NORMAN

Norman Virus Control for Windows 95

User's Guide

Version 4.70

Norman ASA
Mailing address: P.O. Box 43, N-1324 Lysaker, Norway Physical address: Strandveien 37, Lysaker
Tel. +47 67 10 97 00 Fax. +47 67 58 99 40 E-mail: norman@norman.no

Norman Data Defense Systems Inc
9302 Lee Highway Suite 950a, Fairfax, VA 22031, USA
Tel. +1703 267 6109 Fax. +1703 934 6367 E-mail: norman@norman.com

Norman Data Defense Systems GmbH
Kieler Str. 15, D-42697 Solingen, Germany
Tel. +49 212/26718 0 Fax. +49 212/26718 15 E-mail: norman@norman.de

Norman/SHARK BV
Mailing address: P.O. Box 159, NL-2130 AD Hoofddorp, The Netherlands
Tel. +31 23 563 3960 Fax. +31 23 561 3165 E-mail: sales@shark.nl

Norman Data Defense Systems AG
Postfach, CH-4015 Basel, Switzerland
Tel. +41 61 487 25 00 Fax. +41 61 487 25 01 E-mail: norman@norman.ch

Norman Data Defense Systems Pty. Ltd.
6 Sarton Road, Clayton, Victoria, 3168 Australia
Tel. +61 3 9562-7655 Fax. +61 3 9562-9663 E-mail: norman@norman.com.au

Limited warranty

Norman guarantees that the enclosed diskette/CD-ROM and documentation do not have production flaws. If you report a flaw within 30 days of purchase, Norman will replace the defective diskette/CD-ROM and/or documentation at no charge. Proof of purchase must be enclosed with any claim.

This warranty is limited to replacement of the product. Norman is not liable for any other form of loss or damage arising from use of the software or documentation or from errors or deficiencies therein, including but not limited to loss of earnings.

With regard to defects or flaws in the diskette/CD-ROM or documentation, or this licensing agreement, this warranty supersedes any other warranties, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

In particular, and without the limitations imposed by the licensing agreement with regard to any special use or purpose, Norman will in no event be liable for loss of profits or other commercial damage including but not limited to incidental or consequential damages.

This warranty expires 30 days after purchase.

The information in this document as well as the functionality of the software is subject to change without notice. The software may be used in accordance with the terms of the license agreement. The purchaser may make one copy of the software for backup purposes. No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the explicit written permission of Norman.

Table of Contents

Conventions

We use the following conventions throughout this manual:

When we give examples of what you should type in order to use a particular program, the examples look like this:

```
format a: /s /u [Enter]
```

We designate certain keys by surrounding the keyname with "[" and "]", as in:

[Ctrl]

When we describe a series of menu choices for you to choose, we will use the following:

Start|Run

This means that you should click on "Start" and from there click on the "Run" menu item.

Hints and important notes appear in boxes like the one below:

Note: Here is a hint about how to use NVC95...

Individual words or phrases that we intend to stress are in bold:

This virus is **very** dangerous and will...

System Requirements

Norman Virus Control for Windows 95 can run on any machine that runs any national language version of Windows 95 or Windows 98.

About This Version

The Scanning Engine

The scanning engine has yet again undergone substantial changes. The most prominent improvement is boot sector cleaning. In previous versions, we used the DOS-based program NVCLEAN for removal of boot sector viruses. As of this version, the scanning engine itself can repair infected boot sectors. NVCLEAN is removed altogether.

Removing boot sector viruses is not riskier than removing a binary file virus, for example. However, if things go wrong, a damaged boot sector is a serious situation. For this reason we do not allow *automatic* repair of boot sector viruses. Whenever you order NVC to remove a boot sector virus, you will be prompted for backing up your current boot sector. We'll spare you the details until the situation occurs, and guide you from there.

Other changes to the scanning engine are:

- Support for Excel Formula viruses
- Extended detection of polymorphic macro viruses

Live Update of NVC

Updates to the scanning engine (definition files, DLL/VxD) are still available from our web sites. In addition, we introduce a polling program, Norman Internet Update, that automatically will check for updated files on Norman servers. This program requires that you're connected to the Internet, and it's available for Windows 9x and Windows NT.

Please refer to "Updating NVC" on page 127 for more information about this feature.

General

As always, there are a number of bug fixes and minor changes to the program. Please refer to the readme text file for an overview.

Norman Virus Control for Windows 95

Microsoft Windows™ is a familiar sight on desktops around the world. The newest addition to Microsoft's operating systems is Windows 98. Although Windows served as the basis for the design of Windows 95/98 (from now on referred to as Windows 9x), Windows 9x has many more features. In addition, it is an operating system, whereas a Windows installation depended upon the presence of DOS. The main difference between the two, from an anti-virus product's perspective is that Windows 9x has full 32 bit memory addressing and is a multi-threaded, preemptive multi-tasking operating system.

A *thread* is a sub-unit of a *process* (application), and Windows 9x can use CPU cycles more efficiently to service threads.

Multi-tasking is the ability to execute applications simultaneously. In Windows 3.1 and Windows 3.11, multi-tasking is *cooperative*, meaning that one application can use the CPU at the cost of another application. *Preemptive* multi-tasking — found in Windows 9x — is a process by which 9x takes control of the CPU allotment and preempts applications. The result is a smoother running system and the ability to run simultaneous applications without worrying about their toll on the system.

In addition, Windows 9x is a more stable environment. Unlike Windows 3.1 and Windows 3.11, if one Windows application crashes in Windows 9x, it is not likely to bring the entire Windows 9x system down. In Windows 9x, all 32

bit applications are protected from the behavior of other applications. However, when running 16 bit Windows applications in Windows 9x, one 16 bit application's crash can bring down any other 16 bit application.

Other Windows 9x features worth noting from an anti-virus product's perspective are its backwards compatibility with DOS and Windows 16 bit applications and its support for 8+3 filenames and long filenames.

Even though Windows 9x can support 16 bit Windows applications, the advantages of a 32 bit operating system call for 32 bit applications to be written. Therefore, Norman has developed Norman Virus Control for Windows 9x (NVC95).

NVC95 is a true 32 bit application which was specifically designed to run under Windows 9x.

Functions in NVC for Windows 95

NVC95.EXE and its supporting programs will be installed into the C:\NORMAN\ directory, and \WIN95, \DOS, and \NSE subdirectories by default, and its icons appears in the Norman program group. During the installation process, however, you will be given the opportunity to specify an installation directory of your own choice.

NVC for Windows 95 is comprised of several functions:

- Windows scanner

  A true Windows 9x virus scanner that takes advantage of the Windows 9x 32 bit environment.

  The scanner detects all viruses contained in NVCBIN.DEF and NVCMACRO.DEF (our virus definitions files), and can be configured to remove viruses automatically.

  You can also use the Windows scanner to perform on-demand and scheduled scans.

You may even create your own icons which run NVC95 with certain command line parameters.

- Right-click scanner for on-demand scanning.
- Command Line Scanner

  The command line scanner is not dependent on any other modules. It can send virus alert information to FireBreak through IPX communications, SNMP traps (except for the Windows 3.1x version), and it can be run from batch files. For more details, see "Norman programs and IPX communications" in the *Administrator's Guide*.

- Cat's Claw

  Cat's Claw is an on-access (real-time) scanner.

  Cat's Claw will scan for viruses in files and boot sectors. Whenever possible, an infected file is repaired before the file is handed over to the application.

  If repair is not possible, you will receive a message and access to the infected file is blocked.

- Smart Behavior Blocker

  Resident, smart behavior blocking™ device driver. Monitors activity and intercepts virus-like behavior. Protects against known and unknown file viruses. Detects known and unknown boot viruses on hard drives and diskettes. Also removes known and unknown boot viruses from diskettes.

  This is the cornerstone of NVC's anti-virus protection.

  Does not identify viruses by name. Use one of Norman's scanners for identification.

- Scheduler

If you wish to schedule automatic scans for specific dates and times, use the scheduler function. You may configure scans to run once, hourly, daily, weekly, or monthly. You may even configure several "styles" to run daily.

- A Book on Viruses in Windows help file format
- Help file for NVC for Windows 95
- Virus Library
- Display function
- Norman Internet Update

Note: If you have used NVCW.EXE, Norman's anti-virus scanner for Windows 3.1x, then you will notice the absence here of a supporting file called NVC.INI. NVC.INI contains all of NVCW's configurations, but this is not necessary in Windows 9x because NVC95's configurations are stored in the Configuration Registry.

Installing NVC for Windows 95

What's Right for You?

The default installation of NVC for Windows 95 consists of a scanner, a scheduler, a real-time scanner (Cat's Claw), and the Smart Behavior Blocker. Together, these functions provide a satisfactory level of protection.

In addition, you can optionally install Canary for generic virus detection.

Before Installing

1. Many anti-virus products are incompatible. Therefore, if you have a version of an anti-virus product other than Norman's installed, you should uninstall this before installing NVC.
2. If you abort the setup program during the installation, the files already copied to your hard drive will not be automatically removed.

IMPORTANT:

You should **always** disable The Smart Behavior Blocker (SBB) before you install new software applications. Installing new software frequently involves making changes to memory, files, and boot sector monitored by the SBB. The SBB can mistake attempts to write to these areas for virus-like behavior, and therefore intercepts the installation.

Remember to reload the Smart Behavior Blocker when the software installation is complete.

Step by Step

Note: If you receive your NVC version on CD-ROM, then follow the installation procedure in the CD booklet.

1. Close all Windows applications. From Program Manager you choose Start|Run. On the command line, type:

   ```
   a:setup
   ```

2. Norman Virus Control will start to install.
3. Follow the instructions on the screen.
4. The default installation is Typical. This choice provides the basic level of protection and is sufficient for most users. The following modules are included in the Typical installation:
   - Norman Virus Control (NVC), which includes the following functions:
     - Windows scanner
     - 32 bit command line scanner
     - scheduler
   - Norman's Smart Behavior Blocker
   - Help Files for NVC
   - Cat's Claw
   - Right-click scanner
   - Norman Internet Update (See number 6 below.)

If you want to customize your installation, you can choose from additional modules in the display "Select Components". Check the [ ] **Custom** radio button.

Please refer to the section "Functions in NVC for Windows 95" on page 5 for an explanation of the functionality.

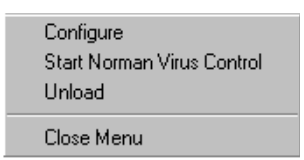
Currently installed components of Norman Virus Control will be updated. If no previous version of NVC is found on your system, the radio button [ ] **Update** is grayed out.

5. If you selected [ ] **Typical** installation, you can choose directory for the NVC files from the display "Choose Destination Location". Click on the **Browse** button and choose directory for installation.
6. When you install Norman Internet Update (NIU) you will be presented with the option of adding it to the Startup group. If you choose Yes (default), NIU automatically checks for upgraded definition files on Norman servers 5 minutes after you have started the PC. See "Norman Internet Update" on page 127.
7. Before the display "Setup Complete" appears, the Smart Behavior Blocker is loaded into memory. By default it is also placed in the StartUp folder to ensure that it is always active.

   When the Smart Behavior Blocker is active, you will see this icon in the notification area:

   Click once with the right mouse button, and you will see:

   From here, you can configure the Smart Behavior Blocker, start the anti-virus scanner for Windows 95, or unload the Smart Behavior Blocker.
8. Norman Virus Control is now installed on your PC. If you want to check possible late changes implemented shortly before the release of this program, then check the [ ] **Read Me File** radio button. You can also launch NVC right away by checking the other available option.

Prevention

Norman believes that preventing virus infections is of utmost importance. As a result, two of the major components in NVC for Windows 95 are:

1. A smart behavior blocker which prevents infections from known and unknown boot and file viruses.
2. Cat's Claw which checks files for viruses before the file is handed over to the application.

Viruses in Windows 9x

Before discussing the concept of behavior blocking there are a few characteristics about viruses in Windows 9x that should be pointed out. For most of the computer virus's lifetime, we have only had to deal with them in the DOS/Windows environment. As a result, for most of us, our experiences with and assumptions about viruses are biased towards DOS/Windows. In Windows 9x, however, we must revise our thinking somewhat. First let us look at the different types of viruses and how they behave in Windows 9x. Then we will discuss how Norman handles these viruses.

File Viruses

There are several different types of file viruses, but the ones that are the most critical to consider are memory resident, direct action, and macro viruses.

Memory Resident

In DOS, a memory resident file virus infects by going into memory, staying there and then infecting other programs.

This is an effective method of propagating because a resident program can see all actions on the PC and has a large amount of control over the PC. Therefore, memory protection is extremely important in DOS.

In Windows 9x, however, there are two issues to consider with respect to memory resident viruses.

When you start Windows 9x, DOS version 7 is loaded first into memory. The DOS portion is the first megabyte of the physical memory. Then Windows 9x and the different applications are loaded into memory.

When Windows 9x is running and you start a virtual DOS session, this session inherits all the properties of the initial start-up session.

In other words, if you started Windows 9x with a resident virus in DOS memory, this virus will be present in **all** virtual DOS sessions you run afterwards.

However, if Windows 9x started from a clean machine (no virus in DOS memory), then a virus that goes resident in a *virtual DOS session* will **not** infect the original DOS memory. In this case, a resident virus will be removed from memory when you close the virtual DOS session.

As a result, pre-checking of the DOS memory area is of utmost importance. Not only will a possible infection appear in all virtual DOS sessions, but a virus in DOS memory may also affect Windows 9x and cause unpredictable repercussions.

Because of the nature of these virtual DOS sessions in Windows 9x, it is no longer necessary to prevent a DOS virus from going resident. That is, in Windows 9x we have virtual DOS sessions which have memory areas that are unique to that particular program. If a DOS virus goes resident when you run a program from a DOS window, you can remove the virus from memory by closing the DOS box. (This is one of the features of Windows 9x that anti-

virus vendors appreciate). When you open a new DOS box you start a different virtual DOS session with its own 1 MB region of RAM, even though it does not look like it to the user. In other words, memory resident DOS viruses cannot infect across DOS boxes.

Therefore, if a DOS program simply goes resident, that action in itself **should not** be dangerous in Windows 9x. The focus should rather be on the damage that memory resident file viruses may perform.

Direct Action

Direct action viruses perform their destructive actions (including continuing to infect other programs) immediately upon running an infected program. In Windows 9x you should be looking for a solution that prevents such actions from taking place.

Macro Viruses

By their nature, macro viruses do not in general change program files, but they may contain code that destroy either programs or the boot area. Therefore, you need a program like Cat's Claw to detect the destruction before it occurs.

The present version of the scanner and Cat's Claw detect and remove file viruses known to NVC.

Boot Viruses

There are two kinds of boot virus detection:

1. On a diskette

   Detecting boot viruses on diskettes is very important because diskettes are the method that boot viruses use to propagate.

2. On a hard disk

   Your anti-virus solution should stop any destructive

action of a boot virus on a hard disk. In addition, after the Windows 9x interface has started, a boot virus resident in a DOS session (but **not** in the physical DOS memory) is removed from memory by Windows 9x when you close the DOS session.

Other Effects of Viruses in Windows 9x

Viruses are like any other software and can contain bugs. As a result, it is possible for them to crash Windows 9x.

Behavior Blocking Concepts

Behavior blocking is a relatively new technique in the fight against viruses. One of the reasons Norman uses behavior blocking is that it protects users by warning when an infection is attempted and not simply alerting after an infection has occurred.

Behavior blocking is technically defined as the process of dynamic code analysis. The sequence of actions in a program are monitored to determine if the actions are consistent with the behavior of viruses. The technique used by one behavior blocker may differ from the one used by another, but the underlying principle will be the same: a sequence of code execution will be monitored until it is determined that the sequence is safe or is harmful. If harmful, the code will not be permitted to actually execute and the user will be notified.

Note: Do not confuse behavior blocking with resident scanning. Behavior blocking does not rely on virus scan strings, whereas resident scanning does.

Norman's behavior blocker is "smart" in terms of using statistical analysis to determine the probabilities that particular behavior sequences are those of a virus rather than those of a user. If this statistical analysis were not done, then a behavior blocker might simply halt any action

that writes to a .COM file. The problem with this is that the action might be valid. On the other hand, a simplified view of Norman's smart behavior blocker reasons as follows:

Action	Analysis
A process opens a .COM file.	Nothing suspicious so far.
The process reads to the end of the file and then adds to the end, increasing its size.	Becoming suspicious.
The process returns to the beginning of the file and patches the code to point to the segment that was appended to the file.	Definitely something wrong. Virus-like activity that must be halted, reversed, and reported.

Another advantage of behavior blocking is its long life. Norman's Smart Behavior Blocker uses advanced algorithms so that it need not be updated with the same frequency as with scan string virus scanners. That is, because the smart behavior blocker monitors behavior rather than looking for specific characteristics of each virus, it does not warrant upgrades each time a new virus is written and released.

Norman's Smart Behavior Blocker

As discussed above, the Smart Behavior Blocker does not scan for specific virus patterns in files being run or in system areas. Instead, the Smart Behavior Blocker monitors all activities in the system and is able to recognize all program behavior that represents typical virus techniques. In this way, the Smart Behavior Blocker detects both known and unknown viruses and prevents viruses from infecting.

To date, our behavior blocking technology has been implemented in Smart Behavior Blocker as a DOS device driver. It is not possible to run this SYS file in Windows 9x, and it's not feasible to incorporate behavior blocking into an EXE or a DLL because they have limited access to the operating system. Therefore, we have built our Windows 9x Smart Behavior as a VxD.

A VxD is a "virtual x driver", where x stands for any device driver. VxDs were made available originally because many applications had to access the same piece of hardware. Therefore, drivers had to be made that looked like (virtualized) the hardware to each application. This allowed all the applications to access the hardware in an organized way.

These days, a VxD is more than this. It is more of a general purpose way of doing things in the operating system that you are not allowed to do in a normal application. In other words, the VxD has full rights to the operating system. In Windows 3.x in enhanced mode, VxDs also exist, but they are loaded when you load the operating system — they cannot be loaded dynamically. However, in Windows 9x, you can load VxDs dynamically.

In the section called "Viruses in Windows 9x" on page 11, we described how certain types of viruses behave in Windows 9x. Now let us look at how Norman's Smart Behavior Blocker for Windows 95 reacts to these viruses.

Reaction to File Viruses

Memory Resident

As described above, it is not as important in Windows 9x for us to stop a DOS virus when it goes resident.

Therefore, Norman's Smart Behavior Blocker will see the DOS virus going resident, but it won't alarm at this point. Instead, it will wait until the DOS virus attempts to perform

a destructive action (including attempting to infect) and then warn the user.

Note: Because of the nature of Windows 9x, the Smart Behavior Blocker does not remove DOS viruses from memory. To do so, simply close the DOS session.

Direct Action

Norman's Smart Behavior Blocker will detect these viruses as soon as they attempt to perform a destructive action. At this point, the Smart Behavior Blocker can prevent the action from occurring.

Note: However, the Smart Behavior Blocker will not remove the virus from the original infected program.

Macro Viruses

If the macro virus has a destructive payload (i.e., to modify files or the boot area), then Norman's Smart Behavior Blocker will see the action and attempt to prevent it.

Again, the Smart Behavior Blocker will not remove the virus from the original infected program.

Boot Viruses

The Smart Behavior Blocker will detect and optionally remove boot viruses on diskettes. When the Smart Behavior Blocker is active and you access a diskette, the Smart Behavior Blocker looks at the boot sector of the diskette. If a boot virus is found and you choose to remove the virus, a generic cleaning routine replaces the infected boot sector with a new, special boot sector.

The special boot sector disallows booting from the diskette on which it resides. In other words, if a diskette with the special boot sector is placed in A: and the machine is

rebooted, the machine will boot from C: and not A:, even if your CMOS setting specifies a boot sequence of A: and then C:.

Note: In order to detect the same boot virus on the same diskette on consecutive tries, you must take the diskette out of the drive after the first Smart Behavior Blocker warning.

If a boot virus has infected the hard drive, then it will go resident each time you boot the PC. All Windows 9x DOS sessions inherit the characteristics of the PC as it was when the PC was booted. Therefore, on a Windows 9x PC with a boot virus on the hard drive, the boot virus will become active in memory when any DOS session starts. At this point, the boot virus will attempt to infect any diskettes that are accessed. However, Windows 9x itself will prevent most boot viruses from infecting diskettes.

