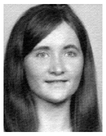
MacroList by Padgett v1.10

This document is designed to add a new button on the toolbar that will permit the user to examine any document received for the presence of possibly malicious macros, check for existing macros in the global template file, and verify that these are what are desired. Please read the *documentation* below.

Double-click   to begin installation

note: should the macro fail to start, pull down TOOLS, select MACRO, and doubleclick on appFix



Dedicated to my beloved and loving wife, Linda

About the ABOUT

For full details, visit my web page **http://www.netmind.com/~padgett/** and look under **Anti-Virus Hobby** for a section on **<u>TRIALS</u>*.***

Documentation

Please see the caveat before the PGP signatures
version 1.10 - January 27, 1997 - adds check for key assignments in document
version 1.02 - January 21st, 1997
  adds CLOSE DOC capability to document dialog box for safe exit when macros cannot be deleted. Also groups possibly language-related string variables at the beginning of each macro. (not distributed)
version 1.00 - January 14th, 1997 - first public release

This template contains six macros:

appAO:	Template to place an AutoOpen call to the MacroList function every time a document is openedi (only if decision is made not to disable AutoMacros)
appFix:	The general installation program
appTL:	Macro repair macro
auto1:	Template for an AutoExec which will DisableAutoMacros (least risk)
auto2:	Template for an AutoExec which will EnableAutoMacros (higher risk)
-	both will turn the "Prompt to Save NORMAL" option to ON
MacroL:	The Macro which will display macros.

Once installed, the MacroList will be reachable with a button in the "standard" toolbar. This will be in the leftmost position and identified by a capital "M". There will generally be added three macros to the NORMAL list: AutoExec, APTM, and APMACRO. Should it be selected that AutoMacros are enabled, a fourth macro, AutoOpen, will also be added.

It is **strongly** suggested that the installation be permitted to <u>disable</u> automacros (the question will be asked) and that the "M" button be pressed whenever a document is opened. Enabling automacros ("NO" answer) will add a slight but significant risk of infection.

Operation

Whenever an unknown document is opened, it is suggested that the “M” button be pressed *first*. If AutoMacros were not disabled, then this will occur automatically. In this case if the dialog box *does not* appear on opening a document then the document contained an AutoOpen macro which has taken control. It could be a virus (why disabling AutoMacros is strongly urged (cannot say often enough but will try 8*).

Opening display will be of a list of macros found in the currently opened document. If none are found, a message box to that effect will be displayed. If one or more macros is found, the names will display in a listbox. Options will be RETURN, NORMAL, ABOUT, DELETE ALL, and CLOSE DOC.

The NORMAL button will toggle between messages found in the document and the global template. The DELETE ALL and CLOSE DOC buttons will not be displayed when the global template is selected, each macro will have to be removed individually.

Note: if you are concerned about what is displayed in the open document it is suggested that CLOSE DOC be selected. This will close the document without saving any changes and uses what I believe to be a non-interceptable mechanism to do so.

From either NORMAL or DOCUMENT, if a doubleclick is made on a macro name, additional options and a listing of the macro will appear. The macro may not be edited from this display but may be scrolled using the pageup and pagedown buttons. Other options are DELETE and EXECUTE. Confirmation is required for DELETE, DELETE ALL (for documents only), and EXECUTE.

When in doubt, it is suggested that CLOSE DOC be selected immediately (and hopefully before any harm has been done) closes the document without any changes being made. You can then contact the originator to determine if this is a valid template.

Note: “DELETE” and “DELETE ALL” operate only within the current context. A separate action (save) is required to make permanent change to the original document though if selected, AutoSave can accoplish this.

Use: Whenever a document is opened, the “M’ button will tell you if the document contains macros. In general *any* document unexpectedly found to contain macros should be suspect, particularly if AutoOpen, AutoClose, AutoNew, and /or AutoSave (the “AutoMacros”), FileOpen, FileSave, FileSaveAs, FileNew, FileNewDefault, or FileClose since WORD will transfer control to the document macros on loading but well structured macros will generally create their own rather than replacing existing macros. Special Note: If the MicroSoft SCANPROTECT macros have been installed, one of them is FileOpen however be sure that this is the source before continuing.

