Safeguarding Your Computer System

The Differences Between Viruses, Trojan Horses, and Worms

Viruses, trojan horses and worms are all malware that can damage your computer. A computer virus is something that enters a computer with the intention and ability to do things such as harming the system software or corrupting and destroying data. It can enter a computer and self reproduce. Named after the war-winning strategy used by the Spartans in the Trojan War, a Trojan Horse is a program that appears harmless but is actually malicious. Trojan horses are often used for fraud and stealing important data. Worms are malicious that are downloaded without the users knowledge and damage the computer unbenounced to the user. They can make changes to and delete files. Worms can recreate themselves to deplete system resources like bandwidth and hard drive space.

Viruses are known to be self reproductive. The main difference between trojan horses and viruses is that trojan horses cannot reproduce themselves. The main difference between worms and viruses is that worms do not need a host file or executables to spread from system to system. Worms, intern, can “slither” around from computer to computer, much like a real life worm. Also worms do not need any human action, unlike trojan horses and viruses. Viruses can erase and corrupt information, trojan horses can steal and change data, worms can consume a systems resources and halt it completely. These are the main differences between viruses, trojan horses and worms.

The Origins and Evolution of Malicious Code

Computer malware has been around for as long as computers themselves. In 1949 John von Neumann wrote a paper titled “Theory and Organization of Complicated Automata” which explains how a computer program could reproduce itself. A few years later, a game called “Core Wars” was developed by employees at Bell Labs. The game consisted of programmers that would release ‘organisms’ that would compete for control of the computer. Later, Bob Thomas at BBN Technologies created “Creeper Worm”, which is a self replicating program. This is widely regarded as the first computer virus.

Fred Cohen later coined the term “virus” in his 1986 Ph.D thesis. In a single sentence, he defined a virus as: “A program that can infect other programs by modifying them to include a, possibly evolved, version of itself.”.

Early malware used to spread almost solely offline. It would spread through floppy disks. With the progress of the internet, malware quickly adapted to take advantage of it. In the early 2000’s malware grew in size and intelligence. Malware then became a huge hotspot for organized crime and has the global economy billions of dollars. Nowadays many malware concentrate on attacking cryptocurrency.

Procedures to Safeguard Data and Programs

Malware can spread in many different ways. One common way of spreading malware is through phishing attacks. If you are aware of the consequences of clicking suspicious links and opening suspicious emails, you will not open them. Discarding suspicious email and not visiting unknown websites along with not clicking random links will tremendously lower your chances of getting a virus. Another way to protect against viruses and other malware is to have a functioning antivirus software. Some effective antivirus software are Norton and McAfee. Incase you do end up getting some sort of malware, make sure to have all of your important data backed up, either locally or on the cloud. You can easily replace the corrupted files with the backups either on the cloud or a local drive. Some common cloud servers are Dropbox and Google Drive. You can also store your information on USB and other drives. Be sure to check up on all these procedures to make sure everything is functioning properly.

The method I have prepared is very simple and will safeguard all of my data and programs very effective. First, I have a created a spam folder in my email inbox to automatically discard any malicious emails. I am also educated enough to know not to click suspicious links and visit suspicious websites. I have also downloaded McAfee onto my computer to further protect against the spread of malware. I also back up all of my personal and important files and programs on the cloud. For all my documents and files I use a melange between Google Drive and Dropbox. All of my programs are backed up on GitHub. Using the antivirus and backing up my data, I have a very nice system of protecting my data.

References

“A Brief History of Malware-Its Evolution and Impact.” Lastline, 14 May 2018, [www.lastline.com/blog/history-of-malware-its-evolution-and-impact/](http://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/).

Brunelli, Mark. “Five Simple Ways to Protect Your Data from Viruses.” Carbonite, [www.carbonite.com/blog/article/2015/09/five-simple-ways-to-protect-your-data-from-viruse](http://www.carbonite.com/blog/article/2015/09/five-simple-ways-to-protect-your-data-from-viruse).

Colby, Clifford. “The Best Antivirus of 2019 to Protect Windows 10.” CNET, CNET, 12 July 2019, [www.cnet.com/news/best-antivirus-protection-in-2019-for-windows-10/](http://www.cnet.com/news/best-antivirus-protection-in-2019-for-windows-10/).

“Difference Between Virus and Worms(with Comparison Chart).” Tech Differences, 10 June 2019, techdifferences.com/difference-between-virus-and-worms.html.

“Home.” Article Details, support.symantec.com/us/en/article.tech98539.html.

“How to Protect Your Computer from Viruses and Trojans -.” All About Cookies, [www.allaboutcookies.org/security/](http://www.allaboutcookies.org/security/).

“What Is A Computer Virus?” NORTONâ¢ - Antivirus Software and Spyware Removal, ca.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

“What Is a Computer Worm and How Does It Work?” What Is a Computer Worm and How Does It Work?, us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html.

“What Is Trojan Horse (Computing)? - Definition from WhatIs.com.” SearchSecurity, searchsecurity.techtarget.com/definition/Trojan-horse.