Microsoft Word Macro Virus Protection Tool Readme

October 2, 1995

Please read this entire document for important information about the Macro Virus Protection tool, including problems you may encounter when running it.

Contents:

Installing the Macro Virus Protection Tool

The Macro Virus Protection tool includes two files:

scanprot.dot	The template which sets up the protection macros on the user's machine
readme.doc	This file, which provides information about the tool and its operation

To install the Macro Virus Protection tool, use Word's File Open command to open scanprot.dot. The protection tool will be automatically installed, and will prompt you for any additional input required.

This installation procedure is the same whether you run Word as a single-user setup, as a workstation install from the network, or if Word is run from the network directly. In particular, since the setup requires changing the users' Normal template on the local machine, there is no shortcut method of installing the protection macros on a large number of machines. The macro must be run on each desktop which is to be protected against macro viruses.

If for any reason you need to re-install the protection tool, follow these steps:

1. Bring up the list of macros by selecting the Tools Macro command. If a macro called InstVer appears in the list, select it and press the Delete button.

2. Open the scanprot.dot template using File Open.

3. The Warning alert will be displayed. Choose "No" so that the protection tool setup will run.

Now the protection tool will be re-installed completely.

Removing the Macro Virus Protection Tool Macros

To completely remove the Macro Virus Protection Tool, choose Macro from the Tools menu. Select the AutoExit macro and press the Delete button. Repeat this procedure to also delete the following macros: FileOpen, ShellOpen, and InstVer. This will remove macro virus protection from your system.

Common Questions About the Macro Virus Protection Tool

Q: What are macro viruses?
A: Macro viruses are a new type of virus that use an application's own macro programming language to distribute themselves. Unlike previous viruses, macro viruses do not infect programs; they infect documents. For more information about macro viruses, see the section below on "Common Questions About Macro Viruses."

Q: What is the Macro Virus Protection tool?
A: The Macro Virus Protection tool is a free tool that installs a set of protective macros which detect suspicious Word files and alert customers to the potential risk of opening files with macros. Upon being alerted, users are given the choice of opening the file without executing the macros, thereby ensuring that no viruses are transmitted. Although the primary purpose of the Macro Virus Protection tool is to alert users to the existence of macros in their documents and allow then to open their documents without macros, the tool also contains an updated version of the scanning code for the Concept virus and can be used to scan your hard disk for Word files that contain the Concept virus.

Q: How does this new tool work?
A: The Macro Virus Protection tool installs a set of protective macros into the user's Normal template. If the user opens a document containing macros, the protective macros are activated and the user is alerted to the potential risk of opening files containing macros. The user is given the choice of opening the file without executing the macros, opening the file as is, or canceling the file open operation. Opening the file without macros ensures that macro viruses are not transmitted and does not affect the content of the document. Unless the user can verify that the macros contained in the document will not cause damage, Microsoft recommends opening the file without macros.

Q: What does the Macro Virus Protection tool protect against?
A: The Macro Virus Protection tool is a general alerting mechanism that will alert users to *any macros* found in a document. Although the tool scans for the Concept virus, its primary purpose is not to detect or repair specific viruses, but to alert users to the fact that they are opening a document which contains macros and that these macros could contain viruses. Users are able to protect themselves against macro viruses by opening the file without the macros.

Q: Does the Macro Virus Protection tool change my files?
A: Upon installation, the tool offers to scan for any files which contain the Concept virus. If any infected files are found, the Concept virus is deleted from them and the files are re-saved. After the tool is installed, if a document with macros is opened, the protection alert is displayed. If a user cancels the File Open operation, or chooses "No," then nothing in the file is changed and the operation continues as if the tool were not installed. If the user chooses "Yes" and opens the file without the macros, a new document

containing all of the document's content but none of its macros is created. The user can choose to save this new document with the same name as the original (thus overwriting the original and permanently removing the macros), or they can close the new document without saving, to preserve the macros.

Q: What is the difference between the Macro Virus Protection tool and Scan831.doc?

