Main window

This is the main control and information window of AMON – the resident Anti-virus MONitor program. AMON is in charge of constant and automatic detection of virus threats regardless of their source (a floppy disk, internet, etc.).

The pulsing NOD logo in the upper left corner of the window indicates that the program is in its default mode. In this mode, all objects (a floppy disk boot sector or a file) are automatically tested/scanned for a virus infiltration.

Clicking on the pulsing logo sets the second program mode. As one would expect, no scanning is carried out in this regime and, in addition, the logo becomes "frozen". To return to the active scanning mode and safety-proclaiming pulsing logo, double click on the logo area again.

The scanning-disabled mode is designed for specific purposes and critical, rarely occurring situations. Therefore, the active scanning mode is set automatically after system start-up.

The right side of the main window contains a set of four buttons with the following functions:

- *Hide* - hides the *main window* leaving the program running
- *Setup* - displays the *setup window*
- *Uninstall* - terminates the program
- *Help* - opens the help window

Finally, valuable information on:

- Number of tested files
- Number of infected files
- Number of cleaned files
- Name of the last tested file
- Program version

is listed in the lower left information window.

Targets Tag

The Targets tag allows you to specify the objects to be scanned (type of the file, media, boot sector, etc.) and conditions under which the scanning will be performed.

The tag is comprised of two sections: the *Files* and *Scan boot sectors on* sections.

The Files section itself contains three groups of check boxes and one button. The first group contains the following check boxes:

- *Executables* – executable files (COM, EXE, DLL, VXD, BAT, ...) will be scanned
- *Documents* – documents and worksheets which can contain macros will be scanned

In the *Scan on* group it is possible to specify scanning of files on:

- *Open*
- *Rename*
- *Execute*
- *Create*

The *Media* group enables more detailed specification of disk drives to be scanned:

- *Floppies*
- *Local* – all fixed and removable disk drives with the exception of floppies
- *Network* – remote disks shared over the network

The *Extensions* button shows the editor of scanned files extension list.

The *Check boot sectors on* section is used to specify events when scanning of the floppy boot sectors will be performed. The following options are available:

- *access* – the test will be performed at the time of first access to a newly inserted floppy
- *shutdown* – the test will be performed at the time of shut-down

Methods Tag

This window allows you to select the scanning method and the depth of the Heuristic analysis – one of the strongest tools NOD32 brings you.

The Methods group, located in the upper part of the windows, contains two check boxes: Signatures and Heuristics.

- *Signatures* - enables identification of particular viruses based on their "signatures" , i.e. specific virus code sequences
- *Heuristics* - enables heuristic analysis (based on the virus behavior) of the code

Below the Method group, the depth of the heuristics analysis can be selected within the Heuristic analysis switch. In general, the deeper the heuristic analysis, the longer it takes to perform the scanning, but, at the same time, the safer the analysis is. The user can choose from three options:

- *Safe* - minimizes false alarms
- *Standard* - option for balanced detection
- *Deep* - provides maximal sensitivity

Actions Tag

This Tab serves to set the program parameters and actions upon virus detection.
It contains nine checkboxes divided into three groups.

If the uppermost, *Display warning panel* checkbox is selected, a warning window appears upon virus detection, allowing the options of further actions. Otherwise, the program only automatically disables access to the infected file.

Upon selection of the second checkbox: *Try to clean automatically first*, the program attempts to clean every infected file without user's intervention. If cleaning is not successful a alert window is displayed, and/or access to the infected file is disabled depending on the selection of the previous checkbox.

Both sets of remaining checkboxes control the contents of the alert window. If displaying of the latter is not enabled these checkboxes are inaccessible.

The first set - *File viruses* checkboxes, specifies the program response to a file infection and allows the following buttons in alert window to be enabled:

- *Clean* – cleans the infected file
- *Rename* – renames the infected file
- *Delete* – deletes the infected file
- *Exclude* – includes the infected file into the list of files temporarily excluded from scanning

The second, *Boot viruses* set is used in case of a boot-sector infection and may cause the following buttons to appear in the alert window:

- *Clean* – cleans the boot record
- *Replace* - replaces the code in boot record with an appropriate standard code
- *Exclude* - excludes current floppy disc boot-sector from scanning

Exclude Tag

This tag is used to handle the list of files, directories and boot sectors excluded from scanning. It contains a window where the listed items appear. There are also four buttons below the list.

The window is divided into four columns with adjustable width. These columns are:

- *Name* - specifies the path to the item/object
- *Type* – shows the item type
- *Subdirectories* – if the item selected is a directory this column specifies whether its corresponding subdirectories are also excluded from scanning
- *Temporarily* – if "Yes" is displayed in this column, then exclusion of this item from scanning is applicable only until the next program execution, after which this item is deleted from the list.

Each column widths can be changed, if necessary, by pointing the mouse cursor at the line dividing two neighboring columns (which triggers a special mouse pointer), pressing the left mouse button and moving the pointer to the right, or to the left, in order to change the with.

The four buttons in the lower section have the following uses:

- *Add* - adds new item(s) to the list
- *Change* – changes item(s) in the list
- *Remove* - removes an item from the list
- *Default* – replaces current items with the default values

Network Tag

This Tab serves to set the parameters of the program for operation in a computer network and the parameters of the Centralized Update. It consists of the following two sections:

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 AMON, 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 is entered in place of a name, then the messages are mailed to the group members to which the current user belongs.

