**Subject:** **Cyber Security Advisory – Prevention Against Kill Net Russian APT, (Advisory No. 24)**

**Context**. Kill Net is a Russian APT group that has been targeting Pakistan's military and civil setups with numerous attack vectors including DDoS attack. Detailed profile, modus operandi of APT Kill Net and recommended preventive measures against the kill Net APT group are mentioned in ensuing paras.

2. **Profile of Kill Net Russian APT**. A Pro-Russian APT group operating from Kremlin, Russia and active since January, 2022. Kill Net is known for causing DDoS campaigns against USA and other Ukraine allies (NATO countries) in the backdrop of Russia-Ukraine war. Kill Net has often targeted Pakistan's military and civil setups.

3. **Modus Operandi**. Kill Net uses DDoS and brute, force dictionary attacks as main weapons to cause mass service disruption of vulnerable public facing CII. In most cases, Kill Net DDoS attacks have caused at short downtime for victims. However, it leads to embarrassment for nations globally.

4. **Preventive Measures**. An APT group may frequently change its techniques, tactics and procedures. However, recent DDoS attacks warrant to adopt proactive preventive measures against DDoS and other cyber-attacks. Few preventive measures (but not limited to) are as follows: -

a. **Anti-DDOS Measures (Administrator Level)**

(1) Monitor networks including file hashes, file locations, logins and unsuccessful login attempts.

(2) Use reputed firewalls, IPS/IDS and SIEM solutions.

(3) Use separate servers/routing for offline LAN and online networks.

(4) Restrict incoming traffic and user's permissions to maximum extent by implementing system hardening at OS, BIOS and application level.

(5) Allow internet access to specific users on need basis and restrict data usage/ applications rights.

(6) Verify software and documents before downloading via digital code-signing technique.

(7) Implement MFA in mailing systems administrator controls and other critical systems.

(8) Always maintain back up of critical data periodically.

(9) Regularly change passwords at administrator level.

(10) Regularly patch and update all OS, applications and other technical equipment.

(11) Ensure anti-DDOS service is provided with website domain hosting from ISP.

(12) Enable firewalls including Next Gen Firewall (NGF), Web Application Firewall (WAF) and Network Based Firewall etc.

(13) Enable SIEM and event logging 24/7 to detect anomalies in internet usage and traffic spikes.
(14) Ensure fragmentation and multi-content delivery network (MCDN) to minimize attack surface.
(15) Filter incoming traffic and block suspicious traffic after deep packet inspection.
(16) Timely update all apps and services including patches.
(17) Ensure hardening of all IT equipment at all levels.
(18) Keep strong passwords on BIOS, OS level, drives (via bit locker) and documents.
(19) Use adequate website and application development practices including defense against brute force attacks.
(20) Ensure zero trust model and develop and incident response plan including contingency plan.
(21) Conduct regular pen testing along with red teaming practices and internal phishing email awareness practices.
(22) Ensure the data backups are regularly dumped and stored in multiple offline locations while discourage storing sensitive data over the cloud.

b. **Blocking of Malicious Domains/ URLs**. Block all malicious domains, URLs and hashes of documents at firewall/network including APT Kill Net. Have access to latest hacking threat intelligence forums and feeds to remain update with attacker's innovations regarding evasion techniques.