NORMAN

Norman Virus Control for OS/2

User's Guide

Version 4.70

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.

The Norman logo is a registered trademark of Norman ASA.

Names of products mentioned in this documentation are either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

NVC documentation and software are

Copyright © 1999 Norman ASA.

All rights reserved.

Contents

Introduction

About Norman

Norman ASA is a multi-national company that was established in Norway in 1984. Then, as today, Norman's business was developing and selling security software for PCs and data security consulting. We also offer protection with FireWall in an integrated software/hardware solution. Over the years, Norman has opened offices in the United States, Germany, Australia, the Netherlands, Switzerland, Sweden, Finland, and the UK, and has partners in the Far East.

As computer use rises, so does our dependence on the information stored in those computers. The value of computers today must be measured not by the worth of the hardware but by the worth of the information inside. We have all heard the adage "an ounce of prevention is worth a pound of cure". If you are concerned about data integrity, this is advice truly worth heeding. To properly and efficiently defend your data, you must prevent unauthorized entry and action that can lead to data disaster. Norman provides computer users with a wide range of products designed to work together in order to prevent data loss both on workstations and network servers.

Norman's approach to data defense is based on a Cross-Platform Strategy, which includes security solutions for DOS, Windows, Windows 95, Windows NT, OS/2, and Novell NetWare. All anti-virus products belong to the Norman Virus Control (NVC) family.

Why Use Norman Virus Control

One of the most high-profile threats to data integrity is the computer virus. Computer viruses are an international problem, which is becoming more severe each year as the number of viruses written each year grows exponentially. The effects of computer viruses can range from loss of productivity to data loss, but a computer virus incident almost always results in high levels of frustration and most importantly, gross expenditures for virus removal.

Norman Virus Control for OS/2 identifies viruses on both workstations and file servers. NVC will identify viruses that already exist on your system and remove them. Having a routine for scanning all removable media such as diskettes will prevent infected files from getting into your system.

NVC for OS/2 is a powerful, configurable scanner, with one of the top virus detection rates in the industry. It is written from the ground up as a true 32-bit multithreaded OS/2 program, eliminating the need for middleware.

Flexibility

NVC for OS/2 uses various methods to detect viruses and remove viruses:

- system monitoring by a behavior blocker
- boot area protection
- generic, non-resident "bait" for file viruses
- on-demand and scheduled scan for boot and file viruses

You can configure NVC in numerous ways, including:

- areas to be scanned
- scanning options
- how to manage infections
- save all options as "styles"

And you can use NVC to:

- view files and system areas in hexadecimal format.
- view descriptions of viruses with the Virus Library.
- access context-sensitive help at any time.
- browse through on-line information about viruses in general

Quality

Norman software is of high quality, based on advanced technology, but we realize that no software is perfect. Through feedback from our customers and cultivation of new techniques, we continuously seek to improve the quality of our products.

Support

Understanding viruses and how to deal with them is not always easy. Having Norman products installed helps, but sometimes you may need some help with a virus or with deciding what the best configuration is for you. That's why we provide you with solid technical support, whether you simply have a question about how to use our products or whether a virus is making the rounds in your organization.

How This Documentation Is Organized

We have defined 3 areas as critical to fight viruses and therefore have corresponding functions in NVC. These areas are:

- Prevention
- Detection
- Removal

Please refer to the *Administrator's Guide* for details about issues relating to use on a network and network messaging.

We hope this structure helps you get the most out of NVC. If you have comments or suggestions for improvement, please do let us know.

Who Should Read This Manual?

This manual is intended for users familiar with the OS/2 Warp user interface.

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

Reference to the Modules

NVC is comprised of modules with different functions. In this manual we refer to the specific modules by specifying

the program's filename. The filenames and their corresponding modules are:

NVC.SYS	The Smart Behavior Blocker
BG2.EXE	BootGuard
CANARY.COM and CANARY.EXE	DOS based, on-demand, non-resident "bait" for file viruses
NVC32.EXE	Command line scanner
NVC32.CFG	Configuration file for NVC32.EXE and NVCPM.EXE
NVCBIN.DEF and NVCMACRO.DEF	Virus definition files for NVC32.EXE and NVCPM.EXE
NVCPM.EXE	Menu-driven scanner, virus remover, and scheduler
NVC.INI	Configuration file for NVCPM.EXE

Conventions

Throughout this manual, we use several typeface conventions.

Examples of commands that should be typed or messages that appear on the screen look like this:

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

If certain keys should be used, they will appear with square brackets around the name of the key, as in:

[Ctrl]

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

Help|General Help

And if there is an associated button, we will present it as:

 <u>H</u>elp|<u>G</u>eneral Help

Important notes appear as:

Note: This is important...

And particularly important text appears in **bold**.

Virus Control Basics

In order to use NVC for OS/2 efficiently, we recommend that you use the product as follows:

1. Install NVC for OS/2. For more details, refer to "Installing" on page 8.
2. Run the scanner frequently in order to detect and remove viruses from your removable and/or fixed drives. To help you achieve this on a regular basis, we provide a scheduling feature.
3. Use BootGuard to protect your boot areas.
4. If you find a boot virus on a FAT partition, then remove it using the repair option in NVCPM (see "Repairing Infected Files" on page 84) or the command line scanner (see "Scanning from the Command Line" on page 101). For HPFS or HPFS386 formatted partitions, see "Boot Guard, Generic Boot Area Protection" on page 30.
5. If you find a file virus, then either:
   • move the infected file to a safe location where it will not be executed
   • delete the infected file
   • clean the infected file

Installing

Before You Install

Many anti-virus products are not compatible with each other. Therefore, if you have an anti-virus product other than NVC installed, we recommend that you uninstall it before installing NVC.

Step by Step Instructions

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

First execute A:INSTALL.EXE.

You will see the NVC splash screen and any last-minute instructions, if they exist.

Click **Continue** to proceed or **Cancel** to begin exiting from the install procedure.

The dialog box you will see next depends on whether any previous version of NVC for OS/2 can be found.

First Time Installs

If no previous version of NVC for OS/2 is found, you will next see a dialog box that displays information about the version you are installing.
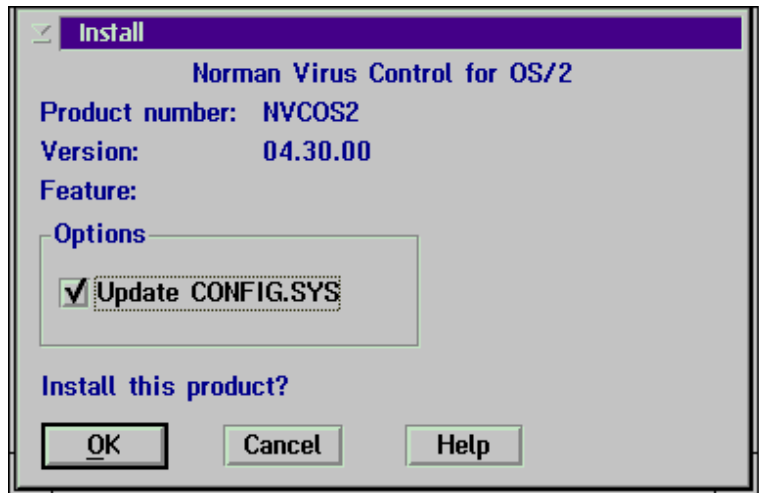
The installation will update the PATH and LIBPATH statements in CONFIG.SYS. Make sure that the update option is checked if you want to update CONFIG.SYS.

Click **OK**, and the available modules are displayed:
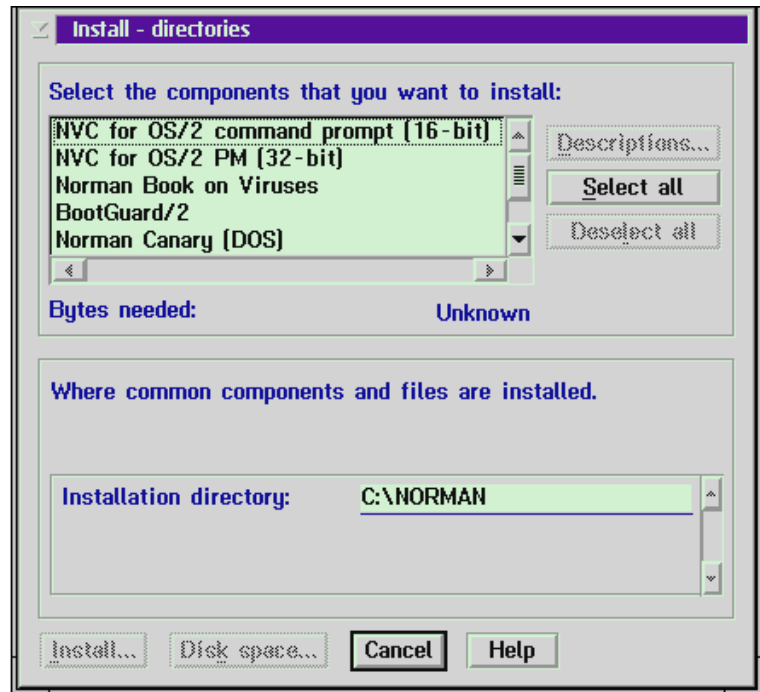
Select those components that you wish to install and specify the installation directory. C:\NORMAN will be suggested as the default.

Click **Install...** to continue, and the progress of the install will be displayed.

After completion, you will be notified as follows:
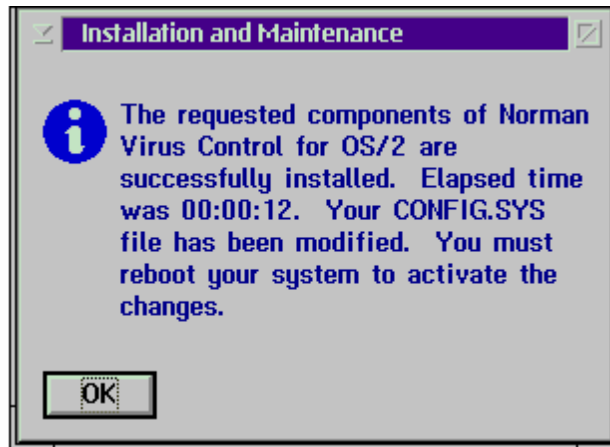
On the desktop, you will see a Norman Virus Control folder whose contents look like this:
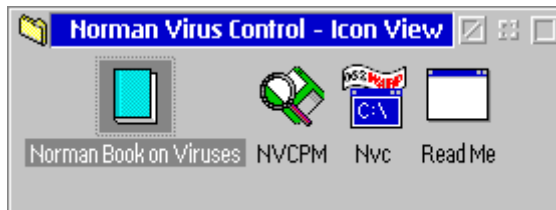
Updating an Old Installation

If a previous version of NVC for OS/2 is found, you can either update the currently installed product or delete it and install the new version.

Installation options

The product has already been installed. Select an option from the list below that indicates how you would like to proceed.

○ Update the currently installed product
◉ Delete the installed product and re-install

Continue   Cancel
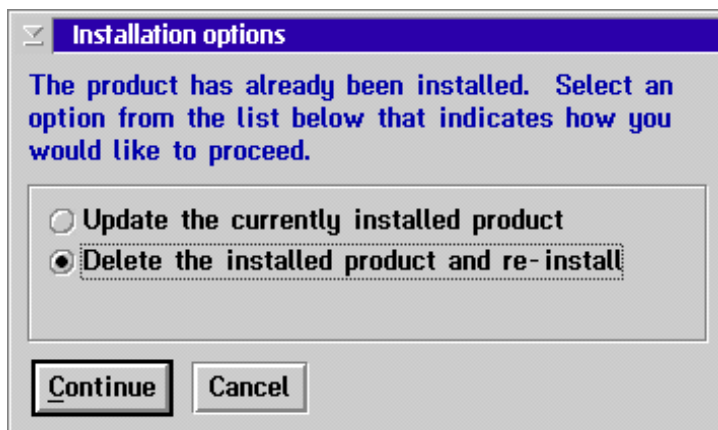
Click on **Continue** and then choose the components that you wish to delete:

Delete

Norman Virus Control for OS/2
Product number: NVCOS2
Version: 04.30.00
Feature:

Select the components that you want to delete:

NVC for OS/2 command prompt (16-bit)
NVC for OS/2 PM (32-bit)
Norman Book on Viruses
BootGuard/2
Norman Canary (DOS)

Select all
Deselect all

☐ Delete only the backup versions

Delete   Cancel   Help
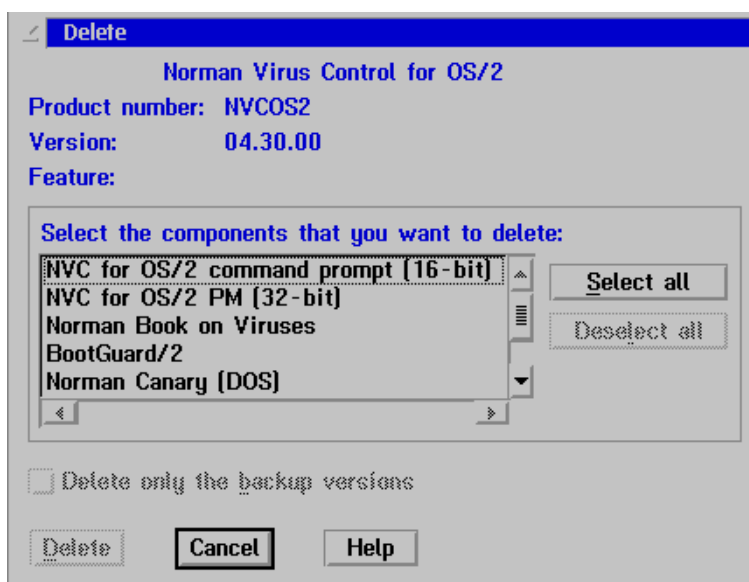
If a backup version is found, you can select all or only the backup by selecting the [ ] **Delete only the backup versions** option.

> **Note:** if you choose to delete all, then all files in the C:\NORMAN directory will be deleted.

Click on **Delete.**

The install procedure will confirm the deletion and then ask if you wish to install the current version.

Click **OK** and continue as described above in "First time installs".

Uninstalling NVC for OS/2

To uninstall NVC for OS/2 either:

- manually delete all the files and subdirectories in C:\NORMAN

  or

- run A:\INSTALL from the installation disks and select the option to [ ] **Delete the installed product and re-install**.
- Then click **Select all** from the next dialog box.
- Click on **Delete** and all NVC for OS/2 files will be deleted.

You will then be asked if you wish to install NVC for OS/2:
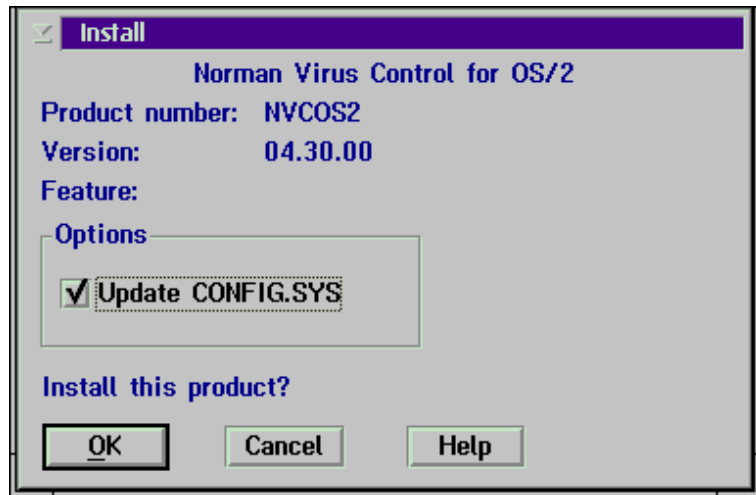
If you click on **Cancel** here, the NVC for OS/2 files are deleted and no new files installed.

