

Report on Malicious Software

Submitted by: Omar Mostafa Abdelsttar

ID: 932230123

Submitted to: Dr. Osama Emam

Malware

The term "malware" is short for malicious software. This term covers various types of harmful programs, including viruses, worms, Trojans, logic bombs, and adware and spyware. Malware has evolved dramatically to include the ability to steal passwords, personal information, and identities. In some cases, it can also damage hardware.

Categories of Malware

The main categories of malware include viruses, worms, Trojan horses, spyware, and adware. Additionally, rootkits are a modern form of malware that can hide within a system's core components, staying undetected by modern scanners. Their techniques include renaming a package to a legitimate program's name and altering other files to prevent them from being detected and running.

Viruses

Viruses are by far the best-known form of malicious software. This type of malware is designed to replicate and attach itself to other files on a system. They typically require some form of user action to initiate their infectious activities. Once a virus is launched, it can alter data, infect other programs, replicate itself, and even encrypt and transform itself. It can also alter configuration settings, destroy data, and corrupt or destroy hardware.

The Process of Developing a Virus:

1 Design:

The author envisions and creates the virus, either from scratch or by using one of the many available construction kits.

2 Replication:

Once deployed, the virus spreads through replication, multiplying and ultimately spreading to different systems. This process can be very rapid.

3 Launch:

The virus begins its intended task, such as destroying data or changing system settings, once it is activated by a user action or other predetermined event.

4 Detection:

The virus is recognized as such after it has infected systems for some time. The nature of the infection is usually reported to antivirus makers, who begin their initial research on how the software works and how to eradicate it.

5 Incorporation:


Antivirus makers determine how to identify the virus and incorporate the process into their products through updates. This is typically done by adding the new malware to signature files that are downloaded and installed by the antivirus application.

6 Elimination:

Users of antivirus products incorporate the updates into their systems to eliminate the virus.

Examples of Virus Creation:

A simple virus can be created using Notepad and a utility like bat2com. The process involves creating a batch file named virus.bat with code that can delete system files, then converting it to a .com file.

 **Warning:** This exercise is a proof of concept for illustrative purposes only, and executing the code can result in extensive damage to a system.

Another way to create a virus is to use a utility such as "JPS Virus Maker" or "Terabit Virus Maker". These tools allow the user to select options from a graphical user interface (GUI) to create a new executable file that can infect a host. The "TeraBIT Virus Maker" has options to turn off the monitor, mute system volume, slow down PC speed, disable Task Manager, format all hard drives, and delete all files in My Documents, among many others.

Worms:

Worms are an advanced form of malware compared to viruses. One of their main characteristics is their inherent ability to replicate and spread across networks extremely quickly. They do not require a host application or user interaction to function. Worms replicate rapidly, consuming bandwidth and system resources.

Spyware:

Spyware is a type of malware designed to collect and forward information about a victim's activities to an interested party. Its defining characteristic is that it acts behind the scenes to gather information without the user's consent or knowledge. Spyware has been used to target ads, steal identities, generate revenue, and alter systems.

Methods of Spyware Infection:

- **Instant Messaging (IM):**

Delivering malicious software via IM is easy, as IM software has historically lacked strong security controls.

- **Internet Relay Chat (IRC):**

IRC is a commonly used mechanism to deliver messages and software due to its widespread use.