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 are entered into the *Message layout* dialogue box. Required contents of the message are 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.

Security Tag

The *Security* Tab is used to set the program security settings.
It is comprised of two sections.

In the Security section, password protection of some items can be set. There are two check boxes in the upper portion:

- *Disable un-install and turn-off of Amon* – disables the option of un-installing (or turn off) of the resident protection using a standard approach.
- *Do not show Amon icon in Taskbar* – if this check box is selected, the execution of Amon is not indicated on the Taskbar.

Warning: Redisplay of the icon on the Taskbar is achieved by executing the Amon program with the parameter /SHOWICON and new reboot of the system.

The set of check boxes below controls access to particular Tabs:

- *Targets*
- *Methods*
- *Actions*
- *Exclusion*
- *Network*
- *Security*

Checking any of the above listed check boxes prevents access to the *Security* Tab automatically.

There are two buttons in the lower portion of this section:

- *Password* – is used to enter a new password to access prohibited parts of the program.
- *Select all* – automatically selects all check boxes in this section.

The second (lower) section contains a check box *Automatic activation of Amon at the system startup*. If selected, the resident virus protection is activated automatically upon every system start-up.

Press the *Default Amon Configuration* button to set the default (manufacturer's) Amon configuration.

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

Adding Items to Exclusion List

The dialogue box in the upper portion of the panel serves to set the path to the object. There are four switch boxes underneath:

The switch box *Add to the list of* has the following positions:
- *permanently excluded* – makes exclusion of the object from scanning permanent
- *temporarily excluded* - excludes the object until the end of Amon program execution

The *Excluded Item* switch contains three options:
- *directory* - excludes the whole directory
- *file* - excludes only a single file
- *boot sector* - excludes from scanning the system areas of the disk

The *Exclude also subdirectories* switch permits two options:
- *no* - the subdirectories of an excluded object will be scanned
- *yes* - the subdirectories will also be excluded from scanning

The *Diskette boot sector* switch has two options:
- *A:* – the boot sector of the floppy inserted in the A: drive is excluded
- *B:* – the boot sector of the floppy inserted in the B: drive is excluded

The bottom portion contains four switches with the following functions:
- *OK* – current settings are confirmed and the object is added to the list
- *Cancel* – the operation is cancelled without adding the item to the list
- *Browse* – invokes a standard system dialog to select a directory from those available on the disk(s)
- *File* – triggers standard file selection process to select a file from those available on the disk(s)

Modifying Items in Exclusion List

The dialogue box in the upper portion of the panel serves to set the path to the object. There are four switch boxes underneath:

The switch box *Add to the list of* has the following positions:
- *permanently excluded* – makes exclusion of the object from scanning permanent
- *temporarily excluded* - excludes the object until the end of Amon program execution

The *Excluded Item* switch contains three options:
- *directory* - excludes the whole directory
- *file* - excludes only a single file
- *boot sector* - excludes from scanning the system areas of the disk

The *Exclude also subdirectories* switch permits two options:
- *no* - the subdirectories of an excluded object will be scanned
- *yes* - the subdirectories will also be excluded from scanning

The *Diskette boot sector* switch has two options:
- *A:* – the boot sector of the floppy inserted in the A: drive is excluded
- *B:* – the boot sector of the floppy inserted in the B: drive is excluded

The bottom portion contains four switches with the following functions:
- *OK* – current settings are confirmed and the object is added to the list
- *Cancel* – the operation is cancelled without adding the item to the list
- *Browse* – invokes a standard system dialog to select a directory from those available on the disk(s)
- *File* – triggers standard file selection process to select a file from those available on the disk(s)

Virus Alert Window

The window is displayed if the program detected a virus. Prior to displaying it Amon **DISABLES** access to the infected file so there is no need to worry about virus activation. The appearance of the window depends both on capabilities and settings of your graphical adapter.
There are two buttons in the left upper part:

- *Close* – closes the alert window (access to the infected file remains disabled)
- *Information* – displays information window with a short description of recommended action

Below, there is an area that contains whole path to the infected object and a type of virus detected. It also displays additional information about system activity when the virus was detected and whether Amon can clean this virus.

Below this area a checkbox with the *Display this alert window* text is displayed. It can be used under specific circumstances. If for example a program that opens hundreds of infected files is running and this program can not be interrupted you can temporarily disable displaying alert window to speed up program completion. The access to files remains disabled. The window displaying can be enabled again either in the *Actions* tag or after Amon is restarted.

In the right-hand part there is a group of four buttons:

- *Clean* – instructs the program to clean the virus (if Amon can not clean the virus this button is greyed out and can not be pressed)
- *Rename* – renames infected file to prevent later infection
- *Delete* - deletes infected file
- *Exclude* – in case of false alarm this button excludes the object from scanning

In case of boot sector infection the *Rename* button is missing and the *Change* button is substituted for the *Replace* button. After the button is pressed Amon replaces an infected code in the boot sector with a clean standard code.

Information Window

Displays additional information about what to do in case of a virus infiltration.

There are two buttons in the lower part:

- *Cancel* – closes information window
- *Export file* – creates a file containing a suspected object to be sent for analysis to the ESET LLC company.

About Amon

NOD - AMON

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.

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