Macro Viruses and Viruses in Microsoft Word

Paul Ducklin, Sophos Plc, Oxford, England

Part # tr00006u/980313

Introduction

Viruses which infect Microsoft Word documents have recently received massive publicity – not all of which is exaggerated: such viruses do indeed exist, and are known to be in the wild in several countries. These viruses can be actuated by opening infected documents, and may spread rapidly in organisations which are used to sharing and exchanging documents. Viruses have traditionally been associated with programs and not with data files; consequently, these new Word viruses have provoked considerable fear.

Nevertheless, neither the theory nor the reality of this group of viruses is new. They are generally known as *macro viruses*, and rely on an environ-ment in which data files are not just passive information holders, but may contain active commands to manipulate that environment.

A lot of software products allow this, because they allow their data files to contain programmatic commands that would more typically be typed at the keyboard or issued with a mouse. The aim is to carry out a whole sequence of program functions automatically, rather than having to type them in over and over again.

Many programs with macro support allow their macros to access a substantial range of functions such as opening, manipulating and closing files, and even issuing direct operating system commands. Some macro systems go even further – they allow macros to be mixed into regular data files, rather than requiring macros to be stored separately. They may also define special types of macro (typically identified by a predefined name) which will automatically be fired up when a file is loaded or the system is started.

Clearly, when you combine data files, a macro language and the automatic execution of special macros, you end up with a potential security nightmare. Viruses, Trojan horses and modification-of-service attacks are all remarkably possible in such an environment.

One of the first macro virus attacks that made it into the wild was *Dukakis*, a virus which appeared in 1988 and which was written in the language *HyperTalk* [Schn94]. HyperTalk files are not regular programs – they are data files for a hypertext information system called *HyperCard*, which supports a programming environment powerful enough for writing viruses. HyperCard data files (known as *stacks*) are extremely common in the Macintosh world, not least because software to access these stacks is shipped as standard on every new Macintosh.

In the PC world, the possibility of macro viruses for common software packages was investigated at about the same time Dukakis appeared. Prof Harold Highland, writing in Computers and Security [High89] in 1989, described a Lotus 1-2-3 virus. Presciently, Highland asked his readers to "...note that a macro virus is not limited to Lotus 1-2-3 [...]. Similar techniques can be used in any program that permits a user to write his own macros. This includes not only spreadsheets but also database programs. One researcher with whom we spoke believed that such viruses might even be created with some of the text editors that permit the writing of macros..."

The Present

Highland was right. MS Word 6.0 has a particularly rich macro language (WordBasic), and a number of macro hooks with which an unsuspecting user can be lured into executing a hitherto unseen and unknown macro simply by loading a document. Writing a Word document virus turns out to be fairly easy.

Actually, Word itself differentiates between *Documents* (which cannot contain macro commands) and *Templates* (which can), but the two can be made to appear almost indistinguishable when using Word. So, although Word purists might argue that "a document infected with a Word virus" is technically impossible, we shall say this sort of thing here because it reflects reality.

This reality includes a number of convenient, but potentially dangerous, features:

- a document can contain a macro which will be executed transparently and automatically when that document is opened;
- a macro, once running, can make changes to a set of global macros that may end up being transparently included in many or all documents created in the future;
- there are numerous automatic triggers that malicious macro code is able to exploit, in addition to the one which operates when a document is opened;
- macros can be defined which transparently override the normal behaviour of many Word functions commonly accessed via menu or toolbar;
- malicious Word macros will typically work on all operating systems for which the Word environment is available, including Windows 3.x, Windows 95 and Macintosh.

These features are already exploited in the Word macro viruses known to date: *Concept*, *Nuclear*, *Nuclear-b*, *DMV*, *Colours*, *Hot*, *Atom*, *Xos* and *Imposter*. The first of these has become widespread, with reports from many countries; the others have produced only a handful of reports between them.

