COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

41st Edition

January - March 2026

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) Cap. 411A, 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)

As we journey into the new year, we look forward to the opportunities that lie ahead. The Authority remains cognisant of the persistent cyber threats that continue to impact individuals, organisations and entire sectors. Threats including ransomware, Distributed Denial of Service (DDoS) attacks, phishing and other social engineering scams, and system misconfigurations continue to feature prominently among the key cybersecurity concerns. These threats not only disrupt business operations but also compromise data privacy, erode public trust and result in significant financial losses and reputational damage.

Ransomware attacks have become increasingly sophisticated and targeted, while phishing and other social engineering scams continue to exploit human vulnerabilities. DDoS attacks continue to disrupt service availability whereas system misconfigurations remain a key factor in data breaches. These developments, both globally and nationally, highlight the need for robust policies, legal and regulatory frameworks, public awareness and user education campaigns, and the integration of a risk-based approach to the management of cybersecurity.

Over the period January - March 2026, the National KE-CIRT/CC detected over 3.3 billion cyber threat events, most of which exploited system vulnerabilities. This represented a decrease of about 26 per cent compared to the previous period, October - December 2025. In response to these threats, we issued over 20 million cyber threat advisories during the same period, representing a decrease of about 5 per cent compared to the previous period.

Majority of these cyber threat advisories were focused primarily on enhancing critical cybersecurity protocols, including running updates and patch management for operating systems, software applications and firmware, the adoption of strong authentication measures such as multi-factor authentication (MFA), the use of antivirus, anti-DDoS and other software utilities, and the hardening of network firewalls and other security devices. These measures were recognised as critical to enhancing organisational cyber resilience in the face of a rapidly evolving cyber threat landscape.

In alignment with the Authority's 2023–2027 Strategic Plan, the Authority, in partnership with the UK's Foreign, Commonwealth & Development Office (FCDO), conducted a training programme on information sharing and building trust networks for members of the National KE-CIRT/CC Cybersecurity Committee (NKCC). The objective of the programme was to strengthen Kenya's national cybersecurity information sharing capabilities through a better structured, well coordinated and trust-based approach.

Participants explored both the strategic and operational dimensions of information sharing, emphasising the importance of timely, accurate and secure exchange of cyber threat intelligence across diverse sectors, and with international partners and other stakeholders. The programme was focused on enhancing national cyber resilience by improving governance frameworks, defining the roles of different constituents and strengthening coordination mechanisms especially during national cyber crises.

The Authority remains committed to strengthening cybersecurity not only as a technical requirement but as a shared responsibility. As the digital landscape continues to evolve, so too must our approaches to cyber defence. We envision this year as one marked by heightened awareness, stronger collaboration and greater resilience in addressing both emerging and persistent cyber threats. With continued commitment and the right mindset, these challenges present opportunities for growth, innovation and a more secure digital future for Kenya.

Mr. David Mugonyi, EBS
Director General/CEO

Cyber Threat Landscape Overview

Global Cyber Threat Landscape Overview

1. Ransomware

Ransomware activity remained elevated globally during January–March 2026, with threat actors intensifying attacks against Critical Information Infrastructure (CII), public services and enterprise environments. Adversaries continued to leverage Ransomware-as-a-Service (RaaS) models, combining data encryption with data exfiltration, disclosure threats and DDoS-enabled extortion, alongside increased use of AI-assisted social engineering. Across Africa, including Kenya, campaigns persisted, targeting government, financial and telecommunications sectors, often exploiting phishing and credential compromise.

In response, the National KE-CIRT/CC issued advisories urging organisations to maintain offline backups, enforce zero-trust network segmentation, ensure timely patching and enhance threat intelligence sharing to strengthen resilience and recovery capabilities.

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

Distributed Denial-of-Service (DDoS) activity remained elevated globally during January–March 2026, with threat actors launching high-volume and multi-vector attacks targeting critical services, cloud platforms and public-facing applications. Adversaries increasingly leveraged IoT botnets and protocol amplification techniques such as DNS and NTP, often using DDoS as a standalone disruption tool or alongside ransomware and extortion campaigns. Across Africa, including Kenya, attacks persisted against government, telecommunications and financial sectors, aiming to disrupt service availability and erode public trust.

