Annie Sharp
(619)466-6965
muchogusto@andreasharp.com
May 21, 2014

Computer Viruses

What they are, and how to prevent them

A computer virus is a kind of "malware"—software that's designed to do something on your computer that you don't want to have happen.

In almost all cases, software is designed to tell the computer how to interact with you so you can get it to do things you want, like properly start everything up; properly shut everything down; add together numbers you give it and show you the sum; or let you draw a circle and fill it with color.

But malware is designed to make your computer do things you do not want, and usually without your knowledge, like monitor keystrokes when you type passwords; delete, steal, or alter your data; or turn on your webcam. When you discover a malware infection, it's usually because, and after, damage has been done.

Since nobody wants malware on their systems, its creators find ways to "hack" in. Common hacker strategies include sending malware as an email attachment that's designed to work when it's opened, and disguising malware as something legitimate that people would willingly download.

Different kinds of malware have different names. Some examples:

Malware that uses the attacked computer's legitimate software to function and spread is called a virus. A Trojan horse is harmful software that's snuck into your system disguised as something harmless, like a game. Malware that finds security weaknesses on networks to spread itself from one computer to another is called a worm. Spyware sends information from the attacked computer back to the hacker.

Malware has done billions of dollars' worth of damage around the world. Thousands of malware threats circulate the internet all the time. If you use the internet, it's impossible to keep malware from contacting your computer and trying to get in. Distributing malware is against the law, of course, and criminals who do it are regularly arrested, prosecuted, and punished. But the problem is huge nevertheless, and not likely to be solved soon.

How to protect yourself from viruses and other malware

Annie Sharp
(619)466-6965
muchogusto@andreasharp.com
May 21, 2014

To protect yourself:

- Always run anti-virus (AV) software. It's essential. More about this below.
- Routinely open your AV tool and check for messages, alerts, and maintenance tasks such as scanning for threats. See Figure 1 on page 2.
- Be sure to use up-to-date operating systems and browsers. Old ones are less secure.
- Stay away from questionable web sites.
- Never download anything you're not absolutely sure is safe.
- Never open email attachments unless you're absolutely sure they're safe.
- Never install software you're not absolutely sure is safe.
- Keep your data backed up on an external hard drive.
- Disconnect cameras, or cover up camera lenses, when you're not using them.
- Use passwords that are hard to guess, and change them every few months.

Figure 1. Example of an AV status window. Remember to open your AV tool and check for tasks and alerts.

Anti-virus software is essential.

You can, and should, install AV software. It detects and prevents most attacks. Without it, you WILL undoubtedly be attacked and infected at some point.

Annie Sharp
(619)466-6965
muchogusto@andreasharp.com
May 21, 2014

Many internet service providers, like Frontier, Cox, and Comcast, offer AV software to their customers for free. Many companies that sell AV software offer a free version, for minimum protection, along with more secure tools that you can use for an annual fee. You can buy it from a store that sells boxed software products, and install it before your computer is ever connected to a network, or download it from the web site of the company that makes it.

Once installed, it will try to check all data before it goes into your computer to see if it's harmless or malware. AV systems maintain records of almost all circulated malware, and constantly update these records so they can identify malware if it reaches one of their customer's computers. Most of the time, they catch and stop it.

When it detects a possible threat, AV software displays a graphic on the user's monitor to alert them, and let them get rid of it. See the example shown in Figure 2 on page 3.

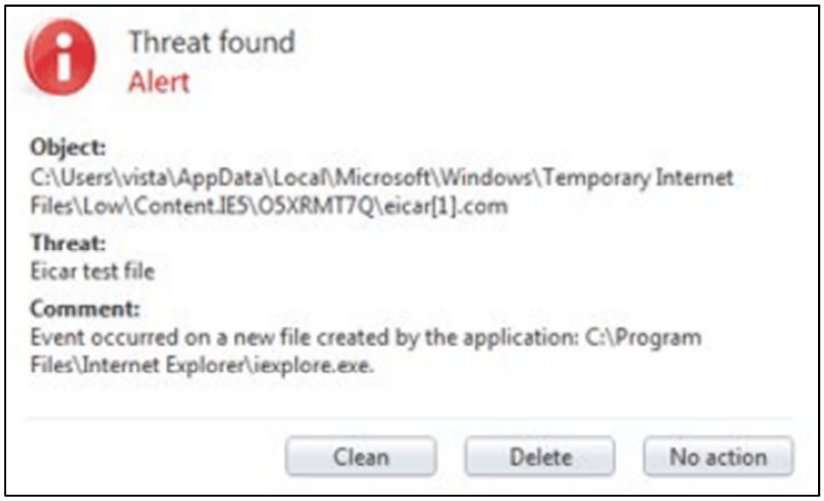

Figure 2. Example of a virus alert.

When it can't tell if something is a threat, AV software gives you the option to allow or block the process that contains the threat. If you're not absolutely sure the possible threat is actually safe, block.