COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

42nd Edition

April - June 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)

The Authority continued to observe elevated activity across the national cyber threat landscape with ransomware, Distributed Denial-of-Service (DDoS) attacks and social engineering scams remaining the most prevalent threat vectors. Globally, ransomware continued to be the dominant cyber threat, with coordinated attacks increasingly targeting both public and private sector organisations. Some of the critical sectors affected included Internet Service Providers (ISPs), cloud service providers and the health sector.

At the same time, data breaches continued to pose a significant threat, resulting in the exposure and compromise of sensitive personal, financial and organisational data. These events raise concerns about the protection of Personally Identifiable Information (PII), the resilience and security of the Critical Information Infrastructure (CII) sector, and the need to ensure adherence to relevant legal and regulatory frameworks.

The Authority further observed that DDoS attacks remained widespread, with hacktivist groups often orchestrating targeted attacks amid ongoing global geopolitical tensions. Social engineering techniques also continue to become increasingly sophisticated. Threat actors often impersonate technical support personnel to exploit human weakness and to gain unauthorised access to systems and sensitive information.

The evolving cyber threat landscape highlights the need to strengthen our national cyber hygiene, enhance our collective capabilities for proactive threat detection and incident response through continuous public education and awareness, and capacity building.

Over the period April - June 2026, the National KE-CIRT/CC detected over 2.3 billion cyber threat events which represented a decrease of about 30% from the previous period, January - March 2026. Despite this decline, the National KE-CIRT/CC issued over 20 million cyber threat advisories between this period. This therefore represented a marginal increase of approximately 1% from the previous period, January - March 2026.

In alignment with the Authority's 2023 – 2027 Strategic Plan, the Authority, in partnership with Huawei Technologies Kenya, hosted the 2026 Cybersecurity Bootcamp Competition (Students' Track). The programme brought together relevant stakeholders from the CII sector, as well as students from diverse universities, colleges, technical and vocational training institutions from across the country. The competition was aimed at supporting and empowering the development of local cybersecurity capabilities to bridge the existing cybersecurity gaps, especially among the youth.

The competition, which was held between April and May 2026, attracted over 3,000 participants, indicating the ever-growing interest and need for similar initiatives across the country. The final phase of the competition entailed *Cybersecurity Study and Mentorship Tours*, which were aimed at providing the winning students with industry experience and professional mentorship opportunities. These tours accorded them the opportunity to visit various organisations within the CII sector, providing them with a better understanding of the regulatory landscape shaping Kenya's digital ecosystem. Further, it enabled them to gain a deeper understanding into the institutional aspects of cybersecurity outside of the classroom setting.

The Authority remains committed to advancing Kenya's cybersecurity posture through the continued implementation of the National Cybersecurity Management Framework, that is supported by a robust policy, legal and regulatory framework. By strengthening collaboration and equipping stakeholders across the cybersecurity ecosystem with the requisite tools, knowledge and capabilities, the Authority will continue to enhance the country's cyber resilience and support a secure, trusted and resilient digital economy.

Mr. David Mugonyi, EBS
Director General/CEO

Cyber Threat Landscape Overview

Global Cyber Threat Landscape Overview

1. Ransomware

Ransomware groups continued to target government institutions, health, academia and the financial sectors, while credential-based attacks increasingly replaced traditional intrusion methods. Organisations across Africa, including Kenya, remained at risk from ransomware operators exploiting stolen credentials and supply chain relationships. Attackers exploited compromised user credentials, unpatched system and trusted third-party access to gain initial entry before deploying ransomware. AI-assisted reconnaissance enabled cybercriminals to identify vulnerable systems more rapidly.

In response, the National KE-CIRT/CC issued advisories urging organisations to strengthen identity security through Multi-Factor Authentication (MFA), continuous monitoring of privileged accounts, regular patch management and maintaining offline backups.

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

Distributed Denial-of-Service (DDoS) attacks continued to target government digital services, web applications and online platforms, demonstrating that service disruption remained a significant threat to national digital infrastructure. Threat actors used compromised devices such as botnets to generate large volumes of malicious traffic, while simultaneously exploiting system vulnerabilities to overwhelm online services.

In response, the National KE-CIRT/CC issued advisories urging organisations to expand the use of cloud-based DDoS protection, traffic filtering, rate limiting and AI-based traffic anomaly detection to distinguish malicious traffic from legitimate user activity before services become unavailable.

