UGANDA
COMMUNICATIONS
COMMISSION

COMMUNICATIONS SECTOR CYBER SECURITY POSTURE REPORT FY 2024/25

Table of Contents

Table of Figures

1.0 Introduction

The communications sector plays a crucial role in Uganda's economy, supporting business, organization, and government functions. However, its complex and interconnected infrastructure makes it a prime target for cyber threats that can jeopardize 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 the year 2024/2025 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, promoting a resilient cyber ecosystem. Our goal is to raise awareness, guide licensed operators 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:

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

The CERT provides:

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

2.0 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 forms of cyber 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 unauthorized 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 behavior or unexpected software installations.
Incident	An event or occurrence, often a security breach or attack, that 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 unauthorized access to a computer system.

Malware Infections	Instances where malicious software has successfully infiltrated a computer system, causing harm or unauthorized access.
Memory	The component of a computer where data is stored for quick retrieval and execution.
Misconfiguration	This refers to incorrect or insecure settings in software, hardware, or network systems that leave them vulnerable to attack.
Network Intrusions	This refers to any unauthorized activity or access within a computer network. It involves a malicious actor breaching a system's defenses to steal data, disrupt operations, or gain control over network resources.
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 (PUAs) or potentially unwanted programs (PUPs) installed.
Ransomware	A type of malware that makes computer files inaccessible and demands payment to restore access.
Risk	The potential for loss or damage if a threat takes advantage of a vulnerability.
Security Ratings	Data-driven measurements of cybersecurity performance.
Server	A specialized computer or software system that provides services or resources to other computers over a network.
Spambots	Malicious software designed to send spam emails automatically.
Spam Propagation	The distribution of unsolicited and often irrelevant emails sent in bulk.
Vulnerabilities	Weaknesses in a system that can be used by attackers to gain unauthorized access or cause harm.
Vulnerability Exploitation	This occurs when attackers take advantage of flaws or weaknesses (vulnerabilities) in software, hardware, or systems

3.0 Communications Sector Cyber Threat Landscape

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

3.1 Cyber Security Posture

3.1.1 Global Cyber Security Trends

The global cybersecurity landscape is rapidly evolving, posing significant strategic risks and opportunities for the telecommunications sector. As digital transformation accelerates with 5G, IoT, and AI, so too does the complexity of threats.

i. **Sophistication and Diversity of Attacks**: Cyber threats are increasingly complex, combining various methods from ransomware to physical sabotage. In July 2024, coordinated attacks targeting French telecom providers involved both digital intrusions and physical cable cutting, causing widespread service outages, highlighting a multi-pronged threat.

ii. **Rise of AI-Powered Threats and Defenses**: AI is now a tool for both attackers and defenders. While it enhances our defenses, adversaries use it to create more convincing and effective attacks. Throughout late 2024 and early 2025, AI-generated phishing and "vishing" campaigns, using highly realistic voice synthesis, surged, specifically targeting telecom customers to steal credentials or install malware.

iii. **5G and IoT Vulnerabilities**: The expansion of 5G and IoT introduces new, complex attack surfaces that require robust security measures. A critical pre-authentication vulnerability (CVE-2025-32433) in the Erlang/OTP SSH server, widely used in 5G core networks and IoT, was disclosed in May 2025, risking unauthorized control over vital telecom systems.

iv. **Supply Chain Risks**: Our reliance on third-party vendors for critical software and hardware creates cascading risks if any part of the supply chain is compromised. Intelligence reports from late 2024 indicated a projected increase in supply chain attacks in 2025. While no singular major telecom incident was public, ransomware groups continue to target smaller vendors supporting critical infrastructure, posing indirect but significant risks to telecom operations through compromised software or vendor access.

v. **Data Privacy and Regulatory Compliance**: Stricter global data privacy regulations demand rigorous compliance and carry significant financial penalties for breaches or procedural lapses. In August 2024, a Belgian telecom company was fined €100,000 for a delayed response to a data access request, illustrating the financial repercussions of even procedural non-compliance with privacy regulations.

3.1.2 Uganda Cyber Security Trends

Uganda's cybersecurity landscape, particularly within the telecommunications sector, mirrors global trends while presenting unique local challenges. According to the threat intelligence gathered in FY 2024/2025, below are some of the most notable threats:

i. **Mobile Malware**: Mobile devices remain a primary target, as 9 of the top 10 detected malware were specifically designed to infiltrate mobile devices, emphasizing the vulnerability of the mobile user base. For the period under review, InMobi Android mobile malware was the most prevalent, with 4.4 million infections. This indicates a persistent threat vector through mobile applications.

ii. **Apache Web Server Vulnerabilities**: Web servers, particularly those running on Apache, continue to present significant vulnerabilities that malicious actors can exploit. This poses a risk to websites and online services hosted by Ugandan entities. Boundary Read Error (CVE-2023-31122) was identified as the most prevalent Apache vulnerability observed. This underscores the continued presence of known, albeit older, flaws within the local landscape, emphasizing the need for timely patching and configuration management for Apache web servers used by Ugandan organizations.

iii. **Advertising Malware**: Adware constitutes a substantial portion of the malware landscape, often leading to unwanted advertisements, redirection, and potential data collection without user consent. Analysis of threat data indicated that the bulk of malware identified in Uganda's top 10 list was various forms of adware. These often bundle with legitimate software or exploit browser vulnerabilities, affecting user experience and potentially compromising privacy across the telecommunications networks.

iv. **Distributed Denial of Service (DDoS) Attacks**: DDoS attacks aim to disrupt online services by overwhelming them with traffic, causing outages and operational downtime. Such attacks can severely impact critical services.

v. **Ransomware Attacks**: Ransomware continues to be a growing and severe threat, directly impacting business continuity and data integrity by encrypting data and demanding payment for its release.

vi. **AI-generated Phishing Attacks**: There was a notable increase in AI-driven phishing attacks and deepfake scams, which significantly enhanced the effectiveness of social engineering tactics by making them more realistic and difficult to detect. Cybercriminals leveraged AI-generated voices and videos to convincingly impersonate high-profile executives and government officials. Furthermore, phishing emails created using AI exhibited improved language quality and fewer grammatical errors, increasing their credibility and success rate.

3.2 Cyber Threat Intelligence and Security Ratings

To monitor and enhance the cybersecurity posture of telecommunication operators, the Commission Cyber Threat Intelligence (CTI) platform is utilized.

This platform offers valuable insights into potential or ongoing cyber threats and evaluates the security performance of operators. It delivers indicators of compromise, which are pieces of forensic evidence that a system or network security has been compromised.

This section of the report is generated using data from the CTI platform, which additionally provides 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 577.5** for FY 2024/25, indicating a basic security posture and elevated risk (see Table 1). Despite **a 0.8% increase** in the security rating from **572.5 in FY 2023/24**, the rating category remained basic. This highlights the need for stronger governance and collaboration, targeted capacity building, heightened cybersecurity awareness, and reinforced policy and legal frameworks with particular emphasis on Internet Service Providers (ISPs) as critical infrastructure operators.

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: CTI platform security rating categories.

To combat the risks identified, the Commission's Cyber Threat Intelligence (CTI) platform provides essential Indicators of Compromise (IoCs). IoCs are forensic data and artifacts identified on operator networks that signal potential intrusions or malicious activities.

These indicators offer crucial information about emerging threats and are derived from a focus on key risk vectors, including Compromised Systems, Operator Diligence, User Behavior, and Public Disclosures within Ugandan cyberspace.

