Subject: **Advisory – Prevention Against Installing Fake Android Applications (Advisory No. 19)**

1. **Introduction.** Malicious Android packages (APKs) are being circulated through messages (WhatsApp, Social Media and SMS). Messages are designed to attract users attention by social engineering techniques. Therefore, it is requested not to click and download malicious APKs from these links.

2. **Technical Details**

   a. **Application Names.** P-Hub Premium.apk, Pixel Tools.

   b. **Package Name.** droid. Pixels.

   c. **Type of Malware.** Over permissive File Stealing Application.

   d. **Spreading Mechanism.** Text Messages.

   e. **Malware Download Links.** Following are download links for this malicious APK.

      (1) http://tinyurl.com/y485gdjo.

      (2) http://spiceworld.rf.gd/Premium.php.

   f. **Capabilities.** The malicious APK has following capabilities: -

      1. After installation, the APK file hides itself.
      2. The application asks for location, SMS, Calls, Calls, Contacts, Accounts, Storage, Record Audio and Camera permissions.
      3. Data comprising of files, photos, SMS, Calls, Contacts and documents is uploaded to C&C server mentioned in Para 2,f(4) after regular intervals.
      4. **C & C Services**

Ser	C & C Server URL	IP address	Country
a.	https://newsbroadcastlive.ddns.net	8.23.224.108	USA

4. **Recommendations.** Following are recommended in case compromise: -

   a. Uninstall the application by going to Setting > App> Pixel Tools.

   b. Do not download and install applications from untrusted sources {offered via unknown websites / links on unknown messages}

   c. Always check app details, number of downloads and reviews section before installing and application.

d. Verify app permissions and grant only those permissions which have relevant context for the app's purpose.

e. In settings, do not enable installation of apps from "Untrusted Sources".

f. Don't click links on untrusted sites.

g. Install Android updates and patches as and when available from Android device vendors.

h. Do not download or open attachment in emails received from untrusted sources.

i. Do not use unknown Wi-Fi networks at public places