UGANDA COMMUNICATIONS COMMISSION

COMMUNICATIONS SECTOR CYBER SECURITY POSTURE REPORT FY 2023/24

Table of Contents

1 Introduction 2

2 Background 3

2.1 Terminology 3

3 Communications Sector Cyber Threat Landscape 5

3.1 Cyber Security Posture 5

3.1.1 Global Cyber Security Highlights 5

3.1.2 Uganda Cyber Security Trends 6

3.2 Cyber Threat Intelligence and Security Ratings 7

3.3 Year-on-Year Trends Analysis 8

3.3.1 Malware Infections Trend 9

3.3.2 Top Malware Infection Trend 10

3.3.3 Botnet Infections Trend 11

3.3.4 Potentially Exploited Devices Trend 12

3.3.5 Spam Propagation Trend 13

3.3.6 Year-on-Year Trends Summary 13

3.4 Analysis of FY 2023/24 14

3.4.1 Malware Infections 14

3.4.2 Malware Infections per Month 14

3.4.3 Botnet Infections 16

3.4.4 Spam Propagation 17

3.4.5 Potentially Exploited Devices 18

3.4.6 Top Malware Infections 20

3.4.7 Changes in the Malware Landscape 22

3.4.8 Critical Vulnerabilities 22

4 Current Efforts to Improve Cyber Hygiene 25

5 Way forward 27

1 Introduction

The Communications Sector plays a crucial role in Uganda's economy, supporting businesses, organisations, and government functions. However, its complex and interconnected infrastructure makes it a prime target for cyber threats that can jeopardise national security, economic stability, public safety, and health. While advancements in technologies such as cloud computing, the Internet of Things (IoT), and 5G networks drive efficiency and innovation, they also increase susceptibility to cyberattacks.

Cybersecurity is a cornerstone of the Uganda Communications Commission's (the Commission) regulatory mandate, and the annual Cybersecurity Reports underscore our commitment to safeguarding Uganda's digital landscape. This report for FY 2023/2024 delves into evolving cyber threats, vulnerabilities, and best practices for protecting critical communications infrastructure and data. The Commission collaborates with experts and industry partners to provide up-to-date insights that promote a resilient cyber ecosystem. The goal is to raise awareness, guide stakeholders in enhancing their cybersecurity posture, and fortify the sector's digital resilience, aligning with our mission to ensure a secure and trusted digital environment for all.

In collaboration with the International Telecommunications Union (ITU), the Commission established the Computer Emergency Response Team (CERT) in June 2013 to:

i Coordinate responses to cyber incidents in the communications sector.
ii Advise owners and operators of critical information infrastructure on cybersecurity best practices.
iii Raise awareness about cybersecurity.

The CERT provides:

a) **Proactive services**: Advisories, security alerts, and vulnerability assessments.
b) **Reactive services**: Minimising damage when security incidents occur.
c) **Digital forensics services**: Investigations of cyber or computer-related crimes.
d) **Situational awareness**: Spreading awareness of various cyber threats, focusing attention on security, and sensitising users to different threats and malicious behaviours to improve cybersecurity in the sector.

2 Background

Telecommunication operators in Uganda are integral to the country's modern infrastructure, playing a critical role in voice and data transmission through complex networks that handle vast volumes of sensitive information. This pivotal position makes them significant targets for cyberattacks, including data breaches, service disruptions, and other threats. Ensuring the secure operation of these networks is essential not only for maintaining reliable communication services but also for safeguarding national security and individual data privacy. Given their constant exposure to such threats, the importance of implementing robust cybersecurity measures within the sector cannot be overstated.

2.1 Terminology

Term	Definition
BitTorrent	A file-sharing protocol that distributes data and electronic files over the internet by downloading segments of a file directly from different end-user devices.
Botnet	A network of devices infected with malicious software and controlled as a group without the owners' knowledge is often used to perform malicious activities.
Botnet Infections	Devices that are compromised by botnet malware and controlled remotely by attackers.
Cyber Threat Intelligence (CTI)	The structured collection, analysis, and dissemination of data regarding potential or existing cyber threats.
DoS (Denial of Service)	A cyber-attack makes a device or network resource unavailable to its intended users by disrupting services.
Firewall	A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Honeypot	A security device is set to detect and deflect attempts at unauthorised use of information systems by simulating a vulnerable system to attract cyber attackers.
Indicators of Compromise (IoC)	Evidence that suggests a network or system has been breached or attacked, such as unusual Network traffic behaviour or unexpected software installations.
Incident	An event or occurrence, often a security breach or attack, which affects the integrity, confidentiality, or availability of information or a system.
Internet Protocol address (IP address)	This is a unique identifier assigned to each device connected to a computer network.

Malware	Software designed to disrupt, damage, or gain unauthorised access to a computer system.
Malware Infections	Instances where malicious software has successfully infiltrated a computer system, causing harm or unauthorised access.
Memory	The component of a computer where data is stored for quick retrieval and execution.
Potentially Exploited Application/Program (PUA/PUP)	Software that is not inherently malicious but can be exploited by attackers to perform unwanted actions on a system.
Potentially Exploited Devices	Devices that have potentially unwanted applications (PUA) or potentially unwanted programs (PUP) installed.
Ransomware	A type of malware that makes computer files inaccessible and demands payment to restore access.
Risk	The potential for loss or damage arises when a threat exploits a vulnerability.
Security Ratings	Data-driven measurements of cybersecurity performance.
Server	A specialised computer or software system that provides services or resources to other computers over a network.
Spam Propagation	The distribution of unsolicited and often irrelevant emails sent in bulk.
Vulnerabilities	Weaknesses in a system that attackers can use to gain unauthorised access or cause harm.

3 Communications Sector Cyber Threat Landscape

Critical Communication infrastructure is increasingly vulnerable to cyber threats, as cybercriminals target these systems due to the significant impact downtime can have on industrial processes and the customers they serve.

3.1 Cyber Security Posture

3.1.1 Global Cyber Security Highlights

The cybersecurity landscape is facing significant challenges due to evolving threats and increasing complexities:

I. **Rise in DDoS Attacks**: Distributed Denial of Service (DDoS) attacks are becoming more frequent, targeting businesses, government agencies, and internet infrastructure globally. Notably, a group known as Anonymous Sudan claimed responsibility for DDoS attacks that disrupted digital services in Uganda, Kenya, and Nigeria, affecting hospitals, institutions, companies, and major telecom firms.

II. **Increased Sophistication of Attack Vectors:** Cyberattacks are growing more complex, utilising advanced techniques like zero-day exploits and supply chain attacks. For example, around March 2024, Salt Typhoon nation-state hackers compromised at least eight US telecommunications providers, accessing bulk call records and intercepting limited call and text data in a month-long campaign. These sophisticated methods make detection and defence more difficult for organisations, emphasising the need for regular security assessments and proactive defence strategies.

III. **AI and Machine Learning in Cyber Attacks:** While Artificial Intelligence (AI) aids in detecting complex threats by analysing large data volumes, it also presents new risks. Malicious actors are exploiting AI for automated, evasive, and personalised attacks, complicating detection and attribution. WormGPT, a malicious variant of OpenAI's ChatGPT designed specifically for cybercriminal activities, can generate compelling phishing emails tailored to individual recipients. Organisations must enhance their defences with updated AI-driven security tools to counter these evolving threats effectively.

IV. **Increase in Social Engineering Attacks**: Attackers are increasingly exploiting human psychology to gain unauthorised access or compromise sensitive information through techniques like phishing, pretexting, and baiting. Employee education, vigilance, and robust security protocols are essential defences against these manipulative tactics. Attackers in March 2024 exploited Apple's high CAPTCHA limits to flood users with MFA (Multi-Factor Authentication) requests, leading some to approve out of frustration (MFA fatigue).