The Commission continuously monitors the cybersecurity risk categories below to effectively detect, notify, and respond to evolving cyber threats, ensuring a robust defense against potential attacks.

i) **Compromised Systems:** This involves assessing operator infrastructure devices exhibiting signs of malicious or unwanted software. For example, detecting a server in an operator's network that has been infected with ransomware that causes disruptions to services.
ii) **Operator Diligence:** This assesses the proactive steps operators have taken to prevent attacks on their 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 operator 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 operator 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 2023/24 to 2024/25, 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

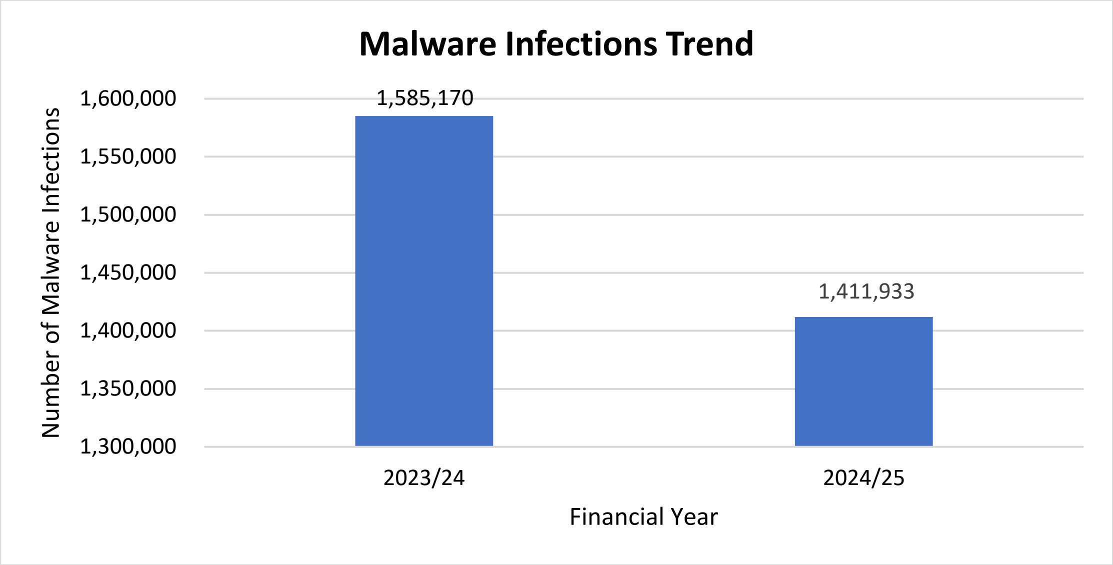

Figure 1: Malware infections trend FY 2023/24 - 2024/25.

Figure 1 illustrates that in **FY 2023/24**, there were **1,585,170** reported malware infections. This number significantly decreased in **FY 2024/25**, with **1,411,933** infections, indicating a substantial decline.

This positive trend indicates that efforts to strengthen cybersecurity are yielding results. However, constant vigilance is vital, as cybercriminals adapt quickly and new threats continue to emerge. Sustained investment in resilient cybersecurity infrastructure and continuous user awareness training remains critical.

3.3.2 Top Malware Infection Trend

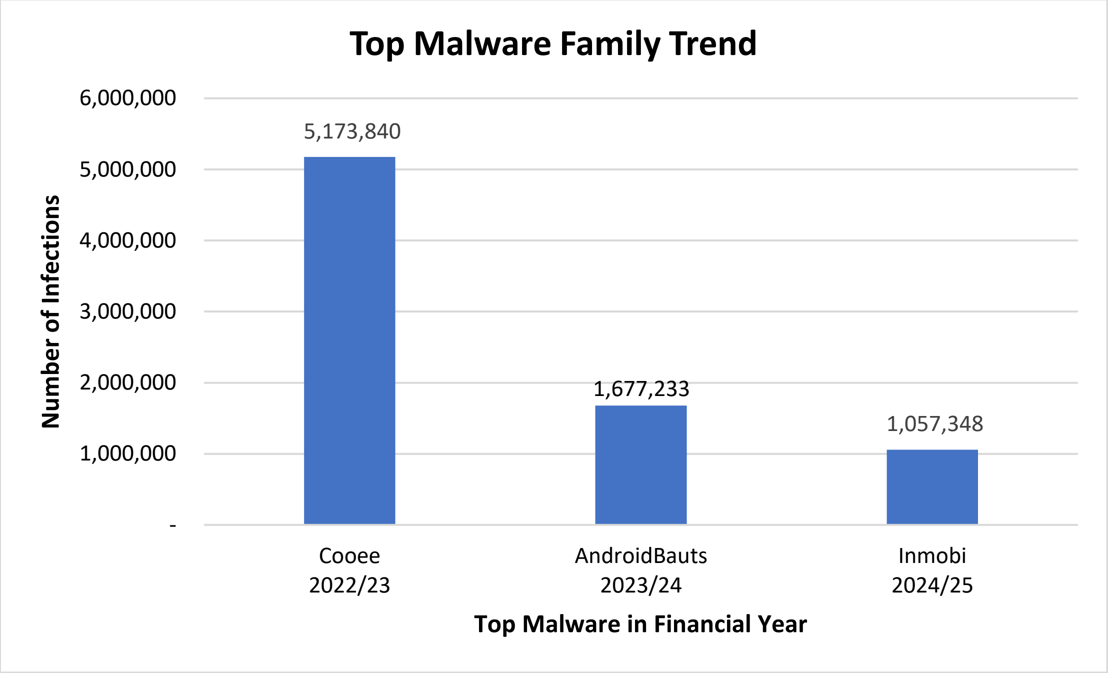

Figure 2: Top malware families trend FY 2022/23 - 2024/25.

Figure 2 presents the number of infections attributed to the most prominent malware families in FY 2022/23, FY 2023/24 and FY 2024/25. In FY 2022/23, malware family “Cooee” had highest number of infections, with a total of **5,173,840** (five million, one hundred seventy three thousand, eight hundred forty) whereas in FY 2023/24, "**AndroidBauts**" led with **1,677,233** (one million six hundred seventy-seven thousand two hundred thirty-three) infections. In FY 2024/25, "**InMobi**" advertising malware emerged as the most widespread malware, responsible for **1,057,348** (One million, fifty-seven thousand, three hundred forty-eight) infections.

This change in the leading malware underscores the rapidly evolving nature of malware threats. While AndroidBauts dominated in FY 2023/24, the rise of InMobi in the following year highlights the need for continuous monitoring, mobile device security assessments, and adaptive cybersecurity measures to counter emerging threats.

3.3.3 Botnet Infections Trend

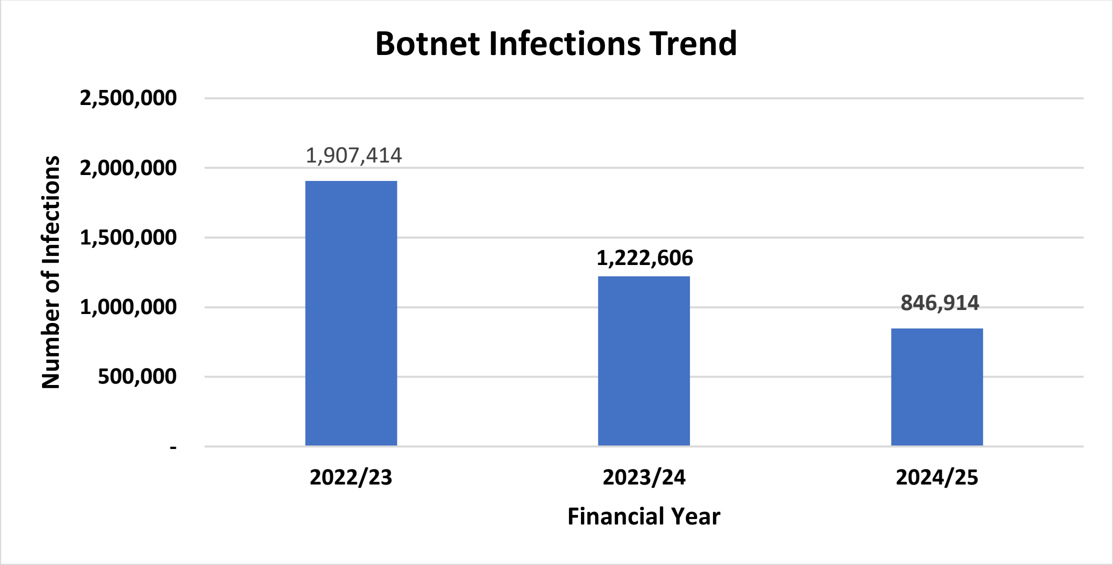

Figure 3: Botnet infections trends FY 2022/23 - 2024/25.

Figure 3 shows a continued decline in botnet infections over two financial years. In FY 2023/24, there were 1,222,606 (one million two hundred twenty-two thousand six hundred six) botnet infections. This number further decreased in FY 2024/25 to 846,914 (eight hundred forty-six thousand nine hundred fourteen) infections, signifying a 31% decrease.

This downward trend suggests that efforts to detect and disrupt botnet activity, such as continuous monitoring, improved threat intelligence, and coordinated takedown operations, are yielding positive results. However, with nearly 850,000 infections still recorded in FY 2024/25, botnets remain a persistent threat that requires sustained vigilance and adaptive countermeasures such as DNS filtering, patching, and configuration hardening, etc.