Because of the nature of virtual DOS sessions, the Smart Behavior Blocker will not alarm on the boot virus in memory. However, if the boot virus attempts to perform a destructive action (excluding infecting diskettes), the Smart Behavior Blocker will intercept the action.

In addition, the Smart Behavior Blocker stops writes to the boot area (Master Boot Sector, System Boot Sector and extended partition table) after the Windows 9x interface has started. However, it will not remove boot viruses from hard drives.

Note: A module within NVC for Windows 95 called NVCPRE.EXE scans the PC's memory before Windows 9x begins. If a virus is found, it is an indication of a boot virus on the hard drive, and the user will be warned.

Generic Identification

Because the Smart Behavior Blocker does not rely on specific scan strings to detect viruses, the Smart Behavior

Blocker does not provide the name of the virus when it issues an alarm. Instead, the Smart Behavior Blocker points you to the name of the infected program or tells you that a boot virus is present. The message that it displays depends on the type of virus that it finds.

In the case of file viruses, the Smart Behavior Blocker attempts to obtain the name of the infected program as well as the violating thread.

As with file viruses, the Smart Behavior Blocker does not display the name of the boot virus but rather that a boot virus is detected.

Note: To obtain the name of the virus, you must run Norman's anti-virus scanner for Windows 95.

Communication with Other Norman Programs

The Smart Behavior Blocker communicates over the network to Norman Virus Control for NetWare via IPX and SNMP messages.

Loading the Smart Behavior Blocker

The installation procedure automatically places the Smart Behavior Blocker (SBB) in the Startup group so that it is loaded automatically when Windows 9x starts.

If your Startup group contains multiple programs, and you wish to launch certain programs before the SBB, you can delay the SBB by entering the following command:

```
NORMISA /DELAY:10
```

The SBB will then wait for the specified number of seconds before it starts. SBB will wait for 5 seconds before it's loaded if you don't specify a number with the /DELAY command.

And if you don't want to display the Norman logo every time the SBB starts, enter:

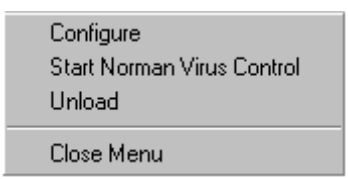
NORMISA /NOLOGO

If you unload the Smart Behavior Blocker and then want to reload it without restarting Windows 9x, simply run NORMISA.EXE from the C:\NORMAN\WIN95 directory.

When the Smart Behavior Blocker is active, you will see this icon in the notification area:

Either double click with the left mouse button or click once with the right mouse button, and you will see:

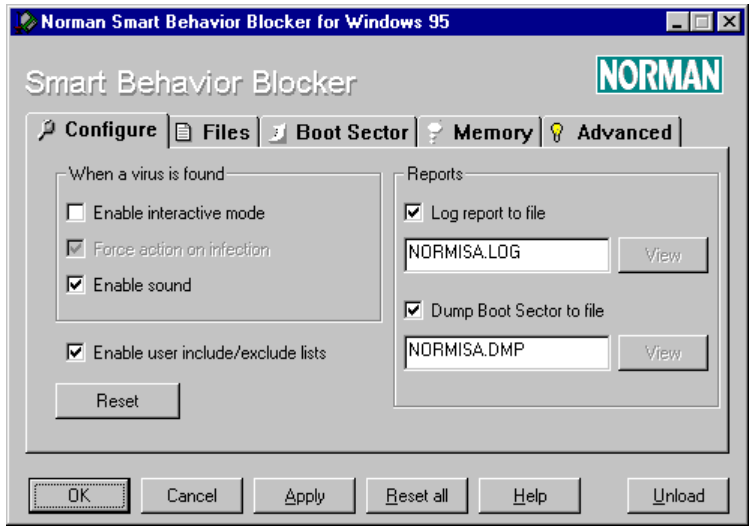
From here, you can configure the Smart Behavior Blocker, start the anti-virus scanner for Windows 95, or unload the Smart Behavior Blocker.



If you want to delete the Smart Behavior Blocker from your PC, use the Uninstall function in Control Panel in Windows 9x.

Configuring the Smart Behavior Blocker

Choose Configure to display the following configuration interface:



Choose from the buttons at the bottom of the screen:

OK will accept all configuration settings and close the Configuration dialogs.

Cancel will cancel all configuration settings and close the Configuration dialogs.

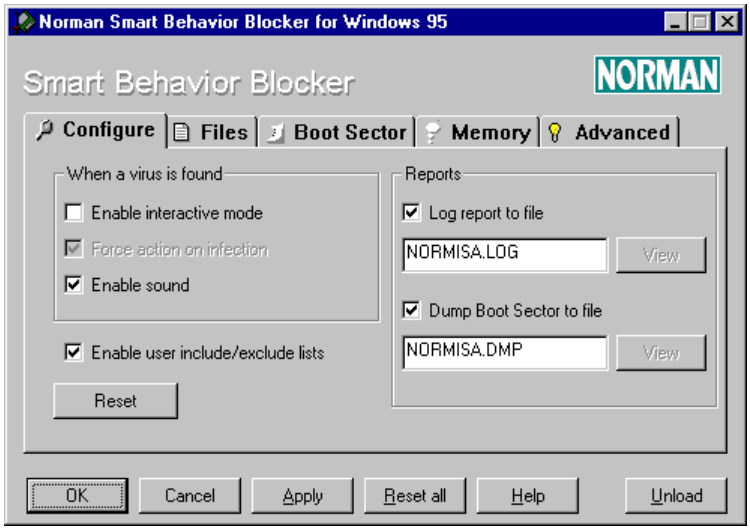
Apply will accept all configuration settings and keep the Configuration dialogs open.

Reset all will reset all configuration settings to their default values and keep the Configuration dialogs open.

Help will display a short help file.

Unload will remove the Smart Behavior Blocker from memory. To activate it again, you must run NORMISA.EXE either manually or place it in the Startup group and then start Windows 9x again.

The Configuration Interface



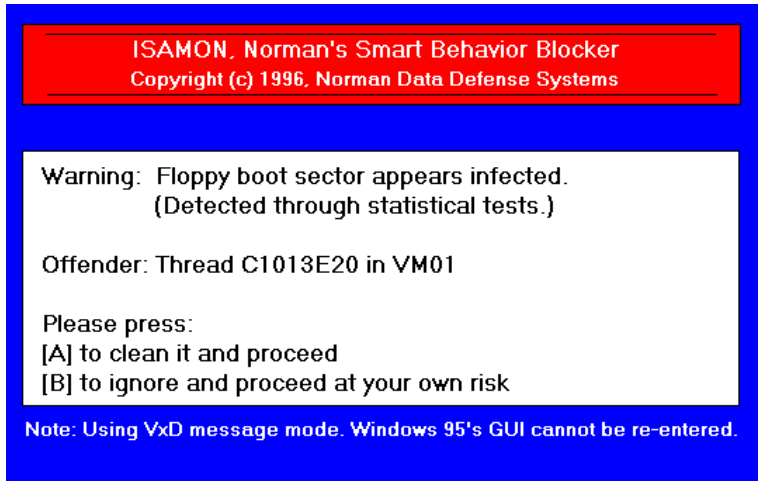
From the configuration screen you can access five different tabbed dialog boxes and specify your basic configuration. These fall into three categories:

1. what to do when a virus is found
2. reporting
3. including/excluding files

When a Virus Is Found

[ ] Enable interactive mode

When you are running in interactive mode, you will be notified and prompted for action whenever the Smart Behavior Blocker detects virus-like activity. Normally, this will consist of two choices.



This warning pops up in “text mode” and not the interface that you are accustomed to seeing. The reason for using text mode here is that when an infecting process is stopped, we need to notify the user, wait for a response, and perform the desired action. The module in Windows 9x that handles this function is not a multitasking function and can therefore only handle one access at a time. You must therefore select an action in order for Windows 9x to resume control.

If you choose to use interactive mode, you have the additional option of turning on the setting

[ ] Force action on infection

Normally, the user has the option to ignore the virus warning and continue with the task at hand without preventing the virus action. However, with this option turned on, the virus warning cannot be ignored.

See the section called “What to Do When the Smart Behavior Blocker Warns” on page 36 for more information.

Note: In Automatic mode you will be notified if the Smart Behavior Blocker detects virus-like activity, but you will not be prompted for action. Instead, the Smart Behavior Blocker handles the problem in the background.

The following is an example of notification under Automatic mode:

In addition, you can choose to have an audible alarm sound when virus-like behavior is detected.

Reporting

[ ] Log report to file

[ ] Dump boot sector to file

You can log both virus incidents as well as infected boot sectors to files. The default filenames are NORMISA.LOG and NORMISA.DMP, respectively.

If you so choose, you may view the most recent NORMISA.LOG from this menu.

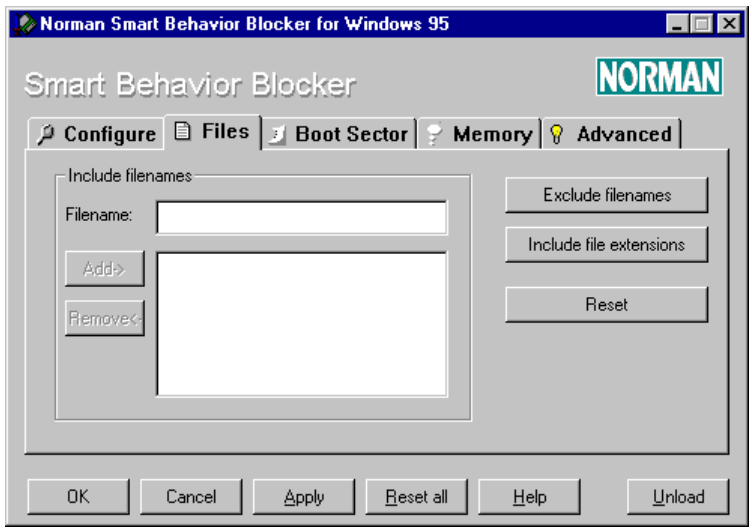
Note that you can view NORMISA.DMP only if a boot sector virus has been detected. Dumping a boot sector to a file is not dangerous, and you cannot spread the boot virus in this fashion.

Specifying Files for Special Treatment

[ ] Enable user include/exclude lists

Checking this option in the Configure dialog box makes the "Files" tabbed dialog available. From here, you can specify files that you want to be closely monitored or excluded from monitoring altogether. These could be files that you know are exposed to virus infection, files vital to your system, or files that have produced false alarms.

Click on the Files tab. The following screen appears:



We refer to all areas that the Smart Behavior Blocker monitors as "hot". For example, we have "hot files", "hot extensions", and "hot areas".

"Hot files" are files with the extensions of EXE (with MZ, NE, or PE headers), DLL, VBX, OCX, CPL, VXD, 386, COM, SYS, DRV, PDR and MPD. The Smart Behavior Blocker monitors access to these files (activities that include file creation, deletion, rename and write).

Note: The files CONFIG.SYS and MSDOS.SYS are excluded from all monitoring.

We must take a little detour here and explain how the

Windows 9x shell handles files so that you understand how the Smart Behavior Blocker will react.

Most users will not notice this, but when you press "DEL" in Explorer, the file is not deleted, but rather moved to the Recycle Bin under the same extension but different **filename**. The file will actually be deleted only when you empty the Recycle Bin.

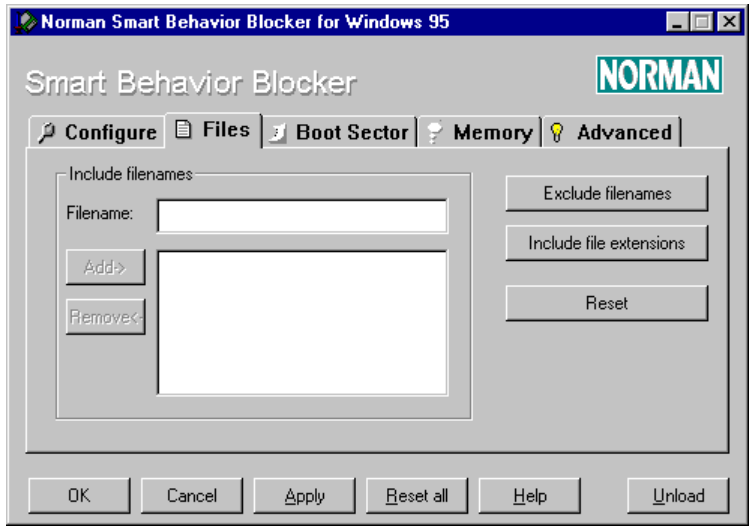
If you have set the Smart Behavior Blocker to "strict" mode (see "Advanced Functions" on page 32), then emptying a Recycle Bin that contains hot file extensions will result in a virus warning.

Since files with these extensions are system properties, options are not provided for the user to include or exclude these extensions. Therefore, users should not name a data file ACCOUNT.EXE, for instance.

Note: If you are a programmer and are working on the file MYPROG.EXE, the following will happen when you link the file:
the Smart Behavior Blocker deletes the file and saves it as a temporary file. When the process is complete, the temporary file is renamed MYPROG.EXE and you may receive a false alarm. This will happen even if you have excluded the file.

If you are having this problem, then please call Norman for help.

From this dialog, there are three different groups of settings:

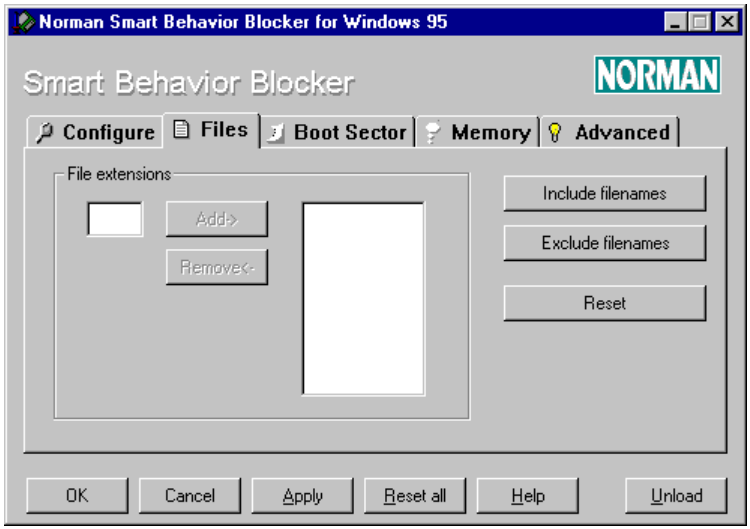


[ ] Include filenames

In this dialog box you can establish up to 16 specific filenames that should be included as “hot files”.

1. Enter a filename (even long filenames) in the Filename box.
2. If you do not specify the path, then ALL files found (even on remote drives) with this name are included.
3. Click the **Add** button to include the file in the list.
4. You may also **Remove** any files that are already in the list.

You may also include up to 16 sets of file types by specifying extensions. Click on **Include file extensions**, and you will see:



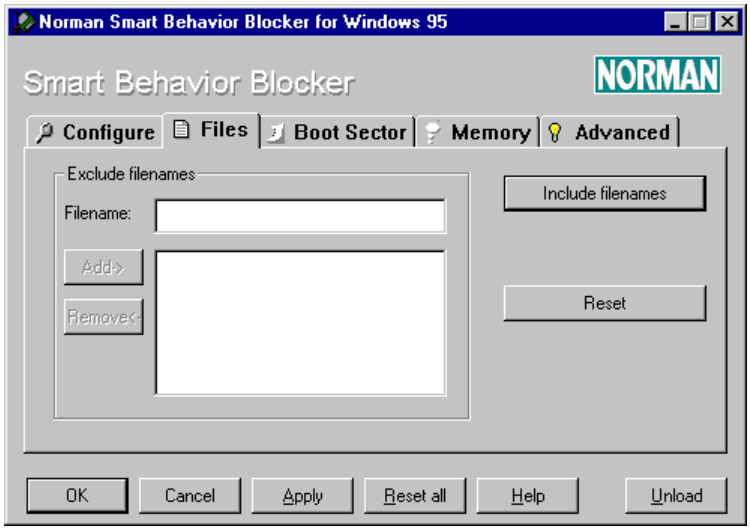
Specify types by entering their file extensions. You do not have to include the leading dot (e.g., `INI`).

Note: If you include a filename and then try to delete the file using "DEL", etc., the Smart Behavior Blocker will warn. To delete the file successfully, unload the Smart Behavior Blocker first or remove the file from the include list.

To navigate to the exclude filenames function from here, click on **Include filenames** and then click on **Exclude filenames**.

Exclude Filenames

From the "Include filenames" dialog, you can click on Exclude filenames from the Smart Behavior Blocker's monitoring.



1. Enter a filename (even a long filename) in the Filename box.
2. If you do not specify the path, then ALL files found (even on remote drives) with this name are excluded.
3. Click the **Add** button to put the file in the list.
4. You may also **Remove** any files that are already in the list.

Note: You can specify a maximum of 16 files to be excluded, but unlike the “Include” functions, you may not exclude groups of files by their extensions.

Precedence of Checking Files

Since you have many options to include files/file extensions and exclude files, it is important to understand how the Smart Behavior Blocker processes these exceptions. The precedence for determining the status of a file is as follows:

1. User specified files for exclusion
2. User specified files for inclusion

3. System specified files for exclusion
4. User specified files by extension
5. System specified files by extension

Specifying Boot Sectors for Special Treatment

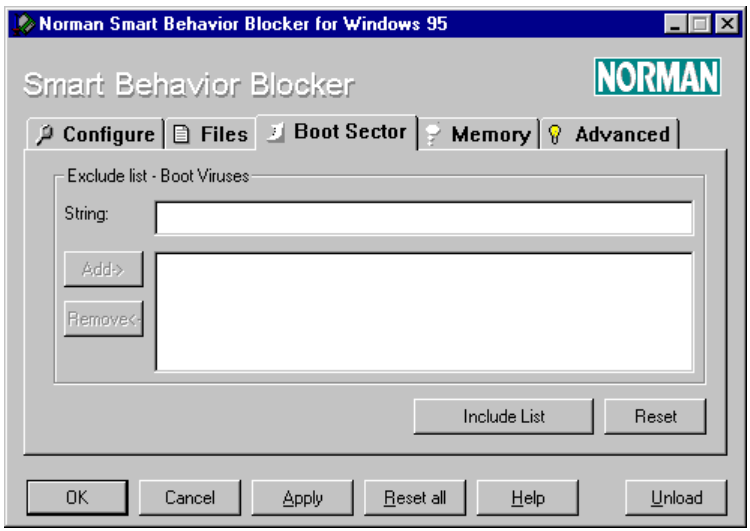
We predict that this function will not be used by end-users but rather by administrators.

"Hot areas" are considered to be the Master Boot Sector, System Boot Sector, and extended partition table. All writes to these areas will be monitored by the Smart Behavior Blocker.

As with including and excluding files, you may also include and exclude certain strings within boot sectors. You can specify a maximum of 32 strings.

Note: This function's purpose is not to exclude detection of certain boot viruses but rather to exclude monitoring of a stream of hex strings that cause false alarms.

Clicking on the Boot Sector tabbed dialog displays this screen:



As with including and excluding filenames, you can toggle between the include and exclude lists.

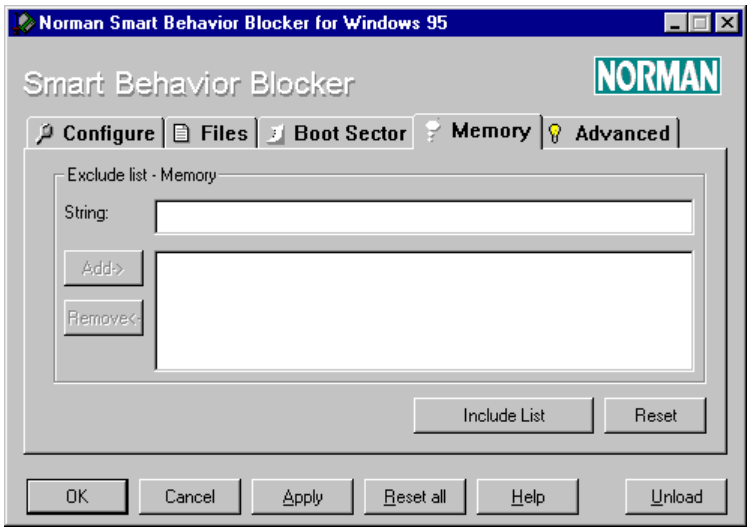
Note: You must enter a hex string in the text box marked "String". All hex strings are to be provided by Norman to our customers. We do not recommend that customers define their own strings.

