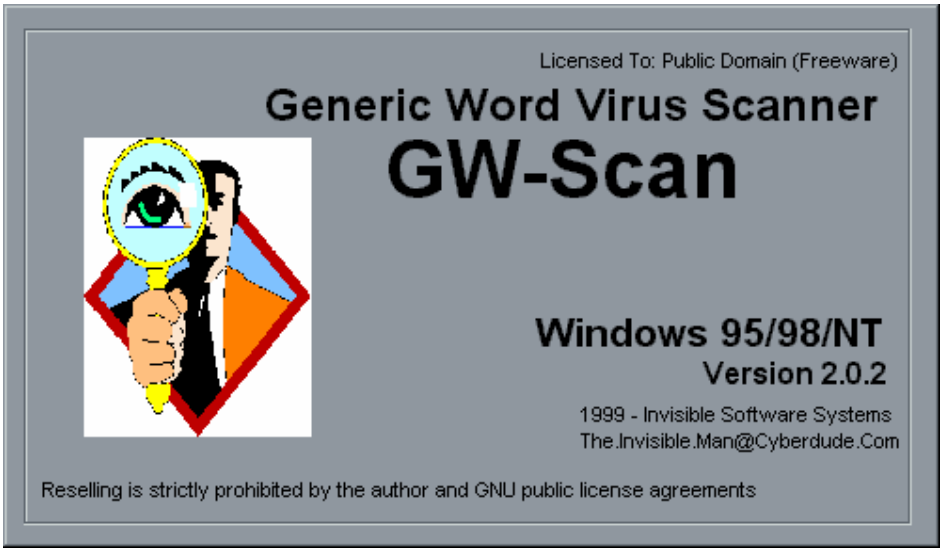
Appendix D – GW-Scan Userguide

To allow a user with a little understanding of Windows, how to operate GW-Scan.



Introduction

It is possible to spread a virus by a Microsoft Word document. The macrocode used with word allows it to incorporate visual basic programs, which like many other programming languages make viruses possible.

This program is a "Generic" scanner, which means that it is able to detect and disable word macro viruses both old and new. It does not require updates allowing it prevent new viruses, it exploits the names that macro viruses use to infect other documents. Searching for a range of common macros like AutoOpen, AutoClose etc, it warns the user if it finds documents with these macros, then allows the macros to be renamed. This stops the macro from triggering automatically when they are loaded into Word.

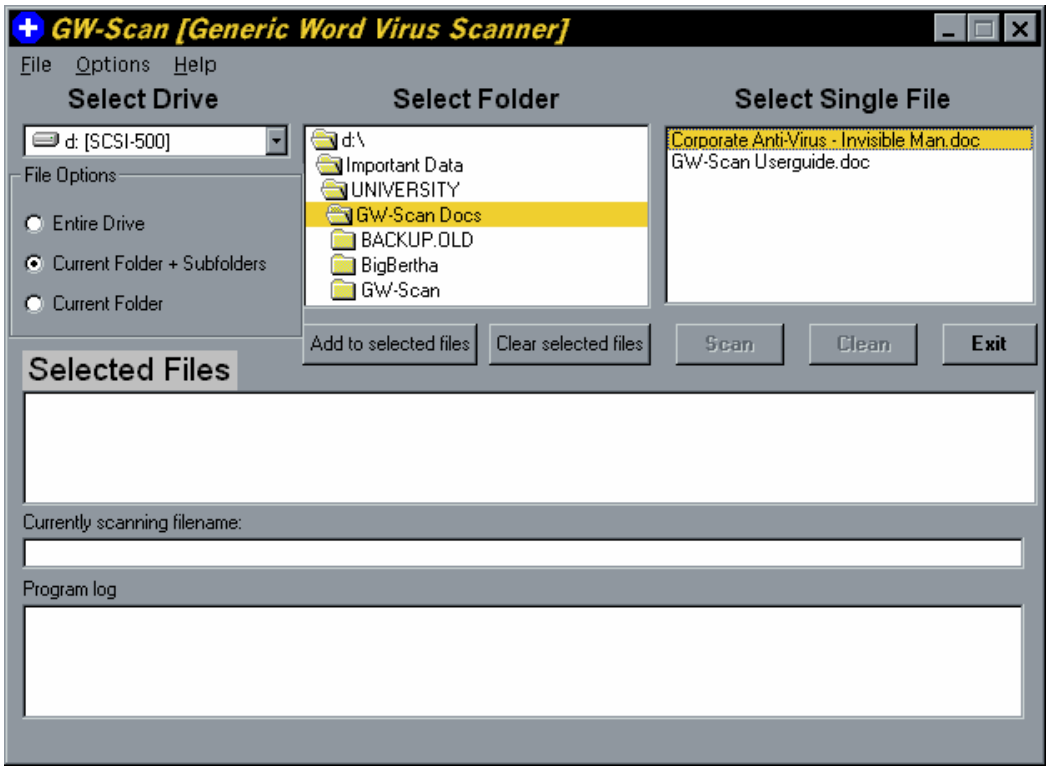
Because there are documents that do contain innocent macros, you will have to exclude certain documents that use these macros to perform automatic tasks. Microsoft word uses a range of template wizards to produce reports, faxes and HTML Internet web pages. These usually reside in the directory of:

