WordMacro/DMV

WordMacro/DMV is probably the first Word macro virus to have been written. It is test virus, written by a person called Joel McNamara to study the behavior of macro viruses. As such, it is no threat - it announces its presence in the system, and keeps the user informed of its actions.

WordMacro/Concept

WordMacro/Concept - also known as Word Prank Macro or WW6Macro - is a Word macro virus written with the Microsoft Word v6.x macro language. It has been reported most countries in the world, and seems to have no trouble propagating in the wild. It was originally found in the summer of 1995 and was the first widespread macro virus.

WordMacro/Nuclear

WordMacro/Nuclear was recently discovered. Like WordMacro/DMV and WordMacro/Concept, it spreads through Microsoft Word documents. The new virus was first spotted on a FTP site in Internet, in a publicly accessible area which has in the past been a notorious distribution site for viral code. Apparently, the viruse's distributor has some sense of irony; the virus was attached to a document which described an earlier Word macro virus, WordMacro/Concept.

Whereas WordMacro/DMV is a test virus and WordMacro/Concept is only potentially harmful, WordMacro/Nuclear is destructive, harmful and generally obnoxious. It consists of a number of Word macros attached to documents. When an infected document is opened, the virus is executed and tries to infect Word's global document template, NORMAL.DOT.

Unlike WordMacro/Concept - which pops up a dialogue box when it infects NORMAL.DOT - WordMacro/Nuclear does not announce its arrival in the system. Instead, it lays low and infects every document created with the *File/Save As* command by attaching its own macros to it. The virus tries to hide its presence by switching off the "Prompt to save NORMAL.DOT" option (in the Options dialogue, opened from Tools menu) every time a document is closed. That way, the user is no longer asked whether changes in NORMAL.DOT should be saved, and the virus is that more likely to go unnoticed. Many users relied on this option to protect themselves against the WordMacro/Concept virus, but it obviouisly no longer works against Nuclear.

WordMacro/Nuclear contains several potentially destructive and irritating routines. The next time Word is started after initial infection, one of its constituent macros, "DropSuriv", looks up the time in the computer's clock. If the time is between 17.00 and 17.59, the virus tries to inject a more traditional DOS/Windows file virus called "Ph33r" into the system (as the viruse's author has commented in the viruse's code: "5PM - approx time before work is finished"). "Suriv" is, of course, "Virus" spelled backwards. However, due to an error, this routine does not work as intended in any of the popular operating environments.

WordMacro/Atom

WordMacro/Atom was found in February 1996. It's operating mechanism is quite similar to WordMacro/Concept, with the following differences:

- All the macros in this virus are encrypted (Word's *execute-only* feature)
- The virus replicates during file openings as well, in addition to saving files
- The virus has two destructive payloads

First activation happens when the date is December 13th. At this date the virus attempts to delete all files in the current directory.
Second activation happens when a *File/Save As* command is issued and the seconds of the clock are equal to 13. If so, the virus will password-protect the document, making it unaccesible to the user in the future. The password is set to be **ATOM#1**.