How to Use InoculateIT PE

When you run the InoculateIT PE program, the initial window that appears will display both the Browser and the Reports windows.

When you select one of the menus a drop-down menu will display further options. A brief description of the menu options associated with the command or icon appears in the Status Bar (bottom left) of the InoculateIT PE screen.

These options explain the various activities associated with the use of these windows.

Introduction to the Browser window

Introduction to the Report window

How to set the defaults

InoculateIT PE Application Functions

Selected from the top left corner of window, this function offers the standard Windows commands **Restore**, **Move**, **Size**, **Minimize**, **Maximize** and **Close** (which has a Hot Key ALT F4).

Restore, **Minimize** and **Close** operate when the InoculateIT PE window is full size.   All the commands except **Restore** operate when the InoculateIT PE window is less than full size.

InoculateIT PE Installation Switches

These switches can be used when installing InoculateIT PE to a single machine.

/Back Setup will normally only proceed if the version information in the Setup directory indicates a later version than that installed in the local product directory. This command-line switch allows an older version to be re-installed. Hence, any version number difference will result in the installation proceeding.

/DiskCopy Some installation programs do not operate correctly or generate error messages when run directly from a floppy disk on some computers, but run perfectly well when the files on the diskette are copied to the hard disk and run from there. This switch causes the files on the floppy diskettes to be copied to a temporary directory on the computer's hard disk, and then calls the Installation Program from there. This switch is only available when running Setup from a floppy disk.

/IniFile=xxx When Setup starts up, it reads a number of parameters from an initialization file with the same base filename as the Setup program, but with an ".inf" file extension, *e.g.* if the Setup program filename was called "Setup.exe", then the initialization filename would be "Setup.inf". This switch allows you to explicitly specify an alternative initialization filename, including absolute path name.

/OSNoError If you try to run Setup on an operating system for which there are no instructions in the Setup initialization file, it will normally display a message on the screen. This switch stops that message from being displayed, and simply aborts silently.

/Update Causes Setup to be invoked in minor update mode (as opposed to major upgrade). By storing only the files that have been updated separately, the Installation Program can selectively update these files. The Configuration Wizard is not called for a minor update.

/Version Causes operating system version information to be displayed on the screen.

/WaitStart= When Setup is called on a hardware platform that supports 16-bit Windows, *i.e.* Intel-based computers, the entry-level Setup program is a 16-bit program. If this program detects that it is running on a 32-bit operating system, *e.g.* Windows 95 or Windows NT, it starts up the 32-bit Setup program and terminates, leaving only the 32-bit Setup program running. The "/WaitSatart=" switch will cause the 16-bit Setup program to wait for the 32-bit Setup program to complete before terminating. See below for more discussion about waiting for Setup to complete. This option is not available when running Setup from floppy disks.

Note: Setup always waits for the Installation Program to complete before starting up the Configuration Wizard.

Notes:

- The following options are not available when Setup is called from DOS (in MS-DOS mode, *i.e.* not a window under Windows 95, 98 or NT):

  "/DiskCopy", "/IniFile=xxx", "/Minor", "/WaitStart=".

Toolbar Buttons

The InoculateIT PE program uses standard Windows icons, buttons (*i.e. Minimize, Maximize, Cascade,* and *Close*), slider bars, and menu commands such as **File**, **Edit** and **Help**. Menu commands, icons and buttons specific to InoculateIT PE usage are explained below.

When you position the cursor above a toolbar button without selecting the button, a help text will appear in a small pop-up window beside the button.

Select the options below for information on:

Directory Tree View button

Move up button

Large Icon button

Small Icon button

List button

Details button

Change options

Go button

Stop button

The Tree View Button

This button allows you to enable/disable the tree view on the InoculateIT PE interface. We recommend you use it as it will give you more information as you scan files. This method of viewing the InoculateIT PE interface can also be toggled using the View | Tree view menu option.

The Move Up Button

Select this button to move to the parent directory of the directory currently displayed.

The Go Button

Select this button to scan the selected item(s) using InoculateIT PE. If no item(s) have been selected, then InoculateIT PE will prompt you to specify a path and then to try again. The results of the scan will be noted in the Report window and the second, third and fourth panels at the bottom of the InoculateIT PE window will note the number of files scanned, the number of scanned files found to be infected and the number of scanned files suspected of being infected.

The Stop Button

Select this button to stop the scanning process. The Report window will note that the operation was interrupted. The second, third and fourth panels at the bottom of the InoculateIT PE window will note the number of files scanned before the scan was interrupted, the number of scanned files found to be infected and the number of scanned files suspected of being infected.

The Large Icons Button

Select this button to display large icons in the Browser window. Either specific or generic icons may be displayed, depending on the file they refer to and the **All Icons** option under the View menu .

The Small Icons Button

Select this button to display small icons in the Browser window. Either specific or generic icons may be displayed, depending on the file they refer to and the All icons option under the View menu .

The List Button

Select this button to display the list of files, folders or drives in the Browser window. Either specific or generic icons may be displayed, depending on the file they refer to and the View menu .

The Details Button

Select this button to display the list of files, folders or drives in the Browser window along with their various details such as type, size, and date last modified.   Selecting the title of one of these details sorts the window according to that category of information. Selecting the same category again will reverse the order of details.

This option uses the small icons associated with each item. Either specific or generic icons may be displayed, depending on the file they refer to and the View menu

What the InoculateIT PE | Window menu does

To activate any menu item press both the <ALT> key and the first letter of the menu required. To select an option from the menu, press both <Shift> and the letter that is underlined in the option. (once the menu is displayed the arrow keys can be used to navigate to the selected menu option)

i.e. Select an item(s) with the mouse, press down both the <ALT> and <F> keys to activate the File menu, then both <Shift> and <V> to run the scan.

Select the options below for information on:

- File
- Edit
- View
- Options
- Tools
- Window
- Help

The File Menu

Go: Scans the selected item(s). If no item(s) have been selected, then InoculateIT PE will prompt you to specify a path and then to try again. The results of the scan will be noted in the Report window and the second, third and fourth panels at the bottom of the InoculateIT PE window will note the number of files scanned, the number of scanned files found to be infected and the number of scanned files suspected of being infected.

Stop: Stops the scanning process. The Report window will note that the operation was interrupted. The second, third and fourth panels at the bottom of the InoculateIT PE window will note the number of files scanned before the scan was interrupted, the number of scanned files found to be infected and the number of scanned files suspected of being infected.

Exit: Quits the InoculateIT PE application.

The Edit Menu

Copy: Standard Windows command (Ctrl C). This command can be used to cut sections of the log file for storage on the Clipboard. Such item(s) can be then pasted to a Word document.

Select All: Selects all files, folders or drives displayed in the Browser window if it is the active window. Selects all the text in the Report window if it is the active window.

Invert Selection: When the Browser screen is active this will invert the previous selection. That is, if one or more files, folders or drives were previously selected, this command will select the remaining files, folders or drives to the exclusion of those previously selected.

The View Menu

These options will alter the way the icons and information about files is presented in the browser window. The first four options are mutually exclusive. That is, selection of one will cancel the previous selection.

Large Icons: Displays large size icons in Browser window.

Small Icons: Displays small size icons in Browser window.

List: Displays list of files, folders or drives in Browser window.

Details: Displays details (e.g. Name, Size, Type, Date Last Modified, Total Size, Free Space) of files, folders or drives in Browser window.

Arrange Icons: Directory contents can be arranged by Name, Size, Type and Date of last modification. (Depending on the option **All icons** either specific or generic icons may be displayed.)

All icons: Switches the Browser display between generic and file specific icons.

Directory Tree: Enables the directory tree structure to be viewed or hidden.

Refresh: Cancels the selection of any item(s) in the Browser window. Also checks to see if there have been any changes to the items displayed in the Browse window (it will update the list if there have been any new files added, removed or any other changes made to the directory that is currently displayed).

The Options Menu

Program: Selecting this menu item opens the Program dialog, which allows changes to the default settings for every subsequent scan. Program dialog

Real-Time Protection: Selecting this item opens the Real-Time Protection dialog, which allows changes to the way the Real-Time protection operates Real-Time dialog

Alerting : Selecting this item opens the Alert Properties dialog, which can enable, disable and configure the sending of an Email message when a virus is detected.   See Alerting for further details.

Options Wizard: Selecting this item will run the configuration wizard. For further details on the Installation/Configuration wizard please select the on-line help button that is on each dialog of the wizard. Options Wizard

Password Protect Options: Password protection has been added to stop unauthorized alterations to your InoculateIT PE configuration. The password protection can be enabled by selecting Options | Password Protect Options and entering a password.

NOTE: The password that is entered is case dependent, so an "e" is not the same as an "E". The default password is IPE.

See Password protection for further details.

The Options Wizard

Please select the Wizard Option that you want more information on.

Scanning Options	For more information Click here
Scan File Types	For more information Click here
Program Virus Detection Actions	For more information Click here
Macro Virus Detection Action	For more information Click here
Reporting Options	For more information Click here
Boot Sector Scanning	For more information Click here
Memory Scanning (Windows 95/98 only)	For more information Click here
InoculateIT PE Start-up Options	For more information Click here
Progressive Scan	For more information Click here
An Index of all the Real-Time Protection options	For more information Click here
Real-Time Protection Components	For more information Click here
Real-Time Floppy Disk Boot Sector Protection	For more information Click here
Real-Time File Monitor Options	For more information Click here
Real-Time File Infection Actions	For more information Click here
Real-Time Macro Infection Actions	For more information Click here
Real-Time File Monitor Reporting	For more information Click here
Virus Alerting	For more information Click here
SMTP E-Mail Configuration	For more information Click here
Out-of-date Warning	For more information Click here

The Window Menu

Report: Selecting this option will activate the Report window.

Browser: Selecting this option will activate the Browser window.

Directory Tree: Enables the directory tree structure to be activated or deactivated.

The Help Menu

Help Topics: Accesses InoculateIT PE On-line Help

Virus Information: Accesses The Virus Encyclopedia. For a full list of the Viruses detected by this version of InoculateIT PE select Start | Programs | InoculateIT PE | Viruses Specifications or select VIRUSES.HLP from your InoculateIT PE directory.

About: This dialog will always contain the version number of your current copy of InoculateIT PE. Provided the name of the registered user, the name of the registered company and the InoculateIT PE customer number were entered during installation, these details will also be displayed in this box.

How to use the InoculateIT PE Browser Window

The InoculateIT PE Browser window can be used to view the contents of folders, directories, drives, and to select items for scanning.

To open (display the contents of) a folder, directory or drive that is in the Browser window, double-click on the item or click <Enter> if the item has already been highlighted.   If you do this on a file it will be scanned.

Press the "Level Up" toolbar button to move to the parent directory of the directory currently displayed.

How to select files in the browser window

How to start scanning the selected files

Virus Data File updates are available to update InoculateIT PE

You must then either get the Update Kit sent out to you   or download it from the website. To download it go to the InoculateIT PE website http://www.cai.com/antivirus/personal/updates, and follow the instructions form there.

Once the Setup program has been run:

The .DAT files will be copied to your InoculateIT PE directory. If you wish to update your Real-Time protection you will need to reboot your PC. Once it has been rebooted InoculateIT PE will be able to find automatically all of the latest macro viruses.

Selecting the File, Folder, Directory or Drive for Scanning

To select an item in the Browser for scanning, click it with the mouse.