With version 1.10 I have added detection of any key assignments in the open document. If such are found, a second window will open listing the key combination and the connected macro. The key codes are basically the decimal value of the ASCII
code with extensions for the keypads and may be found under HELP / WORDBASIC / TOOLSCUSTOMISEKEYBOARD, however movement of the scroll bar and double- clicking in this window will have no effect. To examine the referenced macro, double-click on its entry in the macro (first) window.

Again, should it be deemed necessary to enable AutoMacros, an AutoOpen macro will be created which, following the opening process, will invoke MacroList.

In this manner, should a document open and the MacroList display *not* appear, the M button should be pressed and any present AutoOpen in the document opened be examined for malicious activity. Special Note: if the MicroSoft SCANPROT is installed, and FileOpen is selected, the Microsoft macro will execute instead.

Personal note: I have found that the MicroSoft SCANPROT is very limited, both in identification and the fact that most direct launches of WORD from E-Mailers such as
ccMail (tm) will be ignored (see exception 6 in the SCANPROT readme). Please be aware of this if you decide to use both. (registered names belong to whomever they belong to).
Removal: Should it be necessary or desired to remove these macros from the global template, the following procedure should be followed:
1) Pull down TOOLS/MACRO
2) Select AutoExec with single click only (double click will execute)
3) Select DELETE
4) Select OK
5) Repeat 2-4 for other macros (AutoOpen (if present), APTM, & APMacro)

Do 6-10 only if you are using the default standard toolbar, otherwise delete the
"M" button manually (see WordBasic/DeleteButton in help)

6) Pull down VIEW/TOOLBARS
7) Select STANDARD with single click (may already be highlighted)
8) Select RESET
9) Make sure that lower display panel indicates "All Documents (NORMAL...)"
10) Click OK

Removal is complete.

Why do we have a problem ?

In the early 1990's when WORD version 6.0 was developed, several design decisions were made. First, the WORD macro language was greatly expanded. Second, the "automacros" (see above) were left active by default. Third, macros found in a document automatically took effect, replacing any similarly named functions in the program (note: not all functions can be captured - if they could, this macro could not have been written). Fourth, the user had little control over these functions. These factors taken together provided viruses written for it a "target rich environment".

Legend has it that the first macro virus, *CONCEPT*, was written inside Microsoft by an employee as a demonstration when superiors refused to take the matter seriously. Whatever its origin, it is currently (January, 1997) the most widespread type of computer virus reported.

About

This macro was created by Padgett Peterson, an information security professional who
has also been programing for over 30 years and studying viruses since 1987.

While many people feel that macro viruses cannot be controlled from inside WORD, it is my opinion that they can, rather it is the difficulty of detecting macros and the defaults built into WORD that has created the problem (particularly the fact that the document takes precidence over anything and without warning).

Unlike scanners, this program/macro knows nothing about viruses however it will reveal the presense of macros to the user and, unless expected, *any* document containing one or more macros (particularly the ones listed above - see *Operation*) should be treated with suspician.

This program/macro is an attempt to return control (or at least knowlege) to the user without also requiring them to become programmers.

Warmly,
Padgett

caveat: I have tested this program on every platforn I could gain access to: PC-Win 3.1, 3.11, PC-W95, NT 3.5.1, & NT 4.0 as well as Macintosh MACOS 7.5.x on SE/30, IIci and PowerPC. WORD versions ranged from 6.0c to 7.0a but have been told there is a problem under Office97. Will fix and post here as soon as I get a copy.