3.3.4 Potentially Exploited Devices Trend

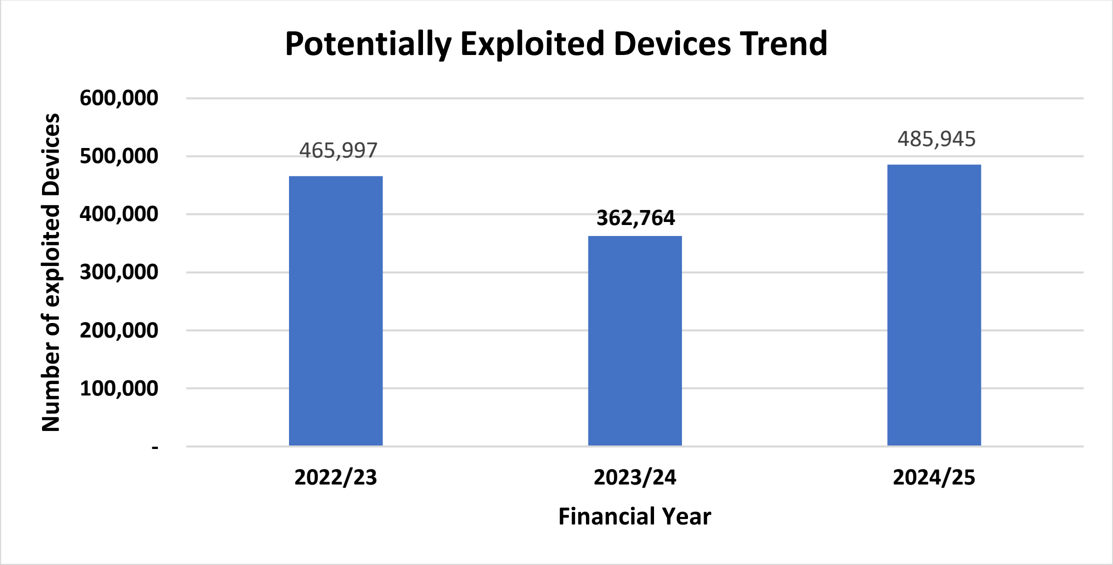

Figure 4: Potentially exploited devices trends FY 2022/23 - 2024/25.

Figure 4 shows an upward trend in the number of potentially exploited devices over the past two financial years. In FY 2023/24, there were **362,764** (three hundred sixty-two thousand seven hundred sixty-four) such devices identified. This number increased in FY 2024/25 to **485,945** (four hundred eighty-five thousand nine hundred forty-five).

This rise suggests that while previous efforts, such as timely patching, improved network security and user education, may have had some impact, the resurgence was driven by new and prevalent malware, InMobi. The continued growth in potentially exploited devices highlights the need for enhanced security measures, including stronger endpoint protection, detection, automation, and increased awareness and drills among users and organizations.

3.3.5 Spam Propagation Trend

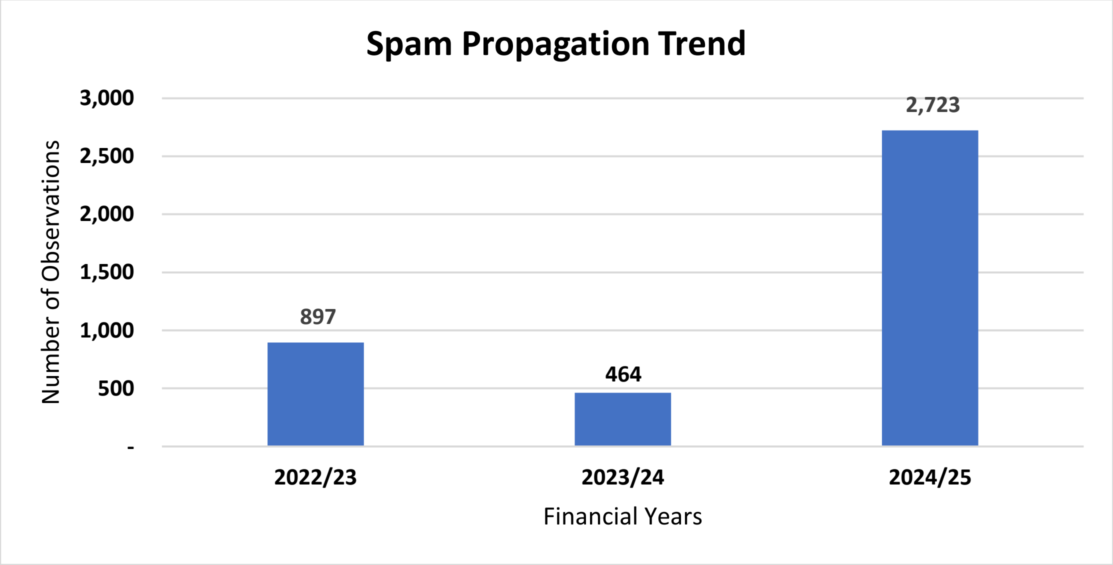

Figure 5: Spam propagation trends FY 2022/23 - 2024/25.

Figure 5 illustrates a sharp increase in spam propagation cases over the two most recent financial years. In FY 2023/24, there were **464** (four hundred sixty-four) reported cases. However, this number rose significantly in FY 2024/25 to **2,723** (two thousand seven hundred twenty-three) cases.

This surge suggests a resurgence in spam-related activity such as unsolicited/bulk messaging and malicious lure distribution (phishing, scams) across mail, SMS, and social channels, potentially driven by evolving tactics used by threat actors or lapses in preventive measures. The increase highlights the need to reinforce earlier successful strategies, such as the consistent dissemination of monthly indicators of compromise reports and adherence to the recommendations, such as;

- Strengthen email/SMS channel security
- Blacklisting identified malicious Ips.
- Use of multi-factor authentication
- Disabling legacy protocols

3.4 Analysis of FY 2024/25

3.4.1 Malware Infections per Operator

Malware[1] 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

[1] 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.

websites, or even social engineering tactics that trick users into installing malware.

Summary

1. In FY 2024/25, a total of **1,411,933** malware infections were recorded across Ugandan telecom networks.
2. This represents a **10.9% decrease** from 1,585,170 infections in FY 2023/24, indicating a positive trend in threat reduction.

Between FY 2023/24 and FY 2024/25, Uganda's telecommunication sector experienced a 10.93% decrease in total malware infections across all operators. This reflects a notable improvement in overall cybersecurity posture, particularly among the major providers.

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

Nevertheless, this trend should not reduce the emphasis on vigilance or proactive cybersecurity practices. Regardless of the current infection levels, operators must sustain continuous networking monitoring, strengthen preventive controls, and actively collaborate with industry peers and the commission's cybersecurity team to ensure early detection, rapid response, and overall resilience against emerging threats.

3.4.2 Malware Infections per Month

Figure 6 below shows the distribution of malware infections per month in FY 2024/25.

The notable decrease in specific malware variants like AndroidBauts and Mocean, coupled with the rise in others like InMobi and my0v, underscores the dynamic nature of cybersecurity threats. Continuous improvements in consumer education, malware detection, and software security are crucial in maintaining this downward trend and mitigating the impact of evolving cyber threats.

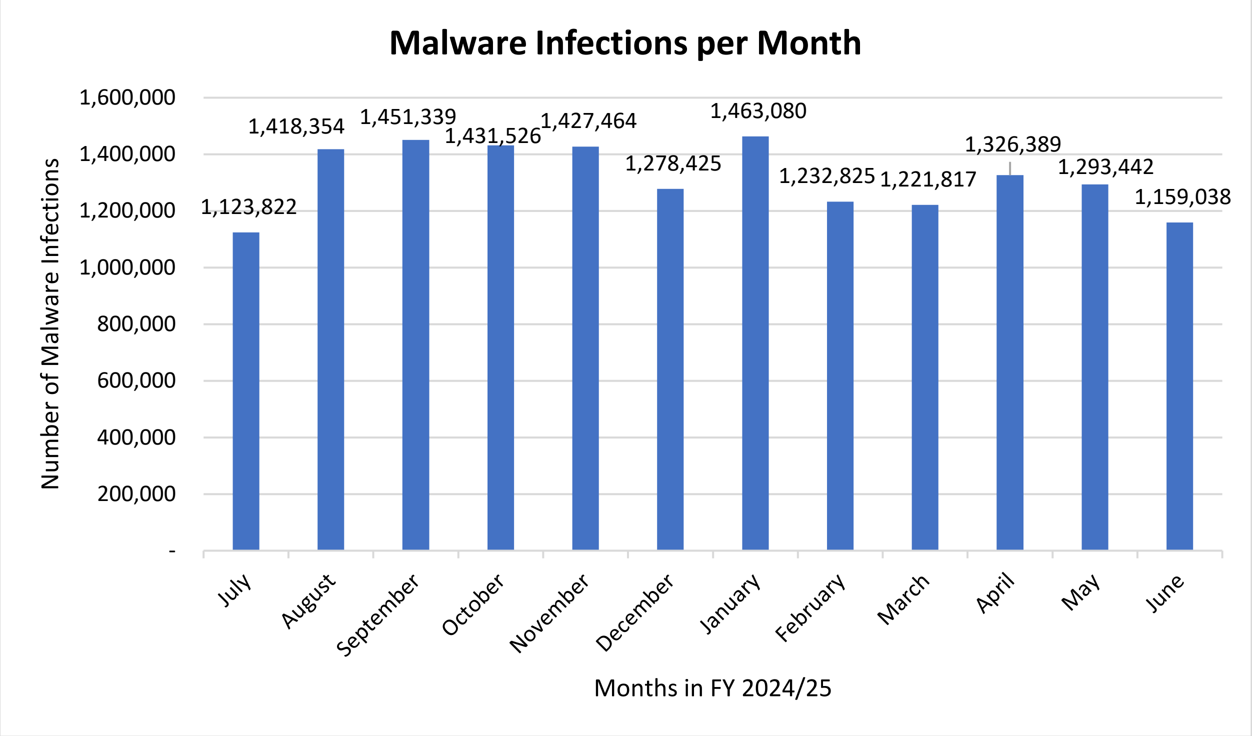

Figure 6: Infections per month in FY 2024/25.

