**MAY 2024 CYBER MIR**

In the month under review, the DHQ and MORAN CSOC team recorded incidents of insecure web configurations including unnecessary PORTs exposure on the MOD mail server and missing Domain Name System Security Extension (DNSSE) on the ndu.ac.ke domain. Further, high number of vulnerability cases were recorded due to missing critical security updates in internal systems including at Master Chief Clerk Office, StratComm and CT Offices Consequently, malicious external IP addresses made network intrusions attempts Thro phishing campaigns and vulnerability exploitations.

**Nationally**

Kenya’s Department of Immigration and Citizen Services is evaluating Google Cloud’s CyberShield solution and Mandiant expertise to strengthen the defense of its eCitizen platform IOT defeat cyberthreat capabilities, protect web-facing infrastructure and helps teams develop skills and processes that drive effective security operations.

**Globally**

Global Threat landscape highlights an increase in sophisticated cyber-attacks by the cybercriminals targeting vulnerabilities IOT steal sensitive data, disrupt essential services through the distributed denial-of-service (DDoS) attack and carry-out Ransomware attacks.

**COMMENT**

Both the DHQ and MORAN CSOC teams carried out the recommended necessary actions IOT mitigate the attendant risk of vulnerability exploitations and ransomware targets.

MOD Pers advised to observer cyber hygiene practices IOT evade phishing campaigns that paves way for the vulnerability exploitations leading to further attacks.