COMMUNICATIONS SECTOR CYBER SECURITY POSTURE FOR THE PERIOD JANUARY 2021 TO DECEMBER 2021

1.0 Introduction

Information and Communications Technology (ICT) is an integral component of the Ugandan economy since it is an engine for the operations of many businesses, organizations, and the government. As a result, the infrastructure that supports ICT is often prone to attack by individuals intending to steal, expose, alter, disable, or destroy information through unauthorized access to it.

To better address these risks, Uganda Communications Commission (UCC), with support from International Telecommunications Union (ITU), established the Computer Emergency Response Team (CERT) in June 2013 as an initiative to:

i. Support coordinated response to sectoral cyber incidents and investigations.
ii. Provide guidance to owners and operators of critical information infrastructure.
iii. Raise awareness levels of cyber security within the sector.

The CERT further provides:

i. Proactive services in form of advisory security alerts and vulnerability assessments.
ii. Reactive services when security incidents occur, to minimize the damage.

iii. Digital forensics services, including cyber or computer related crime investigations.
iv. Situational awareness, which involves spreading awareness of the different kinds of cyber threats, and to focus attention on cyber security, making the average user knowledgeable about different threats and malicious behaviours.

Cyber criminals use the following vectors to propagate cyber-attacks:

i) Malware: a computer program that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
ii) Phishing: the fraudulent practice of sending emails purporting to be from a reputable company or organization to entice individuals to reveal personal information, such as passwords, Personal Identification Numbers (PIN) and credit card numbers.
iii) Ransomware: a malicious computer program designed to block access to a computer system until a certain sum of money has been paid.
iv) Vulnerability: a flaw or weakness in a computer system that weakens the overall security and can be exploited by cyber criminals to gain authorized access to the system.

2.0 Methodology Used to Assess Cyber Security Posture

Three Cyber Threat Intelligence (CTI) sources were used to obtain the information used in this assessment:

i) Indicators of Compromise: An artifact observed on a computer network or in a computer's operating system that, with high confidence, indicates presence of an unauthorized intrusion. UCC receives this information from partner Internet research and security entities, and it helps isolate which infrastructure within Uganda's Internet network is infected with malware and thus vulnerable to cyber-attacks.

ii) Sensor's network: UCC has deployed a network of sensors within the Internet Service Providers (ISP) in Uganda. These sensors help gather information on various attacks directed at those networks as well as detect any suspicious programs that are aimed at compromising the security of these systems.

iii) Public information on vulnerabilities: Software and hardware companies often publish known vulnerabilities so that their customers can take necessary precaution to minimize cyber-attacks. UCC aggregates and visualizes this information to generate reports on how many systems in the ISP network infrastructure are affected by these vulnerabilities.

3.0 General Observations

For the period January to December 2021, the following was observed through the information gathered and analyzed from various sources:

i) There is a general increase in the frequency, scale, and level of sophistication of the malicious activity aimed at disrupting the operations of computer systems in the Ugandan Internet space.

ii) Due to COVID-19 lockdown, many people were working from home and using the Internet. There was an upsurge in attacks on personal devices targeting users that were connecting directly to the Internet without any security considerations or protection for their devices and networks.

iii) Ransomware was the most significant threat, given the potential impact on the operations of the ISPs and their customers.

iv) There was an increase in registration of malicious websites under the ".ug" domain - a 77% increase from 13 domains in 2020 to 59 domains in 2021.

4.0 Interpretation of Data

i) Compromised computer networks

The average number of infections observed monthly across all monitored ISP networks was 421,024. As shown in *Figure 1* below, the highest infections were seen in the month of January 2021 (over 140,000). This was attributed to the COVID-19 pandemic that forced most of the workforce to work from unsecure environments at home. Many cyber criminals took advantage of the pandemic to send malicious computer programs to unsuspecting people through email. However, a steady decline in infections was observed towards the end of 2021 as many people resumed working from offices.