C:\Program Files\Microsoft Office\Templates

The list of files that have innocent macros have already been added to the excluded file list. These are stored in EXCLUDE.TXT, see excluding files for more information. Once the list is complete, you will be able to detect virus attack and be sure that these macros belong to a macro virus.

The Main Screen

This is the main interface to GW-Scan, where you select the documents and templates that you want it to scan. This is all mouse controlled.



The example above is adding files to the scanning list by double clicking on the documents in the select single file box. To add files to the list in greater quantity, see the options listed below to select drives and folders.

Selecting file options

To scan an entire drive

Select the drive to scan e.g.

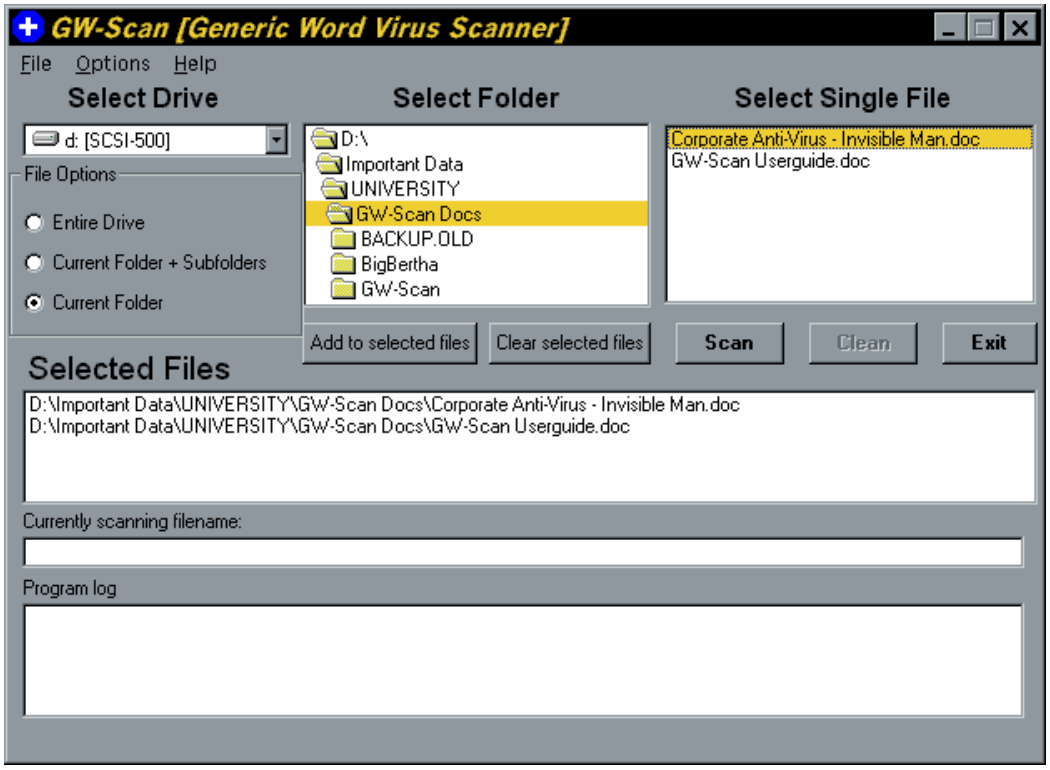
Click on the drive box and select drive and click on a drive letter to change it.

- Drive A = Floppy Drive
- Drive C = Hard Disk

Click on the entire drive circle
Click on Add to selected files
Click on Scan

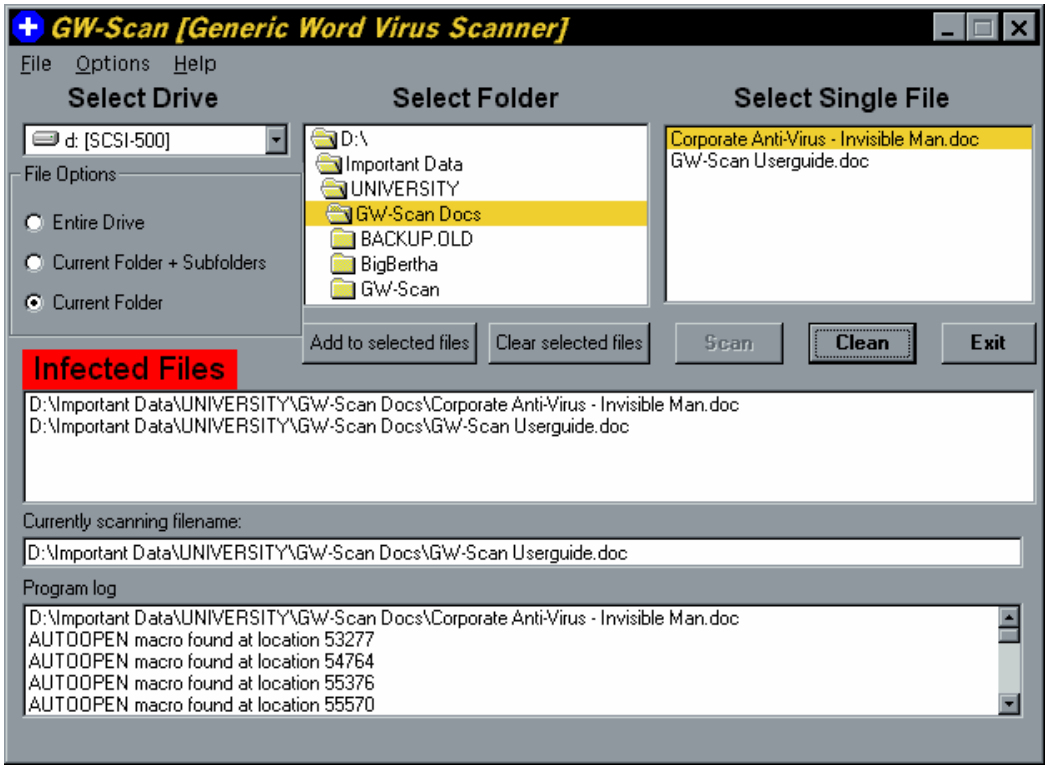
To scan for directories and all directories within it, click on Current Folders + Subfolders. This will work when you select the folder in the Select Folder box, then use the Add to selected files button.

To scan for directories without subfolders, click on Current Folder, then select the folder to scan with the Select folder box, and click Add to Selected files.



Scanning for viruses

When the selected files have been chosen, it's now time to scan the documents for viruses. Click on the Scan button to search these files for macro viruses.
A wait message will appear while the program scans the documents. If you can still see the text 'Selected Files' with a grey background, the documents are clean. Otherwise you will see a screen like the one below, and you may have infected documents that need to be addressed.