Multiple items can be selected by using standard Windows actions with the <Shift> and <Ctrl> keys. All items in the Browser window can be selected by using the **Edit | Select All** command.

If you select individual files to be scanned they will be scanned.

If you select directories or drives, only the files with extensions in the executable list will be scanned.

For further information on the list of files considered executable click here.

How to start scanning the selected files

How to Start a Scan

Once item(s) have been selected for scanning, any of the following actions will initiate the scan:

1. pressing the GO toolbar button;
2. selecting the **File** | **Go** menu item;
3. pressing the right mouse button and selecting the `InoculateIT PE' option in the pop-up menu;

Results of the scan are displayed in the Report window and also written to the log file. (see the **Options** | **Program** | **Reporting** menu for the name of the log file). Depending how the item(s) for scanning were selected, one of the following options will have occurred;

1. If the Browser window is active when a scan is started:
2. If the Report window is active when a scan is started:

If the Browser Window is active when the scan is started:

Item(s) that have been selected in the Browser window will be scanned.

The Browser window will be active immediately after item(s) have been selected.

If no item(s) are selected and a scan is started InoculateIT PE will not know which item(s) to scan and will put up a message box prompting you to select a file, folder or drive in the Browser window and then to try again.

If the Report Window is active when a scan is started:

InoculateIT PE will not know which item(s) to scan and will put up a message box prompting you to select item(s) and then to try again.

This will happen even if an item has been highlighted in the Browser box.

Click on the Browser icon to make it active, and then try again

About the Report Window

The report window displays the results of scans. The Options | Program | Scanning menu allows changes to the types of files scanned (either all files or executables only) and also allows sub-directories to be scanned.

The Options | Program | Reporting menu can set the report window to show all files scanned or only those that are infected or suspected. Checking the check box **Cumulative report** causes the report window to show the results of the current scan after the results of the last i.e. causes a log. Not checking the box will cause the report window to be cleaned before the results of a scan are displayed.

How to use the InoculateIT PE Report Window

The Report window displays the results of scans done in the current session.

The various options possible while using the Report window are described below;

1. Text can be copied to the Clipboard using the **Copy** command;
2. All the text in the Report window can be selected for copying using the **Edit | Select All** command;
3. The results that are displayed in the Report Window can also be emailed. See the Options menu for further details.
4. The names of the files that have been scanned can be displayed in the report window. Either *all* of the file names scanned can be displayed or *only those that are suspected* of having a virus can be displayed. This option can be set under the Options | Program | Reporting menu

How to Edit the Defaults (Options | Program menu)

The Program dialog is opened by selecting **Options | Program** from the menu. It provides an opportunity to change the InoculateIT PE default options for Scanning, Actions, Reporting, Boot Sectors and Memory. Each option can be examined by selecting the appropriate tab at the top of the window. The processes involved in adjusting the default settings are detailed below:

NOTE: Set **All files** and **Full Scan** if you suspect that you may have a virus or you have just had a virus - it may find infected overlay files with obscure extensions that the **Executable Only** test may not test, as well as any non-executable files the virus has corrupted by trying to infect.

Select the options below for information on:

Scan Options

Include subfolders

Skip renamed files

File Types

File Types to scan

Reporting

Reporting when a virus is found

Display `Out-of-date' warning

Program Viruses

Infected program files

Suspect program files

Macro Viruses

Infected document files

Boot Sectors

Scan boot sectors plus options

Memory (Not available for NT users)

Real-Time memory checking

Start-up

Start-up Scan

How to customize the Start-up Scan

The Tools Menu

The Tools menu (<Alt> T) allows a template or reference disk to be created for each disk drive. A template is a copy of the current boot sector. InoculateIT PE can compare the saved copy of the template with the current template to determine if changes have occurred. The reference disk stores copies of the templates to a floppy disk.

The re-installation of an old template can cause files to be lost if the drive structure was changed after the template was made. For this reason the ability to re-install templates (emergency functions) are protected with a password.

NOTE: New templates will be required if more drives are added, the partitions of current drives change or the operation system is updated.

Record Templates

Record Reference Disk

Emergency functions

Emergency password

Change Password

Auto Downloads

How to Record Templates

The tools menu allows a template to be created for each local hard disk drive. InoculateIT PE will check that the template matches the current boot sector as part of the first scan of any session.

A dialog will display all of the drives available. Click on each drive (or use the space bar and arrow keys) to select the drive(s) that you wish to make templates for.

Options:

OK: A template for each of the selected drives is made.

Cancel: No templates are made.

Help: Displays this help screen.

Record Reference Disk

Emergency functions

Emergency password

Change Password

Auto Downloads

How to make a Reference Disk

A reference disk can be made to store copies of the current templates. These templates can be re-installed at a later date if the drive has been corrupted by an unrecoverable virus.

Insert a blank formatted disk, or preferably a system disk, into the floppy drive. (If you do not have a new disk see NOTE: below)

Select the floppy drive that will produce the reference disk by using the arrow keys or selecting from the scroll-down menu. Enter a caption in the Identification field (<Shift> I) so that copies of the current template(s) can be recognized at a later date. As a default, the Identification field type-in box will store the time and date that the templates are created.

This disk should now be kept in a safe place.

NOTE: To format a new disk insert it into the floppy drive, in Explorer click the drive, then click the right-hand mouse button. Select Format, Full and Start.

Record Templates

Emergency functions

Emergency password

Change Password

Auto Downloads

Emergency Services

The re-installation of an old template can cause files to be lost if the drive structure was changed after the template was made. For this reason the ability to re-install templates is protected with a password .

When the correct password has been entered the Emergency Services dialog will appear. Select the local hard drives that you wish to verify then select <Enter> to begin the comparisons. As each of the drives are checked a dialog will appear with the results of the comparison.

If a drive template was not created, a dialog will confirm that no comparison is possible. It is only possible to check local hard drives.

If the Boot sector, DOS and large IDE template attributes match the current drive configuration, select the OK button to begin the next comparison.

If the template does not match the current drive configuration, InoculateIT PE will offer to replace it with the original template.

YES: Loads the original template over the current configuration.

NO: The template remains the same and is not replaced.

Record Templates

Record Reference Disk

Emergency password

Change Password

Auto Downloads

How to change the Emergency Functions Password

For security reasons the password should be changed periodically.

To change the emergency password;

1. Enter the current emergency password in the Current Password text box
2. Enter the new password in the New Password text box
3. Re-enter the new password in the Confirm New password text box
4. Select the OK button

Record Templates
Record Reference Disk
Emergency functions
Emergency password
Auto Downloads

How to use the Report File Dialog

This dialog allows the user to define the location of the log file. The file structure can be navigated and new files/folders can be created as required.

This dialog is accessed from the **Options | Program | Reporting** menu command and pressing of the **Browse** button. It enables you to browse for alternate files to use as the log file or to create a new file in a chosen directory.

NOTE: As the log file has to be able to be edited in DOS the name must NOT contain spaces; unprintable characters or contain directory names longer than eight characters.

Toolbar buttons used in this window are explained below:

Up One Level Press the "Level Up" toolbar button to move to the parent directory of the directory currently displayed.

Create New Folder Used to create a new folder in the folder, directory or drive displayed in the Report File window.

List Select this button to list the files, folders, directories and/or drives available. The *List* and *Details* buttons are mutually exclusive.

Details Select this button to display the details (type, size, and date last modified) for the files, folders, directories and/or drives available. The *List* and *Details* buttons are mutually exclusive.

The **File name** type-in box allows the name for a new log to be entered

Save as type changes the type of file to be displayed.

Save & Cancel Buttons

Virus in Memory

The **Virus in memory!** dialog will immediately appear if a virus is detected in resident memory. The first function performed by InoculateIT PE when a scan is activated is to check resident memory for viruses.

Resident memory (RAM) is checked for viruses at the start of each InoculateIT PE session (i.e. when the first scan is requested InoculateIT PE will check resident memory and then check the item(s) requested for scanning.)

InoculateIT PE is normally installed to scan each time a machine is booted (started) and the memory will automatically be the first item checked. If InoculateIT PE is started from the desk top and the **Options | Program | Memory** menu option is enabled the resident memory will be checked before the first scan is performed.

Options:

Yes A message will confirm if InoculateIT PE has disabled the virus(es). If it has not been possible to disable the virus E-mail Customer support

Once InoculateIT PE has dealt with the virus in memory it will automatically check the boot sectors of all hard drives. See below.

No Check the **Help | Virus Information** menu for details on virus payloads. **WARNING:** If the virus present on your computer has a "payload" it may severely damage your files(s) and drive(s).

Details The Detail of viruses in memory dialog will display the number, name and memory location of the virus(es) that have been found.

Help Displays this help page.

Details of the Virus(es) in memory

This dialog will be displayed when the **Details** option is chosen on the Virus in memory dialog.

This dialog displays the number, name and memory location of the virus(es) that have been found in resident memory.

Selecting the **OK** button will close the dialog and return to the Virus in memory dialog.

Virus in memory dialog

If InoculateIT PE finds a Hard Disk Boot Sector Virus

InoculateIT PE checks drive boot sectors if the **Options | Program | Boot Sectors** menu has the *Scan boot sectors* option enabled and the infected drive is scanned.

If a virus is detected the Repair infected boot sector? dialog will be displayed. This will display the name of the drive and the type of virus found. It will also display options to repair the boot sector (if it is possible to repair it).

Options:

Yes InoculateIT PE will display the Make a Rescue Disk dialog. A rescue disk can be made to store copies of the current file structure. The structure can be re-installed at a later date if the drive is corrupted by an unrecoverable virus.

No The fact that the virus has been found will be recorded in the log file.

WARNING: If the virus present on your computer has a "payload" it may severely damage your files(s) and drive(s). Check the **Help | Virus Information** menu for details on virus payloads.

Help Displays this help page.

YES - Make a rescue disk

Payloads and Warheads

The first virus writers were content with proving that they could write a virus, but now most add a PAYLOAD or WARHEAD. This may be in the form of a message put to the screen or it may be something that interferes with the operation of the computer in an `amusing', irritating or destructive manner.

With warheads, there is a conflict between the desire to show off and the need to be inconspicuous so that the virus will propagate widely. This is usually achieved by making a warhead wait a certain amount of time or wait for an unusual event, so that the virus does not declare itself until it has had a chance to propagate.

WARNING: It is unwise to deliberately trigger a virus's warhead. There are often variations and revisions made to viruses. Viruses that have been harmless in the past may have been modified to cause substantial damage. Some people cannot resist the temptation to run a virus and the consequences of doing so can be disastrous.

How to make a Rescue Disk:

A rescue disk can be made to store copies of the current boot sector. The current boot sector can then be re-installed at a later date if the virus has corrupted the original boot sector and it is unrecoverable. This dialog is activated by selecting **Yes** in the *Repair infected boot sector?* dialog.

Insert a blank formatted disk in the floppy drive. (If you do not have a new disk see NOTE: below). Select the floppy drive that will produce the reference disk by using the arrow keys or selecting from the scroll-down menu. Enter a caption in the Identification field (<Shift> I) so that the rescue disk can be recognized at a later date. As a default, the Identification field type-in box will store the time and date of the disk's creation.

NOTE: To format a new disk check that the disk can be written to (i.e. the hole in the top, right side of the disk is open), insert it into the floppy drive, in Explorer click the floppy drive once, then click the right-hand mouse button. Select **Format, Copy system files only** and **Start**.

