COMMUNICATIONS AUTHORITY OF KENYA

# Cybersecurity Report

40th Edition

October - December 2025


A report by:

**The National KE-CIRT/CC**

+254-703-042700 or
+254-730-172700

incidents@ke-cirt.go.ke

www.ke-cirt.go.ke

# Strategic Direction

## Our Vision

Digital Access for All

## Our Mission

Enabling a Sustainable Digital Society through Responsive Regulation

## Our Core Values

Integrity, Innovation, Excellence, Inclusion, Agility.

# Cybersecurity Mandate

The Communications Authority of Kenya's 5th Strategic Plan (2023 - 2027) aims to build upon past achievements, tackle present challenges, and exploit opportunities in the evolving ICT landscape in order to enhance the realisation of the Authority's obligations towards digital access for all. This plan will guide the Authority's activities and ensure its continued contribution to the growth and development of the ICT sector in Kenya.

The Kenya Information and Communications Act (KICA) of 1998, mandates the Authority to develop a framework for facilitating the investigation and prosecution of cybercrime offences. It is in this regard, and in order to mitigate cyber threats and foster a safer Kenyan cyberspace, that the government established the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC), which was officially launched in 2014.

The National KE-CIRT/CC is a multi-agency framework that coordinates response to cyber security matters at the national level in collaboration with relevant actors locally and internationally. The National KE-CIRT/CC, which is domiciled at the Communications Authority of Kenya, comprises of technical staff from the Authority and various law enforcement agencies.

The enactment of the Computer Misuse and Cyber Crimes Act (CMCA) in 2018 has further enhanced the multi-agency collaboration framework through the establishment of the National Computer and Cybercrimes Coordination Committee (NC4). Under the CMCA, and following the enactment of the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations in 2024, the role of the Authority has been enhanced to include the establishment and operation of the Cyber Security Operations Centre (CSOC) for the ICT and Telecommunications Sector.

# Director General's Perspective

*Mr. David Mugonyi, EBS, Director General/CEO, Communications Authority of Kenya (CA)*

The Authority observed that the global cyber threat activity remained elevated and is increasingly becoming sophisticated, with organisations facing persistent risks from ransomware, Distributed Denial-of-Service (DDoS) attacks and advanced social engineering campaigns. At the same time, various emerging threats such as Advanced Persistent Threats (APTs), supply chain attacks, zero-day exploitation and AI-enabled techniques continue to expand the cyber threat landscape.

Critical Information Infrastructure (CII) across key sectors including e-government, ICT and telecommunications, banking & finance and academia, remained a primary target of cyber attacks. Threat actors exploited multiple attack vectors to disrupt essential systems and services, increasing risks to business continuity. These developments reinforce the need for enhanced cyber hygiene, proactive threat detection and continuous user awareness training to counter an increasingly sophisticated and adaptive threat environment.

Over the period October - December 2025, the National KE-CIRT/CC detected over 4.5 billion cyber threat events, most of which exploited system vulnerabilities. In response to this, the Authority issued over 21 million cyber threat advisories during the same period, representing an increase of about 9.3 per cent compared to the previous period, July - September 2025.

The cyber threat advisories largely focused on reinforcing essential security controls, including timely updates and patch management for operating systems, applications and firmware, the adoption of strong authentication measures such as multi-factor authentication (MFA), the use of antivirus and other security utilities, and the proper configuration of network firewalls. These measures were identified as fundamental to enhancing organisational cyber resilience in the context of an increasingly dynamic and evolving threat environment.

In alignment with the Authority's 2023–2027 Strategic Plan, which prioritises the strengthening of national cybersecurity frameworks, enhanced preparedness and increased collaboration with both domestic and international partners, the Authority, working in partnership with the UK's Foreign, Commonwealth & Development Office (FCDO), undertook a series of specialised capacity building initiatives for members of the National KE-CIRT/CC Cybersecurity Committee (NKCC).

The initiatives comprised targeted trainings and workshops, including programmes on proactive cyber defence and threat analysis, the design of a national CIRT/CERT/CSOC ecosystem and cybersecurity for Operational Technology (OT) and Industrial Control Systems (ICS) environments. Collectively, these programmes sought to enhance national cyber resilience by strengthening technical and strategic capacity, promoting knowledge exchange and facilitating the adoption of international best practices tailored to Kenya's national context.

The Authority reiterates its commitment to strengthening capabilities across the cybersecurity ecosystem by equipping stakeholders with the skills, insights and resources necessary to effectively anticipate and respond to the evolving cyber threat landscape. Through focused capacity building initiatives, the application of recognised industry best practices and the building of strategic partnerships, the Authority will continue to advance national cyber resilience and strengthen the digital certification and digital trust value chain.

**Mr. David Mugonyi, EBS**
**Director General/CEO**

# Cyber Threat Landscape Overview

# Global Cyber Threat Landscape Overview

## 1. Ransomware

Ransomware activity remained elevated globally during the period, with threat actors intensifying attacks against critical information infrastructure (CII), public services and enterprise environments. Adversaries continued to pursue financial gain and reputational damage through Ransomware-as-a-Service (RaaS) models, increasingly combining data encryption with data exfiltration, disclosure threats and DDoS-enabled extortion, alongside growing use of AI-assisted social engineering and automation.

In response, National KE-CIRT/CC issued advisories urging organizations to maintain robust offline backups, zero-trust network segmentation, timely patching and continuous threat intelligence updates to strengthen resilience and recovery capabilities against ransomware incidents.

