How Did I Get My Viruses

Watch what you download!!!

Many freeware programs, and P2P programs like Limewire, Facebook Games, Frostwire, Bearshare and others are amongst the most notorious, come with an enormous amount of bundled spyware that will eat system resources, slow down your system, clash with other installed software, or just plain crash your browser or even Windows itself.

Strange as it may sound, the computer virus is something of an information age marvel. On the other hand, viruses show is how vulnerable we are. A properly engineered virus can have devastating effect, disrupting productivity and doing billions of dollars in damage. On the other hand, they show us how sophisticated and interconnected human beings have become.

What Is A Virus

- **Viruses** - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.
- **E-mail viruses** - An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double-click -- they launch when you view the infected message in the preview pane of your e-mail software [source: Johnson].
- **Trojan horses** - A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage

when you run it (it may erase your <u>hard disk</u>). Trojan horses have no way to replicate automatically.

- **Worms** - A worm is a small piece of software that uses <u>computer networks</u> and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.
- **Adware program-** is any program that randomly displays pop-up ads on internet pages, they also may monitor internet activity and send it to a third party website

How Do I Prevent Getting Another Virus

Computer viruses are nasty and can wreak havoc on your computer. The following steps may not completely protect you from viruses, but they can significantly reduce your chances of being harmed by them:

1) Install anti-virus software on your computer.

2) Update your anti-virus software regularly. At least once a week.

3) Avoid downloading any unnecessary applications.

Some questionable Web sites will automatically offer to install various programs or plug-ins, hoping you will click "Yes" just to close the screen. Be aware of this practice and only install applications you consciously decide to.

4) Avoid opening unknown email attachments.

Many recent viruses and worms come as email attachments in your mailbox. Be sure to know who is sending you an attachment, and even then, be wary if the attachment is unexpected and has no accompanying text that makes sense. Never open an attachment from an unknown!

Rule of Thumb: Prepare for the worst.

For more information contact us at:
Simplified Technology Solutions, LLC
313 3rd Ave NE Austin MN 55912
507.437.TECH (8324)
www.simplifiedtechsolutions.com

Simplified
Technology
Solutions LLC.

Why Do People Make Viruses

1. To Take Control of a Computer and Use It for Specific Tasks

This is the most common type of virus, which is better classified as a Trojan. These types of viruses are usually downloaded unknowingly by the computer user thinking that the file is something else, such as a file sent from a instant messenger friend or email attachment.

Once the host computer has been infected (known as a zombie computer), the Trojan joins a private chat channel and awaits orders from its "Zombie Master". This Zombie Master who is often the virus creator, will gather thousands of infected machines called a Botnet and use them to mount attacks on web servers. The Zombie Master can command each of these infected computers will send a tiny bit of information to a web server – because there are potentially thousands of computers doing this at once, it often overloads the server.

The Zombie Master may want to do this to another website because it is a rival website, a figurehead website (such as whitehouse.gov) or it may be part of an extortion plan. "Send me $5000 or your Toy selling website will be offline over the Christmas holidays".

The Zombie Master can also use these infected computers to send spam while the zombie master remains anonymous and the blame goes to the infected computers.

2. To Generate Money

These types of infections often masquerade as free spyware or virus removal tools (known as Rogueware). Once ran, these fake applications will "scan" your computer and say it found has some viruses (even if there aren't any) and in order to remove them, you must pay for the full version of the application. A good example of such a infection is called Myzor.fk which is a type of Trojan.

For more information contact us at:
Simplified Technology Solutions, LLC
313 3rd Ave NE Austin MN 55912
507.437.TECH (8324)
www.simplifiedtechsolutions.com

Simplified
Technology
Solutions LLC.

3. Steal Sensitive Information

These types of viruses can sniff the traffic going in or out of a computer for interesting information such as passwords or credit card numbers and send it back to the virus creator. These types of viruses often use key logging as a method of stealing information where it maintains a record of everything that is typed into the computer such as emails, passwords, home banking data, instant messenger, etc.. The above mentioned method also allows an attacker to gather an incredible amount of data about a person which can be used for identity theft purposes.

4. To Prove a Point, To Prove it Can Be Done, To Prove Ones Skill or For Revenge Purposes

A perfect example of this type of virus was the famous MS.Blaster virus (aka Lovesan) which infected hundreds of thousands of computers in August 2003.

This virus would cause the system to restart after 60 seconds and had two hidden messages written in its code: One was *"I just want to say LOVE YOU SAN!!"* which is why the virus is sometimes called Lovesan, and the other message was "Bill Gates why do you make this possible? Stop making money and fix your software!!" It is believed that purpose of this virus was to prove how easily exploitable a Windows system is.

5. To Cripple a Computer or Network

Few viruses now days are intended to disable a computer because it stops viruses ability to spread to other computers. Computer crippling viruses still exist, but nowhere near as common as the viruses mentioned above. The worst type of computer crippling viruses were back in the days of the 486 computers where the virus would overwrite the Master Boot Record (MBR) of the computer which would often prevent the computer from starting up at all.

Unlike computer crippling viruses, network crippling viruses are all too common now days. Most viruses that are designed to launch a Denial of Service attack will cause a significant load on a computer network, often bringing it down completely.

For more information contact us at:
Simplified Technology Solutions, LLC
313 3rd Ave NE Austin MN 55912
507.437.TECH (8324)
www.simplifiedtechsolutions.com

Simplified
Technology
Solutions LLC.