Subject: **Advisory - Prevention against Iran Cyber warfare Surveillance (Advisory No. 33) Jul 18**

1. **Background.** Reliable sources have revealed Iran's involvement in cyber warfare by spreading **spyware-enabled apps (Mobogram)** for **"cyber-surveillance and repression"** with goal of **"monitoring and preventing"** new political uprisings. Reports claim that Iran is now using these apps internationally after its successful test on Iranian masses.

2. These apps are available on **Google Play store, App Store,** and **GitHub,** potentially exposing millions of users worldwide to the regime's spyware and surveillance.

3. **Technical Analysis**

   a. **Hanista** is an **Islamic Revolutionary Guard Corps (IRGC) front company,** introduced as programming group, which focus on enabling Iran's Cyber commerce with mobile apps in Farsi language.

   b. **Mobogram,** an app developed by **Hanista,** is presented by the regime as **alternative to Telegram.** Its controlled environment let the regime surveil users, identify and arrest protesters.

   c. Similar projects are also being carried out by other advanced powers of the world for global cyber surveillance.

4. **Affected Products.** These malicious apps affects following platforms, as under:-

   a. Android

   b. iOS

5. **Mitigation Measures**

   a. Perform a comprehensive scan of android phone to identify any malicious app especially **"Mobogram",** uninstall any such apps immediately if found installed.

   b. Update and install latest security patches for OS and all installed applications.

   c. Enable Google Play Protect security feature on the device. This feature will remove (uninstall) malicious apps from user's Android smartphone to prevent further harm.

   d. Download app from Google's Official Play Store vigilantly and always verify' app permissions and reviews before downloading any app. It is advised to **disable installation of apps from third-party sources.**

   e. Install an antivirus app (e.g. Avast) on smartphone that can detect and block malicious apps before they can infect a device.

f. Always pay attention to **misspelled app names,** small numbers of downloads, or !dubious **requests for permissions -** any Of these things should raise flags.

6. **Recommendations.**

a. Strictly follow all mitigation Measures discussed at para 5.

b. Remove all unnecessary apps installed in smart phone.