They are all hot news, however, because they came to the world's attention so suddenly. No macro virus has ever been as widespread as Concept, and no other virus has ever got its first chance at freedom in such a fashion: shipped worldwide on an official Microsoft CD-ROM [Secu95]. Although this was a relatively low-volume CD distribution, it was enough to produce a critical mass of infections in the wild, and more than enough to set news-wires abuzz.

Word documents that are not viral, but nevertheless malicious, are just as easy to create. Two Word Trojans are known, *FormatC* and *Wiederöffnen*. Both seem to have originated in Germany, and run malicious macros automatically when they are opened. Because they cannot spread into your documents, however, they are of much less concern than viruses.

There is also a single virus for Ami Pro: *Green Stripe*. Fortunately, macro viruses are unlikely ever to be a significant problem in this environment, because Ami keeps documents and macros in separate files. This means that an Ami document file on its own cannot be used to transmit a virus. This fortunate design feature of Ami, combined with the difficulty that some researchers have expressed in getting Green Stripe to work correctly, suggests that this virus is of theoretical interest only and represents effectively no threat in the wild.

Concept

Being the most prevalent, this is obviously the best known of the current macro viruses. Unfortunately, despite the rapid presentation of information about it in virus-related groups on the Internet [Duck95], and the timely publication of a high-quality analysis [Gord95], Concept remains widely misunderstood.

Concept – operation

Infected documents contain a set of viral WordBasic macros, including one which is automatically invoked by Word when an infected file is opened. The virus then infects the Word environment by copying its malicious macros into the global macro environment – we talk of DOS viruses "going resident" in memory when they are executed; Concept effectively does the same thing within Word. The first Word security hole, therefore, is the feature which allows the transparent automatic execution of a macro inside a document when that document is loaded.

The second security hole appears when that automatic macro runs: it is able to make transparent changes to the global macro environment. This includes a modification which alters the behaviour of the built-in File/Save As menu option – our third security hole. Once the virus is resident, the use of File/Save As triggers a viral macro which replicates a copy of Concept into the document being saved.

Lastly, Word's default behaviour is to save permanently and automatically any changes to the global macro environment when you exit the program. This preserves such changes until the next time you load Word, when Concept will again be resident and active.

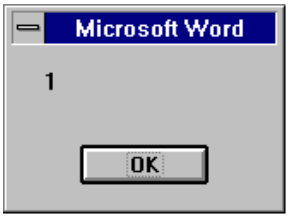

Fig 1: Dialogue box on initial Concept actuation

There is an obvious giveaway of Concept's actuation. When an infected document is first loaded, and the virus installs itself into the global environment, a dialogue box entitled "Microsoft Word" pops up, containing the single character "1" and an OK button (Fig 1). Note that looking out for this giveaway is relevant only to Concept, and is not a generic measure against macro viruses.

Concept – detecting and cleaning

To check your macro environment, you can use the Tools/Macro option (Fig 2). If you see (inter alia) the macros AAAZAO, AAAZFS, AutoOpen, PayLoad and FileSaveAs, then you are probably infected with Concept. Delete each of these macros to clean the current environment; by default, Word will save this cleaned environment for you when you exit.

A document is infected if it contains these same macros. Clean infected files as above, by going into Tools/Macro and deleting the offending macros. Be sure to save the cleaned document. Once you have loaded, cleaned and saved an infected document, three of the viral macros will be left behind in your global environment. Although they will no longer replicate, you might want to remove them before exiting Word, to leave your global template totally clean.