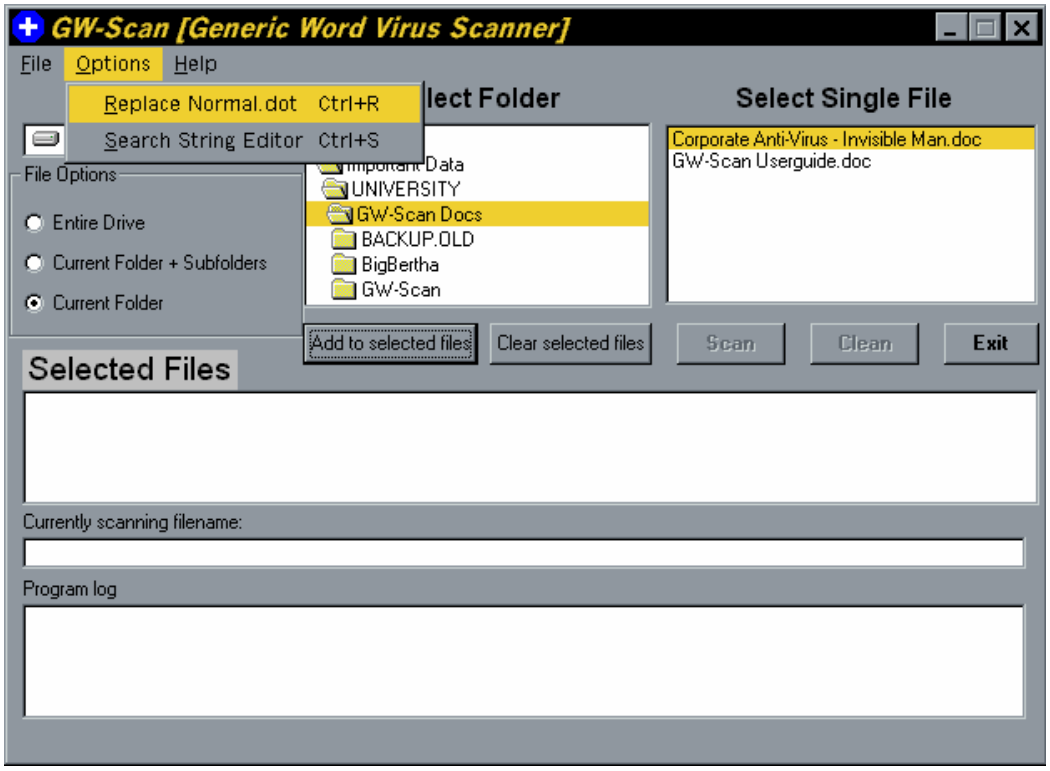


The red "Infected Files" text warns you that possible macro viruses have been found. The macros it detected will be in the program log box, with the name of the document and the macros it has found.

Click on the clean button to rename the macros if you are sure that the documents contain macro viruses. This will reset the screen after cleaning, allowing you to scan again or to exit the program.

It is highly recommended that the Normal.Dot overwriting option be used when a virus has been found. This will replace the main template with a fresh copy for the correct version of Word, and prevent possible word basic errors created by disabling the virus. (See the next section on options for more details).

The Options Menu



There are three main features available to change the operation of GW-Scan:

Options Menu - Replace Normal.Dot
Overwrites the main template with a fresh copy

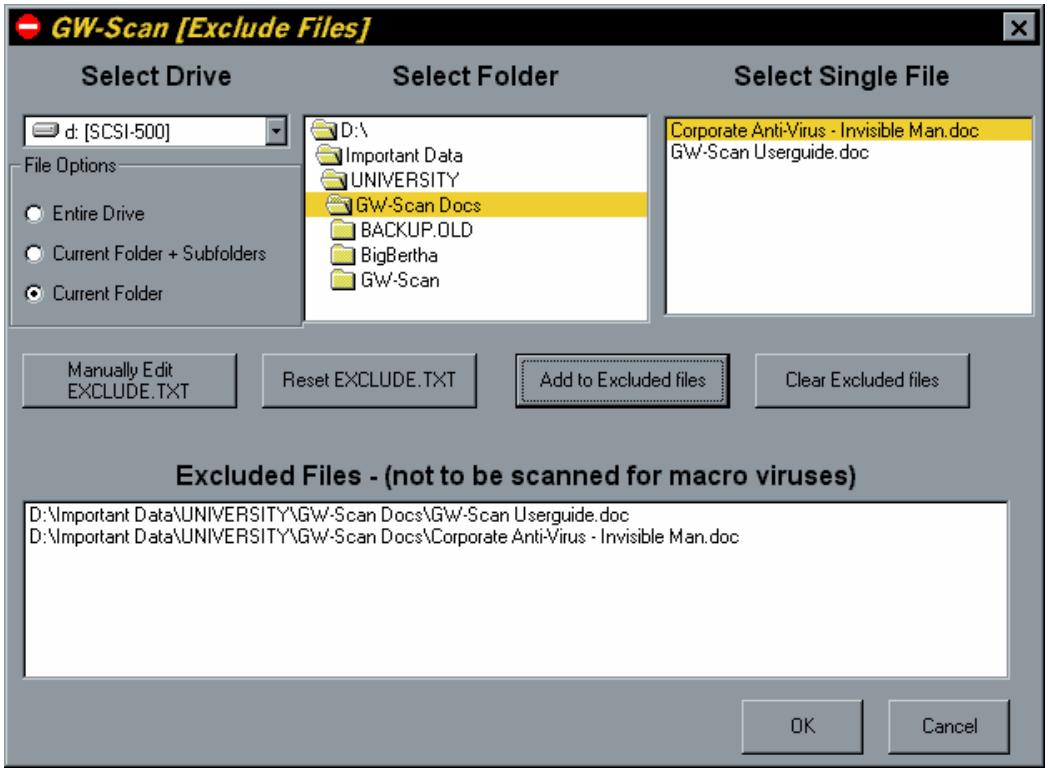
Options Menu - Search String Editor
Allows you to modify names of macro virus search strings

File Menu - Exclude Files
Prevents files from being scanned to stop false alarm

The next three pages of this manual help you use these options correctly.