STOP! As soon as the rescue disk is created **it will be infected** with the virus and has the potential to infect other PCs. Do not use this disk in any other PC.

Options:

Yes The rescue disk will be created allowing InoculateIT PE to recover the current boot sector if the original has been corrupted by the virus. Once the disk is created, InoculateIT PE will check to see if the original boot sector is recoverable and will display the Ready to replace boot sector? dialog.

No The virus will be removed. If the original boot sector can be found and it has not been corrupted InoculateIT PE will display the Ready to replace boot sector? dialog. If the original boot sector has been destroyed by the virus InoculateIT PE will display the Master boot record damaged dialog.

Help Displays this page.

Ready to replace boot sector?

Master boot record damaged

If the original Boot Sector has been corrupted:

If the virus has damaged or destroyed the original boot sector, InoculateIT PE will display the Master boot record damaged dialog. This allows the option of installing of a standard boot sector which will recover the drive for almost all systems. But there is no guarantee that it will work for yours. If the installation fails to recover the drive, the rescue disk (if one was created) can be used to reverse the cleaning process. Email Customer support

NOTE: If a standard boot sector is installed on a non-standard drive, the drive will be corrupted and all files may be lost. A rescue disk can reverse the cleaning process and re-install the infected (but functional) boot sector.

Options:

YES Installs a standard boot sector.

NO The fact that the virus has been found will be recorded in the log file.

Installing the Boot Sector:

At this point the original boot sector (or a standard replacement if the original was not recoverable) is able to be installed as the boot sector for the hard drive.

NOTE: If a standard boot sector is installed on a non-standard drive, the drive will be corrupted and all files may be lost. A rescue disk can reverse the cleaning process and re-install the infected (but functional) boot sector.

Options:

YES Replaces the boot sector.

NO The fact that the virus has been found will be recorded in the log file.

"Replace Floppy Boot Sector?" dialog

InoculateIT PE checks floppy boot sectors if the **Options | Program | Boot Sectors** menu has the *Scan boot sectors* option enabled and the infected drive is scanned.

If a virus is detected the Repair infected boot sector? dialog will be displayed. This will display the name of the drive and the type of virus found. It will also display options to replace the boot sector (if it is possible to repair it).

Options:

Yes InoculateIT PE will replace the existing boot sector with a standard floppy boot sector.

No The fact that the virus has been found will be recorded in the log file.

WARNING: If the virus present on your floppy has a "payload" it may severely damage your files(s) and spread to other drive(s) and floppies. Check the **Help | Virus Information** menu for details on the amount of damage this virus can cause.

How to remove File Viruses

File viruses will be automatically, if the *Options* | *Program* | *Action* tab has been set to Clean infected files. Other possible options are to automatically delete or rename the file. Whichever option is selected, the name of the virus and the name of the infected files will be written to the log file.

When a scan is performed on a group of files the file name of the infected file(s) along with the name of the virus and the action InoculateIT PE has taken will be displayed in the InoculateIT PE Report window. By default only those files that are infected will be displayed. All the files scanned can be displayed if the Options | Program | Reporting *All files scanned* option is selected.

How to clean Office97 documents

Word97 and the other components of Office97 have a different file structure to the documents created by Word 6, Word 7 and other products prior to Office97. This new structure (VBA5) requires a different method for detecting and cleaning macro viruses.

The good news is that all of this is now transparent to you the user!

InoculateIT PE can automatically detect and clean all Word, Excel and Access macro viruses.

On Demand Scanning Default Settings

These default settings determine how InoculateIT PE will perform a scan when you start InoculateIT PE and scan a file, directory or drive. To alter these defaults select the Options | Programs menu item.

Scanning:
Include sub-folders is on. For further information click here.
Skip renamed files is on. For further information click here.
File types to scan is set to `Files of these types'. For list of default extensions click here.

Actions:
Infected program files is set to clean. For further information click here.
Suspect program files is set to report only. For further information click here.
Infected document files is set to clean. For further information click here.

Reporting: For further information click here.
Filenames reported is set to Infected or suspect files only
Cumulative report is on. The default name of the log file is C:\Program Files\InoculateIT PE\VIRUSLOG.TXT
Display Out-of-date warning is on.

Boot Sectors: For further information click here.
Scan boot sectors is on
Replace bad boot sectors is on
Treat as a bad boot sector is set to known virus only

Memory: For information click here.

Enable memory scanning is on

Real-Time Protection Default Settings

By default Real-Time protection is enabled when InoculateIT PE is installed. To alter any of these settings select Options | Real-Time Protection. For more information click here.

Floppy Boot Sector: For information on the this option click here.
Consider the boot sector bad if it contains a known virus
Replace any boot sector considered bad is on

File Monitoring: For information on this option click here.
Monitoring executing programs is on
Monitoring opening files is on
Monitoring closing files is (off for Windows NT but on for Windows95/98)
Action for infected files is set to clean file
Action for suspect files is set to report and deny access
Beep on detection is off (for Windows95/98 only)
Invisible mode is off (for Windows95/98 only)
Write log file is off (There is no default name for the log file) (for Windows95/98 only)

Macro Monitoring: For information on the this option click here.

Clean infected documents is On/Clean documents

The OK/Save and Cancel Buttons

OK/Save	Closes the dialog and saves any changes or selections that you have made.
Cancel	Closes the dialog without saving any changes or selections.

Real-Time File OK and Cancel Buttons

OK Closes the Real-Time Protection Options dialog A summary of the current settings will be displayed Selecting **OK** will save the changes that have been made.

Cancel Closes the Real-Time Protection Options dialog without saving any changes or selections that you have made in this dialog box.

Password Protecting Your InoculateIT PE Setup

Many system administrators have asked that we provide password protection to stop unauthorized alterations to the InoculateIT PE configuration. This password protection can now be enabled by selecting Options | Password Protect Options and entering a password.

NOTE: The password that is entered is case dependent, so an "a" is not the same as an "A".

Contact Information

The developers of InoculateIT Personal Edition have always aimed to provide software that will operate in the background until a virus attempts to infect and damage your PC.

If you have a technical support question please see the FAQs for immediate answers, or email IPE_Support@cai.com. InoculateIT Personal Edition technical support staff have a support level target to answer all e-mail with 48 hours of it being delivered.

If you suspect that you have a file that is infected with a virus that IS NOT detected by InoculateIT Personal Edition please email a copy of the file to IPE_Virus@cai.com. The InoculateIT Personal Edition virus dissection team will send an updated DAT file back to you within 48 hours. This will allow you to detect and clean the virus. (Standard response time is within 24 hour hours).

Computer Associates International has offices in the following countries:

Argentina, Australia, Austria, Bahrain, Belgium, Brazil, Canada, Chile, China, Colombia, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Malaysia, Mexico, The Netherlands, New Zealand, Norway, Philippines, Poland, Portugal, Russia, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Kingdom, United States and Venezuela.

Select an office for additional details. If you are not sure which office serves you, call 1-516-DIAL CAI (342-5224) for information.

ARGENTINA

Computer Associates de Argentina S.A.
Av. Davila 400 - Piso 2
1107 Buenos Aires
Argentina
Tel: (54)(1) 317-1500
Fax: (54)(1) 317-1515

AUSTRALIA

Computer Associates Pty. Ltd.
407 Pacific Highway
Artarmon, NSW, AUS 2064
Tel:(61)(2) 9937-0500
Fax:(61)(2) 9937 0600

AUSTRIA

Computer Associates Ges. m. b. H.
A-1100 Wien
Wienerbergstrasse 3
Tel:(43)(1) 605 80-0
Fax:(43)(1) 605 80-99

BAHRAIN

Computer Associates Middle East
Ground Floor, Diplomat Tower
Building 315
Road 1705, Block 317
Manama
Tel:(97)(3) 537 977

BELGIUM

Computer Associates S.A. - N.V.
34, Boulevard de la Woluwe
Woluwedal
B-1200 Bruxelles
Tel:(32)(2) 773 28 11

BRAZIL

Computer Associates do Brasil Ltda.
Av. Engenheiro Luiz Carlos Berrini
1253 - 1,5,6 andares
São Paulo - SP
04571-010
Tel:(55)11 5503-6000
Fax:(55)11 5503-6001

CANADA

Computer Associates Canada Ltd.
5935 Airport Road
Mississauga, Ontario L4V 1W5
Tel:(1)(905) 676-6700

CHILE

Computer Associates de Chile Ltd.
Av. Andres Bello, 2777
Oficina 1501
Edificio La Industria
Santiago
Tel:(56)(2) 203-3151
Fax:(56)(2) 203-3161

CHINA

Computer Associates (China). Ltd.
Room No. 2307, Capital Mansion
No. 6, Xin Yuan Nan Road
Chao Yang District
Beijing 100004
People's Republic of China
Tel: +86-10-6466 0322/0336
Fax: +86-10-6466 1135

COLOMBIA

Computer Associates Colombia
Avenida 82 No. 12-18
Oficina 305
Santafé de Bogotá - DC
Tel:(57)(1) 623 7886

CZECH REPUBLIC

Computer Associates Czech Republic
Donska 9
100 00 Praha 10
Czech Republic
Tel: ++420-2-67206360
Fax: ++420-2-67206363

DENMARK

Computer Associates A/S
Kongevejen 195B
DK-2840 Holte
Denmark
Tel: +45 45 47 41 41
Fax: +45 45 47 41 10

FINLAND

Computer Associates Finland OY
Itälahdenkatu 15-17
Helsinki SF-00210
Tel:(358) 9 34 84 84
Fax: (358) 9 348 48 585

FRANCE

Computer Associates S.A.
14 Avenue François Arago
BP 313
92003 Nanterre Cedex, 92003
Tel:(33)(1) 40-97-50-50

GERMANY

CA Computer Associates GmbH
Hauptverwaltung Darmstadt
Marienburgstrasse, 35
64297 Darmstadt
Tel:(49)6151 / 949-0
Fax:(49)6151 / 949-100

HONG KONG

Computer Associates International Ltd.
21/F World Trade Centre
280 Gloucester Road
Causeway Bay, Hong Kong
People's Republic of China
Tel:(852)2587-1388
Fax:(852)2587-1018

HUNGARY

Computer Associates Hungary
Kapas u. 11-15
1027 Budapest

Tel: +361 457 91 40

INDIA

Computer Associates India
511/512 Merchant Chambers
98A Hill Road
Bandra, Mumbai 400 050
India
Tel: 91 22 643 4681/82
Fax: 91 22 643 0843

INDONESIA

Computer Associates Indonesia
Wisma 46, Kota BNI
Level 34-05/06
Jl Jend Sudirman Kav. 1
Jakarta - 10220
Indonesia
Tel: 62-21-251-5030
Fax: 62-21-251-5029 / 251-5038

IRELAND

Computer Associates Plc
Embassy House
Ballsbridge
Dublin 4
Ireland
Tel:(353)(1) 478 0800

ISRAEL

C.A. Computer Associates
Israel Ltd.
Debora Hanevia St.
Neve Sharet, Atidim
Tel Aviv 61580
Tel:(972)(3) 6481120

ITALY

Computer Associates S.p.A.
Palazzo Leonardo
Via Francesco Sforza, 3
Milano 3 City
20080 Basiglio Milan
Tel:(39)2 90 464 1
Fax:(39)2 90 464 2501

JAPAN

Computer Associates Japan
Computer Associates Japan, Ltd
Shinjuku Mitsui Bld.

