Malware Issues

Trojan Horse

Trojans are a class of malware that take their name from the way they infect computers. Trojans hide themselves within seemingly harmless programs or try to trick you into installing them.

Trojans do not replicate by infecting other files or computers. Instead, Trojans survive by going unnoticed: they may sit quietly in your computer, collecting information or setting up holes in your security, or they may just take over your computer and lock you out.

Some of the more common actions that Trojans take are:

Creating backdoors: some Trojans will make changes to your security system so that your data and device can be accessed by their controller.

Spying: some Trojans are designed to wait until you access your online accounts or enter your credit card details, and then send your data back to whoever is in control.

Steal you passwords: some Trojans are made to steal your passwords for your most important online accounts.

Worms

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.

Malicious Bots

"Bot" is derived from the word "robot" and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information (such as web crawlers), or interact automatically with instant messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites.

Bots can be used for either good or malicious intent. A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers. In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information etc.

Adware

Adware software can display and/or download advertisements and may be considered privacy-invasive. Adware tracks your computer's web usage to feed you undesired ad pop ups or redirect you to unwanted pages.

Adware can hijack your home page and take you to sites you aren't interested in, allow pop up ads that are disruptive to your system. Since they run every time you turn on your computer, they can cause slowdowns and software conflicts that can make your computer unstable.

Rootkit

Rootkit is an application (or set of applications), that hides its presence or presence of another application (virus, spyware, etc.) on the computer, using some of the lower layers of the operating system, which makes them almost undetectable by common anti-malware software.

Rootkit can get to a computer using various ways. The most common way is through some trojan horse or some suspicious email attachment. Also surfing the web may result in installation of a rootkit, for example when "special" plugin (pretending to be legitimate) is needed to correctly view some webpage, to launch some file, etc.

Ransomware

Ransomware stops you from using your PC. It holds your PC or files for ransom. There are different types of ransomware. However, all of them will prevent you from using your PC normally, and they will all ask you to do something before you can use your PC.

They can:

- Prevent you from accessing Windows.
- Encrypt files so you can't use them.
- Stop certain apps from running (like your web browser).

Often the ransomware will claim you have done something illegal with your PC, and that you are being fined by a police force or government agency.

These claims are false. It is a scare tactic designed to make you pay the money without telling anyone who might be able to restore your PC.

There is no guarantee that paying the fine or doing what the ransomware tells you will give access to your PC or files again.