In the Name of GOD

Malware

Course: Specific English

Professor: Dr.Mahvash

Isfahan university

Researcher: Parastoo gholami

Student number: 993613048

Fall 1400

Malware or malicious software is designed to disrupt, damage, or gain unauthorized access to a computer system. Malware authors use a variety of physical and virtual means to spread malware and infect or exploit your system. Malware can steal your information, like identification codes, passwords, credit card numbers, photos, etc. It is also used against companies and governments to get money or overthrow them. Depending on the type of malware and the goal, it has different effects. The damage could be benign or even a disaster. There are several types of malware, such as viruses, adware, trojans, worms, rootkits, and ransomware. In the following paragraphs, we are going to discuss all these types.

The most common type of malware is viruses. It is a malicious code or program written to alter the way a computer works and is designed to spread from one computer to another. First, the purpose of viruses is to create a copy of themselves and insert them into the machine code instructions. Second, after the program runs or the disk is booted, it will send your files to the virus writer or corrupt and destroy your data. Before Internet access became widespread, computers got infected by executable programs or boot sectors of floppy disks. Nowadays, these bugs are normally attached to an email, document files, etc. When the virus infects your computer, it can happen to all the computers on the same network.

A computer worm is standalone malware that replicates itself in order to spread to other networks. The first worms originated not on personal computers, but on multitasking Unix systems. Unlike a virus, this worm does not insert itself into other programs. Instead, it exploited security holes in network server programs and started running as a separate process. They can modify and delete files or inject additional malicious software, but the main purpose of this type of malware is only to make copies of themselves over and over again and take up all your computer's available memory or hard disk space. They cause harm by consuming bandwidth and overloading web servers.

A Trojan horse, or a Trojan, is any kind of malware that misleads users by disguising itself as a harmless file. It usually comes in the form of an app or software pretending to either be useful or fun. Cybercriminals use psychological manipulation to convince people to welcome the infected software into their devices. They send emails that appear to be from a trusted source, help messages, convince you that you are under attack, and trick you into downloading a Trojan horse. Once installed, the Trojan malware can start infecting other files, sometimes without you even noticing. There are some common types of Trojan malware. Banker Trojans aim to access and steal your financial data. Downloader Trojans download new versions of malware to your computer on their own. Malfinder Trojans collect and steal all of the email addresses on your device.

For sure, you have seen unwanted or sometimes even irritating pop-up adverts on your computer or mobile device during your installation process. These are generated by adware. Adware or advertising-supported software can also track your search and browsing history to display ads that are more relevant to you. So, adware will generate 4 types of revenue for its developers: First, each time an ad is shown to the user, Pay-per-view (PPV), second, each time the user opens an ad, Pay-per-click (PPC), third, each time bundled software is installed on a device, Pay-per-install (PPI), and lastly, by selling collected data about the users.

Ransomware has highly evolved and now leads the list of the world's most dangerous new cyber threats. It is designed to block access to a computer system until a sum of money is paid. It is mostly spread through drive-by downloading or phishing emails that contain malicious attachments. Drive-by downloading happens when a user unknowingly visits an infected website, and then malware is downloaded and installed. One of the most well-known and damaging types of ransomware is crypto-ransomware or encryptors.

A rootkit is designed to give unauthorized access to a computer or other software. It is hard to detect them because they can conceal their presence. Hackers use this type of malware to remotely access and control your computer. They typically infect devices via phishing emails. Like Trojan malware, they need help to get installed. For installing a rootkit, a dropper and a loader must work together. A dropper is a program or a file used to install a rootkit on a target and a loader is a malicious code used for loading another executable file onto the infected device. There are four main types of rootkits. The most dangerous one is a kernel-level rootkit because it infects the core of a system, and the other three are user-mode rootkits, bootloader rootkits, and memory rootkits.

Day by day, the world becomes increasingly dependent on computers. We save our personal information, company documents, and other things on them, so security is one of the most important issues these days. As the number of security breaches is growing, we must get more familiar with these threats. The best way to guard against malware is to install antivirus software. On the other hand, you must take caution. Not just installing programs could be harmful but also clicking on them can be risky. Keep your computer and software updated. Don't open any unrecognized files thoughtlessly. Be careful about opening email attachments and images. Don't trust pop-up windows. Break the habit of opening every random ad. Don't allow every application to get access to your personal data.