FEATURE SERIES

Macro Viruses – Part 3

Dr Igor Muttik
AVERT Labs, UK

When different macro viruses meet on one user system they may mate. WordBasic copies macros by name. If two viruses have the same macro name one virus may copy a macro belonging to another virus. Then this cocktail may be able to travel with one (or several) macros substituted. Such mated viruses do exist and they replicate happily with the macros 'borrowed' from other macro viruses.

Viruses can also snatch macros from a set of legitimate macros in NORMAL.DOT. For example, there are many known macro viruses which are the result of mating between the ScanProt macro (the anti-Concept macro released by *Microsoft*) and this or that other macro virus.

VBA5/6 viruses also are able to mate. Apart from just two sets of macros being present in one document, they now can merge inside a single module. Most contemporary viruses live in the class module called 'ThisDocument' (or 'ThisWorkbook' for *Excel 97* or *Excel 2000*). If two viruses using the same class module infect one DOC file they can:

1) stop working if they use the same functions (e.g. two functions for 'Document_Open' in one module produce a VBA error)
2) live happily together (e.g. one infects on 'Document_Open', another on 'Document_Close') and spread together, one attached to another
3) produce a mixture, the behaviour of which would depend on which virus' function is used to replicate the cocktail. Such behaviour can be very complex depending on the history – it may devolve to non-replicating samples, lose some modules or functions, etc.

Devolving

Some viruses are badly written and can lose their own macros. For example, the original virus consists of a set: {AutoOpen, FileSave, and FileSaveAs}. If it replicates via AutoOpen the whole macro set is preserved, but if the user invokes FileSaveAs the virus fails to copy FileSave.

The resulting virus – {AutoOpen, FileSaveAs} – is called a devolved macro virus (of course, only if this reduced set is able to replicate recursively, i.e. we have a 'viable devolved virus') and the original virus is known as devolving. A virus can devolve more then once (losing different macros) resulting in many different variants. Such variants are distinguished by attaching a digit to the name, e.g. WM/Rapi.A and WM/Rapi.A1 (the WM/Rapi family is famous for having several devolved variants).

In some cases a devolved virus no longer works and we get a 'non-viable devolved virus'. These do not replicate but anti-virus programs should still be able to detect and clean them as they occur as a result of a viral activity.

Naming

There is an email group called VMacro consisting of the most active anti-virus researchers in the field. They share the identification data (not the virus samples – they are sent more carefully within *CARO*), discussing the family relationship of macro viruses, their names and other issues related to macro viruses.

It was decided that names of macro viruses start with a platform identifier – WM (*Word* Macro for viruses using WordBasic), XM (*Excel* Macro for VBA3), APM (*AmiPro* Macro), A97M (*Access 97* Macro), W97M (*Word 97* Macro), X97M (*Excel 97* Macro), PP97M (*PowerPoint 97*), CSC (*CorelDraw Script*).

Then, the family name (e.g. Wazzu) goes after the slash separator, followed by a dot and a variant suffix (which can be omitted). Variant suffixes start at .A and go through to .Z, then start again at .AA to .AZ, etc. If the virus devolves the index is attached to every variant. For viruses which infect all *Office 97* applications an O97M prefix can be used or multiple prefixes can be grouped in curly brackets {W97M/X97M}. This also applies to multi-partite infectors hitting, say, DOCs and EXEs {W97M/Win95}:

WM/Wazzu.A

WM/Concept.A

WM/Npad.BV

APM/GreenStripe

WM/Rapi.E2

XM/Laroux.B

W97M/Appder.B

X97M/Laroux.JH

O97M/Tristate.A

{W97M/X97M}/Shiver.A

{W97M/Win95}/Coke.22231.A

A97M/AccessiV

CSC/CSV

If the virus is language-specific (e.g. it replicates only under a localized version of *WinWord*) the virus name can be followed by a country designator. Internet abbreviations are used, such as ':De' (for Germany) or ':It' (for Italy). [*This is the final part of the consecutively published series on macro viruses. Ed.*]