## 2. Distributed Denial-of-Service (DDoS ) Attacks

DDoS attacks remained prevalent, particularly against online services, financial platforms and government portals during peak service periods and public events. Kenya experienced increased probing and short-lived DDoS bursts aimed at service disruption rather than long outages. Attacks leveraged compromised devices and abused internet services such as domain name system (DNS) and Network Time Protocol (NTP) to amplify traffic volumes. Some attacks were launched as distractions to mask other malicious activities.

The National KE-CIRT/CC issued advisories to organizations to implement scalable cloud-based Distributed Denial of Service (DDoS) mitigation and traffic scrubbing services, enforce rate-limiting controls and deploy AI-based traffic anomaly detection to identify, filter and block malicious traffic in real time before it reaches core systems and disrupts services.

## 3. Social Engineering

Social engineering attacks became more personalised and context-aware, exploiting seasonal activities such as end-year travel, festive promotions and financial bonuses. Kenyan users were increasingly targeted through mobile-centred attack methods. Attackers impersonated trusted institutions, employers, delivery services and government agencies through phone calls, SMS and messaging platforms. Psychological pressure and a sense of urgency were commonly used to manipulate victims.

The National KE-CIRT/CC issued advisories to organisations to strengthen user awareness programmes focusing on behavioural red flags, implement verification procedures for financial and sensitive requests and reinforce continuous user education across both public and private sectors

# Global Cyber Threat Landscape Overview... cont'd

## 4. System Misconfiguration Exploits

System and cloud misconfigurations continued to expose sensitive data and services, particularly as organisations accelerated digital transformation and the adoption of cloud services. Kenyan organisations faced increased risk from publicly exposed services and poorly secured cloud storage. Threat actors scanned for open ports, weak access controls and misconfigured cloud environments. In some cases, exposed systems were later used as entry points for ransomware or data theft.

The National KE-CIRT/CC issued advisories to organisations to adopt configuration audits, Infrastructure as Code (IaC) scanning and continuous security assessments. Emphasis was placed on securing all possible entry points rather than isolated systems.

## 5. Emerging Threats

During this period, Advanced Persistent Threats (APTs) and data-driven cyber espionage remained a concern, particularly targeting government, telecommunications and critical infrastructure (CII) sectors across Africa, including Kenya. These threats relied on stealthy techniques such as spear-phishing, exploitation of unpatched vulnerabilities and long-term network persistence to gather sensitive information.

The National KE-CIRT/CC issued advisories to organisations to Improve threat intelligence sharing, behavioural monitoring and collaboration with regional and international cybersecurity partners helping to enhance early detection and response capabilities.

## 6. Phishing

Phishing attacks remained one of the most reported threats during this period, with an increase in credential-harvesting campaigns targeting email, cloud services and mobile banking users in Kenya. Emails and messages mimicked legitimate brands, payment platforms and internal organisational communications. Some campaigns used QR codes and shortened links to bypass traditional email security controls.

The National KE-CIRT/CC issued advisories to organisations to apply email filtering, multi-factor authentication (MFA) and domain monitoring were widely promoted. These advisories encouraged timely reporting of phishing incidents to reduce wider impact.

# Cyber Threat Landscape Roundup

## *Total Cyber Threats Detected*

**4,559,229,985** | **441.27%**

The National KE-CIRT/CC detected over **4.5 billion** cyber threat events during the three-month period between **October - December 2025**. This represented a **441.27% increase** from the threat events detected in the previous period, July - September 2025. As part of its proactive approach to the evolving cyber threat landscape, the Authority continued to enhance the dissemination of cyber threat advisories to critical information infrastructure sectors.

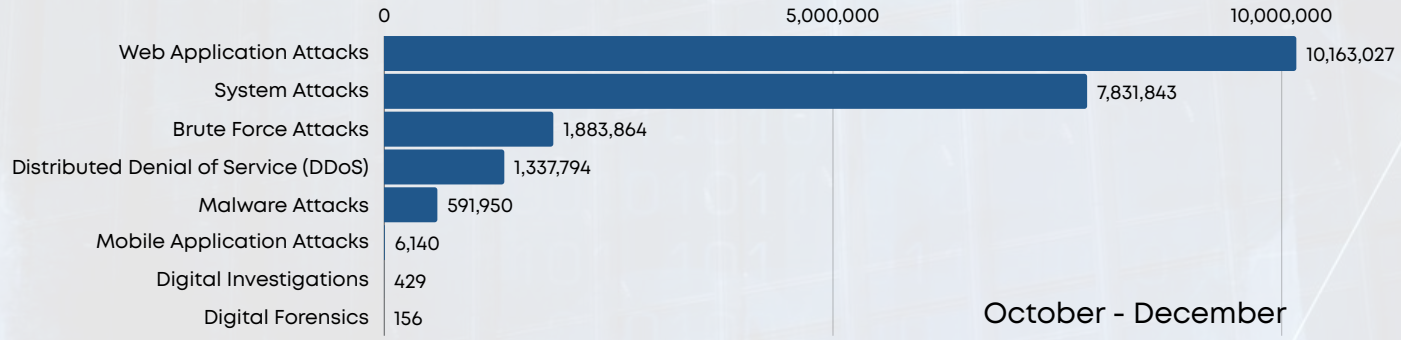
The cyber threats detected were largely attributable to inadequate system patching, insufficient user awareness of phishing and other social engineering threat vectors, and the increasing exploitation of AI-driven and machine-learning technologies by malicious actors.