In response, the National KE-CIRT/CC issued advisories urging organisations to adopt scalable DDoS mitigation and cloud-based traffic scrubbing solutions, strengthen network resilience, and implement AI-driven traffic anomaly detection to identify and block malicious traffic in real time and minimize service disruption.

3. Social Engineering

Social engineering attacks remained prevalent globally during January–March 2026, with threat actors increasingly exploiting human vulnerabilities to gain unauthorized access to systems and sensitive information. Adversaries leveraged phishing, spear-phishing, business email compromise (BEC) and AI-generated content to craft more convincing and targeted attacks, often serving as initial access vectors for ransomware and financial fraud. Across Africa, including Kenya, campaigns intensified against government institutions, financial services and enterprises, exploiting trust, urgency and weak verification processes.

In response, the National KE-CIRT/CC issued advisories urging organisations to strengthen user awareness on behavioural red flags, enforce verification procedures for financial and sensitive requests, and implement multi-factor authentication (MFA) to reduce the risk of compromise.

Global Cyber Threat Landscape Overview... cont'd

4. System Misconfiguration Exploits

System misconfiguration vulnerabilities remained a key attack vector globally during January–March 2026, with threat actors exploiting improperly configured cloud environments, exposed databases and weak access controls to gain unauthorized access. Misconfigured services enabled privilege escalation, data exposure and lateral movement, particularly across rapidly digitizing environments. Across Africa, including Kenya, organisations faced increased risk due to gaps in configuration management and limited visibility over cloud and hybrid systems.

In response, the National KE-CIRT/CC issued advisories urging organisations to implement secure configuration baselines, continuous monitoring, regular audits and least-privilege access controls to reduce exposure and strengthen system integrity.

5. Emerging Threats

Emerging cyber threats continued to evolve globally during January–March 2026, driven by the growing adoption of Artificial Intelligence (AI), supply chain dependencies and expanding digital ecosystems. Threat actors leveraged AI-powered malware, deepfakes and automated attack tools, while also exploiting third-party vulnerabilities and zero-day flaws to scale attacks. Across Africa, including Kenya, these threats exposed gaps in preparedness and incident response capabilities.

In response, the National KE-CIRT/CC issued advisories urging organisations to enhance threat intelligence sharing, invest in advanced detection capabilities and strengthen incident response frameworks to address evolving risks.

6. Phishing

Phishing attacks remained widespread globally during January–March 2026, with threat actors leveraging AI-generated emails, spoofed domains and social engineering tactics to deceive users and harvest credentials. Campaigns became more targeted and convincing, often serving as entry points for ransomware, fraud and data breaches. Across Africa, including Kenya, phishing campaigns intensified against government, financial and enterprise sectors, exploiting low user awareness and weak email security controls.

In response, the National KE-CIRT/CC issued advisories urging organisations to strengthen email security controls, conduct continuous user awareness training and implement multi-factor authentication (MFA) to mitigate phishing and other related risks.

Cyber Threat Landscape Roundup

Total Cyber Threats Detected

3,367,113,840 | **26.15%**

The National KE-CIRT/CC detected over **3.3 billion** cyber threat events during the three-month period between **January - March 2026**. This represented a **26.15%** decrease from the threat events detected in the previous period, October - December 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.