V. **Expanding Attack Surface Due to Technology Adoption**: The rapid adoption of advanced technologies such as 5G/6G, Internet of Things (IoT), cryptocurrency, cloud computing, and blockchain has expanded the attack surface. Many of these innovations lack adequate security considerations,

making them vulnerable to breaches. In early 2024, critical zero-day vulnerabilities in widely used Ivanti products were exploited en masse, affecting sectors like government, military, telecoms, and finance, highlighting the risks of widespread technology adoption. Organisations need a fundamental understanding of these technologies' implications on their cyber-resilience posture and must prioritise cyber defence strategies accordingly.

VI. **Supply Chain Exploitation**: The complex supply chain in the telecommunications industry presents potential vulnerabilities. In 2023, sophisticated adversaries exploited relationships between organisations, suppliers, customers, vendors, and service providers, leading to large-scale attacks. High-profile incidents included compromises of software development servers and breaches in identity and access management firms. Okta, a leading provider of third-party identity and authentication management services, experienced a significant breach where attackers gained unauthorized access to private customer data through its support management system. These events highlight the necessity for robust defences and vigilant cybersecurity measures across interconnected networks.

VII. **Geopolitical Events Impacting Cybersecurity:** Escalating geopolitical unrest is exacerbating cyber and physical threats. Ongoing conflicts such as the Russia-Ukraine war, the Israel-Hamas conflict, strategic tensions in the Taiwan Strait, and upcoming crucial elections add layers of complexity to the global threat landscape, affecting cybersecurity on multiple fronts.

3.1.2 Uganda Cyber Security Trends

Malicious cyber activities in Uganda are escalating alongside increased digital adoption. According to the Annual Communications Sector report, 2023, mobile subscribers reached forty-five (45) million, with thirty-seven (37) million of these active subscriptions. The report also records fifteen (15) million smartphones connecting to the mobile networks. This surge in digital connectivity significantly expands the attack surface for potential cyber-attacks, underscoring the vital need for robust cybersecurity measures to effectively safeguard critical infrastructure.

3.2.1 Notable Threats in the Sector

The telecommunications sector, a cornerstone of our digital society, faces distinct cybersecurity challenges as the reliance on digital technology grows. Understanding and addressing these challenges is crucial to maintaining a secure and resilient infrastructure. Below are some of the most notable threats

I. **Distributed Denial of Service (DDoS)**: On February 6, 2024, Anonymous Sudan announced a significant cyber-attack involving DDoS attacks targeting Uganda's telecommunications infrastructure. The attack specifically impacted major telecom providers in Uganda.

II. **Widespread Mobile-based Malware**: There has been a notable increase in malware attacks targeting mobile devices, particularly those running on the Android operating system. Two prominent threats include **AndroidBauts,** a sophisticated banking Trojan that specifically targets financial apps, and **Mocean,** which floods users with unwanted ads and redirects them to advertising websites. These threats underscore the importance of using official app stores, regularly updating devices, and employing reputable mobile security solutions to mitigate the risk of mobile-based malware infections.

III. **Apache Web Server Vulnerabilities**: The cybersecurity landscape in Uganda is characterized by several vulnerabilities associated with Apache web servers used to host online content, including websites. Despite their reputation for security and reliability, Apache web servers are susceptible to exploitable vulnerabilities. These weaknesses provide opportunities for attackers to gain unauthorized access to an organization's sensitive information and potentially execute harmful actions. Addressing these vulnerabilities is crucial for maintaining the security and integrity of digital assets in Uganda, emphasizing the need for proactive security measures and timely patches to mitigate risks associated with Apache web servers.

IV. **Rise of Ransomware 2.0:** Ransomware continues to be a significant threat to critical infrastructure, with increasing ransom demands. Obtaining comprehensive data on this threat remains challenging due to the reluctance of victims to disclose ransomware attack details. Ransomware is a form of malware that encrypts files on computers (laptops, desktops, servers, and portable mobile devices), to deny access to the computer system, data, and files until a ransom is paid. Organizations must enhance incident response capabilities, implement robust backup strategies, and collaborate with law enforcement. Prevention remains crucial to avoid ransom payments.

To address these cybersecurity threats in telecommunications, constituents should implement and promote advanced security measures and cybersecurity best practices, maintain rigorous monitoring systems, and foster a culture of cybersecurity awareness among their clients.

3.2 Cyber Threat Intelligence and Security Ratings

This section of the report gives an overview of the security posture of the sector using an objective security rating scale from 250 to 900. A higher rating reflects a robust cybersecurity posture, while a lower rating may reveal vulnerabilities needing attention.

The sector's **overall security rating is 572.5**, indicating a basic security posture and elevated risk (see Table 1). This underscores the need for increased

collaboration, enhanced capacity building, improved cybersecurity awareness, and stronger policy and legal measures to drive risk improvements.

Category	Security Rating Ranges	Description
Advanced	740 – 900	Strong security performance and lower risk
Medium	640 – 730	Fair security performance and moderate risk.
Basic	250 – 630	Poor security performance and higher risk

Table 1: Security rating categories.

To combat the risks identified, the Commission provides essential Indicators of Compromise (IoCs). IoCs are artifacts identified to signal potential intrusions or malicious activities.

The Commission continuously monitors these IoCs below to effectively detect, notify, and respond to evolving cyber threats, ensuring a robust defence against potential attacks.

I. **Compromised Systems:** This involves assessing devices within operator infrastructure that exhibit signs of malicious or unwanted software. For example, detecting a server that has been infected with ransomware causes disruptions to services.
II. **Operator Diligence:** This assesses the proactive steps taken to prevent attacks on the infrastructure. For instance, implementing regular security patches and updates to servers and network equipment to mitigate vulnerabilities.
III. **User Behavior:** This evaluates file-sharing activities that may introduce malicious software into the network infrastructure. An example would be an employee downloading a phishing email attachment that installs malware on the company's computers, compromising sensitive data.
IV. **Public Disclosures:** This involves assessing information on breaches, security incidents, and disclosures related to unauthorized access to company data. For example, an organisation publicly disclosed a data breach that exposed customer information due to a cyber-attack on their systems.

3.3 Year-on-Year Trends Analysis

This section delves into the trends analysis of key cybersecurity threats observed from FY 2022/23 to 2023/24, specifically focusing on malware infections and families, botnet infections, potentially exploited devices with Potentially Unwanted Applications/Programs (PUAs/PUPs), and spam propagation. These trends help us understand the current state of cybersecurity within the sector and identify emerging threats and areas that require enhanced security measures.

