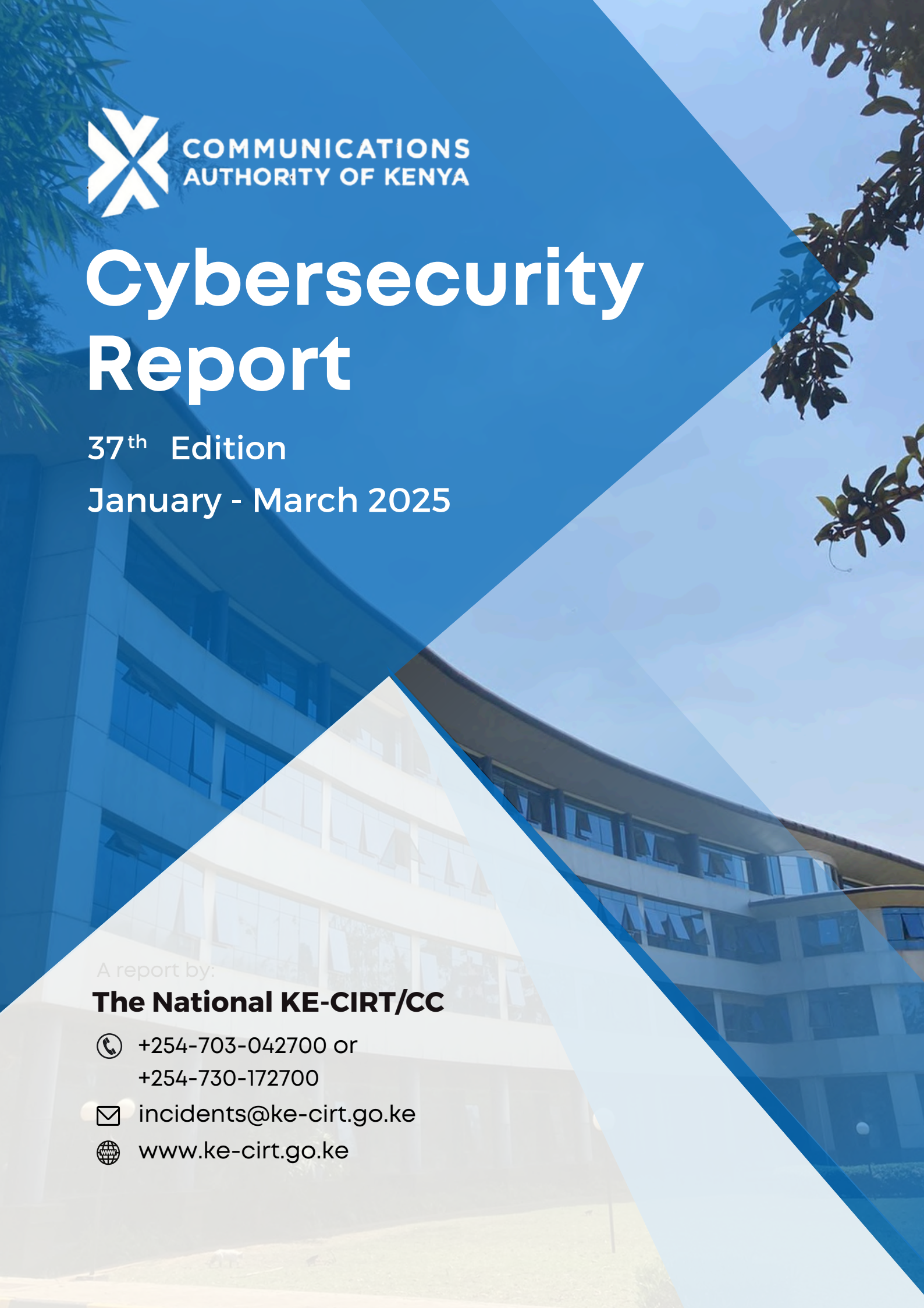
COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

37th Edition

January - March 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 realization 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 Telcom Sector.

Director General's Perspective

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

As we begin the year 2025, we look forward to the opportunities and innovations that lie ahead. At the same time, the Authority remains cognisant of the persistent cybersecurity threats that continue to challenge individuals, organisations and entire sectors. Threats such as ransomware, Distributed Denial of Service (DDoS) attacks, social engineering and phishing scams, and system misconfigurations remain at the forefront of security concerns. These threats not only disrupt business operations but also compromise data privacy, undermine user trust and cause significant financial and reputational damage.

Ransomware attacks are becoming more targeted and sophisticated, while phishing and social engineering tactics continue to exploit human weakness rather than technical vulnerabilities. DDoS attacks continue to impact service availability and basic system misconfigurations can lead to major data breaches. These ongoing challenges on the global cyber threat landscape highlight the importance of implementing comprehensive cybersecurity strategies, continuous public awareness and user training, and proactive approaches to risk management.

Over the period January - March 2025, the National KE-CIRT/CC detected over 2.5 billion cyber threat events which represented an increase of over 200% from the previous period, October - December 2024. In response to the detected cyber threat events, the National KE-CIRT/CC issued over 13 million cyber threat advisories between the period January - March 2025, which represented an increase of about 14% compared to the previous period, October - December 2024.

During the period, there was a significant increase in the number of advisories on implementing organisational access controls, hardening antivirus software and firewalls, regularly patching vulnerable systems, and utilising multi-factor authentication and strong passwords.

These ongoing global trends are largely driven by the rapid growth of Internet of Things (IoT) devices, which often lack comprehensive security features. Additionally, the continued widespread utilisation of botnets and other DDoS attack techniques have also contributed significantly to these trends. Botnets remain a key tool for malicious actors due to their decentralised structure, making them highly effective for large-scale attacks.