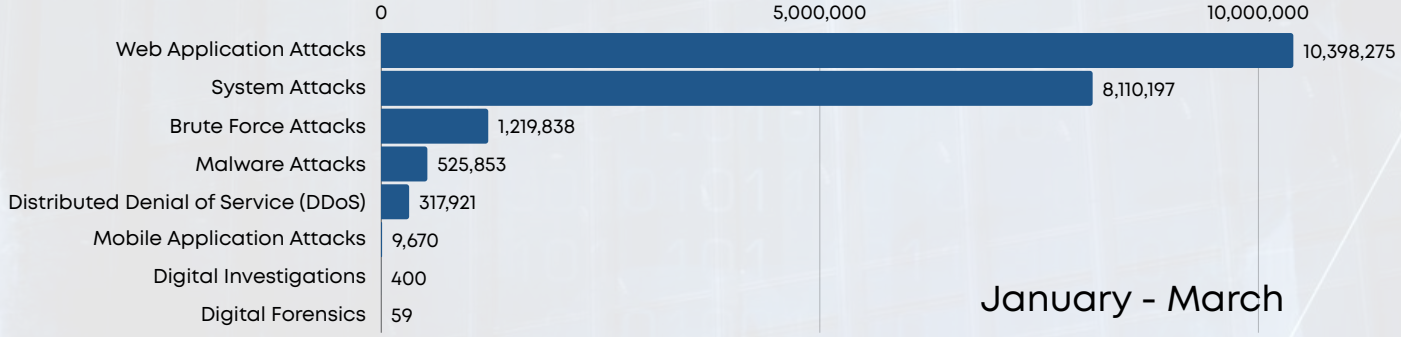
The cyber threats detected were largely attributable to inadequate system patching, insufficient user awareness of phishing and other social engineering threat vectors, and the increasing exploitation of AI-driven and machine-learning technologies by malicious actors.

Total Cyber Threat Advisories Issued

20,581,754 | **5.7%**

The National KE-CIRT/CC issued **20,581,754** advisories between the period **January - March 2026**, in response to the detected cyber threat events. This represented a **5.7%** decrease compared to the advisories that were issued during the previous period, October - December 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.

