



All About Computer Viruses

by: Kara Glover

Feel Free to reprint this article in newsletters and on websites, with resource box included. If you use this article, please send a brief message to let me know where it appeared: kara333@earthlink.net

Word Count = 1,500

Word Wrapped to 60 characters per line

URL: <http://www.karathecomputertutor.com>

Author photo: <http://www.karathecomputertutor.com>

Date of copyright: November 2004

All About Computer Viruses

by Kara Glover

kara333@earthlink.net

Your computer is as slow as molasses. Your mouse freezes every 15 minutes, and that Microsoft Word program just won't seem to open.

You might have a virus.

Just what exactly is a virus? What kind is in your computer? How did it get there? How is it spreading and wreaking such havoc? And why is it bothering with your computer anyway?

Viruses are pieces of programming code that make copies of themselves, or replicate, inside your computer without asking your explicit written permission to do so. Forget getting your permission down on paper. Viruses don't bother to seek your permission at all! Very invasive.

In comparison, there are pieces of code that might replicate inside your computer, say something your IT guy thinks you need. But the code spreads, perhaps throughout your office network, with your consent (or at least your IT guy's consent). These types of replicating code are called agents, said Jimmy Kuo, a research fellow with McAfee AVERT, a research arm of anti-virus software-maker McAfee Inc.

In this article, though, we're not talking about the good guys, or the agents. We'll be talking about the bad guys, the viruses.

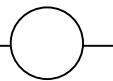
A long, long time ago in computer years, like five, most viruses were comprised of a similar breed. They entered your computer perhaps through an email attachment or a floppy disk (remember those?). Then they attached themselves to one of your files, say your Microsoft Word program.

When you opened your Microsoft Word program, the virus replicated and attached itself to other files. These could be other random files on your hard drive, the files furthest away from your Microsoft Word program, or other files, depending on how the virus writer wanted the virus to behave.

This virus code could contain hundreds or thousands of instructions. When it replicates it inserts those instructions, into the files it infects, said Carey Nachenberg, Chief Architect at Symantec Research Labs, an arm of anti-virus software-maker Symantec. Corp.

Because so many other types of viruses exist now, the kind just described is called a classic virus. Classic viruses still exist but they're not quite as prevalent as they used to be. (Perhaps we could put classic viruses on the shelf with Hemingway and Dickens.)

These days, in the modern era, viruses are known to spread through vulnerabilities in web browsers, files shared over the internet, emails themselves, and computer networks.



As far as web browsers are concerned, Microsoft's Internet Explorer takes most of the heat for spreading viruses because it's used by more people for web surfing than any other browser.

Nevertheless, "Any web browser potentially has vulnerabilities," Nachenberg said.

For instance, let's say you go to a website in IE you have every reason to think is safe, Nachenberg said.

But unfortunately it isn't. It has virus code hidden in its background that IE isn't protecting you from. While you're looking at the site, the virus is downloaded onto your computer, he said. That's one way of catching a nasty virus.

During the past two years, another prevalent way to catch a virus has been through downloads computer users share with one another, mostly on music sharing sites, Kuo said. On Limewire or Kazaa, for instance, teenagers or other music enthusiasts might think they're downloading that latest Justin Timberlake song, when in reality they're downloading a virus straight into their computer. It's easy for a virus writer to put a download with a virus on one of these sites because everyone's sharing with everyone else anyway.

Here's one you might not have thought of. If you use Outlook or Outlook Express to send and receive email, do you have a preview pane below your list of emails that shows the contents of the email you have highlighted? If so, you may be putting yourself at risk.

Some viruses, though a small percentage according to Nachenberg, are inserted straight into emails themselves.

Forget opening the attachment. All you have to do is view the email to potentially get a virus, Kuo added. For instance, have you ever opened or viewed an email that states it's "loading"? Well, once everything is "loaded," a virus in the email might just load onto your computer.