DDos attacks, in particular, can severely disrupt essential services, leading to financial losses and reputational damage for organisations. Furthermore, cybercriminals are increasingly leveraging artificial intelligence (AI) to enhance the magnitude, accuracy and complexity of cyber attacks. By using AI, threat actors can automate and adapt their methods, making them harder to detect and defend against.

Going into the new year, the Authority will continue to strengthen cybersecurity as not just a technical requirement but as a shared responsibility. As the digital landscape evolves, so must our cyber defences. Let this year be one of increased awareness, collaboration and resilience in the face of emerging and persistent cyber threats. With the right mindset and commitment, we can turn these challenges into opportunities for growth and innovation.

In line with the 2023 - 2027 Strategic Plan, the Authority remains committed to advancing cybersecurity by promoting best practices, strengthening threat detection capabilities, and supporting ongoing public awareness and education initiatives to help all stakeholders in the cybersecurity value chain to navigate the constantly evolving cyber threat environment.

Mr. David Mugonyi, EBS
Director General/CEO

Cyber Threat Landscape Overview

Global Cyber Threat Landscape Overview

1. Ransomware

Ransomware attacks became more sophisticated, with attackers increasingly using double extortion tactics to not only encrypt data but also threaten to leak it if the ransom was not paid. Critical sectors, including healthcare, finance and infrastructure, were heavily targeted. The *CLOP* ransomware gang exploited a vulnerability in MOVEit Managed File Transfer (MFT), affecting over 2,600 organizations and exposing 77 million records and impacting government entities in the energy sector. Additionally, the Black Basta ransomware group exploited privilege escalation vulnerabilities, allowing them to infiltrate unpatched systems.

Organisations that had patched systems promptly and implemented offline backups were able to recover faster. The use of zero-trust architecture and enhanced endpoint detection also helped prevent lateral movement of ransomware within networks.

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

DDoS attacks continued to increase in frequency becoming larger in scale. Attackers increasingly leveraged botnets to disrupt business operations. The Gorilla botnet launched over 300,000 attacks, targeting government agencies and critical infrastructure. Attackers also made use of DDoS-as-a-Service, where botnets could be rented for as low as $5 per hour, making attacks more accessible to cybercriminals. Some of the largest attacks exceeded 71 million requests per second, overwhelming even well-defended systems.

Organisations that used AI-driven DDoS mitigation tools and cloud-based protection services managed to counteract attacks effectively. Those that had scalable bandwidth solutions and traffic filtering mechanisms suffered less downtime.

3. Social Engineering & Phishing

AI-generated phishing attacks and deepfake scams saw a significant rise, making social engineering tactics more convincing and harder to detect. Cybercriminals used AI-generated voices and videos to impersonate high-profile executives and government officials, tricking employees into transferring funds or disclosing sensitive information. Additionally, phishing emails crafted using AI had fewer grammatical errors, making them more credible.

Organisations that implemented phishing-resistant authentication methods, such as passkeys and biometrics, were better protected. Security awareness training focused on identifying deepfake threats also helped reduce successful scams.

Global Cyber Threat Landscape Overview... cont'd

4. System Misconfiguration Exploits

Misconfigured systems led to major security breaches, with attackers exploiting known vulnerabilities in widely used software. The GOAnywhere Managed File Transfer (MFT) breach allowed attackers to create admin accounts and take full control of systems, affecting organizations that had not updated to version 7.4.1. Additionally, a PHP vulnerability in Windows servers using default XAMPP configurations led to ransomware infections, with attackers demanding payments of 0.1 Bitcoin (BTC) per attack.

Organisations that performed regular security audits, applied software patches promptly, and disabled unnecessary default configurations significantly reduced their exposure.

5. Emerging Threats

State-sponsored cyberattacks and AI-powered cyber threats increased in complexity, targeting government agencies and critical sectors. Nation-state actors launched targeted cyber espionage campaigns against government institutions and critical infrastructure providers. Meanwhile, cybercriminals leveraged AI-powered malware and automation to launch large-scale attacks with minimal human intervention. The rise of poorly secured Internet of Things (IoT) devices further expanded the attack surface, leading to increased breaches.

Countries that strengthened diplomatic cyber agreements and enforced strict cybersecurity compliance within critical sectors experienced fewer successful attacks. The implementation of AI-driven threat detection also helped mitigate AI-powered cyber threats .

Cyber Threat Landscape Roundup

Total Cyber Threats Detected

2,538,283,798 | **201.85%**

The National KE-CIRT/CC detected over **2.5 billion** cyber threat events during the three-month period between **January - March 2025**, which represented a **201.85% increase** from the threat events detected in the previous period, October - December 2024. We continued to enhance the dissemination of cyber threat advisories to critical information infrastructure sectors, in response to the cyber threats observed.