3.3.1 Malware Infections Trend

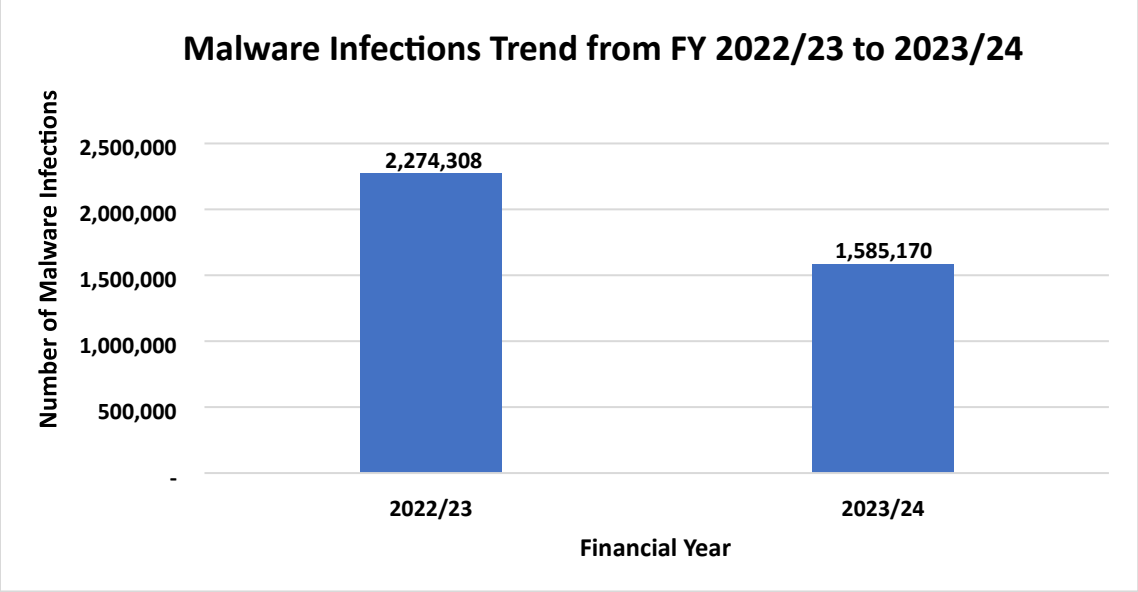

Figure 1: Malware infections trend FY 2022/23 – 2023/24.

Figure 1 illustrates that in **FY 2022/23**, there were **2,274,308** (two million, two hundred seventy-four thousand, three hundred eight) reported malware infections. This number significantly decreased in **FY 2023/24**, with **1,585,170** (one million, five hundred eighty-five thousand, one hundred seventy) infections, indicating a substantial decline.

This positive trend suggests that efforts to bolster cybersecurity have borne fruit. Organizations and individuals have adopted better security practices, such as regular software updates, stronger passwords, and heightened vigilance against suspicious links. Additionally, advancements in security solutions alongside increased awareness about cyber threats may have contributed to this improvement.

However, it is crucial to remain vigilant because cybercriminals adapt swiftly, and new threats emerge constantly. Continued investment in robust cybersecurity infrastructure and ongoing user education remains essential.

3.3.2 Top Malware Infection Trend

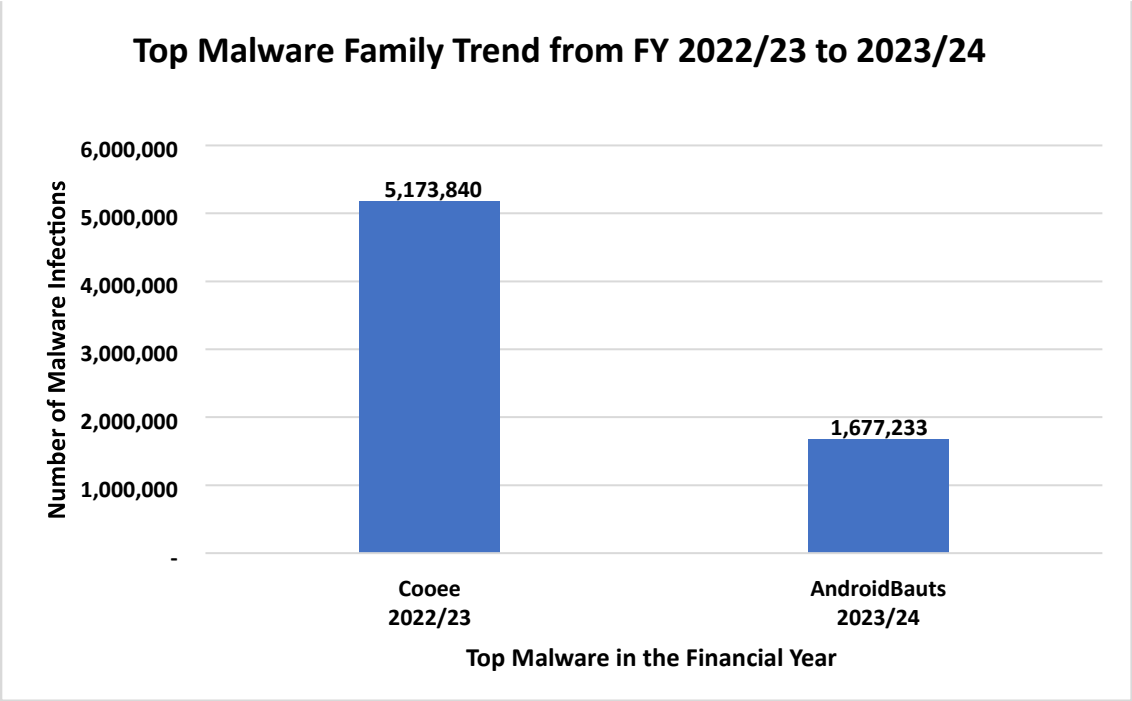

Figure 2: Top malware families trend FY 2022/23 - 2023/24.

Figure 2 illustrates the number of infections caused by the most prominent malware families in the past two financial years. In **FY 2022/23**, the malware family "**Cooee**[1]" was responsible for **5,173,840** (five million one hundred seventy-three thousand eight hundred forty) infections. In contrast, in **FY 2023/24**, the malware family "**AndroidBauts**[2]" was the leading malware with **1,677,233** infections.

This significant decline in infections indicates a substantial decrease in the overall impact of the most prevalent malware families. Cooee has exhibited a declining trend over the past three years, with its infection rates consistently decreasing from 39.4% in 2021 to 14% in FY 2023/24. Although considerable progress has been made in combating malware like Cooee, it is essential to maintain continuous vigilance and adapt to new and evolving threats such as AndroidBauts.

[1] Cooee malware allows the installation of other malicious applications and comes pre-installed on some budget Android devices.

[2] AndroidBauts is a high-risk mobile-based malware that steals user information, such as geolocation and phone contacts.

3.3.3 Botnet Infections Trend

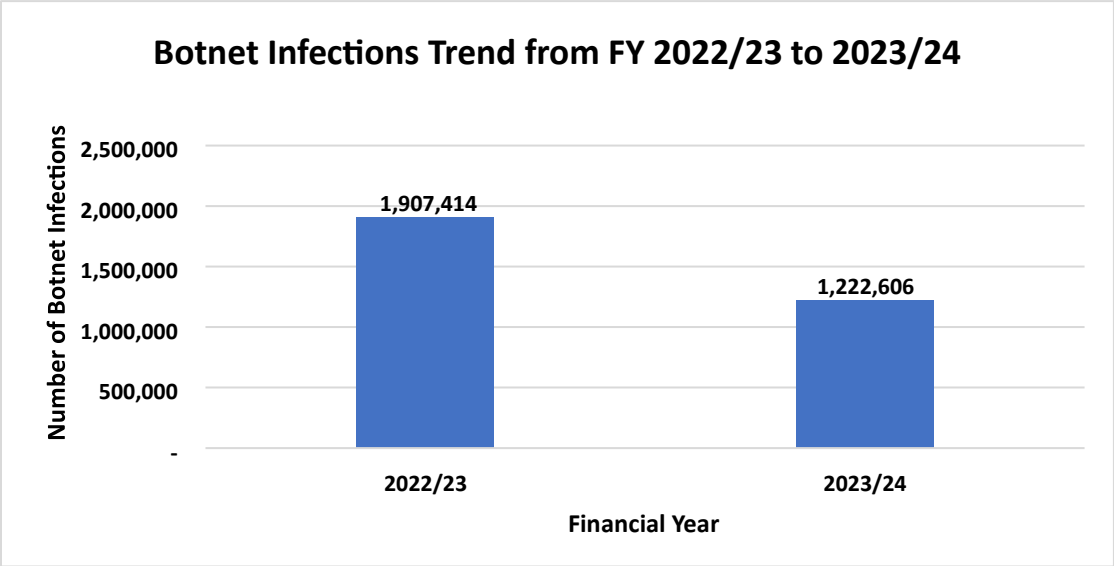

Figure 3: Botnet infections trends FY 2022/23 - 2023/24.