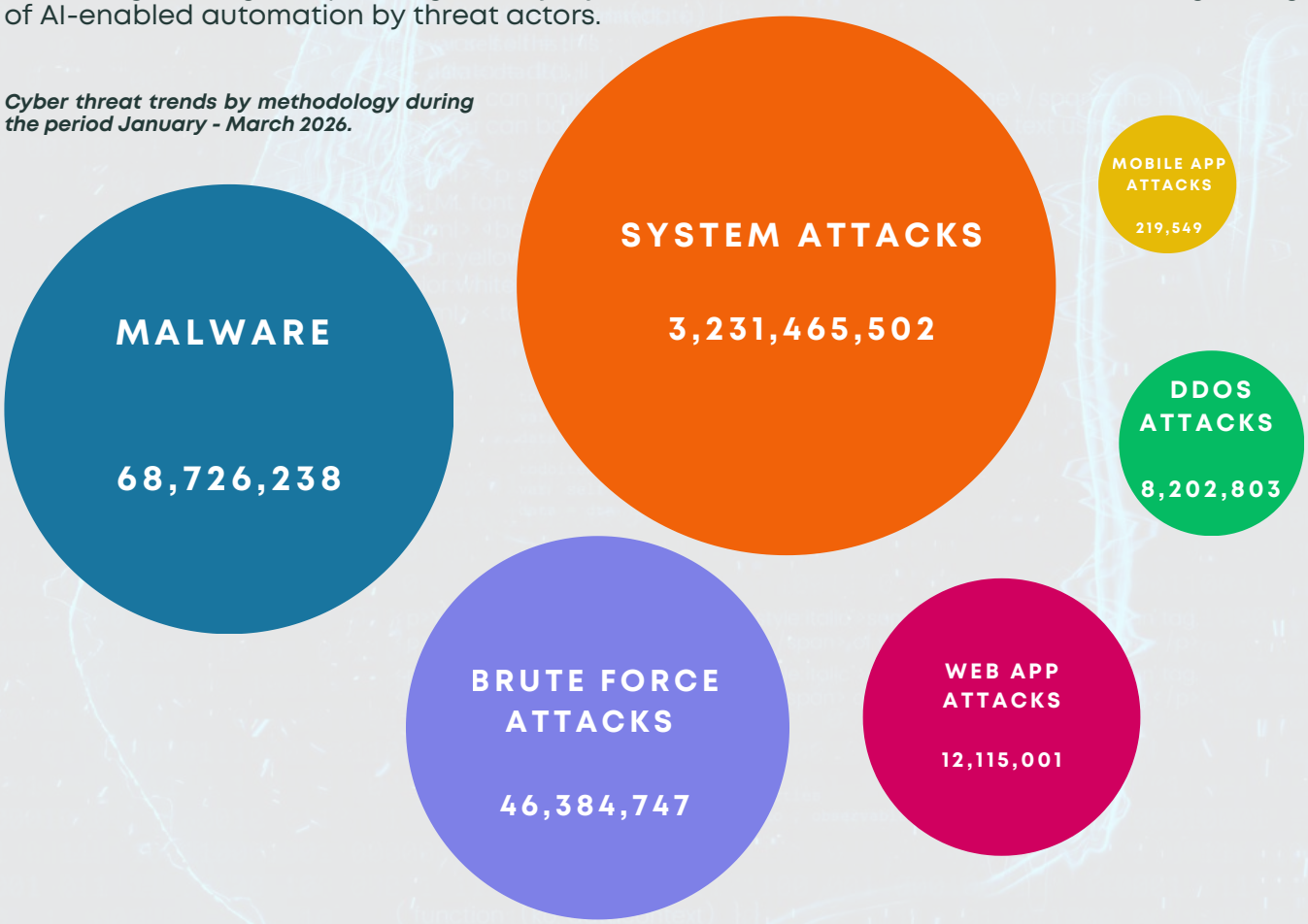


Cyber Attack Vector Trends

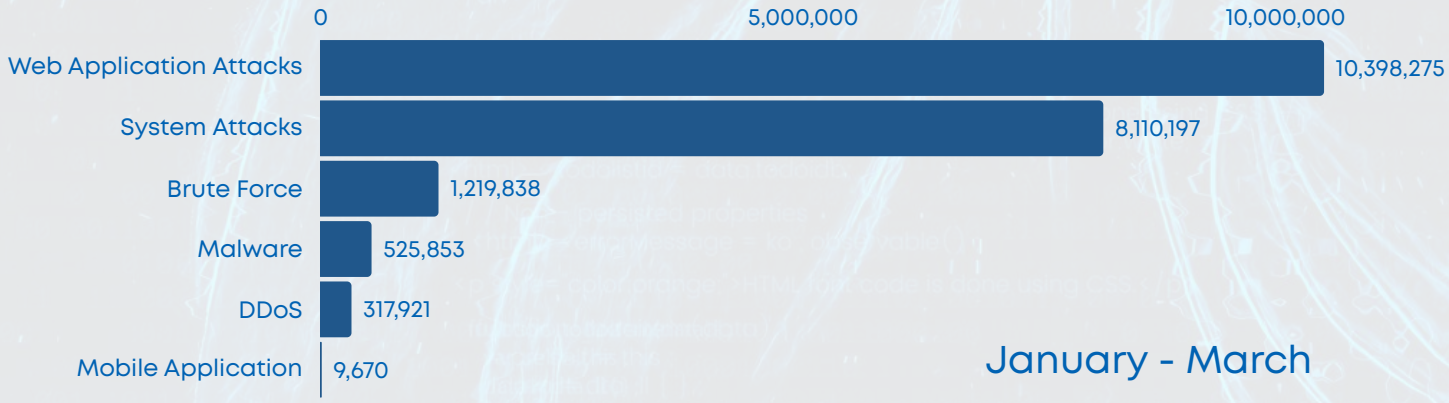
During the period under review, system and malware attacks constituted the most prevalent threat vectors, in line with global cyber threat trends. Incidents arising from system misconfigurations were largely attributable to inadequate cyber risk awareness, continued reliance on deprecated systems, the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

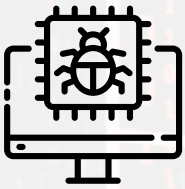
Cyber threat trends by methodology during the period January - March 2026.



Comparison of cyber threat advisories (per vector) issued during the period **January - March 2026.**



Malware Trends



Threats Detected

68,726,238

3.08%

Advisories Issued

525,853

11.17%

During the three-month period between **January - March 2026,** the National KE-CIRT/CC detected **68,726,238** malware threat attempts targeted at the critical information infrastructure sector. This represented a **3.08%** increase from the previous period, October - December 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

12,115,001

4.71%

Advisories Issued

10,398,275

2.31%

The National KE-CIRT/CC detected **12,115,001** web application attack attempts targeted at the critical information infrastructure sector, during the three-month period between **January - March 2026**, This represented an **4.71%** increase from the previous period, October- December 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