Specifying Memory Addresses for Special Treatment

This is an extremely advanced feature that end-users will not utilize.

In the event of false positives or false negatives on memory addresses, you may include or exclude up to 32 memory addresses.

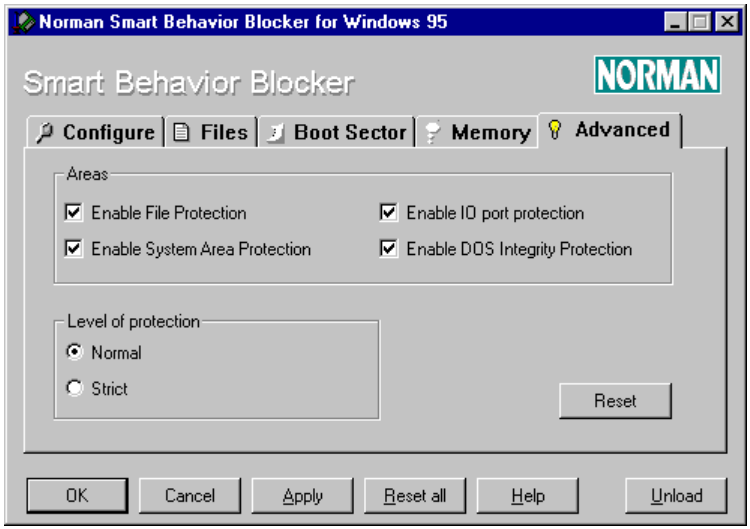
The dialog for specifying memory strings look like this:



Note: As with Boot Sector hex strings, memory address strings must be provided by Norman.

Advanced Functions

These functions are not intended for end-users but rather for administrators.



You can choose settings from two groups:

1. Areas to monitor

   By default, all of these options are turned on.

   When [ ] **Enable File Protection** is checked, then the Smart Behavior Blocker will monitor both the default and user-defined hot files and extensions.

   When [ ] **Enable System Area Protection** is checked, then the Smart Behavior Blocker will monitor modifications to any system area on hard drives and diskettes.

Note: we do not recommend that these two options both be turned off at the same time.

   When [ ] **Enable IO port protection** is checked, then the Smart Behavior Blocker will monitor all attempts to access the diskette drive or the hard drive from the outside (i.e., protecting the software that is handling such activities).

   When [ ] **Enable DOS Integrity Protection** is

checked, then the Smart Behavior Blocker will monitor activity on all critical DOS files.

Windows 9x still very much depends on DOS for some of its internal system housekeeping. Whereas Win32 programs run in their own address space safely hidden in the System Virtual Machine, and all DOS boxes are Virtual Machines which are not supposed to threaten the stability of the Windows 9x system as a whole, all the Win32 programs and DOS boxes still share one copy of DOS. Although this copy of DOS is shared, the TSRs ("terminate and stay resident programs) loaded from the DOS boxes are not. In brief, it is still possible for a virus to modify this one copy of DOS in a way that it will affect all the Win32 programs and DOS boxes. Therefore, it has a system-wide impact. The Smart Behavior Blocker watches for this, but you can turn off DOS integrity protection.

2. Level of protection

   You may choose between two levels of protection:

   Normal and Strict.

   Normal security is the default provides protection for all default hot areas (files, file extensions, and boot areas.

   Strict security is the "paranoid mode" in which no modifications to any hot areas — files, file extensions and boot areas — are allowed.

Note: Regardless of mode, all hot files are treated with strict security.

Following are charts that describe both modes in more detail.

Normal Mode Chart

User action	Smart Behavior Blocker action
Delete hot files and hot extensions	Tracks
Rename hot files and hot extensions	Tracks
Create new COM file exists	Alerts if EXE
Replace existing hot files, hot extensions, and hot areas	Tracks/amends
Write to hot files, hot extensions, and hot areas	Tracks if MZ, NE, COM or SYS. Alerts if PE, LE or W3.

Note that “track” means that the Smart Behavior Blocker will allow modifications to occur until the point at which they are deemed to be as a result of virus-like activity.

Strict Mode Chart

User action	Smart Behavior Blocker action
Delete hot files and hot extensions	Alerts
Rename hot files and hot extensions	Alerts
Create new COM file exists	Alerts if EXE
Replace existing hot files, hot extensions, and hot areas	Alerts
Write to hot files, hot extensions, and hot areas	Alerts

The Configuration Files

It is also possible to configure the Smart Behavior Blocker from the configuration interface as described above, but you can also edit the configuration files manually, if you wish.

- ISAMON.CFG

  This is the default system wide configuration file and is not meant to be edited.

- ISAMON.INI

  This is the default system wide **user** configuration file. The file contains what has been specified in the configuration interface and can be edited from here as well.

- ISAMON.UPD

  This file supplements ISAMON.CFG and should normally not be edited. If necessary, Norman may issue updates to this file between official releases of NVC.

What to Do When the Smart Behavior Blocker Warns

When the Smart Behavior Blocker warns, you will either be presented with choices appropriate to the situation or the Smart Behavior Blocker will prevent the destructive action automatically, depending on whether Interactive or Automatic mode is turned on.

In Interactive mode, we recommend that you always choose option "A" in order to prevent the destructive action from occurring.

When the Smart Behavior Blocker warns, it does not provide the name of the virus. If you want the name, you must run the Windows 95 scanner. Start the scanner from

the Smart Behavior Blocker's menu, or click on the icon in the Norman Virus Control folder.

For more information about running the scanner, refer to the section "Detection" on page 52.

To remove the virus from the original infected file or boot area, you must first unload the Smart Behavior Blocker and then run one of the scanners against it. If you do not unload the Smart Behavior Blocker first, the Smart Behavior Blocker might warn when NVC attempts to remove the virus.

Macro Viruses

Macro viruses is the fastest growing segment among virus makers all over the world. The number of new macro viruses is literally increasing by the hour. While "traditional" viruses in general represent a serious threat, macro viruses are easier to detect and remove - simply because we have the know-how and established technology to handle these viruses.

The macro virus affects *anybody* running applications with a built-in macro language. In other words, if you have installed Microsoft Word or Excel, for example, you are exposed to infections from macro viruses.

This situation is serious. Documents and files are frequently exchanged between users in a network, via e-mail and Internet, and on diskettes circulating between work, home and school. When you open a Word or Excel file containing a macro virus, your machine gets infected.

Norman's solution to the new threat is:

Cat's Claw

Cat's Claw is an on-access (real-time) scanner that detects and repairs binary file viruses and macro viruses, and

detects boot sector infections. This application is based on Norman's established virus protection technology.

Cat's Claw will scan for viruses in files as they are being opened. Whenever possible, an infected file is repaired before the file is handed over to the application.

If repair is not possible, you will receive a message and the application is not allowed to open the infected file.

The present version of Cat's Claw can detect and remove file and macro viruses known to NVC automatically.

Cat's Claw can not remove boot viruses automatically on hard drives, but will guide you through the established procedure for boot sector virus removal. See "About Repair" on page 53 for information on removal of boot sector viruses.

Limitations in This Version

In a Novell network with Novell 32 bits client in Windows 9x, Cat's Claw can not check files from the server.

In an environment like this, Cat's Claw should not reside on the server, but on the workstation.

We recommend that you copy the file from the server to the workstation and access the file locally or use FireBreak on the server.

Configuration Concepts

Users are not a homogenous group, and we therefore provide you with the option of configuring Cat's Claw to best suit your needs. If you run Cat's Claw with the default settings, the following options apply:

- Cat's Claw will be loaded into memory at start-up
- you will be prompted for action when a virus is found

- you will receive a warning if Cat's Claw is unable to scan a file
- uncertified macros will not be removed

The following discussion covers the different dialogs and their options. Cat's Claw is not equipped with default options that we believe provide the optimal protection for you. One reason is that users have very different needs, another is that regulations in some countries do not allow a program to remove files without the user's explicit consent. This legal restraint is blocking our wish to set automatic removal of viruses as default option.

About Warnings from Cat's Claw

The following discussion will guide you through the configuration option and thus provide you with a better understanding on how the application works. Cat's Claw will always warn you about what's happening by displaying dialog boxes. You will only see a couple of examples of warnings from Cat's Claw. However, all possible warnings are described, and if or when they pop up, click on help for assistance.

Cat's Claw Factory Settings

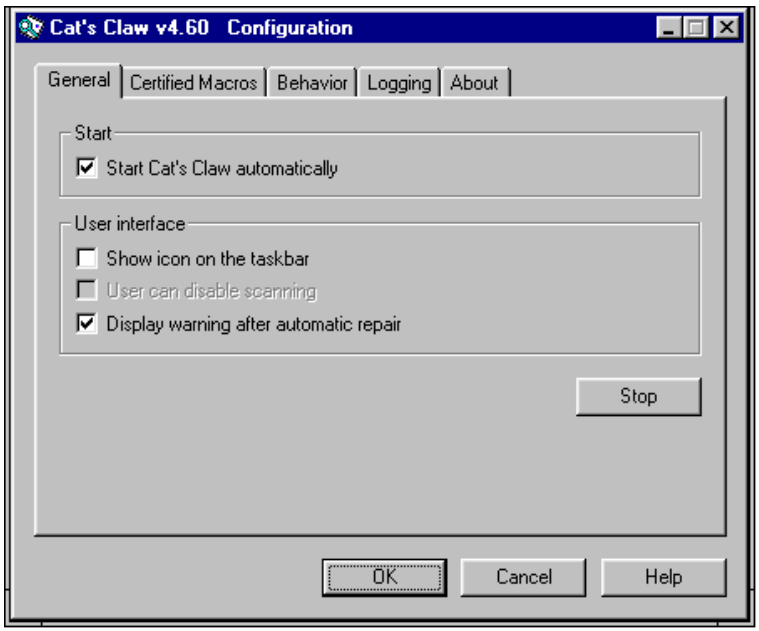
The factory settings in the Cat's Claw configuration program should not be considered as recommended options.

From a security point of view, we strongly recommend that you check the option [ ] **Load Cat's Claw on startup** in the tabbed dialog General.

However, you should use the configuration options to make Cat's Claw work smoothly and efficiently on your PC anyway.

Configuration Dialogs

To access the configuration tabbed dialogs, double-click the Cat's Claw icon in the Norman program group, and you will see:



General

[x] Start Cat's Claw automatically

If you want Cat's Claw to be active on your system at all times, then run the application with this default option on to ensure that Cat's Claw is loaded into memory when you start your machine.

[ ] Show icon on the taskbar

For a visible confirmation that Cat's Claw is active, you can check this option to display an icon like this on your desktop.

[ ] User can disable scanning

If you're an administrator and don't want to allow the users to turn off scanning, you should not check this option. The user will then be prevented from disabling Cat's Claw by clicking on the Cat's Claw icon on the desktop.

[x] Display warning after automatic repair

If you select [ ] **Remove virus from file** (see page 49), you will be informed when Cat's Claw has removed a virus from an infected file.

If Cat's Claw is already loaded, the **Start** button will appear as **Stop**.

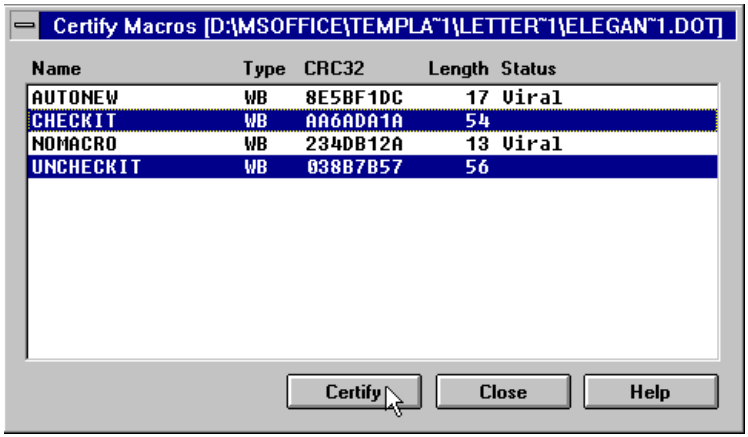
Certified Macros

From this dialog box you can certify the macros that Cat's Claw shall allow in your files. Deciding whether to certify macros or not is a critical decision. Using this function will protect you against new macro viruses not yet identified. We consider this extremely important because new macro viruses pop up every day. On the other hand, 'healthy' but unknown macros can be removed and inflict damage on files. The decision on whether to use the certify macro function is consequently a matter of balancing security versus convenience.

If you certify macros, only these macros will be accepted. See "Handling of Uncertified Macros" on page 46 for more considerations on certified and uncertified macros.

Follow these steps to certify a macro:

1. Click on the **Add** button and choose a file from the Open file dialog.
2. If the selected file doesn't contain any macros, the list box will be empty. Possible macros appear in the Certify Macros list box:



3. Highlight the macros you wish to include and click on **Certify**. You are returned to the Certified Macros dialog.
4. When you highlight a macro in the Certified Macros dialog, the **Delete** and **Comment** buttons become available.
5. Click on **Add** and repeat step 1 through 4 to certify more macros.

Note: If you check the **No action** option in the "Handling of uncertified macros", you will disable the certified macro function.

Fields in the Dialogs for Certifying Macros

There are six fields in the two dialog boxes ("Certified Macros" and "Certify Macros"). Except for the Comments field in the Certify Macros dialog, the information is provided by Cat's Claw:

Status:

There are three types of status that can appear in this field:

1. Empty: if the status field is empty, you can certify the macro.

2. Certified: since this macro is already certified, you cannot certify it again.
3. Viral: macro viruses are made up of multiple macros. This macro is/has been part of a virus and cannot be certified.

Name:

Cat's Claw will use the macro's actual name, or as many characters as possible if it's a long name, to make it possible to recognize for a user.

Cat's Claw will use the following three fields to identify a certified macro. This is internal read-only information.

Type:

Three different types can appear in this field:

1. WB, denoting a Word 6/7 macro
2. VBA3, denoting an Excel 5 macro
3. VBA5, denoting an Office 97 macro

CRC32:

A checksum established as one of the three distinguishing marks for a macro. If the macro is changed after being certified, the changed macro must be certified.

Length:

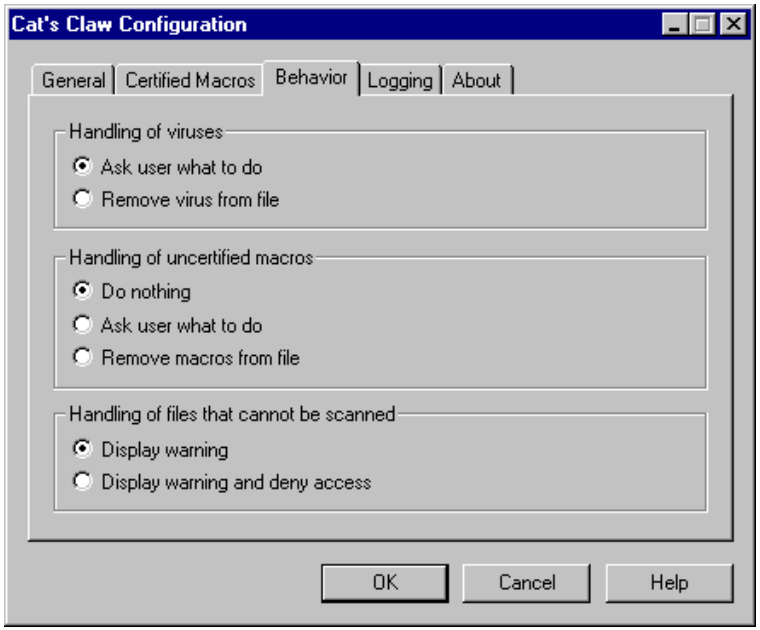
Like any other file, a macro has a certain length. This field displays the macro length used by Cat's Claw to check that a certified macro hasn't been changed after certification.

Comment:

Whatever information you add to a certified macro. This is the only field available for user input.

Behavior

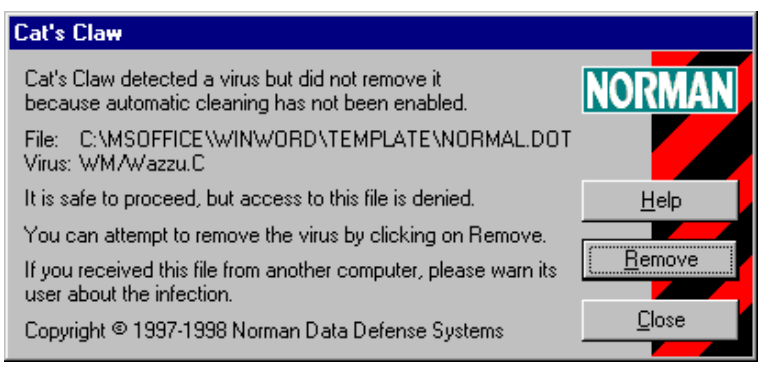
This tabbed dialog box is divided into three sections. This is where you instruct the application how to handle viruses, uncertified macros, and files that cannot be scanned:



Handling of Viruses

[ ] Ask user what to do

If you don't want automatic removal of viruses when you access infected files, you must check this option. When you try to open an infected file, you'll see this dialog:



Manual Virus Removal Warning

You have specified [ ] **Ask user what to do** in the tabbed dialog Behavior, and access to this file is therefore denied. Try to remove the virus manually by clicking on the **Remove** button. Then try to access the file again. For automatic removal of viruses, change your configuration to [ ] **Remove virus from file**.

[ ] Remove virus from file

Checking this option will automatically remove possible viruses from infected files. You will, however, receive a message about the infection.

Virus Removed Warning

If you check the box [ ] **Don't show this message again today** in this dialog, you will not be informed about other possible cleaning operations until you reboot your machine. However, you can keep track of removed viruses by checking [ ] **Viruses removed** in the tabbed dialog Logging.

Virus Not Removed Warning

In some situations Cat's Claw cannot remove a detected virus. When this happens, you will receive a warning.

Note that your system has not been infected, but the file still is. You will never be granted access to an infected file, and it is therefore safe to proceed.

A virus cannot be removed if the infected file resides on a:

1. Write-protected diskette
2. CD-ROM
3. Network drive and the file is write-protected,

   or if

4. The file is in use (i.e., you do not have write access).

Handling of Uncertified Macros

An uncertified macro does not necessarily contain a virus. However, all unknown macros are possible virus carriers, and you can therefore decide how to handle these. If you have certified certain macros, then these are the only macros that Cat's Claw will accept.

[ ] Do nothing

Cat's Claw will not touch the macro, nor inform you about it. Remember that if the macro contains a known virus, Cat's Claw will take action anyway.

Note: The certify macro function is disabled if you choose this option.

[ ] Ask user what to do

Note: If you run with this option on, ALL macros will be removed except for previously certified macros.

With this options checked, Cat's Claw will warn when an uncertified macro is found.

Uncertified Macro Not Removed Warning

The detected macro is not a virus, but it does not appear on your list of certified macros. Your choices are:

1. Click on **Remove** to clean the file.
2. If you want to access the file without removing the macro, check the option [ ] **Do nothing** and try to open the file again.

[ ] Remove macros from document

Note: If you run with this option on, ALL macros will be removed except for previously certified macros.

When you open a file with an uncertified macro, you will receive the:

Uncertified Macro Removed Warning

Cat's Claw removed macros from this file because:

1. They did not appear on the list of certified macros.
2. You checked the option [ ] **Remove macros from document** in the tabbed dialog Behavior.

With this option checked, Cat's Claw will remove all macros not specified in the tabbed dialog Certified Macros.

Other Messages on Uncertified Macros

Other situations may stop removal of uncertified macros even if you have specified removal:

Cannot Remove Uncertified Macro Warning

The macro(s) cannot be removed if they reside on a:

1. Write-protected diskette,
2. CD-ROM,
3. Network drive and the file is write-protected,

or if

4. The file is in use (i.e., you do not have write access).

Handling of Files That Cannot Be Scanned

In some situations Cat's Claw is unable to scan a file. Examples are Word 8 files with password protection, damaged files, or when internal system errors occur. The following options decide how Cat's Claw should react under such circumstances.

[ ] Display warning

When you receive a warning when you access a file, you know that this file has not been checked for viruses. You can, however, proceed at your own risk.

