Syllabus subtopic: Awareness in the fields of IT, Space, Computers, robotics, nano-technology, bio-technology and issues relating to intellectual property rights.

Prelims and Mains focus: About StrandHogg bug and cyberthreats associated with it; types of malware

News: The Union Home Ministry has sent an alert to all States warning them about the vulnerability of the Android operating system to a bug called ‘StrandHogg’ that allows real-time malware applications to pose as genuine applications and access user data of all kind.

What is the threat?

- While all versions of Android, including Android 10, are vulnerable to this bug, it may not be apparent to the affected users that malware applications are already on board their device. These malware can then potentially listen to their conversations, access photo album, read/send messages, make calls, record conversations and get login credentials to various accounts.
- This apart, things that such malware can access include private images, files, contact details, call logs, and location information.
- At least 500 popular apps are at risk because of this malware that hackers can deploy to attack mobile phone users. An alert has been sent to all senior police officials to sensitise them to the threat. Steps will be taken to create awareness among the public on the vulnerability of Android to ‘StrandHogg’.

How does it enter the system?

- Pop-ups asking for permission to send notifications, messages etc., are one of the main entry points for ‘StrandHogg’ to launch the attack.
- An app in which the user is already logged in asking him/her to login again is another anomaly pointing to the possibilities of a cyberattack. Once users approve such requests, the malware would instantly access the mobile phone or tablet for specific purposes.
- It can activate the microphone, allowing a hacker in a remote location to listen to live conversations. The camera can also be switched on to capture visuals.
- Links and buttons that become non-functional, apps asking for permissions that are not required are among the other warning signs.

How can you be safe from this attack?
Currently, there is no effective block or even detection method against StrandHogg on the device itself. However, as an user, you should be alert to the following discrepancies in your device:

- An app or service that you’re already logged into is asking for a login.
- Permission popups that does not contain an app name.
- Permissions asked from an app that shouldn’t require or need the permissions it asks for. For e.g., a calculator app asking for GPS permission.
- Typos and mistakes in the user interface.
- Buttons and links in the user interface that does nothing when clicked on.
- Back button does not work like expected.

What is a Malware?

Malware is software written specifically to harm and infect the host system. Malware includes viruses along with other types of software such as trojan horses, worms, spyware, and adware. Advanced malware such as ransomware are used to commit financial fraud and extort money from computer users.

Common Types of Malware

**Virus:** As discussed, Virus is a specific type of malware by itself. It is a contagious piece of code that infects the other software on the host system and spreads itself once it is run. It is mostly known to spread when software is shared between computers. This acts more like a parasite.

**Adware:** Adware is also known as advertising-supported software. It is software which renders advertisements for the purpose of generating revenue for its author. The advertisements are published on the screen presented to the user at the time of installation. Adware is programmed to examine which Internet sites, the user visits frequently and to present and feature related advertisements. Not all adware has malicious intent, but it becomes a problem anyway because it harms computer performance and can be annoying.

**Spyware:** This type of malicious software, spies on you, tracks your internet activities. It helps the hacker in gathering information about the victim’s system, without the consent of the victim. This spyware’s presence is typically hidden from the host and it is very difficult to detect. Some spyware like keyloggers may be installed intentionally in an organization to monitor activities of employees.
**Worms:** This type of malware will replicate itself and destroys information and files saved on the host PC. It works to eat up all the system operating files and data files on a drive.

**Trojan:** Trojans are a type of virus that are designed to make a user think they are a safe program and run them. They may be programmed to steal personal and financial information, and later take over the resources of the host computer’s system files. In large systems, it may attempt to make a host system or network resource unavailable to those attempting to reach it. Example: you business network becoming unavailable.

**Ransomware:** Ransomware is an advanced type of malware that restricts access to the computer system until the user pays a fee. Your screen might show a pop-up warning that your have been locked out of your computer and that you can access only after paying the cybercriminal. The cybercriminal demands a ransom to be paid in order for the restriction to be removed. The infamous WannaCry one type of ransomware.

A **software bug** is an error, flaw or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways. The process of finding and fixing bugs is termed "debugging" and often uses formal techniques or tools to pinpoint bugs, and since the 1950s, some computer systems have been designed to also deter, detect or auto-correct various computer bugs during operations.