NORMAN®

Cat's Claw
for Windows 3.1x and
Windows 95

User's Guide

Version 4.70

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

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

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

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

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

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

Limited warranty

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

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

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

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

This warranty expires 30 days after purchase.

Contents

Conventions

We use the following conventions throughout this manual:

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

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

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

[Ctrl]

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

Start|Run

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

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

Note: Here is a hint about how to use Cat’s Claw...

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

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

System Requirements

Cat’s Claw for Windows 3.1x and Windows 95 and Windows 98 (from now on referred to as Windows 9x) can run on any machine that runs any national language version of these operating systems.

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 on hard drives. 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

Installing Cat’s Claw

Run the following command to install Cat’s Claw:

```
a:setup
```

and follow the instructions on the screen.

For Windows 95 users:

If you have a previous version of NVC installed, you must unload the Smart Behavior Blocker.

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

Either double click with the left mouse button or click once with the right mouse button, and choose Unload from the menu.

About Norman Virus Control

Norman Virus Control (NVC) is a modular virus protection tool, which is available for the following platforms:

- DOS
- Windows 3.1x
- Windows 95
- Windows NT
- OS/2
- NetWare
- Groupware

NVC for Windows 3.1x and Windows 95 include the program Cat’s Claw. Cat's Claw is an application specially designed to monitor and protect your system against viruses by scanning files as they are being opened. In addition, Cat’s Claw will check boot sectors on diskettes and hard drives and remove boot sector viruses whenever possible.

Cat’s Claw can remove boot sector viruses from diskettes on-the-fly. When your hard drive is infected by a boot virus, you will be instructed to back up your boot sector to a diskette before the virus is removed.

Cat’s Claw does not provide on-demand or scheduled scanning. For those who do not require a complete NVC package, we offer Cat’s Claw as a stand-alone program.

Macro Viruses

Macro viruses is the fastest growing segment among virus makers all over the world. Cat’s Claw was originally designed to handle this particular virus type only, but it’s now upgraded to remove binary file viruses too. Macro viruses still represent a serious threat by the way they are distributed (e-mail attachments, file exchange, etc), but they are easier to detect and remove - simply because we have the know-how and established technology to handle these viruses.

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

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

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

Norman’s solution to the new threat is:

Cat’s Claw

Cat's Claw is an application specially designed to monitor and protect your system against viruses. One of its unique features is the Certify Macro function (page 9). This function allows you block Word and Excel files with unknown and possibly infected macros from your system.

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

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

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

Limitations in This Version

For Windows 95:

In a Novell network with Novell 32 bits client in Windows 95, Cat’s Claw can not check files from the server.

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

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

Configuration Concepts

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

- Cat’s Claw will be loaded into memory at start-up
- you will be prompted for action when a virus is found
- you will receive a warning if Cat’s Claw is unable to scan a file
- uncertified macros will not be removed

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

About Warnings from Cat’s Claw

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

Cat’s Claw Factory Settings

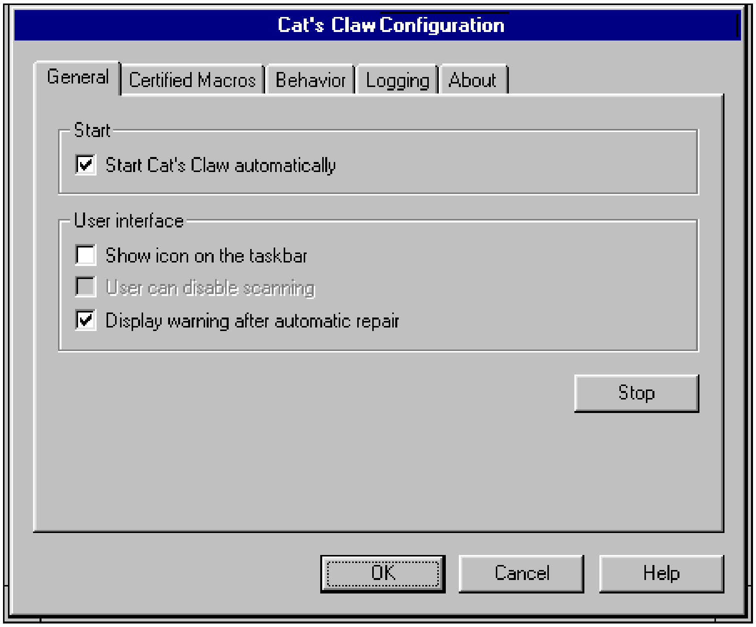
The factory settings in the Cat’s Claw configuration program should therefore not be considered as recommended options.

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

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

Configuration Dialogs

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



Cat's Claw Configuration

Start

☑ Start Cat's Claw automatically

User interface

☐ Show icon on the taskbar

☐ User can disable scanning

☑ Display warning after automatic repair

General

[ ] Load Cat's Claw on startup

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

[ ] Show icon on desktop

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

[ ] User can disable scanning

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

[x] Display warning after automatic repair

If you select [ ] **Remove virus from file** (see page 13), you will be informed when Cat’s Claw has removed a virus from an infected file.

