SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit III- Network Threats

Topic : Adware - Spy ware – Trojans

Adware

- Adware (or **advertising software**) is the term used for **various pop-up advertisements** that **show up on your computer** or mobile device.
- Adware has the potential to become **malicious and harm your device** by slowing it down**, hijacking your browser** and installing viruses and/or spyware.

How to detect adware

The most common way to recognize adware is the **appearance of pop-up advertisements and applications that you are unfamiliar** with and on browsers where they had not been displayed before.

- **Lagging performance** and eventual crashing
- **Unrequested changes** to your browser homepages
- **Appearance of new extensions and toolbars**
- Web pages **not displaying properly**
- **Unwanted software installing**

Types of adware

Adware **commonly takes the form of irritating pop-up** windows and banners; however, it can act in many different ways:

- Acting similarly to spyware, some types of adware **track your movement and activities online** in order to tailor specific adverts to you
- Operating as a **middle man**, adware can **redirect** your activities through them in order to share adverts with you
- **Adware uses up your data**, with every pop-up download eating away at your allowance
- Slowing down your computer, running adware uses up power **affecting your device's performance**

How does adware removal work?

- In cases where Adware has already affected your device, an **antivirus program is recommended for secure removal.**

- **There are many free tools for removing adware from your device** however, not all of these are safe and viable options.

- **Installing Anti-virus software will help prevent** any viruses that could attack your computer through the form of adware as well as providing a safe removal option.

- If you have an antivirus program installed – **be sure to back up your files and data before beginning a scan to remove any potential adware on your device.**

Spy ware

- **Spyware is malicious software** that enters a user's computer, **gathers data from the device and user, and sends it to third parties without their consent.**

- A commonly accepted spyware definition is a strand of malware designed to access and damage a device without the user's consent.

- Spyware is basically meant for **spying on the users** and **collect their sensitive information like browsing habit, banking details, credit card details, and more.**
- Cybercriminals can then use that information for hacking, extortions, and more such illicit activities.
- Spyware programs are also used **for stealing your internet data** and **remotely taking control of your system**.
- Usually, after entering the device, Spyware works in **stealth mode.**

Indications of Spyware infection

- If your **browser is hijacked**, i.e., homepage, search engine, etc., are changed on its own without your intervention.

- **Spyware install browser hijacker malware to collect your browsing information like search history, IP addresses, and more.**
- If you notice your system is consuming unusual internet data without much use, it might be because Spyware is secretly using the data in the background to transfer your data to cybercriminals.
- The **system gets crashed repeatedly and slowed down frequently** without heavy use because of Spyware running in the background.
- The **CD/DVD case of your system opens up randomly.**
- You found some mails on your sent folder that you don't remember sending. It might be because a cybercriminal is controlling your system through Spyware.

How to remove Spyware?

- **Open the Device Manager and look at which program or service is unnecessarily taking up the RAM.**

- **Take note of such applications or processes and delete/uninstall them.**

- Clear your **recycle bin and temporary files** folder.

- For complete **removal of Spyware,** use a robust antimalware program.

How to prevent Spyware Infiltration?

- Spyware can be devastating after entering your system. It is essential to stop them from **infiltrating your system**. Here are some of the measures you can take.
- Keep your **Operating System and Software updated**. Malware programs like Spyware take advantage of vulnerabilities in the system or software to enter your device.
- **Updating them will fix the vulnerabilities and reduce the risk of infection.**
- **Avoid downloading software, movies, etc., from unknown, unreliable sources. Never download anything from torrent sites.**

- While **installing any software, ensure that no other unwanted application is getting installed** along with the primary one.
- Never **interact with attractive pop-up and banner ads**. They are specially designed to trick users into clicking them so that malware can be downloaded into the system.
- Keep **installed a robust security solution on your system**. A security solution would detect an incoming Spyware and block it before it makes its way into your device.
- Manage the **permissions you give to your apps**. **Never provide unnecessary grants to software programs.**

Trojan

- The Trojan is a **type of malware program or code that presents itself** as a useful legitimate program so that users would get fascinated by it and install it.

- It usually **tricks users by using social engineering techniques.**

- Cyber attackers design Trojan to control the system to **perform various unwanted tasks such as stealing private information & secret files, damage the operating system, infecting the system with other harmful malware, and more.**

- Trojan is often referred to as other names such as **Trojan Virus**.

Common Types of Trojan

Based on their infiltrating and attacking nature, Trojans are classified into the following types.

SMS Trojan

- This type of Trojan, after infiltrating your device, can **intercept and send messages.**

- SMS Trojans are mostly used for **sending texts to premium-rate numbers to generate** revenues by cutting user's phone costs.

Backdoor Trojan

- This type of Trojan acts as **a backdoor for other malware to enter your device.**
- It can also be a **backdoor for intruders to take control of your system.**
- Your private data can be stolen, and attackers could also install spyware.

Ransom Trojan

- Ransom Trojans are meant particularly for introducing Ransomware to your system.
- It would **lock your files with strong encryption and demand ransom** in return for the decryptor.

Downloader Trojan

- The downloader Trojan is responsible for **downloading the malicious programs on your system**, including other Trojans and malware.
- Usually, such trojans hide in the **background of your device and work silently.**

Fake AV Trojan

- Such Trojans act as **antivirus programs and ask users to buy them to protect their system from harmful threats.**
- In reality, it is just a rogue security program that produces fake results to force users to buy the premium version.

How Trojan Works?

- First, the developers behind the Trojan would use **social engineering tricks like sending gifts via email, throwing a pop-up of an intriguing offer, and similar schemes.**

- Next, after the victim clicks on such emails or pop-ups without knowing the intention behind it, the **Trojan would enter the system and start working on its purpose.**

- It can also **spread to different locations of your device and infect other programs.**

How to get rid of Trojans?

Following steps can be taken to get rid of Trojans from the system manually:

- Recognize which application or service is causing the trouble. For that, you can take the **help of the Task Manager** and look for the application or process using system resources abnormally.

- **Stop** the **system restore** so that the files you erase couldn't be recover.

- **Reboot the device in Safe Mode to control the Trojan**.
- Remove the **suspected programs from the system**. You must be careful while removing the programs, as removing a legit system app can enhance the problem.
- Clear your device junks like **Temporary Folder and Recycle Bin.**

Any Query????

Thank you……