The following are possible warnings from Cat's Claw when you have checked the option [ ] **Display warning**:

Password Protected File Warning

Cat's Claw will not deny access to this file because you selected the option [ ] **Display warning**. You can enter the password and open the file at your own risk. Cat's Claw can not guarantee it's free for viruses or uncertified macros.

Damaged File Warning

Cat's Claw will not deny access to this file because you selected the option [ ] **Display warning**. The file is damaged and has not been scanned. You can open the file at your own risk. Cat's Claw can not guarantee it's free for viruses or uncertified macros.

Internal Error Warning

Cat's Claw will not deny access to this file because you selected the option [ ] **Display warning**. Due to an internal error in Cat's Claw or Windows, the file has not been scanned. You can open the file at your own risk. Cat's Claw can not guarantee it's free for viruses or uncertified macros.

[ ] Display warning and deny access

Checking this option involves that you are warned about an unscanned file, and access is denied.

The following are possible warnings from Cat's Claw when you have checked the option [ ] **Display warning and deny access**:

Password Protected File Blocked Warning

You checked the option [ ] **Display warning and deny access**. Password protection stopped Cat's Claw from scanning the file, and you cannot access it. Possible

solution is changing your configuration to [ ] **Display warning** only and access the file at your own risk.

Note: This situation will occur only when a password protected Word 8 file is detected. Cat's Claw can detect and remove macro viruses from password protected files in Word 6 and Word 7.

Damaged File Blocked Warning

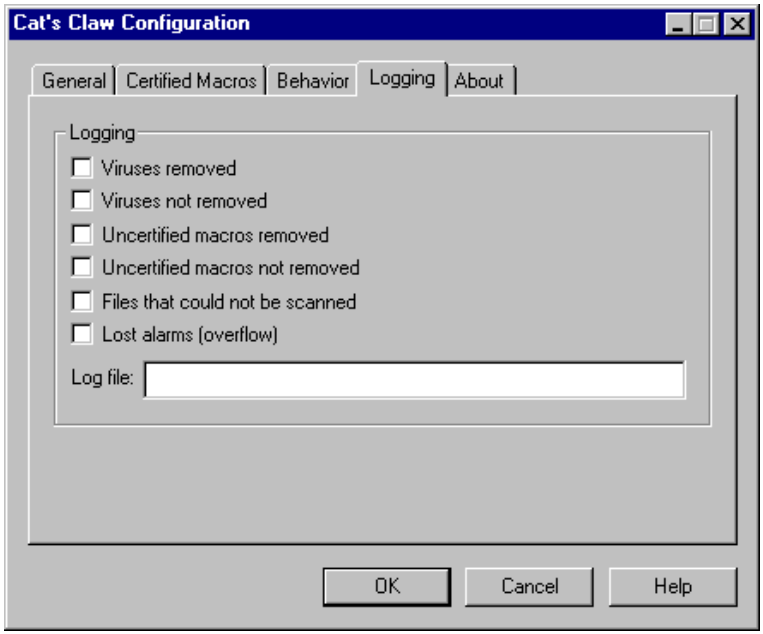
You checked the option [ ] **Display warning and deny access**. Cat's Claw could not scan the file because it's damaged, and you cannot access it. Possible solution is changing your configuration to [ ] **Display warning** only and access the file at your own risk.

Internal Error Denied Access Warning

You checked the option [ ] **Display warning and deny access**. Due to an internal error in Cat's Claw or Windows, the file has not been scanned. Possible solution is changing your configuration to [ ] **Display warning** only and access the file at your own risk, or reboot your machine and try again.

Logging

Cat's Claw will register vital activity in a log file. In this dialog you can decide what kind of information the log file should hold.



As for the other configuration dialogs, you should decide for yourself what kind of information that is important to you.

[ ] Viruses removed

Logs path, file name and name of removed viruses.

[ ] Viruses not removed

Logs path, file name and name of viruses detected but not removed.

[ ] Uncertified macros removed

Logs path and file name of removed uncertified macros.

[ ] Uncertified macros not removed

Logs path and file name of uncertified macros not removed.

[ ] Files that could not be scanned

Logs path and file name of files that Cat's Claw could not scan. Cat's Claw cannot scan files which are:

- password protected, possibly containing macros
- corrupted

[ ] Lost alarms (overflow)

Due to limitations of system's resources assigned to Cat's Claw, a maximum of, for example, 20 alarms can accumulate waiting for user response. If the unlikely situation should occur that you run into e.g. 25 infected files without responding to any of the waiting messages, then you will not be warned from infection number 21 and upwards. This option will give you the *number of infections* that Cat's Claw was unable to handle. If this happens, Cat's Claw will block access to the files rather than ask user what to do.

Loosing alarms does therefore not represent a security risk.

Log file

Enter a valid path and file name for the log file, for example `c:\norman\win95\claw95.log`.

Detection

About Scanning

Scanning is a way to identify viruses that already exist in memory, files, or boot areas. Identifying these by name requires that the scanner recognizes the virus, which means that scanners must be frequently updated for information about new viruses. See "Updating NVC" on page 127 for information on how to get hold of updated files.

The 32-bit scanner can detect and remove unknown macro viruses using heuristic methods. Unknown boot sector viruses and polymorphic viruses are also disclosed by means of this method. When the scanner detects an unknown Word 6/7 macro virus, the virus name will be reported as WM/GENERIC. If the 'Repair file if possible' option is ON, all macros in the document are removed. Through internal testing it has been established that the detection rate for unknown macro viruses is about 80%.

With NVC95 you can scan from the menu-driven Windows scanner, the Right-click scanner, or from the command prompt.

In general, Norman's command line scanner have the same functionality as the menu-driven scanner.

The following section about scanning is based on the functions in the Windows scanner, which is the one most frequently used.

About Repair

Note: In NVC software and documentation, “repair”, “removal”, and “cleaning” are comparable terms. They all refer to the process of removing viruses from files or boot sectors, and restore the infected area to its original condition.

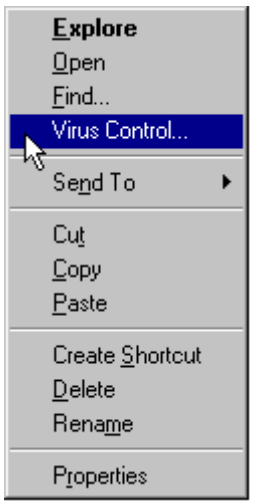
The core technology in all NVC components is the scanning engine. The scanning *options* reflect the capability of the engine. In addition to detect viruses, the engine can also *remove* them (*repair* the file or boot sector, and thereby *clean* the machine). This process is technically more complicated than detection.

If anything goes wrong, repairing a file is less hazardous than repairing a boot sector. A corrupted boot sector may render the system useless. To ensure that a failed boot sector repair will not put you in an awkward situation, we do not allow automatic repair of boot sectors on hard drives.

If a boot sector virus is detected, you will see a dialog box that recommends that you back up the necessary data to a diskette. If the repair fails, you can boot your machine from the restore diskette. A dialog box complete with online help will guide you through the process if a boot sector virus is detected.

In addition to the protection provided for unknown viruses by the Smart Behavior Blocker (see page 15) and the on-access (real-time) scanning by Cat’s Claw (see page 37), you can use the Right-click scanner, the Windows scanner, and the command line scanner for on-demand and scheduled scans. The following sections will cover the use of these scanners.

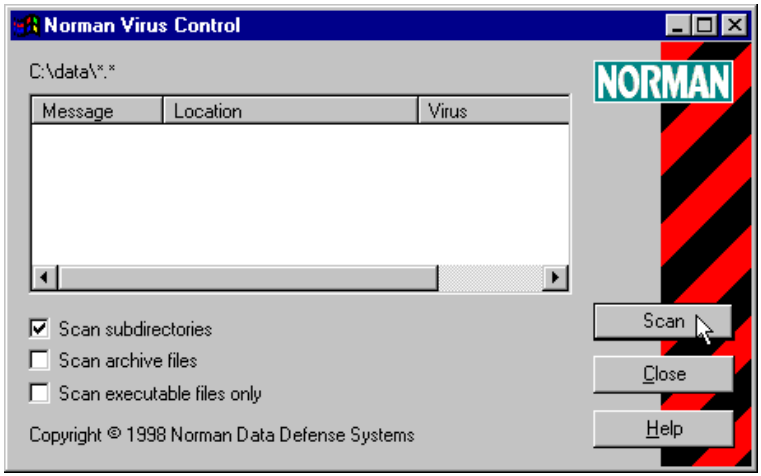
The Right-click Scanner



The purpose of the Right-click scanner is to make scanning easier and more available. You can use it to scan file system objects, like drives, directories, and files. Many users consider virus scanning a necessary evil. Making virus control easier to perform, we believe that the average user will be encouraged to scan more frequently. The Right-click scanner does not require double-clicking an icon or an executable file. Simply select the area you want to scan, for example from Explorer or My Computer, and choose *Virus Control* from the pop-up menu. The Right-click scanner employs the same scanning engine as the other NVC scanners, and therefore provides the same protection as any other Norman scanner.

Using the Right-click Scanner

1. Highlight the object you want to scan, for example a drive, directory, or file. To select more than one object, press the [Ctrl] key and highlight all objects you wish to include in the scan.
2. Click on your right mouse button.
3. Select *Virus Control* from the pop-up menu, and the following screen appears:



Your options include:

[x] Scan subdirectories

If you have selected a drive or directory, check this option to include subdirectories in the scan.

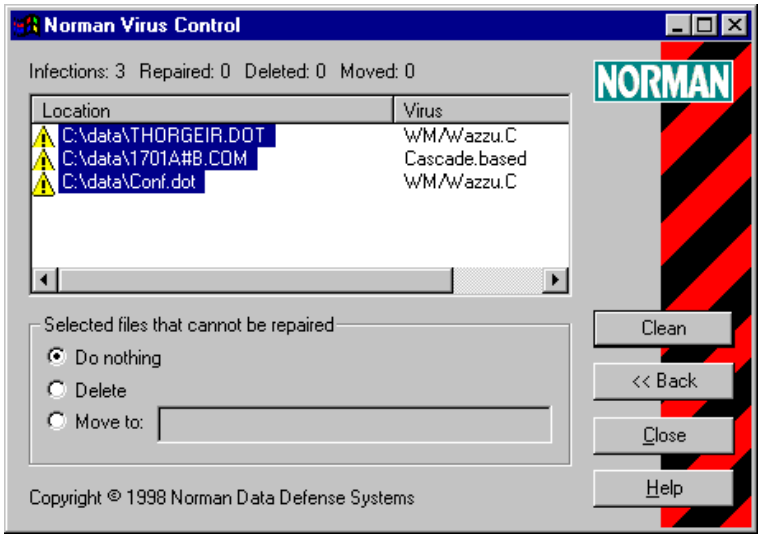
[ ] Scan archive files

Check this option to include archived files in the scan. In this version, only ZIP and ARJ files are supported.

[ ] Scan executable files only

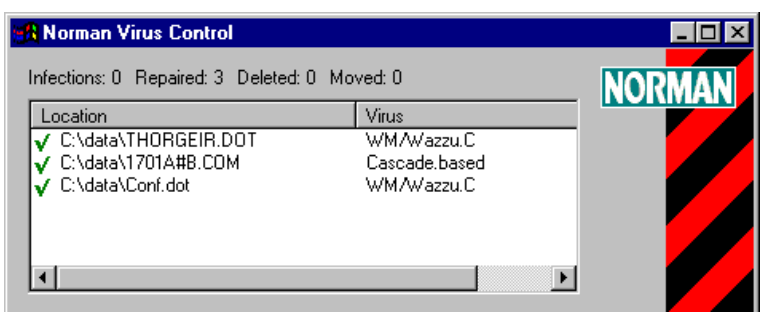
Check this option if you only want to scan executable files.

4. Click on the **Scan** button when you've made your choices.
5. If no viruses are found, the message section of the scanning dialog will inform you about the number of files scanned, files that couldn't be scanned, etc.
6. If viruses are detected, you will see:



The infected files are highlighted, so you can click on the **Clean** button right away to remove the viruses. When a file has been cleaned, it will appear with a green checkmark in the list box. You will also find information on the number of files which are infected, repaired, deleted, or moved.

Note that the scanner will always try repair first. Then, if repair fails, it will perform your selection in the section "Selected files that cannot be repaired". Infected files that cannot be repaired, will therefore be treated in accordance with your choice among the options **[ ] Do nothing**, **[ ] Delete**, and **[ ] Move to**.



Viruses cannot be removed in the following situations:

1. The file resides on a write-protected diskette or CD-ROM.
2. The file resides on a network drive and is write-protected.
3. The file is in use (i.e., you do not have write access).

Note: You can treat the files individually by highlighting certain files for cleaning, others for deletion, etc.

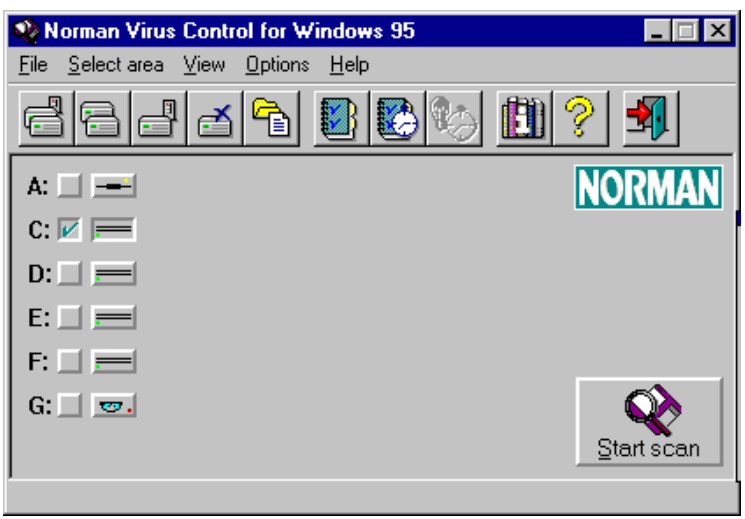
When the **Back** button is activated, you can go back to the scanning dialog to view statistics and possible messages.

Click on **Close** to exit the Right-click scanner.

The Windows Scanner

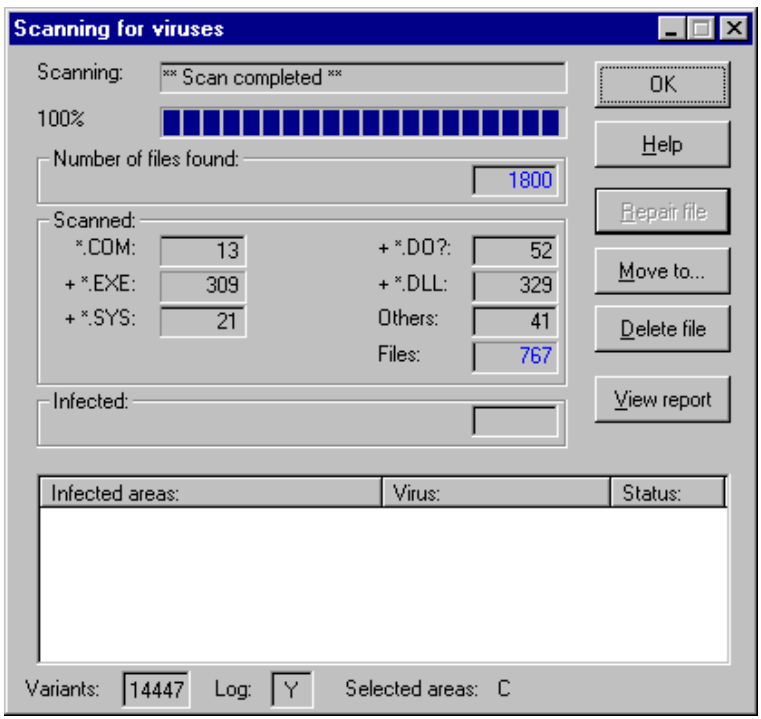
In this section, we'll first give examples of how a normal scan appears. We used all the default options and asked NVC95 to scan the entire C: drive.

From the main window, check the C: drive and then click on **Start scan**:



NVC95 pops up a dialog box called "Scanning for viruses" which shows NVC95's progress as it scans files on the C: drive.

In the uppermost part of the dialog box, NVC95 displays the following information, updating it as the scan progresses:



In the "Infected areas" list box at the bottom of the "Scanning for viruses" display, you will receive information on infected files when you run an on-demand scan. The scanner reports the path and name of the infected file, the virus name, and the status of the infected file.

There are four possible status types:

Status:	Reason:
Repaired	You checked the [ ] **Repair file when possible** option, and the scanner automatically removed a virus.
Deleted	You did not check the repair option, and/or the infected file could not be repaired. You also specified that infected files should be deleted.
Moved to...	You did not check the repair option, and/or the infected file could not be repaired. You also specified that infected files should be moved.
Infected	You did not check the repair option, and/or the infected file could not be repaired, and/or you specified [ ] **No action when virus found**.

If the status is “Repaired” or “Deleted”, the virus is already taken care of. You can check the details in the scanning report.

See “Managing Infections Options” on page 80 for details about options for handling infected files.

If the status is “Moved to” or “Infected”, you still have one or more infected files on your machine. Remove the virus(es) by running the scanner with the option **[ ] Repair file when possible** ON, or highlight the virus in the list box and click the **Repair** button.

If NVC cannot remove the virus(es), you should delete the file(s) altogether.

Note: If an infected file resides on a write-protected diskette, a CD-ROM, or a protected area on a server, the scanner cannot repair, move, or delete the file. When this is the case, the status for the file will always be listed as "Infected".

You can highlight all entries in the "Infected areas" list box, and then click on one of the following buttons: **Repair file**, **Move to**, or **Delete file**. Note that:

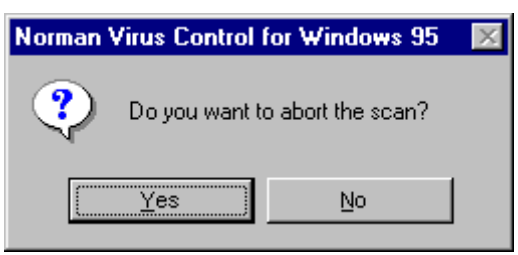
- A repaired file cannot be highlighted to ensure that it's not accidentally deleted.

The following buttons are available in the "Scanning for viruses" display:

Help. Gives direct access to the NVC95 help system, which is context sensitive. That is, when you click the help button, NVC95 brings you directly to the help screen which explains the use of the function you are currently using.

Cancel/OK. This button will appear either as **Cancel** or **OK**, depending on the status of the scanning. Note that you cannot cancel an ongoing scan of zipped files.

While NVC95 is scanning, the button will appear as **Cancel**. When you click on the **Cancel** button, you instruct NVC95 to abort the scan, and the following dialog box will appear:



If you answer **Yes**, NVC95 will abort the scanning process, and the "Scanning" area will now appear as follows:

If you answer **No**, NVC95 will continue scanning.

When you abort an ongoing scan or when the scan is completed, the button will appear as **OK**. Clicking on the OK button closes the dialog box and returns you to the main window.

You may also abort a scan by pressing the [Esc] key.

The following information is also useful during a scan:

Files: the number of files that have been found in the specified location so far in the process.

Scanned: the number of files that have been scanned so far in the process.

Note: The number of files found in the specified directory will almost always be different than the number of files scanned because NVC95 only scans files with certain (default) extensions in addition to the user-specified extensions you specify. Please refer to the Read Me file for more information on which extensions NVC95 scans.

COM:, EXE:, SYS:, OV?:, DLL:, Others: how many files of these different extensions that have been found and scanned for viruses. The total of all these will be equal to the total number of files scanned.

Infected: the total number of infected files that NVC95 has found so far in the process.

Scanning: this shows the area that is currently being scanned.

The dialog box also contains a **progress bar** which shows the percentage of the scan that has been completed.

The list box at the lower part of the screen displays the path and filename of possibly infected files and/or boot areas

along with the name of the virus that has infected these areas. In our example, no infections were found.

If the list of infected files is long, you can scroll through the list box by using the scrollbar or the [PgUp] and [PgDn] keys.

At the bottom of the dialog box is a status line, which summarizes three pieces of information:

Variants: shows the number of viruses and variants this version of NVC95 is able to recognize. See "Finding Out More About Viruses" on page 111.

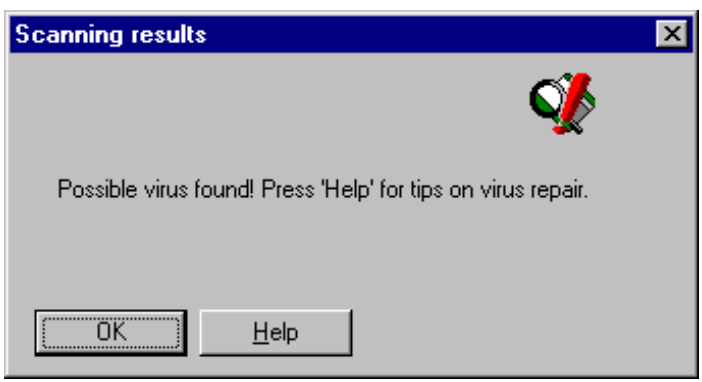
Log: shows you whether or not the report function is activated. This field can have the values **Y** or **N**.

Selected areas: displays the areas that you have selected for the scan.

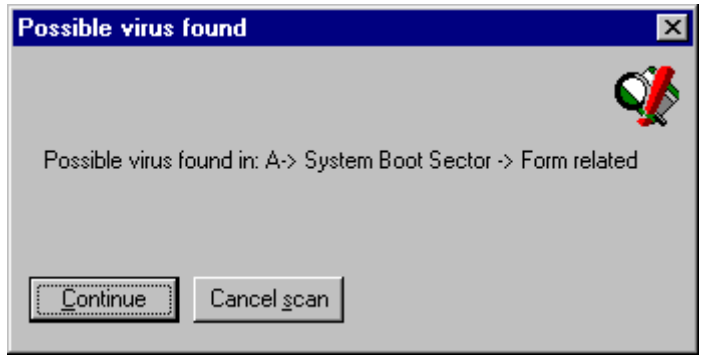
If you are using a style other than the <NORMAL> style for the scan, the name of the style will appear in the title bar of this screen. Refer to "Saving Your Configurations as Styles" on page 87 for more information.

Virus found

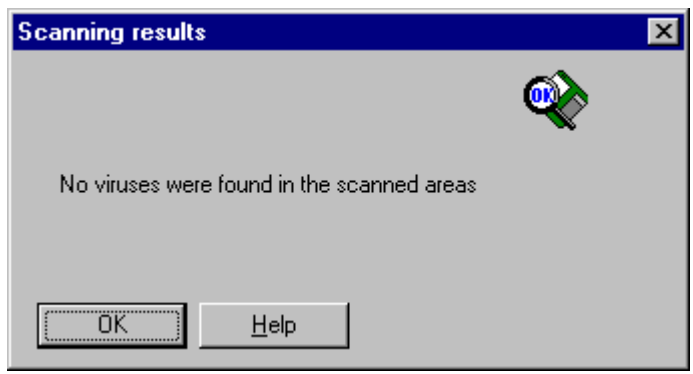
If NVC95 finds a virus, it pops up one of two dialog boxes:



or

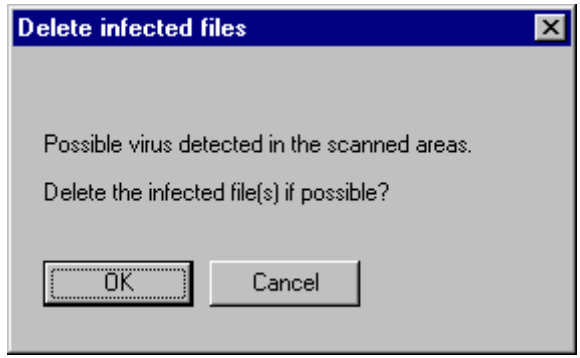


And if NVC95 does not find a virus, it pops up this dialog:



If NVC95 finds an infected file, the following three buttons will be available on the "Scanning for viruses" dialog box when you highlight the infected file:

Delete file: If you did not check the [ ] **Delete infected files** in the Managing Infections tabbed dialog, then highlight the infected file in the list box and click on the **Delete file** button:



Click on **OK** to confirm deletion.

*When you delete a file from the "Scanning for viruses" dialog box, the file is **not** overwritten before it is deleted.*

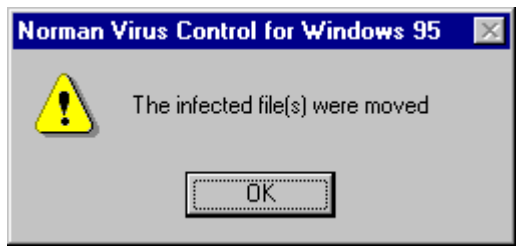
Move to: This button permits you to move selected infected file(s) -- even if you did not set NVC95 to move infected files to a specified directory.

To move an infected file, click once on the file (in the "Infected areas" list box), and then click on the **Move to** button.

NVC95 will ask you to confirm that you want to move the infected file to the directory specified in the "Managing infections" tabbed dialog.

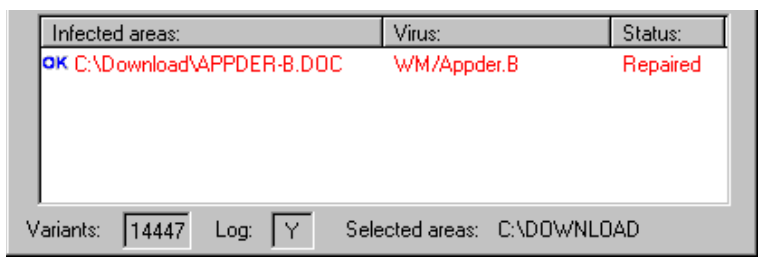
The default directory is `C:\NORMAN\INFECTED`. If you specify a different directory and the directory does not exist, NVC95 will create it. Click on the **Other dir** button to select a different directory.

When you move an infected file, you will see this dialog:



You might have several infected files which happen to have the same name. If NVC95 tries to move a file to a certain directory and finds that the filename already exists in that directory, it will change the name of the newest file until it is unique.

Repair file: This button is activated if you highlight a file infected by a virus that the scanner can remove. Highlight one or more files, and click on the **Repair file** button. The file appears like this in the Infected areas listbox:



Note: If you highlight several infected files, click on **Repair file**, and receive the message "Cannot repair file", try to highlight and repair one at the time.

The scanner is able to remove viruses on-the-fly. When a virus is found, and automatic removal is **not** selected, the infected files will appear in the "Scanning for viruses" list box as infected.

Remember that automatic removal of boot sector viruses on hard drives is not possible. If you're infected by such a virus, follow the instructions on the screen. See also "About Repair" on page 53.

The scanner can detect and remove unknown macro viruses using heuristic methods. When the scanner detects an unknown Word 6/7 macro virus, the virus name will be reported as WM/GENERIC. If the 'Repair file if possible' option is ON, all macros in the document are removed. Through internal testing it has been established that the detection rate for unknown macro viruses is about 80%.

If the scanner is unable to remove a virus, this message appears:

Renaming infected files

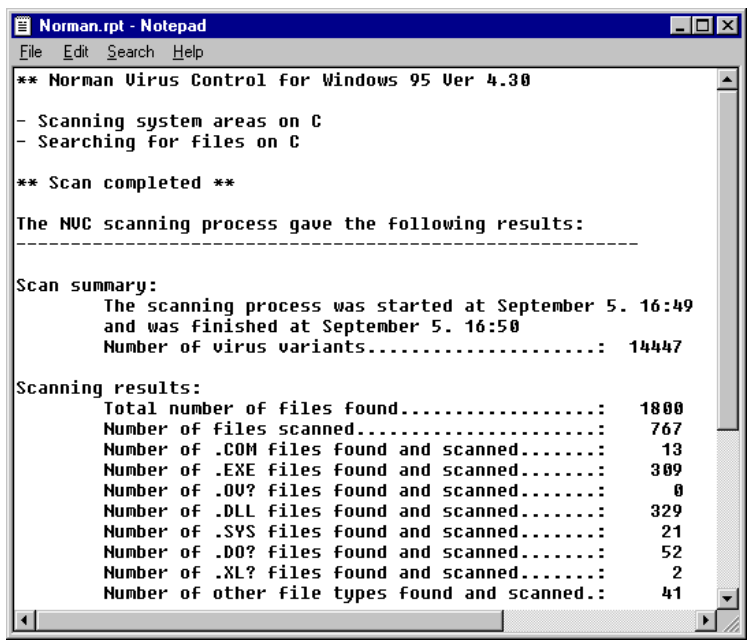
The technique that NVC95 uses increments the first eight characters of the file's name only -- extensions are left untouched. First, if the name is less than eight characters, it is padded with "@" to achieve full length. Then characters are incremented until they reach "Z" -- starting with the last character, going forward.

For example, say you have an infected file named `COMMAND.COM`, and NVC95 moves it to the `C:\NORMAN\INFECTED` directory. Then NVC95 finds another copy of `COMMAND.COM` that is infected and moves it to the `C:\NORMAN\INFECTED` directory. The second instance of `COMMAND.COM` now becomes `COMMAND@.COM`. The third instance would become `COMMANDA.COM`, the fourth would be `COMMANDB.COM` and so on until you reach `CZZZZZZZ.COM`. (But let's hope that you don't have this many.)

View report: If you have chosen either of the report options from the "Reporting" tabbed dialog box in the Scanning options dialog, you have the opportunity to view the report on the screen.

This button appears grayed until the job is done or if the report option is not selected.

After NVC95 has created the report, you can click on the **View report** button, and Notepad will display the report.



You can scroll through the report by using either the scroll bar or the [PgUp] and [PgDn] keys. You can also save it as a different filename, print it, and so on.

Report File Structure

The report file consists of:

- A file header, stating the program name and version.
- A scan report section, containing information about directories and files scanned, and possible virus infections.
- A summary section.

Please refer to the *Administrator's Guide* for more details about the report file structure, and to "Reporting Options" on page 77.

Configuration Concepts

To make the most out of NVC95, you should have a strong understanding of how it can be configured. Before you start a scan, you should set configurations from 3 functional areas:

- Where do you want to scan?
- How, specifically, do you want to do the scan?
- What do you want NVC95 to do if it finds a virus?

Related sections: "Choosing Where to Scan" on page 68, "Configuring the Scanning Method" on page 71, and "Saving Your Configurations as Styles" on page 87.

Choosing Where to Scan

The easiest choice to make is to determine where NVC95 should scan. NVC95 automatically detects all available physical and logical drives and displays them on the left side of the main window.

There are several methods for selecting a drive which is to be scanned. Either:

- click on its associated check box

or

- click on Select area and then choose from the list:

or

- click on a toolbar button

Your choices include:

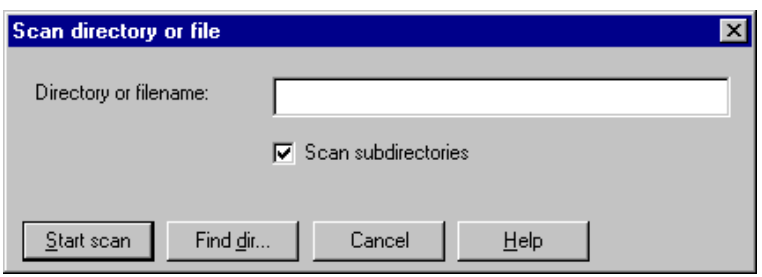
- Local and network hard drives
- Local hard drives
- Network hard drives

- Remove all selections and let you to choose any combination of drives to be specified for scanning.
- Directories/files (use this when you wish to only scan certain directories or files)

Note: When you select network drives, the boot areas of these drives are not scanned.

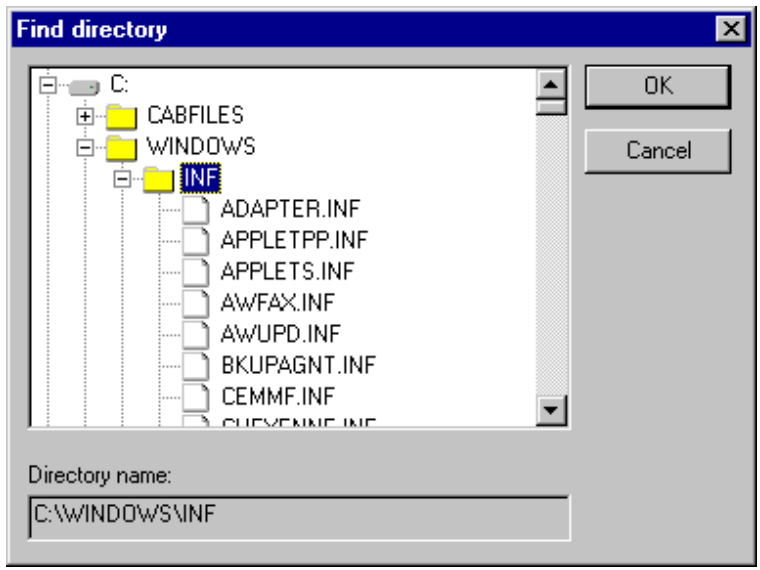
To **deselect** a drive, click on the drive's associated check box, click on Select area|Deselect drives, or click on this toolbar button:

If you choose "Directories/files", then you can:



- type in the name of the directory or file that you wish to scan
- clear the [ ] **Scan subdirectories** checkbox if you do **not** wish to scan directories underneath the directory you specify. This option is turned on by default.

- find the file or directory to scan by clicking on the **Find dir** button:



When you click on **Start scan** back in the “Scan directory or file” display, then the scan will start with the current configurations. These may not be the settings that you wished for this scan. Therefore, when you wish to use the "Directories/files" feature, be sure to set all configurations **before** you select "Directories/files".

Configuring the Scanning Method

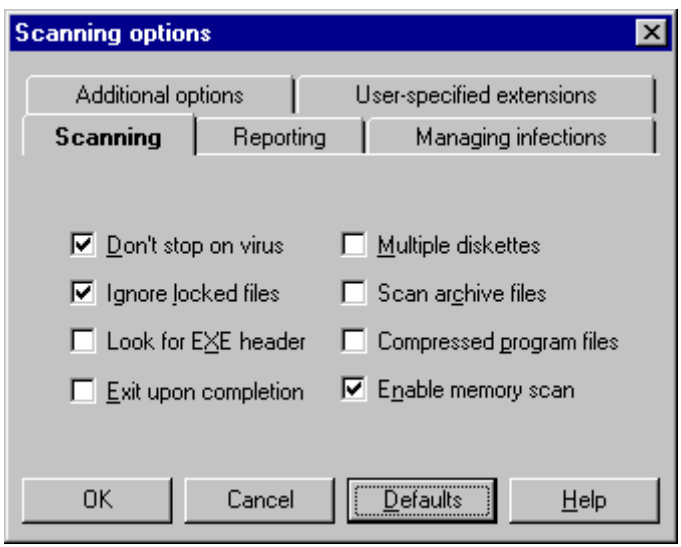
Once you have chosen where you wish to scan, you should determine how you want the scan done.

You can configure the scan using one of two methods:

- click on Options|Scanning options to use the "Scanning options" configuration dialog box

Go to the section "Scanning Options" on page 73 for a more detailed discussion of this dialog box.

Scanning Options Dialog Box



These five dialog boxes contain tabs for configuration screens relating to:

- scanning

- reporting
- managing infections
- additional options
- user defined file extensions

The default settings are:

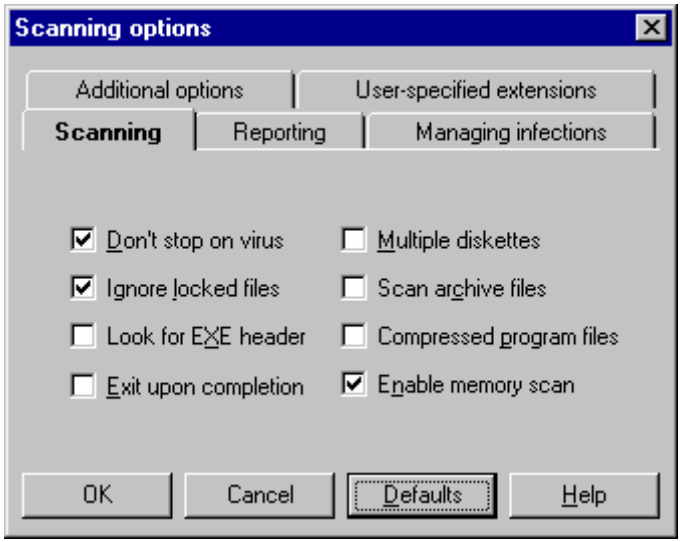
- Don't stop when a virus is found
- Ignore locked files
- Save results to a log file called NORMAN.RPT in the directory in which the scanner resides
- Overwrite previous report(s)
- Log infected files
- Take no action when a virus is found
- Beep when an infection is found

Scanning Options

In the following discussion on scanning options, all default settings are marked like this: **[x] Don't stop on virus**.

When a function has a corresponding command line parameter, it's referred to like this:

Command line parameter: /[parameter]



Available options include:

[x] Don't stop on virus

Click on this option when you do not want to sit and watch the scanner working. This is especially useful when scanning a network. Usually, when the scanner detects a virus, it asks for keyboard input, but in this mode, the scanner does not require keyboard input when a virus is found and proceeds until the scan is done.

Command line parameter: /U

---

[x] Ignore locked files

During normal use, the scanner will stop processing if it cannot open a file. You will see a dialog box showing you which file is locked. At this point, you may press **Cancel** in order to continue the scan but ignore all subsequent locked files.

To avoid error messages when locked files are found, turn this option on.

If you have logging turned on (either report to file or report to printer), then the log will contain the name(s) of the locked file(s).

Command line parameter: /O

[ ] Look for OLE2 header

Files generated in MS Word and Excel can be renamed and thus receive file types other than .doc and .xls, for example, which the scanner is always looking for. However, these files can be identified by their header, which will be OLE2. To detect camouflaged Word and Excel files, which are possible macro virus carriers, this option instructs the scanner to scan files with OLE2 headers.

[ ] Exit upon completion

This is handy when you wish to terminate the scanning session when the scan is complete.

For maximum efficiency, use this option along with the "Minimize while scanning" and "Report only if infection" options. With **all** these options turned on, the scanner will appear as a minimized icon while the scan progresses, a report will be generated only if a virus is found, Notepad will display the report (if it exists), and the scanner will exit when the scan is complete.

[ ] Multiple diskettes

If you have several **diskettes** that you want to check during one scanning session, check this option. You may click on **Cancel** any time you wish to stop.

Any reporting done when this option is checked will result in one report for all diskettes scanned instead of separate reports.

Command line parameter: /R

[ ] Scan archive files

Archiving files is an efficient way to transfer files as well as freeing up space on your hard drive, a diskette, or a server. Since many viruses attach themselves to programs, it is possible to archive an infected file. We provide this option to temporarily uncompress an archived file and scan the files within.

Note: When a file is archived, the scanner can only tell you whether or not it is infected. It cannot take any action on the infected file while it is archived.

The scanner will scan .ZIP and .ARJ files **internally**. This task is performed by the scanner's internal decompression system. The .ZIP and .ARJ files will therefore not be decompressed into "TMP" or "TEMP".

When archived files are being scanned, the **Cancel** button in the Scanning for viruses display is unavailable.

If the archived files are other types than .ZIP and .ARJ, then the scanner automatically reverts to **external** decompression, assuming that you have the archive system necessary for decompressing the archive files you want to scan. It also assumes that these programs are available in your path. If they are not in your path, then the scanner cannot decompress the files.

Command line parameter: /C

[ ] Compressed program files

Many users apply PKLITE, DIET, LZEXE or ICE, for example, to compress executable files. A compressed executable is better protected against viruses because the compression works almost like encryption. Still, if the compressed executable contains a virus, then the virus is activated whenever you run the executable. Even though you can scan for and detect the virus externally, the virus is

still there and will be activated the next time you run the program.

This option makes use of a decompressor emulator to open and scan the file in memory. Scanning compressed program files is more time-consuming than scanning archive files. This is a good reason for not choosing this option unless you have strong reason to believe that a compressed executable is infected.