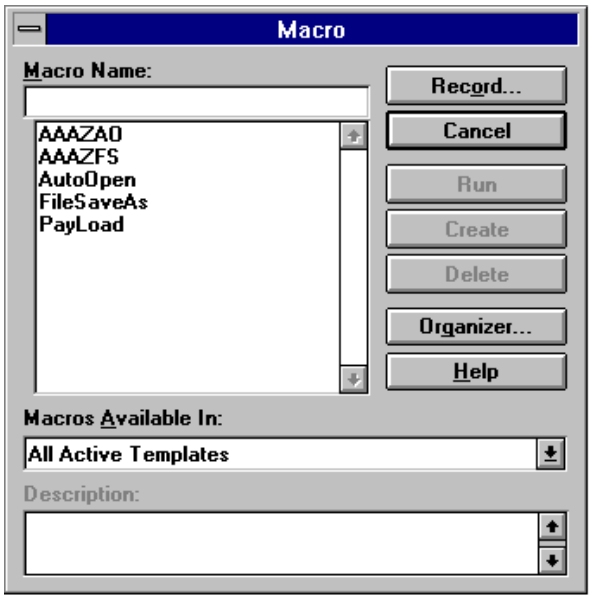

Fig 2: Tools/Macro box after Concept infection

Concept does not contain an explicit warhead or payload. However, the author of this virus has included a viral macro called PayLoad, which consists simply of a comment statement (a comment is a macro command that is ignored at execution-time, and is typically used for annotating macro programs to make them easier for others to understand). The comment states:

```
That's enough to prove my point
```

It is indeed.

Nuclear

Nuclear's first public appearance was on the Internet in an openly accessible area that has been used in the past for the uncontrolled distribution of viral code. Ironically (and, presumably, by malicious design) the virus was attached to a Word document which contained a brief overview of Concept.

Since then, a variant of this virus (Nuclear-b) has appeared in the wild in France.

Nuclear – operation

Like Concept, Nuclear is actuated when an infected document is opened. Unlike Concept, there is no obvious giveaway when the virus first runs. Nuclear simply goes resident by copying its macros into your global environment.

Additionally, when going resident, Nuclear executes its own PayLoad macro, which is not benign like that of Concept: on the fifth of April, it attempts to wipe out your system files if you are running on top of DOS (this includes Windows and Win95). Fortunately, this macro does not work correctly, and terminates prematurely without damaging anything.

Once resident, the virus alters the usual behaviour of several Word functions, the most important of these being File/Save As – this allows it to spread, like Concept, whenever a previously clean document is saved in this way.

Also, roughly every twelfth document you print will have the following text added at the end:

```
And finally I would like to say:
STOP ALL FRENCH NUCLEAR TESTING IN
THE PACIFIC
```

Additionally, next time you start Word, the virus looks at the clock. If it is between 17h00 and 17h59 (or, as a comment in the virus suggests, "5pm -approx time before work is finished"), the virus attempts to inject a DOS file virus named *Ph33r* (pronounced "fear") into your system. A bug in the virus prevents this warhead from detonating correctly, so you will not experience Ph33r, even if you are hit by Nuclear.

Nuclear-b treats 5pm slightly differently, dispensing with the attempt to inject the Ph33r virus, and triggering the fifth of April warhead intead.

Lastly, the virus switches off the menu setting *Tools/Option/Prompt to save NORMAL* every time you close a file. This means that you are less likely to notice Word saving changes that the virus has made to your global environment, because the dialogue box which warns you that this is about to happen will not appear.

Nuclear – detection and cleaning

As with Concept, an infected Word environment will contain a number of curiously named macros, which you can look for with the Tools/Macro menu option. One of the obvious names to look for is InsertPayload, the routine which adds the anti-nuclear remarks.

You can delete the viral macros both from documents and from the environment via the Tools/Macro dialogue box. With the original Nuclear virus, however, you cannot view or change the macros because they are marked "execute-only". This means that they cannot be edited using Word, and that they are scrambled inside infected files, so that inquisitive users will be unable to look at them directly.

The scrambling algorithm is trivial, however, and can be deduced simply by observation. This has allowed anti-virus experts to use their own tools to extract and analyse the offending macros.

DMV

This came to the attention of anti-virus researchers some time after Concept, although it was probably the first Word virus ever written – in December 1994. It claims to have been created by a person called Joel McNamara from the USA (joelm@eskimo.com) as a research exercise. McNamara wrote a lengthy paper outlining some of the security holes in Word which make virus writing possible, and describing a Word virus which he called the Document Macro Virus (whence the name DMV) in some detail. In case his description was insufficient, he included the actual virus itself in the document file, so that interested parties who cared to read about his virus could also actually experience it infecting their systems.