Preparing to Use NVC

Understanding What's in the Package

NVC is a set of programs that you may use in whichever combination that is best for you. The following table charts out the modules and their functions.

Module	Function	See
Smart Behavior Blocker (NVC.SYS)	Resident, behavior blocking device driver for DOS. Monitors activity and intercepts virus-like behavior. Does not identify viruses by name. Use one of Norman's scanners for identification.	page 17
Boot Guard (BG2.EXE)	Generic boot area protection and restoration.	page 30
Canary	Non-resident, early warning detector of file viruses.	page 36
Command line scanner (NVC32.EXE)	On demand detection of known viruses in already-infected boot areas and files.	page 103
Menu driven scanner (NVCPM.EXE)	On demand and scheduled detection of known viruses in already-infected boot areas and files.	page 42

Understanding How the Modules Work Together

Now that you know what each module does, you should know more about how the modules work together in order to decide which ones to use.

Module	Works with...
NVC.SYS	**FireBreak**: NVC.SYS sends virus alert messages to FireBreak, which in turn, sends messages to the user, a NetWare group, the server console, and a network printer. FireBreak can also send this alert along as an SNMP trap.
BootGuard/2	Standalone program.
Canary	Standalone program.
Command line scanner (NVC32.EXE)	**SNMP**: if you have the SNMP extension for our command line scanner, you can send messages over the network via SNMP traps. Please ask your network administrator for more details.
Menu driven (NVCPM.EXE)	**FireBreak**: The menu-driven scanner sends virus alert messages to FireBreak, which in turn, sends messages to the user, a NetWare group, the server console, and a network printer. FireBreak can also forward this alert as an SNMP trap. **SNMP**: NVCPM.EXE can send SNMP traps over the network, if it has been so configured by your network administrator. Please ask your network administrator for more details.

Prevention

Norman's Main Philosophy

Norman believes that preventing virus infections is of utmost importance. As a result, a major components in NVC is a smart behavior blocker which prevents infections from known and unknown boot and file viruses.

Although we place much emphasis on behavior blocking, we employ other methods of prevention that rely on generic protection of boot areas and executable files.

Tie these two concepts together with identification and removal of viruses, and you have an all-around anti-virus product.

Behavior Blocking Concepts

Behavior blocking is a relatively new technique in the fight against viruses. One of the reasons Norman uses behavior blocking is because 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 (i.e. previous knowledge of the virus), whereas resident scanning does.

Norman's Smart 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. A simplified view of Norman's Smart Behavior Blocker's reasoning:

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, it does not warrant upgrades each time a new virus is detected.

NVC.SYS is Norman's Smart Behavior Blocker, a DOS device driver that is loaded from `config.sys`. Following is a detailed discussion about NVC.SYS.

NVC.SYS, Norman's Smart Behavior Blocker

Interdependence with other NVC modules:

NVC.SYS protects DOS boxes against file viruses and makes sure that such viruses don't infect the DOS environment as such.

The functioning of other modules is not dependent upon NVC.SYS. It also passes virus alert information to Norman FireBreak and Novell NetWare through IPX communications (see "Norman Programs and IPX Communications" in the *Administrator's Guide*).

Background

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

Therefore, we recommend that you use NVC.SYS.

Note: Because of the way it works, it is important to disable NVC.SYS before you install any new DOS or Windows based software.

Protection

There are three areas on your PC that are vulnerable to viruses: memory, the boot area, and files.

NVC.SYS protects all three areas from becoming infected, and it displays options for next steps appropriate to the type of virus-like behavior that is found.

Because NVC.SYS does not rely on specific scan strings to detect viruses, NVC.SYS does not provide the name of the virus when it issues an alarm. Instead, you are informed of which program is infected or that a boot virus is present.

In the case of file viruses, NVC.SYS attempts to obtain the name of the infected program that is running, and you will receive a warning.

The virus name may not always be available, but NVC.SYS will provide the memory location of the infected program.

As with file viruses, NVC.SYS 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 one of our scanners. See "Specific Detection by Scanning" on page 41 for more information on how to use Norman scanners and "Messages from NVC.SYS in DOS" on page 26 for information on what to do when NVC.SYS issues a warning.

To remove a boot virus from a hard drive or from a file, see "Boot Sector Repair" on page 42 for more on removing boot viruses.

User Interaction

When NVC.SYS intercepts suspicious behavior, it issues audible and visual warnings. In DOS, all warnings are accompanied with up to 3 choices for next steps, based upon the virus activity that is detected. See "Messages from NVC.SYS in DOS" on page 26 for information.

Loading NVC.SYS

If you allow the setup program to modify your startup files, then NVC.SYS is already loaded in `config.sys`. However, you may have chosen to make modifications to `config.sys` manually. In this case, you should have a better understanding of the issues regarding loading NVC.SYS in `config.sys`.

Configuring NVC.SYS

During installation, it is recommended that NVC.SYS be added to `C` without any parameters. There are, however, several parameters that you can use in order to optimize NVC.SYS's performance for your environment.

To use any of NVC.SYS's parameters, simply add them to the end of the line that calls NVC.SYS in `config.sys`. If you are using more than one parameter, remember to add spaces in between the parameters, such as:

```
device=c:\norman\nvc.sys /t /f
```

The available parameters are:

/B Automatically press (B)

Purpose	When to use
/B forces NVC.SYS to automatically select option (B) each time NVC.SYS issues a warning. This means that any virus run will always be disabled in memory, and you will always be permitted to continue your work.	Use this parameter when you wish to always disable a virus in memory.

/C Disable option (C)

Purpose	When to use
/C forces NVC.SYS to disable the "C" option when it displays its warning. Pressing (C) when NVC.SYS warns normally allows a virus to infect.	This is ideal for users who want to prevent accidentally (or intentionally) pressing this key.

Note: This is our recommendation for how NVC.SYS should be installed in most organizations. See "Messages from NVC.SYS in DOS" on page 26.

/F Turn off file tracking

Purpose	When to use
/F prevents NVC.SYS from performing file tracking.	When you are experiencing false alarms with NVC.SYS.

/L Disable logging to local hard drive

Purpose	When to use
/L parameter prevents NVC.SYS from logging its activities to NVCSYS.LOG in the root of C:. By default, NVC.SYS will log virus warning information to C:\NVCSYS.LOG.	If you decide you have no need for a log of NVC.SYS's warnings.

/M Use monochrome

Purpose	When to use
/M forces NVC.SYS to handle the display as monochrome even though your machine may support color.	This can be useful on some laptops. This parameter is automatically enabled when NVC.SYS detects MDA (Mode 7) mode.

/S Suppress warning beep

Purpose	When to use
/S suppresses the beep that normally accompanies a message from NVC.SYS.	When you do not wish to hear the beep.

/T Disable virtual file testing on TSRs

Purpose	When to use
This parameter stops NVC.SYS from conducting a "virtual file" test on programs going TSR.	If a TSR hangs immediately on loading and NVC.SYS does not warn, the TSR might be trying to manipulate the virtual file.

Purpose	When to use
Normally, NVC.SYS performs various tests on programs that go resident in memory. One of these tests is called the Virtual File Test. The file used in the test does not actually exist, but to TSRs, it looks real. Some TSRs, like the EZLAN and SUN NFS redirector, however, attempt to manipulate the virtual file and end up hanging the computer. Viruses, on the other hand, never get confused by the virtual file.	If your machine is configured to be a NetWare Lite Server, you must use /T. If you do not, the computer hangs immediately after SERVER.EXE terminates. If you are loading any of the following programs: 386MAX.SYS, BLUEMAX.SYS, PCNFS.SYS, ELFAX.

Note: If you use the /T parameter for NVC.SYS, then NVC.SYS will not stop the majority of viruses at the moment that they attempt to go resident. However, NVC.SYS will detect the virus when it attempts to infect a file or boot area.

Preventing NVC.SYS from Loading

You should edit `config.sys` by deleting or rem out the line

device=c:\norman\nvc.sys

See also the topic "DOS" in the OS/2 online help index.

Before Installing/Upgrading Software

The only time NVC.SYS might call a legitimate action a virus is during the installation/upgrade of new DOS or Windows software. Therefore, before installing/upgrading new software, you should first scan the new software diskettes for possible viruses **and then you <u>must</u> temporarily disable NVC.SYS.**

This is not necessary when upgrading to new versions of NVC.

Messages from NVC.SYS in DOS

The current version of NVC.SYS is a 16 bit DOS device driver. As such it displays its messages in the DOS environment.

"Possible Virus" Attempts to Trace

When this warning appears, you have executed an infected program, and the virus is now trying to bypass NVC.SYS.) You have three choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will abort the DOS process and the attempt to trace through.
B	Disable It And Continue	NVC.SYS will stop the tracing and let you continue with your work. Most viruses will freeze the DOS process when you choose this option. If this happens, kill the DOS process.
C	Just Continue (At Your Own Risk)	NVC.SYS will allow the tracing to proceed when you press [C]. Do not press this key if you are unsure. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See "Configuring NVC.SYS" on page 21 for detailed information on loading and configuring NVC.SYS and how this affects `config.sys`.

Note: For options A and B, although NVC.SYS has stopped the virus from tracing through, NVC.SYS does not

remove the virus from the infected file.

NVC.SYS reacts differently in situations when Windows is active: NVC.SYS does not offer you choices and instead automatically performs the "B" option.

"Possible Virus" Attempts to Infect

When this warning appears, you have executed an infected program and the virus is now trying to infect other files. This warning is normally generated by direct action (non-resident) file viruses. Such viruses usually search through directories and try to infect a few files before passing the control back to the original program. You have three choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will abort the DOS process and the attempt to trace through.
B	Disable it and continue	NVC.SYS will stop the virus from infecting other files and let you proceed with your work.
C	Just Continue (At Your Own Risk)	NVC.SYS will allow the virus to infect other files. Do not press [C] if you are unsure. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See "Configuring NVC.SYS" on page 21 for detailed information on loading and configuring NVC.SYS and how this affects `config.sys`.

Note: For options A and B, although NVC.SYS has
prevented the virus from infecting other files, NVC.SYS
does not remove the virus from the infected program. Run
the scanner with the option *Repair files when possible* to
remove the virus.
If NVC.SYS prompts you with this message 3 times, this
means that the virus is trying to infect 3 different files.
Sometimes a virus tries to infect ALL the files on a hard
drive. If this happens, NVC.SYS will prompt you with this
warning ceaselessly. At this point, the best solution is to
press [A] and then run the scanner with the Repair option
ON.

"PROGRAM.EXT" Is a Virus Carrier

When this warning appears, you have executed an infected
file, and the virus is now trying to become resident in
memory. NVC.SYS is able to differentiate between an
uninfected TSR program and an infected TSR program,
even though both of them stay resident. You have three
choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will abort the DOS process and the attempt to trace through.

| B | Disable It And Continue | NVC.SYS will unhook the virus so that it cannot infect other files and let you continue with your work. |
| C | Just Continue (At Your Own Risk) | NVC.SYS will let the virus go memory resident. Do not press this key if you are unsure. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See "Configuring NVC.SYS" on page 21 for detailed information. |

Note: For options A and B, although NVC.SYS has prevented the virus from becoming resident, NVC.SYS has not removed the virus from the infected file. To do so, run the scanner with the Repair option ON.

If you use the /T parameter for NVC.SYS, then NVC.SYS will not stop the majority of viruses at the moment that they attempt to go resident. However, NVC.SYS will detect the virus when it attempts to infect a file or boot area.

"PROGRAM.EXT" Attempts to Format the Hard Drive

When this warning appears, a virus or a program is trying to perform a low-level physical format of the hard drive. Even DOS's FORMAT does not perform a low-level

format, so this is highly suspicious behavior. You have three choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will kill the DOS process and stop the attempt by the virus or program to reformat the hard drive.
B	Disable It And Continue.	NVC.SYS will stop the program from reformatting the hard drive and let you continue with your work.
C	Just Continue (At Your Own Risk)	NVC.SYS will let the virus or program do its deed, reformatting the hard drive. Do not press this key if you are unsure. You may disable the availability of this option by installing NVC.SYS with the /C parameter.

Note: For options A and B, although NVC.SYS has stopped the attempt to reformat the hard drive, NVC.SYS has not removed the virus from the infected file. To do this, run the scanner with the Repair option ON.

Boot Guard, Generic Boot Area Protection

In addition to the Smart Behavior Blocker, NVCPM provides one module that uses generic methods to protect the boot area and one module that uses generic methods to protect files.

NVC for OS/2 now includes BG/2, an utility for saving, verifying and restoring boot sectors on OS/2 computers.

Background

Most boot sector viruses expect to find FAT partiotioned disks, and will in most cases leave the system unusable if your partitions are formatted with the HPFS or HPFS386 file systems.

The ability to safekeep, verify and restore boot sectors will normally be an efficient cure in case this happens.

BG/2 is meant as a tool for system administrators and technically qualified users. Used correctly, BG/2 will not harm the integrity of your disks. However, as other software, BG/2 may fail in some very unlikely situations and cause irrepairable damage to the data on your disks. Therefore, Norman recommend that you implement proper backup routines for all data that you cannot afford to loose. Also, remember to verify the backups so you know that they contain valid data.

Getting Started with BG/2

For an overview of the functionality, execute the BG2 command without any parameters:

BG2

BootGuard/2 will respond with the following:

NORMAN

Norman Boot Guard for OS/2 v1.00
Usage: BG2 [-v] {-c | -d | -r}

BG/2 Options

-c

Compare disk boot sectors to data in file BG2.DAT.

-d

Dump disk boot sectors to file BG2.DAT.

-r

Restore disk boot sectors from file BG2.DAT.

`-v`

Verbose. Hexdump differences when used with `-r` or `-c`.

`-V`

More verbose. Hexdump all boot sectors found.

Saving boot sectors

To save the boot sectors of an OS/2 computer, execute the following command:

`BG2 -d`

BootGuard/2 will respond with something like:

```
NORMAN

Norman Boot Guard for OS/2 v1.00

Partitions and boot sectors found:

  Physical disk 0:

   Master Boot Sector.
   Boot manager SBS.
   Disk partitions:

     0 Drive C, Primary partition, HPFS, OS2TEST
     1 Drive D, Logical disk, HPFS, OS2
     2 Drive E, Logical disk, HPFS, SWAP
     3 Drive F, Logical disk, HPFS, DATA

Data saved in file BG2.DAT.
```

BG2.DAT will, in addition to the boot sector data itself, store information about the disk geometry, about where each boot sector is located, and CRCs for all the data. All this information locks the file to this given configuration for this given computer.

In case you need to restore the boot sectors, BG/2 will deny to restore data if the disk geometry is changed, if the disk is repartitioned, or if the location of the individual boot sector is changed. All these rigorous rules will also prevent you

from accidentally restore a BG2.DAT from another computer.

A header identifying the file is also added.

To view this information, execute the following command:

```
TYPE BG2.DAT
```

```
  File produced by Norman Boot Guard for OS/2
  v1.00
  On 27. August 1997 11:20:08
  Contains boot sector data for:
  Physical disk 1: MBS, Boot manager, SBS for
  Drive C, D, E, F.
```

Keep BG2.DAT in a safe place

Now you should copy both BG2.EXE and BG2.DAT to a floppy or to a network drive.

Label the floppy with information that positively identifies the computer.

Keep the floppy in a safe place, for example together with the emergency boot diskettes. If you do not have emergency boot diskettes, this is the time to create them.

To create Emergency boot diskettes, open the "System setup" folder and start "Create Utility Diskettes". You need three formatted 1.44MB floppies for this task.

Checking for Changes in Boot Sectors

Execute the following command to check for changes:

```
BG2 -c
```

BootGuard/2 will respond with something like:

```
NORMAN
```

```
Norman Boot Guard for OS/2 v1.00
Partitions and boot sectors found:
  Physical disk 0:
```

```
      Master Boot Sector.
      Boot manager SBS.
      Disk partitions:
      0 Drive C, Primary partition, HPFS, WARP3
      1 Drive D, Logical disk, HPFS, OS2
      2 Drive E, Logical disk, HPFS, SWAP
      3 Drive F, Logical disk, HPFS, DATA
Comparing data...
      Physical disk 0, Drive C: SBS is different
      from stored data.
      * Volume label changed.
```

To get more information about the changes, add the $-v$ option:

BG2 -c -v

This option will print the differences as a hex dump of the current boot sector and the stored boot sector. Hex dumps of all boot sectors, stored and current, will be printed if you use the option $-V$ (capital V).

Restoring Boot Sectors

1. Boot the computer from the emergency start diskettes.
2. Insert the floppy with BG2.EXE and BG2.DAT and execute the following command:

   BG2 -r

BG/2 denies any restore if you have added or deleted partitions since the last dump:

BG2: Error restoring boot sectors.
The file might be damaged or might belong to
another computer.
If the file is from this computer, the disks
have been repartitioned.
In either case, boot sector data cannot be
restored.

Other changes to the master boot sector of the disk, caused by a boot sector virus or by other means, will make BG/2 respond with something like:

```
Physical disk 0: Master Boot Sector is dif-
ferent from stored data.
* Jump address changed.
* Boot code changed.

Do you want to restore this boot sector
(Y/N)?
```

Type Y to continue, anything else to abort. If you typed Y, BG/2 will respond with:

```
WARNING!

Restoring a boot sector will overwrite the
current boot sector on your hard disk. Do not
proceed unless you know exactly what you are
doing.

Do you want to proceed (Y/N)?
```

Type Y to proceed, anything else to abort. The master boot sector will now be restored.

For changed system boot sectors, BG/2 will ask:

```
Physical disk 0, Drive C: SBS is different
from stored data.
* Other areas changed.

Do you want to restore this boot sector
(Y/N)?
```

Type Y to continue, anything else to abort. You will be asked to confirm the restore as for the master boot sector.

Detection

Generic Detection with Canary

Usually, virus detection is accomplished by knowing characteristics about each individual virus. As a result, the anti-virus vendors must play a game of "catch up" with the virus authors.

However, Norman provides a generic method of detection using Canary.

Note: Canary is not dependent on any other NVC module and is not critical for any other module's functioning.

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 DOS-based Canary programs (CANARY.COM and CANARY.EXE). The Canary programs work as one-time, **non-resident** "bait" for known and unknown file viruses that infect .COMs and .EXEs, and they alert you if 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 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, however, 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.
```

And if a virus has infected the .COM file, the message will read:

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

```
COM:The Canary Bird is Dead!
```

You can suppress these messages and report by errorlevel instead. See "Canary's Errorlevels" on page 40 .

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 "Specific Detection by Scanning" on page 41 for more information on scanners.

Using Canary

You must run Canary 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 Canary frequently. Here are three ways to ensure maximum protection:

1. To ensure that the system always activates Canary after you have used a program, insert 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.
2. Implement a resident scheduling function that will start Canary at regular intervals.
3. Develop a good habit of starting Canary manually several times a day.

Frequent use of Canary means swift detection, and swift detection results in less damage.

The syntax for running Canary is:

