F. No. 1-5/2003/24(NTISB-II) Islamabad, the 13 February, 2024

Subject: - **Cyber Security Advisory – Apple Products Zero Day Attack Latest Mitigation Measures (Advisory No. 02)**

Introduction. Recently, Kaspersky has introduced a lightweight method called iShutdown to detect zero click spywares e.g. Pegasus, Reign and Predator on Apple iOS devices.

2. **Technical Details**. Kaspersky analyzed Shutdown.log file present within the sysdiagnose archive further identifying anomalies during reboots linked to Pegasus. Entries in the log file indicated reboot delays caused by sticky spyware processes. The log file also showed a common infection path (/private/var/db) shown by other iOS malware families.

3. **Mitigation Measures**. To Safeguard against advanced spyware on iOS, following recommendations must be incorporated:

a. Reboot the device daily/regularly as it causes hindrance for attacker by compelling them to infect devices each time after reboot.

b. Enable lockdown mode on the device to block iOS malware infection.

c. Disable iMessage and FaceTime on the device which can serve as an attractive exploitation vector.

d. Avoid clicking on suspicious links received in messages, SMS other messengers or emails.

e. Regularly check backups and sysdiags (system diagnosis) for potential malware.

f. Install latest OS version and keep all applications updated.

g. Additionally, use Kaspersky's new self-check spyware detection tool available on GitHub. (https://www.github.com/KasperskyLab/iShutdown)

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