Introduction to Viruses & Virus Hoaxes

Jennifer Vesperman

jenn@linuxchix.org

2002-02-24

Revision History

Revision 0.1 2002-02-17 Revised by: MEG
Converted from text file. Modified wording.
Revision 0.2 2002-02-23 Revised by: MEG
Incorporated Jenn's comments.
Revision 0.3 2002-02-24 Revised by: MEG
Conforming to LDP standards. Added abstract

In this article, the author describes what computer viruses are, a general method for identifying the presence of a virus, and what virus hoaxes are.

1. Introduction

1.1. Copyright Information

1.2. Overview

Computer viruses are hostile programs written to create havoc and mayhem. They can only do damage if you, or some program acting on your behalf, actually runs the virus program. To be absolutely safe from viruses, never run any programs. Of course, that makes the computer rather pointless.

To be reasonably safe, be very careful what programs you run. Buy or download programs from trusted sources, use an up-to-date virus checking program regularly, and definitely before running any newly installed programs.

Be aware of programs which don’t look like programs! Microsoft Word documents can have mini-programs in them, called ’macros’. These mini-programs can spread in Word documents. To be safe from macro-viruses, never open someone else’s Word document - have the other person export them into another format that doesn’t include macros. RTF, or Rich Text Format, is a good one to use.

Email used to be safe, because you had to actually download and save, then manually run, any programs which came in your email. Microsoft decided to enable Outlook to automatically run programs, ’to make email easier to use’. Unfortunately, they made this the default setting. To keep your email safe, turn this off! There is a link at the bottom of this article telling you how.

Java programs on web pages are usually safe, because Java is designed so that web page applets can’t write to or read from your own hard drive, only the hard drive on the computer that actually hosts the web page. (Minor exception: web pages can ask your web browser to write ’cookies’ onto your hard drive. Because your web browser actually does the work, I can’t imagine anyone figuring out how to write a ’cookie’ virus. I *think* it’s impossible - but I’m learning to say ’nothing’s impossible’.)

2. Virus Checkers

Several companies make programs you can use to search your computer and locate or remove viruses from the computer. They can scan the existing files, or scan files as they are added - most do both.

These programs are only as good as their databases - which are usually up-to-date the day the program is installed (or the package is sealed), but which age. For this reason, most of these companies provide regular updates for free on their web pages. Read the instructions which come with your particular program, and follow them carefully.

Be aware that there is always a lag period during which your computer is vulnerable to any new virus. The period consists of

- The time between when the virus is released, and when it is first noticed
- The time between when it is noticed, and when detection and repair software is created
- The time between when the software is created, and when you download it to your hard drive

You’re only protected after the third stage. But it’s better to be protected then, than not at all.

3. Virus Hoaxes

There's something easier than writing a program to make computers mess themselves up. It's writing a letter to make humans mess computers up.

Virus hoaxes are just that - hoaxes. They're letters which pretend to be a virus alert, or some other sort of computer security alert, and which aren't. They're worded to frighten people and get them to forward the message to 'everyone they know' - or at least to a lot of other people.

This forwarded email can slow down or even stop a mail server, fill peoples' mailboxes, and, of course, frighten them and cause them to lose time and waste time and energy on something which is just a hoax.

You can't really defend yourself against receiving virus hoaxes except by educating everyone you know. But you can avoid sending hoaxes on. In a corporate environment, just forward the virus alert to the IT department. It's their job to know which ones are hoaxes and which are real.

If you're not in a corporate environment, and you feel you must pass on a virus alert, don't just forward the one you received. Write your own.

First, check with a list of virus hoaxes. Links to several of them are at the bottom of this article. If the forwarded email is a hoax, send the URL of the hoax page to the person you forwarded the mail to you, with a gentle note saying 'hey, you were hoaxed'.

If it's not a hoax, your mail should include:

- The URL of a reputable site which contains verified information about the virus - the actual URL of their page for that virus is best. Links to virus information sites are at the end of this article. You can probably find this information at the same place where you checked whether the message was a hoax.
- The date you send the message, and a guess at an expiry date (a 'don't pass this on after date ' date). Make the expiry date no more than a month after the date you send it - if it's dangerous, it'll be all over the papers anyway. And after a month or so, most peoples' virus-check software will have that virus in the database.
- Why you think it's worth passing it on to the people you're sending it to.

Don't write a sensational letter. Just write something calm and helpful. People in this culture have learned to ignore sensationalism anyway.

4. Links

- A beginner's guide to viruses
- Symantec's list of virus hoaxes (http://www.symantec.com/avcenter/hoax.html)

- McAfee’s list of virus hoaxes (http://vil.mcafee.com/hoax.asp)
- F-secure’s anti-virus centre (http://www.f-secure.com/virus-info/)
- Symantec’s anti-virus centre (http://www.symantec.com/avcenter/)
- McAfee’s anti-virus centre (http://www.mcafee.com/anti-virus/default.asp?)
- Securing Microsoft Outlook (http://rr.sans.org/email/sec_outlook.php)