So if I were you, I'd click on View on the toolbar in your Outlook or Outlook Express and close the preview pane. (You have to click on View and then Layout in Outlook Express.)

On a network at work? You could get a virus that way. Worms are viruses that come into your computer via networks, Kuo said. They travel from machine to machine and, unlike, the classic viruses, they attack the machine itself rather than individual files.

Worms sit in your working memory, or RAM, Nachenberg said.

OK, so we've talked about how the viruses get into a computer. How do they cause so much damage once they're there?

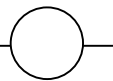
Let's say you've caught a classic virus, one that replicates and attacks various files on your computer. Let's go back to the example of the virus that initially infects your Microsoft Word program.

Well, it might eventually cause that program to crash, Nachenberg said. It also might cause damage to your computer as it looks for new targets to infect.

This process of infecting targets and looking for new ones could eventually use up your computer's ability to function, he said.

Often the destruction a virus causes is pegged to a certain event or date and time, called a trigger. For instance, a virus could be programmed to lay dormant until January 28. When that date rolls around, though, it may be programmed to do something as innocuous but annoying as splash popups on your screen, or something as severe as reformat your computer's hard drive, Nachenberg said.

There are other potential reasons, though, for a virus to cause your computer to be acting slow or in



weird ways. And that leads us to a new segment – the reason virus writers would want to waste their time creating viruses in the first place.

The majority of viruses are still written by teenagers looking for some notoriety, Nachenberg said. But a growing segment of the virus-writing population has other intentions in mind.

For these other intentions, we first need to explain the “backdoor” concept.

The sole purpose of some viruses is to create a vulnerability in your computer. Once it creates this hole of sorts, or backdoor, it signals home to mama or dada virus writer (kind of like in E.T.). Once the virus writer receives the signal, they can use and abuse your computer to their own likings.

Trojans are sometimes used to open backdoors. In fact that is usually their sole purpose, Kuo said.

Trojans are pieces of code you might download onto your computer, say, from a newsgroup. As in the Trojan War they are named after, they are usually disguised as innocuous pieces of code. But Trojans aren't considered viruses because they don't replicate.

Now back to the real viruses. Let's say we have Joe Shmo virus writer. He sends out a virus that ends up infecting a thousand machines. But he doesn't want the feds on his case. So he instructs the viruses on the various machines to send their signals, not of course to his computer, but to a place that can't be traced. Hotmail email happens to be an example of one such place, Kuo said.

OK, so the virus writers now control these computers. What will they use them for?

One use is to send spam. Once that backdoor is open, they bounce spam off of those computers and send it to other machines, Nachenberg said.

That's right. Some spam you have in your email right now may have been originally sent to other innocent computers before it came to yours so that it could remain in disguise. If the authorities could track down the original senders of spam, they could crack down on spam itself. Spam senders don't want that.

Ever heard of phishing emails? Those are the ones that purport to be from your internet service provider or bank. They typically request some information from you, like your credit card number. The problem is, they're NOT from your internet service provider or your bank. They're from evil people after your credit card number! Well, these emails are often sent the same way spam is sent, by sending them via innocent computers.

Of course makers of anti-virus software use a variety of methods to combat the onslaught of viruses. Norton, for instance, uses signature scanning, Nachenberg said.

Signature scanning is similar to the process of looking for DNA fingerprints, he said. Norton examines programming code to find what viruses are made of. It adds those bad instructions it finds to its large database of other bad code. Then it uses this vast database to seek out and match the code in it with similar code in your computer. When it finds such virus code, it lets you know!

©2004 by Kara Glover

About the author:

Kara Glover is a Computer Tutor and Troubleshooter.

You can find her articles and tutorials on topics such as

Microsoft Word®, Excel®, and PowerPoint® on her website:

<http://www.karathecomputertutor.com>



*This book may be given to a third person as a gift but cannot be modified in any manner.
This rule have been established to protect the rights and ownership of the authors and to ensure that their work is upheld as their own*