Excluding files

Because some documents may produce false alarms because they contain innocent macros, these files have to be avoided by the scanner. The interface is very similar to the main screen file selections, so you need to read the page on selecting files which works in exactly the same method as the main scanner screen. The exclude option:



The example above will exclude the filenames:

D:\Important Data\UNIVERSITY\GW-Scan Docs\Corporate Anti-Virus - Invisible Man.doc
D:\Important Data\UNIVERSITY\GW-Scan Docs\GW-Scan Userguide.doc

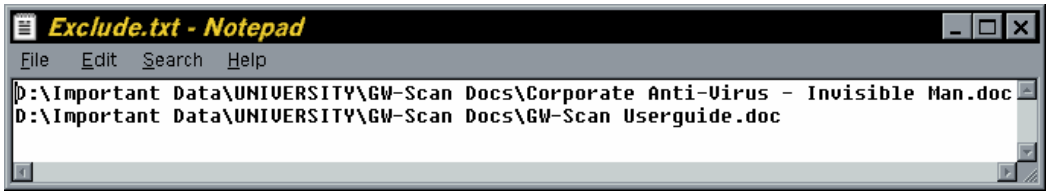
If there is another file by the name “GW-Scan Userguide” in a different folder, this will be scanned, so it is important to distinguish between the documents that contain your own automatic macros.

The controls ‘Add to Excluded files’ and ‘Clear Excluded files’ will add and remove files from the listbox below it, showing which files will not be scanned.

Once files have been selected for exclusion, press the OK button to save these changes to the EXCLUDE.TXT file, or press Cancel to ignore these changes.

Manual Edit of EXCLUDE.TXT

The options Manually Edit EXCLUDE.TXT will open notepad as a file editor and allow you to make changes more directly to the file. Here is an example of what happens when you click on this option, and it contains typical file exclude text:



For more help about using notepad, load notepad from your Start, Programs, Accessories menu, and select the help menu from notepad.

Resetting the EXCLUDE.TXT file

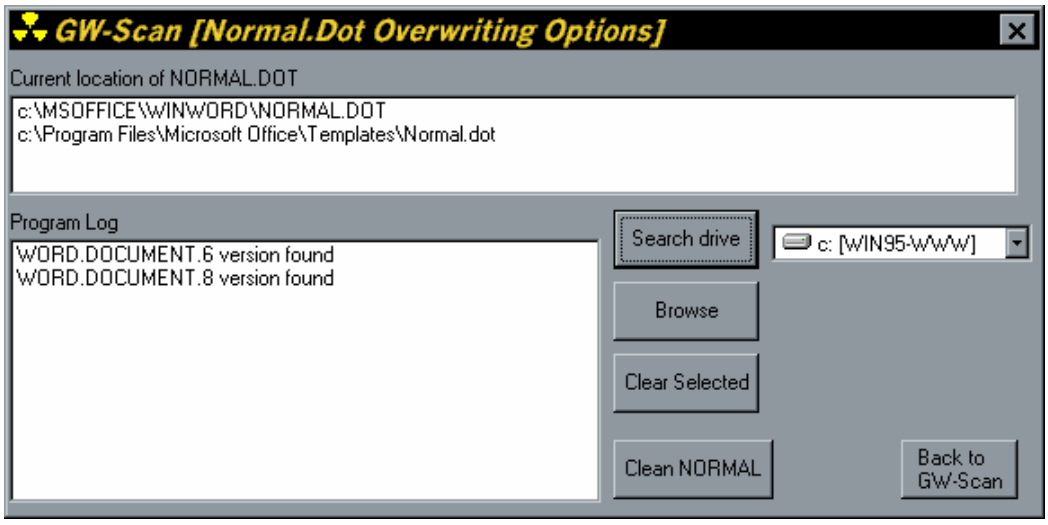
Selecting this option will remove all filenames within the file as well as the currently selected filenames on-screen. This is when you have excluded a set of files that no longer exists or have been moved elsewhere.

