Software Engineering Institute
Carnegie Mellon University

Frequently Asked Questions About the Melissa Virus

CERT Division

http://www.sei.cmu.edu

REV-03.18.2016.0

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 Frequently Asked Questions

This list of questions and answers, last updated on May 24, 1999, pertain to the Melissa virus.

Can Melissa spread through .RTF (Rich-text format) files?

We received reports on May 24, 1999 that the Melissa virus is spreading as RTF files. Files that are true RTF format do not contain macros. Because macros are not in true RTF files anti-virus scanning tools do not scan the files for macro viruses by default. This is being taken advantage of by simply renaming a Word document containing the Melissa macro virus to end in the .RTF extension.

How many reports have we received?

We have first-hand reports of more than 300 organizations affected, covering more than 100,000 individual hosts.

Is the damage limited only to denial-of-service?

No. Under some circumstances, confidential documents can be leaked without the user's knowledge. These circumstances include the use of a single template file by more than one user, and the transmission of an infected document to another user who has not previously been infected. Additionally, if you fail to clean up the virus correctly and completely (for example, by not cleaning the normal.dot file) you may expose confidential information at a later time.

What about Papa, and other variants?

We have received reports of other variants of Melissa, including one named Papa. At the present time, we have not received a significant number of reports of Papa outbreaks. If you practice anti-virus precautions on a regular basis, you can protect yourself against Papa and other variants of Melissa.

Are Macro viruses new?

No. According to the Department of Energy's Computer Incident Advisory Capability (CIAC), macro viruses for Microsoft Word appeared as early as 1995, with over 1000 variants for Word and other products by 1998. See http://www.ciac.org/ciac/bulletins/i-023.shtml for more information.

Why was Melissa so serious?

Melissa was different from other macro viruses because of the speed at which it spread. The first confirmed reports of Melissa were received on Friday, March 26, 1999. By Monday, March 29, it had reached more than 100,000 computers. Some sites had to take their mail systems off-line. One site reported receiving 32,000 copies of mail messages containing Melissa on their systems within 45 minutes.

Are Macro viruses limited to Microsoft Word?

No. Macro viruses can affect other products, including other products from Microsoft such as Excel and Powerpoint. The Papa virus, for instance, is reported to be spread via Excel.

Is Melissa a worm?

Melissa requires user interaction to propagate, therefore we do not consider it a worm. However, Melissa can propagate quickly from one computer to another with minimal interaction required by the user.

Does the Melissa virus affect MacOS?

The Melissa virus can infect files stored on and shared with MacOS-based systems running Word 98. However, when the virus runs on MacOS systems, it is not able to send electronic mail, and its propagation will be slower on MacOS systems.

Can I protect myself by marking the normal.dot file read-only?

At best, marking the normal.dot file read only is a stop-gap protection. On Windows 98/95 systems and on MacOS, viruses can circumvent the read-only protection. Instead, we recommend setting Word to prompt the user before making any changes to the normal.dot file if you are concerned about changes to that file.

How can I protect myself against variants of Melissa?

Disable macros by default. Use caution when operating any product when macros are enabled. Keep your antivirus products up-to-date. Be leery of unsolicited documents or executable programs received in electronic mail. Beware of software that comes from untrusted sources.

Who wrote Melissa? Why was Melissa written? What crimes has the author committed? What is the status of the investigation?

The CERT Coordination Center is a technical organization. We concentrate on the technical aspects of computer security problems. We have no legal authority and we do not "catch the bad guys."

Can I be affected if I don't use Outlook?

If it is installed, Outlook is used by the virus to send mail. Otherwise, Melissa behaves like a normal virus: you can infect others by carelessly sharing files.

I use a mail package other than Outlook. Am I affected?

The mailer you use to read mail doesn't matter. The virus will use Outlook, if Outlook is installed, to send copies of itself. How you receive it doesn't matter.

How effective are systems that look at the subject of the mail message?

Systems that rely solely on pattern matching to recognize the virus can be used as a stop gap measure to prevent the spread of a particular virus, but will fail as soon as the virus mutates so that it no longer matches the pattern. This can be very effective as a short-term fix, but will not provide long-term protection.

Is Melissa the most dangerous virus possible?

Melissa was relatively non-destructive and easily detected. Variants could be significantly more destructive or stealthy. We strongly encourage you to be aware of the risks posed by viruses and other computer security concerns at all times.

Are you aware of the connection between the Melissa virus and the television show *The Simpsons*?

Yes.

What products are affected?

Outlook 98 and Outlook 2000 for Windows platforms can be used to propagate the virus. Microsoft Word 97 and Word 2000 for Windows and Word 98 for Macintosh can be used by the virus to infect other documents. Earlier versions of Word, including Word 95, cannot be used to infect other documents, nor can Outlook Express on any platform be used to propagate the virus via email.

Why is it called Melissa?

It was named Melissa by the antivirus software vendors.

Do you have to open the email attachment to be infected?

Yes. To be affected by Melissa and other, similar macro viruses, you must open the attachment and permit macros to run. You cannot be affected by Melissa or similar viruses merely by receiving the email.

If I receive the virus mailed to me by someone, should I notify them?

Yes. We encourage you to notify them. More information about dealing with incidents can be found in our Incident Reporting Guidelines at http://www.cert.org/tech_tips/incident_reporting.html

I am a novice user and know little about computer language. I read your virus alert and tried to determine whether or not my Word macros were disabled. I use Office 97, professional version, and did not find a way to disable the macro function. However, under the menu options "Tools/Options/General" I found a checked box that says "Macro virus protection." Will this option provide adequate protection against the Melissa macro virus and other, similar viruses?

If this option is checked, Word will give you a warning any time you open a document that has macros embedded in it. The warning will give you the opportunity to prevent any macros from running.

Are the Melissa macro virus and Happy99 the same thing?

No. While Melissa is a macro virus, Happy99.exe is a Trojan horse program. For more information about Happy99.exe, please see Incident Note IN-99-02 Happy99.exe Trojan Horse at http://www.cert.org/incident_notes/IN-99-02.html