Subject: - **Cyber Security Advisory – Protective Measures against Hermit Spyware (Advisory No. 30)**

1. **Context**. An **Android / iOS** family spyware **"Hermit"** has recently been identified. Reportedly, the spyware is developed by RCE Lab, Italy. Hermit spyware has been used by government of **Italy, Kazakhstan** and **Syria** to target their opposition, business executives, human rights activists, academics and government officials. **Use of Hermit by HIAs** against own **civil / military leadership**, other critical government appointment holders and business executives etc cannot be ruled out. Modus operandi and protection measures against Hermit have been elaborated in ensuing paras.

2. **Modus Operandi**

a. **Installation Process**. Hermit spyware is installed in **victim's mobile** with the help of an insider of an ISP through **push message notification.** In this type of tactic, victim's mobile network is disappeared and a message from authentic ISP is sent to victim's mobile number to regain network access. As the victim's network disappears, therefore, victim is left with no option other than to open the malicious link to restore his / her network connectivity; and clicking on this malicious link installs Hermit spyware. After installation, Hermit extracts user's personal data and uploads to its C&C servers.

M (IR-Ops)	
M (IR-P)	
M (Cus-Ops)	
M (Cus-P)	
M (Admin/HR)	✓
M (IT)	✓
M (FATE)	
M (Legal)	
M (Reforms)	
M (Legal & Act. Cus)	
M (Acc. & Audit)	
Addl. Secy (Rev.Div.)	✓
SA / SPS	

b. **Use of App Masquerading Technique**. App masquerading technique for popular apps such as **Facebook, WhatsApp** and **Instagram** may also be used to compromise the targeted users.

3. **Features – Hermit Spyware**

a. Hermit is as sophisticated as **Pegasus** spyware developed by NSO and Gamma Group. It can attack target and covertly performs set of actions such as **infiltrate in victims' device, monitor & capture data** and send **stolen data to its C&C server**.

b. Hermit remains **undetected** by an anti-malware solution as it masks various **legitimate certificates** from Android and iOS trusted platforms.

c. Hermit requires user's action to complete its installation. **Without user's action, the spyware is unable to extract personal data.**

(PR)

4. **Recommendations**. With sophisticated data collection capabilities of Hermit and the fact that mobile devices are carried all the time, therefore, it is obvious that mobile devices are perfect target for surveillance. Following are few recommended measures to safeguard against the spyware: -

a. **Update your Phone and Applications**. Operating systems and apps often have **vulnerabilities** that need to be **patched**. Always update operating system and apps to ensure that exploits are resolved.

b. **Don't Click on Unknown Links**. One of the most common way for an attacker to **deliver malware** is by sending a **message pretending to be a legitimate source**. Don't click on links, especially when the source is unknown.

c. **Don't Install Unknown Applications**. Exercise caution when installing unknown apps, even if the source of app seems **legitimate**.

d. **Periodically Review your Applications**. Sometimes malware can change **settings** or install **additional content** to mobile phone. Always check mobile phone periodically to ensure that nothing unknown has been added.

5. For any query or reporting malware, please forward the same on following email addresses: -

a. eagle1978@mail.com
b. falcon098@writeme.com
c. asntisb2@cabinet.gov.pk