Returning to the main screen

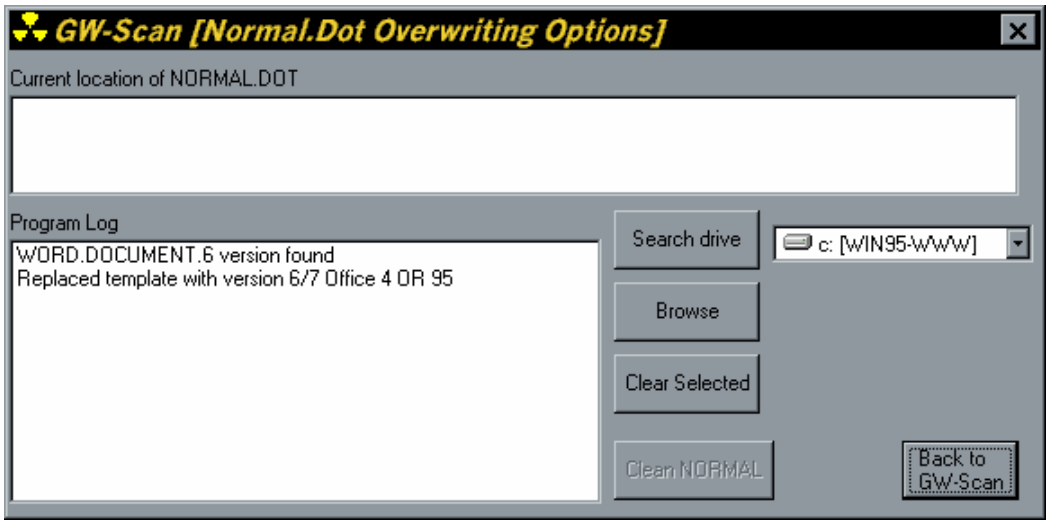
The ‘OK’ button will make changes to the text file and return to the main screen, and the ‘Cancel’ button will just return to the main screen ignoring new selected files.

Replacing Normal.Dot

Use this option if viruses have been found, because it is possible that the main template has been infected. This will replace it with a new uninfected copy.

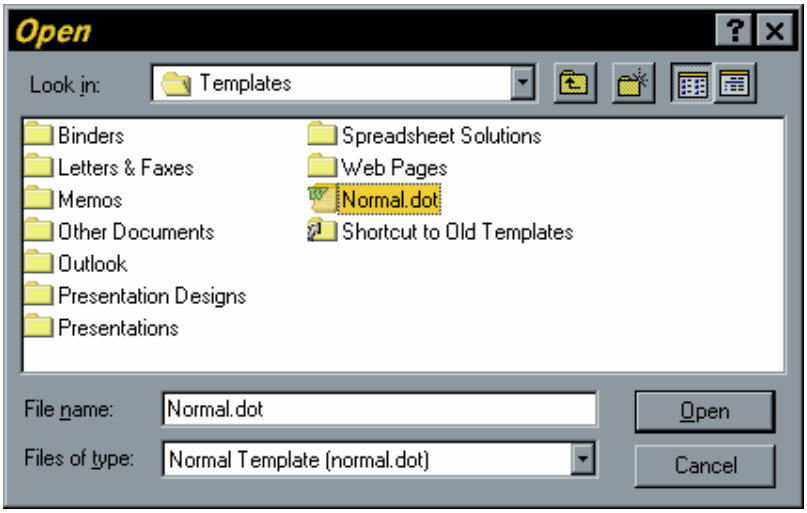


The example above shows the output produced when 'Search drive' has found NORMAL.DOT and displays the version of Word being used. When you press the 'Clean NORMAL' button, it will replace the file and show this screen:



Once the Normal template has been replaced, press 'Back to GW-Scan' to return to the main screen.

There is another method to find the Normal.Dot file manually rather than seraching the entire drive. This uses the 'Browse' option to display a common file dialog box:



This options presumes a known location of the template, the usual locations are:

C:\WORD6\TEMPLATES
C:\PROGRAM FILES\MICROSOFT OFFICE\TEMPLATES
C:\WINWORD\TEMPLATES

This option may be quicker on a large disk drive because you locate the file yourself.

Search String Editor

Using check-boxes to select the macros that will be scanned, it is possible to save time by scanning for less macros. This is not advisable to catch all macro viruses, but allows you to prevent scanning a macro that you use yourself to prevent false alarms.

Manual Editing of Search Strings

This will open the notepad and display a list of macros that were checked on the form above. It allows you to add new macronames to search for, including foreign names to help catch international word viruses. For more help about using notepad, load notepad from your Start, Programs, Accessories menu, and select the help menu from notepad.

An example of the file SEARCH.TXT