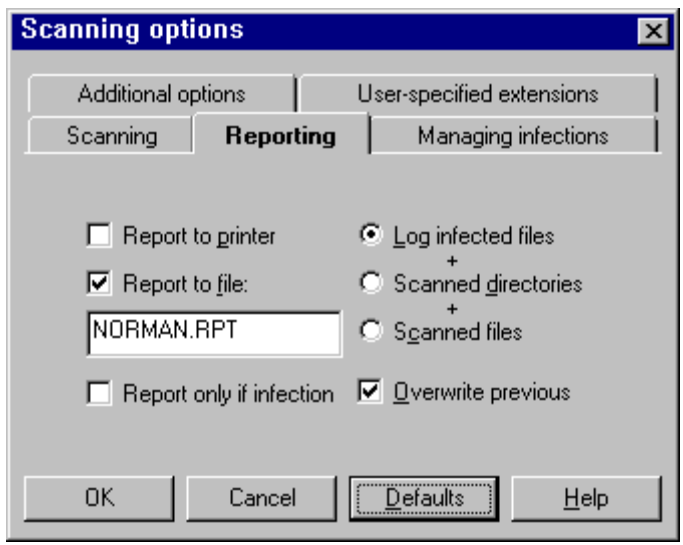
Command line parameter: /CP

[x] Enable memory scan

When you scan the memory area, NVC95 looks for resident viruses. You should always make sure that no viruses exist in memory, and this option is therefore the default.

See the section "Additional Options" for more information.

Reporting Options



If you want NVC95 to give you a status report after a scan, you must choose the [ ] **Report to printer** and/or [ ] **Report to file** option(s).

[ ] Report to printer

The scanner will send its report straight to the default printer that is set up through Windows 95.

[x] Report to file

This default option will create the report NORMAN.RPT in the directory where the scanner resides. You may, however, specify another report name and directory.

Note: NVC now allows the use of UNC (Universal Naming Convention) names and environment variables wherever file and directory names can be entered. Please refer to the *Administrator's Guide* for details.

Command line parameter: /LF

---

[x] Overwrite previous

By default, the previous report is overwritten. If you want to keep track of previous scans on your PC, you should uncheck this option. The report will then be appended to the previous report(s).

If you are running several unattended scheduled scans, you should specify different report names for the different styles or uncheck this option.

See also "Scheduling Several Unattended Scans" on page 98.

Note: If reporting to a file is disabled, then the [ ] **Overwrite previous** option will be grayed.

[ ] Report only if infection

The report will only be generated if an infection is found. If this is turned on, then the only reporting level available is [ ] **Log infected files**. See the list below for more details on reporting levels.

Command line parameter: /LQ

You may choose among three reporting levels:

1. **[x] Log infected files**

   This level will only report the infected files that are found. The report is short and concise.

   This level is the default.

2. **[ ] Scanned directories**

   This level will make a list of all the directories that were scanned *in addition to* all the files that were found to be infected.

3. **[ ] Scanned files**

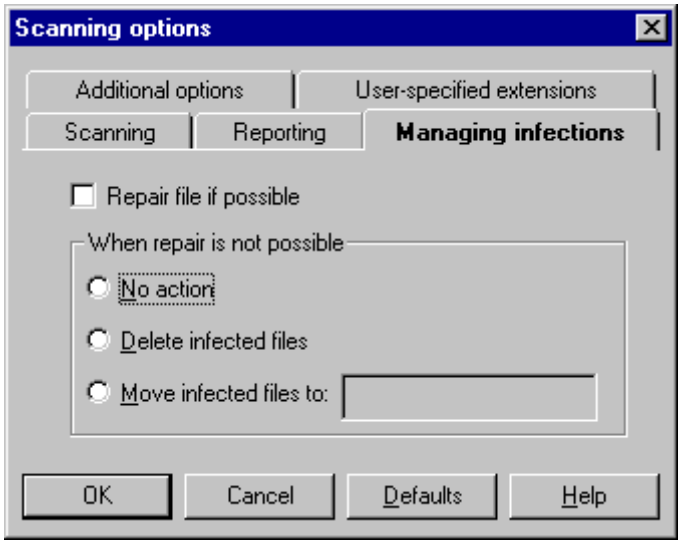
   This level generates a list of all scanned directories and files. Infected files will be specifically marked. Of course, if you scan many files, this report will be quite long.

The "plus" signs between these reporting levels means that when you choose higher levels of reporting, the characteristics of the lower level(s) will be included.

You will see that the reporting level choices on the right side of the dialog box are only available if reporting to file or printer is turned on.

Note: Provided that you selected one of the reporting options, you may at any time view the last report that the scanner generated. Click on View|Report from the main window.

Managing Infections Options



The option of automatic removal of known viruses is implemented in the scanning function. During on-demand and scheduled scans, the scanner will check for known viruses. If a virus is found, the scanner will try to remove it on-the-fly.

Viruses cannot be removed in the following situations:

1. The file resides on a write-protected diskette or CD-ROM,
2. The file resides on a network drive and is write-protected,
3. The file is in use (i.e., you do not have write access).

[ ] Repair file if possible

This option ensures that viruses detected during on-demand or scheduled scans are removed on-the-fly, if possible.

The present version of the scanner *detects and removes* known file, macro, and boot viruses. The 32-bit scanner can also detect and remove unknown macro viruses using

heuristic methods. When the scanner detects an unknown Word 6/7 macro virus, the virus name will be reported as WM/GENERIC. If the 'Repair file if possible' option is ON, all macros in the document are removed.

Through internal testing it has been established that the detection rate for unknown macro viruses is about 80%.

Note: If you select the repair option, the remaining options in this dialog box are valid only when repair is not possible.

Command line parameter: /CL

[x] No action

If you wish to leave infected files alone at the time they are detected, click on the radio button marked [ ] **No action**. This is the default.

Note: Even if you choose not to delete or move infected files in this dialog, you can highlight infected files and delete or move them from the "Scanning for viruses" display.

[ ] Delete infected files

If you wish to delete infected files as they are discovered, select the [ ] **Delete** radio button.

Command line parameter: /D-

[ ] Move infected files to

If you want to move all infected files as they are detected, you must specify the full path name of the destination. Otherwise, the scanner will move infected files into the directory C:\NORMAN\INFECTED.

To do this, click the [ ] **Move to** radio button and specify the path of the destination in the accompanying text box.

Note: NVC now allows the use of UNC (Universal Naming Convention) names and environment variables wherever file and directory names can be entered. Please refer to the *Administrator's Guide* for details.

If the specified directory does not exist, the scanner will create it for you automatically.

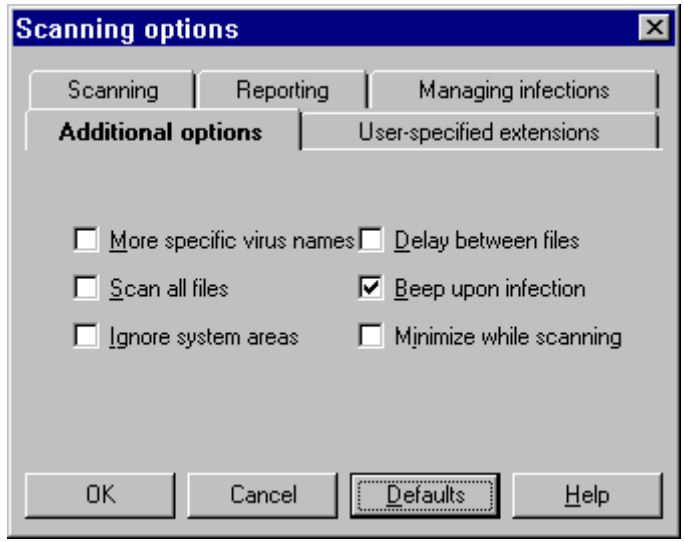
In a network environment, the area that you specify for storing infected files should be off-limits to everyone but the Supervisor.

If you have more than one instance of an infected `COMMAND.COM`, for example, and you choose to move each copy into the same directory, then the scanner will rename each instance of the file as described in the section "Renaming infected files" on page 66.

Command line parameter: /MOV

Additional Options

There are a handful of options that need not be used by everyone, and so we have placed them here:



[ ] More specific virus names

This option allows NVC95 to use secondary virus signatures when it finds a virus, resulting in a more specific name for the virus.

This option does **not** increase the number of viruses detected but does increase scanning time.

Command line parameter: /Y

[ ] Scan all files

One of the goals a virus has is to infect other files. The most efficient way of doing this is to infect executables. Normally, you do not have to scan files other than the defaults. However, when you use this option, NVC95 will scan all files it finds on the specified drive(s). This is a helpful feature if you suspect you have a virus and want to check all files.

Scanning time increases when you use this option.

Command line parameter: /AF

[ ] Ignore system areas

By default, NVC95 scans the system areas (see below for definition) of a diskette or a local hard drive.

In cases where system areas have been severely corrupted, scanning them may cause NVC95 to fail with an error. This option instructs NVC95 to skip these areas and simply scan files.

The system area includes the Master Boot Sector (MBS) and System Boot Sector (SBS).

Master Boot Sector (MBS)

The MBS is located on all physical hard drives.

The MBS contains, among other data, information about the partition table (information about how a physical disk is divided into logical disks), and a short program that can interpret the partition information to find out where the System Boot Sector is located. MBS is independent of type of operating system.

System Boot Sector (SBS)

The SBS is located on all diskette and physical hard drives that are formatted, and it is created with FORMAT.COM. The SBS contains, among other data, a program whose purpose is to find and run an operating system (DOS, UNIX, or OS/2, for example). If the program does not find an operating system to run, the user will be prompted for a diskette with an operating system on it.

Command line parameter: /BS-

[ ] Look for EXE header

More and more often, we encounter viruses that keep track of all activities in individual files. Many look for signatures in .EXE files and make their decision on whether or not to infect based upon what they find (instead of simply looking for a file extension). To detect such viruses, this option instructs the scanner to scan files that have EXE headers.

Note: If you check this option, the scanner will look for the EXE header in **all** files and therefore increase scanning time considerably.

Command line parameter: /X

[ ] Delay between files

If you instruct NVC95 to scan many files, you can use this option to minimize the I/O (read/write from/to disk) load by pausing between each scanned file.

Command line parameter: /W:

[x] Beep upon infection

By default, NVC95 beeps each time it detects an infected file or boot area. Clicking on this check box toggles between turning the beep on and off.

Command line parameter: /B turns the beep off

[ ] Minimize while scanning

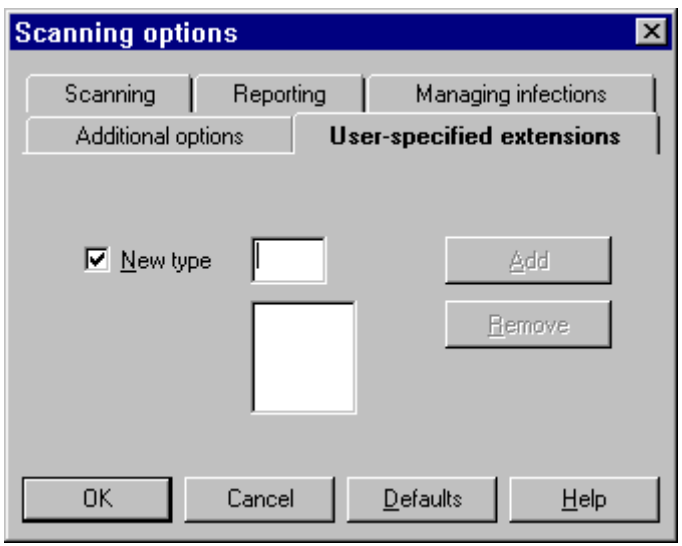
If you wish to have NVC95 minimized while it performs a scan, then click on this option. When the scan starts, NVC95 will appear as an object on the Windows 9x taskbar.

If NVC95 is minimized and you wish to view the results, then you may double click on the icon, and you will see the "Scanning for viruses" dialog box.

User-Specified Extensions

By default, NVC95 scans files with certain extensions. Please refer to the Read Me file for more information on which extensions NVC95 scans.

If you wish to add files with other extensions for scanning, you may use the dialog box shown below to instruct NVC95 to look for up to 20 additional extensions.



To add a new user defined file extension:

1. Click on the [ ] **New type** check box
2. Type the file extension in the accompanying text box.

   All file extensions are limited to 3 characters.
3. Click on the **Add** button.

New file extensions will be saved in NVC95's Registry.

If you would like to have these extensions included in all of your scans, specify them as a setting within the **<NORMAL>** style.

If you would like these extensions to be used during only some of your scans, specify them as a setting within a style other than **<NORMAL>**.

For more information about styles, “Saving Your Configurations as Styles” on page 87.

To remove a user defined file extension, click on the extension you wish to remove and then click on the **Remove** button.

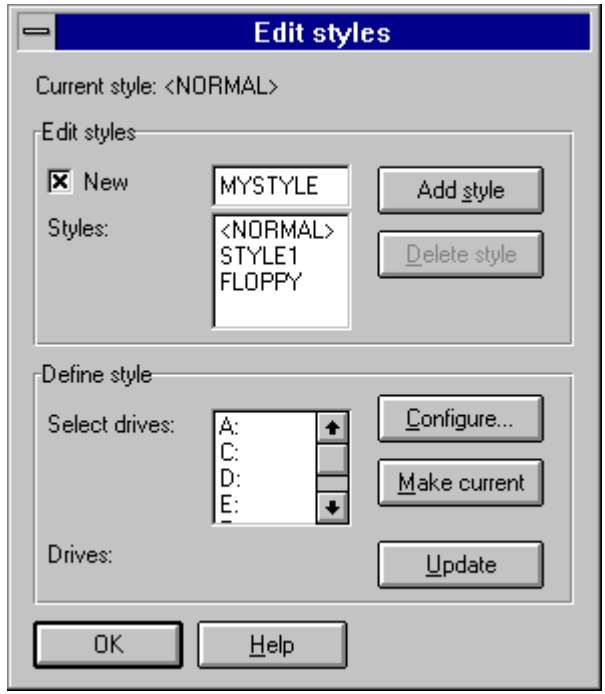
Saving Your Configurations as Styles

You can save yourself time by saving your configurations as styles. For example, if your goal is to run scans in certain combinations (scan diskettes and delete infected files; scan local drives and move infected files to a specific location, for example), then you can simply configure both types of scans as different styles and have NVC95 use the appropriate style at the appropriate time.

Note: NVC now allows the use of UNC (Universal Naming Convention) names and environment variables wherever file and directory names can be entered. Please refer to the *Administrator's Guide* for details.

To access the styles function, click on Options|Styles. You will then see a dialog box titled "Edit styles".

NVC95 is shipped with one style called the **<NORMAL>** style. It contains all the configuration settings that you have made thus far. The **<NORMAL>** style will always be available. You can customize it in any way you wish as well as create up to 20 additional styles, but you cannot delete the **<NORMAL>** style.



Add a Style

1. Click on the check box marked [ ] **New**.

   A new style is always based on the factory default settings.
2. Give the new style a name.

   Do this by entering the new name in the text box located to the right of the control box. The name can be up to 8 characters long.
3. Click your mouse on the **Add style** button.

   Your style's name is added in the list box "Styles" and is now available as an alternative to the <NORMAL> style.
4. Highlight the new style by clicking it once. Select drive(s) from the "Select drives" list box by highlighting the drive letter(s).

5. Click the **Configure** button.
6. Enter your choices in the tabbed dialog "Scanning options". When you click on **OK**, a pop up dialog box will inform you that the style has changed.
7. Click on **Update**.
8. If you wish to make this new style current now (i.e., to activate the settings of the style in this session of NVC95), then click on the **Make current** button.

When you make a style current, the scanner will be configured with the options that are associated with that style until you choose different options for that style or until you make another style current.

Delete a Style

1. Choose the style you wish to delete from the "Edit styles" dialog by clicking it once.
2. Click on the **Delete style** button. Before the style is deleted, you will be asked to confirm the deletion of the specific style.
3. To complete the operation, click on the **Update** button.

You cannot delete a style if it is current. You must first make another style current, select the desired style name from the list box, and then click on **Delete style**.

If a style is specified for a scheduled scan, you'll receive an error message if you try to delete it.

Save as Style

There will always be a current style. Unless you have specified otherwise, <NORMAL> is current.

When you are working with the scanning options, you are therefore editing the current style. If you want to keep the current style as it is **and** save the present changes as a separate style, you should choose Options|Save as style and save your changes from this dialog box:

See the next section for more information about saving scanning options in styles.

Save on Exit

The menu option Options|Save on exit is on by default. If you change the settings for the current style, they are permanently saved when you exit the scanner.

If Options|Save on exit is OFF, changes to a style are only valid for the present scanning session.

Unless you specify otherwise, the <NORMAL> style is the default style. Any configuration changes that you make while the <NORMAL> style is current will become part of the <NORMAL> style, regardless of whether or not you make the configuration changes from the "Edit styles" dialog box.

When a style other than the <NORMAL> style is current, the name of the style will appear in the title bar of the main window, in the title bar of the "Scanning for viruses" dialog box, and right under the title bar in the “Edit styles” dialog box.

Modify the <NORMAL> Style

You cannot change the <NORMAL> style from the "Edit styles" dialog box. To change this style:

1. Make sure that <NORMAL> is the current style.
2. Make sure that Options|Save on exit is on. This is the default setting.
3. Configure your scanning options from the Options|Scanning options tabbed dialog boxes.
4. Click on **OK** when you've made your choices.
5. You have now changed the <NORMAL> style permanently.

   Remember that all new styles are based on the original, factory default <NORMAL> style.

Note: When no other style is specified, the <NORMAL> style will be used. You may specify styles for both on-demand scans and scheduled scans. See "Scheduling Concepts" on page 94 for more information on scheduled scanning.

Specifying Directories In Styles

You can identify drives for scanning by specifying the target areas with scanning options from the "Edit styles" dialog. You cannot specify individual files or directories in the same manner.

You can, however, use the DOS command `subst` to solve this problem.

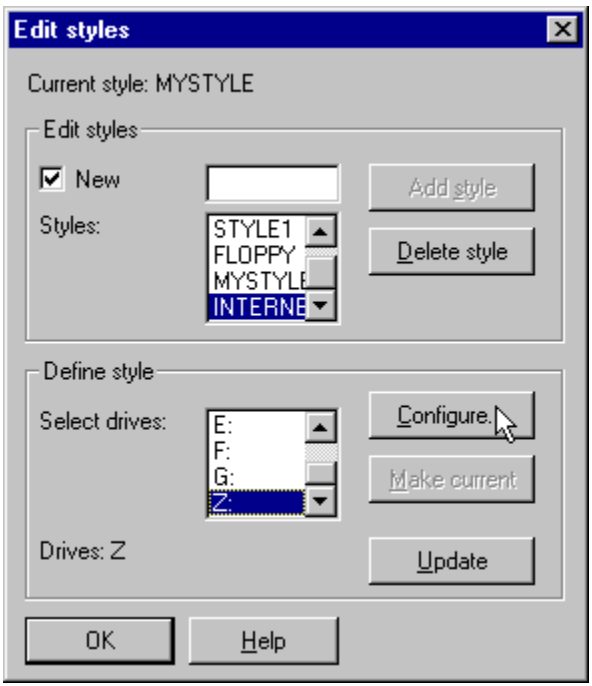
Task: to scan directory `c:\data\internet` only.

1. From the command prompt, type:

   `subst z: c:\data\internet`

   where `z:` is a virtual drive. If a 'z:' drive exists on your system, you must select another drive letter.

2. Select Options|Styles and add the new style INTERNET:



   Note that the virtual drive `z:` now appears in the Select drives list box.
3. Highlight the new style.
4. Select the `z:` drive from the box.
5. Click on **Configure** to determine the scanning options.

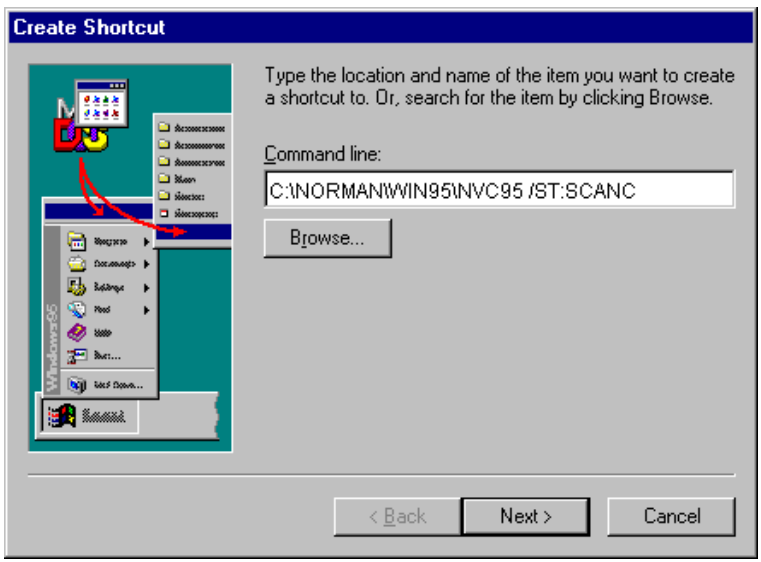
You have now created a style for scanning a specific directory. Like all styles, it is eligible for scheduled scans.