3. Social Engineering

AI-enhanced phishing campaigns and social engineering attacks became increasingly convincing during this period. A rise in deepfake-enabled fraud, spoofed websites and impersonation campaigns targeting government organisations, financial organisations and businesses was experienced. Attackers used AI-generated emails, fake login portals, deepfake videos and voice impersonation to deceive victims into revealing credentials or authorising fraudulent transactions. Cybercriminals also exploited the growing trust in AI applications by disguising malware as legitimate AI tools.

In response, the National KE-CIRT/CC issued advisories urging organisations to implement phishing-resistant authentication, strengthen email filtering and apply independent verification of sensitive requests before approving transactions.

Global Cyber Threat Landscape Overview... cont'd

4. System Misconfiguration Exploits

Weak system configurations, delayed software patching, insecure cloud environments and inadequate authentication controls remained among the leading causes of successful cyber incidents across Kenya. Threat actors scanned Internet-facing systems for exposed services, default configurations, weak passwords and outdated software before exploiting them to gain unauthorised access or establish persistence within networks.

In response, the National KE-CIRT/CC issued advisories urging organisations to strengthen vulnerability management programmes by carrying out regular security assessments, enforce secure configuration baselines, implement continuous patch management and improve authentication controls across critical systems.

5. Emerging Threats

Artificial Intelligence (AI) continued to reshape the cyber threat landscape, with attackers increasingly using AI to automate reconnaissance, generate phishing content, develop malware and conduct deepfake-enabled fraud. Identity compromise also emerged as one of the most significant attack vectors globally and regionally. Threat actors used generative AI to produce realistic phishing messages, malicious websites and social engineering content at scale. AI-powered malware and automated vulnerability discovery reduced the time between identifying and exploiting security weaknesses.

In response, the National KE-CIRT/CC issued advisories urging organisations to adopt AI-enabled threat detection, identity-focused security, Zero Trust Architecture (ZTA), continuous threat monitoring and enhanced threat intelligence sharing to improve resilience against evolving cyber threats.

6. Mapping the Global Cyber Threat Landscape

The alignment between the global cyber threat landscape and the national cyber threat landscape is evident in the similarities in the tactics, techniques and procedures (TTPs) affecting both individuals and organisations.

This convergence outlines the universal nature of cyber threats, where trends and techniques observed on a global level are manifested and adapted within specific geolocations.