A: Scan831.doc is a tool that Microsoft made available to customers to allow them to scan and remove the Concept virus from their Word files. Since the release of Scan831.doc, all of the major anti-virus vendors have either shipped or committed to shipping tools which detect the Concept virus. Although the Macro Virus Protection tool includes an updated version of the Scan831 scanning code, its primary function is to alert users to the existence of macros in their documents and allow then to open their documents without macros.

Q: Are there any known limitations of the Macro Virus Protection Tool?

A: The Protection Tool works by trapping File Open operations. There are some methods of opening files that the tool cannot trap. If a user opens an infected document using one of these techniques, they will not be protected. Microsoft recommends avoiding opening documents in the following manner unless the user is certain that the document is virus free. The methods which bypass the Protection Tool include:

- Selecting an item from the Most Recently Used files list on the File menu.
- Dragging a document and dropping it on the Word application window.
- In the version for the Macintosh®, double-clicking on a Word file in the Finder.
- In the version for Windows® 95 or Window NT™, double-clicking on desktop scraps.
- In the version of Word 6.0 for Windows or Windows NT, opening files through Find File.
- In the version for the Macintosh, choosing a file from the Finder's Recent Files menu.

Q: Which versions of Microsoft Word does the tool run on?

A: The tool works with Word 6.0 for Windows 3.1, Word 6.0.1 for the Macintosh, Word 6.0 for Windows NT, Word for Windows 95 and Windows NT. Currently the tool has not been loacalized for international versions of Word.

Q: Where can I get the Macro Virus Protection tool?

A: The tool can be downloaded from the following on-line services:

- The Microsoft World Wide Web site at http://www.microsoft.com/msoffice
- MSN™, The Microsoft Network using go word: macrovirustool
- The Word forums on other on-line services such as CompuServe® and America Online®
- Customers can also get the tool by calling Microsoft's Product Support Services at 206-462-9673 for Word for Windows, and 206-635-7200 for Word for the Macintosh; or by sending Internet email to wordinfo@microsoft.com

Q: How will you distribute updates to the tool?

A: Any updates which become necessary will be distributed on the following on-line services:

- The Microsoft World Wide Web site at http://www.microsoft.com/msoffice
- MSN™, The Microsoft Network
- The Word forums on other on-line services such as CompuServe® and America Online®
- Microsoft's Product Support Services at 206-462-9673 for Word for Windows, and 206-635-7200 for Word for the Macintosh; or by sending Internet email to wordinfo@microsoft.com

Q: How many different macro viruses currently exist?
A: To date, the anti-virus community is aware of three macro viruses. The three macro viruses currently know by the anti-virus community are the Word Prank Macro also know as the Concept virus, the DMV virus and the Nuclear virus. Specific information about each of these viruses is included at the end of this Q&A.

Q: Does a box of Word or Office that I buy in the store contain macro viruses?
A: Macro viruses do not exist in any version of Word or Office that you would get in a store. You can only get macro viruses by opening a Word document or template that already contains the macro virus.

Q: Can macro viruses be transferred with documents created with or being read by Internet Assistant?
A: Internet Assistant and documents created or read by it cannot be affected. Internet Assistant blocks the mechanism that distributes this type of macro.

Q: Can macro viruses be transferred with documents created with or being read by WordMail?
A: Word cannot send or receive this type of macro as a WordMail message. However, like many email editors, WordMail supports file attachments. If an infected document is sent as a file attachment, you can get infected when you open such an attachment.

Q: Can macro viruses be transferred by documents being read with the Word Viewer?
A: Since the Microsoft Word Viewer cannot save documents, it is unable to transmit macro viruses.

Common Questions About the Concept Virus

Q: What is the Concept virus (also known as the Prank Macro)?
A: The Concept virus is a macro virus which, once it installs itself, only lets you save documents as templates. The macro does not cause data loss or any other serious system, but it will replicate and distribute itself through Word documents. The first time you open a document containing the macro you will see a dialog box that only contains the number "1" and an "OK" button. You can also verify whether or not the macro is installed by selecting the "Macro" command from the "Tools" menu -- if the list contains the following macros: AAAZAO and AAAZFS it has been installed.