DMV – operation

Unlike Concept and Nuclear, DMV is self-contained in a single macro which is automatically invoked by Word when an infected document is closed. Since the viral macro is triggered both when you close the document explicitly yourself and when you close it implicitly by exiting Word, there is no obvious escape from the virus once you have opened an infected file.

By way of justifying itself as a "research" virus, DMV pops up dialogue boxes each step of the way as it executes. On closing an infected file, the virus infects NORMAL.DOT (the default global macro template); on closing an uninfected file once NORMAL is infected, the virus infects that file. This infection strategy is simple and effective.

The last dialogue box that appears (Fig 3) simply notes that the virus has replicated, and remarks that warhead code could be included at this point.

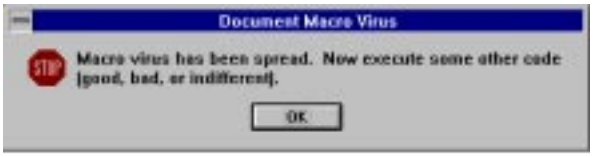

Fig 3: DMV's final dialogue box

DMV – detection and removal

Once again, Tools/Macro lets you see whether your environment is infected. Also, the obvious dialogue boxes when your system gets infected, and thereafter when the virus spreads to new documents, make it unlikely that you will fail to notice DMV.

Infected documents contain a macro called AutoClose, so you can remove the virus from a document by deleting this macro and resaving the document.

Colours

Colours hooks into many more Word functions than its predecessors. Its most notable feature is that infected documents include a macro that replaces the Tools/Macro menu option. Even if the virus fails to get control when you open an infected document, you will actuate the virus yourself if you attempt to hunt it down with Tools/Macro. Also, once an infected document is loaded, the viral replacement for Tools/Macro prevents you getting at the real Tools/Macro to delete the offending macros.

Colours also counts the number of times that its various viral routines have been acutated (this will typically happen at least twice for every document you access), and triggers its warhead every time its counter passes 300. The warhead picks a set of random colours for your Windows environment and saves this random colour set to your WIN.INI file. Next time you start Windows, you will probably be suprised at the bizarre colours which appear on the desktop.

Colours – detection and removal

Using Tools/Macro to search for and remove the viral macros is clearly impossible - Colours subverts this function, so it is no longer safe to use. You can, if you wish, use Files/Templates/Organiser/Macros instead. Here you will find an alternative dialogue box from which macros can be viewed and deleted. Look for a collection of macros including AutoOpen, AutoClose, ToolsMacro, as well as a macro simply called "macros". Delete them, and you have removed Colours.

Hot

Hot, which is deliberately destructive, made its debut in the wild in Moscow. Its warhead is delayed for a

minimum of fourteen days after a PC is first infected, and it went unreported in Russia until the warhead began to be unleashed. This suggests that it enjoyed over two weeks of uncontrolled replication before anyone became aware of it.

Hot – operation

Infected documents contain four execute-only macros: AutoOpen, DrawBringInFrOut, InsertPBreak and ToolsRepaginat. Loading such a document would normally trigger the AutoOpen macro, thus activating the virus. Its first action is to create an entry in the file WINWORD6.INI (the virus thus assumes you are using Word 6 for Windows) which records a "hot date" fourteen days in the future. This is when it will begin to trigger its warhead. On an infected machine, WINWORD6.INI would contain a line such as:

```
QLHot=35432
```

Next, the virus copies the abovementioned macros to the global template (typically NORMAL.DOT), changing their names as follows:

`AutoOpen`	to: `StartOfDoc`
`DrawBringInFrOut`	to: `AutoOpen`
`InsertPBreak`	to: `InsertPageBreak`
`ToolsRepaginat`	to: `FileSave`

So, when an infected document is used on a clean system, Hot uses AutoOpen to spread itself into the Word environment. Thereafter, the virus spreads to other documents via the FileSave macro, which is automatically triggered when you use the menu option File/Save. Once active within Word, the virus uses its AutoOpen macro to decide whether to detonate its warhead.

