**Types of malware**

There are different types of malware that contain unique traits and characteristics. Malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer **viruses**, **worms**, **Trojan** **horses,** and **spyware**. These malicious programs **can perform a variety of functions**, including **stealing**, **encrypting** or **deleting** sensitive data, **altering** or **hijacking** core computing functions and **monitoring** users' computer activity without their permission.

* A **virus** is the most common type of malware, and it's defined as a malicious program that can execute itself and spreads by infecting other programs or files.
* A **worm** is a type of malware **that can self-replicate without a host program;** worms typically spread without any human interaction or directives from the malware authors.
* A **Trojan** **horse** is a malicious program that is designed to appear as a legitimate program; once activated following installation, Trojans can execute their malicious functions.
* **Spyware** is a kind of malware that is designed to **collect** information and **data on users** and **observe their activity** **without** users' knowledge.

Other types of malware include functions or features designed for a specific purpose.

* **Ransomware**, for example, is designed to infect a user's system and encrypt the data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
* A **rootkit** is a type of malware designed to obtain administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system.
* A **backdoor virus** or **Remote Access Trojan (RAT)** is a malicious program that secretly creates a backdoor into an infected system that allows threat actors to remote access it without alerting the user or the system's security programs.

**How malware infects people**

**Infections spread by malware** writers and attackers **exploiting** **unpatched security holes or vulnerabilities** in **older** **versions** of popular software such as Adobe, Java, Windows Media Player and the Windows operating system itself. The software is one of the favorite targets of malware writers who continue to exploit coding and design aggressive vulnerabilities. Cybercriminals constantly devise innovative means to get malware onto your computer. The most common ways that malware, including viruses, worms, Trojans, and spyware, can be spread by exploiting application tools as **email**, the **internet** itself, **outdated** **software**, **local area networks (LANs), instant messaging and peer-to-peer file sharing systems, pop-ups, computer storage media and mobile devices.**

* **Emails** allow cybercriminals include malicious attachments and links in emails that appear to come from friends, reputable organizations, or other trusted sources. Some malicious emails can even infect your computer from the email client’s preview pane, without your opening or download an attachment or a link.
* **The Internet** allows for surfing the Web, which may feel like a private activity, but in fact, you’re exposing your computer to unwanted contact with anyone else who has a computer and Internet access. All you must do is visit a website or click a link and you’re a potential victim. Malware crawls the Internet, looking for vulnerabilities of outmoded software to spread its influence over computer systems.
* Be especially careful if you’re surfing the Web with **outdated software**. Make sure to never connect to the internet without being updated with the latest versions as soon as you can, including your browsers, operating systems, or system plug-ins.
* **Local Area Networks** (LANs) are a group of locally connected computers that can share information over a private network. If one computer becomes infected with malware, all other computers in the LAN may quickly become infected as well.
* Also, if you’re using a client for **Instant messaging** (IM) and **peer-to-peer (P2P) file-sharing** online systems activities, malware may spread to your computer.
* **Social networks** allow malware authors to take advantage of having the ability to infect the massive user-data networks with worms. If a social website account is infected with a worm, just about anyone who visits a poster’s profile page could “catch” the worm on their system. Some of the most sophisticated malware spreads through well-disguised screen pop-ups that look like genuine alerts or messages.
* Malware can be easily spread if you **share computer storage media** with others, such as USB drives, DVDs, and CDs. While it may seem safe to open a CD of photos from a colleague, it’s always best to scan unfamiliar files first for possible corruptions or security risks before you copy or open them.
* **Mobile malware** threats have become increasingly prevalent, as more people use their smartphones and tablets as mini-computers, helping malware problems proliferate across additional platforms.
* Malicious codes also spread into a system through **pirated software**. In the majority of the cases, software seems to be legitimate, when downloaded, instead, they are a be a big trouble for your system.

**How malware works**

Malicious programs **can be delivered physically** to a system through a USB drive or other means. Malware **often spreads via the internet** through drive-by downloads, which automatically download malicious programs to users' systems without their approval or knowledge. These are initiated when a user visits a malicious website. **Phishing attacks** are another common type of malware delivery; emails disguised as legitimate messages contain malicious links, or attachments that deliver the malware executable to unsuspecting users. Sophisticated malware attacks often feature the use of a command-and-control server that allows threat actors to communicate with the infected systems, download sensitive data and even remotely control the compromised device or server.

**Malware Conclusion**

Many infections are contracted and spread by visiting **gaming sites**, **porn sites**, **using pirated software (warez),** **cracking tools**, **hacking tools**and **keygens** where visitors may encounter drive-by downloads through the exploitation of a web browser or an operating system vulnerability.

There is no end to the channels through which malware can attack your computer, and once inside your system, these spread automatically and disrupts internet traffic as well.

Some malware even gives access to your computer. Malware like Trojan horses do not replicate themselves, but they can damage a system badly and these generally come in the form of screensavers or free games.

Fortunately, there are ways through which you can protect your system from these malware attacks and you just need to be a little vigilant to avoid such attacks.