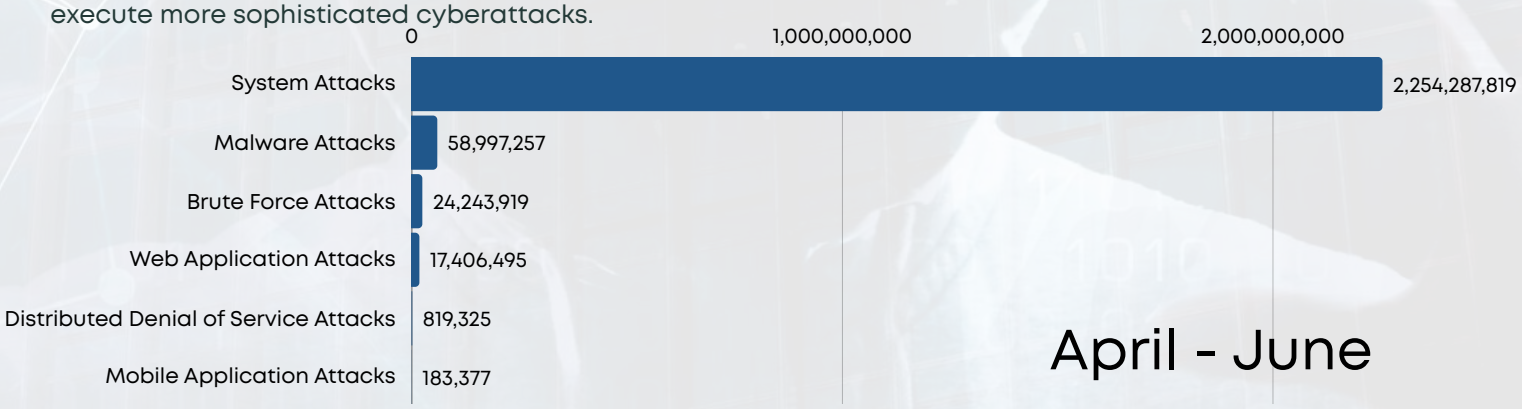
Cyber Threat Landscape Roundup

Total Cyber Threats Detected

2,355,938,192 | **30.03%**

The National KE-CIRT/CC detected over **2.3 billion** cyber threat events during the period between **April - June 2026**. This represented a **30.03%** decrease from the threat events detected during the previous period, January - March 2026. The Authority continued to enhance the dissemination of cyber threat advisories to critical information infrastructure sectors, as part of its broader commitment to enhancing national cybersecurity resilience in response to the evolving cyber threat landscape.

These threats were largely attributed to inadequate system patching, insufficient user awareness of phishing and other social engineering attacks, and the increasing exploitation of AI technologies by malicious actors to execute more sophisticated cyberattacks.

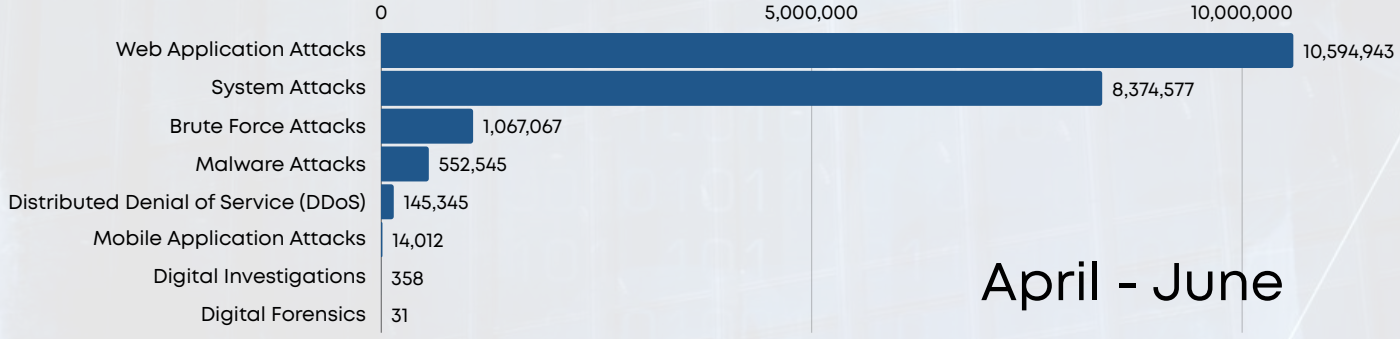


Total Cyber Threat Advisories Issued

20,748,489 | **0.81%**

The National KE-CIRT/CC issued **20,748,489** advisories between the period **April - June 2026**, in response to the detected cyber threat events. This represented a **0.81%** increase compared to the advisories that were issued during the previous period, January - March 2026.

The Authority continued to disseminate its technical threat advisories by promoting timely system and application patching, the implementation of multi-factor authentication (MFA), robust password management practices and the secure configuration of firewalls and antivirus solutions to mitigate emerging cyber threats.