## *Total Cyber Threat Advisories Issued*

**21,815,814** | **9.34%**

The National KE-CIRT/CC issued **21,815,814** advisories between the period **October - December 2025**, in response to the detected cyber threat events. This represented a **9.34%** increase compared to the advisories that were issued during the previous period, July - September 2025.

The Authority continued to enhance its advisories to emphasise regular system and application patching, the implementation of multi-factor authentication (MFA) and comprehensive password policies, and the proper configuration of network firewalls and antivirus software as key measures to mitigate emerging cyber threats.

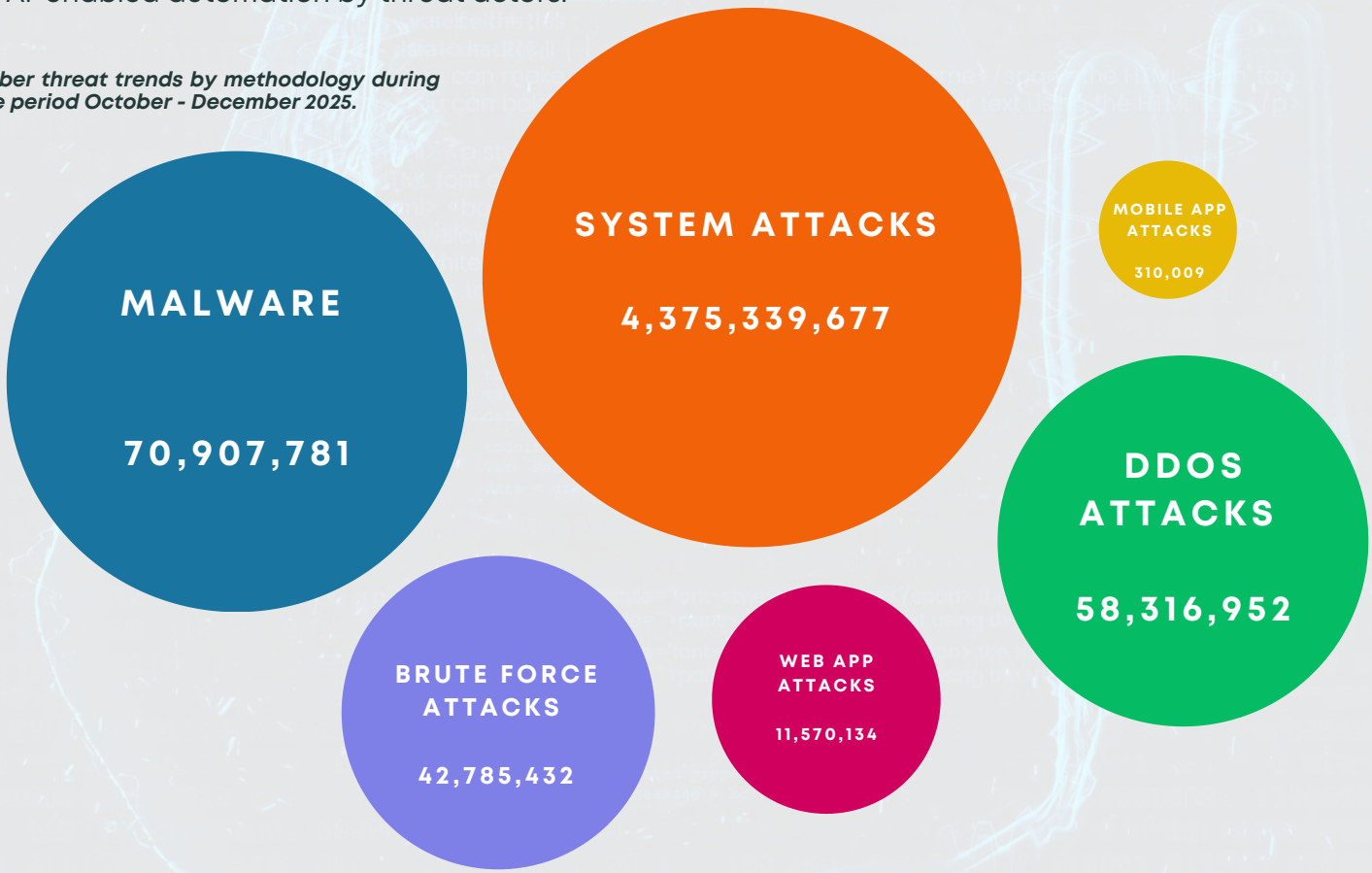


# Cyber Attack Vector Trends

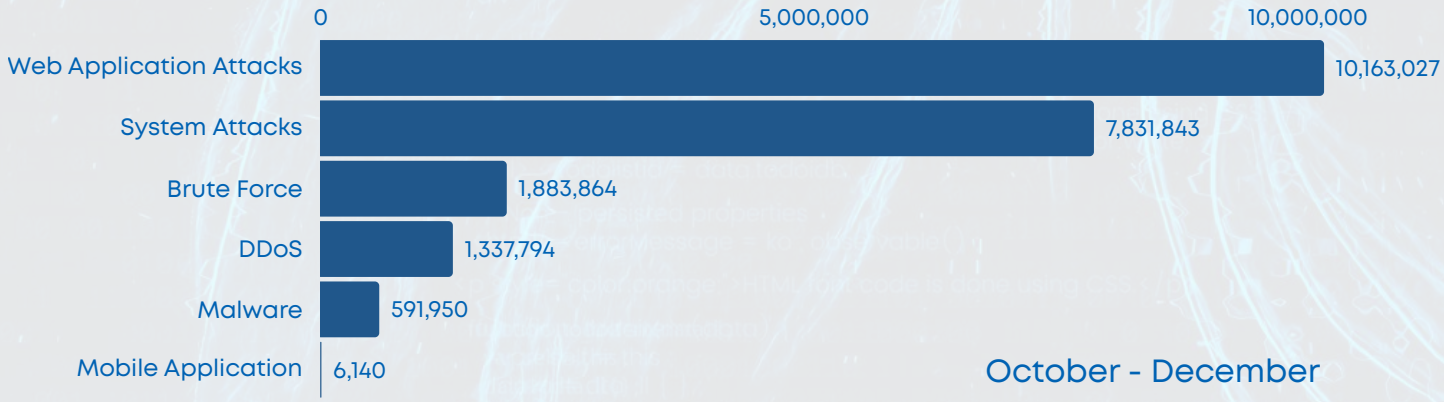
During the period under review, system vulnerabilities and malware attacks constituted the most prevalent threat vectors, in line with global cyber threat trends. Incidents arising from system misconfigurations were largely attributable to inadequate cyber risk awareness, continued reliance on deprecated systems, the use of default credentials and limited investment in modern infrastructure.

On the other hand, malware attacks were largely driven by unpatched vulnerabilities, increased social engineering and phishing activity, cybercrime-as-a-service (CaaS) models and growing use of AI-enabled automation by threat actors.

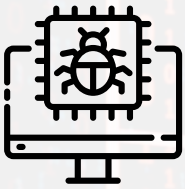
***Cyber threat trends by methodology during the period October - December 2025.***




Comparison of cyber threat advisories (per vector) issued during the period **October - December 2025.**



# Malware Trends



**Threats Detected**

**70,907,781**

**123.85%**

**Advisories Issued**

**591,950**

**1.28%**

During the three-month period between **October - December 2025,** the National KE-CIRT/CC detected **70,907,781** malware threat attempts targeted at the critical information infrastructure sector. This represented a **123.85%** increase from the previous period, July - September 2025.

Internet Service Providers (ISPs), cloud service providers, and government systems remained key targets, with threat actors focusing on end-user devices, Internet of Things (IoT) components, web applications, email systems, network infrastructure and Remote Access Trojans (RATs). Other targeted sectors included government institutions, academia, individuals, and the financial sector, including banks, cryptocurrency platforms, forex and stock trading platforms and online gambling sites.

**Top Targeted Systems**

- **End-User Devices**
- **Internet of Things (IoTs)**
- **Web Applications**
- **Email Systems**
- **Networking Devices**
- **Remote Access Trojans (RATs)**

**Top Affected Industries**

- **Internet Service Providers**
- **Cloud Service Providers**
- **Government**
- **Academia/Education**
- **Individuals**
- **Financial Industry**
- **Cryptocurrency platforms**
