Cyber Security Advisory – Apple Threat Notification against State Sponsored Cyber Attack (Advisory No. 80)

Context Recently, apple has **generated alerts** to inform its user who have likely been **targeted by NSO Pegasus software**. Apple threat notifications are designed to **inform and assist users** who have been **likely targeted** by state-sponsored attackers; however, Apple has not disclosed the means of identification of users which have likely been targeted. In this regard, Apple has already issued updates to counter the threat and sued Israeli company NSO for attacking iOS users.

2. **Apple Information Dissemination Mechanism.** Apple activity monitors its own manufactured devices for signs of compromise. In the recent event, Apple has informed its customers by following mechanism: -

a. iMessage
b. Email
c. Alert on apple ID **(appid.apple.com)**
d. An apple user can **check the validity of iMessage** by visiting **appid.apple.com.** The presence of message at **appid.apple.com** will prove legitimacy of iMessage.

3. **Recommendations / Security Steps for users.** Above in view, users are requested to adopt following measures: -

a. Immediately **upgrade to iOS 15.1 or iOS 15.1.1** (for IPhone 12 or above) which covers security update related to above mentioned attack.
b. It is advised to **protect devices with strong passcodes** and **use two factor authentication** on Apple ID.
c. Install apps from official Apple Store only to avoid malware / infection.
d. Use **anonymity based solutions** (over internet while surfing) and **mask identity** of key appointment holders / individuals.
e. High ranking officials should not purchase phones / SIMs / internet devices on their own names / CNIC numbers / thumbprint.
f. In phonebook / contact list, never save contacts with ranks / appointments / organization name etc with individuals' names.
g. Official identity should never be revealed and sensitive information should never be shared through phone.
h. Always disable location from Apple devices.
i. Strictly avoid using phone at sensitive locations / meetings.