Subject:- **Advisory - Prevention Against Malicious Android Applications (Advisory No.15)**

1. **Context.** An Indian based mobile Remote Access Trojan (RAT) has been found spreading through **social engineering tactics**. 4x malicious applications (**Babble Version 1**, **Babble Version 3**, **TeleChatty** & **Filos**) are used for espionage / information gathering operations. The identified applications are dubbed as **Signal Messaging App**. **Downloading** and **installing** these mobile applications APK executes a Remote Access Trojan (RAT) in the background that compromises victim's phone and uploads all sensitive data to its **C&C servers**. Users are advised to refrain from downloading applications from untrusted sources and follow recommendations provided at **Para-2**.

2. **Recommendations**

a. Do not install the applications promptly. **Check for permissions** that the application requires. If seem beyond what the application should require, do not install such an application. It could be a **Trojan** carrying **malicious code** in an attractive package.

b. **Do not install applications** from **unknown sources**. it mitigates problems associated with mobile Trojans.

c. **Do not download cracked / free versions of applications, which are otherwise paid,** as most of them are infected such as **WhatsApp Plus, Netflix APKs** etc.

d. Only install applications from official app stores, such as **Google Play Store**.

e. **Google Play Protect (android built-in anti-malware)** must not be switched off in any case. It detects suspicious looking applications in your mobile device based on their behavior and generates alerts for users' knowledge.

f. **Do not click on links that promise unusual features or functionalities such as "WhatsApp offers of free Airline Tickets"** are usually an attempt to steal users' personal data. The same applies to phishing attacks including text from friends containing suspicious URLs.

g. Before installing any application, user must read its **privacy policy** explaining that What data it is collecting form users and with whom it **is sharing** that data.

h. It is strongly recommended to ensure keeping all **applications updated** from respective **App / Play Stores**. Do not ignore update alerts.

i. Regularly **Update Mobile Operating Systems.**

j. **Ensure Use of mobile Antivirus** in order to prevent any risk that may affect your personal data on device. These applications not only find and remove Trojans, but also **block websites with malware.**

k. **Ensure physical control of the device,** especially in pubic places.

l. Set **Bluetooth-enabled** devices to **not-discoverable** mode. When in **discoverable mode,** devices are visible to nearby devices, that may alert an **attacker or infected device.** Only allow Bluetooth **pairing options** to

authentic and **trustworthy** device. Do not forget to un-pair the devices once task on Bluetooth is completed.

m. **Be vigilant** when using **social networking applications.** Such applications may request for personal information and later on may sale it to 3rd parties.

n. **Always disable locations tracking / GPS.** Only use it when required and **turn it off again.**

o. **Never keep official** and **personal data** on **online drives** and **emails** like Google Docs, Outlook etc.

.

*** * * * ***