PRESS STATEMENT

31st December 2018

ADVISORY BY THE COMMUNICATIONS AUTHORITY OF KENYA (CA) ON THE EMOTET MALWARE

The Communications Authority of Kenya (CA), through the National Computer Incident Response Team Coordination Centre (National KE-CIRT/CC), has detected a malware targeting network systems, called *'Emotet'*.

The National KE-CIRT/CC has so far detected 11 cases targeting local institutions and has engaged the affected organizations accordingly.

Emotet is an advanced and destructive banking Trojan affecting network systems. *Emotet* is notorious for its modular architecture, persistence techniques, and worm-like self-propagation that rapidly spread network-wide infection. A polymorphic Trojan, *Emotet* can evade typical signature-based detection and has several methods for maintaining persistence, including auto-start registry keys and services.

*Emote*t is disseminated through malicious email attachments or links posing as invoices, payment notifications, bank account alerts, etc., that use branding seemingly coming from legitimate organizations. Once downloaded, *Emotet* establishes persistence and attempts to propagate the local networks through incorporated spreader modules.

Emotet may result in temporary or permanent loss of sensitive or proprietary information, disruption to regular business operations, financial losses related to restoration of systems and files, as well as the potential harm to an organization's reputation.

The Authority wishes to advise the public and organizations to put in place the following measures to limit the effect of *Emotet* and similar malspam, if they believe their systems may be infected with the malware:

i. Immediately scan and isolate the infected computer from the network
ii. Once isolated, proceed to clean and patch the system
iii. Consider proactive protection against future malware spam infections
iv. Adhere to general cybersecurity best practices

The National KECIRT/CC will continue to monitor the prevalence of this malware in the country and provide stakeholders with the necessary assistance to mitigate this threat.

About National KE-CIRT/CC

The National Kenya Computer Incident Response Team - Coordination Centre (National KE-CIRT/CC) is a multi-agency collaboration framework which is responsible for the national coordination of cyber security. It is Kenya's national point of contact on cyber security matters in accordance with the Kenya Information and Communications Act, 1998.

The National KE-CIRT/CC detects, prevents and responds to various cyber threats targeted at the country on a 24/7 basis, and coordinates response to cyber security matters at the national level in collaboration with relevant actors locally and internationally.

Members of the public are advised to contact the National KE-CIRT/CC via the email address incidents@ke-cirt.go.ke or through the dedicated hotlines +254 703 042700, +254 730-172700 to report an incident or seek advice on cyber security.

Issued by,

Tom M. Olwero
For: DIRECTOR-GENERAL