2-1-1 Nishi-Shinjuku, Shinjuku-ku
Tokyo, 163-04 Japan
Tel : +81-3-5320-8080
Fax : +81-3-5320-8095

KOREA

Computer Associates Korea Ltd.
11th Floor, Textile Center Bldg.
944-31, Daechi-Dong
KangNam-Ku
Seoul, Korea
Tel: +82-2-528-4100
Fax: +82-2-528-4111

MALAYSIA

Computer Associates (Malaysia) Sdn. Bhd
Suite 32/03, Level 32
Menara Lion
165, Jalan Ampang
50450 Kuala Lumpur
Malaysia
Tel: +60-3-230-2022
Fax: +60-3-230-6453

MEXICO

Computer Associates Mexico
Insurgentes Sur
1787 - Piso 10
Col. Guadalupe-Innc Morales
Mexico D.F. 11570
Tel:(52)5 327 5210

THE NETHERLANDS

Computer Associates B.V.
Wattbaan 27
3439 ML
Nieuwegein
(31) (30) 604 83 45

NEW ZEALAND

Computer Associates (NZ) Ltd.
Level 11, 34-42 Manners Street
P O Box 997, Wellington, N.Z.
Tel:(64)(4) 801 7654
Fax:(64)(4) 801 7655

NORWAY

Computer Associates Norway AS
Fornebuvn. 7-9
Pb. 450

N-1324 LYSAKER
Norway
Tel. +47 67 52 40 00
Fax +47 67 52 40 01

PHILIPPINES

Philippine Computer Associates International, Inc.
20/F Antel Corporate Center
139 Valerio Street
Salcedo Village, Makati City
Metro Manila
Philippines
Tel: +632-812-1441
Fax: +632-812-8896

POLAND

Computer Associates Poland
Centrum LIM
Al. Jerozolimskie 65-79
00-697 Warszawa

PORTUGAL

Computer Associates International, Inc.
Rua Tomas da Fonseca
Torres de Lisboa, Torre G-3
1600 Lisboa
Tel:(35)(1)727 35 33
Fax:(35)(1)727 35 25

RUSSIA

Computer Associates CIS, Ltd.
Representation Office
Business Center
Tokmakov per.,5
107066, Moscow, Russia
Tel./Fax: +7-095-937-48-50

SINGAPORE

Computer Associates Pte. Ltd.
9 Temasek Boulevard
#10-01/03 Suntec Tower 2
Singapore 038985
Tel: (65) 337 2822
Fax: (65) 337 4822

SOUTH AFRICA

Computer Associates Africa
6 Kikuyu Road
Sunninghill Park
Sunninghill Ext. 56

2157 Sandton
South Africa
Tel.: +27 11 807-5920
Fax: +27 11 807-2151

SPAIN

C.A. Computer Associates S.A
Calle Carabela La Niña, 12
Barcelona 08017
Tel:(34)3 2278100

SWEDEN

Computer Associates Sweden AB
Box 540
Berga Backe 4
182 15 Danderyd
Tel:(46)8-622 22 00
Fax:(46)8-622 58 68

SWITZERLAND

CA Computer Associates AG
Industriestraße, 30
Kloten CH-8302
Tel:(41)(1) 814 03 00

TAIWAN

Computer Associates Taiwan Ltd.
6th Floor, 105, Sec. 2, Tun Hwa South Road
Taipei, Taiwan
Tel: +886-2-2700-9218
Fax: +886-2-2700-9318

THAILAND

Computer Associates Pte. Ltd.
33rd Floor, Abdulrahim Place
990 Rama IV Road
Silom, Bangrak
Bangkok 10500
Thailand
Tel: 66-2- 636-2467-9
Fax: 66-2- 636-2470

TURKEY

Computer Associates Ltd. Sti.
Büyükdere Cad. Oyal Is Hani
Kat: 5 No. 108-1
80280 Esentepe - Istanbul
Tel:(90)(212) 27 27 172

UNITED KINGDOM

Computer Associates Plc
Computer Associates House
183-187 Bath Road
Slough
Berkshire SL-14AA
Tel:(44)(1753) 5777 33

UNITED STATES

Computer Associates International, Inc.
One Computer Associates Plaza
Islandia, NY 11788-7000
Tel:(1)516-DIAL CAI (342-5224)

VENEZUELA

Computer Associates (CAI) de Venezuela
Av. Principal de la Castellana Centro
Letonia Torre Ing Bank - Piso 10 - Ofic. 105
Caracas 1060 - Venezuela
Tel: +58 (2) 264-5144 / 264-4744

Year 2000 Support

We are pleased to advise you that InoculateIT PE currently supports Year 2000 processing.

Computer Associates' basic support for the millennium date change (Year 2000) provides or will provide for proper operation of our products according to the published documentation. In most cases, this means simply assuring that dates are evaluated and processed properly for sequence and comparison. Testing and Quality Assurance processes are carried out to validate the operation of these products as related to the millennium date change, and any functional errors will be accepted as issues (bugs) and resolved according to our standard maintenance and support policies.

As long as your license for each respective CA program remains in effect and active on maintenance, you will be entitled to all of the benefits of CA's implementation of Year 2000 date support as described above. Of course, nothing herein should be deemed to modify in any way any of the terms or conditions of any existing license between us respecting any CA program.

Eicar - A file to test your configuration

This is a program from the **European Institute for Computer Anti-Virus Research** that can help test the virus detection capabilities of Anti-Virus software.

This is a small .COM file for DOS that simply prints the message

EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

when executed. It has the useful property that it consists entirely of printable ASCII characters, so you can easily email or fax it to someone.

Many anti-virus products will detect this file as if it had a virus. Most will give a special message to make it clear that this is a test file and not a real virus. For example, when the EICAR file is scanned, the following message will be displayed:

Detected the EICAR test string. Not a virus.

The main use of the EICAR test file is to test that your Anti-Virus software is configured and operating as you want it to. For example, it could be used to test that Real-Time protection is active and behaving as you expect.

While this file obviously has absolutely no virus code in it, you should only distribute it to people who have a clear understanding of what it does. Also, do not store it on production machines that run anti-virus software (except as part of a deliberate test), as it will probably trigger whatever alarm bells are in place.

Please refer to the EICAR Standard Anti-Virus Test File web page (www.eicar.org/anti_virus_test_file.htm) for more information.

Here is the EICAR test string, in its entirety:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Welcome to InoculateIT Personal Edition

Congratulations on choosing InoculateIT Personal Edition (InoculateIT PE) to protect your computer against viruses, trojans and other malicious software.

InoculateIT is a world class range of anti-virus software which can be deployed to suit any business or organisation. InoculateIT PE is a cutting edge, high performance virus package specifically designed to protect small businesses and home users from everyday virus threats.

InoculateIT PE is designed to protect individual computers without having to be installed from a network server. If you wish to install anti-virus protection to many computers in a business environment we recommend you evaluate other anti-virus products in the InoculateIT range.

This high quality anti virus tool comes with FREE software updates to registered users. It also comes with a promise that if you find a virus that InoculateIT PE is unable to detect or clean we will send you an emergency signature update in approximately 48 hours of receiving a copy of the suspected infected file.

Registered users will also receive FREE Internet E-mail support. The answers to many support questions can be found in the online help. If you open InoculateIT PE then select Help | Help Topics then select "How to get technical support and FAQs" you will find the answers to around 80% of the questions that are asked of our support team.

By registering, you are automatically subscribed to our FREE Virus Threat Notification System as well as our Update Notification Service. Anytime a new virus is found that is actually spreading around the world, this service will send an E-mail to you when a new virus signature update is available. This handy service will ensure that you are kept up to date so that you are protected against the very latest viruses. The Update Notification Service will only alert you when a new virus signature is posted on the Internet.

Frequently Asked Questions

The InoculateIT PE support team has compiled a considerable database of support questions. This appendix lists the more common questions as well as their corresponding answers.

To make finding questions easier, they are grouped into categories. Please take the time to read this appendix before contacting InoculateIT PE for advice as you may already have the answer you need.

Installation/Setup/Configuration Problems
Problems using InoculateIT PE
General Information
Glossary

This appendix also contains the common error messages that InoculateIT PE may display, and what they mean. If InoculateIT PE reports an error that you do not understand, and which is not listed here, please E-mail your question to ipe_support@cai.com for advice.

Installation/Setup/Configuration Problems

This section of the Frequently Asked Questions contains questions that you may have while installing InoculateIT PE. If your question is not answered here then click here to return to the main menu.

1) How do I check which version of InoculateIT PE I am running?
2) I want to install a program and it has told me to disable my anti-virus software. How do I disable InoculateIT PE?
3) After installing InoculateIT PE my icons have changed. Why is this, and how can I change them back?
4) When I remove InoculateIT PE from my Windows 95 system it gets to Removing Lines from the Dosstart.bat file and terminates with an error? How can I get around this problem?
5) I have configured my Windows 95 PCs to use 'user profiles' with access to the Registry disabled. I am now having problems installing InoculateIT PE. What can I do?
6) I get a General file transfer error -3 when I am performing an installation of InoculateIT PE. What is the cause, and the solution?

How do I check which version of InoculateIT PE I am running?

1. In Windows 95, 98 & NT, go to Start | Programs | InoculateIT PE (using the start menu).

2. Open the InoculateIT PE Program Window and go to Help | About.

You should regularly check the InoculateIT PE website www.cai.com/antivirus/personal for newer releases of InoculateIT PE, to keep your Antivirus protection up-to-date. Also, check our website for information on subscribing to our free e-mail notification service so you are informed via e-mail when a new version of InoculateIT PE is released.

I want to install a program and it has told me to disable my anti-virus software. How do I disable InoculateIT PE?

We advise that you don't disable InoculateIT PE Real-Time Protection under any circumstances because while InoculateIT PE is disabled, you are vulnerable to virus infection. Product or demo CD's shipping with viruses unintentionally attached is a rare but genuine threat, which is why the installation of new software is the worst time to disable InoculateIT PE.

However, if it is absolutely necessary to disable InoculateIT PE Real-Time Protection, please follow these instructions.

1. Open the InoculateIT PE program window using the taskbar icon in Windows 95/98/NT
2. Go to Options | Real-Time Protection | Enabling
3. Deselect the Boot Sector Monitoring box and the File / Macro Monitoring box.

You will then need to reboot the computer.

To confirm that InoculateIT PE Real-Time protection. is disabled, you can do the following:

1. Right Click on the InoculateIT PE Icon in the Taskbar
2. Select Status
3. There should be 2 red crosses displayed to indicate the Real-Time protection is disabled.

WARNING: Ensure that you enable the Real-Time Protection Modules by repeating the steps (1-3), this time checking the boxes to again enable the InoculateIT PE Real-Time protection.

After installing InoculateIT PE my icons have changed. Why is this, and how can I change them back?

This can sometimes happen when InoculateIT PE is being installed while other programs are running. This is not a serious problem and can be easily fixed. Simply exit Windows and re-start the computer in safe mode (to restart in safe mode hit the F8 key when the Starting Windows 95 message appears). Once into Safe Mode reboot the PC selecting Normal mode and you will find your icons will return to their original state.