Summary

1. Average monthly infections stood at approximately 1.32 million from July 2024 to June 2025.
2. The trend shows monthly malware infections fluctuating with the highest recorded infection at 1,463,080 in January and the lowest at 1,123,822 in July 2024.

During the period under study, malware infections exhibited notable fluctuations, with a general downward trend. The highest number of infections was recorded in **January 2025**, reaching **1,463,080 cases**, likely reflecting increased cyber activity during the post-holiday period when systems are more vulnerable. In contrast, the lowest levels were observed in **March 2025**, with **1,221,817 infections**, suggesting a period of relative stability or improved threat mitigation.

The **average monthly infection rate** stood at approximately **1.32 million**, indicating a consistently high level of threat throughout the year.
The increase in malware infections from December 2024 to January 2025 can be attributed to large phishing/malware waves that typically surge post-holidays (January) as users return, combined with December change freezes and deferred updates that increase the exposure in January.

3.4.3 Botnet Infections

Botnet infections in Uganda's operator networks pose serious cybersecurity risks. Devices are hijacked into malicious networks used for attacks like DDoS, malware distribution, and data theft. These infections spread through phishing, malicious downloads, and software vulnerabilities. Their frequency increases with new exploits and wider connectivity, but can be reduced through strong security measures and user education.

A significant number of communications service users remain unaware of the risks posed by malware, phishing, and unsafe online behavior, leaving them highly susceptible to botnet infections. Many unknowingly engage with harmful links, download infected files, or disclose sensitive information to phishing sites, enabling cybercriminals to compromise their devices. To address this, telecom operators must lead targeted awareness campaigns that educate users on cybersecurity threats and promote safer digital practices.

Strengthening cybersecurity across all levels is essential to safeguarding users and enhancing Uganda’s overall digital security landscape. The Commission, through its monthly reports, consistently recommends the following measures to reduce botnet infections, which are crucial for safeguarding operator networks, enhancing cybersecurity resilience, and mitigating the impact of cyber threats on Uganda's digital infrastructure.

- Deploy firewalls and regularly updated antivirus software to block malicious activity and prevent device compromise.
- Run targeted awareness campaigns to educate users about phishing, suspicious downloads, and other common infection vectors.
- Implement advanced detection and mitigation tools to monitor, identify, and neutralize botnet-related traffic.
- Segment network infrastructure to contain and limit the spread of infections when they occur.

3.4.4 Spam Propagation

Spam propagation involves sending large volumes of unsolicited messages, often through automated spam systems that harvest email addresses and distribute harmful content. If spam originates from specific devices or email accounts, it may signal a potential infection by these malicious systems.

The operators serve a diverse range of clients in Uganda, including businesses and individual consumers, whose security practices vary significantly, resulting in high spam rates due to the presence of devices with spambots. Spambot infections are spread through various means, such as phishing emails, malicious downloads, or compromised websites.

Spam propagation in Internet service providers (ISPs) is attributed to several factors, including **compromised email accounts and email servers**, and inadequate **spam blocking mechanisms**.

Spam filters play a critical role in blocking unsolicited and potentially harmful messages. However, when not properly configured or regularly updated, they may fail to detect spam, allowing it to spread across an ISP's network.
To address this, the Commission regularly advises internet service providers through its monthly reports to adopt the following cybersecurity measures:

i. Deploy robust spam filtering systems to reduce spam impact on networks and clients.
ii. Utilize AI and machine learning-based filters to enhance detection accuracy.
iii. Apply rate limiting on email servers to control outbound email volume.
iv. Educate users and consumers on the risks of spam and phishing attacks.
v. Monitor networks for botnet activity, investigate anomalies, and mitigate compromised accounts.
vi. Establish efficient abuse reporting mechanisms to address spam incidents swiftly.
vii. Collaborate with other ISPs and anti-spam organizations to share threat intelligence and coordinate response efforts.

3.4.5 Potentially Exploited Devices

Potentially exploited device like computers, smartphones, and IoT gadget may run potentially unwanted programs / applications (PUPs/PUAs) that compromise privacy and security. These programs, often bundled with free software or deceptive ads, can cause intrusive behavior and data collection.

InMobi was the most common observed PUA during FY 2024/2025, known for displaying ads and tracking user data, which can slow down devices and raise privacy concerns, particularly when users are not fully aware of the scope of data collection.

Types of PUAs identified

i. **Adware**: Software that displays advertisements, often bundled with legitimate software to offset development costs. It can collect user data abusively, affect system performance, and redirect browsers to malicious advertising websites.

ii. **Spyware**: Software that secretly monitors user activity and collects information. This can lead to privacy breaches and unauthorized data collection.

iii. **System Optimizers**: Programs that claim to optimize system performance but often provide little benefit and may prompt users to purchase additional features. This can lead to unnecessary expenses and may not improve system performance as advertised.

iv. **Browser Hijackers**: Programs that modify browser settings, such as the homepage or search engine, without user consent. Redirects users to unwanted websites and can lead to privacy issues.

To mitigate risks from potentially exploited devices such as computers and smartphones on network infrastructure, the Commission regularly advises licensed operators through its monthly reports to adopt the following measures:

i. Deploy strong security controls, including firewalls, intrusion detection/prevention systems, and anti-malware tools to block threats.
ii. Maintain continuous security monitoring to detect malicious traffic and identify compromised devices in real time.
iii. Promote user awareness and education to encourage safe digital practices and reduce risky behavior.
iv. Conduct regular security audits and assessments to uncover vulnerabilities and strengthen the ISP's overall security posture.

3.4.6 Top Malware Infections

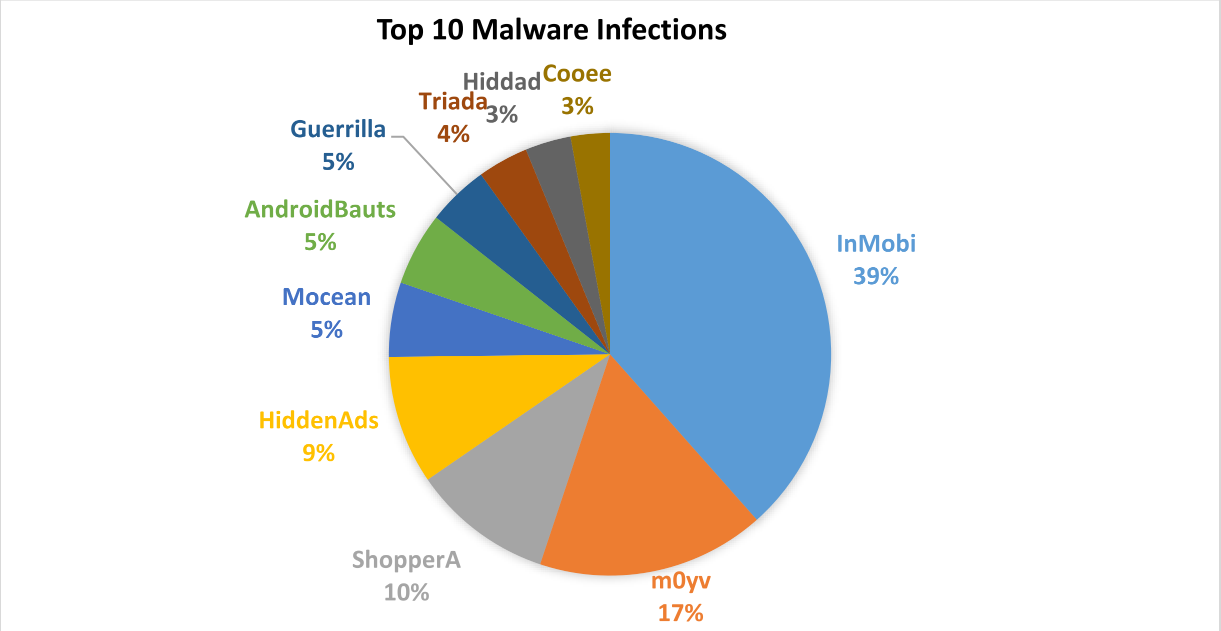

Figure 7: The Communications sector's top ten identified malware.