Q: Does the Macro Virus Protection Tool protect me against the Concept virus?
A: Yes. Upon installation, the tool scans for the Concept virus. If it finds the Concept virus, it deletes it and installs protective macros to prevent the Concept virus from installing in the future. The tool, however, does not detect infected files that are embedded in other OLE files or your mail file. Contact your Anti Virus vendor for an updated version of their scanning tools.

Common Questions About the Nuclear Virus

Q:What is the Nuclear virus?
A: The nuclear virus is the only macro virus currently known to cause damage to your print outs and DOS system files. It uses the following macro names:

AutoExec
AutoOpen
DropSuriv

FileExit
FilePrint
FilePrintDefault
FileSaveAs
InsertPayload
Payload

Possible damage:

- If you open the document between 55 seconds and the next minute, any print job will have the text STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC! appended to it.
- If you open the document between 5 and 6 PM, it will attempt to infect your machine with the ph33r virus. This part is not damaging however, because it installs a Terminate and Stay Resident (TSR) program in a DOS session that ceases to exist when the macro finishes.
- On April 5 of any year, io.sys and msdos.sys are zeroed out, and command.com is deleted from your root directory. DOS can no longer boot, and presumably, by zeroing out the crucial files, won't notify you that DOS is gone at boot time.

Q: Does the Macro Virus Protection tool protect me against the Nuclear virus?
A: The macro virus protection tool alerts users any time a document containing macros is opened. Since the Nuclear virus is spread through macros, users will be alerted when they try and open a document containing the Nuclear virus. Users can protect themselves from the Nuclear virus by choosing to open the file without macros.

Common Questions About the DMV Virus

Q:What is the DMV virus?
A: This virus is very similar to the Concept virus. Instead of using AutoOpen to start the replication it uses AutoClose to install the virus in the user's Normal (Global) template. Other than replicating itself and changing the FileSave As command, it does not do any harm.

Q: Does the Macro Virus Protection tool protect me against the DMV virus?
A: The macro virus protection tool alerts users anytime a document containing macros is opened. Since the DMV virus is spread through macros, users will be alerted when they try and open a document containing the DMV virus. Users can protect themselves from the DMV virus by choosing to open the file without macros.

Integrating the Protection Macros With Existing User Macros

In order to ensure strong anti-virus protection, the Macro Virus Protection tool will disable certain user macros when the tool is installed. Because of the wide variety of user macros and the potential that they could be infected with a virus, it is not possible for the tool to automatically detect "good" user macros, and merge them in so that they coexist with the Protection tool.

This section describes how you can integrate any desired user macros with the macros that the Macro Virus Protection tool provides. This is a technical process which requires knowledge of WordBasic. If you do not have the technical skills required to complete this integration, then you have three options:

- Keep the Macro Virus Protection Tool installed, and do without the functionality that the conflicting user macros provided.
- Remove the Macro Virus Protection tool and reinstall your original user macros, and do without the anti-virus protection functionality.

- Seek technical assistance for the problem, either from your internal help desk, knowledgeable in-house WordBasic users or the original author of the user macros. They should all be able to follow the instructions below to solve the problem.

General Information

Q: What macros are installed when the Macro Virus Protection tool is run and what happens if macros with the same name already exist?
A: During setup, the Macro virus Protection tool installs the following macros to the user's Normal template: AutoExit, FileOpen, InstVer, and ShellOpen. If an AutoExit or FileOpen macro already exists, Setup renames the original macros by appending User to the end of the macro name. For example "FileOpen" becomes "FileOpenUser".