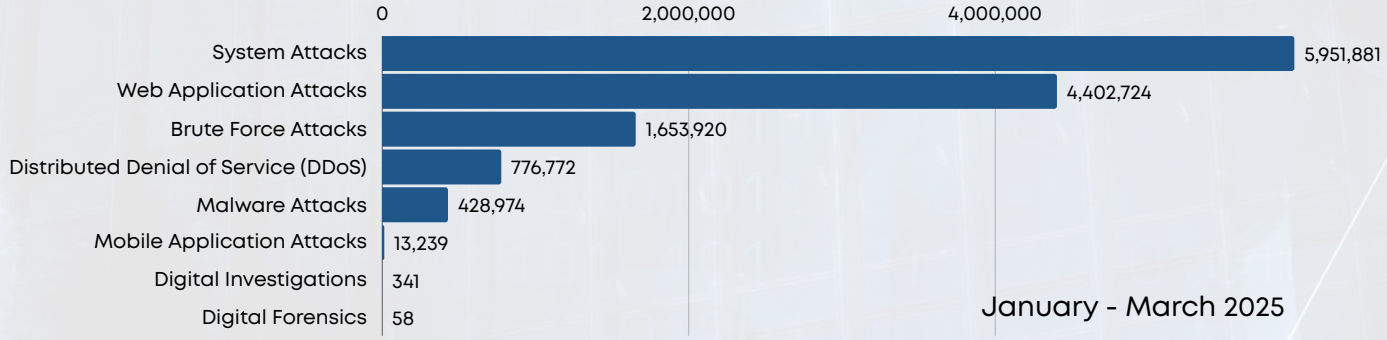
Inadequate patching of systems, low user awareness of various threat vectors including phishing and other forms of social engineering attacks, and the increasing use of AI-driven attacks and machine learning technologies are among the reasons for the rise in cyber threats that have been detected.

Total Cyber Threat Advisories Issued

13,227,909 | **14.18%**

In response to the detected cyber threat events, the National KE-CIRT/CC issued **13,2227,510** advisories between the period **January - March 2025**, which represented a **14.18%** increase compared to the advisories that were issued during the previous period, October - December 2024.

During the period under review, the Authority increasingly disseminated advisories on regularly patching vulnerable systems, using multi-factor authentication and strong passwords, hardening firewalls and antivirus software, establishing organisational access controls, and keeping systems up to date

