Subject: **Advisory - Prevention Against " Stealth Mango " - A Mass Data Collection Campaign (Advisory No. 34)**

1. **Background.** Security researchers have discovered a set of custom built **Android and iOS surveillance applications** that are being used for spying purposes. These surveillance tools are being used to compromise government officials, military personnel and civilians in general. This campaign is code named as **"Stealth Mango"** and **"Tangelo"** and it is being deployed on a large scale against people of Pakistan, Afghanistan, India, Iran and UAE.

2. **Technical Analysis**

   a. Stealth mango typically lure victims via phishing, but they may also have physical access to victims' devices.

   b. 15 GBs of data recovered from one of the C&C servers have revealed that espionage activities are mainly focused to gather following information.

      (1) Detailed travel information.

      (2) Pictures IDs and passports.

      (3) **GPS coordinates.**

      (4) Pictures, IDs and Passports.

      (5) Legal and Medical documents.

      (6) **Photos of military, government and intelligence officials.**

      (7) Call records and messaging information.

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

   a. Android

   b. iOS

4. **Mitigation Measures**

   a. 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.

   b. Download apps 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.**

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

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

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

5. Recommendations.

a. Strictly follow, all mitigation measures discussed at Para 4.

b. Remove all unnecessary apps installed from smart phone.

c. Always use separate **phones** for **official** as well **personal** purpose. It is advised to not to install any app in official phone.

d. It is strictly **cautioned** do not keep any **official document, pictures, maps** etc in mobile phone.