When I remove InoculateIT PE from my Windows 95 system it gets to Removing Lines from the Dosstart.bat file and terminates with an error? How can I get around this problem?

Move the Dosstart.bat file to the C:\ directory and attempt the un-install again.

I have configured my Windows 95 PCs to use 'user profiles' with access to the Registry disabled. I am now having problems installing InoculateIT PE.   What can I do?

InoculateIT PE can only use the privileges of the user that is logged in at the time of installation. For InoculateIT PE to complete a successful installation it must have access to the registry. Therefore, a user who has sufficient privileges to the registry must log in and then perform the InoculateIT PE installation.

I get a General file transfer error -3 when I am performing an installation of InoculateIT PE. What is the cause, and the solution?

During installation InoculateIT PE creates some registry entries, which can normally only be done if you have system administrator privileges. Please ensure that you are logged into the PC with Administrator rights.

Problems Using InoculateIT PE

This section of the Frequently Asked Questions contains questions that you may have while using InoculateIT PE. If your question is not answered here then click here to return to the main menu.

1) InoculateIT PE is causing an illegal operation when Windows starts up, What can I do?
2) I have installed InoculateIT PE for Windows 95 with the Plus Pack. I have noticed that it contains the McAfee Virus Scanner. Is it safe to run both InoculateIT PE and McAfee at the same time?

InoculateIT PE is causing an illegal operation when Windows starts up, what can I do?

This may happen when windows starts up and InoculateIT PE is doing a memory scan.   To fix this, run the InoculateIT PE main program. From the top menu select Options | Programs | Startup. Select Customized start-up command and type in the following command line:

```
C:\Program Files\InoculateIT PE\VET95.EXE. RECURSIVE /WAITSTART=15
```

This will delay the InoculateIT PE startup scan so that the conflict will be bypassed.

I have installed InoculateIT PE for Windows 95 with the Plus Pack. I have noticed that it contains the McAfee Virus Scanner.   Is it safe to run both InoculateIT PE and McAfee at the same time?

It is not advisable to run 2 Anti-Virus programs concurrently. You will need to disable the McAfee software during the installation of the Plus Pack or uninstall the program if it is already installed on the computer.

General

This section of the Frequently Asked Questions contains questions that are not about either installation or using InoculateIT PE. If your question is not answered here then click here to return to the main menu.

1) InoculateIT PE says that my Master Boot Record (MBR) or DOS Boot Sector (DBR) has changed. What does this mean?

2) Am I protected while using the Internet?

3) Why do some zip files take a long time to scan?

4) What are exotic viruses?

5) How can I tell that automatic protection is installed in Windows?

6) Year 2000 Support

7) When I run InoculateIT PE it says it is out of date.

8) Can you please tell me how to check e-mail attachments for viruses

9) I ran <generic brand> DISK EDITOR and found strange messages on the end of all my files.

10) Everytime I turn on my PC InoculateIT PE starts up and runs a scan. How do I turn it off?

11) I need to disable InoculateIT PE as I need to load some new software. How do I turn it off?

12) InoculateIT PE reported that a document may be infected by a virus. What should I do?

13) Another AntiVirus product is reporting the bloodhound virus. Why is InoculateIT PE not detecting this virus?

14) Are `Good Times' `Win a holiday' & `Budweiser' viruses or a hoax?.

15) InoculateIT PE has informed me that I have either Back Orifice or Netbus trojan on my system, and that it was not restored. What are these trojans, and how do I remove them?

InoculateIT PE says that my Master Boot Record (MBR) or DOS Boot Sector (DBR) has changed. What does this mean?

When InoculateIT PE reports that the MBR or DBR has changed, it is comparing a snapshot of this information that was taken when you installed InoculateIT PE, to the current MBR and DBR. Changes may occur when a new operating system is loaded onto the PC.

Also, if you install InoculateIT PE to a PC that was already infected with a boot sector virus and clean it, InoculateIT PE will report the boot sector has been changed.

Am I protected while using the Internet?

Yes. InoculateIT PE Real-Time Protection will scan for viruses when you download files to your computer. That is, as soon as you actually download any files and save them to your hard disk, InoculateIT PE will scan and clean them. Downloading and opening infected files is the only method of virus transfer at the moment, so with InoculateIT PE you are completely covered. To check that Real-Time protection is enabled, move the pointer over the InoculateIT PE symbol in the system tray (located in the bottom right of the taskbar near the clock). You can also open the InoculateIT PE program and select options | Real-Time Protection

Why do some zip files take a long time to scan?

Zip files contain many files inside them which each require scanning and possible cleaning. Zipped files may also contain additional internal zip files which need to be scanned. It takes time to unzip, scan then rezip each file.

What are exotic viruses?

InoculateIT PE distinguishes between "in-the-wild" viruses (viruses that have been reported from a genuine infection) and "exotic" viruses - viruses we have in our collection, but which we have never seen reported as infecting users. If InoculateIT PE says a file "may have" virus X, please send a sample of the file to Computer Associates at ipe_virus@cai.com. If it is a genuine infection, a removal procedure will be added to InoculateIT PE and the virus will be upgraded from "exotic" to "in-the-wild" status.

How can I tell that Real-Time protection is installed in Windows95 or 98?

Run InoculateIT PE for Windows 95/98, then select Options | Real-Time Protection. The box at the bottom of each Real-Time Protection tab reports the current status of that component of the Real-Time Protection.

InoculateIT PE year 2000 support

If you open the InoculateIT PE program window and go to Help | Help Topics | Year 2000 support, you will find Year 2000 Support documentation.

When I start my computer InoculateIT PE displays the out-of-date warning message. What does this mean and why am I getting this message if I have the latest release?

Please ensure that latest InoculateIT PE has been installed properly by opening InoculateIT PE | Help | About, and check the date that the current DAT file was created. If the DAT file is more than a month old you should consider downloading a newer version of the files from www.cai.com/antivirus/personal/updates and installing them.

Can you please tell me how to check e-mail attachments for viruses?

InoculateIT Personal Edition Real-Time protection will check and clean any infected e-mail attachments when you open them. You can also Save the attachment to the hard disk and scan it using the main InoculateIT PE program. To check that Real-Time protection is enabled, move the pointer over the InoculateIT PE symbol in the system tray (located in the bottom right of the taskbar near the clock).

I ran <generic brand> DISK EDITOR and found strange messages on the end of all my files.

Something odd happens, the user goes delving with their favourite disk editor and finds garbage or suspicious messages on the end of all the files. What is more, it changes when they copy a file to another location. "HELP! VIRUS!" Thankfully, no. MSDOS always allocates an integral number of whole clusters, but the file hardly ever fills the last cluster and the remaining space normally contains random rubbish.

Everytime I turn on my PC InoculateIT PE starts up and runs a scan. How do I turn it off??

Some InoculateIT PE users require the ability to conduct a scan when they start their PC each day. During the installation you will be asked if you would like this option enabled. Once enabled, the Start Up Scan can scan a set number of executable and document files on the boot drive every time the computer is started.

You can stop the scan at any time by selecting the CANCEL button from the progress meter.

To permanently stop this scan being started open InoculateIT PE and select Options | Program | Start-up

I need to disable InoculateIT PE to load some new software. How do I do it?

This is a dangerous thing to do. When you are loading new "shrink-wrapped" software people tend to believe that the software must be clean because it is direct from the software manufactures. This is not the case. Everytime you load files onto your PC you should have the Real-Time protection running to catch viruses.

If you have tried to load a piece of software and InoculateIT PE has refused to let you:

1) If the software is on a CD, send it back. Viruses cannot be removed from CDs.

2) If the software is on disks, check that they are write enabled and allow InoculateIT PE to remove the virus before installing the software.

3) If the Real-Time protection is clashing with the new software, do the following. Open InoculateIT PE and select Options | Enable Real-Time Protection. Click the check boxes so that they do not have a check in them and select OK. Close InoculateIT PE and reboot your PC.

When you have finished loading your software you MUST reverse the process and put a check in each box to re-activate the Real-Time protection.

InoculateIT PE reported that a document may be infected by a virus.   What should I do?

InoculateIT PE uses heuristics to detect polymorphic viruses and certain strains that re occur in the wild. Heuristic or generic scanning is a technique for detecting viruses that performs analysis of virus structure and behaviour instead of using specific virus templates and signatures. The advantage of Heuristic Detection is that it can catch unknown viruses - the disadvantage is that it requires a high level of user expertise to use it correctly, and is prone to false alarms. If you are faced with this problem please forward the files to our Support Team through ipe_virus@cai.com.

Another AntiVirus product is reporting the bloodhound virus. Why is InoculateIT PE not detecting this virus?

Bloodhound is a generic name used by one of our competitors indicating that a specific file may have a virus, but they can't work out if it is definitely a virus or if it is a false alarm. Can you please forward any suspect files to our support team through ipe_virus@cai.com. They will be checked as soon as possible. If the files do contain a real virus, we will incorporate support for detecting and cleaning it in our next update, and send an update back to you to clean up the problem.

Are `Good Times' `Win a holiday' & `Budweiser' viruses or a hoax?

The Good Times, Win A Holiday and Budweiser virus message are all hoaxes.

It is currently impossible for your computer to be attacked when you read an e-mail message.   If you would like more info, have a look at our website www.cai.com/antivirus

If you ever get any messages that sound similar and could also be a hoax, please e-mail them to the Technical Support Team at ipe_support@cai.com and we will let you know whether it is a real virus or not! Always verify the authority of such messages (by checking with us or a respected website) before forwarding them to your acquaintances. While hoaxes don't do any damage, they DO reduce people's overall confidence in using computers.

Remember the golden rule: You cannot infect your computer by just opening and reading an e-mail. You can only get infected by opening/running files that are attached to the e-mail. (And provided you have your Real-Time protection enabled you can open/run attachments without fear of a virus infecting your system.

InoculateIT PE has informed me that I have either Back Orifice or Netbus trojan on my system, and that it was not restored. What are these trojans, and how do I remove them?

A Trojan Horse is a malicious program masquerading as a legitimate program. The name comes from the Greek legend of soldiers hiding in a wooden horse which was supposed to be a gift, but which actually allowed them to infiltrate and burn the city of Troy. The best protection against them is to be very careful about obtaining all your software from reputable sources. BackOrifice and Netbus exploit a security flaw in your system, and allows certain remote users to delete your files, use your internet account, open and close your programs and many other undesirable options. If InoculateIT PE reports that BackOrifice or Netbus is on your system, please contact our technical support department by E-mail to ipe_support@cai.com for instructions on how to remove them immediately.

Glossary Of Terms

Unfortunately the computer industry uses a lot of technical terms that the general public has difficulty understanding. Below is a list compiled from customer enquires, if the word or term that you are interested in does not appear below please e-mail InoculateIT PE technical support.

AV short for Anti Virus

CARO short for Computer Anti-virus Research Organisation

Companion viruses

DLL short for Dynamic Link Library

DBR short for DOS Boot Sector (DBR)

Encrypting Viruses

Exotic viruses

File Viruses

GUI short for Graphical User Interface

Heuristic Detection

In the wild

Link viruses

Macro viruses

MBR short for Master Boot Record (MBR)

Multipartite Viruses

ICSA short for International Computer Security Association

OLE2 short for Object Linking and Embeding Version2

Payload

Parasitic viruses

Poly-Morphic Viruses

Real-Time Protection

Stealth

Trojan Horse

VBA5 short for Visual Basic for Applications version 5

VxD short for Virtual device Driver

Warheads

Worms

CARO (Computer Antivirus Research Organisation)

An informal world wide group of anti viral researchers. If a new virus is found by any of the companies that the researchers work for, samples are forwarded to the other members. This allows protection to be built into InoculateIT PE and other anti viral products before the virus is spread. (InoculateIT PE will also forward samples of new viruses to all other members to protect computer users overseas.)

