Subject: **Prevention Against Malicious Android Apps / fake Apps (Advisory No. 1)**

1. **Background.** The National Telecom & Information Technology Security Board (NTISB), working under the aegis of Cabinet Division has been mandated to ensure Telecommunication and Information Technology Security at National Level. To this end all Ministries and Departments are updated by NTISB about emerging threats in the field of Telecom and IT and necessary remedial measure are also suggested by issuing frequent advisories.

2. **Context.** A targeted campaign has been detected against the Armed forces / ISI officers through WhatsApp messages. The campaign aims at installing of a malicious chatting application (Chat Lite) on mobile phones to take full control. These malicious applications are replicas of legitimate applications (Skype, Chrome / FireFox, Safe / Free VPN, Chat Application etc) containing hidden malware inside to lure targets / users into downloading / installing. Hostile actors utilize a range of attack vectors (Websites, Ads, Social Media, Emails, SMS, Telegram and WhatsApp messages etc) to distribute malware for conducting cyber – espionage attempts.

3. **Summary of Malicious Applications**

   a. **Application Name.** Chat_lite_v16.12amm.apk

   b. **Download Link.** bulk.fun//oy

   c. **Size of Application.** 1.91 MB

   d. **Malware Type.** Over – permissive Application

   e. **Distribution Vectors.** Whatsapp, Social Media, Websites, Emails, SMS

   f. **Threat Impact.** Critical

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

   h. **Distribution Source.** Third Party Fake Websites propagated through SMS / WhastsApp

   i. **Apk Hash.** 954449f6afa8cc9414f20795f2081dc4 (MD5 Checksum)

   j. **Permissions.** The Application requires following permissions upon installation:-

      (i) Reading Contacts
      (ii) Network and GPS Based Information
      (iii) Recording Audio

(iv) Call Phone Number, reading call log, reroute outgoing call
(v) Read / received text messages (SMS, MMS)
(vi) USB Storage

4. **C&C servers**

Ser	IP address	C&C URL	IP / URL Location
a.	178.62.185.188:443	-	Netherlands
b.	82.196.5.24:443	(1) apkv5.ppadaolnwod.xyz (2) bulk.fun	Netherlands

5. **Capabilities / Modus Operandi**

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

b. As soon as the device connects to internet, **it uploads user data including IMEI number, Gmail account ID, contacts, SMS logs, geo-location, call logs & pictures to its C&C server** (ref para 3).

c. This malicious application possess **ability to bypass anti-malware solutions and analysis by virtual environment**.

d. Upon installation, **the APK icon disappears and it hides itself among android preinstalled packages** with name "**System Service**".

6. **Recommendations**

a. Do not download or click on links received from untrusted sources via SMS / Email / WhatsApp and similar communication apps.

b. FoI best practices be adopted: -

(i) Install app from Google Playstore and Apple Appstore only.
(ii) Install reputed antivirus solution and keep them updated.
(iii) Before installing apps, review app permission, details, user reviews and "ADDITIONAL INFORMATION" Section.
(iv) In settings do not enable installation of apps from "UNTRUSTED SOURCES".
(v) Avoid using unsecure and unknown wifi networks.
(vi) Use two factor authentication on all internet banking apps, WhatsApp, Social Media apps and Email accounts.