Automatic repair of boot sector viruses on hard drives is not possible. With the Remove virus from file option ON, boot sector viruses will automatically be removed from diskettes.

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

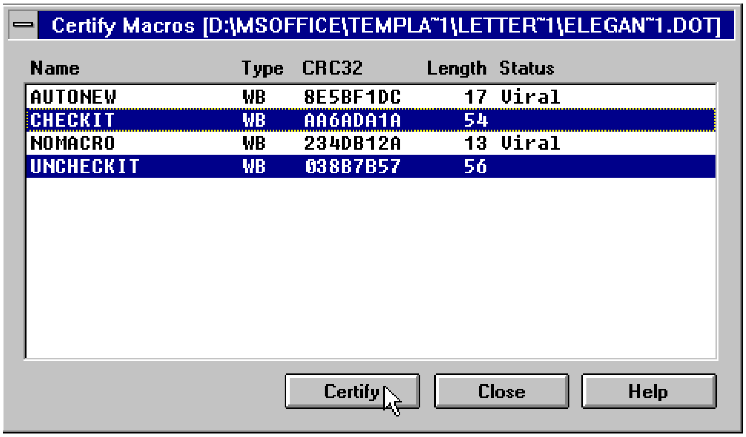
Certified Macros

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

If you certify macros, only these macros will be accepted. See “Handling of Uncertified Macros” on page 14 for more considerations on certified and uncertified macros.

Follow these steps to certify a macro:

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



Name	Type	CRC32	Length	Status
AUTONEW	WB	8E5BF1DC	17	Viral
CHECKIT	WB	AA6ADA1A	54	
NOMACRO	WB	234DB12A	13	Viral
UNCHECKIT	WB	038B7B57	56	

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

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

Fields in the Dialogs for Certifying Macros

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

Status:

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

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

Name:

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

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

Type:

Three different types can appear in this field:

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

CRC32:

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

Length:

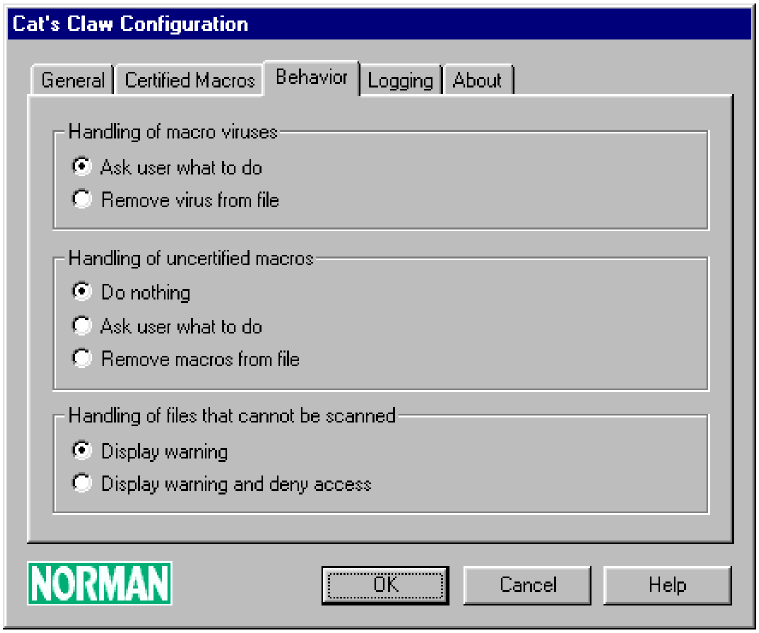
Like any other file, a macro has a certain length. This field displays the macro length used by Cat's Claw to check that a certified macro hasn't been changed after certification.

Comment:

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

Behavior

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



Handling of macro viruses

● Ask user what to do
○ Remove virus from file

Handling of uncertified macros

● Do nothing
○ Ask user what to do
○ Remove macros from file

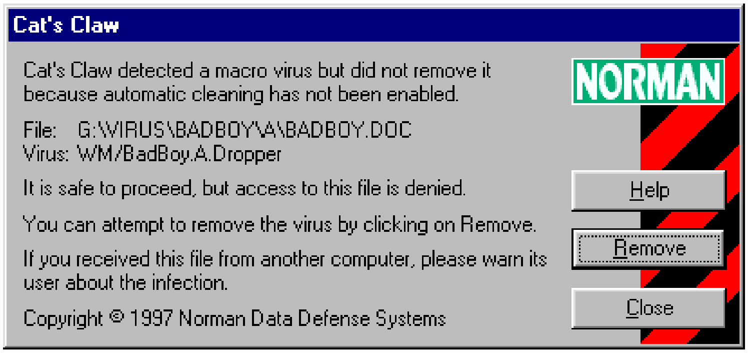
Handling of files that cannot be scanned

● Display warning
○ Display warning and deny access

Handling of Viruses

[ ] Ask user what to do

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



Cat's Claw

Cat's Claw detected a macro virus but did not remove it because automatic cleaning has not been enabled.