DLL (Dynamic Link Library)
A collection of small programs that can be loaded and used by other programs.

GUI (Graphical User Interface)
A GUI product is one that allows you to "point and click" rather than typing in commands.

ICSA (International Computer Security Association)
A U.S. company that provides quality assurance ratings for products. InoculateIT PE is NCSA accredited.
For further information see http:\\www.icsa.com.

OLE2 (Object Linked and Embedding version 2)

A standard for applications to exchange information across application boundaries. This standard allows for example embedding an Excel spreadsheet into a Word documents. It includes specifications for visual editing (in-place editing).and storage of data. Microsoft Office applications use the OLE2 provided storage mechanisms to store documents, including macros.

VBA5 (Visual Basic for Applications version 5)

This is the macro programming language used by most recent MS applications. The macro language used for Word 6.0 and 7.0 was WordBasic.

VxD (Virtual Device Driver)

When you install a new device into your PC you also need to install a driver so that the operating system can communicate with the new device. A Virtual device driver lets the operating system communicate with software as if it were a physical hardware device.

Stealth

A virus using stealth techniques takes active measures to hide its presence. For example if you read the boot sector of a disk infected with the Brain virus while it is active, it shows you the original boot sector, not the infected one. Frodo infects files, but the infection cannot be detected while it is active, as it disinfects files before it lets you read them. DIR will show the correct file lengths and programs that monitor checksums will report that infected files have not been modified. Frodo does not trap any interrupts, but instead modifies DOS itself so that monitor programs do not detect any unusual activity. However, these tricks make the virus extremely finicky and it will not run on some PCs and many infected programs will crash.

A few viruses have gone to such lengths to hide themselves that they are called Armoured viruses. The best known of these is the Whale virus. This research virus is multiply encrypted and only decrypts each section immediately before use and then re-encrypts it using a different key. The whole virus is further encrypted, using one of a number of alternative encryption procedures, chosen at random, so that there is no single signature to search for. However, like all armoured vehicles, it is extremely cumbersome and slows an infected PC down so much that it is immediately obvious.

What is Real-Time Protection

When Real-Time protection is loaded it will automatically check files and floppy disks for viruses as you go about your daily work. Real-Time Protection is loaded every time you start your PC, unless you specifically requested that it not be loaded during installation.

The level of protection can be modified from the Real-Time Protection dialog. See the on-line Help topics in your version of InoculateIT PE for further details as the method for altering these settings is different for each operating system.

File Viruses

Although there are a lot of different ways of grouping and classifying viruses, we can say that file viruses are those viruses which spread via files that are either executable or contain executable components.

File viruses can be further divided into the following groups:

- Parasitic viruses
- Companion viruses
- Link viruses
- Macro viruses

Parasitic Viruses

These represent the majority of all file viruses and they spread by modifying the code of executable programs. A parasitic virus attaches itself to an executable file and changes its contents in order to activate itself as soon as the operating system tries to execute an infected program.

Since there are a few ways in which a virus can attach its code to another file, we can subdivide still further, into overwriting, appending, prepending and inserting viruses. An overwriting virus simply overwrites the beginning of the file so that the infected file doesn't change its length but it no longer runs. Because of their destructive nature, overwriting viruses are relatively easy to detect and are not very common.

Appending and prepending viruses add their code to the start or the end of the file (respectively) and redirect the entry of the infected program to the start of the virus code. In that way infected programs increase in length but since the virus can pass control to the original program, the difference between executing a clean and an infected file is hard to notice.

Inserting viruses place their code (in one or more blocks) inside infected programs. They can search for an unused area (e.g. headers of .EXE files) or split the files and add their code in between the blocks of the infected file.

Companion Viruses

These take advantage of the DOS system's feature related to the sequence of loading and executing programs. If the file specified for execution has no extension, the system always tries to execute fname.COM, then fname.EXE and at last fname.BAT. A companion virus infects .EXE file by copying itself to a file with the same name but with .COM extension and usually hidden attributes. If the user enters the fname command, the file fname.COM (ie the virus) will be executed first.

A companion virus doesn't modify the infected program and usually passes control to the original .EXE file, but once detected it is easy to clean - you simply delete the relevant .COM file.

Link Viruses

These infect programs by changing information in the directory structure and modifying the file pointers, so every infected program starts at the same location (usually the last cluster on the disk) which contains virus code. Cleaning disks infected with a link virus requires a specific approach.

Every file virus can incorporate different techniques to improve the infection rate or to avoid detection. Each of the above viruses can be memory-resident, can have stealth capabilities, can use encryption or can use a polymorphic engine.

Macro Viruses

Technically another form of parasitic virus, the thing that makes macro viruses rate a class of their own is that they are transmitted as an executable component in an otherwise non- executable data file. Most macro viruses are written in WordBasic (Microsoft Word's macro language in version prior to version 8) or VBA (the macro language developed for other Microsoft products including Word version 8).

Macros are executable code intended to automate tasks in applications. However the underlying macro language is extremely powerful, and can call out to external programs, making macro viruses potentially quite dangerous. They are also the first "platform independent" virus, in that they will run on Macintosh computers as well as PCs. Another way of looking at it is that they depend on MS products (Word, Excel, Access etc) as their platform. Macro viruses have rapidly become the most reported viruses in the world.

Multi-Partite Virus

This is a virus that infects both boot sectors and executable files and exhibits characteristics of both boot sector and parasitic viruses.

Encrypting Virus

This is a virus which hides its code or even a whole infected file by encrypting it. The only plain text that can be seen inside an infected file is a decrypting procedure.

Polymorphic Virus

This is a self-modifying encrypting virus. Polymorphic viruses incorporate a special algorithm to create many different-looking copies of the same virus. Every next generation of a polymorphic virus can look slightly or even completely different from the previous one. The majority of new polymorphic viruses use specially designed libraries (engines) containing subroutines to produce different encryption schemes and encryption keys. The most famous polymorphic engines are:

DAME or MTE (Dark Avenger Mutation Engine);

TPE (Trident Polymorphic Engine);

SMEG (Simulated Metaphoric Encryption Generator).

Trojan Horse

This is a program that doesn't replicate and doesn't infect any other executable files and whose execution will result in undesired (often destructive) effects.

Worm

This is a program that distributes multiple copies if itself across the system. The most famous was the Internet Worm, which in 1988 virtually shut down the Internet in the US. It exploited holes in the Unix sendmail and finger programs.

Warheads (Also known as Payload)

The first virus writers were content with proving that they could write a virus, but later writers have become more ambitious and added a payload. This can be a taunt (Your Computer is now Stoned!) or it may interfere with the operation of the computer in an amusing, irritating, or destructive manner. Again there is a conflict between the desire to show off and the need to be inconspicuous, so that the virus will propagate widely. This is usually achieved by making the payout wait some time or depend on some rather unusual event, so that the virus does not declare itself until it has had a chance to propagate. It is generally unwise to deliberately trigger a virus's warhead; we know of at least one user who was infected with the Michelangelo virus who advanced his system clock to March 6th just to see what would happen and thereby lost the data on his hard disk. Even joke viruses aren't funny when they go wrong on a non-standard PC.

Heuristic Detection

Heuristic or generic scanning is a technique for detecting viruses that instead of using specific virus templates and signatures, performs analysis of virus structure and behaviour. The advantage of Heuristic Detection is that it can catch unknown viruses - the disadvantage is that it requires a high level of user expertise to use it correctly, and is prone to false alarms.

Password

The password can be invoked by either selecting **Options | Password protect options**, or **Tools | Emergency.**

Options | Password protect options:

This feature is in InoculateIT PE for Windows 95, 98 and NT workstation because many system administrators asked that we provide password protection to stop unauthorised alterations to the InoculateIT PE configuration. The password protection can be enabled by selecting Options | Password Protect Options and entering a password.

The password protection of the Options menu can be disabled by selecting Options | Password Protect Options and entering the correct password. (The password protection for the Tools | Emergency menu is not affected by disabling the Options menu password).

Tools | Emergency:

The re-installation of an old template could cause files to be lost if the drive structure was changed after the template was made. For this reason the ability to re-install templates is protected with a password.

The Emergency Password dialogue will appear when the **Tools | Emergency** functions menu is selected. It prompts for a password to allow access to the emergency options, and will continue to prompt until the correct password is entered.

NOTE: The password can be up to 11 printable characters and is case dependant, so an "a" is not the same as an "A".

Scan Type (Options **|** Program **|** Scan Options)

Include subfolders: Causes InoculateIT PE to check the subdirectories or subfolders of the current directory or folder.

Skip renamed files: Causes InoculateIT PE not to check those files which have been renamed by InoculateIT PE during previous scans. Renaming will occur if the default in **Options | Program | Scan Options** is set to Rename and a suspect file is found. The file extension will be changed so that the first letter will be an underscore. So .exe will become ._xe.

File Types to Scan (Options | Program | File Types)

This dialog allows you to determine which files types will be scanned for viruses.

All files: Causes InoculateIT PE to check *every* file it encounters for viruses. You can choose either All files or Files of these types, but not both.

Files of these types: Causes InoculateIT PE to check files that it considers to be executable (or `runable'). By default InoculateIT PE considers files with the .386, .BIN, .COM, .DLL, .DOC, .DOT, .DRV, .EXE, .MDB, .OVL, .PPT, .SCR, .SYS, .VXD, .XLA, .XLS and .XLT extensions to be executable. You can choose either All files or Executable only but not both.

Add, Delete and Default buttons: For more information Click Here

Scan archives (zip): If this option is enabled InoculateIT PE will scan ZIP files.

Compressed archives can contain other compressed archives (this is called nested archives). InoculateIT will scan ten levels deep into any compressed archive that it scans.

Include InoculateIT PE in Windows context sensitive menus for these file types: If this option is selected and you are using MS explorer (or other navigation tool) you can select a file, directory or drive, right click the mouse button, and InoculateIT PE will scan your selection.

NOTE: When you are upgrading InoculateIT PE and chose Next> to continue past this screen InoculateIT PE will check your current list of file extensions. If you don't have all of the file extensions that we recommend (as they are susceptible to infection) a dialog will appear and prompt update your extension list.

Add, Delete and Default Buttons

These buttons allow you to change the list of file extensions that InoculateIT considers when determining if a file may be infected.

Add: Allows you to add to the list of file extensions InoculateIT will consider executable. With the advent of Macro language viruses, it is now possible for a file with any extension to contain a virus that can infect your PC. Selecting this button causes an input window to appear. You then have the opportunity to enter the new file name extension in the type-in box. If you wish to scan compressed archives we recommend you use the `scan compressed archives' option rather than adding them to the list of file types to scan.

Delete: If you select a file extension from the displayed list and press this button, the file extension will be removed from the list that InoculateIT considers executable.

Default: Restores the default list of file extensions that InoculateIT considers executable.

Infected & Suspect Program Files (Options | Program | Program Viruses)

The following mutually exclusive options are available for actions dealing with infected files.