The data in Figure 3 shows a notable decline in botnet infections over two financial years. In **FY 2022/23**, there were **1,907,414** (one million nine hundred seven thousand four hundred fourteen) botnets[3] infections, which decreased to **1,222,606** (one million two hundred twenty-two thousand six hundred six) in **FY 2023/24**. This reduction suggests that measures to combat botnets, such as improved detection and mitigation strategies, have been effective. However, the continued presence of botnet infections at significant levels, with 1.2 million infections still occurring, indicates that there is still work to be done to fully address this threat.

[3] A botnet refers to compromised computers manipulated by a singular attacker, or bot-herder, for various malicious activities.

3.3.4 Potentially Exploited Devices Trend

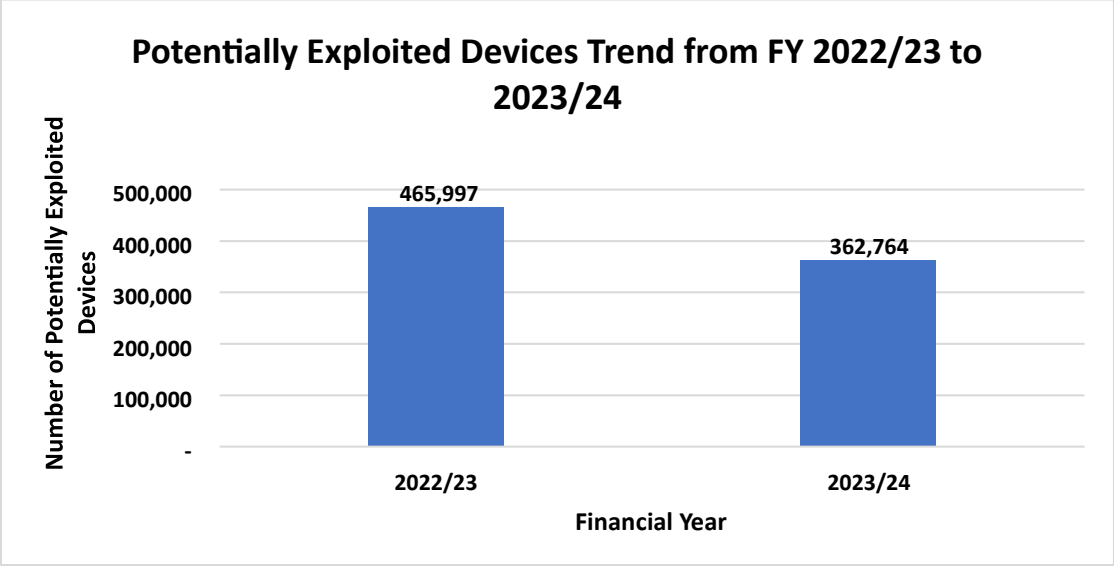

Figure 4: Potentially exploited devices trends FY 2022/23 - 2023/24.

The number of potentially exploited devices [4] decreased as indicated in Figure 4, from **465,997** (four hundred sixty-five thousand nine hundred ninety-seven) in **FY 2022/23** to **362,764** (three hundred sixty-two thousand seven hundred sixty-four) in **FY 2023/24**. This downward trend suggests that efforts to secure devices and prevent exploitation such as timely patching, improved network security, and user education are making a positive impact. Nonetheless, the persistence of exploited devices indicates a need for continued vigilance and improvement in device security practices.

[4]= Potentially exploited devices are devices running programs potentially unwanted applications/programs that can cause unwanted behavior, such as displaying intrusive ads, tracking user activity, or slowing down device performance.

3.3.5 Spam Propagation Trend

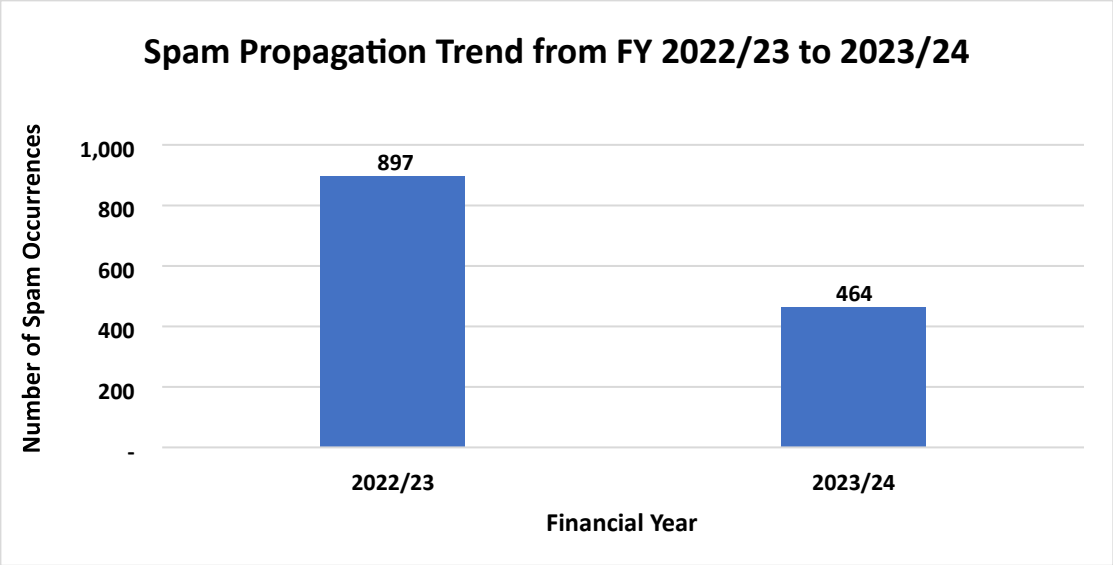

Figure 5: Spam propagation trends FY 2022/23 - 2023/24.

The spam propagation trend in Figure 5 shows a significant reduction, with cases falling from **897** (eight hundred ninety-seven) in **FY 2022/23** to **464** (four hundred sixty-four) in **FY 2023/24**. This steep decline can be attributed to the continuous sharing of monthly indicators of compromise reports. Feedback from operators indicates that they have adopted key Commission recommendations such as;

a) Issuing advisories to their respective customers to install and configure firewalls to restrict malicious traffic.
b) Proactively guiding customers on installing anti-malware software on their systems.

3.3.6 Year-on-Year Trends Summary

The observed trends indicate a positive trajectory in combating cybersecurity threats such as malware, botnets, potentially exploited devices, and spam. The decline in these threats suggests that current cybersecurity measures are effective. However, ongoing investment in cybersecurity infrastructure and education remains essential. Continuous efforts to enhance security practices and educate users are crucial, as cyber criminals continuously adapt and develop new methods.

3.4 Analysis of FY 2023/24

3.4.1 Malware Infections

Malware [5]=Infections are communication sessions that devices with malware establish with botnets or command and control servers. These sessions indicate that devices were compromised with malware delivered through various methods, such as email attachments, software downloads, visiting infected websites, or even social engineering tactics that trick users into installing malware.