```
canary [reporting level] [Enter]
```

Note: If no file extension is specified, then DOS will first look for the filename as a COM. If found, the .COM will be run. If not found, then it will look for the filename as an EXE. When you run CANARY.COM, CANARY.EXE will be called. Since we want to launch Canary as bait for viruses that infect both .COMs and .EXEs, there is no need to specify an extension when running CANARY.

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 allows Canary to avoid being attached 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 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, but 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 are modified/infected.
2	CANARY.EXE is modified/infected.
1	CANARY.COM is modified/infected.
0	CANARY.COM and CANARY.EXE files are normal.

Specific Detection by Scanning

Scanning is a way to identify viruses that already exist in files or boot areas. Identifying these by name requires that the scanner recognize the virus, which means that scanners must be frequently updated for information on new viruses.

NVC for OS/2 includes a command line scanner (NVC32.EXE) and a menu-driven scanner (NVCPM.EXE).

Both scanners share some functions:

1. They use the same configuration (NVC32.CFG) and definition files (NVCBIN.DEF and NVCMACRO.DEF) .
2. They scan certain pre-defined file extensions. Refer to the Read Me file for more details.

Because we believe most of you will use the PM scanner, we will first discuss NVCPM.EXE and then discuss NVC32.EXE.

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.

Boot Sector Repair

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 backup diskette. A dialog box complete with on-line help will guide you through the process if a boot sector virus is detected.

Starting NVCPM

To start NVCPM, simply open the Norman Virus Control folder and click on the "NVCPM" icon.

After NVCPM has started, the steps to follow are:

a. Select areas to scan — a single drive, multiple drives, single directory, single file, or group of files. See "Selecting Areas to Scan" on page 47 .

b. Configure scanning options. See "Scanning Options Notebook" on page 50.

c. If desired, save the current configuration as a style. See "Styles" on page 67 for a discussion of styles.

d. If desired, set up a scheduled scan. See "Scheduling" on page 95.

The Main Window

After you start NVCPM, the main window appears.
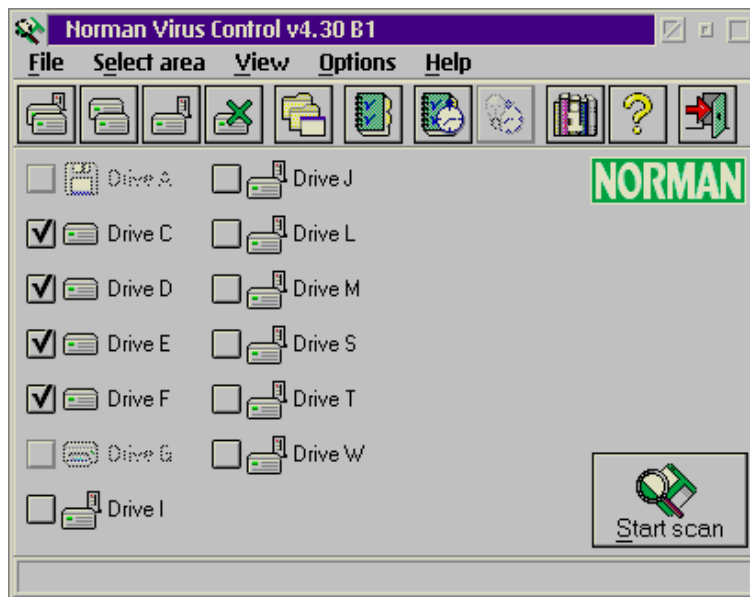
It consists of the following parts:

The menu bar

> Access menu items for functions such as displaying files or boot areas in hexadecimal format; selecting areas to scan; viewing reports, the Virus Library, or the Book on Viruses; configuring scanning and scheduling options; and displaying on-line help.

> Press [F1] when a menu item is in focus to get help about that item.

The button bar

> Contains shortcuts for the most frequently used commands. See the section below for more details on the button bar.

Drive icons

Set or clear check marks to enable or disable scanning for the given drive.

Disabled items are those that are currently unavailable due to missing media or for other reasons.

The Start scan button

Select this button to start scanning the selected drives.

The Button Bar

The button bar contains shortcuts for the most frequently used commands:

 Select area|Fixed drives

Select all fixed and network drives for scanning. Floppy drives are **not** included in this selection, and the boot areas of network drives are **not** scanned.

See "Selecting Areas to Scan" on page 47.

 Select area|All local drives

Select all local fixed drives for scanning. Floppy drives are not included in this selection.

See "Selecting Areas to Scan" on page 47.

 Select area|Network drives

Select all networked drives for scanning. This function is not available unless you have a corporate license. Note that the boot areas of network drives are **not** scanned.

See "Selecting Areas to Scan" on page 47.

 Select area|Deselect drives

Remove the check marks for all selected drives.

See "Selecting Areas to Scan" on page 47.

Select area|<u>D</u>irectories/files.

Scan a given directory, single file, or group of files. See "Directories/files" on page 48.

See also "Selecting Areas to Scan" on page 47.

<u>O</u>ptions|Scanning <u>o</u>ptions

Configure the scanning options. See "Scanning Options Notebook" on page 50.

<u>O</u>ptions|<u>S</u>cheduler options

Configure the scheduler options. The scheduler must be set up before it can be turned on.

This is the case when NVCPM is started for the first time or if no NVC.INI was found when the program started.

Note: All NVCPM options and settings are stored in a file named NVC.INI, which is found in the working directory of NVCPM.EXE. NVCPM may behave erratically if this file is damaged. If you suspect damages, exit NVCPM, delete NVC.INI and restart the program. A new file with default settings will then be created automatically.

See "Scheduling" on page 95.

Options|Scheduled scan on

This icon indicates that the scheduler has been configured and turned on.

This icon can also be disabled, as in [icon], indicating that the scheduler has not been configured. Therefore, it is not possible to start the scheduler.

See "Scheduling" on page 95 for more information.

Options|Scheduled scan o<u>ff</u>

When on, the icon will show a lit light bulb. Execute this command, or click the icon to turn it off.

<u>V</u>iew|<u>V</u>irus Library

View the virus library. Refer to "Virus Library" on page 88.

For more general information on viruses, see "Book on Viruses" on page 93.

<u>H</u>elp|<u>G</u>eneral help

View the general help for the main window.

<u>F</u>ile|E<u>x</u>it

Exit NVCPM.

Default Configuration

When you start NVCPM for the first time or if NVC.INI is not found, then certain options are set by default:

- all local drives are selected
- the scanner will not stop scanning when a virus is found
- the scanner will ignore locked files
- the scanner will log all infections to the file NORMAN.RPT in the directory in which NVCPM.EXE resides.
- all previous instances of the report file will be overwritten.
- the scanner will leave infected files where they are found
- the scanning thread will execute at idle priority.

- • the scanner will beep when an infection is found
- • all changes to the scanning options will be saved upon exiting NVCPM

The following sections discuss all options within NVCPM.

Selecting Areas to Scan

Prior to starting a scan, you should first select the area that you wish to scan.

You may select these areas using three methods:

1. Use the left-most buttons on the button bar.

2. Use the "Select area" pull down menu.

Note: Selecting areas from the pull down menu is an additive function. That is, if you first select all local drives and then select fixed drives, NVCPM will select the superset, which is fixed drives in this case.

---

3. Specify drives or directories/files from the command line. Refer to "Using the Command Line Scanner" on page 103 for more details.

Fixed drives

Select all fixed and network drives for scanning. Floppy drives are not included in this selection, and the boot areas of network drives are **not** scanned.

Command line parameter: /AD

All local drives

Select all local fixed drives for scanning. Floppy drives are not included in this selection.

Command line parameter: /ALD

Network drives

Select all networked drives for scanning. This function is not available unless you have a corporate license. Note that the boot areas of network drives are **not** scanned.

This function is not available from the command line.

Deselect drives

Remove the check marks for all selected drives.

This function is not available from the command line.

Directories/files

Scan a given directory, single file, or group of files.

From the command line, specify the desired path entries.

If you choose "Directories/files", you will see:
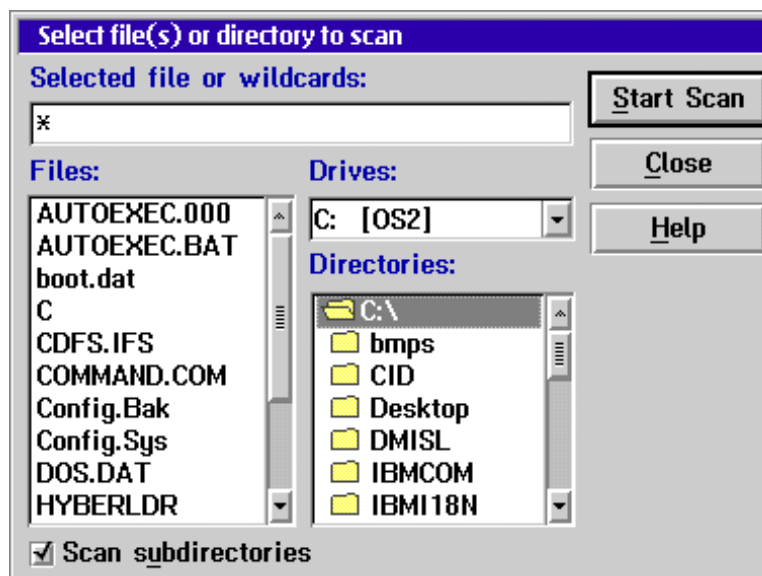
1. Use the Drives: list to select the desired drive.
2. Select the desired directory in the Directories: list.

A "*" appears in the Selected file or wildcards: field. NVCPM will accept wildcards so that you may enter "*.com", for example, in order to scan a group of files.

Or you can click on one or several files in the Files: list.

Set a check mark next to "Scan subdirectories" if you wish to include the subdirectories of the selected directory.

Note: From the command line, use the parameter "/S" for subdirectories if you are specifying a directory rather than a drive.

Then click "Start scan" in order to begin scanning.

Note: When choosing directories/files, ensure that your scanning options are set up prior to entering this dialog.

Scanning Options Notebook

After selecting the area that you wish to scan, you should configure the scanning options that you wish to use.

You may access these options using three methods:

1. Use the scanning options button on the button bar.

2. Click on the "Options" menu item on the main window and then select "Scanning options".
3. Use command line parameters. Refer to "Using the Command Line Scanner" on page 103 for more details.

The first two methods bring you to the scanning options notebook, which allows you to change the way NVCPM scans for viruses, how it treats infected files, and how it creates reports.
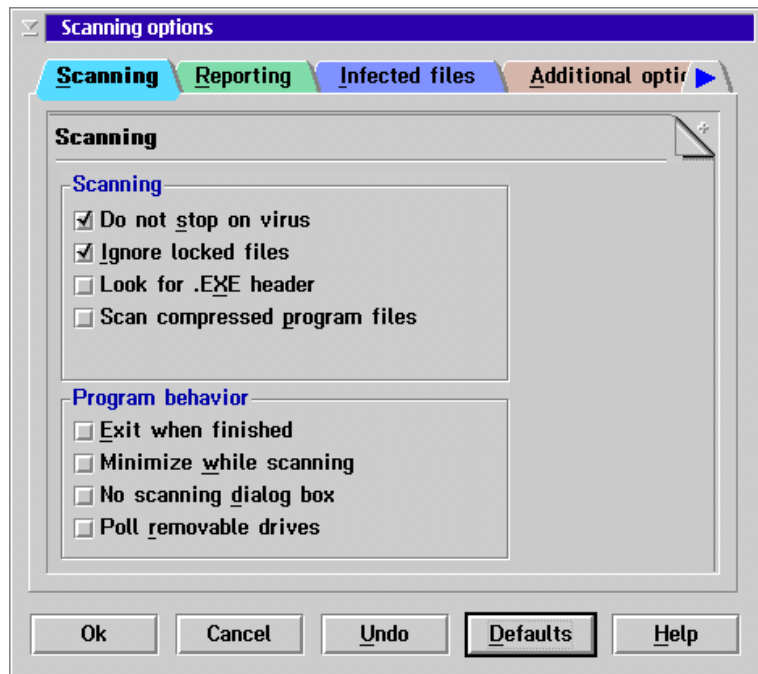
Five buttons always appear at the bottom of the notebook:

OK

Save all changes and close

Cancel

Discard all changes and close

Undo

Undo all the selections you have made so far.

Defaults

Load default values. See "Default Configuration" on page 46.

Help

Display help on the scanning options notebook.

Scanning Options Page

There are two sections on this page: "Scanning" and "Program behavior".

Scanning options

Scanning | **Reporting** | **Infected files** | **Additional optio** ▶

Scanning

Scanning
- ☑ Do not <u>s</u>top on virus
- ☑ <u>I</u>gnore locked files
- ☐ Look for .E<u>X</u>E header
- ☐ Scan compressed <u>p</u>rogram files

Program behavior
- ☐ <u>E</u>xit when finished
- ☐ Minimize <u>w</u>hile scanning
- ☐ No scanning <u>d</u>ialog box
- ☐ Poll <u>r</u>emovable drives

| Ok | Cancel | Undo | Defaults | Help |
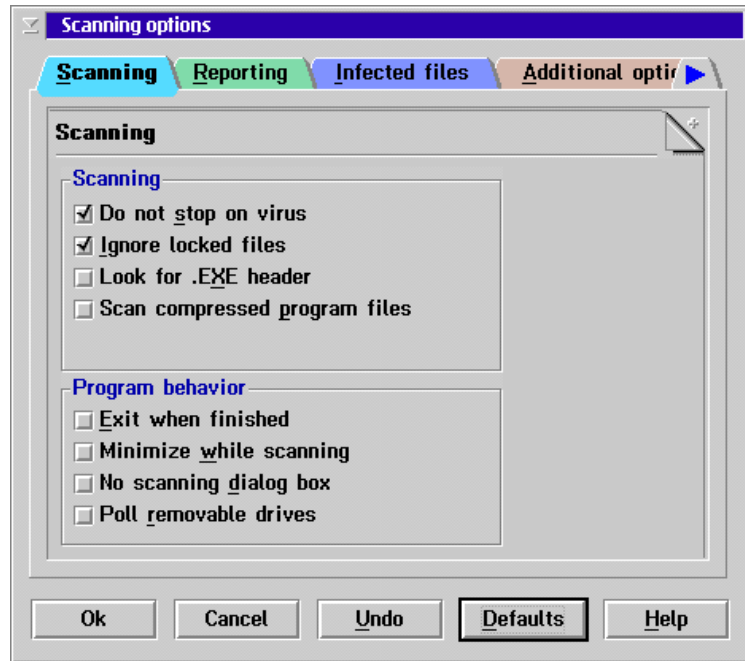
In the section called "**Scanning**", there are 5 options:

Do not stop on virus

Check this option if you do not want NVCPM to stop when an infected file or area is encountered. It will handle the infection as specified on the "Infected files" options page. Refer to "Infected Files Options Page" on page 59.

Removing the check mark will force the NVCPM to pause when an infected file or area is encountered. You will be asked about what to do with the infected file.

Possible Virus Found

Possible virus found in:
C:\viruses\ANTHRAX.COM

Virus type:
Anthrax

Status:
Infected

Continue

Cancel scan

Virus info...

Delete file

Move file...
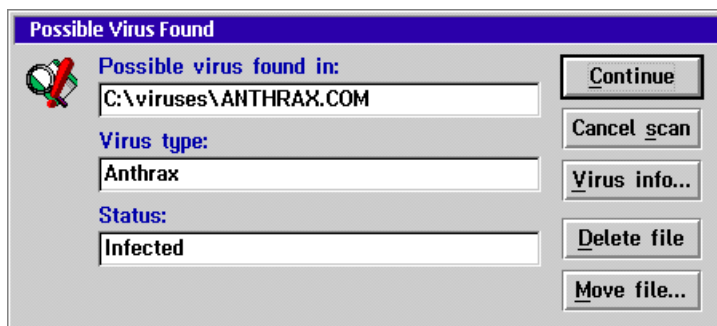
Default setting: On

Associated command line parameter: /YH forces NVCPM to **pause** at each virus it finds.

Ignore locked files

A locked file is a file that cannot be opened by NVCPM for some reason. The system paging file, C:\OS2\SYSTEM\SWAPPER.DAT is an example of such a file.

Removing the check mark will make NVCPM display a message box when a locked file is encountered.

Default setting: On

Associated command line parameter: /O

Look for .EXE header

Most viruses find candidates for further infection by looking for the file type *.EXE or *.COM. But some look at all file types for the unique pattern found in the beginning of an executable program. By setting this check mark, and the "Scan all files" option on the Additional options page, NVCPM will also look for the same pattern in all files. Refer to "Additional Options Page" on page 61.

Default setting: Off

Associated command line parameter: /X

Scan compressed program files

Set the check mark if you want compressed program files (executables that have been PKLITE'd, DIET'ed, LZEXE'd or ICE'd) to be decompressed and scanned for viruses.

Note: This option is different from the "Scan archive files" option on the Archive files page. Refer to "Archive Files Options Page" on page 65.

Default setting: Off

Associated command line parameter: /CP

In the section called "**Program behavior**", there are 4 options:

Exit when finished

Forces NVCPM to exit when the scanning is complete.

Note: When this is turned on and a virus is found, the results of the scan will not be displayed as a dialog.

Default setting: Off

Associated command line parameter: None

Minimize while scanning

Minimizes NVCPM into an icon for the duration of the scanning.

Default setting: Off

Associated command line parameter: /Q

No scanning dialog box

If this option is checked, then the "Scanning for viruses" dialog will not be displayed when the scan starts. See "The Scanning for Viruses Dialog" on page 75.

Instead, the "Start scan" button on the main screen will act as a toggle between starting and stopping the scan, and the bottom line of the main window will display the areas that are being scanned and a progress bar.

Default setting: Off

Associated command line parameter: None

Poll removable drives

Set the check mark if you want NVCPM to poll all removable drives for media periodically. If not checked, the list of available drives will be those found when NVCPM was started.

Default setting: Off

Associated command line parameter: None

Reporting Options Page

There are two sections on this page: "Reporting" and "Include in report".
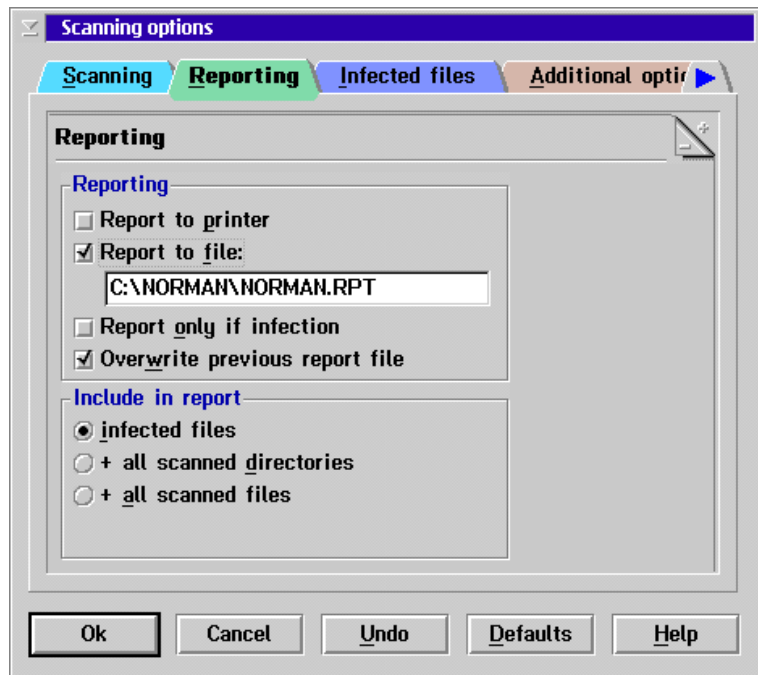
In the section called "**Reporting**", there are 4 options:

Report to printer

Set the check mark if you want NVCPM to send the report as ASCII text to :PRN when the scanning ends.

Default setting: Off

Report to file

By default, NVCPM writes a report to the file NORMAN.RPT in the directory in which NVCPM.EXE resides. Remove the check mark if you do not want any report. Change the filename if you want the report to be written to another file. Make sure that the path exists.

The file will be created if it does not exist.

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 it does exist, you will be given the opportunity to append to the existing file, to overwrite it, to give the new information a new filename, or to skip the report file.

If this option is unchecked, all other options under this one become grayed.
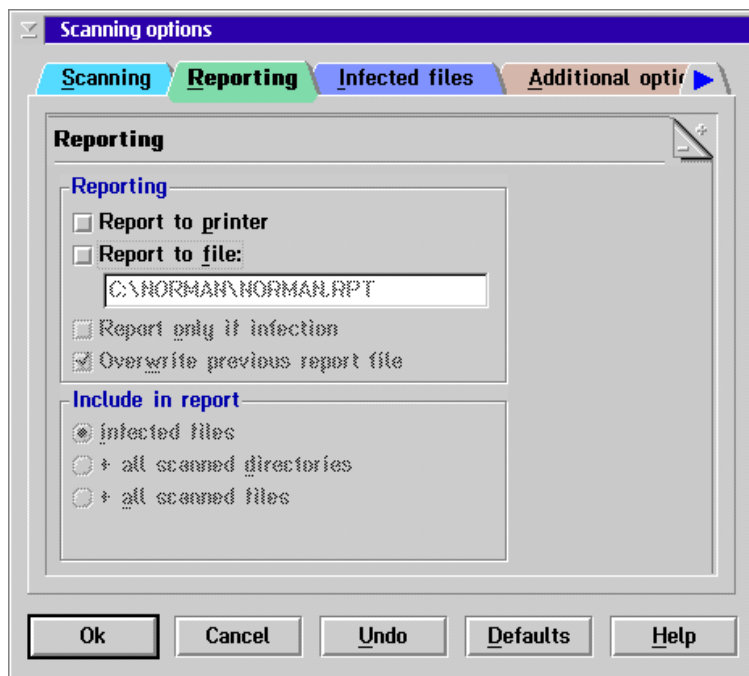
Default setting: On

Associated command line parameter: /LF:[filename]

Report only if infection

If checked, NVCPM will only create the report file if infected files or areas are encountered.

When this is checked, NVCPM will automatically enable the "infected files" option in the "Include in report" section. See "Reporting Options Page" on page 55.

Default setting: Off

Associated command line parameter: /LQ

Overwrite previous report file

Normally, NVCPM appends information to the end of a report file, if the given filename matches a file that already exists.

Set the check mark if you want the report file to replace the file that already exists.

Default setting: Off

Associated command line parameter: /LG forces NVC32.EXE to **append** to the log file.

In the section called "**Include in report**", there are 3 options:

Infected files

If checked, then NVCPM will include the filenames of only the infected files in the report.

Default setting: On

Associated command line parameter: None. This is the default.

+ all scanned directories

If checked, then NVCPM will also include the names of all scanned directories.

Default setting: Off

Associated command line parameter: /LS

+ all scanned files

If checked, then NVCPM will also include the names of all scanned directories and files. This will make the report quite long. NVCPM will ask for permission to continue without reporting, if all available disk space is exhausted by the report file.

Default setting: Off

Associated command line parameter: /LA

Infected Files Options Page

There is only one section on this page, and it contains 5 options.
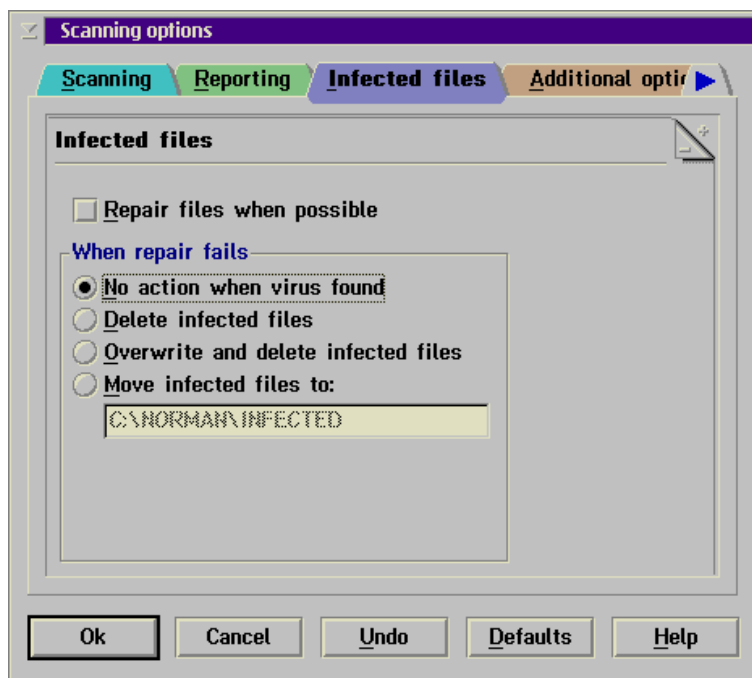
Repair files when possible

This option ensures that viruses detected during on-demand or scheduled scans are removed on-the-fly, if possible. If this option is checked, you are well protected against all known viruses.

Default setting: Off

Associated command line parameter: /CL

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

No action when virus found

This is the default, forcing NVCPM to leave infected files alone.

Default setting: On

Associated command line parameter: None. This is the default.

Delete infected files

Set this option if you want NVCPM to delete infected files. Infected files on write-protected media cannot be deleted. NVCPM will alert you if the delete fails.

The file will be deleted in a way that prevents recovery by the OS/2 UNDELETE command.

Default setting: Off

Associated command line parameter: /D-

Overwrite and delete infected files

Same as "delete infected files", but all sectors occupied by the file will be overwritten by 0xFF and then 0x00 before the file is deleted.

Default setting: Off

Associated command line parameter: /D

Move infected files to:

Set this option if you want all infected files to be moved into a safe location. The default location will be a subdirectory called "INFECTED" off the Norman home directory (C:\NORMAN\INFECTED by default).

First the infected file will be copied then deleted. NVCPM will alert you if any of these operations fail.

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.

Default setting: Off

Associated command line parameter: /MOV:[path]

Additional Options Page

There is one section on this page, and it has 5 options:
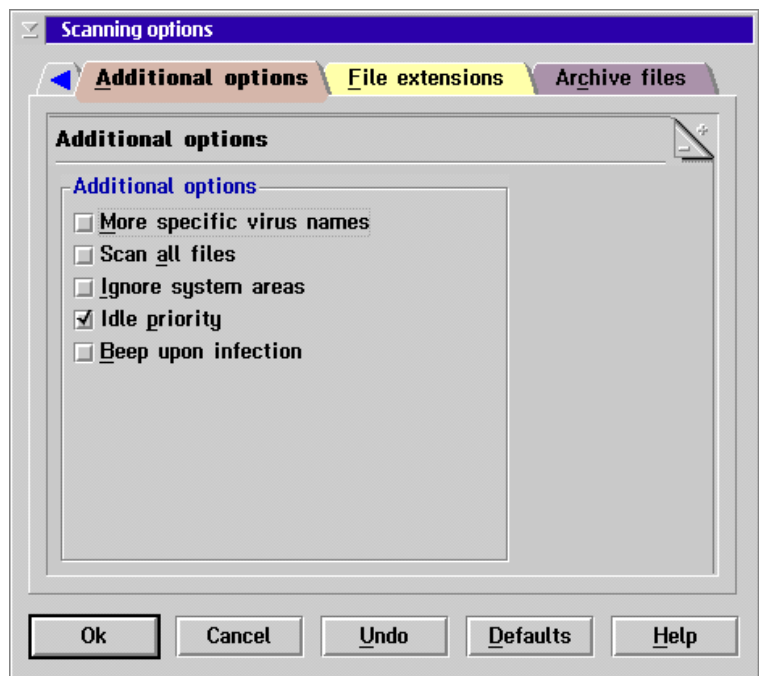
More specific virus names

Enable this option if you want detailed virus names to be displayed. Disable it if names of the type "Jerusalem related" are sufficient. Note: This does **not** increase the number of viruses detected.

Default setting: Off

Associated command line parameter: /Y

Scan all files

Set this check mark if you want NVCPM to scan all files regardless of file extension. Because all files are scanned, scanning time and the possibility of false alarm both rise. Use this option in conjunction with the "Look for .EXE header" option (see "Scanning Options Page" on page 51).

Note that compressed program files will only be scanned if you have turned on the [ ] **Scan compressed program files** option.

> *Default setting:* Off

> *Associated command line parameter:* /AF

Ignore system areas

Set this check mark if you do not wish to scan the system areas (the Master Boot Sector [MBS] and System Boot Sector [SBS]) on all drives. This means that boot sector viruses will **not** be found.

> *Default setting:* Off

> *Associated command line parameter:* /BS-

Idle priority

Set this check mark if you want the scanning thread to execute at idle priority. Otherwise, the scanning thread will execute at normal priority. That is, scanning will occur at a priority level similar to other applications.

All applications executed on the system are given CPU priority depending on the process's priority class. The priority classes are: Time Critical, Server, Normal, and Idle.

The first class is used for programs that must react very quickly to system events, such as interrupts. The server class is used mainly for other time critical processes. User applications will normally belong to the next lower class, Normal. In this class all programs have their priority

adjusted dynamically, boosting the foreground program ahead of programs currently in the background.

Processes running in the Idle class will get the CPU only when no other process is running.

> *Default setting:* On

> *Associated command line parameter:* None

Beep upon infection

If checked, NVCPM will emit a small beep when infections are found.

> *Default setting:* On

> *Associated command line parameter:* /B turns **off** the beep.

File Extensions Options Page

Unless the [ ] **Scan all files** option on the "Additional options page" is set, NVCPM will scan for viruses in files with certain extensions.

See the Read Me file for more information.

Scanning options

| ◄ | Additional options | **File extensions** | Archive files |

File extensions

─ User defined file extensions ─

☐ New type