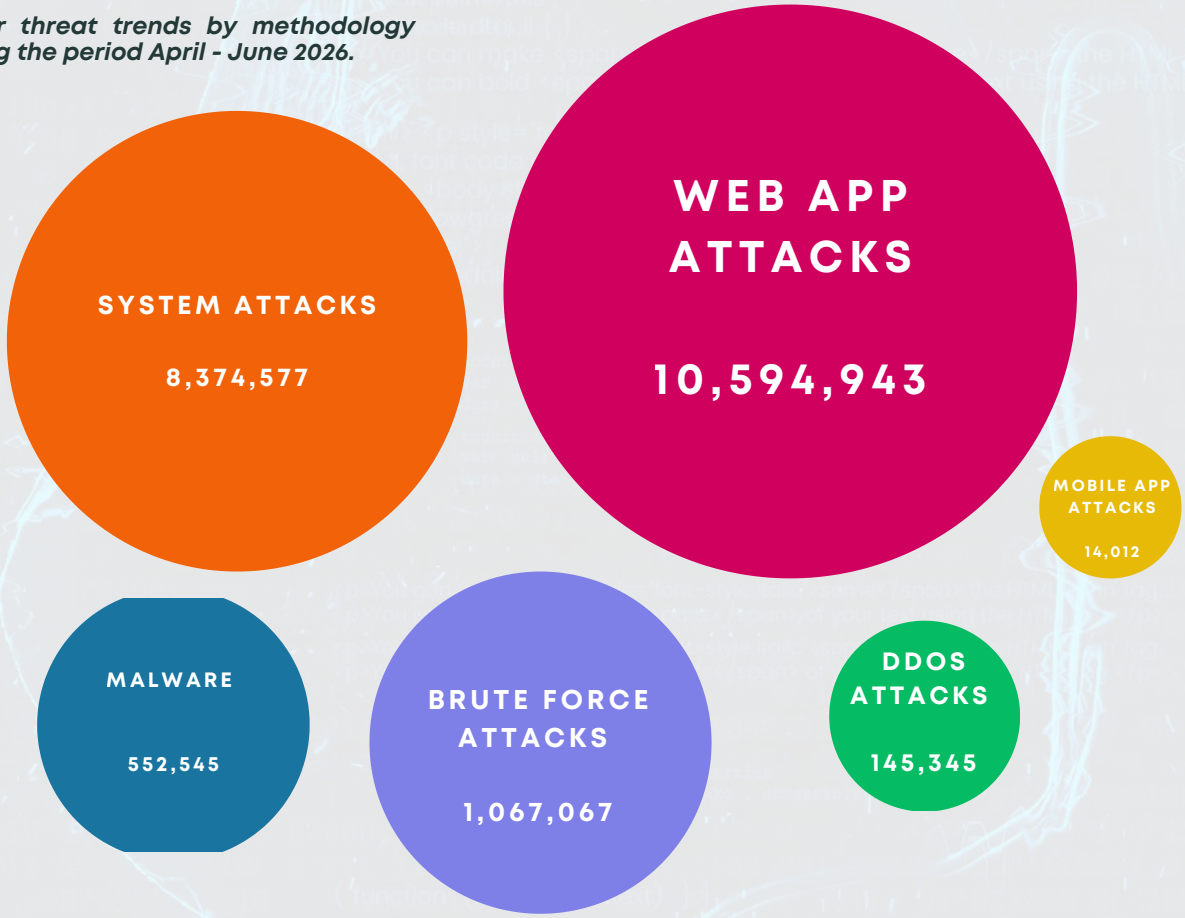


Cyber Attack Vector Trends

Web application attacks and system attacks constituted the most prevalent threat vectors during the period under review. The majority of web application attacks were attributed to the exploitation of vulnerable third-party libraries, inadequately secured APIs, insecure serverless configurations and weaknesses in open source software dependencies.

On the other hand, system attacks were largely driven by malware designed to steal credentials and exploit weak access controls, information leakage, the continued use of outdated and vulnerable operating systems and users interacting with malicious links, among other attack vectors.

Cyber threat trends by methodology during the period April - June 2026.



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

Malware Trends

Threats Detected

58,997,257

14.16%

Advisories Issued

552,545

5.08%

During the period between **April - June 2026,** the National KE-CIRT/CC detected **58,997,257** malware threat attempts targeted at the critical information infrastructure sector. This represented a **14.16%** decrease from the previous period, January - March 2026.

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 devices and Remote Access Trojans (RATs). Other targeted sectors included academia, individuals and the financial sector including banks, cryptocurrency platforms, forex 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

17,406,495

43.68%

Advisories Issued

10,594,943

1.89%

During the three-month period between **April - June 2026**, the National KE-CIRT/CC detected **17,406,495** web application attack attempts targeted at the critical information infrastructure sector. This represented a **43.68%** increase from the previous period, January - March 2026.

Government systems and Internet Service Providers (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, enabling unauthorised access to systems and the interception of sensitive data during transmission.

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

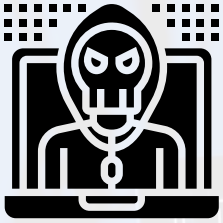
- **Government**
- **Internet Service Providers (ISPs)**
- **Cloud Service Providers**
- **Academia**

These 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

24,243,919

47.73%

Advisories Issued

1,067,067

12.52%

During the three-month period from **April - June 2026**, the National KE-CIRT/CC detected **24,243,919** brute force attack attempts majorly targeting the critical information infrastructure sector. This represented a **47.73%** decrease from the previous period, January - March 2026.