- **Forex - Stock trading platforms**
- **Gambling sites**

Malware attacks were largely directed at vulnerable systems due to the sensitive data they hold, with attack objectives including data encryption or corruption, reputational damage, the deployment of backdoors to enable persistent access and the exfiltration of confidential data.

To mitigate this risk, the National KE-CIRT/CC recommended the following actions to affected organisations:

- Security by design, including security during development of software.
- Asset management with patch management.
- Deployment of Domain-Based Message Authentication Reporting and Conformance (DMARC) and spam filters.
- Improve end-user cyber hygiene and awareness.

# Web Application Attack Trends

**Threats Detected**

**11,570,134**

**11.07%**

**Advisories Issued**

**10,163,027**

**8.61%**

The National KE-CIRT/CC detected **11,570,134** web application attack attempts targeted at the critical information infrastructure sector, during the three-month period between **October - December 2025**, This represented an **11.07%** increase from the previous period, July-September 2025.

Government systems and ISPs constituted the primary targets, with threat actors prioritising the compromise of user authentication credentials, vulnerable web browsers and database servers. A significant proportion of attacks exploited weaknesses in SSL/TLS security configurations to facilitate unauthorised access and the interception of sensitive data.

**Top Targeted Systems**

- **Widely used libraries like Log4J to exploit and compromise web applications.**
- **APIs with limited security features.**
- **Insecure configurations in serverless functions.**
- **Vulnerabilities in open-source libraries.**

**Top Affected Industries**

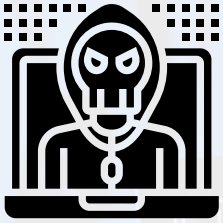
- **Government**
- **Internet Service Providers (ISPs)**
- **Cloud Service Providers**
- **Academia**

Web application attacks exploited vulnerabilities such as unauthenticated remote code execution, privilege escalation, and reflected cross-site scripting to gain unauthorized access, elevate permissions, and expose sensitive information, leading to data breaches and reputational damage to the affected organisation.

To mitigate this risk, the National KE-CIRT/CC recommended the following actions to affected organisations:

- Disabling SSL 3.0 support in system/ application configurations.
- Upgrading end-of-life (EOL) products.
- Apply relevant patches and updates as provided.

# Brute Force Attack Trends



**Threats Detected**

**42,785,432**

**127.44%**

**Advisories Issued**

**1,883,864**

**13.99%**

The National KE-CIRT/CC detected **42,785,432** brute force attack attempts majorly targeting the critical information infrastructure sector during the three-month period from **October - December 2025**. This represented a **127.44%** increase from the previous period, July - September 2025.