STOP! If you chose for files to be **Clean**ed and a file has been infected with an overwriting virus , InoculateIT PE will offer to ignore, rename or delete the file, as no disinfection is possible. By default InoculateIT PE will offer to delete the file.

Report only: Causes InoculateIT PE to report, but not attempt to clean, infected files.

Clean: Causes InoculateIT PE to attempt to disinfect virus-infected files, returning the files to working order. If the file has been infected by an overwriting virus, InoculateIT PE will **Delete** the file, as no disinfection is possible

Rename: Causes InoculateIT PE to change the first letter of the extension of any file infected with a virus to an underscore `_' (.EXE becomes ._XE). This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes InoculateIT PE to delete irreversibly any file that it finds has been infected with a virus. The file is first overwritten with `D's and then set to zero length, so no recovery of the deleted files is possible.

STOP! Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Suspect Program Files:

The following mutually exclusive options are available for dealing with files suspected to contain a virus.

Report only: Causes InoculateIT PE to report, but not attempt to clean, infected files.

Rename: Causes InoculateIT PE to change the first letter of the extension of any file suspected of infection with a virus to an underscore `_' (.EXE becomes ._XE). This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes InoculateIT PE to delete irrevocably any file that it finds has been infected with a virus. The file is first overwritten with `D's and then set to zero length, so no recovery of the deleted files is possible.

STOP! Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Overwriting Viruses

Most viruses are careful not to destroy the infected file, but overwriting viruses overwrite part of the infected file, so that it will no longer operate. However, this makes these viruses extremely obvious, so they are unlikely to spread far.

The Zeroto-0, or Australian 403 virus, is of this type. When an infected file is run, the virus searches for an uninfected .COM file and replaces it with a 403 byte file which only contains the virus. The original file is destroyed, so infected files appear to run, but do nothing.

Suspect Program Files (Options | Program | Program Viruses)

The following mutually exclusive options are available for dealing with files suspected to contain a virus.

Report only: Causes InoculateIT PE to report, but not attempt to clean, infected files.

Rename: Causes InoculateIT PE to change the first letter of the extension of any file suspected of infection with a virus to an underscore `_' (.EXE becomes ._XE). This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes InoculateIT PE to delete irrevocably any file that it finds has been infected with a virus. The file is first overwritten with `D's and then set to zero length, so no recovery of the deleted files is possible.

STOP! Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Infected Document Files (Options | Program | Macro Viruses)

The following mutually exclusive options are available for dealing with documents, spread sheets or databases that are infected, or suspected, of having a macro virus.

InoculateIT PE can automatically detect and clean all Word and Excel macro viruses. InoculateIT PE is also able to detect Access database macro viruses.

Infected Documents

Report only: Causes InoculateIT PE to report, but not attempt to clean, infected documents.

Clean: Causes InoculateIT PE to attempt to disinfect virus-infected documents, returning the documents to working order. If the document has been infected by an overwriting virus, InoculateIT PE will Delete the document, as no disinfection is possible

Rename: Causes InoculateIT PE to change the first letter of the extension of any document infected with a virus to an underscore `_' (.DOC becomes ._OC). This allows you to keep the file for further examination.

Delete: Delete causes InoculateIT PE to delete irreversibly any document that it finds has been infected with a virus. The document is first overwritten with `D's and then set to zero length, so no recovery of the deleted documents is possible.

NOTE: Use this option with caution, as there is no possibility of recovering documents deleted in this manner.

Suspect Documents:

Report only: Causes InoculateIT PE to report, but not attempt to clean, infected documents.

Rename: Causes InoculateIT PE to change the first letter of the extension of any document suspected of infection with a virus to an underscore `_' (.DOC becomes ._OC). This allows you to keep the file for further examination.

Delete: Delete causes InoculateIT PE to delete irrevocably any document that it finds has been infected with a virus. The document is first overwritten with `D's and then set to zero length, so no recovery of the deleted documents is possible.

Reporting (Options | Program | Reporting)

This dialog controls what will be displayed in the Report window and written to the log file.

File names reported

All files scanned: Causes InoculateIT PE to display on a separate line the name of each file it tests (which in turn causes the name of every file tested to be written to the log file, regardless of whether it had a virus or not). This is useful in explicitly identifying which files are *not* infected (InoculateIT PE uses a separate line for each infected file).

Infected or suspect file only: Causes InoculateIT PE to report on a separate line the name of each file it finds to be suspected or infected.

The *All files scanned* and *Infected or suspect* options tell InoculateIT PE which file names are to be listed in the Report window. These two options are mutually exclusive.

Write log: The name of the log file to which all scan results are written is displayed in the type-in box. The location of the log file can be changed using the Browse button to select an existing file or allow the entry a new file name.

Cumulative report: If this option is enabled the results of each scan will be stored cumulatively in the log file. If it is NOT enabled the log file will be cleaned and overwritten each time a scan is performed.

Limit log size to: Once you perform a scan and the file becomes larger than (the default) 32Kb it will automatically be overwritten with the newer information. The log file size can be configured by editing the "limit log file size to" field.

Configure `Out-of-date' warning

NOTE: As the log file has to be able to be edited in DOS the name MUST NOT contain spaces, unprintable characters or contain sub-directory names longer than eight characters.

Auto Downloads

If you **ARE** connected to the Internet and you are using MS IE 4.0 or equivalent, Auto Downloads offers an easy way to update your software to detect the latest viruses.

How to use the Auto downloads feature:

1. Open InoculateIT and select **Tools | Auto Download**

2. The Auto Download dialog will be displayed.

NOTE: If you have not used Auto Downloads in the past another dialog will pop up and ask you to enter the email address of the person who registered their free copy of IPE.

3. The Save As dialog will be displayed and ask where to store the update files. Leave everything as it is and select **`SAVE'**. The file will be downloaded to your computer. (This may take a few minutes depending how fast your modem is). A message will be displayed when the files have been successfully downloaded. You will then be asked if you want to install the files. Select **`YES**".

4. A message will appear to let you know the Minor Update has completed successfully. Click **`OK'.**

If you are **NOT** connected to the Internet it is not possible to update your computer using this method. If you have access to the Internet but not on the machine that you wish to update, you can download a DAT file update kit from the web site, save it onto a floppy and copy it to other computers.

**Configure `Out-of-date' Warning** (Options | Program | Reporting | Configure `Out-of-date' warning)

Display Out-Of-Date Warning: This option allows you to enable or disable the out of date warning. This warning will pop up to let you know that it is time to update your copy of InoculateIT.

How often would you like to be reminded to update your templates?

This option and the following radio buttons allow you to select when you would like to be reminded to update the DAT files to detect the latest viruses.

Boot Sectors (Options | Program | Boot Sectors)

This dialog sets up the defaults for the treatment of boot sectors.

Scan boot sectors Allows InoculateIT PE to scan boot sectors. Turning this option off causes all the other options in this dialog box to become inactive.

Consider a boot sector bad if it contains: The following options tell InoculateIT PE how to define a bad boot sector; The first option gives adequate protection, whilst the last gives an extremely high level of protection. The three levels of protection are mutually exclusive. i.e. only one can be chosen.

Known viruses only Causes InoculateIT PE to consider a boot sector bad only if it contains a known virus.

Invalid boot sector or known virus Causes InoculateIT PE to consider a boot sector bad if it contains an invalid boot sector or a known virus.

Unknown or invalid boot sector, or known virus

STOP! Replacing unknown boot sectors may cause problems with some backup programs and copy-protected software. You should only use this setting if you are aware of the potential problems. Causes InoculateIT PE to consider a boot sector bad if it contains an unknown or invalid boot sector or a known virus.

Replace bad boot sector Causes InoculateIT PE to replace bad boot sectors. InoculateIT PE will always warn you before replacing a boot sector.

Check for large IDE driver To determine if a large drive is present InoculateIT PE uses direct port I/O to read the Extended Boot sector. This will not work on all PCs. The **Check for large IDE driver** allows users to disable this test if it causes problems on their system. This option is not available in InoculateIT PE for windows NT.

Memory (Options | Program | Memory for Windows 95/98 Only)

Enable Memory Scanning

This dialog enables InoculateIT PE to monitor Real-Time memory for viruses.

If another anti-viral program is running it may cause false alarms as virus templates may be detected from the other program.

Auto Downloads (Options | Program | Auto Downloads)

Proxy Server

A proxy server is the computer that you connect to for access to the Internet. The installation program will automatically try to find these details from your Internet browser. If the installation program is unable to find these details you will need to select the `Use the following proxy server' option and enter the details yourself.

Do not use a proxy server for Auto Downloads

This allows you to enable or disable the use of a proxy server.

Choose the proxy server automatically (From Control Panel)

This is the default option. Selecting this option will cause InoculateIT PE to automatically search your computer for the proxy server details.

Use the following proxy server:

Try the `Choose the proxy server automatically' option first. If this does not allow you to update you will need to find your proxy server details and enter them in the fields below.

How to find your proxy server details

For Internet Explorer:

The `Choose the proxy server automatically' option will automatically be able to find your proxy server details if you have Internet Explorer loaded on you machine.

For Netscape:

Please check the instructions that match your version of Netscape. To determine which version you have, open Netscape and select Help | About Communicator.

Netscape 3.x

Open Netscape, select Options | Network Preferences…| Proxies | Manual proxy configuration | View.

You need to copy the details stored next to the `HTTP Proxy'. You will also need to copy the Port number for the HTTP proxy.

Netscape 4.x

Open Netscape, select Edit | Preferences… | Advanced | Proxies | Manual Proxy Configuration | Configure.

You need to copy the details stored next to the `HTTP Proxy'. You will also need to copy the Port number for the HTTP proxy.

Start-Up (Options | Program | Start-Up)

This option allows you to configure how InoculateIT PE will perform the scans that are performed when you start or reboot your computer.

Run InoculateIT PE automatically when Windows starts up

This option will enable or disable the Start-up scan option.

Start-up Command

Perform progressive scan (recommended)

> This will enable a progressive test which will begin the next test where the last one finished, thus, over a period of days/weeks the entire hard drive will be checked.

Customised Start-up command

> This option allows you to configure your own scan using the InoculateIT PE command line switches.

A summary of the option that you have selected will be displayed at the bottom of the dialog.

The Configure Progressive Scan button allows you to modify the way the progressive scan is performed.

Command Line Switches

Command line switches can be used by selecting **Start | Run…**, typing in the full path and filename (ie. C:\Program Files\InoculateIT PE\VET95, C:\Program Files\InoculateIT PE\VET98 or C:\Program Files\InoculateIT PE\VETNT) and adding any of the command line switches that are listed below.

The following switches are available:

Long-form command line options

All options are able to be abbreviated providing the abbreviation is unambiguous and three or more characters in length.

Scanning

/AllLocalDisks - Include all local hard disk drives in the scan

/bootscan - scan the boot sector(s).
/nobootscan - do not scan the boot sector(s). (replaces /!S)

/cancel - Allow cancellation of the scan
/nocancel - Do not allow cancellation of the scan

/compressed - Scan compressed archives, e.g. zip files
/nocompressed - Do not scan compressed archives

/display=full - default, display the main GUI.
/display=progress - show a progress meter of the scan.
/display=notify - hide the progress meter unless infection detected.
/display=none - do not show anything. (replaces /&)

/ext - specify a list of extensions to scan.
Multiple extensions can be delimited like so: /ext="exe,dll,sys" or
/ext=exe,dll,sys;
/ext=* - scan all files
/ext - scan the default extensions. (replaces /.=)

/maxfiles - specify the maximum number of files to be scanned.
eg. /maxfiles=1000 (replaces /M=)

/memoryscan - scan memory.
/nomemoryscan - do not scan memory.

