Targets Tag

This Tab permits you to specify the objects to be scanned and conditions of the search for anomalies.

In the upper portion of the Tab there is the *Disk drives* window. This allows selection of the disks to be scanned. After entering the window, the cursor may be moved using the direction keys. To select or unselect disk devices, utilize the space bar or double click the left button of your mouse. The window is divided into three columns:

- *Disk* - shows the disk icon and name
- *Type* - describes the disk type
- *Connected to* - shows the disk network name

On the right of the *Disk drives* window there are two check boxes.

- *Local* – selects or unselects only local hard drives
- *Network* – selects or unselects only network drives

Located below these check boxes are two buttons:

- *All* – selects all drives
- *Unselect* - unselects all drives

In the *Directories* window, located in the bottom section of the Tab, a list of individually selected directories to be checked for virus infection is displayed. The list can be edited using two buttons in the right part as follows:

- *Add* – opens the dialog window used to add new directories
- *Remove* – removes selected directory from the list

Log Tag

The main component of this Tag is the *Scanning log* window. The results of the scanning are reported in this Log. Important information on the status of the scanning and its progress are included in this log and are available in a file (with default name: ”Nod32.log”) after the program has finished.

The *scroll log* check box is located in the lower left-hand corner of the Tab. If the *scroll* box is checked, each new log entry is displayed in the lower portion of the window and the older entries scroll upward, otherwise, no scrolling occurs. However, regardless of the actual setting of the scroll box, any part of the *log* can be inspected by using the scroll arrows on the right-hand side of the window.

Entries in the log are distinguished by color. Information on uninfected objects is indicated in the color black, objects infected with viruses are indicated in the red color, and errors in access to the objects are indicated in blue. Cleaned, deleted and renamed files are indicated by the brown color.

On the bottom right side of the Tab the program version number is displayed.

Actions Tag

This Tab serves to specify the program action after a virus was detected.

The Tab contains two separate sections: *Files* and *Boot or MBR sectors*.

On the left side of the *Files* section, there is a switch named *On virus detection*. It contains the following options:

The left part of the *Files* section contains the *On virus detection* switch. The available options are as follows:

- *clean* - cleans infected files automatically
- *offer an action* – displays a panel suggesting an action based upon the actual needs
- *leave unchanged* – leaves the file without making any changes
- *rename* – renames all infected files
- *delete* – deletes all infected files

The *Uncleanable viruses* switch, located on the right side, displays the same options as are those described above, except for, obviously, the *clean* option. These items are applicable when NOD is unable to heal an infected file. This switch is accessible only while the automatic cleaning option is selected.

The *Boot or MBR sectors* section, located in the bottom of the Tab contains similar switches as the upper sections. However, the *rename* and *delete* options are now substituted by a single option:

- *replace* - replaces the viral code in the boot sector by a clean standard code

Network Tag

This Tab serves to set the program parameters effective in a computer network and the parameters of the Centralized Update.
It consists of three sections described below:

In the upper portion of the *Network messages* section, there is a check box *Send Message about virus infiltration over the network*. If selected, and a virus is detected by NOD32, a message is sent to pre-defined users. The list of these users is displayed in the window below the check box.

To add new recipients of the messages, press the button *Add*. The name of the computer or group of computers is entered in the dialogue box, which appears after pressing the button. If an asterisk in entered in place of a name, the messages will be mailed to all members of a group of whom the particular user is a member.

To remove particular entries from the list, move the cursor to the entry, highlight it by clicking the mouse button, and press the delete (DEL) key on the keyboard or, press the *Remove* button.

The mailing option can be immediately tested by pressing the *Test* button.

The contents of the message is entered into the *Message layout* dialogue box. Required contents of the message is entered into this field and the location where the name of the detected virus is to appear is indicated by a string <*virus*> as can be seen in the original field contents.

Warning: When operating system Windows®95 (98) is used, the *Winpopup* program (a standard part of the operating system) must be running on those computers which have been selected to receive messages. In the case of massive infiltrations detected by NOD32, only the message on the first virus is sent in order to avoid potential overload of the system caused by a potentially prohibitive volume of the messages.

The button *Change* is located in the section *Directory for Update File.* Pressing this button opens the dialog window where the information with full path to the directory containing (or which will contain) the files of the centralized Update is stored. If applicable, the automatic update is performed upon the following restart of the computer.

Entry into this Tab can be password protected. To do this, select *the Protect Tab with Password* check box and define the password after pressing the button *Password*.

Setup Tag

This Tab is used to set the basic operational parameters of the program. It contains one separate button and six sections with a multitude of options described below.

