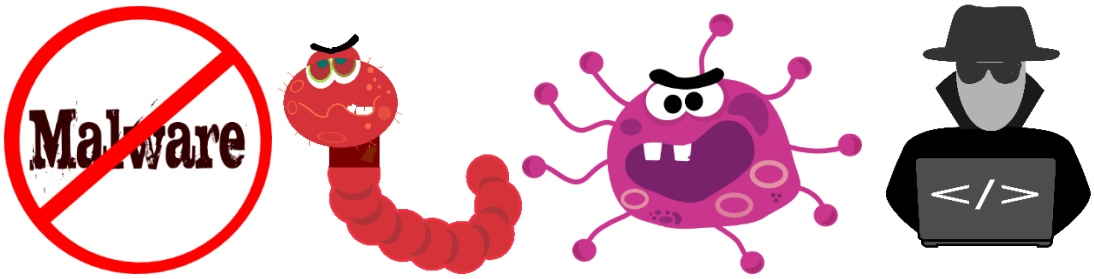

THREE DIFFERENT TYPES OF MALWARE: VIRUSES, WORMS AND SPYWARE

Willie Conway

Park University

MALWARE IN TODAYS WORLD

You may have heard of the term malware before, but do you really know what it is? Malware is a short for malicious software. The term is used to describe a lot of threats on the internet landscape, from computer viruses, BOTS, worms, spyware, ransomware and trojan horses. These are the type of malicious software and malicious threats that bad guys (hackers) use to interfere with your personal identity, personal life, and even worse, your financial living. They may be trying to steal resources from your computer, cell phone, place of bussiness or either trying to steal from you.

Malware attacks can range from planned data breaches on a company or slightly annoying and harmful damage to your personal computer. Although, there is no such thing as 100 % security, there are software programs or applications that are built to help mitigate malware and keep your computer in tip top shape, by scanning every file on your PC. Even though Windows PCs come with Windows defender, it still isn't enough to conquer against malware attacks. In this research paper were going to learn about the three different types of malware that are common among personal computers and bussiness workstations. We will cover how we get them, how we can avoid them from ever happening, and what fundamentals and software is best help prevent or get rid of these malicious threats, if we have them on our computer.

COMPUTER VIRUSES

A hacker's main motive is to get their malicious software on your machine. A hacker can be anybody who uses their knowledge of computer coding, to bypass security measures on a computer device or network. Which brings me to our first topic, computer viruses. The first malicious threat that many users may be aware of is the typical computer virus. According to the

Kaspersky community, “computer viruses earned their name due to their ability to "infect" multiple files on a computer” (Kaspersky, 2019). A computer virus can spread to other machines when infected files are sent via email. This form of malware is most common in businesses then on PCs, although it is very still possible to happen on your personal computer. Viruses are mostly engineered by individuals that have worked in the computer science industry.

The most common way to tell if your computer has a virus is by checking the overall performance of your computer and watching for if it responds to proper instruction. Computer viruses are most common with phishing attacks. Symptoms to look for are unusual error messages and crashes, severe pop-up messages/windows, slow start up and performance, suspicious hard drive activity, security attacks, missing files, email hijacked and high network activity. If you encounter any of these issues with computers at a bussiness work station or on your personal computer, the best option to get rid of this cause would be to install anti-virus software and run scans to search through files to check and eliminate any bad files that may be causing the issue. However, before you do so, make sure the computer is in safe mode. After the process is done set your computer backup point immediately. This will ensure that if you simultaneously get another virus you’ll be able to reboot your computer to the present backup.

COMPUTER WORMS

The second formal type of malware are computer worms. According to the Norton community, “a computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage” (Norton, 2019). A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms are capable of spreading from

computer to computer, but unlike a virus, they have the capability to travel without any human action. The most devasting issue with a worm is that it has the capability to replicate itself on your system. For instance, rather than your computer sending out a single worm, it could send out hundreds to thousands or more copies to create a devastating effect. A great example would be a worm sending a copy of itself out to everyone in your email address book then the receiver address book, this gives it the ability to spread widely. To prevent this issue is to download a virus removal tool, such as Microsoft Malicious Software Removal Tool, create a restore point, use Malwarebytes (anti-malware software) or other anti-virus software to scan and delete files.

COMPUTER SPYWARE

The third and final formal malware is computer spyware. According to the Kaspersky community, "spyware does just what it says: It spies on what you're doing at your computer. It collects data such as keystrokes, browsing habits and even login information, which is then sent to third parties, typically cybercriminals" (Kaspersky, 2019). Spyware is software that is designed to gather data from your device, it can communicate your personal information and confidential information to a user that has malicious intent. As long as your using a device that's connected to the internet, you are in danger of spyware infestation. This issue is not only common among PCs, but also mobile devices like your cell phone. We keep much information stored on our cell phones, if not practically everything.

With social media being such a uprising and how fast mobile technology is advancing, spyware happens to be a playground for hackers. Hackers can get spyware onto your device in many ways. One way is by penetrating your device in the form of a Trojan, which is a type of malware that's described as legitimate software. Hackers may use the trojan in a sneaky process called

social engineering. This is the process of tricking the users to load and execute the virus. To get rid of spyware, enter your computer in safe mode, download and run Malwarebytes, and create a back up restore point for PC. Other ways would be to be cautious of web surfing material, lookout for po-ups, download anti-spyware software, and keep current with operating system updates. It seems that computer security plays many roles in the world of cyber security, and personal life. Protection should always be accounted for, as we all must be wise about what we view and download off the World Wide Web (www). It's important to always stay vigilant and look to prevent or you'll be looking to play the game of identity theft with hacker that just won't let up.

References

Kaspersky. (2019). Computer Viruses and Malware Facts & FAQs. Retrieved March 2, 2019 from https://usa.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

Norton. (2019). What is a computer worm and how does it work? Retrieved March 2, 2019 from https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html