Randomly, within a few days of the viral "hot date", documents you try to open will have their contents erased instead. This warhead is disabled if the file C:\DOS\EGA5.CPI exists – possibly a safety feature used by the author while writing the virus.

The InsertPageBreak macro does, as its name suggests, insert a page break into the current document. However, it is also used by the virus to recognise that a document is already infected.

Hot – detection and removal

Cleaning an infected document is easy: use Tools/Macro to delete all offending macros from the list above. As with the Nuclear virus, you will be unable to view Hot's viral macros as they are marked execute-only.

Atom

Although simple in operation, Atom contains two warheads: one is directly and noticeably destructive, the other is potentially frustrating. It uses AutoOpen to infect the environment, and FileOpen to spread to other documents. Documents are actually infected and resaved during the operation of FileOpen. Newly-created documents are infected during FileSaveAs, which is also hooked by Atom.

On 13 December, Atom's direct warhead is unleashed: the virus issues the command `KILL "*.*"`, which erases all files in the current directory. The second warhead is triggered if it is 13 seconds past the minute when FileSaveAs is selected. This sets a password for the document being saved (whether you intended it to have one or not), which is likely to cause some confusion when you later try to reload it. The password used by the virus is `ATOM#1`.

Atom - detection and removal

As usual, Tools/Macro can be used to find and remove Atom's viral macros, which are: AutoOpen, FileOpen, FileSaveAs and Atom. Documents which have been password-protected by the virus can be recovered by using the password `ATOM#1` to load them into Word before deleting their infective macros.

Xos

Some observers have dubbed this virus *Xenixos* because this text string is used by the virus. Xos is probably a better name, however, given that Xenix is an old and by now venerable Unix-like operating system (OS) for the PC. Since this virus has nothing to do with Xenix, using the term "Xenix OS" to describe it is likely to cause confusion at the very least.

Xos - operation

This is a needlessly complicated virus presented proudly as "der erste MakroVirus im deutschen Sprachraum" (the first MacroVirus for the German-speaking world). It will spread to the environment (typically NORMAL.DOT) under most versions of Word, but requires the German edition of Word to get any further.

Xos hooks no fewer than nine system macros, including AutoExec and AutoOpen. Since these two macros have the same name in the German edition of Word as they do in the English Word, they are triggered even if a document infected with Xos is loaded under a non-German version of Word.

To replicate, however, Xos uses DateiSpeichern and DateiSpeichernUnter (FileSave and FileSaveAs). The viral replacements for these system macros are used

not only to spread the virus, but also to release the more damaging of its numerous warheads.

With DateiSpeichern, there is a 25% chance of the virus setting a password for the document being saved. The text used as the password is always the same: `xenixos`.

Also, during May, the virus adds a command to reformat drive C: to your AUTOEXEC.BAT file. This command assumes that the word for "Yes" in your language starts with "J", as it would if you were using a German-language DOS.

With DateiSpeichernUnter, the above warheads are repeated, but the virus also checks to see if the month is March. If it is, it tries to inject a variant of the DOS virus Neurobasher (also known as Neuroquila) into the directory C:\DOS, and to add a line to your AUTOEXEC file to force this virus to execute next time you boot up. Fortunately, a bug in Xos prevents the correct injection of the virus.

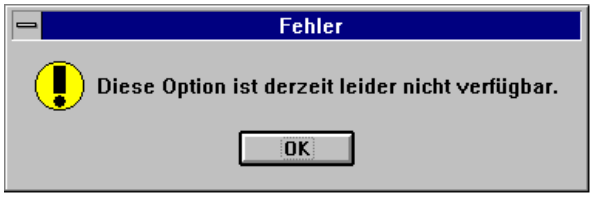

Figure 4: Xos's replacement for Extras/Macro

Further side-effects of Xos include appending the text `Nemesis Corp` to about 5% of documents you print out, and subverting the Extras/Makro (Tools/Macro) menu option to prevent you from using this facility to detect or remove the virus. Once you are infected with Xos, selecting Extras/Makro will produce what looks like a Word error (Fig 4).

