GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad 30 July, 2021

02 AUG 2021

M(Admin/HR)

M(I.T.)

A.S(Rev. Div.)

Subject: **Cyber Security Advisory - Pegasus Cyber Espionage and Intelligence Tool of NSO (Advisory No. 49)**

1. An international investigation has revealed **database of mobile numbers** of famous business executives, politicians, civil & military official and journalists of different countries including Pakistan. This investigation provides evidence of mobile phone surveillance, espionage and cyber intelligence operations of **flagship military-grade** malware named **Pegasus** developed by Israeli surveillance technology firm **The NSO Group**. Pegasus malware delivers complete intelligence for security operations including **stealth monitoring, persistence, communication hooks** and **extracting information** which is forwarded/ uploaded to adversary servers. **Agent** is covertly installed on victim's device through remote installation. In view of this, an advisory is attached at **Annexure-A** to sensitize all concerned and to adopt recommended preventive measures.

2. Forwarded for information and dissemination to all concerned, please.

Major
(Imran Nazir)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of 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. Secretary, NTISB, Cabinet Division, Islamabad
7. Deputy Secretary, NTISB, Cabinet Division, Islamabad
8. Director (IT), Cabinet Division, Islamabad

Just Send to FATE wing

CBO/Chief (C.I.T)

SSL (IT-II)

C(IT)

Annex-A

Cyber Security Advisory - Pegasus Cyber Espionage and Intelligence Tool of NSO (Advisory No. 49)

1. **Context.** An international investigation has revealed **database of mobile numbers** of famous business executives, politicians, civil & military official and journalists of different countries including Pakistan. This investigation provides evidence of mobile phone surveillance, espionage and cyber intelligence operations of **flagship military-grade** malware named **Pegasus** developed by Israeli surveillance technology firm **The NSO Group.** Pegasus malware delivers complete intelligence for security operations including **stealth monitoring, persistence, communication hooks** and **extracting information** which is forwarded / uploaded to adversary servers, through remote agent installation. **Agent** is covertly installed on victim's device through remote installation using the following techniques: -

   a. **Over-The-Air (OTA)** called **zero click**
   b. **Social Engineering**
   c. Tactical network element using **BTS**
   d. **Physical access** to phone

2. **Pegasus Anonymization.** Pegasus maintains delicate anonymization as under: -

   a. Minimal battery, memory and data consumption.
   b. Self-destruction if there is a risk of being exposed or communication has not taken place for a long time.
   c. The NSO Firm has **Pegasus Anonymizing Transmission Network** which is deployed against each customer to avoid traceback.

3. **Detection.** **Infection detection** is *not possible.*

4. **Mobile Infection Detection Technique.** A user may check infection of his / her mobile phone via Pegasus or any other malware by using **MVT (Mobile Verification Toolkit).** MVT is a forensic tool to detect signs of infection in smartphones. Users are advised to install MVT on a standalone PC. After installation, both backup of user's mobile data and running MVT be operated in offline environment. Use of Offline PC will prevent user's data from online / internet exposure.

5. **Recovery Technique from Pegasus.** Only way to get rid of Pegasus malware is to discard infected device completely and change passwords of all applications and accounts.

6. **Recommended Defensive Measures**

a. **User Level**

(1) Mobile devices of all important officials be replaced with **clean devices** and **multi factor authentication** be activated on new accounts.

(2) Social messengers like **Whatsapp** etc not to be used for official work/ correspondence.

(3) Extreme precaution for likely call and messages interception to be exercised during **travel outside country.**

b. **Organization Level**

(1) Awareness campaign regarding Social Engineering and Phishing Email attacks be organized for high-profile government officials.

(2) Mobile jammers be installed at highly sensitive areas and during sensitive meetings.

(3) Scanning of all official mobile phones for finding **Indicators of Compromise (IOCs)** highlighted in the recent campaign.

7. **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email addresses for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk

8. Forwarded for perusal and dissemination of information to all concerned and under command, please.