

Subject:- **Advisory - Prevention Against Cyber Espionage via Malicious Android Application (Advisory No.14)**

1. **Introduction.** Hostile Intelligence Agencies (HIAs) are using advanced and sophisticated mobile Remote Access Trojans (RATs) for Android to exfiltrate sensitive data from government / military personals. These malicious RATs are embedded in applications, namely ChatSpy, Fruit Chat, Cucu Chat and Kako Chat which entice users to download / install these applications. Such applications employ a wide range of attack vectors for distribution including Social Engineering, Honey Trapping, Enticing websites, Ads, Social Media, Emails, SMS, Telegram or WhatsApp messages to conduct Cyber intrusions.

2. **Summary of Malicious Applications**

- a. **Application Name.** ChatSpy, Fruit Chat, Cucu Chat and Kako
- b. **Malware Type.** Over-Permissive Applications / Surveillanceware.
- c. **APT Group.** Pro Indian Group named Confucius.
- d. **Malware Names.** Lookout (UK based Cyber Security Company) named malware as HornBill and SunBird.
- e. **Distribution Vectors.** WhatsApp, Social Media, Websites, Emails, SMS.
- f. **Threat Impact.** Critical.
- g. **Antivirus Detection Rate** 0/56 (None)
- h. **Attack Timeline.** 2017-Ongoing
- i. **Permissions.** These Application commonly requires following permissions upon installation: -
 - (1). Reading Contacts, 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). USB Storage.
 - (7). Photos.

3. **Capabilities / Modus Operandi**

- a. If not connected to internet, the application insists on connecting to internet to unlock full app feature.

- b. As soon as the device connects to internet, it uploads user data, like IMEI number, Files, Gmail account ID, contacts, WhatsApp Voice Notes, SMS logs, geo-location, call logs, pictures / images to its C&C server.

4. **Recommendations.** In this regard following are recommended: -

- a. Always check application permissions before installation of application and install applications from Google Play Store only.
- b. Under command must regularly be sensitized about malicious actors tools, tactics and procedures, moreover, all personnel (officers / staff) be motivated to refrain from engaging in activities that may lead to exploitation.
- c. Install and update strong antivirus solution on android devices like AVAST or Kaspersky. After installation, scan the suspected device with antivirus solutions to detect and clean infections.
- d. Before downloading / installing apps on android devices, review the app details, number of downloads, user reviews, comments and “ADDITIONAL INFORMATION” section.
- e. In mobile settings, do not enable installation of apps from “**Untrusted Source**”.
- f. Install Android updates and patches as and when available from Android device vendors.
- g. Do not download or open attachment in emails received from untrusted sources or unexpectedly received from trusted users and forward them to emails mentioned in para-5.
- h. Avoid using unsecure and unknown Wi-Fi networks as hostile elements use Wi-Fi access points at public places for distributing malicious applications.
- i. Use two-factor authentication on all Internet Banking Apps, WhatsApp, Social Media and Gmail accounts.
- j. All officers / staff must be guided on compliance of cyber security measures at personal smart appliances level.

* * * * *