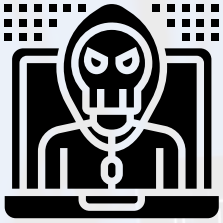
- **Government**
- **Internet Service Providers (ISPs)**
- **Cloud Service Providers**
- **Academia**

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

46,384,747

8.41%

Advisories Issued

1,219,838

35.25%

The National KE-CIRT/CC detected **46,384,747** brute force attack attempts majorly targeting the critical information infrastructure sector during the three-month period from **January - March 2026**. This represented a **8.41%** increase from the previous period, October - December 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

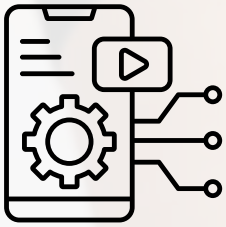
- Cloud Service Providers
- Government

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

219,549

29.18%

Advisories Issued

9,670

57.49%

The National KE-CIRT/CC detected **219,549** mobile application attack attempts targeting end-user devices, during the three-month period from **January - March 2026**. This represented a **29.18%** decrease from the previous period, October- December 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

- Use of malware (ransomware, trojans, worms, viruses) spread via USB devices, social media, and email attachments.
- Weak authentication controls enabling unauthorized access to sensitive data.
- Poor encryption practices leading to exposure of confidential information.
- Over-permissioned mobile applications increasing risk of data breaches.
- Inadequate security controls allowing unauthorized data access and transfer.
- Unauthorized access to data across devices, databases, and networks.

Top Targeted Exploits

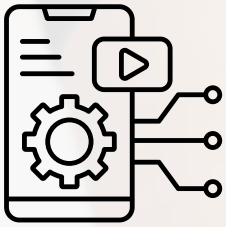
- Improper Credential Usage
- Inadequate Supply Chain Security
- Insecure Authentication
- Insufficient Input/Output Validation
- Insecure Communication
- Inadequate Privacy Controls
- Insufficient Binary Protections
- Security Misconfiguration
- Insecure Data Storage
- Insufficient Cryptography

Threat 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

8,202,803

85.93%

Advisories Issued

317,921

76.24%

The National KE-CIRT/CC detected **8,202,803** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure during the three-month period, **January - March 2026**. This represented a **85.93%** decrease from the previous period, October - December 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. These TVs are also used as bots in cybercriminal activities.

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

3,231,465,502

26.14%

Advisories Issued

8,110,197

3.55%

January - March

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

Training Programme on Information Sharing and Building Trust Networks

The Authority, in partnership with the UK's Foreign, Commonwealth and Development Office (FCDO), conducted a five-day training programme on Information Sharing and Building Trust Networks from 2nd to 6th March 2026, in Nairobi, for members of the National KE-CIRT/CC Cybersecurity Committee (NKCC). The programme brought together 85 participants from 25 organisations across government, critical information infrastructure sectors and academia, with the objective of strengthening Kenya's national cybersecurity information sharing capabilities through a more structured, coordinated and trust-based approach.

The programme focused on enhancing national cyber resilience by improving governance frameworks, defining stakeholder roles and strengthening coordination mechanisms during national cyber crises. Through expert-led sessions and scenario-based exercises, participants explored both the strategic and operational dimensions of information sharing, emphasising the importance of timely, accurate and secure exchange of cyber threat intelligence across sectors and with international partners.

The programme entailed technical sessions that provided hands-on experience in the use of threat intelligence platforms such as the MISP Threat Sharing platform and analytical tools such as PinPoint, enabling participants to collect, structure, analyse and disseminate cyber threat data effectively. The exercises demonstrated how standardised platforms and data-driven analysis enhance situational awareness and support coordinated incident detection and response at the national level.

Discussions further highlighted key enablers of effective cybersecurity collaboration, including trust among stakeholders, clear governance structures and the need for institutionalised information sharing frameworks. Participants also examined practical challenges related to operational sensitivity, legal considerations and cross-sector coordination, reinforcing the importance of structured processes and shared protocols in national cyber operations.

