



What are Worms and Viruses, and How Do They Work?

Most people don't have an IT professional looking over their home computers. Yet in recent years, the quantity and ferocity of Internet worms and viruses has increase dramatically. As more and more computers get connected to the Internet, it isn't surprising that even careful, skeptical users can find their computer loaded with Adware, spyware, viruses, e-mail worms, Trojan horse programs and more. Many home PCs, often without the knowledge of the computer owner, have one or more of the above.

This series of articles attempts to explain some simple steps you can take, and maybe more importantly, some step you should avoid taking, in order to keep your computer running smoothly and your data and privacy safe. This especially important for those who connect to a corporate network from home – your infected computer could put the whole company at risk. Even if you never connect to work, the stakes may be higher than you think.

Installing antivirus software is one of the things that you can do to keep your home network safe. Combined with a firewall, paying attention to the software that you install on your machine and keeping windows updated with the latest service packs and hot fixes, you will be well on your way to a smoothly functioning home PC.

What is malware?

First, some definitions of the common types of bad stuff out there (not an exhaustive list): All these kinds of bad software as a group are sometimes called malware. Adware refers to programs that, while they claim to be useful software, are paid for by making you look at pop-up advertising. And since there's almost always some other legitimate freeware or shareware program (these are the good guys) that does what you want, without the ads, it's hard to imagine anyone putting up with adware.

Many websites use pop-up ads too, so you might not even realize that you're getting ads from software installed on your computer. A major problem with adware is it is often very poorly written software that slows your computer and causes lockups and crashes. There are security concerns as well.

A cousin of adware is spyware, which might also perform a useful purpose to justify its existence, only you pay for it by letting the software spy on you and report back to its home. Mostly your browsing habits, what files you download, that sort of thing, but some spyware has been caught sending sensitive personal information such as name, address, password and credit card number. Like adware, these are often such poorly written programs that they slow down, lock up or crash your computer.

Viruses and worms make no pretense of being useful. Often spread via e-mail or malicious websites, worms try to take over your computer and spread themselves to any computer they can find. For example, an e-mail worm sends itself to everyone whose e-mail address they find on your system.

Trojan Horse programs ("Trojans", "back doors") are evil programs that trick you into installing them or exploit a Windows vulnerability, that then allow hackers to take control of your PC. Again, you might not even know your PC has been compromised, as the hacker might keep a low profile so you won't take the thing in to be fixed.

Zombie is a name sometimes given to computers that are under the control of a virus or Trojan. Crackers typical use these to store illicit files (stolen software, movies, music, etc) that that might get the computer owner thrown in jail if they were caught with these files on their computer. They also like to launch their attacks on other systems using your PC as the launching pad, in case the victim traces the attack back to the source.



Keystroke loggers

Keystroke loggers record the data typed into the computer's keyboard. They are simple programs and easy to install. They have legitimate uses by software testers, security professionals, law enforcement, etc. but criminals find them very useful to capture personal information of unsuspecting users like social security numbers, usernames and passwords.

Phishing

"Fishing" for users' accounts has been around for many years, but recent efforts to trick users to give up personal information like usernames, passwords, etc. have brought Phishing into the mainstream. For more information on Phishing and what you can do to fight it, please visit <http://www.antiphishing.org/>

Rootkits

A root kit is software that is designed to control a computer at a very basic level. Typically the purpose is to control the computer and hide processes and files from the operating system. Not all rootkits are distributed by crackers; Sony recently included a variation of a rootkit in a recent CD music release with the intent of controlling the copying of music.

Worms and viruses are malicious computer programs that spread to lots of computers because users are easy to fool and because programmers make lots of mistakes that lead to security holes.

Viruses

Viruses today usually spread by being attached to an email message that fools the recipient into opening the attachment. The message might say "I love you," or "Great pictures of Anna Kornikova (in provocative poses)" When the user opens the attachment (by double clicking on it, for example), thinking it is a love note or a picture of the tennis player, the infected computer runs the malicious program contained in the attachment, often damaging data or programs on the computer. It usually opens a back door on the computer so that an outsider can control the infected computer. If the virus is intended to spread widely, it forces the infected computer to send the same message and attachment (or a variant) to everyone on the infected computer's email list or to all the email addresses it finds in files on the infected computer.

Worms

The worm scans thousands of IP addresses looking for computers that are running a particular version of a program.

The worm scans thousands of IP addresses looking for computers that are running a particular version of a program. For example, Code Red searched for programs running Microsoft's Internet Information Server (IIS). When it finds one, it tries to infect the machine using code that exploits a known bug that someone who wrote IIS left in the code. The owner of the targeted computer could have protected his machine by installing a security patch, but the process of finding and installing patches is difficult, so worms generally find lots of vulnerable machines (Code Red found 300,000). When the worm infects a victim, it often installs a back door, it sometimes damages files or programs, it sometimes steals files and sends them to other systems, and it nearly always installs its own code on the victim and makes the victim scan the Internet looking for and infecting more victims.

Sometimes the damage that a worm does is indirect. When the Slammer worm spread, it caused the 911 emergency response systems in Seattle to stop operating and the ATM machines of Bank of America and a dozen other banks to stop operating.



The 911 and ATM systems shared networks with infected computers. They didn't get infected, but their connection to the network was flooded out by all the traffic caused by infected systems scanning the Internet looking for victims. Cleaning up after worms is very challenging. Many people find it necessary to wipe all programs and files off their computers and start fresh (hoping they have up to date, uninfected backups).

Antivirus – Don't Just Assume You're Covered

Even if you keep your operating system patched and up to date, we still can be infected if we tell a virus to run. Can you accept never opening another e-mail attachment? I didn't think so. Well then you're going to have to get some good antivirus (AV) software, and learn how to make sure it stays up to date.

This is essential. No one should be allowed to connect a computer to the Internet without functioning, up to date AV. Without it, you're not only a threat to your own data and privacy, but you're likely to be spewing out the malware to everyone else, often so much that it slows the entire Internet and hurts even the people with perfect AV protection.

There is no "set and forget" AV that'll never need your attention after you install it – you have to check in on it, ideally about once a week, to make sure it is getting the latest virus definitions or "signatures". Frequently when I check home computers, I find the AV, if there is any, is a year or so out of date. This is as bad as no AV - or maybe worse, since it's giving you a false sense of security.

If you can't figure out how to update your AV, and how to easily check to see if it's up to date, don't feel bad, much of it is not well written from a user-friendliness point of view. Don't feel bad, but do find someone (maybe your friendly network manager, neighbor or a computer consultant) who can set it up correctly and show you how to keep it updating.

Many antivirus products set the default update frequency to once a week – change that to every day, or twice a day if you can. Updates don't come out every day, but your antivirus should check to see if there's anything new at least once a day. With modern worms spreading so fast, you don't want to be even a week out of date. There are instances of people being hit by viruses within hours of it being released into the wild! If your computer is turned off or not connected to the Internet at the scheduled time, it won't get updated, so run the updater manually if you see you're more than a few days behind.

Once you have up-to-date antivirus, you can open any e-mail attachment that comes along, right? NO, you still need to be suspicious and careful – someone will eventually send you a virus so new that your antivirus hasn't heard about it yet. Unfortunately there's no substitute for calling the sender and asking him/her: Did you really mean to send me that attachment? And is your antivirus up to date?

Installing antivirus software is one thing that you can do to keep your home network safe. Combined with a firewall, paying attention to the software that you install on your machine and keeping windows updated with the latest service packs and hot fixes, you will be well on your way to a smoothly functioning home PC.