Subject: **Prevention Against Malicious North Korean Cyber Activity (Advisory No 01 - January, 2018**

1. **Background.** Reliable reports reveal release of joint technical alerts on malicious North Korean cyber activity, referred as **Hidden Cobra.** North Korea is actively targeting the media, aerospace, financial, and critical infrastructure sectors. Tools and capabilities used by Hidden Cobra actors include **DDoS Botnets, keyloggers, RATs, and wiper malware.**

2. At least **94 static** and **dynamic IP addresses,** registered across various countries have been identified during the analysis of **Hidden Cobra.** Some of these **IP** addresses belong to **Pakistan.**

3. **Recommendations**

a. Perform a comprehensive network scan to Identify systems that may have been compromised by North Korean hackers.

b. Detailed analysis of compromised systems be carried out to identify potential threats and to further enhance security.

c. Update and install latest security patches for OS and applications.

d. Disable all unnecessary services and ports.

e. Install Anti-virus and firewalls to protect critical digital infrastructure.