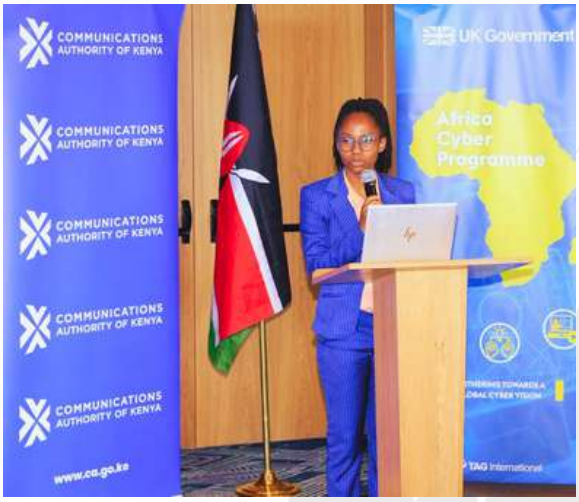
Overall, the training strengthened both the technical and governance capacities required for effective cybersecurity information sharing in Kenya. The outcomes outlined the need for sustained capacity building, expanded stakeholder engagement, operationalisation of threat intelligence platforms and regular simulation exercises at the national level.

This programme marked the final delivery under Phase II of the Africa Cyber Programme (ACP). Throughout its implementation, the ACP has supported the development of cybersecurity policies, skills and partnerships aimed at promoting a safer and more secure digital environment. This final programme not only consolidates the knowledge and expertise built over the course of the programme but also demonstrates the collective commitment of partners and stakeholders to advancing cybersecurity across the region.

Training Programme on Information Sharing and Building Trust Networks... cont'd

Mr. David Mugonyi, EBS, Director General/CEO of the Communications Authority of Kenya (CA), delivering his remarks during the closing ceremony.

Ms. Nerys Cross-Smith, Political Counselor at the British High Commission in Nairobi, giving her speech during the event.



Ms. Clarian Makungu, Africa Cyber Programme Project Manager at the British High Commission (BHC) in Nairobi, addressing participants.

Mr. Mugonyi (second left) and Ms. Cross-Smith (second right), following proceedings during the event. Looking on is Dr. Vincent Ngundi (far left), Director of Cyber Security at CA and Matt Jowett (far right), Head of Cyber at the British High Commission in Nairobi.

A group photo with participants who took part in the training programme.

The InCyber Forum Europe 2026

Members of the Kenyan delegation led by Eng. John Tanui, MBS, CBS (centre), Principal Secretary, State Department for ICT and the Digital Economy, pose for a photo during the InCyber Forum Europe 2026 that was held from 30th March - 2nd April 2026 in Lille, France. The Authority was represented at the forum by Dr. Vincent Ngundi (fourth right), Director of Cyber Security and Mr. Francis Sitati (second left), Principal Officer, Cyber Security Resilience.

The Authority, in collaboration with Expertise France, participated in the InCyber Forum Europe 2026 that was held from 30th March to 2nd April, 2026 in Lille, France. The forum brought together global cybersecurity leaders, policymakers, industry experts and international organisations to deliberate on emerging cyber threats and strategies for strengthening cyber resilience. Other participants at the forum included representatives from the Ministry of Information, Communications and the Digital Economy, the ICT Authority and the National Computer and Cybercrimes Coordination Committee (NC4). It provided a platform for dialogue on the evolving cyber threat landscape, with particular focus on the increasing sophistication of cyberattacks, including ransomware and state-sponsored attacks.

Discussions at the forum centred around the need for enhanced international cooperation in addressing transnational cyber threats, recognising that cybersecurity is a shared global responsibility. Participants highlighted the importance of strengthening public–private partnerships, given the critical role that the private sector plays in managing and securing digital infrastructure. The forum also brought out the growing significance of cyber threat intelligence sharing, that requires structured, timely and trusted information exchange mechanisms among stakeholders.

Another key theme was the importance of capacity building and skills development to address the global shortage of cybersecurity professionals. Countries were encouraged to invest in relevant training programmes, awareness creation and public education initiatives to enhance both technical and strategic-level expertise. The need for robust policy, legal and regulatory frameworks to support cyber resilience was also highlighted, including the need for the harmonisation of cybercrime laws and data protection regimes.

Overall, the forum emphasised the importance of a coordinated and inclusive approach to cybersecurity, combining policy, technical and operational measures. It highlighted the need for proactive and intelligence-driven strategies to effectively manage cybersecurity risks and ensure a secure and resilient digital future.