Summary

1. In FY 2023/24, a total of **1,585,170** infections on Ugandan networks were observed communicating with Command-and-Control servers.
2. Total malware infections decreased by **30.3%,** from 2,274,308 in the previous financial year to 1,585,170 in the current year.

The significant decrease in malware infections reflects a combination of improved cybersecurity measures, such as enhanced user awareness, regular software updates, and technological investments. These efforts collectively contribute to a more resilient cybersecurity posture, reducing the impact of malware on networks and users of the communication services.

However, this does not diminish the importance of vigilance and proactive cybersecurity measures. Even with fewer infections, the operators should continue to engage in monitoring their networks and collaborate with industry peers and the Commission cybersecurity team.

3.4.2 Malware Infections per Month

Figure 6 below shows the distribution of malware infections per month in FY 2023/24.

The data shows a clear downward trend in malware infections from July 2023 to June 2024, with significant fluctuations in certain months. The notable decrease in specific malware variants like Cooee, coupled with the rise in others like Guerilla, underscores the dynamic nature of cybersecurity threats. Continuous improvements in end-user/consumer education, malware detection, and software security are crucial in maintaining this downward trend and mitigating the impact of evolving cyber threats.

[5] Malware, short for malicious software, refers to any intrusive program or software developed by cybercriminals to steal data, damage, or destroy computers, and interfere with computer systems.

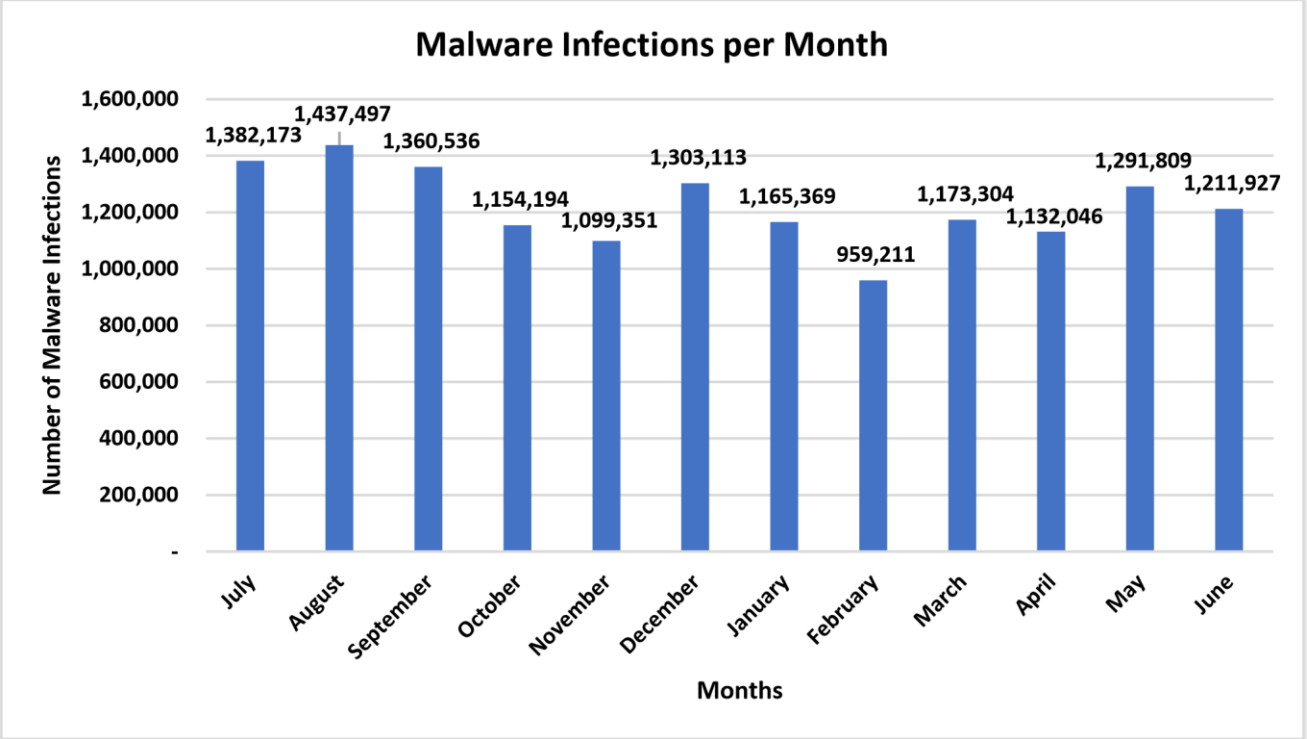

Figure 6: Infections per month in FY 2023/24.

Summary

1. Observed highest Infections in August 2023 with **1,437,497** with average Monthly Infections approximately 1,229,743 from July 2023 to June 2024.
2. A **declining trend in infections** per month from July 2023 to June 2024.
3. From August 2023 to February 2024, **infections decreased by 33.3.%**, indicating an effective response to cybersecurity threats.

In August 2023, the highest number of infections was recorded, totalling 1,437,497 cases due to high infection numbers of leading malware AndroidBauts (steals user device information, such as geolocation and phone numbers) and Cooee (displays intrusive adverts and installs malicious applications). Conversely, February 2024 had the lowest infections, with 959,211 cases, which marked the lowest point in the declining trend of malware infections, majorly caused by a significant decline in Cooee malware.

Infections decreased in the period August 2023 to February 2024. However, March 2024 saw an increase caused by a surge of a new malware strain, InMobi, which is a third-party software development kit (SDK) used to track users without their consent and display intrusive, sometimes malicious ads.

This was followed by a slight decrease in April 2024 due to a reduction in InMobi infections, and another rise in May 2024 due to an increase in infections of the HiddenAds malware that subscribes victims to premium rate services and takes over social media accounts.

Figure 6 illustrates a declining trend in infections per month from July 2023 to June 2024, averaging approximately 1,229,743 infections monthly. This variation stems from changes in infection rates among malware variants. For instance, Cooee malware, experienced a 40.4% decrease in Q2 FY 2023/24, while Guerilla malware which commits advertising fraud using infected devices, spiked by 79.0% in Q3. Both malware variants were targeting Android mobile devices showing the focus of attackers towards mobile devices.

The rise in malware infections results from attackers adopting **new tactics to evade defences**, including leveraging new distribution channels like Telegram channels, online advertising networks, Malware-as-a-Service (MaaS), and updating malware variants.

Conversely, the decline in infections can be attributed to improved user education, enhanced malware detection mechanisms in security solutions, software vulnerability resolutions, and reduced efficiency of certain malware distribution channels. For instance, in 2023, Microsoft issued software updates for more than 800 vulnerabilities affecting Windows, the most widely used operating system. Additionally, in the 2024 half-year report by AV-Comparatives, 17 antivirus solutions scored at least 90% in the Malware Protection Test with zero false alarms on common business software, indicating adaptation to new and sophisticated malware tactics. Starting in May 2024, an international operation, Operation Endgame, coordinated by the FBI and involving a dozen countries disrupted more than 100 servers distributing malware.

3.4.3 Botnet Infections

Botnet infections on network infrastructure in Uganda pose significant cybersecurity risks, where devices are coerced into malicious bot networks controlled by cybercriminals. A botnet refers to compromised computers manipulated by a singular attacker, or bot-herder, for various malicious activities. These include launching DDoS attacks, spreading malware, conducting spam operations, and stealing sensitive data.

In Uganda, botnet infections predominantly propagate through methods such as phishing links, malicious downloads, drive-by downloads, and exploiting software vulnerabilities. Once infiltrated, infected devices become tools for cybercriminals to execute remote commands, perpetuating threats like data breaches and denial-of-service attacks.

The frequency of botnet infections can escalate with the discovery of new security vulnerabilities, exploitation of social engineering tactics, and the broadening of connectivity, which expands the attack surface. Conversely, effective implementation of technical security measures and educating users on

cybersecurity best practices can mitigate these risks and decrease botnet infections over time.
In the financial year (FY) 2023/24, the sector saw a significant shift in the landscape of botnet infections. The overall trend showed a decrease in infections compared to the previous year, FY 2022/23

This trend is attributed to several factors, including the large customer base and extensive network infrastructure of these telecommunications operators. Additionally, varying levels of cybersecurity measures and customer awareness across different operators can influence the prevalence of botnet infections.
In FY 2023/24, botnet infections decreased overall compared to the previous financial year 2022/2023. The absence of infections in certain companies indicates effective cybersecurity practices or highlights the need for increased asset coverage.

Most Consumers of communications services are unaware of the dangers posed by malware, phishing attacks, and suspicious online behaviour, which makes them vulnerable to botnet infections. Users often click on harmful links, download infected files, or share sensitive information with phishing sites unknowingly, allowing botnets to infiltrate their devices. To combat this, there is a need to implement educational campaigns that raise awareness about these risks and promote safer online habits. Improving cybersecurity practices across the board is crucial to protecting users from these threats and enhancing overall digital security in Uganda.
The Commission, through its continuous monitoring reports, recommends the following measures to reduce botnet infections, which are crucial for safeguarding networks, enhancing cybersecurity resilience, and mitigating the impact of cyber threats on Uganda's digital infrastructure.

i. Utilise firewalls and up-to-date antivirus software to prevent botnet infections.
ii. Conduct awareness campaigns about the dangers of phishing and suspicious downloads, which are standard methods for botnet malware distribution.
iii. Implement advanced botnet detection and mitigation solutions to identify and block malicious traffic.
iv. Segmenting networks to limit the spread of botnets if an infection occurs.

By adopting the above proactive defence strategies, among others, stakeholders can collaboratively bolster the cybersecurity posture of the Communications sector and safeguard against emerging threats posed by botnet activities.

3.4.4 Spam Propagation

Spam propagation involves the distribution of unsolicited and potentially harmful messages, known as spam, through different communication channels. Investigations show this risk involves **spambots**, which are devices or systems designed to send large volumes of unwanted messages. Some instances were identified where spambots were **harvesting email addresses** and phone **numbers**

online for spamming. Therefore, if spam originates from specific email addresses or devices, it could indicate a potential infection.
Spam propagation in Internet service providers (ISPs) can be attributed to several factors, including **compromised user accounts**, email servers or clients, and Inadequate or **ineffective spam filtering mechanisms**.
Spam filters are designed to identify and block unsolicited and potentially malicious messages or emails, but if they are not properly configured or regularly updated, spam messages can slip through and propagate within the ISP's network.

The Commission, through its continuous monitoring reports, recommends the following measures for internet service providers to combat spam propagation and enhance cybersecurity:

i. Implement robust spam filtering mechanisms to minimize the impact of spam on their networks and the organizations they serve.
ii. Where possible, use machine learning and AI-based filters to improve detection accuracy.
iii. Implement rate limiting on email servers to restrict the number of emails sent per hour from a single IP address.
iv. Educate users and consumers about the risks associated with spam and phishing attacks.
v. Use of DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to authenticate emails.
vi. Monitor their networks closely for botnet activity, promptly investigate any signs of compromise, and mitigate affected accounts.
vii. Establish effective abuse reporting mechanisms to swiftly address issues related to spam.
viii. Collaborate with other ISPs and anti-spam organizations to share information and collectively combat spam propagation.

3.4.5 Potentially Exploited Devices

Potentially exploited devices are computers, smartphones, IoT devices, or any other network-connected devices that are running a potentially unwanted program (PUP) or potentially unwanted application (PUA). PUAs/PUPs also known as grayware or junkware, are potentially harmful applications that may pose severe risks to the security and privacy of data stored in the system where they are installed. These programs can compromise privacy, weaken computer security, or cause unintended behavior on a device. They might be bundled with free software, downloaded unintentionally, or distributed through deceptive advertising.

The most prevalent PUA/PUP in the period under study was **ArrkiiSDK**, a mobile application advertising module, specifically developed for Android devices. It tracks users' actions without authorization, engages in ad fraud, displays intrusive adverts, and silently installs additional apps without user consent, potentially compromising user privacy and security. ArrkiiSDK is delivered through harmless

applications that unsuspecting users download and install, highlighting the need for vigilant app installation practices and robust security measures.

In FY 2023/24, sector experienced decreases in potentially exploited devices compared to the previous financial year. The decrease in potentially exploited devices may result from reduced vulnerability value due to software patching and upgrades and the integration of secure coding practices in software development lifecycles.

3.4.5.1 Types of PUAs identified.

i) **Adware:** These PUAs display unsolicited advertisements offering free sales and pop-ups of online services when browsing websites.
ii) The **impact** is that they may disturb normal activities, lure victims into clicking on malicious URLs, and issue bogus software or OS reminders.
iii) **Torrent:** When using torrent applications to download large files, users are compelled to download unwanted programs that have features of peerto-peer file sharing. The impact is that it can introduce unwanted programs during the downloading of large files.
iv) **Cryptomining**: Cryptomining PUAs make use of the victims' assets and financial data on the system and perform the digital mining of cryptocurrencies such as bitcoins. This Exploits system resources to mine cryptocurrencies such as bitcoins.
v) **Dialers:** Dialers or spyware dialers are programs that get installed and configured in a system automatically to call a set of contacts at several locations without the user's consent. Dialers cause massive telephone bills and are sometimes exceedingly difficult to locate and delete.

The Commission, through its continuous monitoring reports, recommends the following mitigation measures for potentially exploited devices, such as computers and smartphones, on network infrastructure:

a) Robust security measures like firewalls, intrusion prevention and detection systems, and anti-malware solutions.
b) Continuous security monitoring to identify malicious traffic and compromised devices.
c) User education and awareness programs by the operators to promote good security practices.
d) Regular security audits and assessments to identify vulnerabilities and improve the overall security posture of the ISP's network.

3.4.6 Top Malware Infections

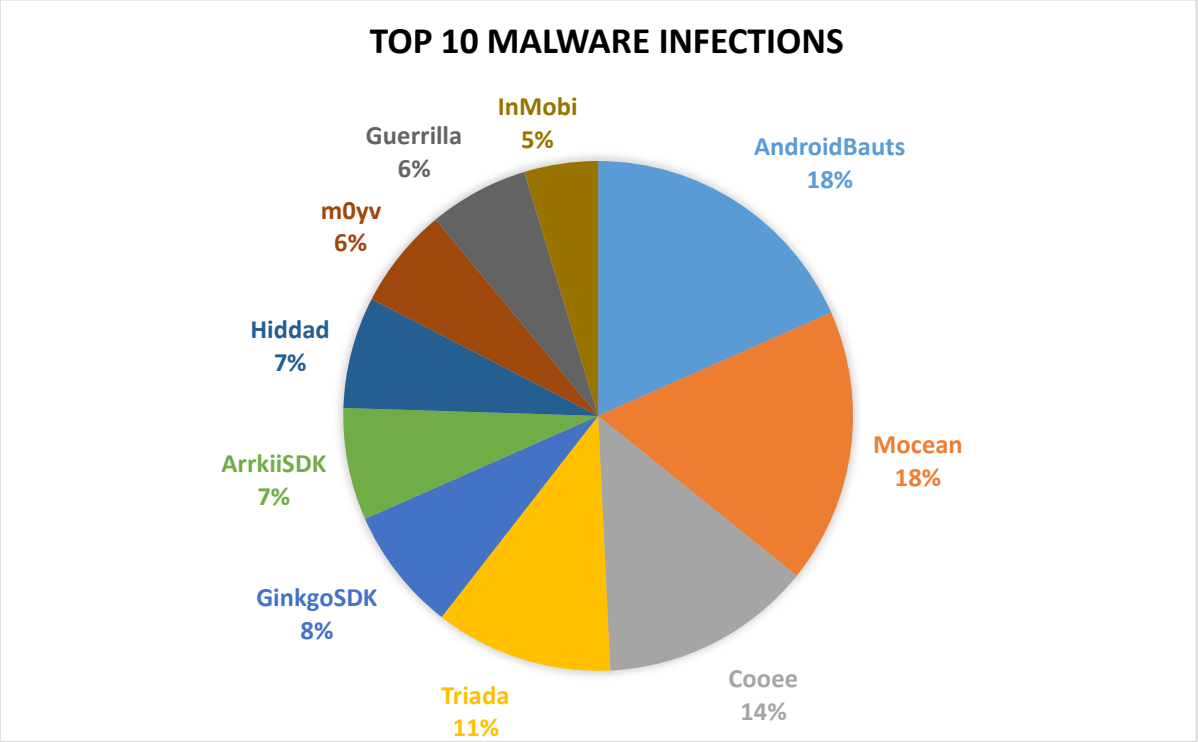

Figure 7: The Communications sector's top ten identified malware.

1. **AndroidBauts and Mocean** were the most prevalent malware strains, each responsible for **18%** of the top infections. Notably, both target Android devices.
2. **Cooee** was responsible for **14%** of the top infections, another significant infection, was preinstalled on some budget Android phones.
3. **Triada** accounted for **11%** of the top infections and is known for its persistence and sophistication.
4. **Invest in robust mobile security software** to scan for malware, detect suspicious behavior, and provide real-time protection against infections.

In FY 2023/24, the Communications sector experienced recurring malware threats targeting mobile devices. The key strains included AndroidBauts, Mocean, Cooee, Triada, and GinkgoSDK, which were also prevalent in FY 2022/23, though their infection rates were higher in the previous financial year. Specifically, in FY 2022/23, their prevalence ranked as follows: Cooee, AndroidBauts, Mocean, Triada, and GinkgoSDK.

Malware type	Description
AndroidBauts	This is a high-risk application that steals user information, such as geolocation and phone numbers.
Mocean	This malware displays ads and allows the installation of additional malicious applications.
Cooee	This malware allows the installation of other malicious applications and comes pre-installed on some Android devices.
Triada	It grants attackers full control over infected devices and silently installs other malware.
GinkgoSDK	Silently installs malicious applications and sends SMS text messages.
ArrkiiSDK	Displays ads with malicious capabilities, such as advertising fraud and silently installing malicious applications.
Hiddad	Steals personal information such as contacts, SMS messages, call logs, and browser history
M0yv	It is a modular ransomware that renders files unusable until a ransom is paid for the decryption key, which restores access to the files.
Guerilla	Generates revenue for its developers by stealthily clicking advertisements and manipulating WhatsApp and Facebook sessions.
InMobi	This adware program shows ads on smartphones that one cannot control as they browse the web.

Table 2: Leading malware infections and their corresponding description.

To tackle the above malware, the following multipronged measures need to be considered:

Measure	Description
Regulatory Actions	Strengthen import controls and enforce certification or type approval processes. Offer subsidies or tax incentives to make genuine devices more affordable.
Industry Partnerships	Collaborate with reputable manufacturers and encourage local production to provide affordable, certified devices.
Consumer Education	Conduct continuous awareness campaigns. Provide guidelines to help consumers verify device authenticity.

Enhanced Security Practices	Promote the use of official app stores. Encourage regular updates and the use of integrated cybersecurity tools through telecom operators.
Community Engagement	Partner with the Ministry of Education, training institutions, and local organizations to expand cybersecurity education and establish feedback mechanisms.

Table 3: Multipronged measures to address malware.

3.4.7 Changes in the Malware Landscape

a) Emerging Malware Variants:
   I. **M0yv Ransomware:** Emerged due to its modular design, effectively targeting both individuals and organizations.
   II. **Guerilla Adware:** Spread easily through social engineering tactics, enticing users to download seemingly harmless files or click on alluring links.
   III. **InMobi Adware:** Gained prominence as developers unknowingly integrated its software development kit (SDK) into their mobile applications.

b) Malware variants such as Reyng, PrizeRAT, and Ztorg became less significant during FY 2023/24.

3.4.8 Critical Vulnerabilities

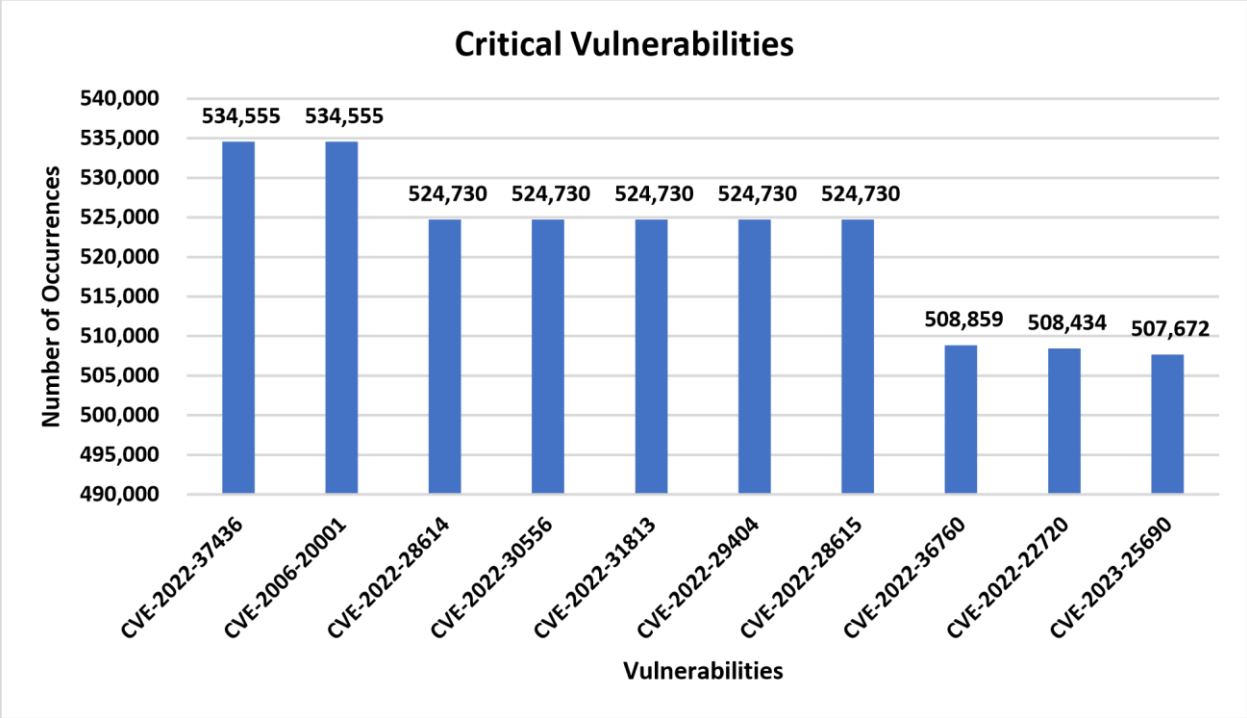

Figure 8: The Communications Sector's Top 10 Vulnerabilities

Summary

1. **CVE-2021-4136 and CVE-2021-26841** were the most prevalent vulnerabilities, each accounting for **8.1%** of the top vulnerabilities.
2. **Apache web servers** had the highest vulnerability count. Despite their reputation for security and reliability, they remain susceptible to exploitable vulnerabilities.
3. **The top five vulnerabilities** remained consistent in both FY 2023/24 and FY 2022/23, underscoring their persistent threat.
4. Ensuring prompt application of security patches and maintaining upto-date software is crucial for mitigating vulnerabilities.

