No.E&A (Agri)6-334/2023
GOVERNMENT OF THE PUNJAB
AGRICULTURE DEPARTMENT

Dated Lahore, the 11th January, 2023

To

1. The Director General Agriculture (Ext. & A.R.), Punjab, Lahore.
2. The Director General Agriculture (Field) Punjab, Lahore.
3. The Chief Scientist Agriculture (Research), Ayub Agricultural Research Institute, Faisalabad.
4. The Director General Agriculture (WM), Punjab, Lahore.
5. The Director General, PW & QC of Pesticides, Punjab, Lahore.
6. The Director General, Soil Survey of Punjab, Multan Road, Lahore.
7. The Director of Agricultural Information, Punjab, Lahore.
8. The Director of Agriculture, Crop Reporting Service, Punjab, Lahore.
9. The Chief, P&E Cell, Agriculture Department, Lahore.
10. The Director of Agriculture (E&M), Punjab, Lahore.
11. The Chief Coordinator, RAEDC, Vehari.
12. The Director of Floriculture (T&R), Punjab, Lahore.
13. The Director, Punjab Institute of Agriculture Marketing (PIAM), Lahore.
14. The Managing Director, Punjab Seed Corporation, Lahore.
15. The Registrar, University of Agriculture, Faisalabad.
16. The Chief Executive, Punjab Agricultural Research Board, Lahore.
17. The Registrar, Arid University of Agriculture, Rawalpindi.
18. The Director, Market Committee Provincial Fund Board, Lahore.
19. The Registrar, Muhammad Nawaz Sharif University of Agriculture, Multan.
20. The Chief Technical Advisor, Agriculture Delivery Unit (ADU), Lahore.
21. The Secretary Agriculture Commission, Lahore.
22. The Chief, Sugarcane Research & Development Board, Faisalabad

Subject:- **CYBER SECURITY ADVISORY – MALICIOUS ANDROID APPS TARGETING USERS IN SOUTH ASIA (ADVISORY NO.55)**

I am directed to refer to the subject noted above and enclose herewith a copy of letter No.SO(FG)3-72/2021 (Vol-II), dated 29.12.2022 alongwith its enclosure received from Section Officer (FG-I), Government of the Punjab, S&GAD is forwarded for information and strict compliance.

SECTION OFFICER (GENERAL)
Ph. No.99210505

CC.

1. All Section Officers/Senior Law Officer & Assistant Director (Stat.), Stat. Cell, Agriculture Department.
2. PS to Secretary Agriculture.
3. PS to Special Secretary Agriculture.
4. PAs to All Additional Secretaries / Deputy Secretaries, Agriculture Department.

No.SO(FG-I)3-72/2021 (Vol-II)
GOVERNMENT OF THE PUNJAB
SERVICES &GENERAL ADMINISTRATION DEPARTMENT
(I&C WING)

Dated Lahore, the 29th December, 2022

Diary No. 8149
Date 05-01-23
Agriculture Deptt.
Civil Secretariat Lahore

1. The Senior Member Board of Revenue, Punjab.
2. The Chairman, Planning & Development Board, Punjab.
3. The Additional Chief Secretary, Government of the Punjab, S&GA Department.
4. The Additional Chief Secretary, Government of the Punjab, Home Department.
5. All the Administrative Secretaries, Government of the Punjab.
6. The Inspector General of Police, Punjab.
7. All the Divisional Commissioners, Punjab
8. The Chairman, Punjab Information & Technology Board, Punjab.
9. All the Deputy Commissioners, Punjab.

DS (P)

SS Agri	
AS (A)	
AS (P)	✓
AS (TF)	
Chief P&EC	
PO	
PS	

Subject: **CYBER SECURITY ADVISORY – MALICIOUS ANDROID APPS TARGETING USERS IN SOUTH ASIA (ADVISORY NO.55).**

SO(FG)

Kindly refer to the subject cited above and find enclosed herewith a copy of letter No.1-5/2003 (NTISB-II) dated 22.12.2022 received from Assistant Secretary-II (NTISB), Government of Pakistan, Cabinet Secretariat, Cabinet Division, (NTISB), Islamabad for necessary action and further distribution to field formation for compliance.

PA to [illegible] Diary No. 88 Date 5-1-....

E & A Section
Diary No. 93
Date 10-1-23
Govt. of the Punjab
Agri. Deptt.

29.12.22
ZARVA SADIQ, PMS
SECTION OFFICER (FG-I)

Pl circulate
9/1
KS

Copy:

1. Assistant Secretary-II (NTISB), Government of Pakistan, Cabinet Secretariat, Cabinet Division, (NTISB), Islamabad w/r to his letter referred above.
2. PSO to Principal Secretary to Governor Punjab, Punjab.
3. PSO to Principal Secretary to Chief Minister, Punjab.
4. PS to Secretary (I&C), S&GAD.

9/1/2023
S/c

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad, the 22nd December, 2022

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 capability to 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 connected devices.

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

4. For any query or reporting malware/cyber incident, please forward the same on following email addresses: -

a. Falcon1947@proton.me

b. asntisb2@cabinet.gov.pk

5. Kindly disseminate the above message to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

(M. Usman Tariq)
Assistant Secretary-II
Ph# 051-[illegible]

All Secretaries of Ministries / Divisions of the Federal Government and Chief Secretaries of the Provincial Governments.

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad