Global Information Assurance Certification Paper

A Sampling of Programs That Execute Text Documents

Chris Covington
5/4/00

Introduction

Most people are familiar with the Melissa macro viruses that infects Microsoft Word documents, but many people do not realize that this type of problem has existed in both Microsoft and UNIX programs long before that. This paper will explore a few of the others.

Background

When a user sits down at their computer and views a text document, it may be easy to believe that this action could not damage their computer, as they have not clicked on a .exe file or instructed the computer to do anything, other than display some text. In actuality, several programs for displaying text documents in Windows, MacOS, and UNIX include the ability to insert code into the text document file, often not displayed, that will change the way the program operates or run other programs.

This has been the case in Microsoft Word for Windows ever since a macro language interpreter was included in Microsoft Word, version 2. Microsoft Word, version 6 for Windows and Macintosh was the first version of Microsoft Word that will correctly run the popular Concept macro viruses due to improvements in the Word.Basic macro language interpreter. Microsoft Excel has a macro functionality in various versions, beginning with Excel, version 5.0, that allowed a similar type of macro virus called Laroux to be spread.

In the UNIX world, a somewhat similar feature set is included in the popular programs "vi" and "troff" (the formatting engine for the "man" command).

Examples

Example: The Microsoft Word Concept macro virus

What it does

Besides containing a text document, a Microsoft Word or Excel file may contain a separate macro section, which can contain a listing of Word.Basic commands. These commands are sometimes used to automate tasks, such as adding a name and address, to several documents in a routine way. The Concept virus uses Word.Basic to display an annoying popup box when the document is opened on an uninfected system, append a line to the winword.ini file, and replace the save-as menu option so that it can replicate itself to other documents.

Date reported

The Concept virus was the first Microsoft Word macro virus to appear in the wild. It proliferated by being included as a prank macro on two official Microsoft CDs, the "Microsoft Windows '95 Software Compatibility Test", and "The Microsoft Office 95 and Windows 95 Business Guide" dated August 17, 1995, and appearing on documents on a ServerWare CD called "Snap-On Tools for Windows NT".

Fix

Approximately two months after the macro was discovered, Microsoft released a fix for Word 95, downloadable as a document file called scan831.doc, which contained a macro fix.

For Word97 and Excel97, turn on Macro Virus protection from the Tools -> Options -> General menu selection. This will present you with a dialog box every time you open a document that contains macros. The user is then given a choice between enabling or disabling macros when they open the document. When they choose the "disable macros" option, they may check the purpose of the macro by looking at it with the Tools -> Macro -> Visual Basic Editor menu selection. The document can be re-opened if desired to enable the macro if things look alright. In addition, the virus can be restricted from infecting the default document template, normal.dot, by starting word, choosing Tools -> Macro -> Visual Basic Editor -> Project Window -> Normal. Then click on the lock project button and type in a write-protect password twice. After you close Word, your normal.dot file will be protected. Also, apply the Word97 template security patch from the Microsoft web site.

In Word2000, set the macro security level from the Tools -> Macro -> Security menu. Medium security will get results similar to the Word97 macro virus protection. Word2000 allows for digitally signed macros, which will allow you to better determine whether the sender approved the macro.

A virus scanner is highly recommended to help catch this and similar macro viruses.

Example: Vi modeline setting

What it does

Vi and its clones are common UNIX text editors installed by default in most modern UNIX systems. Modeline is a special vi option that, when set, executes the first and last five lines of any document that you open, if the lines are formatted in a specific way. The modeline option can be set in a user's ~/.virc file, in the $EXINIT environment variable, or in vi with the command ":set modeline".

To see if you are running a version that has it enabled by default, start vi, then type ":set all". If "modeline" is one of the items returned, it uses modelines. This is normal for many vi clones, including the vim editor included in Redhat Linux 6.2, which limit the modeline option to only interpret "set" commands and not dangerous ones such as "!" and "map".

If modeline is set by default, then you may wish to perform the following: to see if your vi clone allows dangerous options like "!" to be interpreted, create a file containing the line " vi: !id:" (note the leading space). Then, open the file again with vi. If you are greeted with the output of the "id" command (your username) then modeline will interpret all vi commands listed in the modelines.

Versions reported

Here is a small sampling of vi programs currently used:
Redhat Linux 6.2: Vim – Modelines enabled, but dangerous commands are not interpreted.
AIX 4.3.3: Modelines disabled. All commands are interpreted only if re-enabled by the user.
HP/UX 11.00: Modelines disabled. All commands are interpreted only if re-enabled by the user.
Solaris 2.6: Modelines disabled. All commands are interpreted only if re-enabled by the user.