The leading vulnerabilities shown in **Figure 8** are notably linked to Apache web servers, primarily owing to their wide use for hosting web content in Uganda and globally. Throughout all quarters of FY 2023/24, Apache web servers have consistently shown the highest number of vulnerabilities.

These vulnerabilities are inherent to Apache web servers and are observed globally, not just in Uganda. The primary solution to mitigate these vulnerabilities is to ensure timely application of updates. These vulnerabilities persist because some organizations do not update their Apache server software, despite the availability of updates. This failure to update is due to limited IT resources, lack of awareness of the risks of outdated software, and concerns about potential downtime associated with applying updates.

While recognized for their security and reliability, Apache web servers are not immune to exploitable vulnerabilities. Notably, CVE-2022-37436 (refer to Table 4 below) and CVE-2006-20001, affecting Apache web servers were the most prevalent vulnerabilities in FY 2023/24.

Table showing the leading five (5) vulnerability details and affected operators.

Vulnerability	Details
Response Header Manipulation (CVE-2022-37436)	Before Apache web Server version 2.4.55, a malicious backend could cause response headers to be truncated early. If these truncated headers had any security purpose, the client would not interpret them.
Memory Corruption (CVE-2006-20001)	Apache web Server versions before 2.4.55 could crash when a carefully crafted “If:” request header value was sent to it, leading to server downtime
Memory Read (CVE-2022-28614)	The ap_rwrite() function in Apache web Server versions 2.4.53 and earlier may read unintended memory resulting in unauthorized exposure of data.
Information Disclosure (CVE-2022-30556)	Apache web Server versions 2.4.53 and earlier may return more data to applications calling r:wsread() potentially exposing sensitive information.

IP Authentication Bypass (CVE-2022-31813)	Apache web Server versions 2.4.53 and earlier might not send the XForwarded-* headers to the main server due to the client-side Connection header mechanism. This could allow attackers to bypass IP-based authentication.

Table 4: The leading five (5) vulnerability details.

The main cause of the above vulnerabilities includes but is not limited to.

a) insecure programming practices,
b) misconfigured systems
c) outdated software
d) other design flaws

In both FY 2022/23 and FY 2023/24, the top five vulnerabilities remained consistent, highlighting their persistent threat. However, the occurrences of these vulnerabilities increased significantly in FY 2023/24 compared to the previous financial year, emphasizing their heightened impact. Notably, three vulnerabilities (CVE-2022-37436, CVE-2006-20001, and CVE-2023-25690) ranked in the top ten for FY 2023/24 but were absent from the list of top vulnerabilities in FY 2022/23 emphasizing the dynamic nature of cybersecurity risks.

4 Current Efforts to Improve Cyber Hygiene

The Commission, through the CERT, undertook several initiatives aimed at enhancing cybersecurity within the sector. These initiatives include:

	Initiative	Description
1	Minimum Cybersecurity Guidelines for Licensed Operators	The Commission formulated minimum cybersecurity guidelines for licensed operators, which were subsequentl y approved by Management.
2	Digital Financial Services (DFS) Lab Tests	In November 2023, the CERT conducted security assessments on two randomly selected DFS applications, collaborating with the relevant stakeholders. Two mobile applications were thoroughly tested in the Commission's DFS security testing lab to identify vulnerabilities and recommend improvements, thereby enhancing the security of the DFS ecosystem. The cybersecurity division will continue to actively test additional applications and work closely with the respective DFS service providers to the recommended security measures.
3	Cybersecurity Advisories and Indicators of compromise (IoC) information sharing	The CERT diligently shares threat intelligence with the operators, which is a core value of the unit to keep ahead of adversaries and track campaigns and threat groups at scale. IoC reports and advisories were shared with sector stakeholders during the period under review, leading to an improved cyber security posture as the identified threats were addressed.
4	Regional Cybersecurity Summit for Africa	The International Telecommunication Union (ITU), in partnership with the Commission and the CERT, hosted a Regional Cybersecurity Summit for Africa from November 20th to 23rd, 2023. The Summit gathered 183 participants from thirty-nine countries (20-22 November 2023) and forty-seven participants from seventeen countries (23 November 2023) for the ITU-T Study Group 17 Regional Group for the Africa meeting. It introduced ITU-T Study Group 17's work and reviewed key security standards, including ITU-T X.1060, X.1150, and X.1352, and facilitated the exchange of best practices and experiences.

5	Cyber Drill	The Commission, through the CERT, organized a cybersecurity drill for the operators from April 11th to 12th, 2024, aimed at bolstering constituents' cybersecurity skills through practical, hands-on experience.
6	Cybersecurity Awareness	The CERT has consistently promoted cybersecurity awareness by sharing tips through its social media platforms and email with all Commission staff, bolstering organizational readiness and vigilance against cyber threats. Additionally, a sector-specific cybersecurity awareness strategy was developed, outlining key activities to be implemented. To further strengthen this effort, the Commission is in the process of acquiring a computer-based cybersecurity awareness solution for all staff. This tool is designed to educate and train employees on recognizing and responding to cyber threats, reducing the risk of human error, and enhancing overall security posture within the Commission.
7	Operator Cybersecurity consultative meetings	The Commission conducted Operator Cybersecurity consultative meetings with operators, ensuring active engagement and collaboration with stakeholders to enhance cybersecurity measures and practices across the sector. These meetings were instrumental in fostering partnerships and aligning strategies to effectively mitigate cyber threats and vulnerabilities in the sector.

Table 5: Cybersecurity initiatives by the Commission.

During the cybersecurity consultative meetings with operators, it was emphasized that cyberattacks are not limited to large companies or operators. Small businesses are often targeted because they are seen as having weaker security measures. This highlights the importance for all businesses, regardless of size, to be aware of and address cyber risks. To address this, the Commission encourages both small and large licensed operators to participate in cybersecurity initiatives, ensuring that no licensed operator is excluded by adhering to the minimum cybersecurity guidelines developed by the Commission. Additionally, the Commission will formulate distinct guidelines for other subsectors, such as Broadcasting, Radio Communications, Postal Communications, and more. These specific guidelines will be crafted to ensure comprehensive coverage and relevance tailored to each corresponding subsector.

5 Way forward

a) The Commission will continuously monitor network threats and collaborate closely with industry peers to sustain and enhance cybersecurity resilience.
b) The Commission shall prioritise investments in threat mitigation capabilities to mitigate the increasing threat of DDoS attacks, which pose significant disruption risks to the sector.
c) The Commission shall adopt and enforce the minimum cybersecurity guidelines among licensed operators to foster overall sector cybersecurity resilience.
d) The Commission shall maintain rigorous enforcement of the CERT Regulations, 2019, to ensure compliance and strengthen cybersecurity defences.
e) The Commission shall implement a stringent equipment type approval testing and certification process for mobile devices to combat malware on imports.
f) The Commission will work with the different key stakeholders to execute the sector's cybersecurity awareness strategy to promote a security-conscious culture within the sector.
g) The Commission shall continue investing in regular capacity-building programs such as technical training events, cyber drills, and certifications to enhance the cybersecurity skills and knowledge across the sector.