```
386
APP
BAT
BIN
COM
CPL
DLL
DOC
DOT
DRV
```

Add

Remove

| Ok | Cancel | Undo | Defaults | Help |
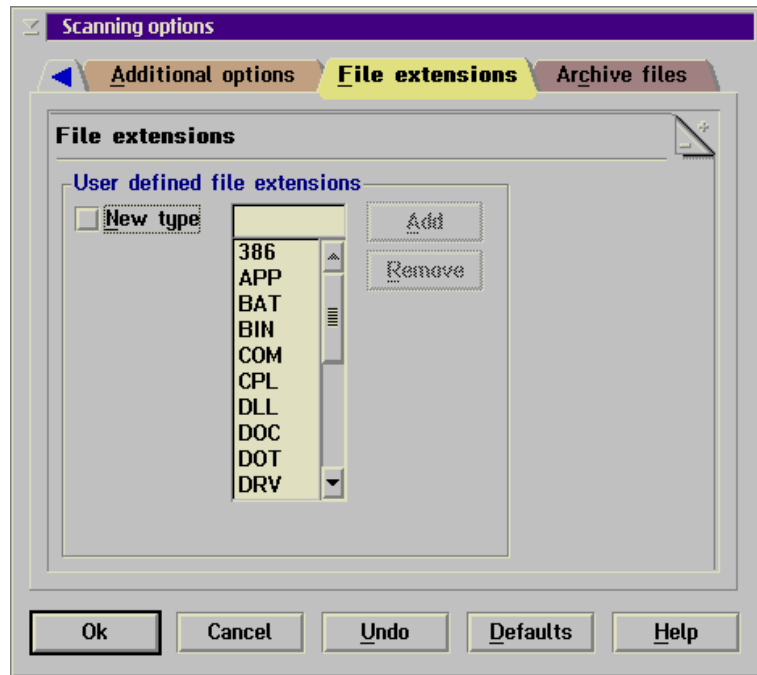
If you wish to add up to 16 file extensions to the search, check the [ ] **New type** box, which is normally unchecked.

Type the desired file extension and select [Add] to add it to the list of desired file extensions.

Highlight unwanted file extensions in the listbox and select [Delete] to delete them.

Both Add and Delete actions can be reversed by selecting the opposite button.

Note: You cannot delete the system's default extensions.

Default setting: Off

Associated command line parameters: None

Archive Files Options Page

By default, NVCPM does not scan archive files (.ZIP, .ARJ, etc.) for viruses. You can, however, instruct it to do so by checking the "Scan archive files" option on the "Archive files" options page.
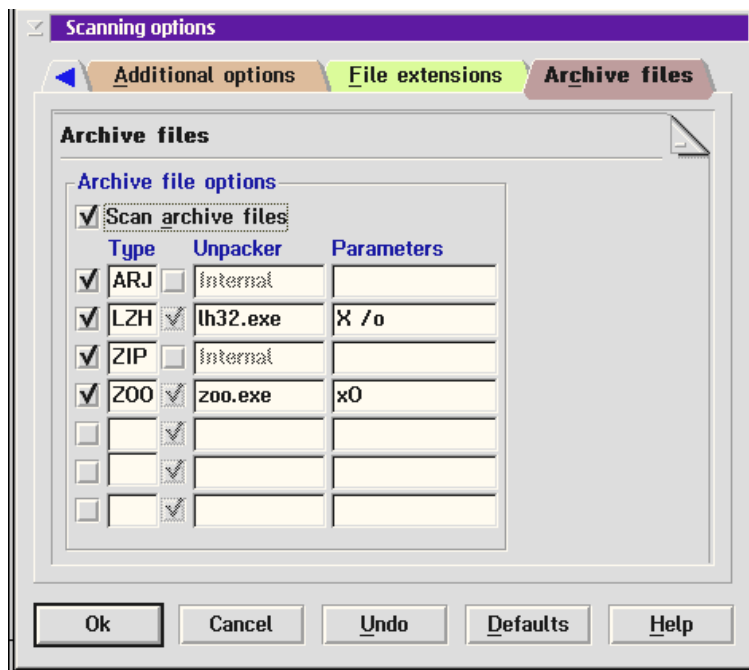
We define an archive file as a single file that contains one or multiple other files. Usually some type of compression is used in order to archive the file so that it is an efficient way to transfer files or to free space on hard drives and floppy disks.

Note: These options are **not** related to the option called "Scan compressed program files". See "Scanning Options Page" on page 51.

Default setting: Off

Associated command line parameter: /C

Underneath this option is a table that allows you to specify up to 7 different file types, what type of unpacking method should be used, and what parameters should be used.

Enable unpacking and scanning of an archive file type by setting the check mark in the left column. Remove the check mark if you don't want this file type to be scanned.

NVCPM uses two types of unpacking methods: internal and external. Where possible, NVCPM uses internal methods in which an external program is not spawned but rather internal functions are called. When internal methods are possible, the middle column is marked "internal".

Alternatively, external methods are used in which the packed files are unpacked onto the hard drive. In this case, the middle column designates the unpacker and any command line parameters to be used.

If you wish to use external methods, place a check next to the middle column and specify an executable to be used for unpacking. The executable must be an OS/2 program found on the path.

Certain default parameters will appear in the last column. These parameters **must** order the unpacker to skip creation of subdirectories found inside the archive file because subdirectories created by the unpacker will be scanned but not deleted correctly. Skipping subdirectory creation is the default action for most unpackers such as PKUNZIP.EXE but not for InfoZip's UNZIP.EXE.

If external methods are used and the specified file type is found, the associated executable will be spawned with the indicated parameters. A subdirectory in the TEMP directory will be used for unpacking the archive. If no TEMP or TMP environment is found, the subdirectory will be created in the directory in which NVCPM resides.

For example, if you have the TEMP environment pointing to E:\TEMP, then scanning A:\TEST.ZIP will result in executing:

