7 Most Common Types of Malware

In today's digital age, the threat of malware attacks will only continue to increase. This increase can make it challenging for businesses and consumers alike to protect themselves regularly from these security threats. While malware is a term that is commonly used to describe a variety of malicious software programs that can infiltrate and damage computer systems, there are numerous types out there that can do more damage than just to systems.

Other types of malware can gain unauthorized access to systems, steal sensitive user and consumer data, and even hold everything at a ransom until payment demands are met. Malware can come in many different types and varieties, most of it with the goal of stealing from consumers and businesses. Continue reading to learn more about the seven most common types of malware, which is the most dangerous type and how you can prevent them.

What Are the Different Types of Malware?

While malware has been around in some form since computers became widely available, the most common types have evolved. Nowadays, there are many different types of malware that can impact consumers and businesses alike. From viruses to ransomware, most malware is designed to exploit systems for the benefit of cybercriminals. Understanding the types of malware is key to protecting your devices and systems from possible cyberattacks.

1. Viruses

Viruses are one of the most common types of malware to date. It's a program that infects a computer, crippling the device in order to self-replicate onto the system. Since viruses are self-replicating, once installed and run, they can spread from one device to another on the same network automatically

without human intervention. Although they are commonly associated with computer worms, viruses often need user interaction in order to deploy successfully.

Viruses often circulate through malicious email attachments, corrupted downloads or compromised through software vulnerabilities. Many malicious viruses are designed to steal personal information, delete files, or even take over your computer system entirely. One of the most notable computer viruses known in history was the ILOVEYOU virus. This virus was sent through phishing emails and once downloaded was duplicated and then deployed onto operating systems, taking down comprehensive company networks.

2. Trojan

A Trojan is a form of malware that is downloaded from the internet or installed by other malicious programs. It can be disguised as a legitimate application, such as an antivirus program, in order to trick users into downloading it, and thus infiltrating your device, network or system. Trojans are customarily used to steal information which can include credit card numbers, other sensitive consumer data or install other malware onto a computer.

An example of a notable Trojan malware attack is the Zeus Trojan that was discovered in 2007. This type of malware attack not only stole classified data, but also duplicated the software by deploying botnets to continue to infect more devices and systems. Trojans may also be included within software packages that claim to be genuine programs but contain hidden spyware and other malicious software programs designed to collect classified data. Many types of trojans can be spread through malicious email attachments and other social engineering methods.

3. Botnet

Botnets are groups of devices infected with malware to perform a specific task. These types of malware bots can be used for malicious reasons, including as sending spam emails, phishing, smishing, launching DDoS attacks or distributing malware. One of the most notable botnet attacks was the Mirai botnet attack in 2016 which provided hackers the ability to overtake many internet of things (IoT) devices. Many botnet kinds of malware are often generated by infecting numerous computers with Trojans or other malware types. Once deployed, it can be difficult to identify and terminate since it involves several infected devices instead of only one computer.

4. Rootkit

Rootkits are a kind of malware created to hide its presence within a computer system. It can be employed to gain unauthorized access to a system or network. Many rootkits are designed to create backdoor access into systems and networks in order to steal data and commit other illicit activities. For example, a rootkit malware called CosmicStrand was discovered in 2022 and said to gain unauthorized access to computer systems while also making changes to the target's CSMCORE DXE driver, which affects both boot services and the runtime environment.

The majority of rootkits are often installed through a Trojan or other malware type that aims to infect a device or system in order to make changes to system drivers to steal data from victims. These types of malware can be difficult to detect and remove given there is not a direct method to detect through an operating system (OS) due to backdoor access.

5. Spyware

Spyware is a type of malware that spies on a user's computer activity. This type of malware can monitor keystrokes, capture screenshots, web browsing activity, and also record audio and/or video. Spyware is commonly installed on the victim's computer without their knowledge. It can steal sensitive information, such as user passwords, credit card numbers and other data.