Q: How can I tell if I need to do any macro integration work?
A: When ScanProt installs, it will look for FileOpen and AutoExit macros in your Normal template. If it finds FileOpen, it will display the message "Your FileOpen macro has been renamed to FileOpenUser". You will see a similar message for AutoExit. If you want to know whether this will happen before installing ScanProt, choose the Macro command on the Tools menu and look through the names of the macros in the Macro Name list. If FileOpen or AutoExit appears in the list, then you will have some macro integration to do. If you have already installed ScanProt and are unsure whether it renamed FileOpen and AutoExit, look in the Macro Name list for FileOpenUser and/or AutoExitUser. In addition, if you have any custom templates that have their own AutoExit or FileOpen macros, then you will have some macro integration to do.

Q: Is it always possible for me to integrate my existing macros with the protection macros?
A: Not always. If any of the user macros are *execute-only* macros, then you will not be able to integrate the existing macros with the protection macros. To determine if your macros are execute-only macros, follow these steps:

1. Choose the Macro command on the Tools menu.
2. Select each of the xxxxUser macros in turn.
3. As you select each macro, look to see whether the "Edit" button becomes disabled. If the "Edit" button becomes disabled when you select one of the xxxxUser macros, it means that that macro is an execute-only macro and it cannot be integrated with the protection macro in its present state.

If the macros are execute-only, customers have two options: They can either 1)contact the author/vendor of the original macros and ask for editable versions of the macros or for a new version of the execute-only macros which are integrated with the protection tool, or 2) decide to install the protection tool macros and forgo the features of the original macros or vice versa.

Specific Information

If you've gotten to this point in the instructions, then you've determined that the Macro Virus Protection tool has renamed at least one of your user macros, and that none of the renamed user macros are execute-only macros. Depending on which user macros have been renamed, you will have to follow different steps. The two sets of steps are described below.

Integrating with FileOpen
The FileOpen code that the Macro Virus Protection Tool installs simply makes a call into the ShellOpen macro. Therefore, in order to integrate your code in the FileOpenUser macro, you need to copy and paste the appropriate code into the ShellOpen macro (instead of the FileOpen macro.) Examine the code in your FileOpenUser macro and determine which parts of the code are to run *before* the actual FileOpen operation, and which parts of the code should run *after* the FileOpen operation. Once you determine

which code goes *before* and which code goes *after*, you need to copy and paste the "before" code, into the ShellOpen macro at the first point in the ShellOpen code where the comment reads "INSERT YOUR CODE HERE." Then copy and paste the "after" code at the second point in the ShellOpen code where the comment reads "INSERT YOUR CODE HERE." Note that copying your macro code into other points in the macro could cause the protection macros to lose their protection capabilities. In many cases you will have to do additional coding or bug fixing to make the integration seamless, but the steps above give the general guidelines to follow.

IMPORTANT: The steps above will let you integrate with any custom FileOpen macro you might have had in the Normal template. However, you also need to integrate with your custom templates that have FileOpen macros in them. Completing this procedure involves 1) copying the ShellOpen macro from the Normal template to each of your custom templates which contain FileOpen macros, 2) integrating the existing FileOpen macro in the template with the ShellOpen macro you just copied into the template, and 3) copying over the original FileOpen macro in your template with the FileOpen macro from your Normal template. If you do not complete these steps on a template which contains a FileOpen macro, then a macro virus could escape detection when a user does a File Open operation when the active document is either the template with the FileOpen macro or a document attached to that template.

Integrating with AutoExit

To integrate with the AutoExit macro, you need to examine the code in your AutoExitUser macro and determine which parts of the code are to run *before* the actual FileExit operation, and which parts of the code should run *after* the FileExit operation. Once you determine which code goes *before* and which code goes *after*, you need to copy the "before" code, and paste it into the AutoExit macro at the first point in the AutoExit code where the comment reads "INSERT YOUR CODE HERE." Next copy and paste the "after" code at the second point in the AutoExit code where the comment reads "INSERT YOUR CODE HERE." Note that copying your macro code into other points in the macro could cause the protection macros to lose their protection capabilities. In many cases you will have to do additional coding or bug fixing to make the integration seamless, but the steps above give the general guidelines to follow.

Once you have completed all of your macro integration, you can delete all of the xxxxUser macros in the Normal template, since they won't actually ever get called.