```
CMD /C unzip.exe -j -o "A:\TEST.ZIP" >
"E:\TEMP\TEMP\NVCTEMP.OUT" 2>&1
```

The file is unpacked in the directory E:\TEMP\TEMP. If this executes without any errors, the unpacked files will be scanned and then deleted. Finally, the directory E:\TEMP\TEMP will be deleted. Output from the "unzipper" will be written to NVCTEMP.OUT. The 2>&1 ensures that both stdout and errout are directed to the output file.

The directory E:\TEMP\TEMP and the file NVCTEMP.OUT in it will remain when NVCPM is finished. In case you have trouble such as running out of disk space while unpacking, this file should be inspected.

Styles

If you have preferences for how the scanner is to be run, you can save those settings as **styles** and then use the styles whenever you wish. Think of styles as templates for scanning.

You can:

1. Set up the style with the desired scanning options prior to using it.

   or

2. Configure NVCPM with the desired scanning options and then save the options as a style.

   or

3. Save configuration changes in the current style when NVCPM exits.

The difference between the first two methods is when you assign a name to the style — before setting the scanning

options or after. And the difference between the last method and the first two is when the changes are saved.

NVCPM is shipped with the style <NORMAL> as the default. This style can be modified but not deleted. In addition to customizing <NORMAL>, you may create up to 7 additional styles.

Styles can be used in on-demand scans as well as scheduled scans.

See "Scheduling" on page 95 for more information.

In addition, you may start NVCPM with a certain style from the command line.

Refer to "Specifying a Style on the Command Line" on page 102.

In order to use a style in the current session of NVCPM, you must make it **current**. All style names except for <NORMAL> will be displayed in three places: NVCPM's title bar, the "Scanning for viruses" dialog box, and the "Styles" dialog box.

When NVCPM starts, it will load the last used "current" style.

Setting Up Styles Prior to Using Them

From the main window, click Options|Styles, and you will see the "Styles" dialog:
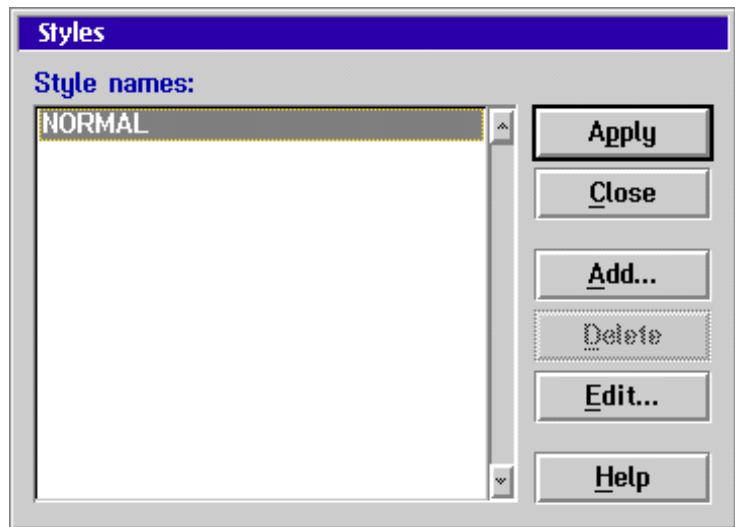
All existing styles are shown in the listbox called "Style names:".

From here, you can select a style and then:

Apply

Apply the selected style and close the dialog box. This will make the selected style **current**. That is, all scanning options will be based on the current style.

If you have made changes in the previous current style, you will be prompted to save the changes before another style is made current.

Close

Close the dialog box.

Add...

Add a new style. This brings up the style editor.

Delete

Delete the selected style. You will **not** be prompted before it is deleted. The style <NORMAL> cannot be deleted.

Edit...

> Edit the selected style.

Help

> View on-line help on this dialog box.

Adding A New Style

When you click the **Add** button, you will see:
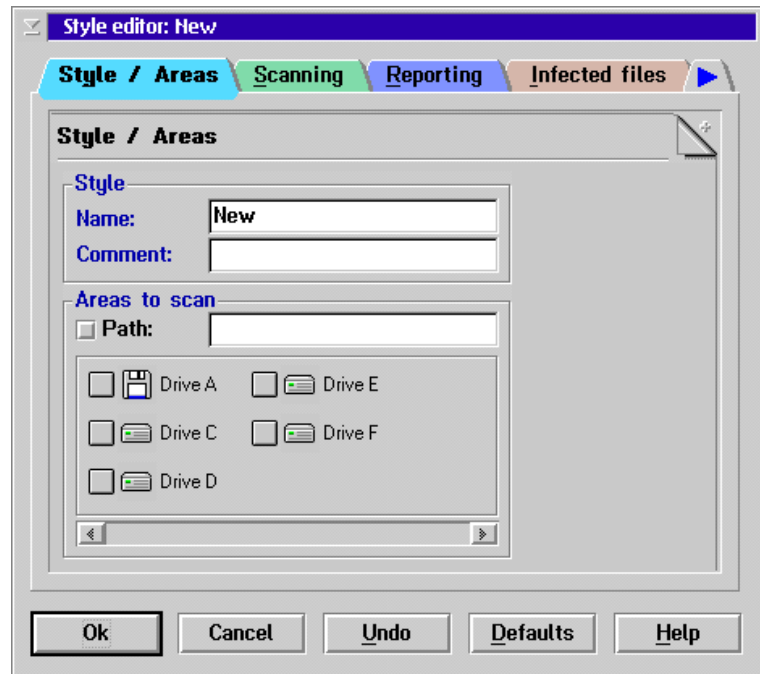
1. NVCPM automatically assigns the style name as \<New>. You must change this to something else because the name \<New> is reserved. Note that the name \<NORMAL> is also reserved. We recommend that you choose a name that describes what the style does. The name can be up to 16 characters long.

2. If you wish, enter a comment about the style, up to 73 characters long.

3. If you wish to scan a specific directory, then set a check mark next to "Path:", and enter the path here.

Note: You may not enter a filename or wildcards here.

4. Or if you wish to scan drives, then set check marks next to the desired drives.

5. Then set the remainder of the scanning options for the style:

    Scanning options page. See "Scanning Options Page" on page 51.

    Reporting options page. See "Reporting Options Page" on page 55.

    Infected files options page. See "Infected Files Options Page" on page 59.

    Additional options page. See "Additional Options Page" on page 61.

    Archives files options page. See "Archive Files Options Page" on page 65.

6. To undo changes, click Undo. To revert back to the factory default options, click Defaults. To discard all changes and exit this function, click Cancel. Or click OK to accept all changes and return to the "Styles" dialog.

7. If you would like to make the new style current, then click Apply.

Editing An Existing Style
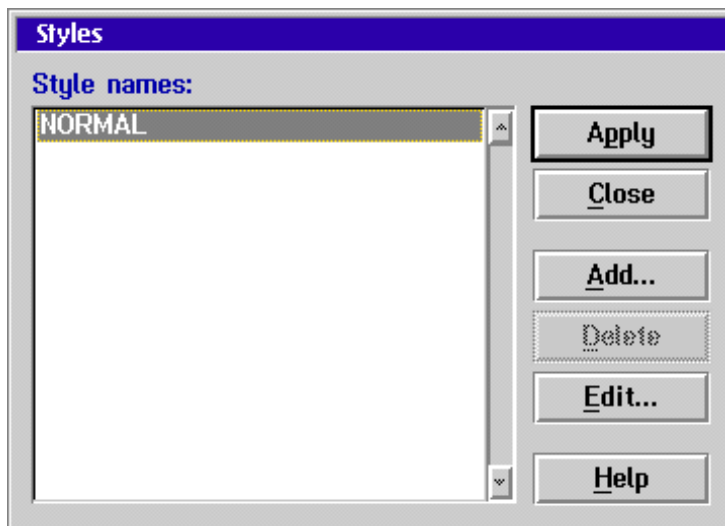
If you have already created a style, and you wish to make changes to it, go to the "Styles" dialog by clicking Options|Styles from the main window.

1.   Select the style and click "Edit...".
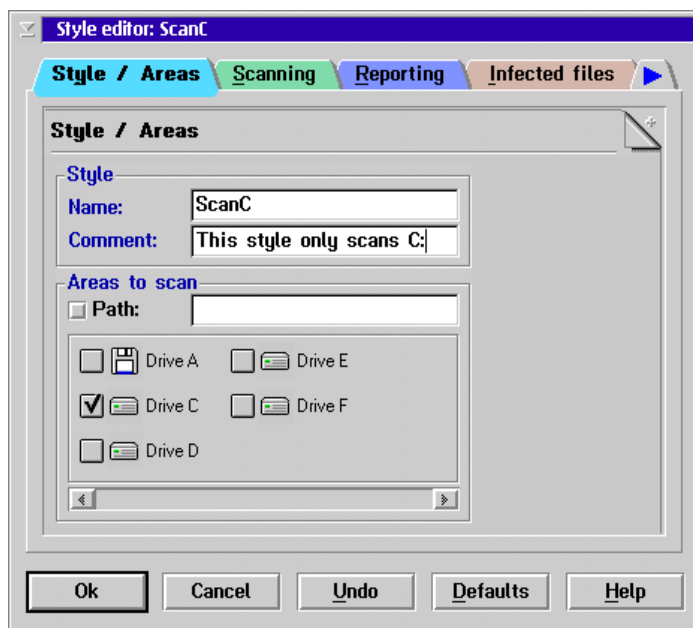
2. Select the areas to be scanned.

3. Then go to each tabbed dialog and set the configurations that you wish.

For further reference see:

Scanning options page. See "Scanning Options Page" on page 51.

Reporting options page. See "Reporting Options Page" on page 55.

Infected files options page. See "Infected Files Options Page" on page 59.

Additional options page. See "Additional Options Page" on page 61.

Archive files options page. See "Archive Files Options Page" on page 65.

4. To undo changes, click Undo. To revert back to the factory default options, click Defaults. To discard all changes and exit this function, click Cancel. Or click OK to accept all changes and return to the "Styles" dialog.

5. If you would like to make the edited style current, then click Apply.

Deleting a Style

To delete a style, click on the Delete button.

You will not be asked to confirm the deletion, and you cannot delete the current style.

Save as Style After Configuring

If it's more convenient, you may configure NVCPM first and then save the options as a certain style. To do so, simply choose the areas to scan and the desired scanning options. Then click on Options|Save as style.

The name of the current style is listed in the listbox. From here, either enter a new style name or choose the name of an existing style. If you choose an existing style, all options that were previously saved in that style will be overwritten.

You may choose to make this style current by checking the [ ] **Make saved style current** box.

Save on Exit

By default, NVCPM will save all configurations in the current style when NVCPM exits. To turn this feature off, deselect the Options|Save on exit menu item.

The Scanning for Viruses Dialog

When a scan begins, the scanning for viruses dialog appears:
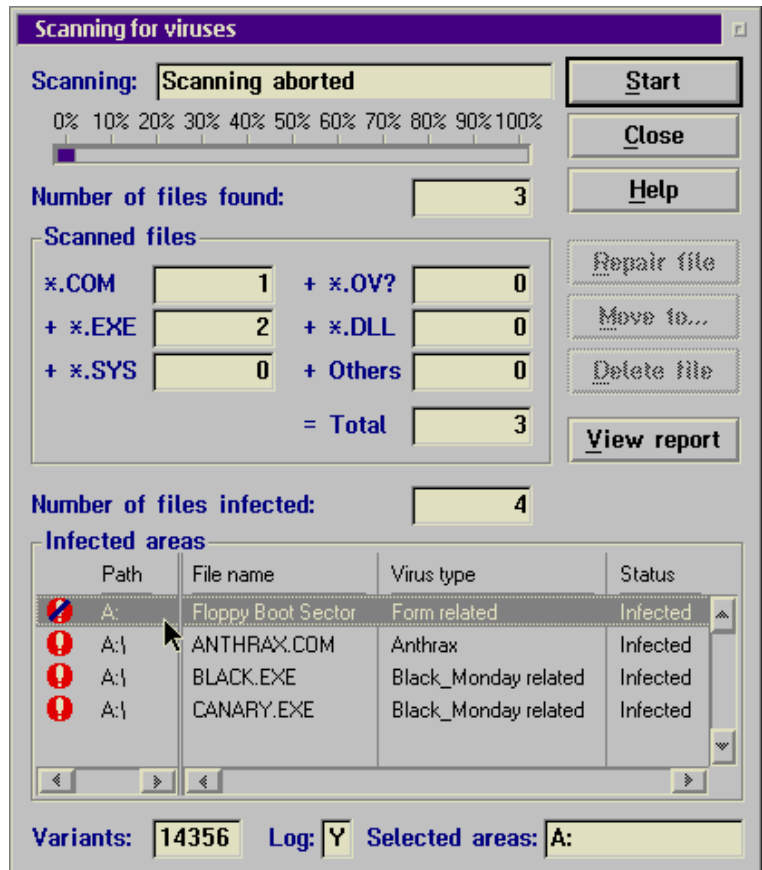
This displays the progress of the scan, and it contains status information, an overview of infected files, and several buttons.

Field	Description
Scanning	the area that is currently being scanned.

Progress bar	the percentage of the scan that has been completed.
Number of files found	the total number of files found in the selected area.
Scanned files	the number of different file types to be scanned in the selected area. **Note**: The number of files found in the specified directory will almost always be different than the number of files scanned because NVCPM only scans files with the default extensions in addition to the user-defined file types you specify. Refer to the Read Me for more details on the default file extensions.
Number of files infected	the total number of files found to be infected.
Infected areas	this listbox contains the path, filename, virus type, and status of infected files.
Variants	the total number of virus variants that can be detected in this version of NVCPM.
Log	the values in this field are either "Y" or "N", depending on whether reporting to a file has been turned on.
Selected areas	shows the area that was selected for the scan.

Button	Description
Start	is disabled while scanning. Select [Start] to restart a stopped scan. This is very useful when scanning a set of diskettes. Select drive A: only as the search area and then start scanning. When the first diskette is scanned, insert a new one and select [Start] to restart the scanning. This method may also be used for scanning other removable media such as Bernoulli disks and CD-ROMs.
Stop	stops an ongoing scan. NVCPM will finish scanning the current directory before the scanning is stopped. This button is changed to [Close] when the scan is stopped, and clicking on it will close the dialog box. **Note**: you can also stop an ongoing scan by clicking on the "Stop scan" button in the main window.
Help	brings up help on the "Scanning for viruses" dialog.
Repair	is disabled while scanning. If an infected file is found, you may highlight it from the "Infected areas" listbox and then click on [Repair file]. A file cannot be repaired if it resides on a write-protected floppy, a CD-ROM, a network drive and the file is write-protected, or if the file is in use (i.e. you do not have write access).

Move to...	is disabled while scanning. If an infected file is found, you may highlight it from the "Infected areas" listbox and then click on [Move to...] in order to move it to a specific location. C:\NORMAN\INFECTED is suggested as the default location. **Note**: NVCPM cannot move infected files if it does not have the access rights to do so (e.g., it cannot remove an infected file from a write-protected floppy).
Delete file	is disabled while scanning. If an infected file is found, you may highlight it from the "Infected areas" listbox and then click on [Delete file] in order to delete it. In this instance, NVCPM will not overwrite the file(s) prior to deletion. **Note**: NVCPM cannot delete infected files if it does not have the access rights to do so (e.g., it cannot delete an infected file from a write-protected floppy).
View report	displays the report file that is specified in the Reporting options page. See "Reporting Options Page" on page 55. **Note**: this button will be grayed out if reporting has not been turned on. You may also view a previously existing report file by selecting View|Report from the main window. For more information, see "Interpreting the Report File" on page 110.

When No Viruses Are Found

If the scanning was completed successfully, and no viruses are found during the scan, you will see:

Scanning finished

No viruses were found in the scanned areas.

Close   View report   Help
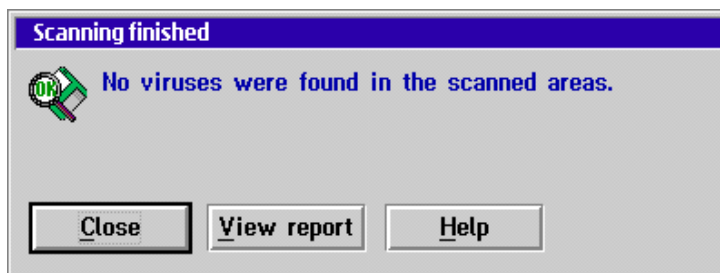
If the scanning was aborted before completion, and no viruses were found in the areas that were scanned, you will see:

Scanning aborted before completion

No viruses were found in the scanned areas.

Close   View report   Help
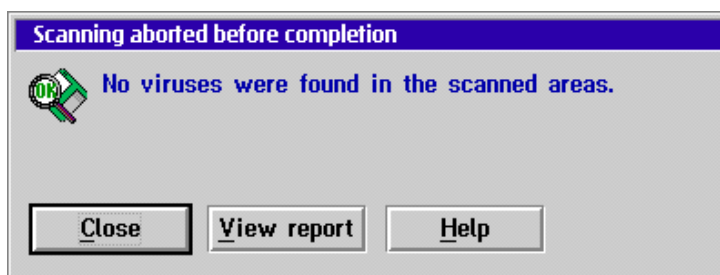
When a Virus Is Found

Unless the [ ] **No scanning dialog box** option has been checked, then you will first see the "Scanning for viruses" dialog:

Then as viruses are found, you will see them listed in the "Infected areas" section of the dialog.

Note: If you have instructed NVCPM to delete or move all infected files, the deletion or the move will occur automatically without requiring user input.

If you have instructed NVCPM to stop on each virus, then you will see the following:
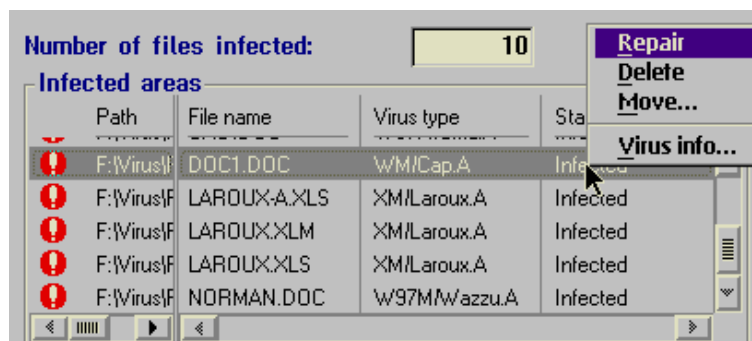
From here, you can choose to continue, cancel the scan, view information about the virus, repair or delete the infected file, or move the infected file.

If you delete the file, it will not be overwritten before it is deleted. And if you choose to move the file, the destination C:\NORMAN\INFECTED will be offered by default.

At the end of on-demand scans (i.e., not scheduled scans), this dialog is shown after the scanning has completed:
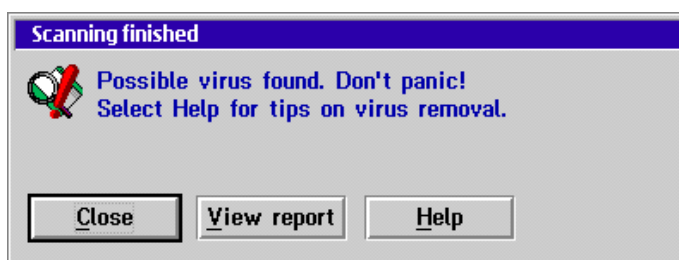
At this point, there is no cause for alarm. An infected file will not infect other files until it is executed, or for macro viruses, until the document is opened.

If you close the dialog box, no information about infected files is lost, and you will be returned to the "Scanning for

viruses" dialog where you will be able to deal with infected files.

First you will see the summary of infections in the "Infected areas" section of the "Scanning for viruses" dialog.

NVCPM can remove all viruses known to NVC.

Therefore, from the "Scanning for viruses" dialog, it is possible to highlight individual infected files or groups of infected files and either repair, delete, or move them to a different location.

After repairing, moving and/or deleting infected files, the icon at the left of the "Infected areas" section will change to a check mark, as in:
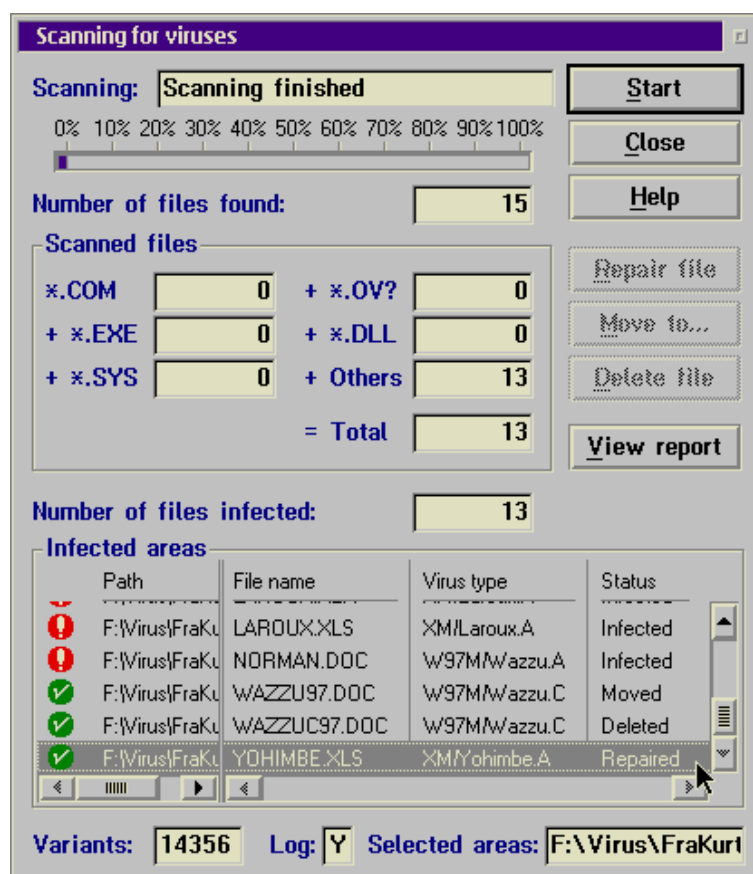
If NVCPM is not able to repair, move or delete the virus, you will see a symbol in the "Infected areas" section of the "Scanning for viruses" dialog.
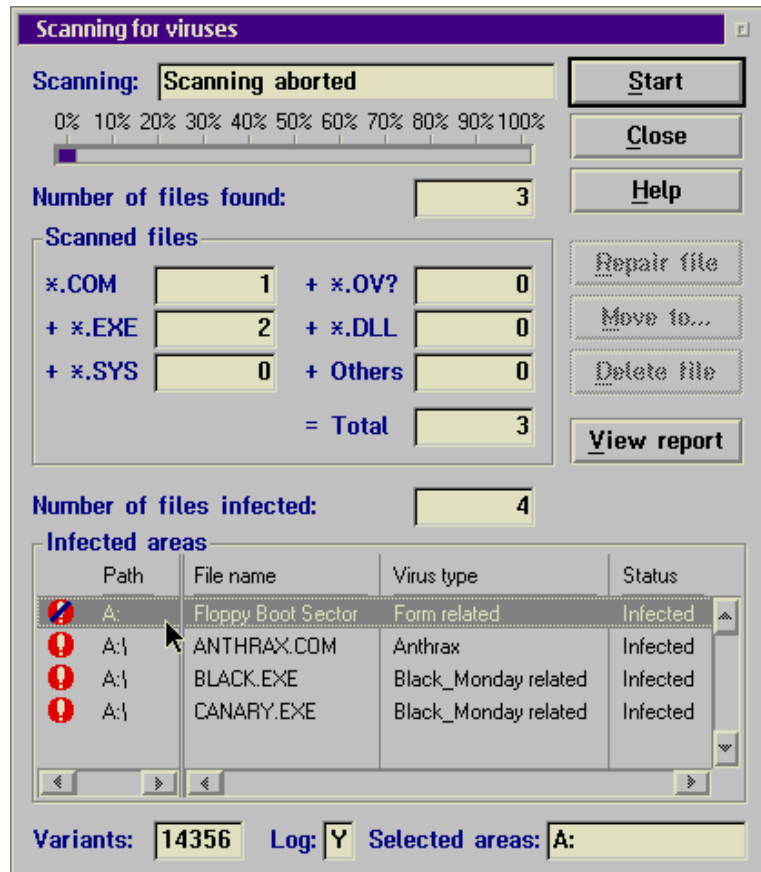
The last column in the "Infected areas" listbox will tell you the status of the infected file. That is, the display will tell you if the file has been repaired, moved, or deleted.

Repairing Infected Files

You can repair a single file or a group of files. A range of files can be highlighted by clicking on the first and last file while holding down the [Shift] key. And a set of files can

be highlighted by clicking on individual filenames while holding down the [Ctrl] key.

Then click on [Repair file], and the infected file(s) will be removed. After a successful removal of a virus, the status field will display "Repaired".

Note: It is also possible to repair infected files by highlighting the file, clicking on the right mouse button [RMB] and then choosing **Repair file**.

Moving Infected Files

You can move a single file or a group of files. A range of files can be highlighted by clicking on the first and last file while holding down the [Shift] key. And a set of files can be highlighted by clicking on individual filenames while holding down the [Ctrl] key.

Then click on [Move to...], and C:\NORMAN\INFECTED will be suggested for a destination. Change this path, if desired, and then click on [Move files].

Move files

Move files to:

C:\NORMAN\INFECTED

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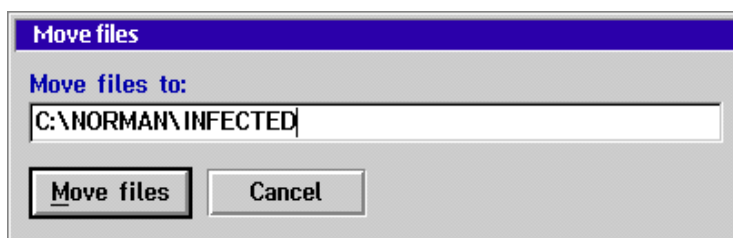
You might have several infected files which happen to have the same name. If NVCPM tries to move a file to a certain directory and finds that the filename already exists in that directory, it will change the name of the newest file until it is unique.

The renaming technique used 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 NVCW moves it to the C:\INFECTED directory. Then NVCW finds another copy of COMMAND.COM that is infected and moves it to the C:\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.)

Note: It is also possible to move infected files by highlighting the file, clicking on the right mouse button [RMB] and then choosing <u>**Mo**</u>ve.

Deleting Infected Files

You can delete a single file or a group of files. A range of files can be highlighted by clicking on the first and last file while holding down the [Shift] key. And a set of files can be highlighted by clicking on individual filenames while holding down the [Ctrl] key.

Then click on **Delete** and NVCPM will automatically delete the selection without asking for confirmation.

Note: using this method, NVCPM will not overwrite the file before deleting it. If you wish to have the file overwritten prior to deletion, then turn the "Overwrite and delete infected files" option on. See "Infected Files Options Page" on page 59.
It is also possible to delete infected files by highlighting the file, clicking on the right mouse button [RMB] and then choosing **Delete**.

Virus Information Dialog

When an infected file is found, you very often want to know more about the virus. You can easily view this information from the "Scanning for viruses" dialog.

Click on the selected file with the right mouse button [RMB] in order to get a context menu:
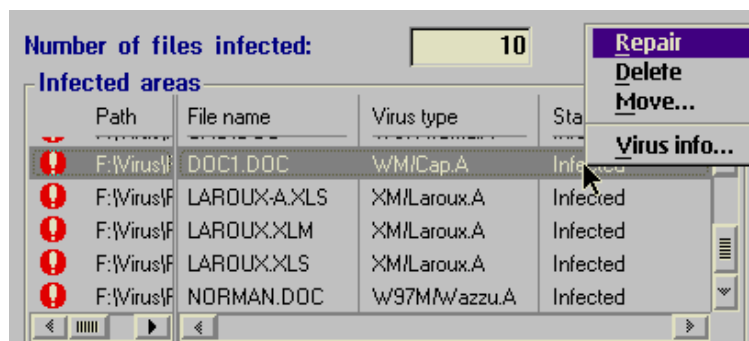
Choose **Virus info**, and you will see the virus information dialog.
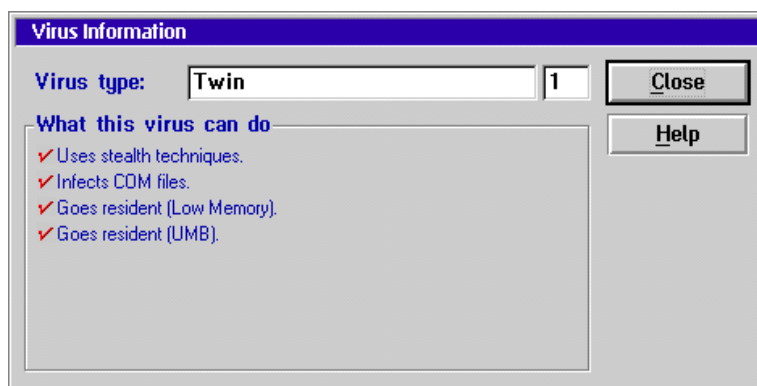
It displays the virus name, the number of variants of the virus, and some basic characteristics.

For a complete list of all the viruses that NVCPM can recognize, go to the Virus Library, which is discussed in the next section.

In addition, you can browse through more general information on viruses in the Book on Viruses. See page 93.

Virus Library

The virus library has two tabbed dialogs, one for binary file and system viruses and one for macro viruses. Here you will find key information for every virus in this list.
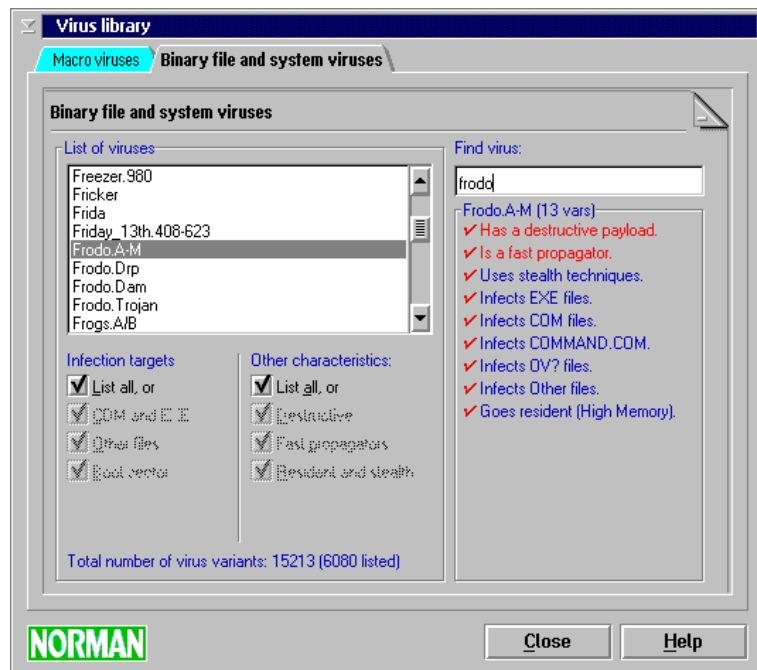
Computer viruses can be categorized in two distinctly different classes: binary and macro viruses.

1. *Binary file and system 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.

To view information about a certain virus:

• Type the first letter of the desired virus in the "Find virus" field. You may also type the following letters of the virus name during the search.

   or

• Scroll the list of viruses until the desired virus is found.

By default, NVCPM will display all the viruses that it can detect. However, you may filter the display to look for viruses that infect only certain targets or that have only certain characteristics.

To use these filters, either uncheck the [ ] **List all** option under "Infection targets" and/or "Other characteristics" or check the desired options.

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 floppy 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
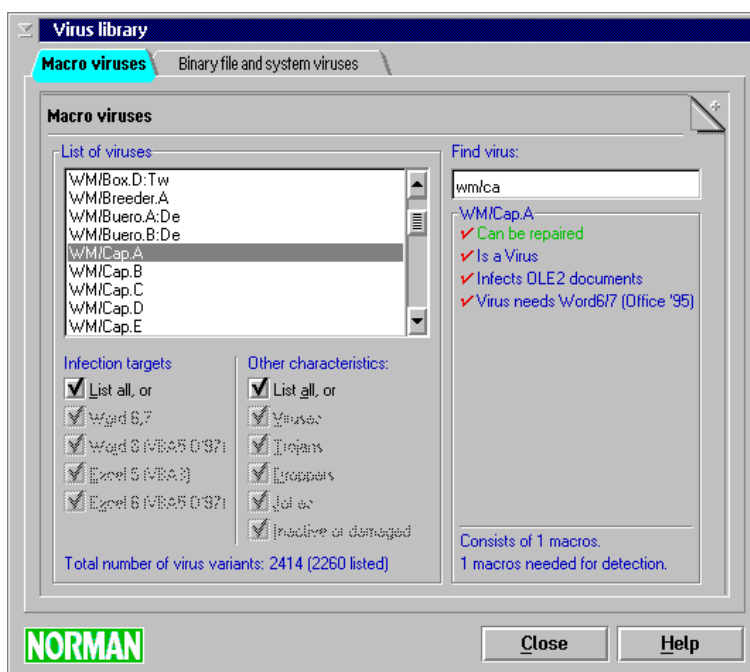
These are the possible attributes for macro viruses:

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 88.

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.

Note: Virus Library is only available on the command line through the command line scanner with the /LV parameter.

Book on Viruses

As an extra feature, the Norman Book on Viruses is available as on-line help. Browse through the Book for more general information about viruses.

Display File and System Areas

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 options in the File menu.

To display a file, select File|Display file.
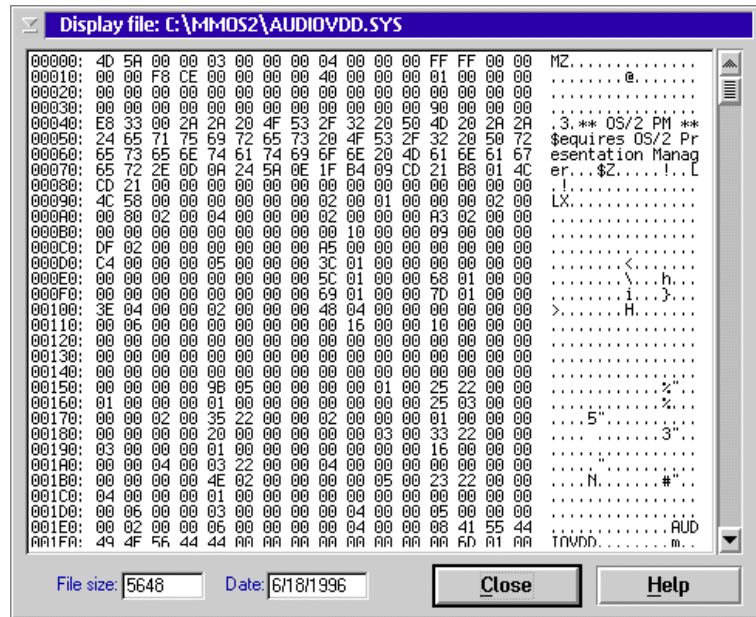
Then select the desired file and click **OK**.

To display system areas, select File|Display system areas.

Physical disks and logical partitions are shown in the "Select area" portion of the display. The right hand side of

the display shows the contents of the corresponding boot sector.

Select a disk or partition icon and scroll the listbox at the right to view the entire 512 byte sector. To exit from this dialog, select **Close**.

Note: These functions are not available from the command line.

Scheduling

Many users like to have the flexibility to schedule virus scans periodically.

From the scheduler you can define:
- when scanning should start
  Today (Default)
  Once at
  Hourly from
  Daily from
  Weekly from
  Monthly from
- what style should be used

To set up a scheduled scan:

1. Save the scanning configuration that you wish to use during a scheduled scan and save it as a style. "Styles" on page 67.
2. Either select **Options|Scheduler options** or click on the scheduler options icon from the main window.

3. Determine when you wish to start the scheduled scan(s).
4. Ensure that NVCPM is running — either maximized, minimized, or hidden.

> **Note:** this function is not available from the command line.

Configuring a Scheduled Scan

The scheduler must be configured before it can be turned on.

When NVCPM is started for the first time or when no NVC.INI is found, the scheduler is not configured, and therefore it is not possible to turn it on. This is how the scheduler status button on the main window will look:

And the **Options|Scheduled scan on** and **Options|Scheduled scan off** menu items will be grayed.

To configure the scheduler, select **Options|Scheduler options** or click on the scheduler options icon from the main window.

When opened for the first time, this is how the scheduler options dialog will look.

Click on **OK** to save the settings, turn the scheduler on, and return to the main window.

Click on **Cancel** to return to the main window without saving your work.

Click on **Undo** to remove all the entries that you have made in this session. All previously saved entries are restored.

Click on **Clear all** to clear all entries on the screen.

To configure the scheduler:

1. Enable events by setting the check mark in the left column.
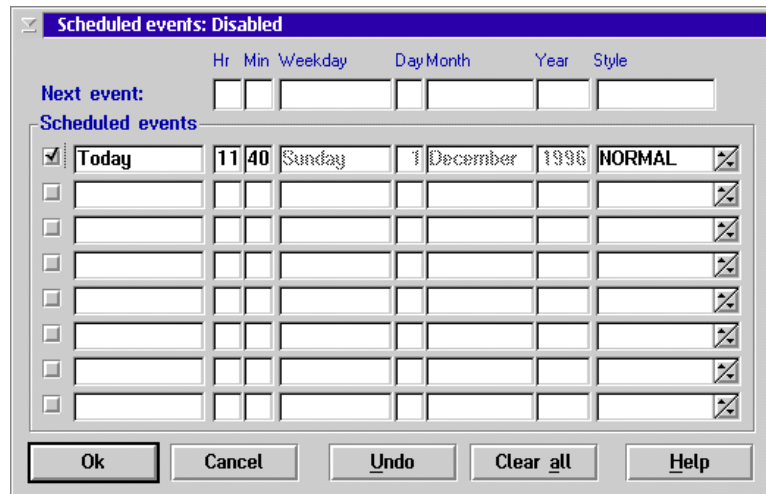
2. In the schedule column, select the type of desired event:
    *   Today (Default)
    *   Once at
    *   Hourly from
    *   Daily from
    *   Weekly from
    *   Monthly from

Make your selections by using the up and down arrow keys, or by clicking on the arrow buttons at the end of the line.

3. Set the desired time and date for when the scan should be started.

    You can specify the time either by clicking on the arrow buttons or by entering hours and minutes manually.

4. Select the desired style.

    Again, make your selections by using the up and down

arrow keys or by clicking on the arrow buttons at the end of the line.

5. Click on [OK] or press [Enter] to save the events. The scheduler will automatically be turned on.

Hints:

Re-use an obsolete event by temporarily selecting Today, as this will change the date to today. Then select the desired event type and edit the time and date.

Events with a time and/or date in the past are removed from the list when the dialog is closed.

Turning the Scheduler On

If you have configured the scheduler from the "Scheduler options" dialog, clicking [OK] will automatically turn the scheduler on. The scheduler status button on the main window then looks like this:

The scheduler status button toggles between turning the scheduler on and off.

Therefore, if the scheduler has been turned off, you may turn it on either by clicking on the scheduler status button or by selecting **Options**|**Scheduled scan on**.

Turning the Scheduler Off

If you would like to keep your scheduled scan entries intact but wish to turn the scheduler off temporarily, you may turn the scheduler off by clicking on the scheduler status button on the main window so that it looks like this:

Remember that the scheduler status button toggles between turning the scheduler on and off.

Alternatively, you may select **Options**|**Scheduled scan off**.

Note: No scheduler settings are lost when the scheduler is turned off.

What Happens in a Scheduled Scan

When a scheduled scan begins, you will see the "Scanning for viruses" dialog unless the **[ ] No scanning dialog box** option has been turned on.

After the scanning finishes, you will **not** see the "possible virus found" or "viruses not found" dialog boxes. Therefore, we recommend that you always turn reporting on for scheduled scans.

If NVCPM is not active at the time that a scan is scheduled, the scan will begin automatically the next time NVCPM is started.

If several scheduled scans were missed during the time that NVCPM was not active, the scans will be run successively the next time NVCPM is started.

Starting NVCPM When OS/2 Starts

If you want NVCPM to be started automatically whenever OS/2 is started, copy the NVCPM object to the Startup folder. This will ensure that scheduled scans will always be executed on time.

If you want NVCPM to be minimized when it is started, change the program object settings (see "Making Special NVCPM Program Objects" on page 101) and add the parameter /MIN (see "Starting NVCPM Minimized" on page 103).

> **Note:** You may also copy an object by clicking on it with the [RMB] and then selecting Copy in the object menu.

Scanning from the Command Line

While NVCPM.EXE is a PM application, it can be started from the command line with certain parameters. Alternatively, you may use the command line scanner.

Using NVCPM from the Command Line

The syntax to use NVCPM from the command line is:

```
nvcpm [drive:] [path] [...] [options]
```

When NVCPM is started from the command line but without command line arguments, it will automatically load the last used style and wait for user interaction.

Started with command line arguments, NVCPM will work as the command line scanner (NVC32.EXE) does, scanning whatever drives and or paths given on the command line. The scanning will be performed utilizing a temporary style with default settings.

See "Scanning from the Command Line" on page 101.

Making Special NVCPM Program Objects

The default NVCPM program object starts NVCPM.EXE without any parameters.

Certain needs such as scanning a single drive are met easier by tailoring an NVCPM program object, rather than starting NVCPM, selecting the desired drive, and then clicking [Start Scan].

To make a special NVCPM program object:
1. Open the folder Norman Virus Control.
2. Copy the NVCPM program object by holding down the [Ctrl] key, clicking and holding down the right mouse

button [RMB], and dragging the copy to a place in the same folder.

3. Give the new program object a descriptive name (e.g., Scan C:).

At this point, the new program object will be exactly the same as the original one, except for the name. The next step will be to change the object so that it scans drive C: only.

4. Click [RMB] to open the new object's object menu.
5. Select Settings.

Fill in the "Parameters" field with the desired parameters, such as `C:`.

See "Scanning from the Command Line" on page 101.

6. Close the Settings notebook.

When started, the new program object will scan for viruses on drive C: and then terminate. The program object can be tailored further by adding other command line parameters, including a style name.

Note: You may also copy an object by clicking on it with the [RMB] and then selecting <u>C</u>opy in the object menu.

Specifying a Style on the Command Line

To start NVCPM from the command line with a certain style, use the syntax:

`NVCW /ST:[name of style]`

There must be **<u>no</u>** spaces between the colon and the name of the style.

If a style is used on the command line along with other command line parameters, the specifications of the parameters override the settings in the style.

When a style is used on the command line, users will not be able to change the configurations within the styles before

the scan begins. In addition, if the style specifies a directory to be scanned, its subdirectories will automatically be scanned. Therefore, there is no need to use the `/S` parameter on the command line along with `/ST:`. See "Scanning from the Command Line" on page 101.

If you begin a scan on the command line with the /ST parameter, NVCPM exits automatically unless the scan was aborted by the user.

Starting NVCPM Minimized

Use the parameter /MIN on the command line if you want NVCPM to be started minimized. It does not change any setting or start scanning.

See also "Making Special NVCPM Program Objects" on page 101.

Restoring System Fonts and Colors

You may drag and drop new fonts and colors onto NVCPM's interface to customize it as you like. These changes are not saved in NVC.INI but rather in a system file when NVCPM exits. Therefore, you could potentially have a situation in which a black color was dropped on the menu bar resulting in not being able to see the menu options. To restore the fonts and colors back to the original settings, start NVCPM with the `/IWPP` parameter.

Using the Command Line Scanner

he 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