These attacks mainly targeted cloud service providers and government systems, with threat actors focusing on compromising database servers and user authentication credentials. Successful attacks were largely driven by vulnerabilities in database infrastructure, weak authentication controls and insecure Remote Desktop Protocol (RDP) configurations, which enabled unauthorised access to critical systems and the exposure of sensitive information.

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

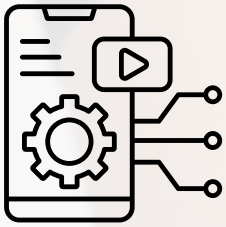
- **Cloud Service Providers**
- **Government**

Threat actors targeted Internet of Things (IoT) devices and remotely accessible systems through exposed Telnet ports and misconfigured RDP services. 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 using service ports
- Implement appropriate access management with strong password management.
- Disconnect devices from network if not in use
- Update libssh softwares to the latest versions.

Mobile Application Attack Trends



Threats Detected

183,377

16.48%

Advisories Issued

14,012

44.9%

During the three-month period from **April - June 2026,** the National KE-CIRT/CC detected **183,377** mobile application attack attempts targeting end-user devices. This represented a **16.48%** decrease from the previous period, January - March 2026.

Mobile devices and Android TVs remained primary targets, with threat actors exploiting weak credential management practices, particularly the use of default credentials, to gain unauthorised access and compromise device security.

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

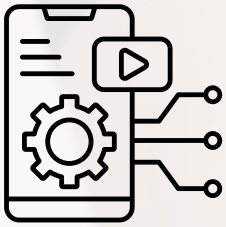
- Improper Credential Usage
- Inadequate Supply Chain Security
- Insecure Authentication
- Insufficient Input/Output Validation
- Insecure Communication
- Inadequate Privacy Controls
- Insufficient Binary Protections
- Security Misconfiguration
- Insecure Data Storage
- Insufficient Cryptography

Attackers compromised vulnerabilities in the Android Debug Bridge (ADB) protocol to gain unauthorised SSH (Secure Shell) access to mobile devices, enabling the compromise of sensitive user information thereby increasing the risk of 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

819,325

90.01%

Advisories Issued

145,345

54.28%

During the three-month period from **April - June 2026,** the National KE-CIRT/CC detected **819,325** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure. This represented a **90.01%** decrease from the previous period, January - March 2026.

Email and web servers remained the primary targets of cyberattacks, with threat actors exploiting weak credential management practices to gain unauthorized access and compromise critical services.

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 this period, hacktivist groups and politically motivated Advanced Persistent Threat (APT) actors continued to target critical systems in an effort to disrupt the delivery of essential public services. These attacks contributed to service degradation for consumers and increased the operational burden and mitigation costs borne by 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

2,254,287,819

30.24%

Advisories Issued

8,374,577

3.25%

Most attacks targeted operating systems and database servers hosted by Internet Service Providers (ISPs) and cloud service providers. Threat actors exploited vulnerabilities in outdated operating systems to gain unauthorised access to systems. The persistence of these vulnerabilities was primarily attributable to improper patch management, reliance on legacy systems and the rapid growth of Internet of Things (IoT) devices with inadequate security protocols, which continue to increase the overall attack surface.

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 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)

Threat actors mainly targeted critical information infrastructure with the intent of financial gain and malware distribution, leading to data breaches, financial losses and widespread 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

2026 Cybersecurity Bootcamp Competition (Students' Track)

The growth of Kenya's digital economy has accelerated the demand for a highly skilled cybersecurity workforce capable of safeguarding the country's Critical Information Infrastructure (CII) against an increasingly sophisticated cyber threat landscape. However, the persistent shortage of cybersecurity professionals remains a significant challenge to strengthening national cyber resilience, enhancing incident response capabilities and sustaining the growth of Kenya's digital economy.

Against this background, and in alignment with the Authority's 2023 – 2027 Strategic Plan, the Authority, in partnership with Huawei Technologies Kenya, hosted the 2026 Cybersecurity Bootcamp Competition (Students' Track). The competition, which took place from 1st April to 22nd May 2026, was aimed at equipping university and college students with practical cybersecurity skills and knowledge through hands-on technical training programmes, mentorship opportunties and exposure to real-world cybersecurity operations.

