First-ever significant anti-spyware declaration

April 7, 2023

In news– Recently, the US and 10 other nations issued the first-ever significant anti-spyware declaration.

About the declaration-

- **Countries involved in the declaration are** Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the United Kingdom and the United States
- The declaration said the nations would take concrete steps to push back on spyware's marketability.
- The declaration committed to "preventing the export of software, technology, and equipment to end-users who are likely to use them for malicious cyber activity, including unauthorized intrusion into information systems, in accordance with our respective legal, regulatory, and policy approaches and appropriate existing export control regimes."
- A recent US think tank report claimed that Israeli spyware (including multiple groups) has conquered a significant majority of the global spyware market.

What is spyware?

Spyware is software with malicious behaviour that aims to gather information about a person or organization and send it to another entity in a way that harms the user—for example, by violating their privacy or endangering their device's security.

Types of Spyware-

Attackers use various types of spyware to infect users'

computers and devices. Each spyware variety gathers data for the attacker, with the lesser types monitoring and sending data to a third party. But more advanced and dangerous spyware types will also make modifications to a user's system that results in them being exposed to further threats.

Some of the most commonly used types of spyware include:

1. **Adware:** This sits on a device and monitors users' activity then sells their data to advertisers and malicious actors or serves up malicious ads.
2. **Infostealer:** This is a type of spyware that collects information from devices. It scans them for specific data and instant messaging conversations.
3. **Keyloggers:** Also known as keystroke loggers, keyloggers are a type of infostealer spyware. They record the keystrokes that a user makes on their infected device, then save the data into an encrypted log file. This spyware method collects all of the information that the user types into their devices, such as email data, passwords, text messages, and usernames.
4. **Rootkits:** These enable attackers to deeply infiltrate devices by exploiting security vulnerabilities or logging into machines as an administrator. Rootkits are often difficult and even impossible to detect.
5. **Red Shell:** This spyware installs itself onto a device while a user is installing specific PC games, then tracks their online activity. It is generally used by developers to enhance their games and improve their marketing campaigns.
6. **System monitors:** These also track user activity on their computer, capturing information like emails sent, social media and other sites visited, and keystrokes.
7. **Tracking cookies:** Tracking cookies are dropped onto a device by a website and then used to follow the user's online activity.
8. **Trojan Horse Virus:** This brand of spyware enters a

device through Trojan malware, which is responsible for delivering the spyware program.