## Advisory Newly Ident Spotting / Cultivation Tech Adopted by Attackers (Advisory No. 87)

**Introduction.** Recently, hostile intelligence agencies are using sophisticated Remote Access Trojans (RATs) for Android mobiles to exfiltrate sensitive data. These malicious RATs are masqueraded as genuine Apps to entice users to download / install these Apps. Some of the feigned Apps include **Yo WhatsApp, WhatsApp Blue, AK WhatsApp, GB WhatsApp, WhatsApp Plus, WhatsApp Reform, WhatsApp Prime, Islamic Chat, Rapid Chat, Skype, Chrome/ FireFox and Secure / Free VPN** etc. Moreover, these RATs employ a range of attack vector for distribution like Social Engineering via young girls, Websites, Ads, Social Media, Emails, SMS, Telegram or WhatsApp messages to launch cyberattacks.

2. **Summary of Malicious Application**

   a. **Malware Type.** Over-permissive / Data Mining Application

   b. **Distribution Vectors.** WhatsApp, Social Media, Websites, Emails, SMS

   c. **Threat Impact.** Critical

   d. **Antivirus Detection Rate**. 0/56 (None)

   e. **Permissions**. These Apps generally require following permissions during installation: -

      (1) Accessing contact list, SMS

      (2) Network and GPS Based Information

      (3) Recording Audio

      (4) Call Phone Number, reading call log, reroute outgoing call

      (5) Read / receive text messages (SMS, MMS)

      (6) Accessing Phone Storage

      (7) Photo Gallery

3. **Capabilities / Modus Operandi**

   a. If not connected to internet, the applications insists on connecting to internet to unlock full app features.

   b. The moment device connects to internet, it uploads user data, like IMEI number, files, Gmail account ID, contacts, SMS logs, geolocation, call logs, pictures etc to its C&C server.

   c. These malicious apps have ability to bypass antimalware solutions and capability to evade analysis in the virtual environment (Sandbox).

4. **Recommendation**

a. Always install apps from Google Play Store only: in phone Setting, **do not enable** installation of apps from **Untrusted Source / Third Party**.

b. Before downloading / installing apps on Android devices, review the app details, number of downloads, user reviews, comments and "ADDITIONAL INFORMATION" section.

c. Always **monitor permissions** being required by app during installation.

d. Under command must be regularly sensitized about malicious actor' tools, tactics and procedure; moreover, all personal be advised to refrain from engaging in immoral activities to avoid any exploitation.

e. Install and update strong antivirus solution like AVAST or Kaspersky on Android devices. After antivirus installation, scan the device to detect and clean infections.

f. Install Android updates and patches as and when available.

g. Do not download or open email attachments received from untrusted sources or unexpectedly received from trusted users.

h. Avoid using insecure and public Wi-Fi as hostile elements use rogue Wi-Fi access points at public places for distributing malicious apps.

i. Use two-factor authentication on all Internet Banking Apps, WhatsApp, Social Media and Gmail accounts.