The section *Diagnostics Targets* contains three check boxes:
- *Files* – enables scanning of executable files and files containing macros
- *Boot sectors* – enables scanning of boot sectors of logical disks
- *MBR sectors* – enables scanning of the main boot sector of the disk

The section *Heuristic sensitivity* contains a switch with the following options:
- *Safe* – analysis with minimum false alarms
- *Standard* – option for balanced detection
- *Deep* – enables maximum depth of sensitivity

In the *Diagnostics methods* section four check boxes are available:
- *Signatures* – enables detection of specific virus code sequences
- *Heuristics* – enables heuristic code analysis
- *Runtime packers* – checks for virus presence also inside the files compressed by a ”runtime” packer (such as PKLite, LZExe, Diet etc.)
- *Archives* – searches viruses also in compressed archive files (e.g. ZIP, ARJ etc.)

The *Log* section contains several elements. In the upper part, there are two check boxes:
- *Enabled* – enables saving the log file on disk
- *Wrap log* – formats a line in a log file with up to 60 characters per line

Below the check boxes, there is a switch controlling the attributes of the log file:
- *Append* – new log shall attached to the end of the old one (if it exists)
- *Overwrite* – the old log file is always replaced by the new one

Finally, there are two entry fields in the *Log* section:
- *Maximum length* – specifies maximum size of the log file in kB
- *Name* – a new log name may be defined in this field if the change of default name “Nod32.log” is desired

The *System* section contains two check boxes:
- *List all files* – the list of all scanned files will appear in the log file, including uninfected files
- *Sound signal* – turns on the sound signal upon virus detection

The *Configuration* section contains three buttons:
- *Save* – saves actual configuration
- *Load* – reads saved configuration
- *Default* – sets the default configuration

In the bottom right hand corner of the Tab, there is a separate *Extensions* button, which permits editing of the filenames extensions to be scanned.

Contact

ESET, LLC
4025 Camino del Rio South
Suite 300
San Diego, CA 92108
Phone: (619) 542-7872
Fax: (619) 542-7701
E-mail: eset@nod32.com
www.nod32.com

Add directory panel

In the upper part of the panel, there is an entry field where the path of the new directory to be added to the list may be entered.

There are three buttons in the bottom part of the panel:

- *OK* – adds specified directory to the list
- *Cancel* – cancels the panel without any changes in the list
- *Browse* – invokes standard system directory selection process to select the directory from available directories on the disk

About the program

NOD32

Extension Editor

Extension editor serves as a tool to define the extensions of the files to be scanned for virus infiltrations.

The current list of the extensions in alphabetical order is displayed in the left-hand side of the window.

The five buttons on the right hand side offer the following functions:
- *OK* – finishes editing of the extensions and records the actual listing of the extensions
- *Cancel* – finishes editing without any changes in the list of extensions
- *Add* – adds the extension from the entry field to the list of extensions in the window
- *Delete* – removes from the list the extension marked by the cursor
- *Default* – cancels the actual list of extensions and replaces it with the default

The check box: *Scan all files* is located in the bottom part of the window. If this check box is selected every file is scanned regardless of its extension. In this case the list of the extensions and the *Add* and *Remove* buttons are not accessible. Selection of this option is not recommended in standard situations.

To add a new extension press the button *Add*. This opens a new window with an entry field where the new extension (maximum 10 characters long) is to be typed. Press the *OK* button to file the extension into the list of the tested extensions.

The current list of the extensions of the tested files is saved after the button *Save* located in the *Setup* Tab is pressed.

Virus detected Panel

Upper part of the panel shows scrollable window with information about the file with virus found. Additional information is displayed such as the name, characteristics of the virus and an information whether the virus can be cleaned using this program.

The *File with virus* section contains four buttons:

- *Leave* – to leave file without any changes
- *Clean* – to activate virus cleaning
- *Rename* – renames the file with virus to prevent unforeseen launching
- *Delete* – deletes infected file

In case of boot virus infiltration the name of the section changes to *Boot sector with virus* and contains only three buttons:

- *Leave* – to leave boot sector without any changes
- *Clean* – to activate virus cleaning
- *Replace* – replaces infected boot sector with standard boot code

The *Actions for next infected files* (or *boot sectors*) section contains the button *Setup*, displaying the *Setup* tag. This button is used to set certain uniform action for all subsequent viruses.

Lower part of the panel contains one button:

- *Terminate detection* – immediately terminates scanning of viruses

Centralized Update

This function is primarily meant to facilitate the network administrators to update the anti-virus system. To enable this function, it is necessary to allow the option of A*utomatic Update* for a particular workstation during the installation of NOD32.

If it is not clear whether the function of *Centralized Update* is to be used, it need not be selected. This option may be set whenever the user deems it necessary. To do this, run the installation program and press the button *Change* in the section *Directory for Update File* located in the *Network* Tab, and set the path to the directory accessible to all users.

The network administrator installs a special Update file, available from ESET, into this directory. Whenever the workstation is booted, the NOD system verifies the version of the Update file and always utilizes the most recent one to update all necessary files. The updated program version runs only after the subsequent restart of the system.

Contents