Xos - detection and removal

Using Extras/Macro to search for and remove the viral macros is clearly impossible - this function is subverted and no longer works (if you have an English-language Word, however, Tools/Macro remains untouched).

Instead, you can use Datei/Dokumentvorlage/Organisieren/Makros. Here you will find an alternative dialogue box from which macros can be viewed and deleted. Look for a large collection of macros including AutoExec, AutoOpen, DateiÖffnen, DateiSpeichern, Drop and Dummy. You should also notice a collection of macros with names ending -Bak. Delete them all to remove the virus.

Documents which have been password-protected by the virus can be recovered by using the password `xenixos` to load them into Word before deleting their infective macros.

Imposter

This virus borrows its structure and operation from two earlier Word viruses, Concept and DMV. It is very simple in operation, and has no explicit warhead. When an infected document is loaded, Imposter uses the AutoClose macro to infect your Word environment when the document is closed.

Figure 5: Imposter claims to be DMV

Thereafter, the virus uses its own FileSaveAs macro, which it installs into your global template, to infect any documents saved using this menu option. On first infecting your environment, the virus pops up a dialogue box which might suggest, to the uninformed, an infection of the DMV virus (Fig 5).

Imposter - detection and removal

Infected documents contain the viral macros AutoClose and DMV; an infected global template will contain the macros DMV and FileSaveAs. Delete all these macros to remove the virus from both the environment and the current document.

FormatC

This is not a virus. However, a widely-disseminated report issued by the United States Department of Energy [DofE96] states not only that it is a virus, but also that it is in the wild. Naturally, this has caused considerable confusion. FormatC is simply a Word document which contains a macro that executes when the document is loaded, and tries to format your hard drive.

It is undesirable — FormatC is a Trojan horse, something which appears harmless on the outside but contains hidden dangers. However, it is not a virus and therefore cannot copy itself to other documents. Avoid loading Word documents from unknown or untrusted sources and you will minimise your risk of being caught by a Word macro Trojan.

Since FormatC cannot attach itself to your documents, it comes only in its original malicious form. The

document without its warhead has no value, and should thus be deleted if found.

Wiederöffnen

This is another Word Trojan — it is actually a Word 2 document, although it works under Word 6, too. The document includes a description in German of the potential risks posed by macros in documents, and (presumably by way of ensuring that you get the point) also includes its own macros that run when the document is opened and closed.

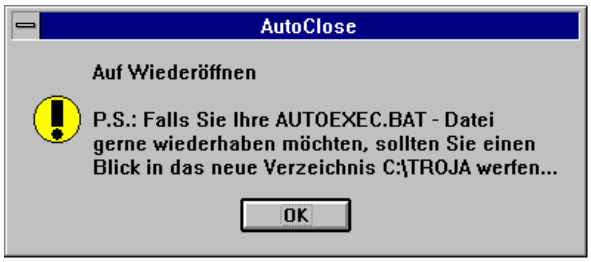

Fig 6: Auf Wiederöffnen

The side-effect of Wiederöffnen is fairly trivial: your AUTOEXEC.BAT file is hidden away in a specially-created directory.

Just in case you fail to notice this next time you boot, the Trojan mentions it when you close the document (Fig 6), explaining that, if you wish to get your AUTOEXEC.BAT file back, you should take a look in the newly-created directory C:\TROJA.

General Measures

If you create a global macro called AutoExec (this is run when Word starts up) that looks like this:

```
Sub MAIN
      DisableAutoMacros
      MsgBox "Auto macros are off"
End Sub
```

then you will be able to load an unknown document without any risk from an AutoOpen macro. Sadly, this is not a panacea – malicious documents (such as those infected with Colours) can use non-automatic macros to alter the functionality of built-in Word features. So, although the above AutoExec macro lets you *load* a document safely, it can do nothing about the safety of your Word environment thereafter.