These attacks targeted cloud service providers and government systems, with threat actors focusing primarily on database servers and user authentication credentials. Exploitation commonly occurred through weaknesses in database infrastructure, insecure login credentials and misconfigured Remote Desktop Protocol (RDP) configurations, enabling unauthorised access to critical systems.

**Top Targeted Systems**

- **Login Pages**
- **Database Servers**
- **Remote Access Systems**
- **Cloud Service Providers**
- **Mail Servers**
- **Content Management Systems (CMS)**
- **User accounts**
- **VPN Access**
- **Point of Sale systems (POS)**
- **Content Delivery Networks**

**Top Affected Industries**

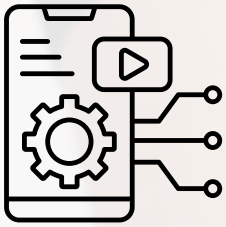
- **Cloud Service Providers**
- **Government**

Over the period, attackers increasingly targeted IoT devices and remotely accessible systems through exposed Telnet ports, misconfigured RDP services and vulnerable libssh versions. These attacks were largely enabled by compromised credentials, lack of multifactor authentication and expanded remote working, with the objective of gaining unauthorised remote access and escalating privileges.

To mitigate this risk, the National KE-CIRT/CC recommended the following actions to the affected organisations:

- Implement patch management on devices running network-based services.
- Implement appropriate access management with strong password management.
- Update libssh softwares to the latest versions.

# Mobile Application Attack Trends



**Threats Detected**

**310,009**

**303.18%**

**Advisories Issued**

**6,140**

**48.15%**

The National KE-CIRT/CC detected **310,009** mobile application attack attempts targeting end-user devices, during the three-month period from **October - December 2025**. This represented a **303.18%** increase from the previous period, July- September 2025.

The majority of attacks were directed at mobile devices and Android TVs, with threat actors exploiting improper credential management to gain unauthorised access and compromise these devices.

**Top Targeted Systems**

- Mobile Devices (Android)
- Android TVs
- Set-Top Boxes
- Google Tv App

**Top Affected Industries**

- Mobile devices
- Set-Top Boxes
- Android TVs

**Top Targeted Exploits**

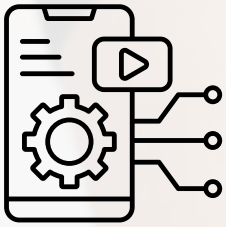
- Improper Credential Usage
- Inadequate Supply Chain Security
- Insecure Authentication
- Insufficient Input/Output Validation
- Insecure Communication
- Inadequate Privacy Controls
- Insufficient Binary Protections
- Security Misconfiguration
- Insecure Data Storage
- Insufficient Cryptography

TThreat actors exploited vulnerabilities in the Android Debug Bridge (ADB) protocol to gain unauthorised shell access to mobile devices, enabling the compromise of sensitive user information and resulting in risks such as identity theft and financial loss.

To mitigate this risk, the National KE-CIRT/CC carried out cyber awareness for end-users recommending the following actions:

- Disable Android Debug Bridge (ADB) on mobile devices.
- Only download applications from trusted sources.
- Check application permissions.
- Keep device and utilities software and applications up-to-date.

# Distributed Denial-of-Service Attacks



**Threats Detected**

**58,316,952**

**1116.06%**

**Advisories Issued**

**1,337,794**

**53.26%**

The National KE-CIRT/CC detected **58,316,952** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure during the three-month period, **October - December 2025**. This represented a **1116.06%** increase from the previous period, July - September 2025.

The majority of attacks were directed at mobile devices and Android TVs, with threat actors exploiting improper credential management to gain unauthorised access and compromise these devices.

**Top Targeted Systems**

- Email Servers
- Web servers
- Database Servers

**Top Affected Industries**

- Health Sector
- Government

**Top Targeted Exploits**

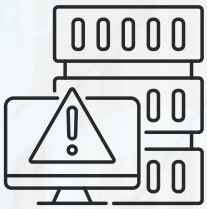
- Reflection/Amplification UDP Abuse: attackers leveraged spoofed UDP services (DNS/NTP/SSDP) to amplify traffic into Tbps floods.
- Missing Source Address Validation (No ISAV): networks allowing IP spoofing enabled large reflection/amplification attacks.
- IoT/Router Botnets: compromised consumer devices with default creds/outdated firmware formed huge, distributed bot armies.

Over the three-month period, hacktivists and politically motivated advanced persistent threats (APTs) targeted critical systems to disrupt public service delivery, resulting in service degradation for consumers and increased operational costs for cloud service providers.

To mitigate this risk, the National KE-CIRT/CC carried out cyber awareness activities that targeted end-users in the following areas:

- Implementing appropriate out-of-band DDoS detection systems.
- Implementing firewalls and intrusion detection systems to detect and mitigate suspicious traffic.
- Using strong passwords for your devices to prevent them from being compromised and used in botnets.
- Keeping devices and utilities software up-to-date.

# System Attack Trends



**Threats Detected**

**4,375,339,677**

**463.44%**

**Advisories Issued**

**7,831,843**

**5.03%**


The majority of attacks were directed at the ICT sector, with operating systems and database servers managed by Internet Service Providers (ISPs) and cloud service providers being the primary targets. Threat actors exploited outdated system vulnerabilities to exfiltrate user authentication credentials, while the continued prevalence of these vulnerabilities is largely attributable to the rapid proliferation of Internet of Things (IoT) devices lacking comprehensive security controls.