Fix

Most versions have already been fixed for their default behavior. It has been said on USENET that soon after the modeline option was first introduced in vi, it was disabled by default because of the possibility for security problems. Later, some versions modified it so that it could not execute dangerous commands if the modeline option was enabled. Fortunately, a small sampling of prominent UNIX distributions reveals that vi editors generally fall into one of those two safe categories. In the rare event that yours does not, obtain the latest version from your vendor.

Example: Troff command (used by "man")

What it does

The commands troff (and possibly groff) are also commands installed on most UNIX systems, that are primarily used to process documents for display as man pages. That is to say, that one or more commands are invoked by the man command for display of new man pages that contain formatting codes in them. Troff is a text formatter and interprets codes inserted in the document. It uses those codes to format the document so that it displays well on the screen. Three of these codes are .sy (system call – execute the rest of the line), .wopen (open a file), and .write (write to the file). Groff has a .pso (execute the rest of the line) code. So by viewing a man page with formatting codes, the man page can execute code, or modify a file.

As an example, create a man1 directory. In the man1 directory, create a x.1 file containing the lines ".pso id", ".sy id", and ".wopen /etc/hosts". Then create a y.1 file in that directory containing the line ".pso id". Change directory to man1's parent directory, and type "man –M `pwd` x y". If your user id is displayed, then man invokes a command which interprets these unsafe features.

Date reported

Those features were mentioned in the Crypto-Gram newsletter on July 15, 1999 as a possible security problem and discussed in the BugTraq security mailing list soon after. Troff has had those features since it was originally written.

Fix

Newer versions of the programs now have a secure option enabled by default, which warns the user if the man page contains the questionable codes and ignores them. Troff formatted files are not normally used by the average user for casual use other than for automated operating system procedures like displaying the default man pages, so the danger is low. Ensuring that all man directories are only writable by the a system account, and searching for the above codes in any new man pages from unreputable sources will help prevent any damage from troff in the event that your troff and groff versions have not been patched.

References

Orvis, William J. "Microsoft Word Macro Viruses." CIAC Notes, Number 95-12. September 25, 1995. URL: http://www.ciac.org/ciac/notes/Notes12.shtml (3 May 2000).

CIAC. "Macro Virus Update." CIAC Information Bulletin I-023. 22 Jan, 1998. URL: http://www.ciac.org/ciac/bulletins/i-023.shtml (3 May 2000).

Microsoft. "Macro Virus Alert." Microsoft Office Update. URL: http://officeupdate.microsoft.com/articles/macroalert.htm (3 May 2000).

Martin, Richard John. "MS Word Macro Virus FAQ." Word 6.x Macro Virus FAQ for Alt.Comp.Virus Newsgroup. Version 2.0. 8 Mar. 1996. URL: http://www.bocklabs.wisc.edu/~janda/macro_faq.html (3 Mar 2000).

Symanec. " WM.Concept." WM.Concept. URL: http://www.symantec.com/avcenter/venc/data/wm.concept.html (3 May 2000).

Microsoft. "XL: Q&A About Excel Macro/Laroux Macro Virus." Microsoft Knowledge Base. Article ID Q154131. URL: http://support.microsoft.com/support/kb/ARTICLES/Q154/1/31.asp (3 May 2000).

Litmaath, Maarten. "vi Reference." vi Reference. Version 10. 26 Sep 1999. URL: http://www.cs.wustl.edu/~jxh/vi.html (3 May 2000).

Dik, Casper H.S. "Re: Was Melissa a bit of a hoax? – When vi got the modeline feature." comp.security.misc. Apr. 15 1999 URL: news:comp.security.misc (3 May 2000).

Moolenaar, Bram. "Vim documentation: options." VIM Reference Manual Version 5.6. Jan 5 2000. http://www.vim.org/html/options.html (3 May 2000).

McNair, Bruce. "Subject: Various." Crypto-Gram. 15 July 1999. URL: "http://www.counterpane.com/crypto-gram-9907.html (3 May 2000).

Wilk, Pawel. "Troff dangerous." BugTraq. 23 Jul 1999. URL: http://www.securityfocus.com/templates/archive.pike?list=1&date=1999-07-15&threaded=1 (3 May 2000).

Kirch, Olaf. "Re: Troff dangerous." BugTraq. 26 Jul 1999. URL: http://www.securityfocus.com/templates/archive.pike?list=1&date=1999-07-15&threaded=1 (3 May 2000).

Thorpe, Jason. "Re: Troff dangerous." BugTraq. 24 Jul 1999. URL: http://www.securityfocus.com/templates/archive.pike?list=1&date=1999-07-15&threaded=1 (3 May 2000).