```
nvc32x /?
```

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 floppies or CD-ROM).

Param.:	Function:
/AD	Scan all disks (not floppies). 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 continously 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 specifed 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 `nvc32x.exe` is installed, type:

```
nvc32x 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:

```
nvc32x *.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.

Interpreting the Report File

If you have chosen to send the results of the scan to a file (see "Reporting Options Page" on page 55), then the resulting report file will look something like this:

```
>>>
Norman Virus Control for OS/2 Ver. 4.70
<
- Scanning drive E:
- Scanning system areas of drive E:
- Searching for files on drive E:
  E:\
  E:\IBMLAN\
      README.DOC
  E:\IBMLAN\ACCOUNTS\
  E:\IBMLAN\BACKUP\
  E:\IBMLAN\INSTALL\
      LANINST.DLL
  E:\VirusSamples\

*** Possible virus found ***
*** E:\VirusSamples\AIDS2.COM -> HLLC.Aids.8064
*** E:\VirusSamples\AIDSLOAD.EXE -> HLLO.Number_1 related
*** E:\VirusSamples\AIRCOP.COM -> Virus_Drp.Boot.B
*** E:\VirusSamples\AIRCOP1.COM -> Virus_Drp.Boot.B
*** E:\VirusSamples\ALABAMA.COM -> Alabama.A-C.Drp
```

```
- Unpacking archive: Virus.ZIP
  E:\TEMP\NVCTEMP\VIRUS.ZIP\
*** E:\VirusSamples\Virus.ZIP : AIDS2.COM -> HLLC.Aids.8064
*** E:\VirusSamples\Virus.ZIP : AIDSLOAD.EXE ->
HLLO.Number_1 related
*** E:\VirusSamples\Virus.ZIP : AIRCOP.COM ->
Virus_Drp.Boot.B
*** E:\VirusSamples\Virus.ZIP : AIRCOP1.COM ->
Virus_Drp.Boot.B
*** E:\VirusSamples\Virus.ZIP : ALABAMA.COM -> Alabama.A-
C.Drp
>
The NVC scanning process gave the following results:
----------------------------------------------------
The scanning started: 06-09 10:30:13
               ended: 06-09 10:31:13
Scan summary:
   Number of virus variants.....................:    9384
Scan options used:
   System areas scanned for known viruses.......:     Yes
   Scanned archive files........................:     Yes
   Scanned compressed program files.............:      No
Scanning results:
   Total number of files found..................:    8304
   Number of files scanned......................:    1009
   Number of .COM files scanned.................:      76
   Number of .EXE files scanned.................:     457
   Number of .OV? files scanned.................:       0
   Number of .DLL files scanned.................:     436
   Number of .SYS files scanned.................:       4
   Number of other file types found and scanned.:      36
   Number of files that could not be opened.....:       0
   Number of infections.........................:      74
Copyright (c) 1993-99 Norman
```

It consists of the following sections:

- a file header, which states the program name and version.

- a scan report section, which contains information about directories and files scanned, and viruses, if encountered.
- and a summary section.

All of these sections are described below.

The Report File Header

The file header states the program name and version, as in:

```
>>>

Norman Virus Control for OS/2 Ver. 3.53
B2 Beta test
```

The Scan Report Section

The scan report section describes areas scanned, all viruses found, and if so configured, all directories and/or files scanned.

The following line headers will be found in this section:

Header	Description
<	Section start. This will be found alone on the line that starts this section.
>	Section end. This will be found alone on the line that terminates this section.
-	This precedes an informational message.
*	This precedes an error message.
**	This indicates a possible virus infection.

This is how scanned drives are logged:

```
- Scanning drive D:

- Scanning system areas of drive D:

- Searching for files on drive D:
```

Scanning a directory (instead of entire drives) will be logged as:

```
- Scanning files in the directory:
E:\Viruses\
```

Scanning for files matching a given pattern will be logged as:

```
- Scanning files matching:
E:\Viruses\*.exe
```

A virus infection will be logged as shown here, with the full path and filename as well as the virus name.

```
*** Possible virus infection found ***
*** D:\VirusSamples\aids2.COM ->
HLLC.Aids.8064
```

Automatic deletion of infected files will be logged as:

```
- File D:\VirusSamples\aids2.COM
deleted.
```

Automatic moving of infected files will be logged as:

```
- File D:\VirusSamples\aids2.COM moved
to C:\NORMAN\INFECTED.
```

If you have chosen to log all directories that were scanned, they will be logged as:

```
C:\
C:\Work area\
C:\Work area\Templates\
```

The entire path name will be shown.

If you have chosen to scan all files, they will be logged as:

```
E:\NORMAN\
NVC32.EXE
NVCPM.EXE
```

Infected files within an archive file will be logged as follows:

```
- Unpacking archive: Virus.ZIP
*** F:\VirusSamples\Virus.ZIP :
aids2.COM -> HLLC.Aids.8064
*** F:\VirusSamples\Virus.ZIP :
aidsload.EXE -> HLLO.Number_1 related
```

The directory set up as the target for infected files will normally not be scanned. This will be logged as:

```
- Files in C:\NORMAN\INFECTED\ NOT
scanned.
```

Error Messages in the Report File

Error messages are preceded by an asterisk, as in:

```
* Scanning aborted.
```

This type of action will also produce the following line in the summary section:

```
* Scanning aborted before completion.
* Could not open this file: FILE.EXT
  SYSxxxx: [OS/2 error message].
```

The given filename could not be opened for the given reason.

```
- Unpacking archive: STARS.ZIP
```

```
* Could not open this file: STARS.ZIP.
```

```
  SYS0002: The system cannot find the
file specified.
```

Something went wrong when unpacking the archive file. The file is probably corrupted or is not recognized as an archive file, despite the file type ".ZIP".

```
- Unpacking archive: REFRAGS.ARJ
```

```
* Could not open this file: REFRAGS.ARJ.
```

```
  SYS1041: The name specified is not
recognized as an internal or external
command
```

Check your archive options. The executable assigned to an archive file type does not exist.

```
* File A:\INFECTED\ASHUZZZZ.COM copied
to C:\NORMAN\INFECTED, but NOT deleted.
```

```
* File A:\INFECTED\ASHUZZZZ.COM NOT
deleted.
```

NVCPM attempted to move or delete an infected file from a write-protected media.

```
* Unable to send SNMP trap to:
[servername]
```

Something went wrong when attempting to send a virus alert to the given SNMP agent.

The Summary Section

This section contains a summary of the scanning process:

```
The NVC scanning process gave the following results:
----------------------------------------------------
The scanning started: 02-09 14:33:12
               ended: 02-09 14:34:13
Scan summary:
   Number of virus variants.....................:    9384
Scan options used:
   System areas scanned for known viruses.......:     Yes
   Scanned archive files........................:     Yes
   Scanned compressed program files.............:      No
Scanning results:
   Total number of files found..................:    2008
   Number of files scanned......................:     754
   Number of .COM files scanned.................:      32
   Number of .EXE files scanned.................:     189
   Number of .OV? files scanned.................:       0
   Number of .DLL files scanned.................:     396
   Number of .SYS files scanned.................:      80
   Number of other file types found and scanned.:      57
   Number of files that could not be opened.....:       0
   Number of infections.........................:       3
Copyright (c) 1993-99 Norman
```

Note: Date and time is given as YYYY/MM/DD hh:mm:ss.

Glossary of Terms

Boot Virus

A virus that infects and spreads through the hard drive's Master Boot Sector or System Boot Sector and/or through floppy boot sectors. It is machine dependent and mostly operating system independent, which means that they thrive on a PC or 100% compatible, regardless of whether the machine is running MS-DOS, OS/2, or Unix. Examples include Stoned and Form.

System Boot Sector

Located on all floppy diskettes and physical hard drives that are formatted and created by FORMAT. It 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 floppy disk with an operating system on it.

Since the System Boot Sector [SBS] contains code that is executed whenever the system is started, it is a likely candidate for virus infection.

Master Boot Sector

The part of the boot area containing the partition table. Unless moved by a virus, it is stored on side 0, cylinder 0, sector 1. Created with FDISK. Not found on floppies.

When the PC is started (or booted), code in the BIOS will read the Master Boot Sector [MBS]. The partition table locates the active system partition, which in turn leads to the SBS being read. The SBS runs its program which loads the operating system or the boot manager, if it is installed.

Since the MBS contains code which is executed whenever the system is started, it is a likely candidate for virus infection.

Updating NVC

General information on installation/updates

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, doubleclick on the file name and follow the instructions on the screen.

Definition file updates are available from our Web site on a regular basis. We recommend that you pay us a visit at:

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

Index

—T—

—U—

—V—

—W—