**Top Targeted Systems**

- Database Servers
- Operating Systems
- Network Devices
- Web Applications
- Remote Access Systems
- Critical Infrastructure
- Mailing Servers

**Top Affected Industries**

- Internet Service Providers
- Cloud Service Providers
- Health care sector

**Top Targeted Exploits**

- Stealer/ Broken Access Controls
- Leakage of Information
- Outdated OS
- Malicious Links
- HTTP Vulnerability
- Vulnerable databases
- Zero-day exploits
- Remote code execution (RCE)

System attacks primarily targeted critical information infrastructure with the intent of financial gain and malware distribution, leading to data breaches, financial losses, potential ransom payments, legal and regulatory consequences and wider malware propagation.

To mitigate this risk, the National KE-CIRT/CC recommended the following actions:

- Keeping software up-to-date and applying patches as soon as they are released.
- Using strong passwords and multi-factor authentication.
- Enhancing firewall configurations.

# Capacity Development & Partnerships

# The 2025 Annual Cybersecurity Conference and Forum of Incident Response & Security Teams (FIRST) Technical Colloquium

On 21st November 2025, the Authority, through the National KE-CIRT/CC, hosted the 2025 Annual Cybersecurity Conference and Forum of Incident Response & Security Teams (FIRST) Technical Colloquium, in Nairobi. Held under the theme "Building Digital Trust Through Coordinated Incident Response Frameworks," the conference convened 197 delegates drawn from government, regulators, critical information infrastructure operators, private sector, academia, professional bodies and international partners, to strengthen Kenya's national cybersecurity ecosystem and incident response capacity.

The conference programme focused on enhancing national cyber resilience and digital trust through coordinated governance structures, effective public–private partnerships and structured incident response frameworks. High-level remarks highlighted the rapid growth of cyber threats, the economic importance of a secure digital economy and Kenya's strategic role as a regional digital hub. Emphasis was placed on timely information sharing, standardised protocols and cross-sector collaboration as foundational elements for sustaining trust in digital services and protecting critical infrastructure .

Through a series of thematic sessions, participants examined key pillars of cybersecurity maturity. Discussions addressed strengthening national coordination mechanisms, the role of digital trust technologies such as digital identities and signatures in service delivery, and the value of public–private partnerships in incident reporting and response. Panels further explored emerging challenges including cybercrime, misinformation, privacy considerations and the impact of AI-enabled threats, highlighting the need for balanced, transparent and legally aligned approaches .

The conference also highlighted cybersecurity capacity building as a national priority. Stakeholders emphasised bridging the skills gaps through coordinated action among universities, professional bodies, government and industry, while expanding practical training, certifications and interdisciplinary participation. The discussions reinforced that cyber resilience depends not only on technology but also on skilled people, shared responsibility and trusted collaboration across society .

Overall, the outcomes affirmed the need to strengthen national coordination through the National Computer & Cybercrimes Coordination Committee (NC4) and the National KE-CIRT/CC, formalise public–private collaboration frameworks, advance digital trust technologies and institutionalise regular cyber drills and awareness initiatives. The Authority concluded that the insights and recommendations from the conference provide a strong foundation for enhancing Kenya's preparedness, coordination and capacity to prevent, detect and respond to cyber threats while reinforcing digital trust across the economy.

# The 2025 Annual Cybersecurity Conference and Forum of Incident Response & Security Teams (FIRST) Technical Colloquium... cont'd


*Mr. Stephen Isaboke, EBS, Principal Secretary, State Department for Broadcasting & Telecommunications, giving his speech during the conference.*


*Dr. Ed Barnett MBE, Chargé d'Affaires, British High Commission & Permanent Representative to UNEP and UN Habitat, Nairobi, making his remarks.*


*Mr. David Mugonyi, EBS, Director General/CEO, Communications Authority of Kenya, addressing delegates.*


*Mr. Lawrence Muchilwa, Africa Regional Liaison, Forum of Incident Response and Security Teams (FIRST), speaking during the conference.*

*A group photograph of participants during the conference.*

# The 2025 Annual Cybersecurity Conference and Forum of Incident Response & Security Teams (FIRST) Technical Colloquium... cont'd


*Dr. Vincent Ngundi, Director of Cyber Security, Communications Authority of Kenya (second left), making a point.*


*Col. (Dr.) James Kimuyu, Director of the NC4 Secretariat (second right), engaging the audience.*

*Dr. Joseph Sevilla, Director of @iLab Africa Research & Innovation Centre at Strathmore University (centre), Nairobi, articulating a point.*

*Mr. Bonface Asiligwa, President of the ISACA-Kenya Chapter, responding to a question.*

*Mr. Joseph Kimanga, Director of Strategy, Research & Project Management (second right), Communications Authority of Kenya, following the deliberations.*

*A section of delegates keenly following proceedings during the conference.*

# Training Programme on Mastering Proactive Defence and Threat Analysis

*Participants pictured during the training programme on Mastering Proactive Defence and Threat Analysis that was held from 13th to 17th October 2025, in Nairobi.*

The Authority, in partnership with the UK's Foreign, Commonwealth & Development Office (FCDO), hosted a four-day training programme on Mastering Proactive Defence and Threat Analysis from 13th to 17th October, 2025, in Nairobi. It was targeted at members of the National KE-CIRT/CC Cybersecurity Committee (NKCC) and was attended by 99 trainees.

