

Anti-Macro Kit

This document is supposed to install or uninstall Anti-Macro Kit. If you previously disabled the execution of the automatic macros, and a dialog box has not shown up immediately after opening this document, you can start the installation or the removal process by double-clicking on the buttons below.

To install AMK double-click on the next line:

To uninstall AMK double-click on the next line:

Or if you only want to scan your system, double-click on the next line:

General description of Anti-Macro Kit

Anti-Macro Kit is a toolkit for the detection and removal of Word for Windows based macro viruses.

This document has the following functions: installs AMK, uninstalls a previously installed version of AMK or only scans the specified directories for macro viruses.

Features of AMK:

After installation the toolkit can be configured to check each opened document for viral macros. The toolkit is able to detect and clean all known macro viruses as of the date of the release. It also has the capability in “High sensitivity” mode to detect new and unknown macro viruses. The toolkit has an on-demand scanner to search for viruses on local or network drives.

Moreover upon each startup the toolkit will check the number of macros in the global template. If this number is changed relative to the saved value the user is prompted for action. A complete list of the global macros is presented to the user (not including the toolkit macros) who can either delete them all or update the integrity information. If any of the toolkit macros is missing the user is informed and advised to reinstall AMK.

Although all of the options of AMK are stored in *win.ini* and can be edited with a text editor it is still preferable to change options via the Options... menu item.

Installing AMK:

The current document contains a macro named AutoOpen which is responsible for installation of the toolkit. If the execution of automatic macros is not turned off, Word for Windows will automatically execute this macro when opening the document. If the automacros are disabled, double-clicking on the “Install AMK” button in this document will start the installation process. First the global template is searched for the presence of known macro viruses. If none of them found, the existing macros in the global template are presented to the user who can delete them or continue the installation. Then then toolkit macros will be copied to the global template. If the AutoExec macro already exists the user can choose either to keep the old one (in this case it will be renamed to AMKAutoExec) or to delete the old one. If an existing FileOpen macro is detected it will be overwritten.

After installation a new menu item, AMK appears in the menubar. The following functions can be selected from the menubar:

Safe commands:

AMK gives the user safe access to functions normally intercepted by macro viruses. These include the most important activities: saving and closing files and accessing the macro tools. Even if a macro virus is active, these functions are safe.

Scan...:

The selection of this menu item pops up a dialog box to select which directories and which type of files the user wants to scan. It is also possible to specify whether the scan should include files in the subdirectories or not. A drawback of the subdirectory scan is that if the selected directory tree contains too much document files not all of them will be scanned. This is a problem with Word for Windows and later versions might be able to overcome it.

Auto macro status:

This menu item gives the user information about whether the processing of automatic macros is enabled or disabled. While executing this command suspicious screen activity is present. There is no need to panic, it is perfectly normal.

Options...:

The user can modify some options of the toolkit. The following options are available in the current version of AMK:

” Check for documents when opened” : when selected, every document will be scanned for macro viruses as opened. Although selecting option slightly increases the time for loading a document this is still acceptable. Note that this protection does not work select a document from the list of recently used files in File menu. It is advised to select this option.

“ Search for user defined signature” : when selected, the user can search for a previously defined signature. It is extremely useful when a macro virus is found and there is no time to wait for the updates.

“ High sensitivity” : when selected, AMK will report every file that contains macros that could possibly belong to viruses (that is that redefine built-in Word commands). This applies only the scanner modul. The resident monitoring modul won't alarm a .DOT file

macros is opened even with in mode (since it is quite normal that document contain macros and all known macro viruses spread in DOC files). Note that while selecting this option will not result in slowdown the rate of false alarms to identify this option unless the presence of a virus is suspected.

“ Disable auto macro processing” : when selected, the the execution of automatic macros is disabled. Note that while upon activation it is selected it doesn't mean that auto macros are disabled. processing status is set after finishing the dialog box. It is not indicator. To query the automacro status you must select the menu item.

Define signature...:

The user can define signatures for new macro viruses. Dialog box will pop up where the necessary information can be specified: the names of the macros belonging to the virus, the total number of viral macros (0 should be specified when unknown) and the name of the virus. The toolkit will use this information for the detection and the removal of the virus.

Uninstall AMK:

Selecting this option the user can uninstall AMK: the AMK menu item will be removed from the menu bar and the toolkit macros will be deleted from the global template. Unfortunately the AMKUninstall macro can not be removed this way. Although it will not affect the normal operation of Word for Windows the user might want to remove it completely. The easiest way is to select Uninstall AMK in this document: this method removes all the macros belonging to the toolkit. Otherwise the user can delete it manually.

macro