MAR 2024 CYBER MIR

In the month under review, the DHQ and MORAN CSOC team recorded incidents of malware detection in STRATCOM and CT Systems. Phishing campaigns and vulnerability exploitation attempts to gain admin privileges within the internal systems imaged as the most prevalent cases. Further, events of sudden increase in system CPU Usage and server memory critical level were reported.

Nationally

On 21 Mar 24, the Communications Authority of Kenya (CAK) and the National Computer and Cybercrimes Coordination Committee (NC4) launched the National Cyber Risk Assessment Report. The team identified a framework of assets and resources that could be vulnerable to cybercriminals.

Globally

The US government, through the joint advisory from the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), published new distributed denial-of-service (DDoS) attack guidance for public sector entities to help prevent disruption of critical services.

COMMENT

Action by the DHQ CSOC team to detect and remove malware, patch software vulnerabilities, and enhance pers cyber-awareness skills will reduce the attendant risk of vulnerability exploitations and ransomware targets.

Phishing campaigns targeting users are identified as the most common initial vector for attackers to exploit vulnerable resources. MOD Pers advised to practice proper cyber hygiene practices IOT evade phishing campaigns and protect user data.