One example of spyware is a keylogger. Keyloggers are often used by hackers to steal passwords and other user data in order to gain unauthorized access to a system. Other types of spyware can be known to monitor and record audio/video calls as well as track user activity on a system. Ultimately, spyware can be challenging to pinpoint given it runs secretly in the system's background, mostly undetected.

6. Adware

Adware is a type of software that displays unwanted advertisements on your computer. It can be distributed through email attachments, downloads and infected websites. Adware can slow down your computer and cause other performance issues. It can take many forms, including pop-up ads, banner ads and sponsored content. For example, the adware program DeskAd pushes deceptive ads and then overtakes the browser windows with a bombardment of ads.

The premise behind the use of adware is often to disrupt the system memory causing processors and other operating system capabilities to crash. Most adware today is often used to generate revenue for its developers by delivering targeted ads to the user. However, some forms of adware may also collect user data for targeted advertising purposes without their consent.

7. Ransomware

Ransomware is malware that encrypts a targeted victim's files and locks access to their computer system. This type of malware demands a ransom payment in order to receive a decryption key or another access method to unlock the system to regain access to it. Ransomware attacks aim to extort money from individuals, businesses and organizations by holding information and systems hostage. A recent example of a ransomware attack that affected an energy supply chain was the Colonial Pipeline attack in 2021. With this attack, bad actors disrupted and caused issues to the gas supply available within the Eastern United States.

Ransomware can be transmitted through various channels, including email attachments, malicious sites, software vulnerabilities and social engineering attacks. As soon as ransomware infects a system, it ordinarily displays a message or notification notifying the victim about the encryption and demanding payment. This payment is often requested to be made in the form of a cryptocurrency,

such as Bitcoin. Once a ransomware attack has occurred, paying the ransom does not guarantee access will be recovered to their files or systems. It may also encourage further attacks on the targeted system.

What Is the Most Dangerous Type of Malware?

It's widely known that most malware types can cause a great deal of damage to systems, networks, files and data. Malware attacks often depend on numerous factors, including the attackers' intent, the target and the vulnerability exploited.

However, ransomware has been proven to be the most dangerous to consumers and organizations. Ransomware is known to spread rapidly, be undetectable for long periods of time, expensive to remedy and restrict access to critical data.

Ransomware is often considered the most dangerous type of malware because it can cause significant damage to individuals, businesses and even governments. Additionally, ransomware has been proven to cause disruption to power grids and other energy supply chain resources that people need every day. Cybercriminals have been able to automate and develop it into a service product for other criminals to deploy themselves with solutions such as ransomware-as-a-service (RaaS). Of the many kinds of malware that can cause cybersecurity issues, ransomware can not only hold entire systems hostage while demanding payment, it also often comes with no guarantee the malware has been alleviated.

How To Prevent Malware

Malware, while challenging to avoid, is preventable in many cases. Counteracting against malware issues is important in order to keep your devices, systems, networks, sensitive information and data safeguarded.

Here are a few quick ways you can prevent malware from impacting your systems and devices:

- **Ensure your devices and computer systems are updated and backed up regularly.** In the event of a malware incident, this can provide quicker remediation and recovery.
- **Install software that supports anti-malware, anti-virus and anti-spyware.** This software should include scanning, identifying, quarantining and removing malware types from systems successfully. By employing the use of software that helps detect and remedy malware threats, such as Bitdefender and MacAfee Antivirus, it can help people and businesses better protect their data.
- **Avoid suspicious emails and websites.** Cybercriminals are always looking for new avenues and methods in order to use malware to attack organizations and individuals. It is best to avoid websites that seem suspicious and report any unsolicited emails and attachments sent to you if you are unsure of the source.
- **Utilize strong passwords.** Given that many hackers and malware programs can use keyloggers and spyware to track user information and data, it is important to use strong passwords. More

complex passwords along with multi-factor authentication (MFA) can help minimize the likelihood of password cracking.