Summary

1. **InMobi** was by far the most prevalent malware strain, accounting for **38.4%** of the top infections, indicating widespread distribution.
2. **m0yv** followed with **16.7%,** maintaining a strong presence across infected devices.
3. **ShopperA**, a newcomer to the top list, contributed to **10%** of infections, highlighting the rise of ad fraud and mobile data-harvesting malware.
4. To mitigate these threats, consumers should install apps only from trusted sources and use reputable mobile antivirus solutions.

In FY 2024/25, the Communications sector experienced recurring malware threats targeting mobile devices. The key strains included InMobi, m0yv, HiddenAds, ShopperA, and AndroidBauts.

Malware	**Description**	**Impact**	**Mitigation**
InMobi	Displays intrusive ads and tracks users	Privacy violations and increased Internet costs	Run regular anti-malware scans and use ad blockers
M0yv	Locks files on Windows until a ransom is paid	Information systems disruptions	Deploy anti-malware solutions on Windows systems
HiddenAds	Displays ads and subscribes victims to premium services	Monetary loss due to unauthorized subscriptions	Uninstall suspicious apps and utilize mobile security solutions
ShopperA	Commits ad fraud and posts fake reviews on the Google Play Store	Privacy violations and fake app reviews	Utilize mobile security solutions and review app permissions.
AndroidBauts	Tracks users and steals mobile identification information	Privacy violation through unauthorized information gathering	Install mobile security apps and uninstall apps showing excessive ads

Table 2: Leading malware infections and their corresponding description.

3.4.6.1 Changes in the Malware Landscape

i. *InMobi* infections surged more than twofold, from 427,552 in FY 2023/24 to just over 1 million, making it the most dominant malware strain in FY 2024/25. *M0yv* ransomware also saw a significant rise, more than tripling to 535,842 infections. These trends suggest large-scale distribution campaigns, possibly through third-party app stores and social engineering.

ii. Whereas *AndroidBauts*, *Mocean*, and *Cooee* previously among the most widespread experienced sharp declines, each dropping by over 220,000 infections. Top malware threats in FY 2023/24, such as *GinkgoSDK* and *ArrkiiSDK,* disappeared entirely from the top rankings of FY 2024/25.

iii. *ShopperA* and *HiddenAds* entered the top 10 for the first time, each exceeding 275,000 infections. Their appearance among the leading malware indicates evolving attacker tactics and the rapid deployment of new advertising malware variants.

3.4.7 Critical Vulnerabilities

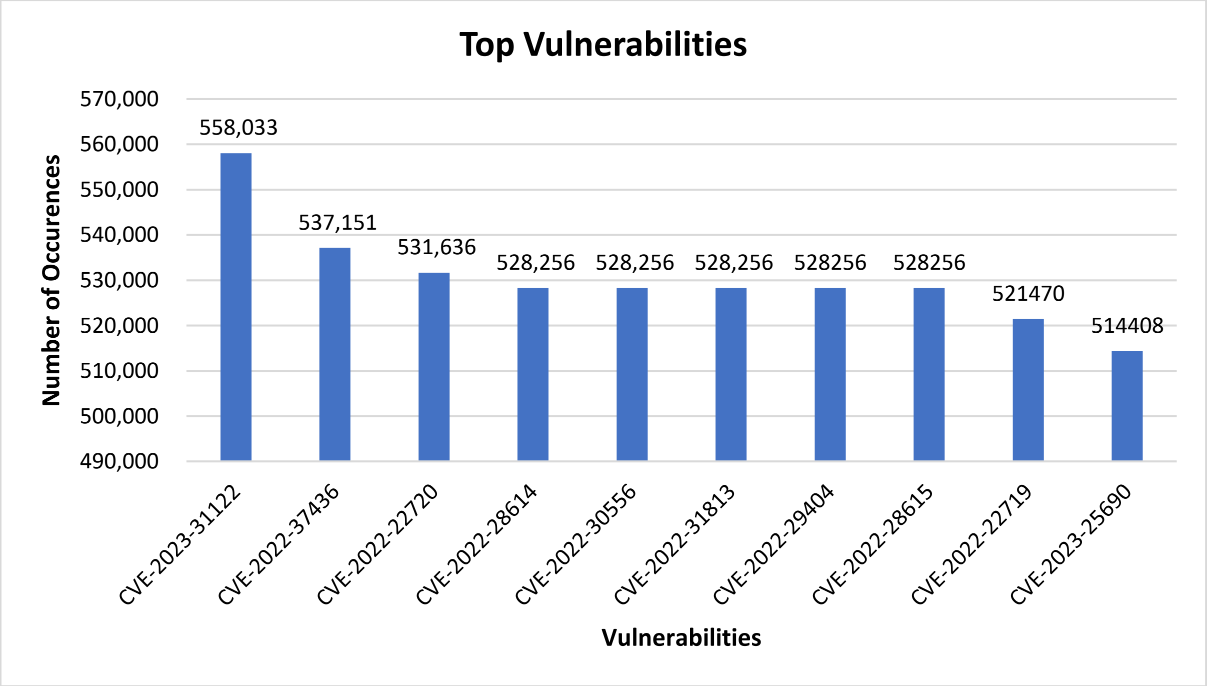

Figure 8: The Communications Sector's Top 10 Vulnerabilities.

Summary

1. **Boundary Read Error** (CVE-2023-31122) and **Response Header Manipulation** (CVE-2022-37436) were the most prevalent vulnerabilities in FY 2024/25, accounting for 10.5% and 10.1% of the top reported vulnerabilities respectively.
2. **Apache web server** vulnerabilities continued to dominate, highlighting the ongoing need for vigilance even in widely trusted platforms.
3. **Seven vulnerabilities** remained consistent across both FY 2023/24 and 2024/25, indicating persistent legacy web servers.
4. Timely patching and proactive vulnerability management are essential to reduce exposure and prevent exploitation of known threats.

Apache web servers accounted for majority of the reported vulnerabilities in both FY 2023/24 and 2024/25 due to their widespread use in Uganda and globally. The most common issue was CVE-2023-31122.

These vulnerabilities persist mainly because some organizations fail to apply available updates often due to limited IT resources, lack of awareness, or concerns about downtime.

Despite their reputation for reliability, Apache servers remain vulnerable, and timely patching is essential to reduce risk and maintain security.

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

Vulnerability	**Details**	**Risk Severity**
Boundary Read Error (CVE-2023-31122)	Causes the Apache web servers to crash unexpectedly, disrupt services, and potentially lead to downtime.	7.5/10
Response Header Manipulation (CVE-2022-37436)	Allows attackers to manipulate data sent to users, which can result in incorrect or misleading information being displayed.	5.3/10
Unauthorized Request Smuggling (CVE-2022-22720)	Allows attackers to send unauthorized requests, potentially accessing or altering sensitive data.	9.8/10
Server Memory Read (CVE-2022-28614)	Exposes sensitive information by allowing attackers to read unintended data, risking privacy breaches.	5.3/10

Buffer Overread (CVE-2022-30556)	May cause Apache web servers to return buffer lengths that exceed allocated memory, potentially leading to information disclosure or application instability.	7.5/10

Table 3: The leading five (5) vulnerability details and affected operators.

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

- insecure programming practices,
- misconfigured systems
- outdated software

3.4.8 Real-Time Cyberthreat Detection (Honeypots)

To enhance the cybersecurity posture of the sector, the Commission in FY 2023/24 deployed advanced threat detection systems, known as honeypot networks. These systems are designed to mimic real services and infrastructure, attracting malicious actors and capturing their behavior in a controlled setting.

This proactive approach provides early warning of emerging threats, generates valuable threat intelligence, and supports the continuous improvement of security tools and policies. By observing attack patterns in real time, the sector is better equipped to anticipate risks and strengthen defenses across the broader ecosystem.

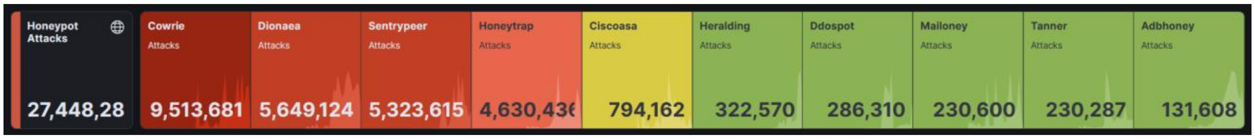

Figure 9: Performance of various honeypots.

Figure 9 illustrates the performance of various honeypots during the period under review, recording 27.4 million attacks. This data provides valuable insights into the threat landscape, highlighting the volume of cyberattacks on key network services.

Below is a table showing the most targeted honeypot services:

Services	Attacks Recorded	Impact
Remote access services (SSH and Telnet)	9,513,681	-Data breaches -System compromises -Operational disruption
Web server and Database services	5,649,124	-Data theft -Website defacement -Unauthorized data access
Voice over Internet Protocol (VoIP)	5,323,615	- VoIP call eavesdropping - VoIP service disruption

Generic TCP Services	4,630,436	- Malware distribution - Network reconnaissance
Firewall and VPN Services	794,162	-Unauthorized network access - VPN credential compromise

Table 4: Most targeted honeypot services

Detailed information on targeted services

3.4.8.1 Remote Access Services (SSH and Telnet)

Remote access services were the most heavily targeted, with over 9.51 million recorded attacks. This high volume underscores the critical risk posed by unsecured or poorly configured remote access protocols, particularly SSH and Telnet. These services, if compromised, can provide attackers with direct entry points into internal systems, enabling them to escalate privileges, move laterally across the network, and exfiltrate sensitive data. The risk is further amplified in environments where legacy systems or default credentials are still in use.

To mitigate these threats, licensed operators should enforce strong authentication mechanisms such as multi-factor authentication (MFA), restrict access through network segmentation and IP whitelisting, and disable Telnet in favor of more secure alternatives. Continuous monitoring and logging of remote access activity are also essential to detect and respond to suspicious behavior in real time.

3.4.8.2 Web Server and Database Services

Web and database services experienced approximately 5.65 million attacks, highlighting their vulnerability to a range of threats such as remote code execution. These attacks can compromise the confidentiality, integrity, and availability of critical business data, potentially leading to data breaches, service outages, and reputational damage.

The risk is particularly acute for licensed operators that rely on customer-facing applications or store sensitive personal or financial information. Effective mitigation requires a multi-layered approach: deploying web application firewalls (WAFs) to filter malicious traffic, conducting regular vulnerability assessments, and ensuring timely patching of software and database systems. Additionally, implementing least-privilege access controls and encrypting data both in transit and at rest can significantly reduce the attack surface.

3.4.8.3 Voice over Internet Protocol (VoIP) Attacks

VoIP services were targeted by 5.3 million attacks, revealing a significant threat to the security and reliability of enterprise communications. These attacks can result in call interception, toll fraud, and denial-of-service (DoS), all of which can disrupt operations and expose sensitive information. The risk is particularly relevant for organizations with distributed teams or those that rely heavily on VoIP for customer service and internal coordination.

To mitigate these risks, it is essential for licensed operators to implement end-to-end encryption for VoIP traffic, deploy session border controllers (SBCs) to secure communication gateways, and monitor for anomalies such as unusual call patterns or unauthorized access attempts. Regular updates to the VoIP infrastructure and strict access controls further enhance the resilience of communication systems.

3.4.8.4 Generic TCP Services

Generic TCP services were the most targeted category overall, with a staggering 4.63 million attacks recorded. This high volume reflects widespread automated scanning and exploitation attempts across a broad range of emulated services, including HTTP, FTP, SMTP, and custom TCP ports. The nature of these attacks suggests significant botnet-driven reconnaissance activity aimed at identifying exploitable services and vulnerabilities. The associated risks include unauthorized access, service disruption, and the potential for these services to be used as entry points for more sophisticated attacks.

To mitigate these threats, licensed operators should implement network segmentation to isolate critical assets, deploy intrusion detection and prevention systems (IDPS) to identify and block suspicious traffic, and enforce strict access controls to limit exposure. Regularly reviewing firewall rules and disabling unused services can further reduce the attack surface.

3.4.8.5 Firewall and VPN Services

Cisco firewall and VPN services were subjected to 794,162 attacks, indicating focused efforts to breach enterprise-grade perimeter defences. These attacks often involve credential brute-forcing, exploitation of known vulnerabilities, and unauthorized access attempts targeting VPN gateways. The compromise of these services can have severe consequences, including unauthorized access to internal networks, data breaches, and loss of control over security infrastructure. The risk is particularly high for organizations relying on VPNs for remote work and third-party access.

To reduce exposure, it is critical for licensed operators to enforce multi-factor authentication (MFA) for all VPN access, ensure timely patching and firmware updates for firewall and VPN appliances, and continuously monitor for anomalous login patterns and access behaviours. Additionally, implementing geo-blocking and rate limiting can help deter brute-force attempts and reduce the likelihood of successful intrusions.

4.0 Cybersecurity Risk and Incident Reports from the Operators

CERT regulations 9(1)(f) mandate operators to submit quarterly cybersecurity incident and risk reports to the Commission. These reports help analyze sector-specific risks and incidents, develop effective solutions, and monitor trends.

4.1 Sector risks and incidents analysis

The period under review registered a steady increase in the number of operators submitting risk and incident registers. This positive trend is largely attributed to the walkthrough sessions held for specific operators to help them understand the reporting template and how to populate it.

In addition, regular follow-ups played a key role in encouraging participation and compliance. As a result, nineteen (19) operators successfully submitted their registers during the year.

To further boost compliance, similar initiatives are planned to continue in the upcoming period, with the goal of increasing the number of operator submissions to thirty (30).

4.1.1 Risks per Quarter

Figure 10 shows that Quarter 3 recorded the highest number of risks in FY 2024/25, reflecting a steady increase from Quarter 1 to Quarter 3. However, this upward trend is largely attributed to the improved compliance by operators with the requirement to submit risk and incident registers.

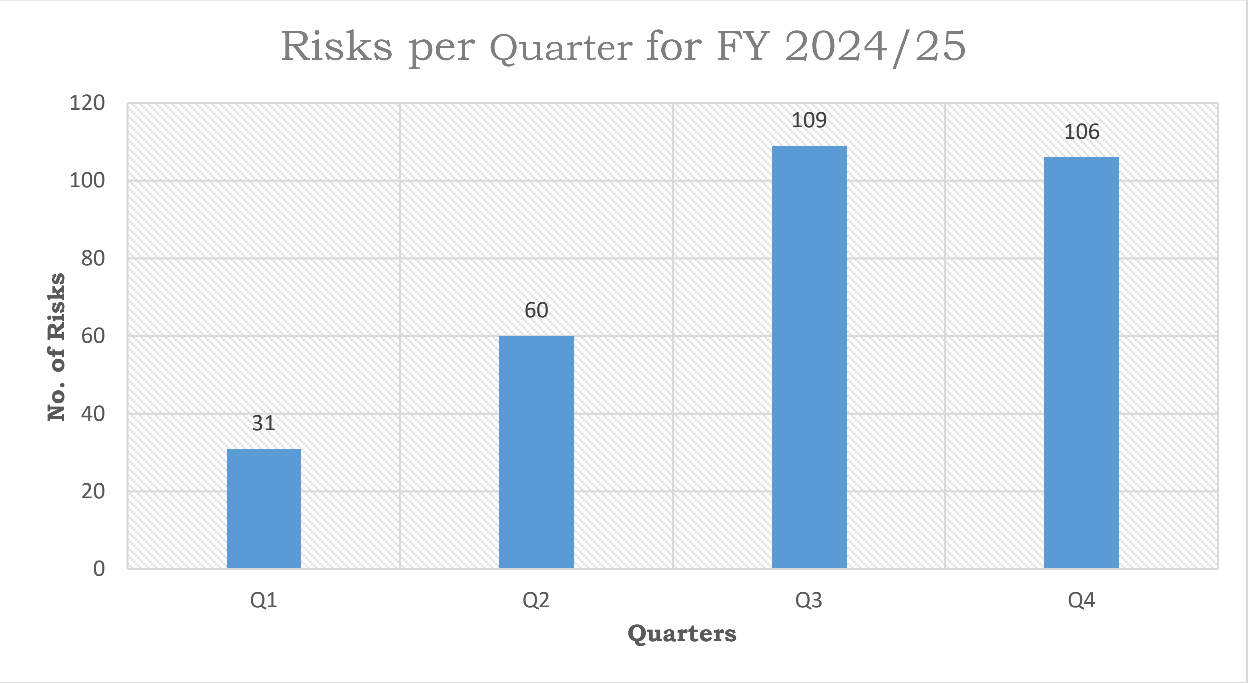

Figure 10: Risks per Quarter.

4.1.2 Risk remediation status

Across the sector, it was noted that 36.7% of the reported risks were remediated, while 51.4% were marked as still in progress. Remediation of about 8% of the reported risks had not yet started, while less than 2% of the reported risks had their remediation measures put on hold, as shown in Figure 11.

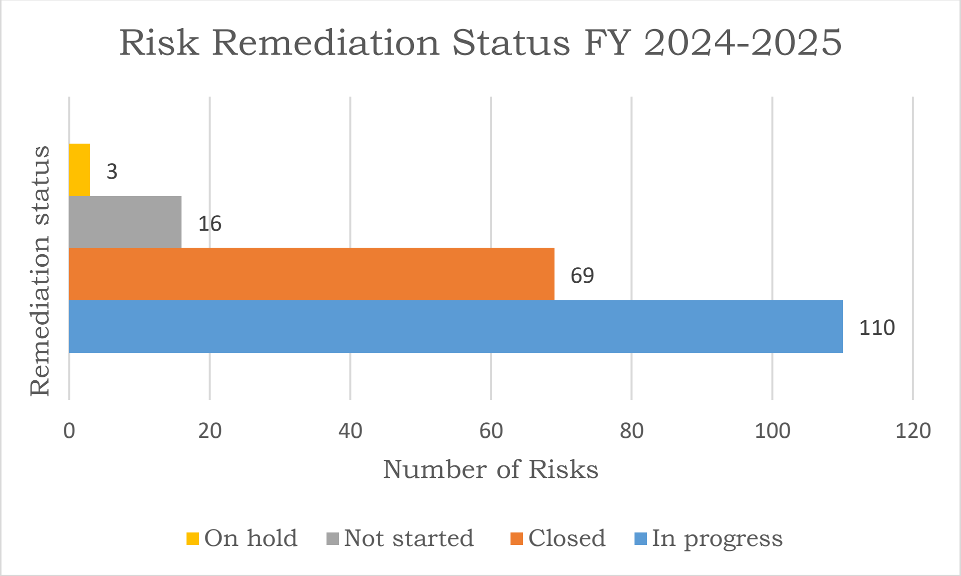

Figure 11: Risk remediation status.

4.1.3 Top Sectoral Risks

The most prevalent cybersecurity risks reported during FY 2024/25 included Distributed Denial of Service (DDoS) attacks, data privacy violations, malicious software (malware), and network intrusions.

Among these, malicious software and data privacy violations consistently recorded the highest number of incidents across all quarters. The continued dominance of these two risk categories highlights the critical need for strengthened endpoint security measures, improved data protection policies, and greater emphasis on staff awareness and training across the sector.

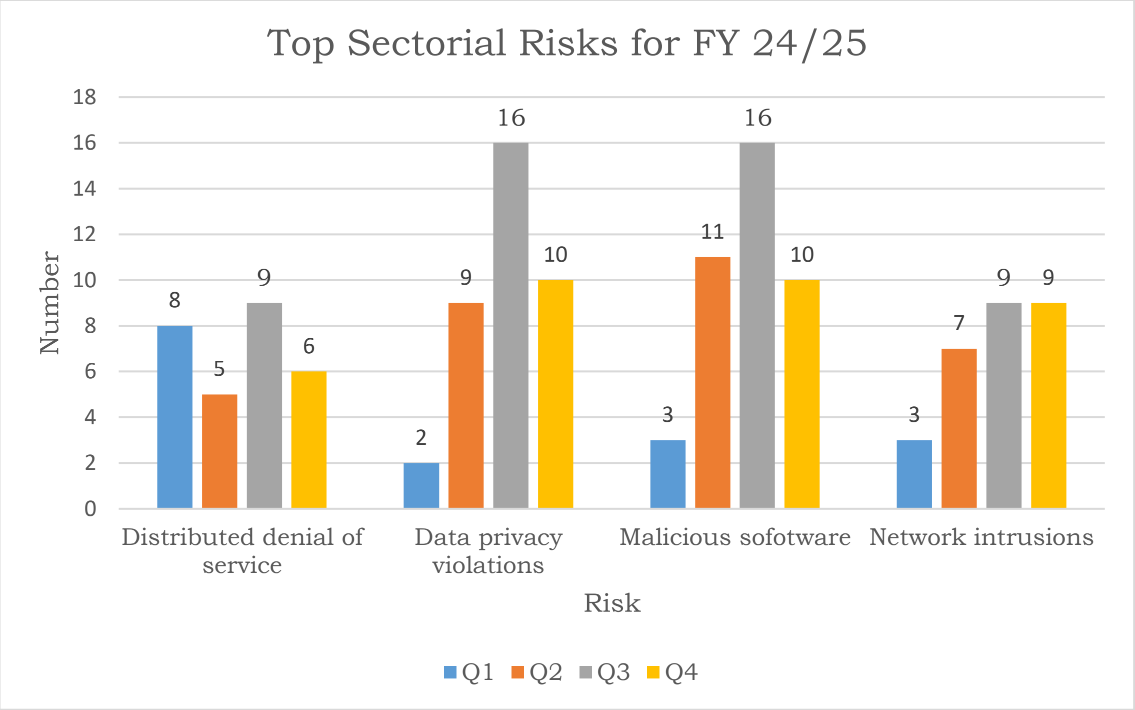

Figure 12: Most prevalent risks

4.2 Incident analysis

whereas the data presented in this section is primarily drawn from incident registers submitted by operators, the Commission also directly received and documented individual incidents during the financial year. These are reported through various channels, including walk-ins, emails, and telephone calls. Most of these cases involved WhatsApp and email account compromises, as well as mobile money fraud. All incidents were promptly addressed, with affected individuals receiving guidance and cybersecurity best practices to help safeguard their accounts and reduce the risk of future compromise.

4.2.1 Incidents per Quarter

Q4 recorded the highest number of operator-reported incidents in FY 2024/25.

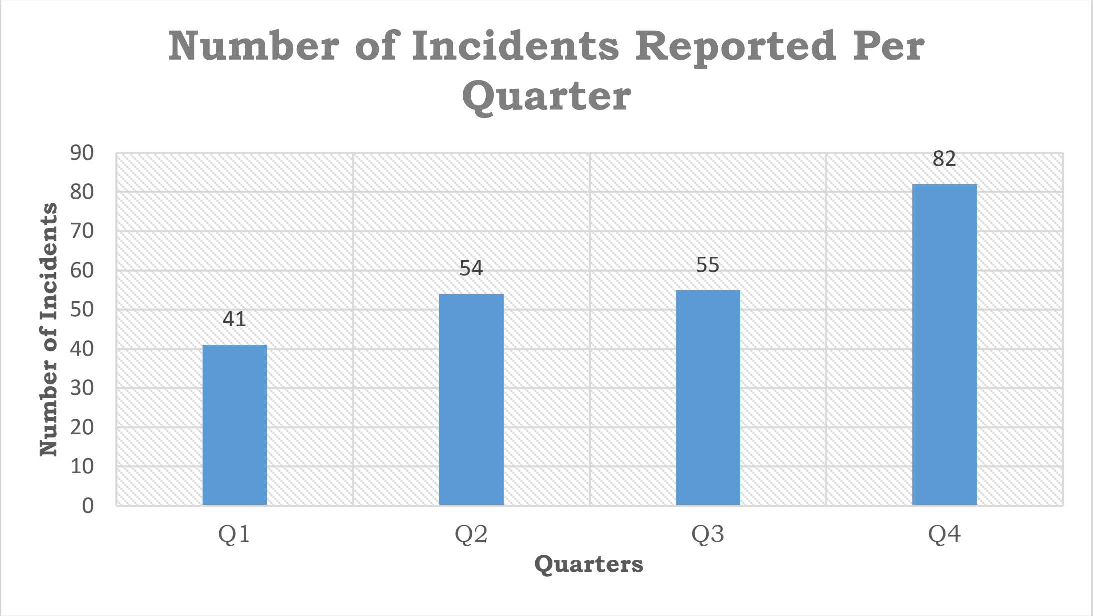

Figure 13: Incidents per Quarter.

4.2.2 Incident Types

As shown in **Figure 14**, the most reported incidents in FY 2023/24 were malware, botnet activity, vulnerability exploitation, and misconfiguration. Malware was the most reported, with thirty-three (33) occurrences.