This year's bootcamp also sought to strengthen the collaboration between academia, government and industry in building a sustainable cybersecurity talent pipeline for the country. The competition focused on promoting practical, industry-led cybersecurity training programmes while empowering young people to become the next generation of cyber defenders to support Kenya's digital transformation agenda.

The programme attracted 3,049 students from universities and tertiary institutions across the country, reflecting the growing interest in cybersecurity among the youth and young professionals. The competition was implemented in four phases, that included self-paced online learning, instructor-led training, practical technical sessions and finally various cybersecurity study and mentorship tours. Participants received training in key cybersecurity domains such as network security, firewall security, encryption technologies, Public Key Infrastructure (PKI), cyber threat detection and response, incident handling, cybersecurity best practices, among others.

Participants were drawn from various universities and colleges across the country that included Catholic University of Eastern Africa (CUEA), Daystar University, Dedan Kimathi University of Technology (DeKUT), Egerton University (EU), Jomo Kenyatta University of Agriculture and Technology (JKUAT), Kabete National Polytechnic (KNP), KCA University (KCAU), Kenyatta University (KU), Kibabii University (KIBU), Maseno University (MSU), Moi University (MU), Multimedia University (MMU), South Eastern Kenya University (SEKU), Strathmore University (SU), Technical University of Kenya (TUK), Technical University of Mombasa (TUM), United States International University-Africa (USIU-Africa), University of Eldoret (UoE), University of Nairobi (UON), among others.

Overall, the programme enhanced the participants' technical competencies and enhanced their capacity to identify, prevent, detect and respond effectively to evolving cyber threats.

2026 Cybersecurity Bootcamp Competition (Students' Track)... cont'd

Eng. Dennis Chepkwony, Director, Universal Service Fund (USF), Communications Authority of Kenya (CA), delivering the Director General/CEO's remarks during the closing ceremony on 20th May 2026 in Nairobi.

Eng. Chepkwony engages with Mr. James Sun, Deputy Chief Executive Officer, Public Affairs, at Huawei Technologies Kenya, during a debriefing session on the sidelines of the closing ceremony.

Eng. Chepkwony (far left) and Mr. Kaine Zhang (far right), Huawei's Country Cybersecurity and Privacy Officer, pose for a photo with the winning team during the closing ceremony.

A section of the competition finalists attentively follows the proceedings during the closing ceremony.

Eng. Chepkwony (third from left, front row) and Ms. Banchale Gufu (second from left, front row) from the Communications Authority of Kenya (CA), together with representatives from Huawei Technologies Kenya, join the winning teams for a group photo.

Youth Mentorship in Cybersecurity: 2026 Cybersecurity Study and Mentorship Tours

The final phase of the 2026 Cybersecurity Bootcamp Competition (Students' Track) entailed diverse *Cybersecurity Study and Mentorship Tours*, which were aimed at providing the winning students with industry experience and professional mentorship opportunities. The top 18 students got the opportunity to visit key organisations within the Critical Information Infrastructure (CII) sector, providing them with a better understanding of the regulatory and operational landscape shaping Kenya's digital ecosystem.

This year's programme further aimed to bridge the gap between theoretical learning and real-world cybersecurity operations through direct interaction with professionals and organisations at the forefront of cybersecurity and digital transformation. As part of the programme, participants undertook educational visits to the Authority's National KE-CIRT/CC, Huawei's Training Centre at African Advanced Level Telecommunications Institute (AFRALTI), the Kenya Network Information Centre (KeNIC), Safaricom PLC and the Konza Technopolis Development Authority (KoTDA). These visits provided the students with practical insights into Kenya's ICT, cybersecurity and digital innovation ecosystem.

The students pose for a group photo at the CA Centre, Nairobi, following a study visit to the Authority's National KE-CIRT/CC.

Participants pictured outside Huawei's Training Centre located at AFRALTI, along Waiyaki Way in Nairobi.

Posing for a photo at KeNIC, Waiyaki Way, Nairobi, following a technical session on Kenya's Domain Name System (DNS).

At Safaricom PLC along Waiyaki Way, Nairobi, following an interactive session on digital technologies and innovation.