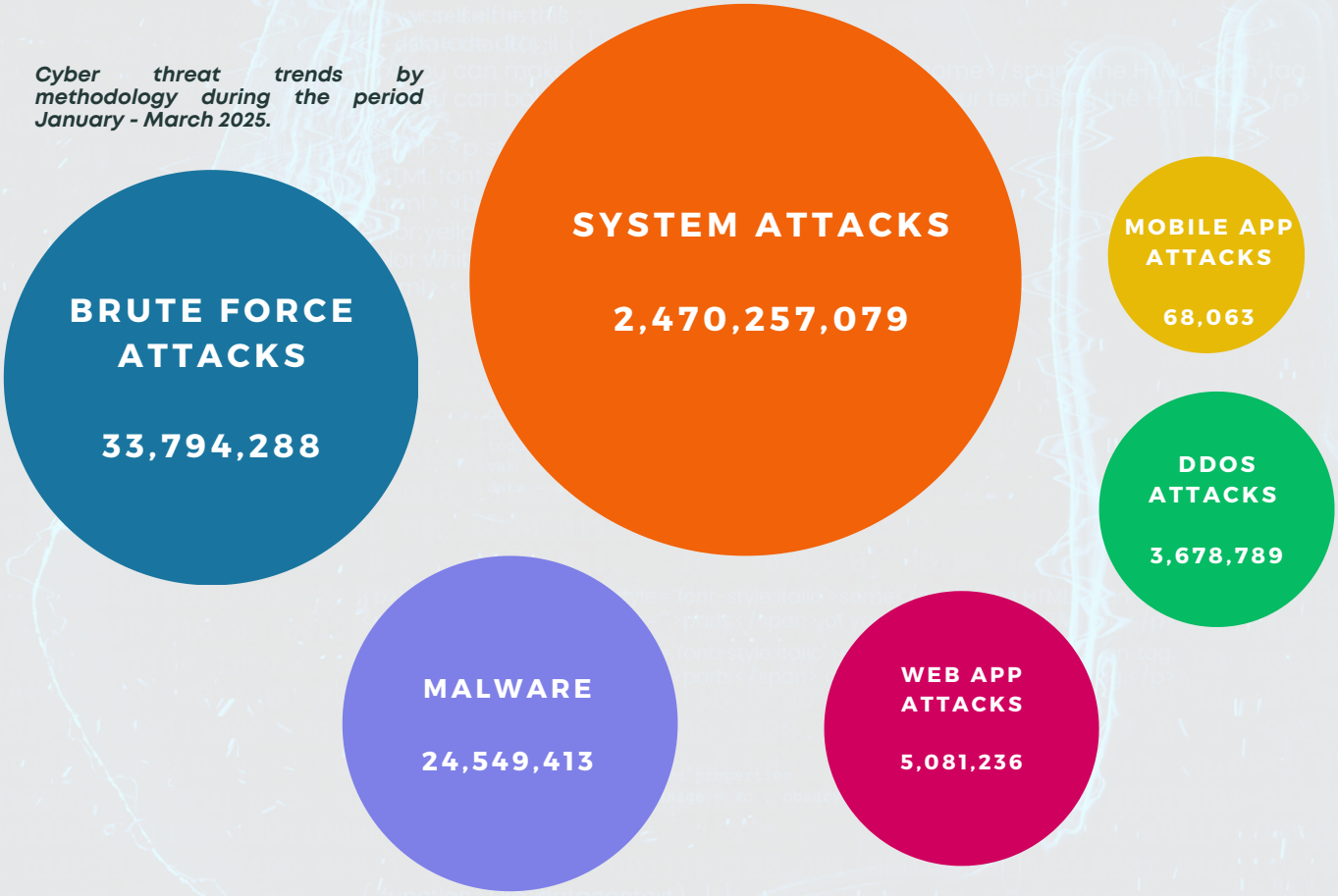


Cyber Attack Vector Trends

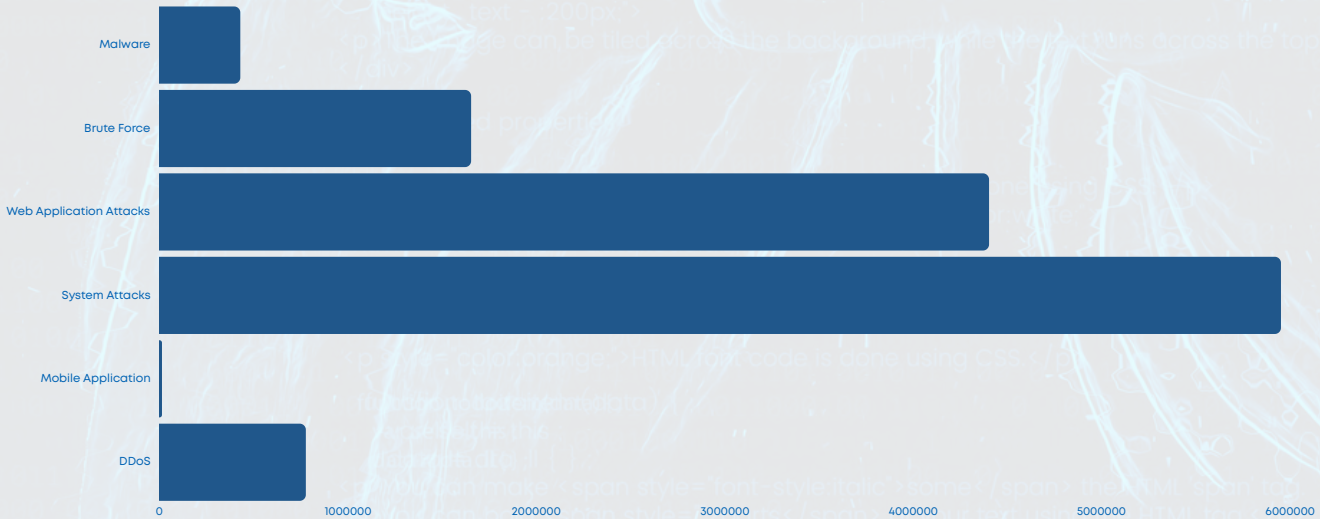
System misconfigurations and brute force attacks remained the most common during the quarter, aligning with global cyber threat trends. Contributing factors to system misconfiguration-related cyberattacks include low levels of cyber risk awareness, the use of outdated or deprecated systems, default login credentials, and insufficient investment in technological infrastructure.

On the other hand, brute force attacks may be attributed to poor password management, increased automation—such as the use of cloud services—and weak security configurations.

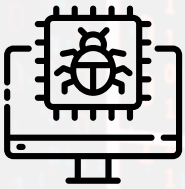
Cyber threat trends by methodology during the period January - March 2025.



Comparison of cyber threat advisories (per vector) issued during the period **January to March 2025.**



Malware Trends



Threats Detected

24,549,413

27.63%

Advisories Issued

428,974

6.02%

During the three-month period between **January to March 2025,** the National KE-CIRT/CC detected **24,549,413** malware threat attempts targeted at the critical information infrastructure sector. This represented a **27.63%** decrease from the previous period, October to December 2024.

Internet Service Providers (ISPs) and cloud service providers were the primary targets of most attacks, with threat actors targeting end-user devices, Internet of Things (IoT) devices, ISP-owned web applications and networking equipment, cloud-based services, and government systems. Additionally, attackers exploited supply chain and zero-day vulnerabilities.

Top Targeted Systems

- End-User Devices
- Internet of Things (IoTs)
- Web Applications
- Networking Devices

Top Affected Industries

- Internet Service Providers
- Cloud Service Providers
- Government
- Academia/Education

Top Targeted Exploits

- FortiManager Missing Authentication (CVE-2024-47575): This vulnerability enables attackers to bypass authentication, potentially allowing them to deploy malware or malicious scripts on compromised systems.
- Oracle WebLogic Server Vulnerability (CVE-2024-21260):Attackers exploiting this vulnerability can gain unauthorized access to deploy malware, such as ransomware or cryptominers, on affected systems.
- CWindows Common Log File System Zero-Day (CVE-2024-49138):This zero-day vulnerability allows attackers to execute arbitrary code. Malware often exploits zero-day vulnerabilities for persistence and further infiltration.

Malware attacks primarily targeted vulnerable systems and those containing sensitive or financial data. These attacks aimed to encrypt or corrupt user data, damage brand reputation, deploy backdoors and exfiltrate information.

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

5,081,236

11.85%

Advisories Issued

4,402,724

0.96%

During the three-month period between **January to March 2025**, the National KE-CIRT/CC detected **5,081,236** web application attack attempts targeted at the critical information infrastructure sector. This represented a **11.85%** increase from the previous period, October to December 2024.

The primary targets of these attacks were government systems and ISPs. Attackers specifically focused on user login credentials, vulnerable web browsers, and database servers belonging to government agencies and ISPs. Most attackers exploited weaknesses in SSL/TLS security configurations.

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/Educa

Top Targeted Exploits

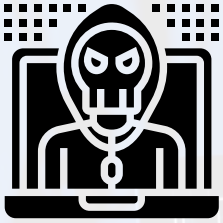
- Broken access control
- Injection
- Insecure design
- Security misconfiguration
- Identification and authentication

During the period, web application attacks targeted systems considered weak and containing valuable data. The goal was to disrupt service availability, alter databases, and leak private information to damage the organisation's reputation.

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

33,794,288

2.85%

Advisories Issued

1,653,920

29.28%

During the three-month period from **January to March 2025**, the National KE-CIRT/CC detected **33,794,288** brute force attack attempts majorly targeting the critical information infrastructure sector. This represented a **2.85%** decrease from the previous period, October to December 2024.