File: G:\VIRUS\BADBOY\A\BADBOY.DOC
Virus: WM/BadBoy.A.Dropper

It is safe to proceed, but access to this file is denied.

You can attempt to remove the virus by clicking on Remove.

If you received this file from another computer, please warn its user about the infection.

Copyright © 1997 Norman Data Defense Systems

Manual Virus Removal Warning

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

[ ] Remove virus from file

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

Automatic repair of boot sector viruses on hard drives is not possible. With the Remove virus from file option ON, boot sector viruses will automatically be removed from diskettes.

Virus Removed Warning

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

Virus Not Removed Warning

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

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

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

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

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

Handling of Uncertified Macros

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

[ ] Do nothing

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

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

[ ] Ask user what to do

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

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

Uncertified Macro Not Removed Warning

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

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

[ ] Remove macros from document

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

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

Uncertified Macro Removed Warning

Cat’s Claw removed macros from this file because:

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

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

Other Messages on Uncertified Macros

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

Cannot Remove Uncertified Macro Warning

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

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

or if

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

Handling of Files That Cannot Be Scanned

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

[ ] Display warning

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

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

Password Protected File Warning

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

Damaged File Warning

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

Internal Error Warning

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

[ ] Display warning and deny access

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

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

Password Protected File Blocked Warning

You checked the option [ ] **Display warning and deny access**. Password protection stopped Cat’s Claw from scanning the file, and you cannot access it. Possible solution is changing your configuration to [ ] **Display warning** only and access the file at your own risk.

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

Damaged File Blocked Warning

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

Internal Error Denied Access Warning

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

Boot Sector Virus Removal

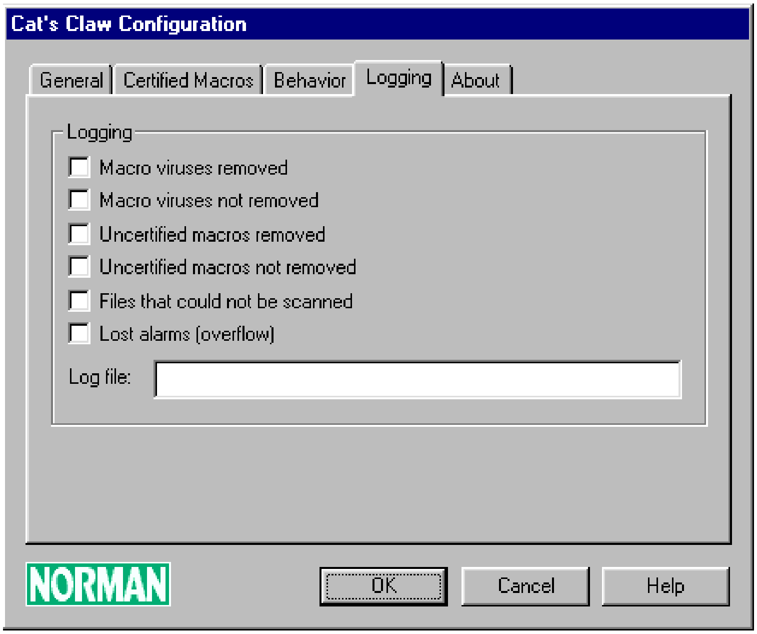
The core technology in all NVC components is the scanning engine. The scanning options reflect the capability of the engine. In addition to detect viruses, the engine can also remove them (repair the file or boot sector, and thereby clean the machine). This process is technically more complicated than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

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

If a boot sector virus is detected, you will see a dialog box that recommends that you back up the necessary data to a diskette. If the repair fails, you can boot your machine from the restore diskette.

Configuration:Logging

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



Cat's Claw Configuration

Logging

□ Macro viruses removed
□ Macro viruses not removed
□ Uncertified macros removed
□ Uncertified macros not removed
□ Files that could not be scanned
□ Lost alarms (overflow)

Log file:

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

[ ] Viruses removed

Logs path, file name and name of removed viruses.

[ ] Viruses not removed

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

[ ] Uncertified macros removed

Logs path and file name of removed uncertified macros.

[ ] Uncertified macros not removed

Logs path and file name of uncertified macros not removed.

[ ] Files that could not be scanned

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

- password protected, possibly containing macros (Word 8)
- corrupted

[ ] Lost alarms (overflow)

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

Loosing alarms does therefore not represent a security risk.

Log file

Enter a valid path and file name for the log file, for example

`c:\norman\win16\claw31.log` (Windows 3.1x),

or

`c:\norman\win95\claw95.log` (Windows 95).

Appendix

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