The Africa CISO Summit 2026

The Authority participated in the Africa CISO Summit 2026, that was held from 11th - 12th March 2026, in Nairobi. The summit convened Chief Executive Officers, Chief Information Security Officers, policymakers, industry leaders and cybersecurity practitioners from across the continent to deliberate on emerging cyber threats and strategies for strengthening organisational and national cyber resilience. The event provided a platform for sharing experiences, best practices and insights on managing increasingly sophisticated cyber threats, including ransomware, supply chain attacks and advanced persistent threats targeting critical information infrastructure. The Authority was represented at the event by Mr. Francis Sitati.

Discussions highlighted the importance of an evidence-based approach to cybersecurity with an emphasis being placed on integrating cyber risk into the governance process. Participants called for greater collaboration between public and private sector stakeholders, recognising that effective cybersecurity requires coordinated efforts across various industries and jurisdictions. The summit also outlined the role of Cyber Threat Intelligence (CTI) in enabling proactive defence, advocating for improved information sharing mechanisms and building trust networks among organisations and across borders.

A key theme was addressing Africa's cybersecurity skills gap through targeted capacity building, professional training and the development of local talent. Overall, the summit reinforced the imprtance of strategic oversight in driving the cybersecurity agenda and building a cyber hygiene culture within organisations. It highlighted the need for continuous investment in people, processes and technology to ensure a resilient and secure digital ecosystem across Africa.

A section of delegates following proceedings during the Africa CISO Summit 2026 that was held from 11th - 12th March 2026.

\

Mr. Francis Sitati from Cyber Security department delivers the keynote titled, "One Person, Many IDs: National Digital Identity as a Security Foundation".

Benchmarking and Study Tour by the Independent Communications Authority of South Africa (ICASA)

The delegation from ICASA led by Ms. Honey Makola (left), the Manager in charge of Cybersecurity. She was accompanied during the tour by Ms. Esther Gopane, Policy Research Analyst.

Capt. Edward Ireri from CA's Cyber Security department, makes his presentation during the benchmark exercise.

The Independent Communications Authority of South Africa (ICASA) conducted a benchmarking visit to the Authority's National KE-CIRT/CC on 24th February 2026. The visit sought to gain extensive insights into Kenya's cybersecurity management framework, including the underlying policy, legal and regulatory regime. It provided an opportunity to examine the structures, processes and governance mechanisms that strengthen national cybersecurity coordination and oversight.

The engagement also facilitated knowledge sharing on best practices in implementing effective cybersecurity strategies and regulatory compliance. Additionally, it enabled discussions on strengthening institutional capacities and enhancing collaboration in addressing emerging and new cyber threats.

The delegates also had the opportunity to visit other relevant institutions, including the Ministry of Information, Communications and the Digital Economy, that provides policy leadership and strategic direction for Kenya's ICT sector, including digital transformation and cybersecurity governance, and the Technology Service Providers of Kenya (TESPOK), that plays a key role in Kenya's digital ecosystem by supporting industry coordination, managing critical infrastructure such as Kenya Internet Exchange Point (KIXP) and facilitating incident response through the iCSIRT.

These engagements provided additional insights into the broader institutional and policy landscape supporting Kenya's digital ecosystem. The visits further facilitated knowledge exchange and strengthened understanding of multi-stakeholder collaboration in advancing national cybersecurity and digital transformation objectives.

54th Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

The 54th National KE-CIRT/CC Cybersecurity Committee (NKCC) meeting was held on 4th March 2026 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. The Committee continues to promote trust, capacity building and information sharing on emerging cybersecurity threats, while coordinating collective response strategies through its quarterly engagements.

During the meeting, members provided updates on ongoing efforts to strengthen cybersecurity across critical sectors, highlighting the deployment of advanced monitoring tools, including email security gateways, SIEM (Security Information and Event Management) systems and network firewalls, as well as progress toward establishing a centralized SOC and developing a national information security framework. Capacity building initiatives were also reported, with training programmes being rolled out across multiple regions to enhance skills in areas such as domain name system (DNS) and network security.

