Tech Notes (Tech Talk)

Brought to you by South Central Communications - Home of the Tech Medics

Viruses & Malicious Software!

What are they?

Many people use the terms *Virus* and *Malware* (malicious software) interchangeably. However, viruses are considered a type of malware, whereas malware is an all-encompassing term. Malicious software is any kind of hostile, invasive or annoying software or code. Malicious Software includes computer viruses, worms, Trojan horses, rootkits, backdoors, spyware, adware, keyloggers, botnets and scareware or ransomware.

So what's the difference between them?

- Virus – A program embedded in to an executable file (for instance an email or music file) that, when ran, causes the infection to spread to other executable files. They may also contain a "payload" to will perform other malicious actions.
- Worm – A program that actively spreads itself throughout your computer and network automatically. You do not need to open a program to activate it, it is automated. Just like a virus, it may carry other malicious payloads.
- Trojan Horses – A Trojan is malicious software that is disguised as something else, for instance a downloaded game from the internet or a toolbar. Or it could simply be bundled in with a legitimate program.
- Rootkits – Programs that embed and disguise themselves in your core system files. Rootkits are notoriously difficult to remove because they tend to attach themselves to files that are necessary for your computer to function.
- Backdoors – These are programs that create a way for "hackers" or other malware to infect your computer easily by bypassing any existing security measures.
- Spyware – This is one of the most common types of malware and can take on numerous forms. It can redirect your web browser, keep track of the web pages you visit to sell to marketing firms or even collect your personal usernames, passwords, bank data and account numbers.
- Adware – Adware typically takes on the form of pop-ups. This is more of a nuisance software than anything; however the presence of adware can often be a sign of a more serious problem.
- Keyloggers – These are programs that log the keystrokes of your keyboard. Doing this allows the program to know what you are typing which can reveal encrypted passwords.
- Botnets – A botnet basically turns your computer in to a "zombie computer". Your system will work in conjunction with other computers on the botnet and will be used to distribute malicious software.
- Ransomware/Scareware – This is the type of program that many find the most annoying and convincing. Ransomware is a program that takes your computer for "ransom" and demands that you pay a certain fee to regain the use of your system. The most common variety home users see is a fake antivirus. You will see a pop-up on your screen that looks like a legitimate antivirus program stating you have hundreds of infected files and you can pay $X amount to remove them. If you do pay the amount, not only will it NOT fix your problem, but you will have been charged that initial fee, plus your credit card information will be sold and used.

Why are they made?

Malware can be made for a variety of reasons. Some are made just for fun to annoy you. For instance, I once received a virus that changed all of my icons to Hello Kitty faces, but it didn't do anything else. But the most common reason is money! The use of malware allows marketing companies to gather targeted information for advertising. Other companies steal your money directly by acquiring your bank and credit card information.

How do you get them?

Though most of users believe they are being safe on the internet, 9 times out of 10 it is the user that installed the virus on their computer. A lot of malware can be installed by accident by installing a legitimate program, but a malicious application came bundled in. Or perhaps you installed software from a not-so-reputable source. Many viruses come from installing "fun" products on the web such as toolbars, screensavers, games and torrents that you didn't scan for

viruses before installing. It is important to ONLY download programs for trusted sources. Also, only open email from people you know and only if it makes sense for them to be sending you that email. Many infections come from hijacked email accounts that send out emails with infected files attached or links that lead to infected sites or programs.
It is also possible to be infected by simply visiting a website. There are security vulnerabilities in many of the programs you use daily; that is why it is important to keep your media applications, such as Flash Player and Java, up to date.
It is also important to have a good, up-to-date anti-virus program installed on your computer and any other computers on your network.

Want more information or have questions? Contact TechMedics@socen.com or call (888) 826-4211