Most attacks were directed at cloud service providers and government systems, with a specific focus on database servers and user login credentials of cloud-based services and government agencies. Attackers primarily exploited vulnerabilities in database servers, login credentials, and the Remote Desktop Protocol (RDP).

Top Targeted Systems

- Login Pages
- Database Servers
- Remote Access Systems
- Cloud Service Providers
- Mail Servers
- Content Management Systems (CMS)

Top Affected Industries

- Cloud Service Providers
- Government

Top Targeted Exploits

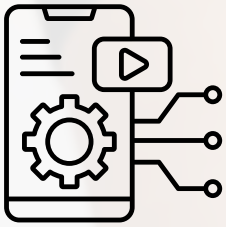
- Exposed Remote Desktop Protocol (RDP)
- Credential Brute-Forcing
- Credential Spoofing
- Credential Sniffing

During the three-month period, systems believed to contain sensitive data—such as login credentials and financial information—were the primary targets of brute force attacks. The main objectives of these attacks were to gain elevated privileges, obtain unauthorized access, and exfiltrate sensitive data for financial gain.

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.
- Disconnect devices from the network if not in use.
- Update softwares to the latest versions.

Mobile Application Attack Trends



Threats Detected

68,063

50.74%

Advisories Issued

13,239

61.17%

During the three-month period from **January to March 2025**, the National KE-CIRT/CC detected **68,063** mobile application attack attempts targeting end-user devices. This represented an **50.74%** decrease from the previous period, October to December 2024.

Most attacks targeted mobile devices and Android TVs, with attackers primarily using malware to 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

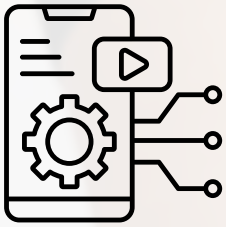
- Improper Credential Usage
- Inadequate Supply Chain Security
- Insecure Authentication
- Insufficient Input/Output Validation

Attackers targeting mobile applications primarily seek to steal sensitive user data, including financial information, login credentials, and personally identifiable information, for illicit purposes.

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

3,678,789

75.63%

Advisories Issued

776,772

158.76%

During the three-month period **January to March 2025**, the National KE-CIRT/CC detected **3,678,789** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure. This represented a **75.63%** decrease from the previous period, October to December 2024.

The majority of attacks targeted government and health institutions, exploiting vulnerabilities in remote desktop services and insecure protocols to flood legitimate servers with requests, thereby preventing authorized users from accessing them.

Top Targeted Systems

- Email Servers
- Web servers
- Database Servers

Top Affected Industries

- Health Sector
- Government

Top Targeted Exploits

- Increase in network time protocol (NTP) amplification DDoS attack
- Windows Remote Desktop Services Denial of Service Vulnerability
- Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability

Over the three-month period, attackers primarily aimed to degrade service quality or render critical services unavailable to system users.

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

2,470,257,079

228.30%

Advisories Issued

5,951,881

15.64%

The majority of attacks targeted the ICT industry, focusing on operating systems and database servers owned by cloud service providers and ISPs. Attackers primarily leaked user login credentials and exploited vulnerabilities in outdated operating systems. The continued prevalence of system vulnerabilities can be attributed to the proliferation of inherently insecure Internet of Things (IoT) devices.

Top Targeted Systems

- Database Servers
- Operating Systems
- Network Devices
- Web Applications
- Remote Access Systems

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

System attacks targeted the critical information infrastructure sector, which holds sensitive data such as financial information. The objectives of these attacks were to disrupt, compromise, and sabotage essential systems and services on a large scale.

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

Workshop on Strengthening Cyber Resilience

The Authority, in collaboration with the UK's Foreign, Commonwealth & Development Office (FCDO), hosted a workshop on Strengthening Cyber Resilience for members of the National KE-CIRT/CC Cybersecurity Committee (NKCC). The workshop took place from February 10th – 13th, 2025 at the Mövenpick Hotel & Residences, Nairobi. This activity aligns with the Authority's commitments to enhancing national cybersecurity resilience through improved incident response capabilities, strengthening collaboration among critical infrastructure organisations, building local expertise to address emerging cybersecurity threats and supporting Kenya's digital transformation agenda and regulatory compliance in cybersecurity. It also aligns with fulfilling the Strategic Goal titled *Empowerment and Protection of Consumers of ICT Services* as outlined in the Authority's 2023-2027 Strategic Plan.

The four (4)-day workshop focused on addressing emerging cyber threats such as fraud, ransomware, forensic investigation gaps, Optical Network Unit (ONU) security vulnerabilities, incident response strategies, cybersecurity workforce development, among others. Ninety-four (94) trainees took part in the training, bringing together key stakeholders from the NKCC sector CIRTs, namely, e-government, telecommunications, banking & finance, academia, health, among others.

During the workshop, the main thematic areas were as follows:

- Cyber Resilience and Risk Management: Discussions centred around the importance of a proactive, risk-based approach to cybersecurity. Participants assessed how organisations can develop their cyber capabilities by integrating cybersecurity into their overall risk management strategies.
- Information Sharing for Enhanced Cyber Resilience: The focus was on the role of information sharing in strengthening cyber resilience. Participants observed that effective information exchange among stakeholders is essential for early threat detection and coordinated response to cyber incidents.
- Strengthening National and Organisational Cyber Resilience: Participants identified the actionable measures that organisations and governments can take to improve cyber resilience. Discussions centred around the need for continuous investment in cybersecurity capacity building, policy development and cross-sector collaboration.
- Cybersecurity Awareness and Cultural Shifts in Cyber Resilience: Discussions centred on the human element of cybersecurity and the need to cultivate a culture of resilience across the cyber security value chain. Participants explored how cybersecurity awareness, behavioural change and organisational culture play a crucial role in mitigating cyber risks.