The programme was designed to strengthen technical and analytical capabilities for proactive cyber threat mitigation. The training focused on building a strong understanding of Cyber Threat Intelligence (CTI) as a core component of modern cybersecurity, emphasising the shift from reactive security measures to intelligence-driven defence. Participants were introduced to the CTI lifecycle, including threat collection, analysis, dissemination and feedback, with practical exposure to intelligence sources such as open source intelligence (OSINT), social media intelligence (SOCMINT) and dark web monitoring.

The programme also emphasised the use of structured analytical frameworks, particularly the MITRE ATT&CK to map adversary tactics, techniques and procedures (TTPs) and improve threat prioritisation and incident response effectiveness. Hands-on sessions using platforms such as the Malware Information Sharing Platform (MISP), enabled participants to practice real-world intelligence sharing and collaborative threat analysis.

The training concluded with tabletop exercises (TTXs) that simulated realistic cyber incidents, allowing participants to apply intelligence-driven decision-making, assess response strategies and evaluate inter-agency coordination under pressure. Key takeaways included the importance of collaboration and information sharing, aligning technical threat intelligence with strategic and policy decisions and embedding CTI functions within operational security teams to enhance national cyber resilience.

# Workshop on National CIRT/ CERT/ CSOC Ecosystem Design

The Authority, in partnership with the UK's Foreign Commonwealth and Development Office (FCDO), hosted a workshop on National CIRT/CERT/CSOC Ecosystem Design from 7th - 9th October 2025, in Nairobi, bringing together key stakeholders from government, regulatory bodies and critical sectors to advance Kenya's national cybersecurity posture. The workshop was structured to conceptualise and operationalise a coherent national cyber incident response ecosystem and was attended by 35 participants.

Discussions focused on defining national priorities and responsibilities, clarifying coordination mechanisms and designing federated models for Computer Incident Response Teams (CIRTs), Computer Emergency Response Teams (CERTs) and Cybersecurity Security Operations Centres (CSOCs) across national, sectoral and organizational levels. Through scenario-based tabletop exercises (TTXs), participants validated proposed frameworks in a simulated environment.

The Authority acknowledged the workshop as a critical enabler of a resilient and intelligence-driven cyber defence architecture, noting that sustainable cyber resilience relies on more than technology alone and requires clear accountability, interoperable processes, and trusted information sharing arrangements, including the Traffic Light Protocol (TLP).

The outcomes reinforced the need to formalise a national responsibility matrix, institutionalize a CIRT federation model and strengthen policy alignment with international standards. The Authority affirmed that the lessons and frameworks developed will serve as a foundation for enhancing Kenya's preparedness, coordination and capacity to prevent, detect and respond to cyber threats effectively.

***Participants pose for a group photograph during the workshop. Looking on is Dr. Vincent Ngundi, Director, Cyber Security & Head of the National KE-CIRT/CC (second right, front row), Communications Authority of Kenya and Mr. Matt Jowett, Head of Cyber - Africa at the British High Commission (front row, centre), under the UK's Foreign, Commonwealth and Development Office (FCDO).***

# Training Programme on Operational Technology (OT) and Industrial Control Systems (ICS)

The Authority, in partnership with the UK's Foreign, Commonwealth and Development Office (FCDO), hosted a four-day training programme on Securing Operational Technology (OT) and Industrial Control Systems (ICS) from 17th to 20th November, 2025 in Nairobi. The programme targeted members of the National KE-CIRT/CC Cybersecurity Committee (NKCC) and was aimed at strengthening participants' technical competence and analytical capability in detecting, analysing and mitigating cyber threats within industrial environments.

The training brought together 35 participants from 16 organisations, promoting cross-sector collaboration and promoting an environment that encouraged knowledge exchange, joint problem-solving and the development of practical skills essential in modern cyber defence. The training also provided a structured blend of theoretical fundamentals, technical hands-on practice and strategic governance discussions designed to enhance Kenya's preparedness for OT/ICS-related cyber threats.

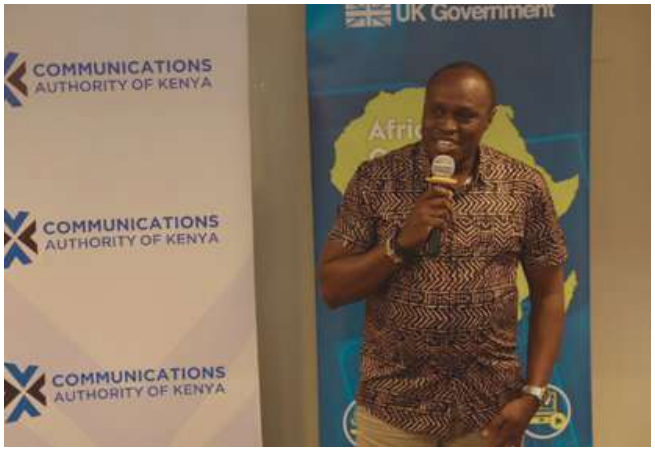
The technical aspect of the training provided participants with an end-to-end understanding of the OT lifecycle, focusing on both data-driven and behavioural approaches to threat detection, incident response and resilience enhancement. The training began by introducing the participants to OT and ICS. After a solid foundation was established, the trainers sought to deepen the participants' understanding of industrial systems through the Purdue Model and key industrial protocols. This was followed by a day entirely focused on hands-on attack-and-detect exercises within a simulated OT environment. The training was finalised by a discussion on strategic governance, resilience building and long-term protection of critical national infrastructure (CNI).

