SPET 2022 CYBER MIR

In the month under review, the DHQ CSOC team detected various intrusions by malicious actors directed to various machines on the MOD network. In addition it was observed that there was rampant use of infected external drives and use of unpatched and vulnerable applications within the ICT environment. Further, several vulnerabilities were discovered in the Windows Server Operating System that could allow attackers to compromise our systems.

Nationally, the former President of the Republic of Kenya HE Uhuru Kenyatta inaugurated the Kenya National Digital Master Plan( 2022\_32) that will guide the structured delivery of ICT in Kenya for the next 10 years. The former head of state also commissioned the roll- out of the Coding Curriculum that has been approved by Kenya Institute of Curriculum Development and to be implemented countrywide in both Primary and secondary schools countrywide.

Globaly, phishing actors are abusing LinkedIn’s Smart Link feature to bypass email security products and successfully redirect targeted users to phishing pages that steal payment information. Smart Link is a feature reserved for LinkedIn Sales Navigator and Enterprise users, allowing them to send a pack of up to 15 documents using a single traceable link.

Comments

The use of software and applications with known vulnerability in our systems allows threat actors to bypass own security measures in turn leading to unauthorized access to restricted files. It is recommended that the IR team and the CSOC admins ensure that all software is updated to the latest edition to avoid malicous intrusion.

The ongoing linkedn phishing campaign creates an unpredictable and hazardous online environment and will result in cyberattacks in the MOD systems. It is recommended that Pers observe the Cyber Hygiene guidelines issued and the CSOC team be proactive in identifying suspicious and malicious cyber activities.

