Malware and Viruses: What They Are and What They're Capable Of

Every day on the news you hear about a new company, city, or person hit with new devastating ransomware or malware that locks everyone in their organization out their computers and forces them to pay a sum of money in order to get their files back. These attacks are why it is incredibly important to take email and password security seriously. Whether it is your personal or work account, if you were to get hit with malware, a virus, and/or ransomware, it can greatly affect your ability to complete even the simplest day to day tasks.

But what exactly is a computer virus or malware? The terms "virus" and "malware" are often used interchangeably. However, they are technically different, so the question of malware vs. viruses is an important one.

Malware is a catch-all term for any type of malicious software, regardless of how it works, its intent, or how it's distributed. A virus is a specific type of malware that self-replicates by inserting its code into other programs. Computer viruses have been prominent since almost the beginning of the commercial internet: The first was created in 1982 for Apple II, and other versions quickly followed.

Viruses spread by attaching themselves to legitimate files and programs within your device, and are distributed through infected websites, flash drives, and emails. A victim activates a virus by opening the infected application or file. Once activated, a virus may have the ability to delete or encrypt files, modify applications, or disable system functions.

Types of Viruses

There are many different types of viruses. These are the three most common examples:

File Infector can burrow into executable files and spread through a network. A file infector can also overwrite a computer's operating system or even reformat its drive.

Macro virus takes advantage of programs that support macros. Macro viruses usually arrive as Word or Excel documents attached to a spam email, or as a zipped attachment. Fake file names tempt the recipients to open the files, activating the viruses. An old but still prominent type of malware, macro viruses, remain popular with hackers.

Polymorphic viruses modify their own code. The virus replicates and encrypts itself, changing its code just enough to evade detection by antivirus programs.

Types of Malware

Besides viruses, other types of malware can infect not only desktops, laptops, and servers, but also smartphones. Malware categories include the following:

Worms are a standalone program that can self-replicate and spread over a network. Unlike a virus, a worm spreads by exploiting the vulnerability of the infected system or through email as an attachment masquerading as a legitimate file.

A graduate student created the first worm (the Morris worm) in 1988 as an intellectual exercise. Unfortunately, it replicated itself quickly and soon spread across the internet.

Ransomware demands that users pay a ransom—usually in bitcoin or other cryptocurrency—to regain access to their computer.

The most recent category of malware is ransomware, which garnered headlines in 2016 and 2017 when ransomware infections encrypted the computer systems of major organizations and thousands of individual users around the globe.

Scareware attempts to frighten the victim into buying unnecessary software or providing their financial data. Many desktop users have encountered scareware.

Scareware uses pop ups on a user's desktop with flashing images or loud alarms, announcing the computer has been infected. Usually urging the victim to quickly enter their credit card data and download a fake antivirus program.

Adware and spyware pushes unwanted advertisements at users and spyware secretly collects information about the user.

Spyware may record websites the user visits, information about their computer system and vulnerabilities for a future attack, or even keystrokes. Spyware that records keystrokes is called a keylogger. Keyloggers steal credit card numbers, passwords, account numbers, and other sensitive data simply by logging what the user types.

Fileless malware, unlike traditional malware, fileless malware does not download code onto a computer, so there is no malware signature for a virus scanner to detect. Instead, fileless malware operates in the computer's memory and may evade detection by hiding in a trusted utility, productivity tool, or security application.

Malware encompasses all types of malicious software, including viruses, and may have a variety of goals. A few of the common objectives of malware are:

> Identity Theft: Trick a victim into providing personal data for identity theft

> Financial Data Theft: Steal consumer credit card data or other financial data

> Denial-of-Service: Assume control of multiple computers to launch denial-of-service attacks against other networks

> Cryptocurrency Mining: Infect computers and use them to mine bitcoin or other cryptocurrencies

IT Extra: You can learn more about the costs of a rogue ransomware/malware attack by watching this clip from CBS This Morning discussing NotPetya, the most expensive and devastating cyber-attack in history.

Article written by IT Support Specialist, Kyle Hauswirth