Key lessons learnt highlighted the need for strengthened integration and coordination between Information Technology (IT) and Operational Technology (OT) environments, the value of sustained multi-stakeholder collaboration and the importance of real-world simulation exercises in enhancing cyber resilience. These insights highlighted existing gaps in preparedness and the need for coordinated, practical approaches to securing critical OT systems.

It was further established that there is a need to develop a comprehensive national OT security framework, with the Authority taking a lead role in the development of sector-specific OT security guidelines. Additionally, the findings emphasised the importance of continuous capacity-building programmes through regular training initiatives, as well as strategic investment in a dedicated national cyber range to support realistic and scalable OT simulation and testing exercises.

# Training Programme on Operational Technology (OT) and Industrial Control Systems (ICS).... cont'd







*Moments captured during the trainng programme on Operational Technology (OT) and Industrial Control Systems (ICS) that was held from 17th to 20th November, 2025 in Nairobi.*

# 53rd Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

The 53rd National KE-CIRT/CC Cybersecurity Committee (NKCC) meeting was held on 15th October 2025 in Nairobi .The NKCC draws its membership from over 50 public and private sector organisations from the critical information infrastructure (CII) sector in the country. It's main objective is to nurture trust networks amongst stakeholders, so as to build capacity and facilitate the sharing of information on new and emerging cybersecurity trends and to identify a collective strategy to address these emerging issues.

The NKCC holds quarterly meetings during which the National KE-CIRT/CC provides updates on emerging threats, tactics, techniques and procedures (TTPs) utilised by diverse threat actors. During these meetings, the various sectoral Computer Incident Response Teams (CIRTs) apprise members on the trends and patterns observed within their respective domains.

During the meeting, members identified insider threats as a key concern, while noting significant improvements in identity and access management following the implementation of Multi-Factor Authentication (MFA). Members further reported that regular internal and external audits had assisted in uncovering previously unidentified vulnerabilities, which are now informing future operational and infrastructure protection plans. Continuous cybersecurity awareness initiatives were emphasised as critical to addressing human-factor risks, with the sector recognising that effective cybersecurity requires a balanced approach combining robust technical controls with behavioural risk mitigation.

Members outlined the importance of social media monitoring as a means of identifying early indicators of cyber incidents and emerging public concerns. Regular vulnerability assessments, strategic partnerships and proactive patching were highlighted as key measures for maintaining platform security. However, client-side risks particularly the sharing of credentials, which undermines the effectiveness of MFA, were identified as a significant challenge, outlining the need for user education and awareness initiatives. In addition, various government agencies noted that disaster recovery and resilience planning efforts were ongoing, and emphasised the critical role of intelligence sharing and continuous capacity building in strengthening national cyber readiness.

In conclusion, the meeting recognised measurable progress in strengthening Kenya's cybersecurity landscape, supported by reduced threat activity, increased cyber threat advisories and continuous capacity building initiatives. However, members acknowledged that insider threats and human behaviour remain persistent challenges. The Chair commended members for their dedication and collaboration in safeguarding the nation's cyberspace.

# 2nd National Conference On Technology-Faciliated Gender-Based Violence (TFGBV) In Universities & TVETs In Kenya

The Authority participated in the 2nd National Conference on Technology-Facilitated Gender-Based Violence (TF-GBV) in Universities and TVETs held from 8th to 10th December, 2025 at Kibabii University, Bungoma. In its role as the regulator for the ICT sector in Kenya, the Authority contributed a regulatory and cybersecurity perspective, highlighting the growing risks of TF-GBV, the importance of online safety, digital hygiene and the use of secure digital platforms within institutions of higher learning .

The Authority also emphasised the need for harmonised institutional policies, effective reporting and response mechanisms and regulatory guidance to support survivor-centred approaches. The participation reinforced the Authority's mandate to promote a safe, secure and trusted digital environment, supported national cybersecurity and digital protection priorities and strengthened multi-stakeholder collaboration with government, academia, youth and civil society in addressing online safety challenges in learning institutions.

*The Cabinet Secretary for Youth Affairs, Creative Economy and Sports, H.E. Hon. Salim Mvurya delivering his speech at the conference.*

*Conference participants pose for a group photograph.*

*Ms. Donna Owiti, Cyber Security Resillience Officer, presenting her perspectives during a panel discussion.*

# Outlook for the Next Quarter

In collaboration with the UK's Foreign, Commonwealth & Development Office (FCDO), the Authority will host a training programme on information sharing designed to strengthen Kenya's national cybersecurity information sharing capability. The programme aims to transition from informal, ad-hoc exchanges to a structured, well-governed and operationally effective national information sharing model.

The programme will focus on strengthening frameworks, governance arrangements, coordination mechanisms and operational workflows to enable effective information sharing among various stakeholders such as the Authority's National KE-CIRT/CC, the National Computer and Cybercrimes Coordination Committee (NC4), various sectoral Computer Incident Response Teams (CIRTs) and Cyber Security Operations Centres (CSOCs), relevant sector regulators and diverse critical information infrastructure operators.

International best practices will be adapted to Kenya's national context, ensuring alignment with national priorities, legal frameworks and institutional mandates.

# Thank You

## We're here to help. Report an incident.

Working round the clock to safeguard Kenya's cybersecurity landscape.

**Email**
incidents@ke-cirt.go.ke

**Hotlines**
+254 703 042700
+254 730 172700

**Website**
www.ke-cirt.go.ke

**Social Media**
@KeCIRT

**Download the KE-CIRT App**
Google Play App Store