Stakeholder Engagement on Compliance with WebTrust for Electronic Certification Service Providers (E-CSPs)

The Authority convened a high-level stakeholder engagement forum on 14th May 2026 in Nairobi, to sensitise stakeholders on compliance with WebTrust for Certification Authorities (CAs) framework. This is a standardised trust services audit framework used to examine the controls and business practices of CAs that issue digital certificates. The framework includes standards developed by the European Telecommunications Standards Institute (ETSI) and the International Organisation for Standardisation (ISO).

The forum brought together licensed and accredited Electronic Certification Service Providers (E-CSPs), as well as prospective service providers, to deliberate on the transition of Kenya's National Public Key Infrastructure (NPKI) towards internationally recognised trust and assurance frameworks. Discussions centred around the integration of the WebTrust framework into Kenya's regulatory ecosystem to enhance the credibility, interoperability and global recognition of the country's digital trust services.

Participants were apprised about the principles, criteria and audit requirements that support the WebTrust framework, such as the governance, operational and security controls required to meet the trust standards recognised by major web browsers and operating systems. Adoption of these internationally recognised standards is aimed at enhancing consumer trust, confidence and to accelerate the deployment of secure digital services across the country.

The forum also provided a platform for stakeholders to deepen their understanding of Kenya's evolving cryptographic and digital trust ecosystem, such as emerging regulatory compliance requirements, technical control frameworks and the implications of global trust store inclusion for digital certificates and electronic signature services.

A total of 28 participants drawn from 10 organisations, comprising Executive Directors, Chief Technology Officers, Compliance Officers and technical experts, attended the forum.

Participants during the Stakeholder Engagement Forum on WebTrust Compliance for Certification Authorities, held on 14th May 2026 in Nairobi.

Banking Sector Security Operations Centre (BS-SOC) Cybersecurity Simulation Exercise

Participants pose for a photo during the Banking Sector Security Operations Centre (BS-SOC) Cybersecurity Simulation Exercise, held on 5th May 2026 in Nairobi.

The Authority participated in a Cybersecurity Simulation Exercise organised by the Banking Sector Security Operations Centre (BS-SOC), held on 5th May 2026 in Nairobi. The BS-SOC was established under the Cyber Fusion Unit (CFU) of the Central Bank of Kenya (CBK) and is a critical component in the implementation of the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024. The BS-SOC is equipped to provide critical services such as Cyber Threat Intelligence, Incident Response, Digital Forensics and Cyber Investigations. among others. The Authority was represented at the forum by Mr. Francis Sitati and Ms. Yvonne Oreno from the National KE-CIRT/CC.

The cybersecurity exercise entailed simulation of large-scale cyber threat incidents affecting critical banking and payment services, with the aim of assessing the sector's preparedness, coordination and response mechanisms. The engagement brought together Chief Information Security Officers (CISOs) from commercial banks, Payment Service Providers (PSPs), Microfinance Banks (MFBs) and other key stakeholders, including the Authority's National KE-CIRT/CC, the Kenya Bankers Association (KBA), Mobile Network Operations (MNOs), the National Computer and Cybercrimes Coordination Committee (NC4), among others.

The exercise sought to evaluate the effectiveness of existing coordination and collaboration frameworks among diverse sectors and other stakeholders during cyber crises. It also examined the effectiveness of intelligence sharing in supporting rapid threat detection and collective defence. In addition, the exercise aimed to strengthen partnerships and promote common approaches to cyber threat detection, incident response and recovery.

The Authority's National KE-CIRT/CC continues to strengthen sectoral cybersecurity resilience through collaboration, information sharing and the coordination of joint cyber incident response capabilities. These collaborative engagements are essential for detecting and mitigating systemic cyber threats that could destabilise critical systems and infrastructure, through threat intelligence sharing and coordinated incident response.

Kenya Women Parliamentary Association (KEWOPA) Digital Upskilling Training Programme

Mr. Eric Kobia (third from right, front row) from the Authority's National KE-CIRT/CC, joins women parliamentarians for a group photo during a Digital Upskilling Training Programme held from 8th - 9th June 2026, in Nairobi.

The Authority participated in a Digital Upskilling Training Programme organised by the Kenya Women Parliamentary Association (KEWOPA), that was held from 8th - 9th June 2026 in Nairobi. The programme was aimed at strengthening the capacity of women parliamentarians to navigate the digital space safely, securely and effectively. The programme further enhanced their ability to promote cyber awareness, encourage responsible online behaviour and champion safe digital participation within the constituencies they represent. The Authority was represented by Mr. Eric Kobia from the National KE-CIRT/CC.

