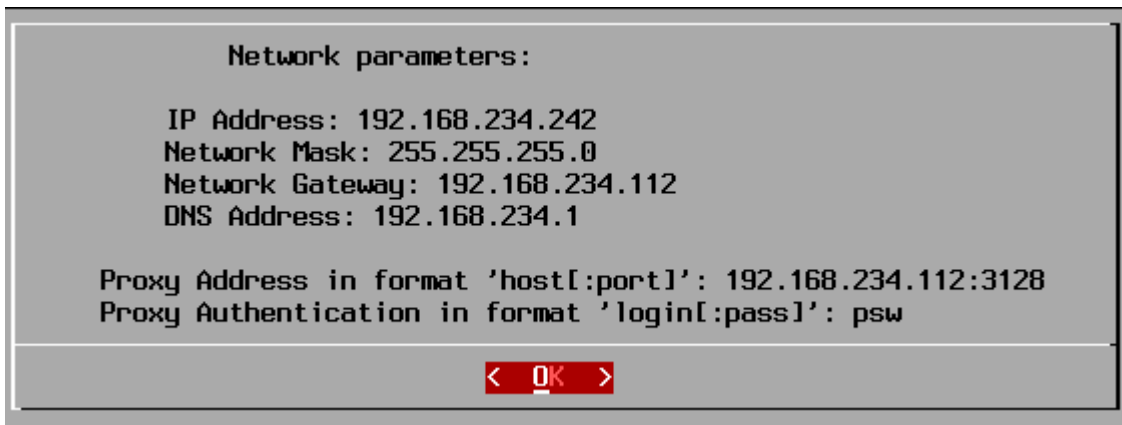


Picture 23 – Automatic network settings window

In manual mode it is necessary to specify computer's IP-address, subnetwork mask, gateway IP-address, DNS-server IP-address.

Menu item **Proxy** allows to specify proxy address in host[:port] format and proxy authorization in login:[password] format. If authorization is not necessary, it is offered to leave this field blank.

With the help of **View** menu item, the network environment configuration can be viewed.



**Picture 24 – Network configuration window**

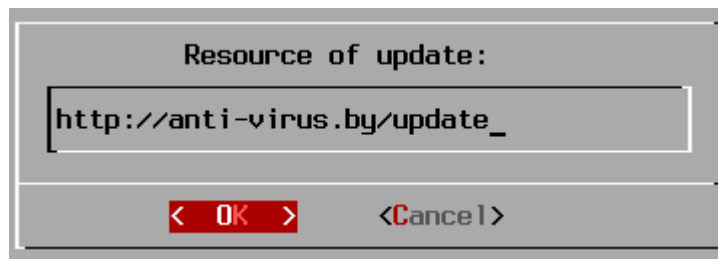
## Update scanner

**Vba32.CS.L** antivirus scanner update is able in two modes: automatic (via menu items of user interface) and manual (via command shell).

### Automatic update

The update is available via menu item **Update scanner**.

After selecting this item it will be offered to update from specified resource, or specify yours.



**Picture 25 – Update resource window**

After this the updating process begins.

```
Current dir is /opt/vba/
Start update from http://anti-virus.by/update
Receiving file list
File list received
Download from 'http://anti-virus.by/update'
Downloading 2 file(s) (3419.33 Kb)
Downloading file win32.udb
```

**Picture 26 – Results of update window**

**Note.** All information about updating process is saved to vba32.rpt log file and can be analyzed by the user later or sent to a Technical Support.

## Update via command shell

To update console scanner via command shell following command should be used:

`/opt/vba/vbaupdx <update path> <options>`

options:        -p=<address:port>                        - Proxy address and port;  
                 -r=[file]                                - Save the report to file;

<code>-r+[file]</code>	- Add the report to file;
<code>-u=&lt;username:password&gt;</code>	- Proxy-authorization;
<code>-no-ntlm</code>	- Disable NTLM support;

## Saving updated scanner to USB-drive

**Vba32 Rescue** Image gives the opportunity to save updated scanner to drive. So, the user can maintain the image up to date permanently. For example, user needs to update image on bootable USB-drive. For this:

1. Boot from USB-drive to **vba32rescue2ram** mode;
2. Configure network environment via menu **Network**;
3. Update **Vba32.CS.L** console scanner via menu item **Update scanner**;
4. Record updated image to USB-drive via menu item **Create bootable drive**.

As a result, the image just re-records to the same drive from which it was booted.

Each of the above items is described in the relevant chapter of this guide.

# Appreciations

«**VirusBlokAda**» thanks following projects used in the development of **Vba32 Rescue** Image:

Aufs	<a href="http://aufs.sourceforge.net/">http://aufs.sourceforge.net/</a>
Bash	<a href="http://tiswww.case.edu/php/chet/bash/">http://tiswww.case.edu/php/chet/bash/</a>
Bzip2	<a href="http://www.bzip.org/">http://www.bzip.org/</a>
BusyBox	<a href="http://www.busybox.net/">http://www.busybox.net/</a>
Dialog	<a href="http://invisible-island.net/dialog/">http://invisible-island.net/dialog/</a>
E2fsprogs	<a href="http://e2fsprogs.sourceforge.net/">http://e2fsprogs.sourceforge.net/</a>
Expat	<a href="http://expat.sourceforge.net/">http://expat.sourceforge.net/</a>
Gentoo Linux	<a href="http://www.gentoo.org/">http://www.gentoo.org/</a>
Gettext	<a href="http://www.gnu.org/software/gettext/">http://www.gnu.org/software/gettext/</a>
Glib	<a href="http://www.gtk.org/">http://www.gtk.org/</a>
Glibc	<a href="http://www.gnu.org/software/libc/">http://www.gnu.org/software/libc/</a>
GRUB	<a href="http://www.gnu.org/software/grub/">http://www.gnu.org/software/grub/</a>
Libxml2	<a href="http://www.xmlsoft.org/">http://www.xmlsoft.org/</a>
Linux Kernel	<a href="http://www.kernel.org/">http://www.kernel.org/</a>
Memtest86+	<a href="http://www.memtest.org/">http://www.memtest.org/</a>
Midnight Commander	<a href="http://www.midnight-commander.org/">http://www.midnight-commander.org/</a>
MHDD	<a href="http://www.ihdd.ru/">http://www.ihdd.ru/</a>
Ncurses	<a href="http://www.gnu.org/software/ncurses/">http://www.gnu.org/software/ncurses/</a>
Ntfs-3g	<a href="http://www.ntfs-3g.org/">http://www.ntfs-3g.org/</a>
Squashfs	<a href="http://squashfs.sourceforge.net/">http://squashfs.sourceforge.net/</a>
Timezone Data	<a href="ftp://elsie.nci.nih.gov/pub/">ftp://elsie.nci.nih.gov/pub/</a>
uClibc	<a href="http://www.uclibc.org/">http://www.uclibc.org/</a>
Zen Kernel	<a href="http://zen-kernel.org">http://zen-kernel.org</a>
Zip	<a href="http://www.info-zip.org/">http://www.info-zip.org/</a>
Zlib	<a href="http://www.zlib.net/">http://www.zlib.net/</a>

Also we would like to thank all beta testers who took part in the product testing.