Note: You must run the `subst` command again to create the virtual drive again if after you have turned off or rebooted your PC.

See also the following section for an alternative way of scanning a specific directory.

Activating Styles from the Command Line

It is possible to create shortcuts on the Windows 9x desktop for different scanning purposes. For example, you might want to have one shortcut for scanning network drives on demand and another one for scanning particular directories during your lunch hour. To do this, simply create a shortcut by clicking your right mouse button on the Windows desktop and selecting "New". Specify the style you wish to use as follows:



In this example, we are loading the SCANC style and asking NVC95 to start scanning immediately after we click on the resulting icon.

The syntax for this feature is as follows:

```
NVC95 /ST:[name of style]
```

There are two rules for the syntax:

1. There must be a colon between the parameter and the name of the style.

2. There must be **no** spaces between the parameter and the name of the style.

If you run the style SCANC as shown above and add other parameters, like:

```
NVC95 /ST:scanc a: d:
```

the added parameters override the corresponding settings in the style. In this example, only `a:` and `d:` are scanned.

Note: When this feature is used, you will not be able to change the configurations within the styles before or after the scan begins. If you wish to change the configuration of a style prior to or following the scan, do not use this parameter. Rather, load NVC95 as you would normally by clicking on its icon. Then follow the instructions in "Configuring the Scanning Method" on page 71.

Scheduling Concepts

Not only does NVC95 perform on-demand scans, it can also scan at scheduled times. You may configure scheduled scans from several different locations:

- click on the pocketwatch icon on the toolbar

or

- click on Options|Scheduler options

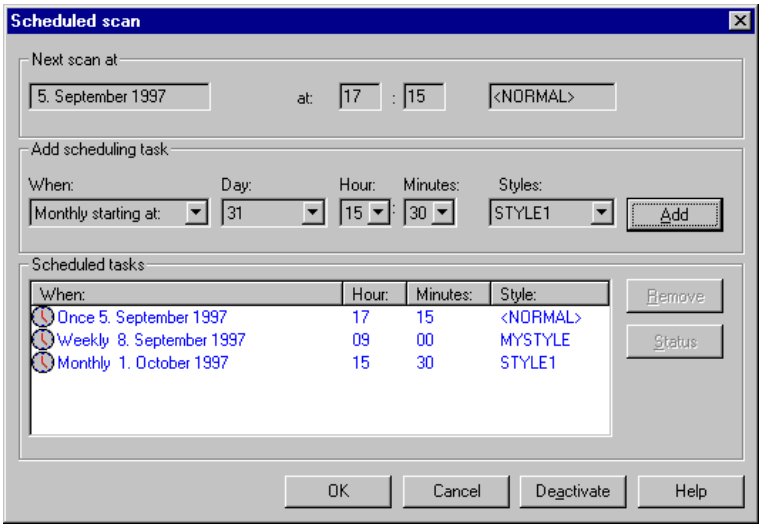
Whether you access the scheduler from the icon or from the "Options" menu, you can set the following:

- the time a virus scan will begin
- how often the process is to be run
- what type of style to use

You can schedule up to 20 scans, ranging from once, hourly, daily, weekly or monthly.

Note: If you schedule a combination of hourly, daily, weekly, and monthly scans, make sure that such repetitive scans are set to begin at different intervals within the hour. For example, if you schedule hourly scans to start at (hour):00, ensure that daily scans are scheduled for (hour):15 etc. If two or more scans are scheduled at the same minute interval, only one scan will be performed.

The dialog box from which you configure the scheduled scan looks like this:



Schedule a Scan

To schedule a scan, first set the frequency of the scheduled scan from the "Add scheduling task" section of the display. Click the [ ] **When** combo box and choose from:

- **Once**
- **Hourly**
- **Daily**
- **Weekly**
- **Monthly**

When you select **Once**, **Hourly**, or **Daily**, today's date is automatically selected.

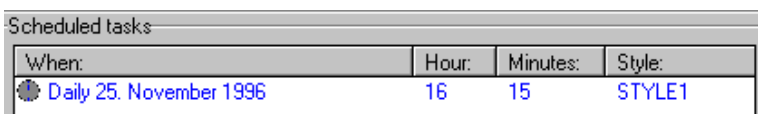
If you select **Weekly**, then you may choose the day of the week on which the scan should occur.

If you click on **Monthly**, the combo box changes to list the numbers 1 through 31. If you choose "5", for instance, then the scheduled scan will occur on the 5th of each month at the time you have specified. If you choose "31", and there are only 30 days in a particular month, then the Scheduler will begin the scan on the 1st of the following month.

Then:

1. Click on the [ ] **Hour** combo and select the hour you wish. Hours are listed in 24 hour format.
2. Click on the [ ] **Minutes** combo and select the minutes you wish. Minutes are given in 15 minute increments.
3. Click on the [ ] **Styles** combo and select the style you wish to use for this particular scheduled scan.
4. Click on the **Add** button, and the scheduled scan appears in "Scheduled tasks" list box.

   Once you have set 20 daily scans, the **Add** *button becomes inaccessible.*
5. When you add a scheduled scan, it pops up in the "Scheduled tasks" list box and activates the scheduler.
6. You cannot change a scan after it's been scheduled. You must highlight the scheduled task by clicking it once, then click the **Remove** button and enter a new scan.
7. The first scheduled scan to be run appears at the top of the list in the "Scheduled tasks" list box, as well as at the top of the display in the list box "Next scan at:".
8. The "Scheduled tasks" list box provides information on future scans. The watch to the left of the scheduled scan tells you that a scan is scheduled:



9. Click on the OK button when you have entered all your scheduled scans.

Make sure that the scheduler is active. The scheduled scan is on by default. You can turn the scheduler on and off from the Options menu or from the scheduler status button on the toolbar.

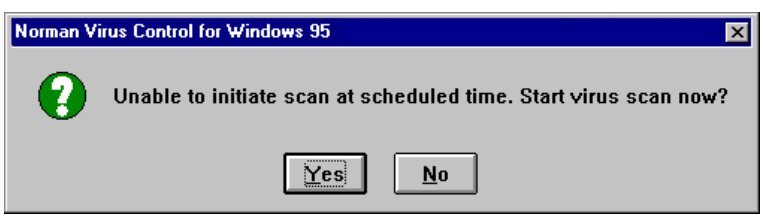
Note: In order for a scheduled scan to occur, scheduled scanning **must** be ON, and the scanner must be active.

When scheduled scan is **on**, the toolbar button is depressed and looks like this:

When scheduled scan is **off**, the toolbar button looks like this:

If no scans are scheduled, the toolbar button is grayed out:

If a scan failed to run at the scheduled time, you'll see this message the next time you access the scheduler:



Scheduling Several Unattended Scans

Like on-demand scans, scheduled scans require user action when the scan is complete. A scan will either inform you that no infected areas were found, or that a possible

infection is detected. In either case, you need to take some action to remove the messages.

However, if a message that has not been closed is blocking an upcoming scheduled scan, NVC will remove the message 30 seconds before the scheduled scan is due to run.

There are nevertheless a couple of options you must be aware of when you're scheduling more than one scan to run unattended at night, for example:

1. In the styles being used, do **not** check the [ ] **Exit upon completion** option in the tabbed dialog "Scanning options". If you do, the scanner will close and consequently not run the remaining scheduled tasks.
2. In the styles being used, you **must** check the [ ] **Ignore locked files** option in the tabbed dialog "Scanning options". If you don't, the scan may be blocked by messages about locked files that could not be opened.
3. Make sure that you specify different names for the reports for the various styles. Alternatively, uncheck the [ ] **Overwrite previous** option in the Options|Scanning options tabbed dialog Reporting for each style being used. If you use default setting, you'll only get the report from the last scan.

Command Line Scanning

The command line scanners are not dependent on any other modules. They can send virus alert information to FireBreak through IPX communications, SNMP traps (except for the Windows 3.1x version), and they can be run from batch files. For more details, see "Norman programs and IPX communications" in the *Administrator's Guide*.

The 32 bit command line scanner is available on the following platforms:

Platform:	Exe file:	Default location:
Windows 3.1x	NVC32X	c:\norman\dos
Windows 95	NVC32	c:\norman\win32
Windows NT	NVC32	c:\norman\win32
OS/2	NVC32	c:\norman\os2

Using the Command Line Scanner

The syntax is:

```
nvc32 [drive]:[path] [/parameters]
[Enter]
```

Note: A space must precede each parameter that you use.

Simply select the combination of parameters that you wish to use and specify them on the command line.

Scanning Options

From the directory where the Norman programs reside, run the command

```
nvc32 /?
```

from the command line to display a list of available options. The following tables chart out the available parameters and their functions. The first table presents parameters that are relevant for the ordinary user. The second table explains parameters that may be useful for system administrators

Param.:	Function:
/?	Show help.
/ALD	Scan all local disks (not diskettes or CD-ROM).

Param.:	Function:
/AD	Scan all disks (not diskettes). Possible network drives are scanned in addition to local fixed drives.
/AF	Scan all files. The default is files with extensions like .exe, .com, .doc etc. The list is continuously reviewed and therefore presented in the readme file.
/B	No alarm when infections are found.
/BS-	Ignore system areas from scanning. The system areas of the same drive will only be scanned once if several file specifications for the same logical drive are specified.
/BS+	Scan system areas only.
/C	Scan archive files. Infected files can be found within archive files, and you can instruct NVC to look inside the archive file.
/CP	Scan compressed program files. A decompressor emulator will open and scan the file in memory.
	The scanner can only tell you whether or not an archive file or a compressed program file is infected. It cannot take any action on the infected file while it is archived/compressed.
/CL	Repair files when possible. With this parameter, NVC will prompt you to confirm prior to cleaning infected boot sectors and files. When /CL is used concurrently with /U or /Q, however, NVC will not prompt you before cleaning.
/D	Overwrite and delete infected files. Recovery of an overwritten file is not possible.

Param.:	Function:
/D-	Delete infected files. Infected files are automatically deleted. Since we are not overwriting the file before we delete, recovery of the infected file is possible with tools such as the Norton Utilities.
	If the /D or /D- parameters above are used together with /CL, /CL will take precedence. If the file cannot be repaired, it will be overwritten and/or deleted.
/H	Show help.
/LA	Log all scanned files. By default, the command line scanner will only log names of scanned directories and infected files. This parameter forces the scanner to log the names of all files that were scanned. If you wish to specify the name of the log file, then pair this parameter with /LF.
/LF:	Log to specified report file. Type in the name immediately after the parameter (no spaces).
/LF	Log to standard report file NORMAN.RPT.
/LG	Append log to existing report file. Default is overwrite.
/LQ	Create report file only when infections found.
/LS	Log all scanned directories.
	Note that in order to produce a report, you must specify one of the L options above.*
/MOV	Move infected files to default INFECTED directory (c:\norman\infected).

Param.:	Function:
/MOV:	Move infected files to specified directory. Type in the name immediately after the parameter (no spaces). If you don't type in a directory, NVC will create it for you relative to where the NSE directory is located. If it is installed in c:\norman\nse, the infected directory will be c:\norman\infected.
/N	Suppress the default memory scan.
/NW	Don't display messages regarding the status of your licence (for example, licence expiration).
/O	Ignore files that cannot be opened. If you have specified a log file, locked files are listed there.
/Q	Quiet mode, i.e. no screen output at all. Overrules the /O and /U parameters.
/R	Repeat the scan. Useful for checking several diskettes.
/S	Scan subdirectories. Use this option if you have specified a directory and want to include subdirectories in the scan. If you have specified a drive letter, subdirectories are automatically included in the scan.
/V	Verbose mode. Display all details during scan.
/W:	Wait specified number of milliseconds between each file.
/X	Look for EXE header in all files. Like /AF, this parameter will increase the scanning time because all files are checked.
/Y	Display detailed virus name.
/YH	Abort the scan when a virus is found and display the path and virus name.

The following command line parameters are useful for system administrators:

Parameter:	Function:
/NVCADMCFG:	Override environment NVCADMCFG, where the program looks for nvcadm32.cfg (if nvc32.cfg is not found). If no such environment is defined, the program will search for the file one level up from where it is executing.
/NVCCFG:	Override environment NVCCFG, where the program looks for nvc32.cfg. If no such environment is defined, the program will search for the file one level up from where it is executing.
/SN	Do not allow user aborts.
/TEMP:	Override environments TEMP/TMP. If no such environment is defined, the program will create it one level up from where the directory NSE is located.
/U	Do not stop when infections are found. Overrules the /O parameter.
/WORK:	Specify where NORMAN.RPT and INFECTED directory is created. If nothing is specified, the program will place the report file one level up from where it is executing.

Combining Different Parameters

The command line scanner is flexible in the sense that you can combine parameters to carry out multiple tasks in one command.

Here are a couple of examples on how you can combine parameters. From the directory where `nvc32.exe` is installed, type:

```
nvc32 a:\*.txt /n /bs- /lf
```

This will scan all files on the diskette with the extension `.txt`, the boot sector will not be scanned, and the `norman.rpt` will be created in the directory where `nvc32x.exe` is installed.

Then type:

```
nvc32 *.txt a: c:
```

to scan `txt` files in the current directory and then the boot areas and default file extensions on `a:` and `c:`.

Note: Specifying `c:\` (with a slash) will scan files only in the root drive, but `c:` (without a slash) will both scan files and the disk's system areas.

Command Line Scanner Errorlevels

You can automate the command line scanners by using errorlevels in batch files. The errorlevels for the command line scanners are::

Errorlevel:	Meaning:
13	Licence does not allow the program to start.
12	The file `NVC32.CFG` was not found.
10	Files skipped (could not be accessed).
9	The scanner was interrupted and did not complete its scan.
8	The scanner stopped due to an error in logic.
6	Disk input/output error.
5	You did not enter valid scanning criteria.

Errorlevel:	Meaning:
4	The hardware configuration has changed since you installed the scanner.
3	The scan began without having any scanning criteria.
2	Detected an active virus in memory.
1	Detected one or more viruses in one or more files.
0	Scanned for viruses and did not find any.

Generic Detection with Canary

Canary is not dependent on any other module and not critical for any other module's functioning. It works well with the Smart Behavior Blocker.

In the old days of coal mining, miners brought canary birds with them down into the shafts. The canaries served as early warning signals, for they reacted quickly to dangerous gases and lack of oxygen. If a canary died, the miners knew that it was time to get out.

Norman used this idea when designing our Canary programs CANARY.COM and CANARY.EXE). The Canary programs work as **non-resident** "bait" for known and unknown file viruses that infect files with the extensions .EXE and COM. If they become infected, they alert you that a virus is active in your computer. Since the Canary programs do not scan for specific viruses, they detect even unknown viruses. And when they become infected, they display messages on the screen and return errorlevels.

The Canary programs are self aware and know everything about themselves — their own file lengths, the precalculated checksums, and the date and time of their installation.

Most viruses attack a file by inserting their own program codes into the file. When this happens, the file length increases, and if the file happens to be Canary, Canary detects this immediately and reports "The Canary Bird is Dead!".

Other viruses overwrite parts of the file without altering the file length. As a result, the program will no longer work properly, and the checksums change. Canary will also react to the altered checksums.

If you run Canary, and CANARY.COM and CANARY.EXE have not been infected, you see the following message:

```
EXE:   The Canary Bird Lives and all is well.

COM:   The Canary Bird Lives and all is well.
```

If, for example, a virus has infected the .EXE file, the message will read:

```
EXE:   The Canary Bird is Dead!

COM:   The Canary Bird Lives and all is well.
```

You can suppress these messages and report by errorlevel instead. See “Canary's Errorlevels” on page 110.

Note: If Canary detects a virus, you can send a copy of your CANARY.COM and CANARY.EXE files to Norman for further study.
Because Canary uses generic methods, it will not tell you the name of the virus it has detected. To find out, you must use Norman's scanners. See “Detection” on page 52 for more information on scanners.

Using Canary

The Canary programs are 16 bit DOS programs and therefore must be run from either the command line or from a batch file. In addition, when you run Canary, you must be in the directory that holds the Canary files; or the directory must be available in the DOS path.

For Canary to be effective, you should run it frequently. Here are three ways to ensure maximum protection:

Always activate Canary after you have used a program by inserting instructions for running Canary at the end of each .BAT or .CMD file; or run your applications from a menu system that activates Canary whenever you return to the menu.

Implement a resident scheduling function that will start Canary at regular intervals.

Develop a good habit of starting Canary manually several times a day. Frequent use of Canary means swift detection, and swift detection means less damage.

In DOS, if you simply type the name of an executable without the extension, DOS will look for the executable as a COM file first. If a COM is not found, it will then look for an EXE.

The Canary programs take advantage of this fact so that you only need to type `canary`, and CANARY.COM will run.

CANARY.COM will then automatically run CANARY.EXE.

The syntax for running Canary is:

`canary [reporting level] [Enter]`

The reporting level determines how many messages will be displayed on your screen when you use Canary. Following is a description of reporting levels.

Reporting Level	Function
no entry	All messages from Canary are displayed.
1	Message is displayed only if a virus is detected or an error occurs.
2	No messages are displayed. Reporting occurs only through errorlevels.

Alternate Filenames for Canary

You can rename CANARY.COM and CANARY.EXE using any name you like, as long as you give the two files the same "first name" (e.g., TESTFILE.COM and TESTFILE.EXE). This protects Canary from being attacked by virus-writers.

Canary's Errorlevels

At the end of each run, Canary returns errorlevels which contain the results of the run. You can use these errorlevels in batch files to tailor Canary's use for your needs.

Errorlevel	Meaning
16	Communication between CANARY.COM and CANARY.EXE is invalid. CANARY.EXE has been started by a program other than CANARY.COM. You may have a virus that uses the companion technique. These viruses create a .COM file with the same name as an .EXE file, taking advantage of the fact that DOS will always start the .COM file first. Examples of such viruses are Aids II and Twin351.
9-15	Not used.
8	Cannot open CANARY.COM or CANARY.EXE. Canary cannot open its own .COM or .EXE file for examination.
6-7	Not used.
5	CANARY.COM is infected, and CANARY.EXE is missing.
4	CANARY.COM is normal, but CANARY.EXE is missing. Ensure that both files exist and are available via the path.
3	CANARY.COM and CANARY.EXE have been modified/infected.
2	CANARY.EXE is modified/infected.
1	CANARY.COM is modified/infected.
0	CANARY.COM and CANARY.EXE are normal.

Other Functions

Finding Out More About Viruses

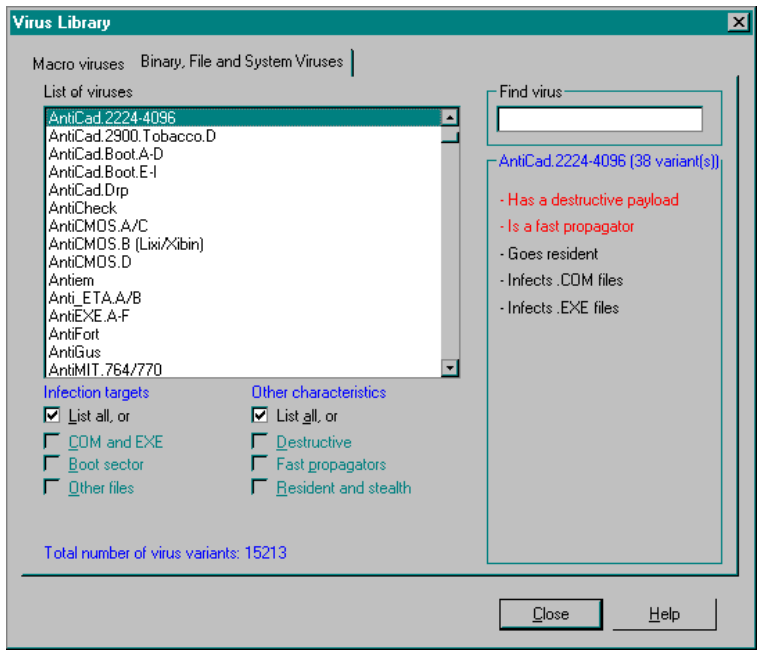
There are two functions within the scanner which allow you to learn more about viruses.