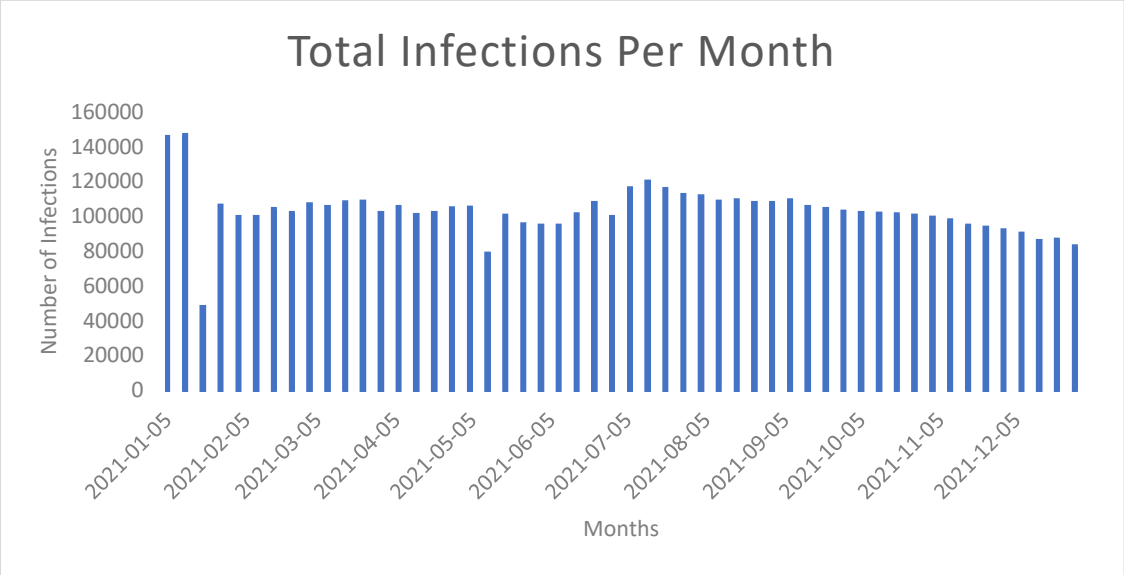

Figure 1: Infections per month

ii) Infections per ISP

The number of users on the network was taken into consideration - the bigger the number, the wider the landscape susceptible to cyber-attacks. A malware type *Cooee* was responsible for most infections. *Cooee* attacks android phones and displays unsolicited annoying advertisements, slows down devices, and installs additional applications without the user's consent. It also makes files installable on Windows even if they are not, hence damaging them and the operating system.

iii) Malware trends

The predominant malware in the Ugandan ISP networks was the *Cooee* malware that was responsible for 39.4% of the infections in the period under assessment. This malware type at times comes pre-installed on some Android devices, which allows for the installation of other malicious applications.

iv) Data collected from sensors

It was observed that small executable malicious programs and computer programs that operate on behalf of cyber attackers were actively prowling ISP networks trying to guess user passwords. 49,332,742 of such attacks were recorded on our sensors during this period.

As shown in *Figure 2* below, 48% of the attacks originated from Ireland while only 3% were from within Uganda.

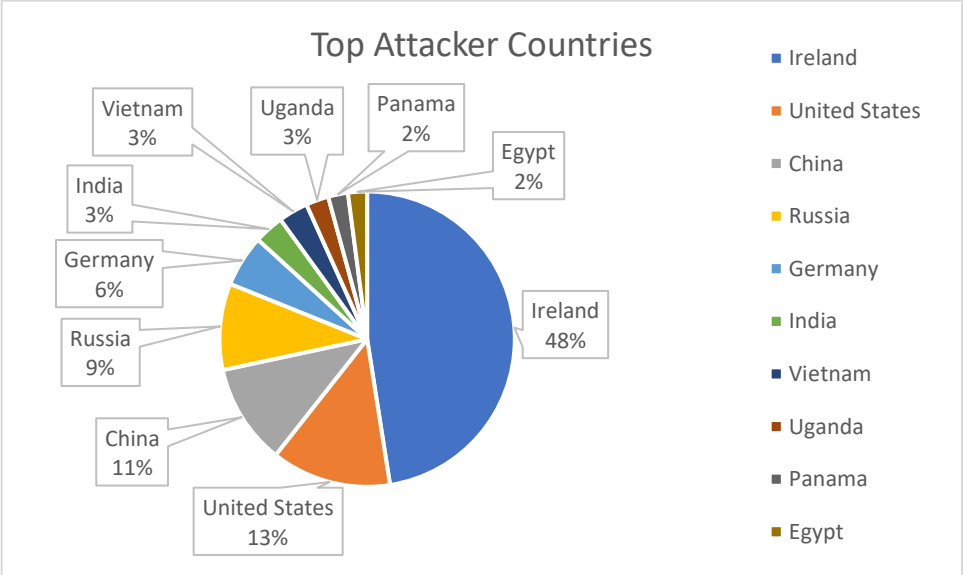

Figure 2: Top origins of attacks to ISP infrastructure

Note that the attacks received from within Uganda originated from six (6) operator networks. The individual licensed operators where notified of this activity within their networks.

v) Vulnerabilities observed

As seen in *Figure 3* below, most vulnerabilities were observed during the month of December - a total of 35,538. This rise is explained by the prevalence of a vulnerability named CVE-2018-19052 that allows a cyber-attacker to bypass the network and computer security measures and therefore obtain illegal remote access to the computers on a network.

