NO.DG-II/ Cyber Advisory/4/111/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY DEPARTMENT

Karachi, Dated: 23rd May , 2025

To

1. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
2. The Chairman, Planning & Development Board Sindh, Karachi
3. The Chairman/Chairperson, Chief Minister Inspection Enquiries and Implementation Team Sindh, Karachi
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh_____
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
9. The Administrative Secretary, Government of Sindh (All). _____
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh_____.
13. The Deputy Commissioner, District _____

SUBJECT: **CYBER SECURITY ADVISORY MALICIOUS APPS FOUND ON GOOGLE PLAY STORE(ADVISORY NO. 09/2025)**

Context In March 2025, **Google** identified and removed several malicious applications from the **Play Store**, including those associated with the **KoSpy spyware** and the **Anatsa (TeaBot) banking trojan**. These apps, often disguised as utility tools like file managers or security applications, posed significant threats to user privacy and device security.

2. **Technical Details**

a. **KoSpy Spyware.** Attributed to **North Korean** groups APT-37 (ScarCruft) and APT-43 (Kimsuky), KoSpy can collect extensive data, including SMS messages, call logs, location, files, audio recordings, and screenshots. It has been distributed through fake utility apps such as Phone Manager, File Manager, Smart Manager, Kakao Security, and Software Update Utility.

b **Anatsa (TeaBot) Banking Trojan** Disguised as a file manager and document reader, this trojan targets banking applications to steal credentials and financial information It has been downloaded over 220.000 times, highlighting its Widespread impact.

3. **Recommendations**

a. Immediately remove any of the identified malicious apps from your device.

b. Stick to trusted sources and verify app legitimacy, before installation.

C Avoid downloading apps from unknown developers or those requesting excessive permissions.

d Enable Google Play Protect to automatically detect and prevent the installation of harmful applications,

4. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.

(DR.RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II
0310-2131415

A copy is forwarded for information and necessary action to: -

1. AS(Staff) to Chief Minister Sindh, Karachi.
2. The Assistant Secretary (NTISB), Cabinet Secretariat, Cabinet Division (NTISB), GoP.
3. PS to Chief Secretary, Sindh.
4. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
5. Staff Officer to S&IT Department, Govt. of Sindh, Karachi.
6. Webmaster, for uploading the advisory on url: *https://www.sindh.gov.pk/*