PRESS STATEMENT

ADVISORY BY THE COMMUNICATIONS AUTHORITY OF KENYA ON SUPPLY CHAIN RISKS IN THIRD-PARTY SOFTWARE.

The Communications Authority of Kenya (CA), through the National Computer Incident Response Team Coordination Center (National KE-CIRT/CC), wishes to issue an advisory on supply chain risks in third- party software.

This follows a growing global concern and trend that shows, cyber criminals going forward will exploit the vulnerability within the supply chains to hit their targets.

Though Kenya has not been adversely affected by such attacks as at now, the trend depicts a serious concern in cybercrime management and thus a precaution should be taken when dealing with outsourced products and personnel. The advisory therefore is to enable ICT users to make informed and risk-free decision on the choices of their products by engaging Cybersecurity experts.

A supply chain attack, also called the value-chain or third-party attack occurs when someone infiltrates a system through an outside partner who validly has access to the systems and data. The attacker takes advantage of the inherent trust between users and their software providers.

It is estimated that a majority of cyber-attacks originate from the supply chain or from the external parties exploiting security vulnerabilities within the supply chain. Supply chain attacks are now moving into the mainstream of cybercrime, and with a number of successful attacks in 2016 and 2017, cyber criminals will focus on this method in 2018 and beyond.

The trend is gaining momentum with the increased offers of free anti-malware products by vendors. The free anti-malware are used as a bait to lure the unsuspecting users, while the real intention is to have the anti-malware installed into a system, then use it to capture personal and confidential data. Such vendors later monetize the data collected or use it to their political or business advantage. This trend applies not only to anti-malware solutions but also any other third party software.

In most instances, vendors introduce complex disclosure statements that are in part designed to obscure intent as to what data is being collected and whether it can be sold or any other breach.

The Authority is therefore advising the public as follows:

a) That end users treat free or low cost cyber security software as potential threats and where possible refrain from the usage. They should strive to determine their monetization methods and their policies. To this end users should endeavour to read the terms and conditions of their usage however lengthy they are.
b) That organizations and government institutions properly vets software vendors in order to ascertain any concealed motive that might work against their interests especially with

products interacting with organization's critical infrastructure. Products or vendors with tainted history should be dealt with as a risk, and constant reviews carried out.

c) Kenyan ICT consumers should be concerned about the safety of their data more than ever before. Cyber criminals have changed tact and are now using third party software to deliver threats to unsuspecting users in an attempt to comprise their personal data. Consumers should thus avoid "they will do it" approach but should rather collaborate with the-service providers in securing the services.

About National KE-CIRT/CC

The National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC) based at the Communications Authority of Kenya (CA) is Kenya's national cyber security trusted point of contact and its mandate is to offer technical advice on cyber security matters nationally and coordinating response to cyber incidents in collaboration with relevant stakeholders locally, regionally and globally.

Members of the public are therefore advised to contact the National KE-CIRT/CC via the email address incident@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,

Christopher K. Kemei
Ag. DIRECTOR-GENERAL