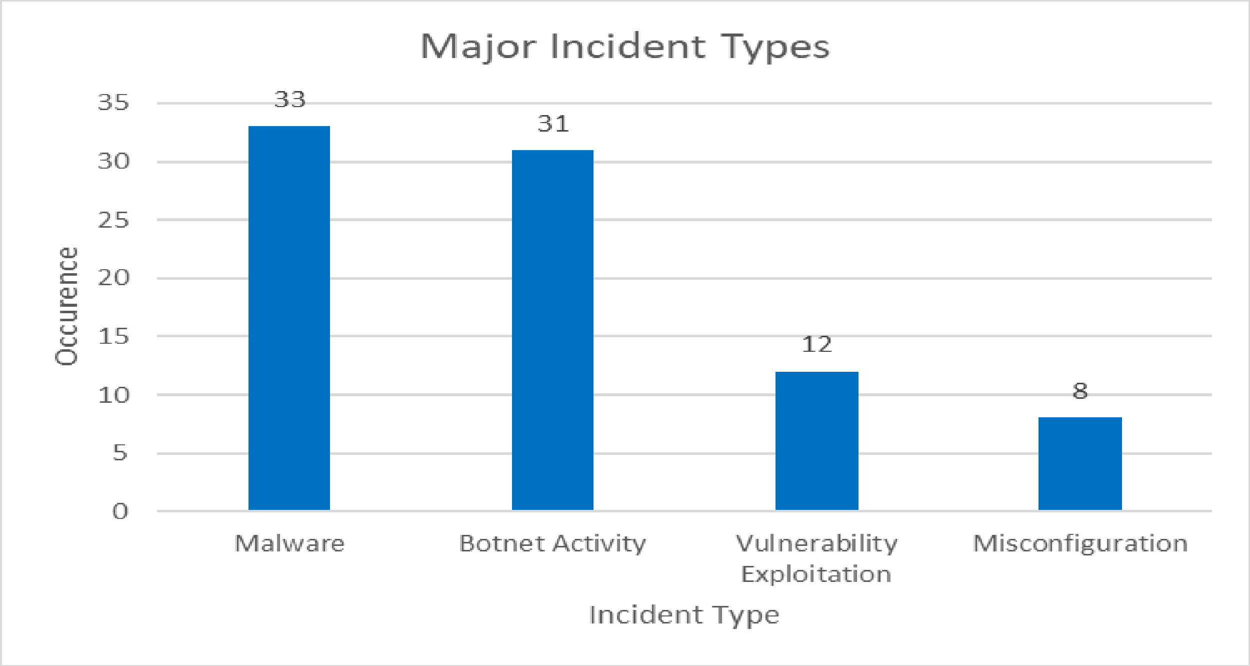

Figure 14: Most dominant Incidents for the year.

4.2.4 Incident Severity

Most incidents reported in the period under review were of **Low** severity (70.5%), followed by **Medium** severity (17.1%). **Critical** incidents were the least reported, accounting for only 0.7%. Refer to Figure 15 for details.

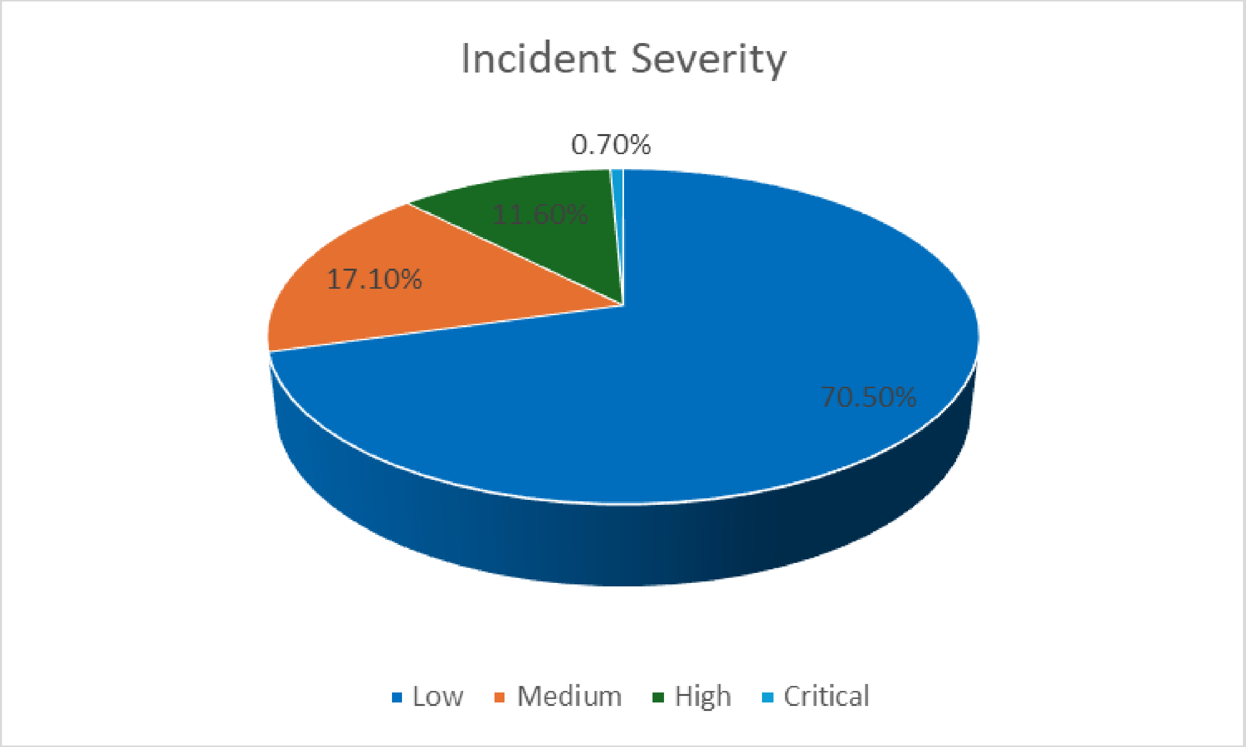

Figure 15: Distribution of Incident Severity.

5.0 Current Efforts to Improve Cyber Hygiene

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

	Initiative	Description
1	Digital Financial Services (DFS) security testing laboratory	The Commission conducted security assessments on four selected DFS applications. • Vulnerabilities were identified, and recommendations were produced for the owners to implement. • The Commission will continue testing additional applications and will work closely with DFS providers and the Bank of Uganda to implement the recommended security measures.

2	Cyber Threat Intelligence Sharing	The Commission shares threat intelligence with the operators, which is core to keeping ahead of adversaries and tracking campaigns and threat groups at scale. • Indicators of Compromise reports are issued monthly to licensed operators. • Weekly honeypot intelligence reports are published on the CERT website. • Operators have access to the Threat Intelligence platforms (CTI and Honeypot platforms) to continuously monitor and identify threats for remediation.
3	Simulation and Cyber Drill Platform Development	The Commission acquired a cybersecurity simulation and learning platform to enhance operator cybersecurity incident preparedness.
4	Cyber Drill	The Commission conducted two (2) operator cyber drills and one cyber stars competition for universities, aimed at strengthening the sector's incident response capabilities and fostering continued collaboration in mitigating cyber threats.
5	Cyber Security Awareness	The Commission has consistently promoted cybersecurity awareness by sharing tips through • Social media platforms • CERT website • Commission consumer outreaches
6	4th CEO Cybersecurity Breakfast	The Commission hosted the 4th Annual CEO Cybersecurity Breakfast, under the theme, "Cybersecurity as a Competitive Advantage: robust cybersecurity measures as a catalyst for innovation and competitive advantage." Focus Areas: • Emerging cyber trends and strategic responses • Building resilient digital infrastructure • Strengthening executive-level cyber governance • Aligning cybersecurity investments with future business objectives Outcome:

		• Reinforced sector commitment to a proactive, innovation-driven security posture and enhanced competitiveness.
7	Cybersecurity Stakeholder Engagement	The Commission engaged: • Secondary school headteachers and ICT teachers across four regional centers, sharing essential cybersecurity tips and online safety knowledge under the theme “Optimal Utilization of ICT”. • Members of Parliament at the Anti-Counterfeit Expo held at Parliament, raising public awareness about cybersecurity risks linked to counterfeit devices.
8	Sector Risk and Incident Reporting	The sectoral risk and incident register was redesigned and updated to improve risk and incident tracking and reporting by operators.
9	Stakeholder satisfaction and Needs assessment	A stakeholder satisfaction and needs assessment survey for licensed operators was carried out to improve service delivery. An overall satisfaction score of 83%, up from 70% in FY 2023–2024.

Table 5: Cybersecurity initiatives by the Commission.

6.0 Recommendations

i) The Commission will conduct targeted meetings with operator CEOs to champion sector cybersecurity priorities and secure concrete commitments.

ii) The Commission will enforce the minimum cybersecurity guidelines among licensed operators to foster overall sector cybersecurity resilience upon the lapse of the one-year transition period.

iii) The Commission shall incorporate Cybersecurity tests in the equipment type approval testing and certification process for mobile devices to combat malware in imports.

iv) Telecom operators are advised to have targeted awareness campaigns that educate users on cybersecurity threats and promote safer digital practices.