StrandHogg

April 26, 2020

Context: The Union Ministry of Home Affairs (MHA) has sent an alert to all States warning them about the vulnerability of Android operating system to a bug called 'StrandHogg'

- Cybercriminals have found an under-investigated vulnerability to breach Android devices. It is called StrandHogg, and it can allow them to listen to microphones, steal login credentials, take photos using cameras, read SMS and even access photos.
- First reported by Norway-based cybersecurity firm Promon and later confirmed by their partner firm Lookout,
- At the heart of the issue is a weakness in the multi-tasking system of Android OS.
    - It basically exploits Android control settings called taskAffinity and taskReparenting to allow apps including malicious ones to freely assume identity of another task in the multitasking system.
    - It allows the malicious activity to hijack the target's task, so the next time, user opens the target app, the hijacked tasks will open up instead of the original tasks.
    - During this interception, the malicious app will seek permission to access the device's camera, microphone, messages, GPS and storage.
    - If the user grants these permissions, the malicious app gains access to these components.
- The malware needs to be installed on the Android device to exploit this vulnerability.
- Malicious apps exploiting the vulnerability did not come directly through Google Play Store.
    - Instead they were installed through dropper apps distributed on Google Play.

    - Dropper apps either have or pretend to have the functionality of popular apps so it can bypass Google Play Protect.
    - After it is installed, the app installs additional apps which may be malicious
- Threat Analytical Unit of Indian Cyber Crime Coordination Centre, has sent an alert to all states and police departments of a bug that can be exploited by malwares posing as genuine apps to spy on users.
- The potential impact of this could be unprecedented in terms of scale and the amount of damage as most apps are vulnerable by default.