Members raised concerns over emerging threats and systemic vulnerabilities, including the misuse of legitimate remote access tools for malicious activities, weak access controls, gaps in third-party risk management and poorly configured security systems. Additional risks identified included cybersquatting, impersonation of legitimate entities and the increasing use of cryptocurrency to facilitate cybercrime, complicating investigative efforts. It was noted that, governance and operational challenges such as undefined roles, limited accountability and inconsistent implementation of key controls, including multi-factor authentication (MFA).

Members further highlighted broader structural challenges, including cybersecurity skills gaps, uneven governance maturity across institutions, rapid technological advancements outpacing existing policy, legal and regulatory frameworks, and resource constraints. Ongoing efforts to operationalise the 2022 - 2027 National Cybersecurity Strategy and enhance stakeholder engagement were noted as critical steps toward strengthening coordination and resilience.

In addition, members reported that ransomware remains a dominant global threat, alongside continued exploitation of system vulnerabilities. Emphasis was placed on the importance of continuous capacity building, strengthened governance frameworks, proactive risk management and enhanced collaboration to address evolving threats.

In conclusion, members recommended enhancing future reporting through sector-based threat analysis, integrating updates on national cybersecurity initiatives and strengthening institutional coordination by formalising roles to support a more unified and resilient national cybersecurity posture.

Bilateral Exchange on Cybersecurity Best Practices with the Energy and Petroleum Regulatory Authority (EPRA)

On 26th March 2026, the Authority's National KE-CIRT/CC, hosted a bilateral exchange on cybersecurity best practices with the Energy and Petroleum Regulatory Authority (EPRA), that has been designated as the Cyber Security Operations Centre (CSOC) for the energy sector. The engagement focused on sharing governance frameworks and operational best practices in establishing and managing a functional CSOC.

EPRA expressed interest in understanding the tools, technologies and processes required to support an effective CSOC, as it is currently in the process of operationalising its own. Discussions also covered incident detection and response, threat intelligence sharing and coordination mechanisms among partners and stakeholders.

The exchange provided a platform for knowledge sharing and collaboration, with the National KE-CIRT/CC highlighting its experience in coordinating national cybersecurity operations and supporting various sectoral CIRTs. The engagement is expected to support EPRA in strengthening cybersecurity within the energy sector and enhancing preparedness against emerging threats.

EPRA is responsible for regulating the energy and petroleum sector in Kenya by setting standards, issuing licences and enforcing compliance with regulatory requirements.

Study Tour by ICT Students from the National Youth Service (NYS)

On 17th March 2026, the Authority had the privilege of hosting a delegation of ICT students from the National Youth Service (NYS) in Ruaraka, Nairobi. The visit provided an opportunity for knowledge exchange and engagement between the Authority and young Kenyans undergoing structured national service and technical training.

As Kenya's ICT sector regulator, the Authority plays a central role in shaping the country's digital ecosystem. The NYS, on the other hand, equips young Kenyans with technical, vocational skills, making it a key partner in advancing inclusive national development.

The engagement also highlighted emerging opportunities in cybersecurity, data governance and digital services as key areas for future growth. Participants were exposed to evolving career pathways and the skills required to thrive in these domains. This visit highlighted the importance of building a skilled workforce to support Kenya's digital transformation agenda.

Outlook for the Next Quarter

In collaboration Expertise France, the Authority will host a training programme on a Threat Intelligence Sharing Platform (TISP) aimed at strengthening Kenya's national cybersecurity information sharing capabilities. The programme seeks to enhance the adoption and operationalisation of structured, secure and timely cyber threat intelligence exchange mechanisms.

The training will focus on building technical and operational capacity in the use of threat intelligence platforms, including the integration of workflows, governance frameworks and coordination mechanisms to support effective information sharing among key stakeholders. These include the Authority's National KE-CIRT/CC, the National Computer and Cybercrimes Coordination Committee (NC4), sectoral Computer Incident Response Teams (CIRTs) and Cyber Security Operations Centres (SOCs), sector regulators and critical information infrastructure operators.

The programme will also incorporate international best practices in threat intelligence sharing, adapted to Kenya's national context, ensuring alignment with existing legal frameworks, institutional mandates and national cybersecurity priorities.

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