The workshop provided useful insights into the complexities of cybersecurity risk management, incident response and information sharing. To build on these discussions, the following recommendations were proposed:

- Adoption of a risk-based approach to cybersecurity by integrating cybersecurity risk management into enterprise risk management frameworks.
- Enhancing threat intelligence sharing through structured mechanisms for information sharing while adhering to the Data Protection Act, 2019, and its attendant regulations.
- Developing and implementing incident response (IR) plans that outline various roles and responsibilities, and the escalation procedures during a cyber incident.
- Conducting cyber awareness and capacity building programmes for diverse target groups to help in keeping up with evolving threats and to promote a national cyber hygiene culture.
- Strengthening legal and regulatory frameworks on cybersecurity to address new and emerging threats. This facilitates compliance with regulations and adoption of industry best practices.

Workshop on Strengthening Cyber Resilience... cont'd

- Leveraging emerging technologies for cyber defence such as the use of AI-driven cybersecurity solutions, automation and threat detection systems. The adoption of a zero-trust security model was also discuseed as a mechanism to mitigate the risk of insider threats and unauthorized access.

The Authority's Director General/CEO, Mr. David Mugonyi, officially closed the workshop, during which participants were also presented with certificates in recognition of their participation.

Highlights from the workshop on Strengthening Cyber Resilience, where participants engaged in hands-on learning and collaborative discussions to enhance their knowledge and skills in cybersecurity. The workshop took place from February 10th – 13th, 2025 at the Mövenpick Hotel & Residences, Nairobi.

50th Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

The National KE-CIRT/CC Cybersecurity Committee (NKCC) draws its membership from over 50 public and private sector organisations from the critical information infrastructure (CII) sector in the country. The main objective of the NKCC 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 emphasised the importance of developing tailored technical training programmes that incorporate new and emerging technologies, as well as the evolving cyber threat landscape. This would be crucial in ensuring that cybersecurity professionals stay ahead of adversaries and are therefore able to effectively protect organisations within the critical information infrastructure sector.

In addition, members highlighted the need for a centralised information-sharing portal or platform to enhance the real-time exchange of cyber threat intelligence within the critical information infrastructure sector. This would improve incident response, promote collaboration and strengthen Kenya's cybersecurity resilience.

To secure leadership buy-in for cybersecurity initiatives, members stressed the importance of increasing senior management representation in technical workshops. This engagement would be crucial for enhancing their understanding of the cybersecurity challenges organisations face, thereby encouraging resource allocation and policy support.

The 50th Meeting of the NKCC was held on 12th February, 2025, on the sidelines of the workshop on Cybersecurity Resilience at Mövenpick Hotel & Residences, Nairobi.

Members follow proceedings during the 50th meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC) that was held on 12th February 2025 in Nairobi.

2025 Cybersecurity Bootcamp Competition

A thriving digital economy calls for a competent workforce with the necessary skills and tools to counter the ever-increasing risks posed by cyber threat actors. However, inadequate capacity continues to be a major challenge in effective cybersecurity management in Kenya's digital landscape.
In view of this, the Authority in its 2023 – 2027 Strategic Plan committed to enhancing the national cybersecurity readiness and resilience through various activities aimed at empowering tertiary, college and university students, industry professionals and leaders, technical officers, government officials and consumers.

The Authority, through the National KE-CIRT/CC, hosted the 2025 Cybersecurity Bootcamp Competition, now in its fourth year. The competition aimed to foster the development of local cybersecurity capabilities, addressing current gaps and enhancing collective cyber readiness and resilience. This aligns with the government's bottom-up economic transformation agenda (BETA), contributing to a safer and more sustainable digital superhighway.

This year, the competition, held in collaboration with Huawei Technologies Kenya, attracted 3,377 applicants from universities, colleges, and tertiary institutions across the country, including the University of Nairobi, Strathmore University, Technical University of Kenya, Meru University of Science and Technology, University of Embu, Machakos University, Dedan Kimathi University of Technology, and Jaramogi Oginga Odinga University of Science and Technology, among others.

This year's theme, 'Building Cybersecurity Capacity to Drive a Digitally Transformed Nation,' highlighted the strategic initiative to equip participants with essential cybersecurity skills while fostering a culture of awareness and preparedness.

The competition was structured into three phases:

- Phase one involved online, self-paced learning, where students independently completed coursework followed by a rigorous assessment.
- Phase two saw successful candidates advance to an online, instructor-led training session.
- Phase three was an intensive in-person training, where the top 15 students from various regions across the country were invited to Nairobi for hands-on practical sessions. During this phase, participants formed teams of three to compete for top positions.

Throughout this competition, the students were trained on various aspects of network security, firewall security, encryption, PKI certification systems and cyber security emergency response. This included but was not limited to network security concepts and specifications, common network security threats and threat prevention, firewall NAT technologies, firewall security policies, firewall user management technologies, firewall intrusion prevention technologies, fundamentals of encryption technologies and technology applications.