During the engagement, the Authority delivered a presentation highlighting the policy, legal and regulatory frameworks governing the protection of women's digital rights in Kenya. The presentation also outlined the Authority's role, through the National KE-CIRT/CC, in monitoring cyber threats, coordinating incident response, promoting cyber resilience and supporting law enforcement agencies in addressing technology-facilitated gender-based violence (TFGBV).

The training programme covered key thematic areas such as cyber safety and security, cyber hygiene, incident response, artificial intelligence (AI), online abuse, election-related digital risks and emerging cyber threats. Participants were also sensitised on practical measures for safeguarding Personally Identifiable Information (PII), recognising and responding to diverse cyber threats, and promoting the safe and responsible use of digital platforms including social networking platforms.

Overall, the programme enhanced participants' understanding of the opportunities and risks associated with the digital ecosystem and strengthened their capacity to promote safe, secure and responsible online engagement. It further reinforced collaboration between the Authority and other stakeholders in advancing digital literacy, strengthening cyber resilience and promoting the protection of women leaders and the communities they serve.

55th Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

Ms. Donna Owiti from the Authority's National KE-CIRT/CC provides an overview of Kenya's cyber threat landscape.

Ms. Lynet Kosgei from Kenya Airways, the national carrier, outlines developments within the aviation sector.

Representing the Kenya Education Network Trust (KENET), Mr. Kennedy Aseda addresses members during the quarterly engagement.

The 55th meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC) was held on 20th May 2026 in Nairobi. The NKCC comprises representatives from more than 50 public and private sector organisations across Kenya's Critical Information Infrastructure (CII) sector. Through its quarterly engagements, the Committee continues to enhance collaboration, build cybersecurity capacity, facilitate information sharing on emerging cyber threats and coordinate collective response efforts to enhance Kenya's cyber resilience.

During the meeting, members provided updates on initiatives being implemented within their respective domains to strengthen cybersecurity resilience. These included cybersecurity capacity building programmes in learning institutions supported through international partnerships. These programmes continue to enhance the skills of senior technical officers in cyber resilience and strengthened cybersecurity governance among institutional leadership. Members also reported progress in deploying Artificial Intelligence (AI)-enabled penetration testing tools to improve vulnerability identification and strengthen the security posture of educational institutions.

The Committee reviewed ongoing cyber simulation exercises designed to assess institutional preparedness, decision-making and incident response capabilities in the event of a cyber crisis. In addition, members discussed a growing trend in cyber-enabled financial fraud and highlighted the need to enhance public education and awareness, and strengthen preventive and response measures to address emerging online threats.

Members were further briefed on emerging cyber risks affecting the aviation sector, including an increase in supply chain attacks targeting Global Positioning System (GPS) service providers and a rise in GPS spoofing incidents with the potential to disrupt aircraft navigation and flight operations. In conclusion, the NKCC reiterated the importance of sustained investment in cybersecurity capacity development, the adoption of emerging technologies such as AI-driven security solutions, proactive cyber resilience testing and strengthened collaboration among stakeholders.

Outlook for the Next Quarter

The Authority will host a two-week cybersecurity bootcamp for professionals with the objective of strengthening national cybersecurity resilience, enhancing incident response capabilities, promoting collaboration among the Critical Information Infrastructure (CII) sector and developing local cybersecurity expertise, in addressing emerging and evolving cyber threats.

This programme will equip participants with practical knowledge and skills in firewall policy design, site-to-site and remote-access Virtual Private Networks (VPNs), intrusion prevention, Distributed Denial-of-Service (DDoS) mitigation, penetration testing, content and URL filtering, network access control using identity-based policies and end-to-end enterprise security deployment, among others.

In recognition of the importance of timely and coordinated cyber threat information sharing, the Authority will also host a Cyber Threat Intelligence (CTI) training programme. This CIT programme is aimed at strengthening participants' technical capabilities in the collection, analysis and dissemination of cyber threat intelligence. Further, it aims to promote structured information sharing, enhance threat detection, incident response and strengthen collaboration, among relevant stakeholders.

These programmes are aligned with the Authority's 2023 – 2027 Strategic Plan, which seeks to empower and protect consumers of ICT services while advancing Kenya's digital transformation agenda.

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