Clearly, vetting Word documents for safety is best done outside Word. Anti-virus programs, such as Sophos' own SWEEP, are a good first line of defence. Automatic authorisation of document files as they are used can also be performed by some anti-virus products, such as Sophos' InterCheck.

In the meantime, it is obvious that more Word viruses are going to appear. Additionally, viruses are entirely possible for a number of other software environments – as the Dukakis virus showed for HyperCard, and Highland demonstrated for a now-antiquated version of Lotus 1-2-3. Word processors (and not just those from Microsoft), spreadsheets and database programs are obvious targets for virus writers. Most organisations, including yours, probably make on-going use of this sort of software.

What this means is that the general security of your information is certainly and directly at risk in any environment in which macro viruses are able to spread. However, control is in your hands. Don't panic, and do take the opportunity to learn more about the features – especially macro programmability – of the software you use.

Test and verify any security features you plan to utilise, and then configure accordingly. Don't treat these new Word viruses as a nightmare, but rather as an opportunity to take stock, and to learn.

Appendix – Word virus detection with Sophos' Sweep

SWEEP 2.83 will detect Word 6 macro viruses and Trojans in its default mode of operation (Quick mode).

If you are using InterCheck, then version 2.11 can be used to give automatic client-server detection of Word viruses. This means that you can use SWEEP and Intercheck to detect Word viruses arriving on diskette, via email or on CD-ROM.

A full list of search patterns for the viruses and Trojans mentioned in this document appears below. These can be used to add detection of viruses not handled by your current version of SWEEP by placing them in a file called SWEEP.PAT in the current directory of the current drive and running SWEEP.

```
Winword/Concept   57573649 6e666563 746f7206 06646f02 6904734d 65240c67
Winword/Nuclear   63e6e5e5 ee8fe6e3 e48fefe3 fd87b1c9 8aeaad8c a7918c93
Winword/Nuke-b    6f616464 6e0467c2 80673b80 0506076a 083a5061 794c6f61
Winword/DMV       740c6c01 0064521a 1d646452 1d690770 72657365 6e740c6c
Winword/Colours   d2cfd0c3 f2efc8d5 d2c7caca c3c2a3cf a7cfa0b8 c2c9a58a
Winword/Hot       a1869dad 889d8ca7 86cde58e 0369ec8e ee69ec8e e868ecef
Winword/Atom      c9cbb4ca a7a6c2c8 aec1e0a6 c2bcbbc2 8fcfa2e7 d2c9cbc3
Winword/Xos       88ea938b e788c0e1 d8e7fcaa 83e784f9 e7e0e7e0 e7fdfafc
Winword/Impost    05690169 126c0000 126c0000 060c6a03 444d561e 646f0269
Winword/FormatC   adb2beab ffbce5ff f0aabb8d b8f25fb8 315fdab5 d89c9092
Ami/GreenStripe   302c302c 342b3130 32342c22 69747322 2c226974 27732229
Word2/Offnen      6572f666 666e656e 1107126a 01110518 0a001106 1107126a
```

Patterns prefixed with "Winword" will be detected by SWEEP 2.83 and later in quick mode. Other patterns will be detected only in full mode.

For more information, please consult your SWEEP manual (look in the index under "pattern, adding a new one").

References

[DofE96] United States Dept of Energy: "CIAC Information Bulletin G-10A: Winword Macro Viruses", February 1996.

[Duck95] Paul Ducklin: Postings to the Usenet groups *comp.virus* and *alt.comp.virus*, August 1995.

[Gord95] Sarah Gordon: "What a (Winword.) Concept", *Virus Bulletin*, September 1995.

[High89] Prof Harold Highland: "Random Bits & Bytes" *Computers & Security*, 1989 (8).

[Schn94] Bruce Schneier: *Protect Your Macintosh*, Peachpit Press, 1994.

[Secu95] "Word Macro Virus Causes Alarm", *Secure Computing*, October 1995.