Subject: - **Cyber Security Advisory – Malicious Android Apps Targeting Users in South Asia (Advisory No. 55)**

Recently, an active malicious campaign has been identified targeting Android users in Middle East and South Asia. The malicious activity is conducted by Bahamut APT group which is a known Indian cyber mercenary. The campaign is active since Jan, 2022 and distributing malware through a fake website "thesecurevpn.com". Trojanized versions of 2x legitimate apps "SoftVPN" and "OpenVPN" are being used by threat actor through 3rd party servers (not available on Google Play Store). The malicious apps have the capabilities to exfiltrate phone calls, chat messages from popular messaging apps including Signal, Viber, WhatsApp, Telegram and Facebook Messenger.

2. **Summary of Attack**

a. **Attack Vector**. The malicious Android apps used in this campaign is delivered through website "thesecurevpn.com"; legitimate website is "securevpn.com".

b. **Detection Ratio**. 17/91

c. **Attribution**. Open Source investigation reveals similarity of malicious code used in malicious app is similar to code used in SecureChat app, attributed to Bahamut APT gp.

d. **Malware Capabilities**

(1) When malware is installed, it can remotely be controlled by Bahamut operators and can exfiltrate various sensitive data such as contacts, SMS messages, call logs, list of installed apps, device location, device accounts, device information (type of internet connection, IMEI, IP, SIM serial no), recorded phone calls and list of files on external storage.

(2) It can steal notes from the SafeNotes apps and actively spy on chat messages and information about call from popular messaging apps such as imo-Intl Calls & Chat, Facebook Messenger, Viber, Signal Private Messenger, WhatsApp, Telegram, WeChat apps.

(3) All exfiltrated data is stored in a local database and then sent to C2 server. Malware functionality include ability to update the app by receiving a link to a new version from C2 server.

3. **Mitigation**. If above mentioned malicious apps are found (installed on smart phones), following remedial measures may be opted: -

a. Disable Wi-Fi/mobile data and remove SIM card-(malware has the cap to re-enable mobile data).

b. Take a backup of personal media Files (excluding device/system apps).

c. Perform a factory reset.

d. Keep your smart phone, OS and apps updated.

e. Regularly check the smart devices/Wi-Fi data usage of apps installed on smart devices.

f. Use a reputed anti-virus and internet security software package on your smart devices.

g. Download and install software only from official app stores like Play Store or the iOS App Store.