Also had available only American English versions of WORD. Other language versions which use different names for functions may require modification of hardcoded string variables to operate properly. With version 1.10 I have tried to collect those hardcoded string variable which will probably need to be changed in the front of appFix and APMacro (MacroL)

Have tried to check every possible operating condition but, like Microsoft, make no warrenty of any kind. At least this is FreeWare 8*)

Following are PGP signatures for each of the six macros

My public key is available from the MIT server or my web page

1) Signature for appAO

```
-----BEGIN PGP MESSAGE-----
Version: 4.0 Business Edition

iQCVAgUBMtRRw4VuK+48ORdVAQGxBQQAqqqWmTak/old4fJ0NXna55DxAqPSZ6Dh
dBRmnuLVfHg68a//1md2ufrPCQbN/eHBWINU0HwYqJGgItMfxOCP6aHU/KmQx2Hi
52rg1iubPA/yG/W2Lf6aYO82NaJSlr6rmGMs02ZiGxVcIiClkAZI3oWYM+zT+Coh
JL58XKDfGb4=
=Whco
-----END PGP MESSAGE-----
```

2) Signature for appFix

```
-----BEGIN PGP MESSAGE-----
Version: 4.0 Business Edition

iQCVAgUBMvkn0oVuK+48ORdVAQHxdwP+K4gi/jmoM5fjVCi79xp6CaB11fqgZsM7
gYVqCAfK+JO4ZMZJHJkNi28N7zFtEN8smwf0KYPBhFr7Q4J8dTUi5WmyfexOdyDe
JwrvfwXipkAjiMMUmOazB7upnI73QRf+TyzFWaxq6Ku4OLe5sPpoabdU95nX4nSL
6Zx/7UWtjyY=
=P4hm
-----END PGP MESSAGE-----
```

3) Signature for appTL

-----BEGIN PGP MESSAGE-----
Version: 4.0 Business Edition

iQCVAgUBMtRSnYVuK+48ORdVAQGrVQQA1SFPjbdKFCNIzrBtR3rSwdZbNhR7ev1b
Fddoqw6W15u8BMLi+vUKLYOEz9cy4GwRUEUbDQ2JtHir3+hNwZbSHX/v8AZM5RMr
KwKGoRCkdj4YhMaKRgNF6fnNAlUVNWv92pRPxYQAo1XaOzV5QdLmPCZSFghfJFzD
FK1VVp22UcE=
=H05m
-----END PGP MESSAGE-----

4) Signature for auto1

-----BEGIN PGP MESSAGE-----
Version: 4.0 Business Edition

iQCVAgUBMtRS34VuK+48ORdVAQEojgP/f9fNgpcPR3oupFZWn0p1EKcqzhcVCMyF
KjPt+kO5jpj5Fd8WzaVF6ZYaWeDCuRfR33bxctljbqiNuuhoY45t0kDca8mDBMTy
5Mb57K8BrKcosrGmDUzEW0A7xKVPYsLmIJNG7F0i89pRx5MlKjBr4+T36aKIemo5
1fDDyFfXjsc=
=JPoL
-----END PGP MESSAGE-----

5) Signature for auto2

-----BEGIN PGP MESSAGE-----
Version: 4.0 Business Edition

iQCVAgUBMtRTD4VuK+48ORdVAQG1TAP+OIumA7DO+vuW34wsSqUnUgfpZJ61pNZX
FF/clGj2oG4x937DcFbRAVePCYJMi0nqCYy1e9eA7k4bSBc+VZT3k1neKg08Bf3d
Q8PchVxPeIQ75bIMey0R1tN61rOUgPk5t1dZg/slLUx/nkb5Vp6DAOP6jFIYihBE
uc1o7pYSJHc=
=QVec
-----END PGP MESSAGE-----

6) Signature for MacroL

-----BEGIN PGP MESSAGE-----
Version: 4.0 Business Edition

iQCVAgUBMvkoIIVuK+48ORdVAQEsGQP/Rp50DXzncRi+uHPvK8xb9XfQEIb8Eewg
sYVufjkBs+nJU12bYJQCp1jBqPp4tD1jOpSTKlawe0PM4Dkp2chKbkEsjSUw5Ywg
IhHxRidBLGIW2B00+WqKDRpaIyedxOaJyCCDaZpzloOHdHnRiDqB2wT855aHXi7c
EAjRGA8hZxU=
=YIRe
-----END PGP MESSAGE-----

ps I have been chided in the past for making my anti-virus programs too small to be taken seriously. Thanks to WORD, this should be large enough.