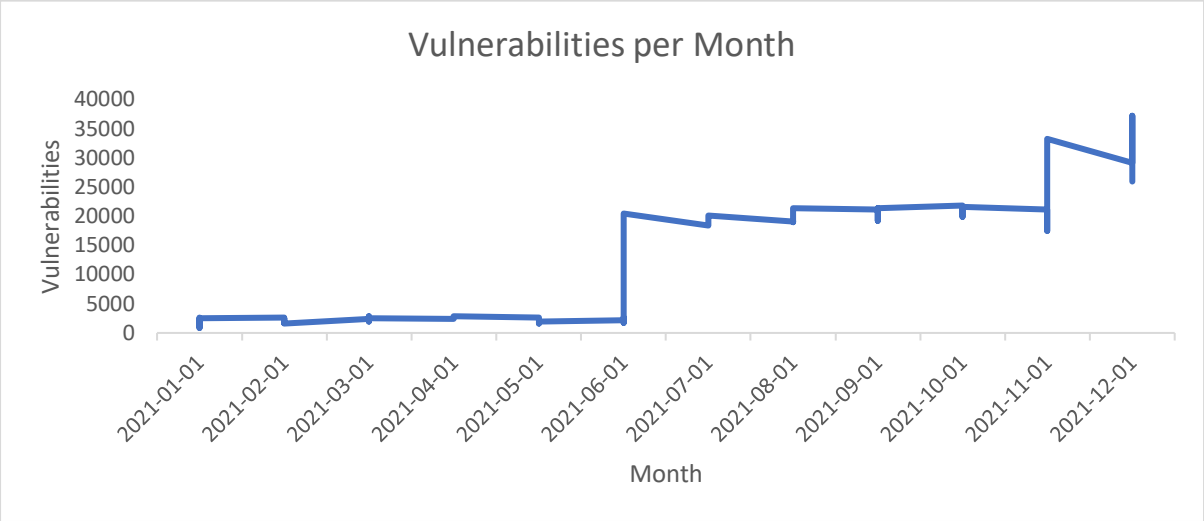

Figure 3: Vulnerabilities observed per month

5.0 Common cyber security incidents

Over the period under review, the CERT responded to 24 cyber security incidents compared to 30 incidents received during the previous year (2020). This drop in reporting is attributed to the fact that COVID-19 made it more difficult for people to report incidents directly at the CERT offices.

Figure 4 below shows the top incidents handled by CERT.

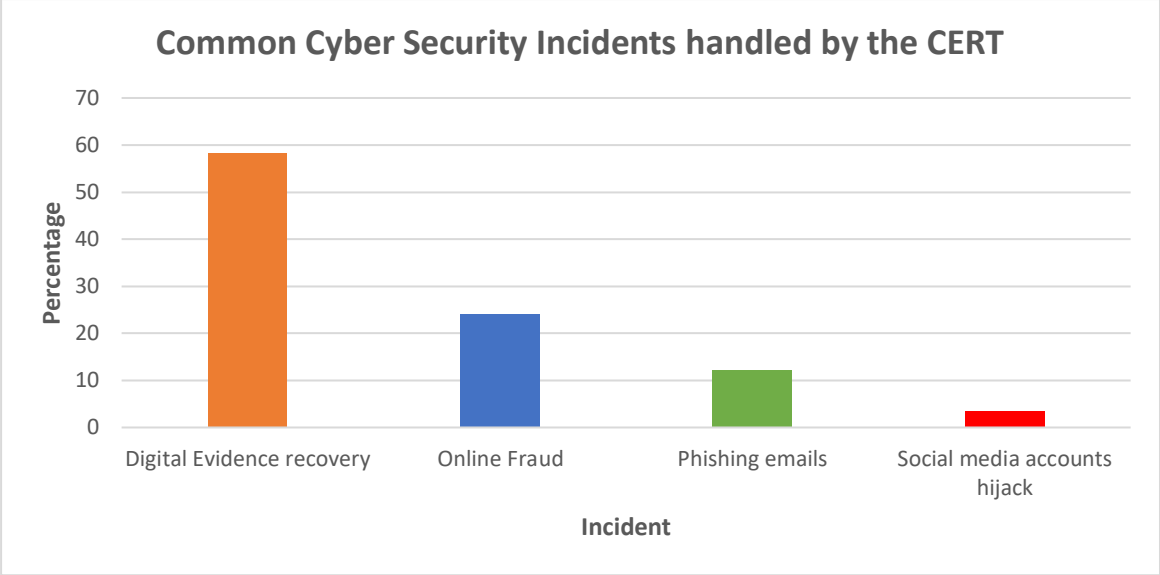

Figure 4: Cyber security incidents handled by CERT

6.0 Initiatives to improve cyber hygiene

UCC through CERT has undertaken several initiatives geared towards improving the ICT security posture as summarized in the table below:

Activities	**Jan – December 2020**	**Jan – December 2021**
Security alerts issued to operators	23	42
Advisories published on website	84	97
Indicator of compromise reports submitted to operators	110	140
Fraudulent domains suspended	13	59
Operator technical training	4	2

7.0 Future initiatives

The CERT intends to undertake the following projects to ensure constant improvement in the cyber security of the communications sector:

a) Introduction of Cyber Security Drill for operators to enhance their technical abilities.
b) Digital Financial Services (DFS) security testing facility. To be set up in collaboration with Bank of Uganda, this will enable FINTECHs

(Financial Technology Service Providers) to gain access to a platform where they can test the security of their applications and services.

c) Automate malware analysis and investigations. This will improve the process of analysing malware samples submitted to UCC.

d) Develop and implement the sector's cyber security strategy. This is ongoing and different stakeholders are being consulted about the same.