Virus library gives an overview of names and characteristics of the viruses that NVC95 can recognize. You can access virus library through the menu option View|Virus Library or by clicking on this toolbar button:

Computer viruses can be categorized in two distinctly different classes: binary and macro viruses.

1. *Binary viruses* contain executable code, i.e. program instructions. Binary viruses can infect program files (frequently referred to as executables), boot sectors, or other executable code on your PC.
2. *Macro viruses* do not contain executable code. They employ the macro programming language used in most word processors and spreadsheets. Macro viruses will infect Word or Excel files, for example, and replicate when infected files are accessed. Macro viruses do not depend on specific microprocessors or operating systems.

The virus library has two tabbed dialogs, one for binary viruses and one for macro viruses. Here you will find key information for every virus in this list.



The total number of viruses identified is virtually increasing by the hour, and the list is consequently quite extensive. Because viruses are treated differently depending on type and property, it is useful to gather as much information as possible about the virus.

The list box on the left of the dialog box contains the names of the viruses that the scanner can recognize. The area on the right describes the most important characteristics of the virus that you have chosen from the list. The complete list is sorted alphabetically. Because of its comprehensive nature, it may be time-consuming to use the arrow keys to navigate through the list. Therefore, you can search for viruses using other methods.

- Use the scrollbar to the right of the list box to move quickly through the list. Then highlight a list item for more information on this virus.
- If you know the first letter of the virus you are looking for, you can simply type its first letter from

the keyboard. The first virus whose name starts with this letter will appear as the first item in the box. Continue pressing the same key until the desired virus appears highlighted.

- If you know the full name of the virus you are searching for, you can use the [Tab] key to set the focus on the text box to the right of the list box. Then type the name of the virus and press [Enter].
- You can narrow your search by clicking the check boxes in the two columns under the list box. The left hand column displays viruses by what they infect, while the right hand column allows you to sort viruses by how they perform.

If you check the [ ] **List all, or** check boxes, the other options in that column are grayed out.

There are many viruses that are known by several names. Hence, a virus you are looking for under one name may be in this list under another name. Call us if you can't find the virus for which you are searching...

Binary Virus Attributes

These are the possible attributes for binary viruses:

It has a destructive payload

While most viruses are relatively harmless, this virus will perform destructive acts such as delete critical files, format your hard drive, or destroy other data.

It is a fast propagator

The virus stays in memory (goes resident) and hooks the services used by other programs to open, read, write and/or close files. Whenever any program opens a file, this will start the virus code, infecting the opened file, or look for another file to infect.

Uses encryption

The virus code itself is encrypted to avoid detection. It can be detected anyway.

Uses stealth techniques

The virus tries to hide itself to avoid detection. It is normally detected anyway.

Overwrites original file

The virus code overwrites parts of the infected file. Files infected this way cannot be cleaned, but must be replaced from backups in order to get rid of the virus.

Boot Sector

Infects boot sectors on diskettes and/or hard-drives. Will in most cases infect the hard drive if left in the diskette drive when the PC is booted.

EXE, COM files

Infects mainly EXE or COM files or both.

COMMAND.COM

Infects COMMAND.COM.

OV? files

Infects overlay files. An overlay file is a part of a program split in separate, overlayed, files.

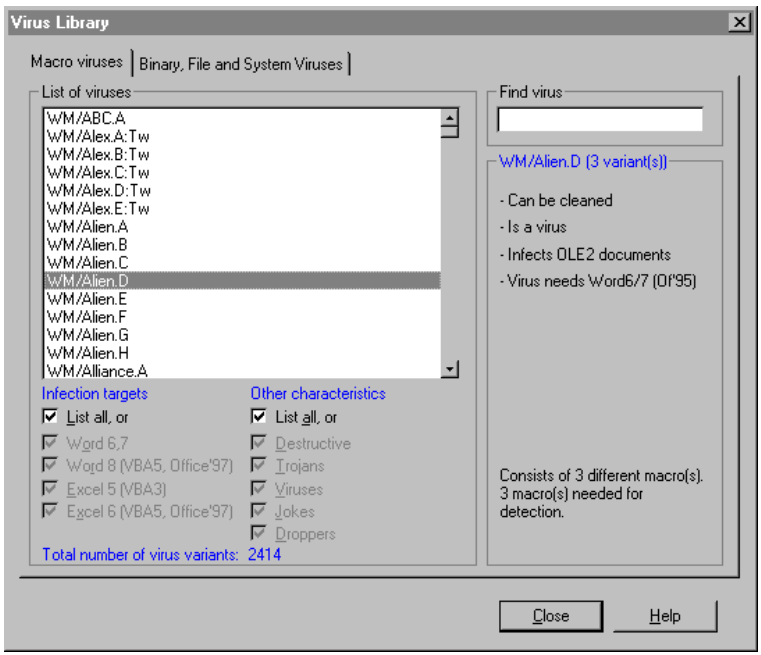
Other files

Infects other files.

Goes resident in Low, High, UMB, Video RAM

The virus stays in memory when first activated.

Macro Virus Attributes



These are the possible attributes for macro viruses:

Can be repaired

Documents or template files infected by macro viruses can in most cases be repaired. Technically, this involves removal of the viral macros, while legal, user defined macros are left intact.

However, some macro viruses "snatch" user defined macros while replicating, making each infection unique. The user defined macros will in most cases be changed to call the main macro in the virus. The WM/CAP family of macro viruses is an example of viruses with this capability. Files infected by this kind of virus are repaired by removing **all** macros.

It has a destructive payload

While most viruses are relatively harmless, this virus will perform destructive acts such as delete critical files, format your hard drive, or destroy other data.

Is polymorphic

The virus changes itself from infection to infection.

Is a Virus

This is a true virus, able to replicate itself. Opening this document will trigger the macros, probably infecting other document files.

Is a Trojan

This is not a virus, meaning that it doesn't replicate. Contains other forms of malicious code.

Drops binary virus

This macro virus contains a binary virus. See Binary viruses on page 111.

Is a joke, non-infectious

This document file contains macro code that performs harmless, sometimes visible, actions. Opening this document will trigger the macros, but no other document files will be infected.

Contains garbage
Is inactive or damaged.

This document file contains remnants of macro viruses, or other macros that don't work as intended.

Infects Word2 documents

This document file contains a macro virus that requires Microsoft Word version 2 to replicate.

Infects OLE2 documents
Virus needs Word6/7 (Office '95)
Virus needs Excel6 (Office '95)

Virus needs Word8 (Office '97)
Virus needs Excel6 (Office '97)

This document file contains a macro virus that needs one of the specified Microsoft applications to replicate.

The Display Feature

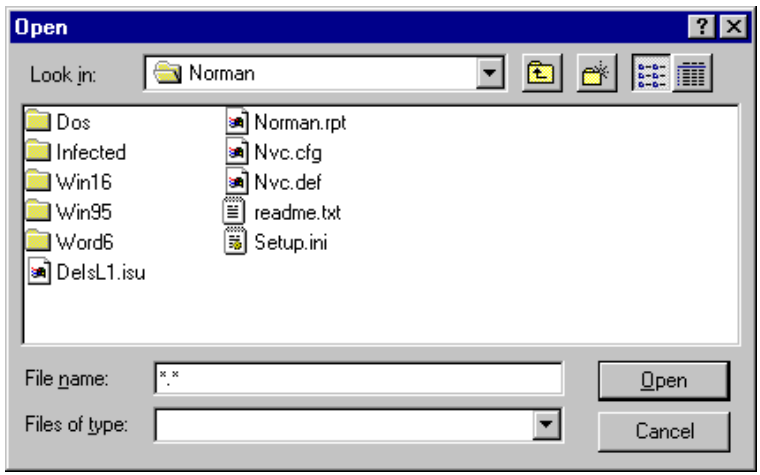
The **Display** feature displays data from files and system areas as hexadecimal values and printable characters.

You can access this function from the File menu.

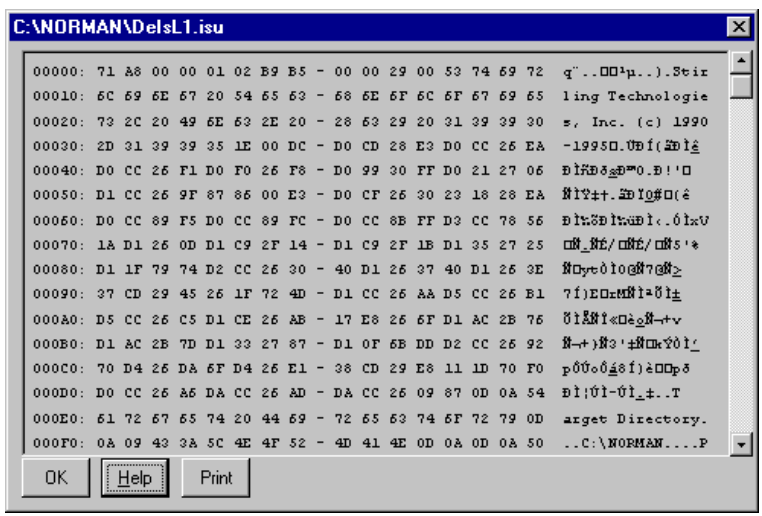
If you want to take a look at the contents of a file (presented as hexadecimal values and printable characters), or if you wish to look at the contents of the system areas on your boot drive, you may choose the "Display" menu option.

Display File

If you choose **Display file**, you will be prompted to choose a file from within a file window.



When you have chosen to display a file, the following dialog box appears:



The dialog box shows you the file contents as hexadecimal values (left) and text (right). To maneuver up and down

within the file, use the scrollbar along the right edge of the dialog box.

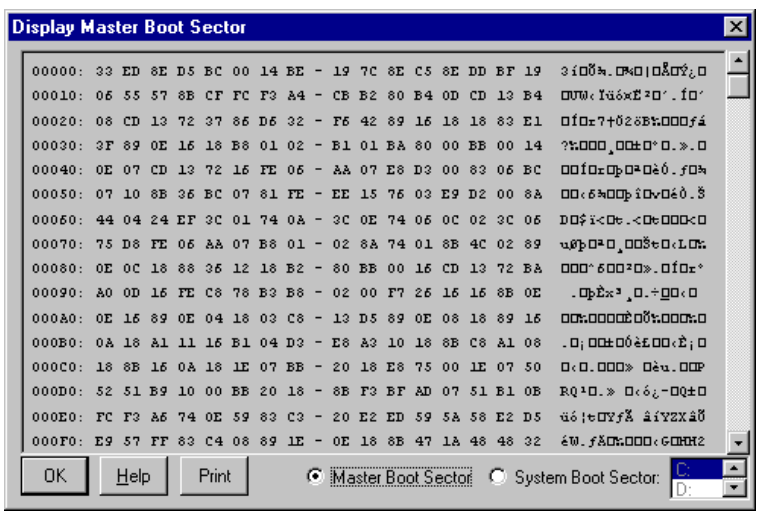
This function is especially useful when technical personnel want to look inside a file or sector for signs of a virus infection.

There are three buttons at the bottom of the dialog box:

Close quits from the function and returns you to the main window. **Print** permits you to send the displayed file to the printer that is set up through Windows. **Help** gives you help on this function.

Display System Areas

If you choose the **Display system area** menu choice, this screen will appear:



The System area includes the Master Boot Sector (MBS) and System Boot Sector (SBS).

You have a choice of viewing the MBS area of the first physical hard drive as well as the SBS on drive C:. In addition, you can view the SBS on all diskettes.

See the sections "Master Boot Sector“and “System Boot Sector (SBS)” on page 84 for an explanation of these terms.

Examples of Common Uses of NVC95

Different Combinations

Because of the scanner's configuration flexibility, there are many ways to run scans. You will no doubt find the best methods for your organization's needs. To get you started, here are several techniques that might be helpful.

Automatically Scan Different Areas at Different Times

Goals: To automatically scan the entire hard drive in the beginning of the day, to automatically scan only the C:\FINANCES directory during lunch, and to automatically scan only the C:\WORDS directory at the end of the day. If any infected files are found, specify repair or move them to the C:\NORMAN\INFECTED directory.

What we will use: Styles and the scheduler.

See "Saving Your Configurations as Styles" on page 87 and "Scheduling Concepts" on page 94.

Steps:

1. Set up 3 styles: ALLOFC, $ONLY, WORDONLY (for example), and configure each style accordingly for scanning areas, scanning options, reporting options, etc.
2. In the scheduler, specify the day and the hours at which to run each of the styles.

3. Remember to click on **Add** and **OK** before exiting the "Scheduled scan" dialog box.
4. Exit the scheduler dialog box.
5. Do **not** exit NVC95.

Decrease Screen Output During Scan

Goal: To have NVC95 run **once** and display only critical messages on the screen.

We will use these options:

[x] Report to file and/or [x] Report to printer,

[x] Report only if infection,

[x] Exit upon completion,

[x] Ignore locked files,

[x] Minimize while scanning, and

[x] Don't stop on virus

Steps:

1. Start the scanner.
2. Click on Options|Scanning options.
3. In the "Scanning" tabbed dialog box, ensure that [ ] **Don't stop on virus** is checked.
4. In the "Scanning" tabbed dialog box, ensure that [ ] **Exit upon completion** is checked.
5. In the "Scanning" tabbed dialog box, ensure that [ ] **Ignore locked files** is checked.
6. In the "Reporting" tabbed dialog box, ensure that [ ] **Report to printer** and/or [ ] **Report to file** are checked.
7. In the "Reporting" tabbed dialog box, ensure that [ ] **Report only if infection** is checked.
8. In the "Additional options" tabbed dialog box, ensure that [ ] **Minimize while scanning** is checked.

When all of this is done, the scanner will run as a minimized icon, and you will only see a report on the screen if an infection is found. Otherwise, the scanner will exit when it has finished scanning.

This method is great for running a single scan at night. If you leave your Windows 9x machine on during the night and use this method, the next morning you will see a report on the screen if a virus was found.

Note: If you are running more than one nightly scan, please refer to the section “Scheduling Several Unattended Scans” on page 98 for details about scheduling more than one nightly scan.

Consequently, any user who wishes to use the machine in the morning will see this notification. If no virus was found, then nothing is displayed on the screen, and the user can continue as normal.

Remember: if you have set the scanner up to always report to a file, then you can always view the most recent report by clicking on View|Report.

Create Icons and Customize the Scan

Goal: To create shortcuts that sit on the Desktop and perform customized scans on demand. By doing so, you can bypass clicking on NVC95's icon and spending time configuring your scan. Instead, you can configure your scan beforehand and then click on your customized icon when you wish to perform the scan. For instance, if you would like to scan the C: and D: drives on demand simply by clicking on an icon, follow the steps outlined below.

What we will use: Styles and the 2 parameters associated with styles.

Steps:

1. Create a style that you wish to use for this purpose. For the example that we gave above, we would create a style named CDONLY, we would choose the C: and D: drives as the search areas, and then we would select other configurations such as reporting, etc.
2. On the Windows 9x Desktop, click once with your right mouse button, select "New", and use the parameter /ST:

The syntax for the command line is:

```
drive:path\NVC95.exe st:[style name]
```

For example, if NVC95.EXE resides in the C:\NORMAN\WIN95 directory and you wish the icon to start scanning immediately using the CDONLY style, then your command line for the new shortcut will be:

```
C:\NORMAN\WIN95\NVC95 /ST:CDONLY
```

You can, of course, combine this method with the configuration described in "Decrease Screen Output During Scan" above by altering the settings in the style.

Scan Automatically after Downloading Programs

Goal: To automatically scan programs that you have downloaded onto your PC.

What we will use: A batch file and styles. The batch file will run your communications software (CompuServe, AmericaOnLine, etc.) and then run NVC95 against the files that you have downloaded.

Steps:

1. If possible, set up your communications software to store all downloaded files in one directory. (If you cannot do this, then find out where the downloaded files are stored by default.)
2. Create a style for this purpose and configure it accordingly. For the search area, you must specify the directory in which your downloaded files are stored.

And since a fair number of downloaded files are archived, you should use the "Scan archive files" option.

3. Create a batch file which first runs your communications software and then NVC95 /ST, with the style you have created.

For example:

```
DOWNSCAN.BAT
rem the next line runs PCPLUS.
pcplus
rem the next line runs NVC95 immediately
rem after PCPLUS exits.
c:\norman\win95\nvc95 /ST:DWNLOAD
rem the above line tells NVC95 to use the
rem DWNLOAD style. I have set PCPLUS to
rem put all my downloads on the
rem E: drive.
rem Therefore, in the DWNLOAD style, I
rem have specified the search area to be
rem E:.
...etc
```

Now you can create a shortcut icon that runs this batch file from the Desktop.

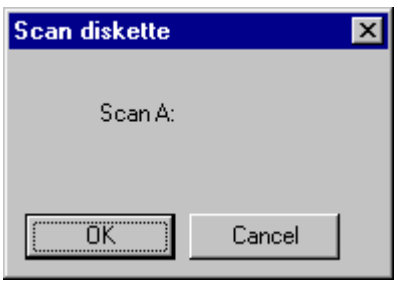
Quick Diskette Scan

Goal: Scan diskettes for viruses without having to select the A: or B: drive and then click on “Start scan”.

What we will use: NVC95 and your mouse.

Steps:

1. Place the mouse-pointer anywhere inside the main window of NVC95.
2. Click the **right mouse button**, and you will see this dialog box:



3. You can only choose one diskette drive at a time. When this is done, click the **OK** button and NVC95 will use the *current* style to start scanning the disk in the selected diskette drive.

Updating NVC

Any virus scanner is only as effective as its most recent update, so obtaining frequent virus signature updates is critical to maintaining a secure computing environment

There are two different kinds of updates for NVC:

Version update: actual program changes for one or more of the modules in the package. To install a version update, run a regular install as described in the setup procedure.

Definition file update: changes to the files `nvcbin.def` and `nvcmacro.def` (in c:\norman\nse). These files hold the virus signatures (fingerprints of known viruses) and are used by the scanning engine. To install a definition file update, double-click on the file name and follow the instructions on the screen.

Definition file updates are available from our Web site on a regular basis:

http://www.norman.no/update.htm

Norman Internet Update

The polling program Norman Internet Update automatically checks for updated files to the scanning engine (definition files, DLL/VxD) on Norman servers and it's available for Windows 9x and Windows NT.

NIU will appear as a separate item in the Norman group. To run NIU, you need a TCP/IP (Internet) connection. You can start the program by placing it in the Startup group or doubleclicking the icon in the Norman group. When you

run NIU, the program will check a Norman server for updated virus definition files. These files reside in the NSE directory.

Configuration Settings

When Norman Internet Update is installed, the section NSE Update is added to the configuaration file (`nvc32.cfg`).

The default settings that apply if you accepted to place NIU in the Startup group, or when you run the program manually bly doubleclicking the icon, are:

```
-hidden -wait:5
```

`Hidden`: without appearing on the screen, the program checks the validation key and the time stamps on your files in the NSE directory versus the time stamps on the available files on the Norman server. You will be notified if the validation key is missing or wrong, if updated files are available, or if any problems occur.

`Wait`: after the program has started, it waits for 5 minutes before it starts working. The `-wait` parameter requires the `-hidden` parameter.

Note: Norman Internet Update will not be invoked on a PC that is running continously. In such instances you can use the scheduler in Windows 98 or Windows NT to invoke the program. On Windows 95, however, you'll have to log out and in, or start NIU manually.

Note well:

If you're running NIU with a modem, make sure that you hang up when a download is completed. You may configure your dialer to hang up two minutes after a download is complete, for example.

How to Use Norman Internet Update

1. Enter the CD key in the Authentication field.
2. Click on **Validate**. The CD key you entered is checked by a Norman server, as well as the time stamp on the virus definition files.
3. When the key is validated, the **Download** button is activated if there are updated files available.
4. Click **Download** for fetching the package with the latest updates. The new files will replace the old files at next reboot.

For network administrators: see the *Administrator's Guide* for more details.

Index

—D—

—E—

—F—

—H—

—I—

—L—

—M—

—N—

—O—

—P—

—Q—

—R—

—S—

—T—

—U—

—V—

—W—