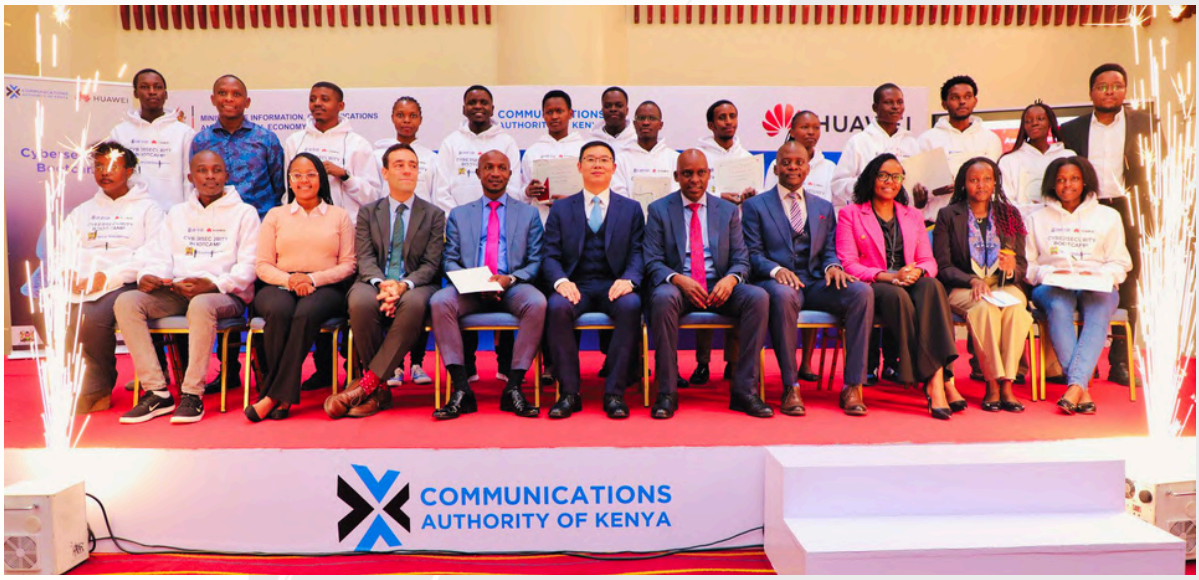
The closing ceremony of the 2025 Cybersecurity Bootcamp Competition, that was held at Mövenpick Hotel & Residences in Nairobi, marked the successful conclusion of this dynamic event.

2025 Cybersecurity Bootcamp Competition... cont'd

The event was graced by Mr. David Mugonyi, EBS, Director General/CEO of the Communications Authority of Kenya, and Mr. Steven Zhang, Deputy CEO of Huawei Technologies Kenya. Also in attendance were senior management representatives from both the Authority and Huawei Technologies Kenya, staff members from both organisations, the 15 competition finalists, and the media.

In his keynote address, Mr. Mugonyi discussed the evolving cybersecurity landscape, emphasizing the critical role that young professionals must play in safeguarding the country's digital future. He encouraged the students to build on their achievements, sharing his own journey from university life to his current leadership position. Mr. Zhang, on the other hand, highlighted the company's commitment to nurturing cybersecurity talent through various development programmes.

The event concluded with an awards ceremony, where the top three teams, comprising three students each, were feted for their outstanding performance.



Participants pose for a group photo during the closing ceremony of the 2025 Cybersecurity Bootcamp competition on 26th March 2025, at Mövenpick Hotel & Residences. Looking on is Mr. David Mugonyi, EBS, Director General/CEO of the Communications Authority of Kenya (front row, 5th from right) and Mr. Steven Zhang, Deputy CEO, Huawei Technologies Kenya (front row, 6th from right).

Cybersecurity Study & Mentorship Tours

The study and mentorship tours took place over three days, from March 26th to 28th, 2025, and involved six key organisations that play significant roles in Kenya's ICT sector. The main objective of these tours was to give participants a comprehensive understanding of the cybersecurity, telecommunications, internet governance, and data center operations industries. Through visits to these organisations, participants gained valuable insights into the operational, regulatory, and technological frameworks that influence Kenya's digital ecosystem.

Additionally, the tours offered networking opportunities with industry experts and an exclusive look at cutting-edge technologies currently in use. A key focus was to understand best practices in cybersecurity, domain management, internet governance and critical infrastructure protection. The tours were particularly valuable for the competition winners, providing them with hands-on insights into the real-world applications of cybersecurity and ICT policies.

The study and mentorship tours included visits to the following organisations:

- Kenya Network Information Centre (KeNIC) – The official registry managing the .KE Country Code Top-Level Domain (ccTLD).
- Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) – The Cyber Security Operations Centre (CSOC) for the ICT and Telcom Sector.
- Safaricom PLC – Kenya's largest telecommunications service provider, offering mobile, Internet and financial services.
- Airtel Kenya Ltd. – The country's second-largest telecommunications provider, offering mobile and Internet services.
- Technology Service Providers of Kenya (TESPOK) - TESPOK plays a key role in advocating for policy, promoting infrastructure development and representing the interests of ICT service providers in Kenya.
- Konza Technopolis – A smart city development project designed to position Kenya as a leading technology and innovation hub.

The study and mentorship tours provided an invaluable opportunity to engage with key players in Kenya's ICT ecosystem. Participants gained a deeper understanding of cybersecurity, regulatory frameworks, and emerging technologies shaping the industry.

The insights gathered by the finalists will be instrumental in guiding future research, policy formulation, and industry engagement. Strengthening industry-academic collaborations, increasing cybersecurity awareness, and enhancing regulatory enforcement are critical steps toward advancing Kenya's position as a leader in technology and innovation.

Based on discussions and feedback from participants, the tours were deemed highly effective and beneficial. They provided practical skills that could be immediately applied in cybersecurity projects and research, as well as in participating in various Capture The Flag (CTF) competitions, helping to reinforce and enhance their technical capabilities.

In particular, and in alignment with the Authority's strategic direction, participants recommended additional support for pursuing cybersecurity certifications like CEH and CISSP, as well as opportunities for internships and research projects tailored to their interests and what they learned during the tour. Additionally, the Authority plans to collect feedback from both students and industry hosts to refine and improve future tours, ensuring they are better aligned with student needs and industry expectations.