/resume - begin scan from where the last scan to use /maxfiles ended.
/resume now resumes a user-aborted scan also. (replaces /P)

/progressive - triggers the progressive scan (options defined within the program).
/autoscan - equivalent to /progressive (redundant as of 9.60)

/renamed - scan renamed files (*._??).
/norenamed - do not scan renamed files. (replaces /!V)

/sub - includes subdirectories in the scan.
/nosub - does not include subdirectories. (replaces /R)

Actions

The Action options will specify one of the following values for how to deal with file viurses: clean, rename, report only, delete
/infected= - specify the action to be taken on infected files.
/infected=clean
/infected=rename
/infected=delete
/infected=reportonly (replaces /!C, /U, and /Z)

/suspect= - specify the action to be taken on suspected file infections.
/suspect=rename
/suspect=delete
/suspect=reportonly (replaces /O, and /Y)

The Action options will specify one of the following values for how to deal with Macro viurses: clean, rename, report only, delete
/macro= - specify the action to be taken on infected files.
/macro=clean
/macro=rename
/macro=delete
/macro=reportonly

/susmacro= - specify the action to be taken on suspected macro infections.
/susmacro=rename
/susmacro=delete
/susmacro=reportonly

Reporting

/report= - specifies how much information is to be output.
Current available values are:
/report=infected - report only infected files.
/report=all - report all files scanned show all files scanned. (replaces /E)

/logfile - use the default log filename.
/logfile="filename" - specify a log filename.
/nologfile - do not write to a log. (replaces /L and /L=)

Miscellaneous

/exit - InoculateIT PE is to exit on completion of the scan. (replaces /X)
/help - print the command line help. The current /? switch will be kept as it is a fairly standard option.
/cancel - default, allow cancelling of the scan.
/nocancel - disable cancelling of the scan
/waitstart= - Specify the number of seconds to wait before starting,

e.g.: /waitstart=15 will wait 15 seconds

Any path or logfile name specified on the command line that contains any of the following characters
MUST be enclosed in quotes = ; - / (and white space)

Progressive Scan Properties (Options | Program | Start-Up | Configure Prog. Scan)

This dialog allows you to configure how the start-up scan will be performed and what will be reported.

Display

Progress of the scan: This will display InoculateIT PE and show you the details as the scan is performed.

Nothing unless infected: InoculateIT PE will not appear unless it has found a problem with a file.

Number of Files to Scan

First boot: This is the number of files that will be scanned when you first start your PC for the day.

Reboots: This is the number of files that will be scanned if you re-boot your PC throughout the day.

Log File

Write log file: By selecting this option you can either select the browse button to specify the name of the log file, or you can type in the path and file name that you wish to call the log file.

Allow Cancellation of Progressive Scan

If this option is NOT selected (NOT checked) you will not be able to stop the scan until it is finished.

Real-Time Protection

The InoculateIT PE suite includes memory Real-Time programs to automatically check files and floppy disks for viruses. Settings for these programs are controlled by this dialog.

The Real-Time Protection Options dialog is initiated by selecting **Options | Real-Time Protection** from the menu. Each of the dialogs can be entered by selecting the appropriate tab at the top of the dialogs.

Enabling	More information
Floppy boot sectors	More information
File Monitoring	More information
File virus action	More information
Macro virus action	More information
Reporting	More information

Enabling (Options | Real-Time Protection | Enabling)

Enable Real-Time floppy disk boot sector protection

You can configure the floppy disk protection by selecting Options | Real-Time protection | Floppy Boot Sectors. Real-Time floppy protection settings

Enable Real-Time File Monitor (File & Macro protection)

This will allow InoculateIT PE to automatically check files, documents and spreadsheets for viruses as they are accesses by Windows.

File monitoring

File virus actions

Macro virus actions

NOTE: Some installation programs recommend that you disable your anti-virus protection before attempting to install their software. Please scan the floppies or CD BEFORE disabling the Real-Time protection as they may be infected with viruses. `Shrink wrapped' software has been found to be infected in the past.

To "Disable your Antivirus software" remove the checks from each of the Options | Real-Time protection | Enabling options, then close InoculateIT PE and save your changes.

NOTE: You MUST open InoculateIT PE and enable these options once you have finished loading the software as the Real-Time protection is the main component of your anti-virus protection.

Floppy Boot Sector (Options | Real-Time Protection | Floppy Boot Sector)

This dialog controls the checking of floppy boot sectors for viruses. You may choose the level of protection required from the three (mutually exclusive) options. The first option gives adequate protection, whilst the last gives an extremely high level of protection. These options will also contain a message to note if this option is currently loaded.

A known virus Causes InoculateIT PE to consider a boot sector bad only if it contains a known virus. This is the default level of protection.

An invalid boot, sector or known virus Causes InoculateIT PE to consider a boot sector bad if it contains an invalid boot sector or a known virus.

An unknown or invalid boot sector, or known virus This option causes InoculateIT PE to consider a boot sector bad if it contains an unknown or invalid boot sector or contains a known virus.

> **STOP!** Replacing unknown boot sectors may cause problems with some backup programs and copy-protected software. You should only use this setting if you are aware of the potential problems. Please call the InoculateIT PE support line if you have any questions.

Replace any boot sector considered bad Causes InoculateIT PE to replace bad boot sectors. InoculateIT PE will always warn you before replacing a boot sector.

File Monitoring (Options | Real-Time Protection | File Monitoring)

This dialog controls which events will trigger InoculateIT PE's automatic file monitors to scan files. There are three events where files may be monitored for viruses. You may enable as many of these options as you wish as they are not mutually exclusive.

An infected file may trigger more than one of the following options. A warning will be issued from each of the options that is activated, so it is possible for a single infected file to create multiple warnings.

Monitor Activation

If the file is infected with a virus it may activate as soon as the file is opened (macro viruses normally infect normal.dot when the infected file is opened). For this reason Opening will automatically be enabled when you select either Executing or Closing if you are using InoculateIT PE for Windows 95 or 98. InoculateIT PE for Windows NT can be fully configured and will allow any configuration to be set by the user.

Executing programs If a virus is found when a Windows application is run the Real-Time protection will prevent the file from running. If the Real-Time protection only suspects a virus is present you will be given the choice of whether or not to run the file.

Opening files Files with extensions specified in the *File types to scan* box of the Options | Program | File types menu are checked for viruses on opening. If a virus is found, you have the option of proceeding.

Closing files Files with extensions specified in the *File types to scan* box of the Options | Program | File Types menu are scanned for viruses on closing. If a virus is found the filename and the name of the virus will appear in the Report window and the log file if it is enabled.

Scan All Files (This option is available for Windows 95 and Windows 98 only)

This option causes Vet to check each file for viruses as the file is used. As each file is used it will be checked for viruses if this option is enabled. If this option is disabled it may take slightly less time for Vet to scan files (as some types of files will not be scanned before use).

File Virus Actions (Options | Real-Time Protection | File Virus Actions)

Action - Infected Files

Report only: Causes InoculateIT PE to report, but not attempt to clean, infected files.

Report & deny access: Causes InoculateIT PE to report when an infected file is detected and to lock the file so that it may not be used by other programs.

Clean file: Causes InoculateIT PE to attempt to disinfect virus-infected files, returning the files to working order. If the file has been infected by an overwriting virus, InoculateIT PE will delete the file, as no disinfection is possible

Action - Suspected Files

Report only: Causes InoculateIT PE to report, but not attempt to clean, infected files.

Report & Deny access: Causes InoculateIT PE to report when an infected file is detected and to lock the file so that it may not be used by other programs.

If this option is viewed form the InoculateIT PE program is will also have a note to indicate if the option is currently loaded and active.

Macro Virus Actions (Options | Real-Time Protection | Macro Virus Actions)

By default InoculateIT PE macro monitoring will check documents and spreadsheets for macro viruses.

The following mutually exclusive options are available for dealing with documents, spread sheets or databases that are infected, or suspected, of having a macro virus.

InoculateIT PE can automatically detect and clean all Word and Excel macro viruses. InoculateIT PE is also able to detect Access database macro viruses

Action - Infected Documents

Report only: Causes InoculateIT to report, but not attempt to clean, infected documents.

Report & deny access: Causes InoculateIT to report when an infected document is detected and to lock the file so that it may not be used.

Clean file: Causes InoculateIT to attempt to disinfect documents infected with macro viruses, returning the documents to working order.

Suspect Documents:

Report only: Causes InoculateIT to report, but not attempt to clean, infected documents.

Report & Deny access: Causes InoculateIT to report when an infected document is detected and to lock the file so that it may not be used.

Reporting (Options | Real-Time Protection | Reporting)

Write log file

Selecting this option will cause a log file to be written when suspect or infected files are detected by the Real-Time file protection. The log file will record the filename and path of any infected files, and results of InoculateIT PE's attempt to clean the files.

SMTP E-Mail Alerting (Options | Alerting | E-Mail)

This dialog allows you to configure the details of the SMTP email message that will be sent when a virus is detected.   At the end of the report that is produced during a scan, there is a summary of the results. If a virus has been found this summary will be copied into the body of a mail message and sent to the address in the TO: field.

If all of the fields are grey Email alerting has not been enabled on the Alerting.

Mail Configuration:

Mail Server: This is the Name or TCP/IP address of your mailserver. Please call your Network Administrator if you are unsure what to enter.

From: Enter your email address. This is so that when the email is sent it is easy to work out which PC it has come from.

To: Enter the email address of your computer support person that you want the message sent to. The email alert can be set to more than one person by placing a semicolon (;) between each of the email addresses that are to be notified.
Ie. SysAdmin@company.com; HeadOffice@company.com

Subject:

This is the Subject line in the email message that will be sent.

Test (send e-mail):

This will send a test message to the address(es) specified in the TO: field. This button is designed to allow you to test that the details you have entered will work when a virus is detected.

Alerting (Options | Alerting | Alerting)

This dialog allows to enable/disable the sending of an Email message when a virus is detected. (Currently email messages can only be sent via SMTP mail protocol)

On-demand scanner:

Alert administrator via email when a virus is found

By selecting (checking) this option you can send an Email when a virus is detected after you have opened InoculateIT PE and started scanning files. In order to successfully send the email alert you must also configure the SMTP Email tab with the details required to send the message.

Real-Time Protection:

Display message box when virus found

By selecting (checking) the "Display message box when virus found" option you will be notified if a virus is detected by the Real-Time protection as you go about your daily tasks.

Alert administrator via email when a virus is found

By selecting (checking) this option you can send an Email when a virus is as you go about your daily work. In order to successfully send the email alert you must also configure the SMTP Email tab with the details required to send the message.

Confirm Configuration Selections

This dialog will display a list with all of the options that the installation intends to install InoculateIT PE with. If you wish to change the settings; click the **<Back** button until you see the dialog with the option that you wish to change, modify the option and then click **Next>** until the Confirm Configuration Sections dialog is once again displayed. Click the **Finish** button to accept the configuration and complete the installation.