Cybersecurity Study & Mentorship Tours... cont'd

The following images are from the Cybersecurity Study & Mentorship Tours, showcasing the participants' immersive learning experiences and professional development opportunities in the field of cybersecurity:

The students' visit to the Kenya Network Information Centre (KeNIC), where they explored domain management, internet governance and cybersecurity best practices.

During their visit to the Authority's National KE-CIRT/CC, the students gained insights into cybersecurity incident response, threat management and national cybersecurity strategies.

Cybersecurity Study & Mentorship Tours... cont'd

A visit to Safaricom PLC, where participants explored innovative telecommunications solutions, cybersecurity strategies and industry best practices.

During a tour of Airtel Kenya, students engaged with industry experts to gain insights into telecommunications, network security and innovative digital solutions.

Above left: During a visit to Technology Service Providers of Kenya (TESPOK), the students gained an understanding of TESPOK's role in promoting infrastructure development and representing the interests of ICT service providers in Kenya.
Above right: The future of smart city development in Kenya outlined during a tour to Konza Technopolis.

Workshop on Capacity Building Actions on Cybercrime and Electronic Evidence Identified in Kenya

The GLACY-e project, which is a joint initiative by the European Union and the Council of Europe, along with INTERPOL, partnered with the Authority and the National Computer and Cybercrime Coordination Committee (NC4) to organize a workshop focused on assessing capacity-building needs for cybercrime legislation in Kenya. The workshop titled *Capacity Building Actions on Cybercrime and Electronic Evidence Idetified in Kenya* was held at Fairview Hotel in Nairobi, from 10th to 11th March 2025.

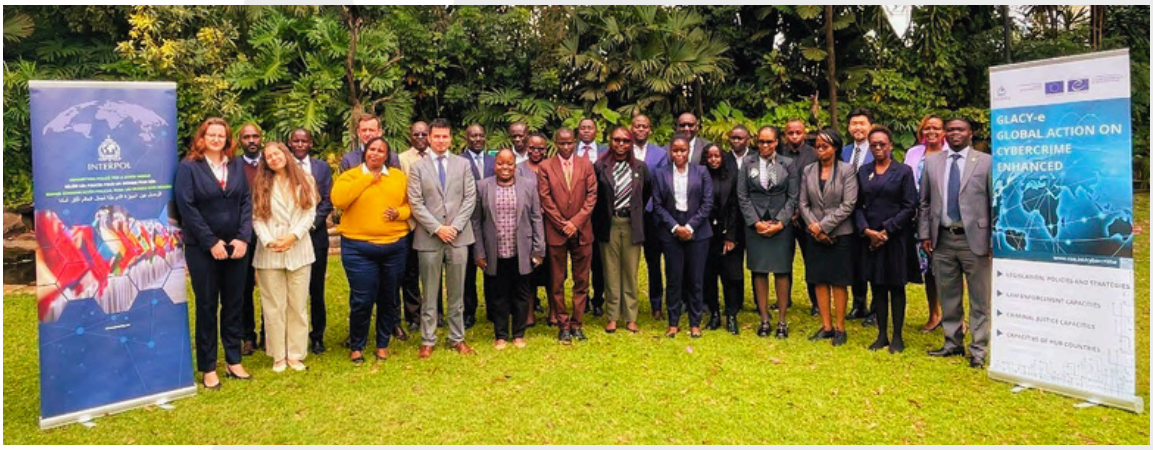
The event brought together officials from various government institutions, including Office of the President, Ministry of Foreign and Diaspora Affairs, Ministry of Interior and National Administration, Ministry of Information, Communications and the Digital Economy, Ministry of Defence, State Law Office, Directorate of Criminal Investigations (DCI), Office of the Director of Public Prosecutions (ODPP), Kenya Judiciary Academy (KJA), Office of Data Protection Commissioner (ODPC), Financial Report Centre (FRC), and eCitizen.

One of the key outcomes of the workshop was a clearer understanding of the benefits and opportunities that come with Kenya's participation in the GLACY-e project. Participants also identified specific areas where capacity building is needed, such as cybercrime policy, legislation and training for the judiciary, prosecution and law enforcement agencies.

The assessment further highlighted Kenya's criminal justice system, including law enforcement and other institutions involved in handling cybercrime and electronic evidence. It also underscored the robust inter-agency collaboration and the expanded role of the National KE-CIRT/CC as the Cyber Security Operations Centre (CSOC) for the ICT and Telcoms Sector.

Additionally, the workshop was part of Kenya's ongoing process to join the Convention on Cybercrime. Following a Council of Europe meeting on 9th October, 2024, Kenya received an invitation to accede to the treaty, which remains valid for five (5) years.

Moving forward, the Council of Europe, through the GLACY-e project, will continue to support Kenya in strengthening its cybercrime laws and enhancing international cooperation.



Participants pose for a photo during a workshop on capacity building actions on cybercrime and electronic evidence identified in Kenya, on 10th March 2025, in Nairobi.

Image courtesy of the GLACY-e Project

Future Insights on Cybersecurity

The Authority, in partnership with various strategic partners, will host a capacity building programme focused on Open Compute technologies in May 2025. As part of our efforts to grow the skills and knowledge amongst our constituents, this programme will offer a practical introduction to Open Compute by defining what it is, how it works and why it matters in today's fast evolving digital landscape.

The Open Compute Project (OCP) is about reengineering how we design and operate data centres. It promotes open, efficient and scalable hardware and software solutions that are transforming the cloud and digital infrastructure landscape. Through this programme, we aim to give participants practical insight into how open technologies, both hardware and software, can help organisations build more flexible, cost effective and energy efficient systems.

The sessions will include expert insights, interactive demos and real-world use cases.

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