COMMUNICATIONS AUTHORITY OF KENYA

# Cybersecurity Report

43rd Edition

July - September 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 Cap.79C (CMCA) in 2018 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 was 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)*

During the period under review, the global cyber threat landscape remained elevated and was characterised by increasingly sophisticated and evolving cyber threats. Organisations continued to face significant threats from ransomware, Distributed Denial-of-Service (DDoS) attacks and social engineering, particularly through advanced phishing scams.

Emerging cyber risks also continued to evolve, notably Advanced Persistent Threats (APTs), supply chain attacks, exploitation of zero-day vulnerabilities and the increasing use of Artificial Intelligence (AI) to orchestrate sophisticated cyber attacks such as deepfakes. Critical Information Infrastructure (CII) across key sectors such as e-government, ICT and telecommunications, banking & finance, and academia, remained a primary target for threat actors.

Further, the exploitation of system vulnerabilities by threat actors continued to pose considerable threats to the delivery of critical services and the continuity of business operations. These developments highlighted the need to strengthen cyber hygiene practices, enhance proactive threat detection capabilities across all sectors and undertake continuous cybersecurity awareness and capacity building programmes.

Between July and September 2026, the Authority's National KE-CIRT/CC detected over 2.6 billion cyber threat events, largely attributed to the exploitation of system vulnerabilities. This represented a 14.45% increase compared to the preceding reporting period of April to June 2026. In response to the threats detected, we issued more than 20 million cyber threat advisories.

The cyber threat advisories disseminated highlighted the need for organisations to strengthen their cybersecurity readiness and resilience through the implementation of appropriate preventive, protective and response measures. These include timely patching of operating systems, software applications and firmware, implementation of password management mechanisms such as Multi-Factor Authentication (MFA), deployment of appropriate endpoint and other security solutions, and effective management of network firewalls. These measures remain essential to addressing system vulnerabilities, strengthening cyber resilience and reducing exposure to emerging and evolving cyber threats.

In line with the Authority's 2023–2027 Strategic Plan, which prioritises the strengthening of cybersecurity frameworks, national readiness and collaboration with domestic and international partners, the Authority participated in a Threat Intelligence Sharing Platform (TISP) training programme under the Kenya Cyber Resilience (KCR) initiative, coordinated by the Ministry of Information, Communications and the Digital Economy.

The programme sought to advance the objectives of the KCR initiative by strengthening national capacity for sharing of Cyber Threat Intelligence (CTI), enhancing coordination among key cybersecurity stakeholders and supporting the development of trusted mechanisms for information exchange. It provided participants with an opportunity to assess existing threat intelligence sharing arrangements, identify priority technical and operational requirements and develop practical approaches for improving situational awareness, and coordinated cyber threat detection and response. The programme also supported the development of a national CTI dashboard, pilot planning and an initial Action Plan to guide the operationalisation of the TISP.

The Authority remains committed to strengthening the capacity of stakeholders across the cybersecurity ecosystem to prevent, detect and respond to evolving cyber threats. Through targeted capacity building programmes, adoption of relevant industry best practices and enhanced strategic partnerships, we will continue to strengthen our national cyber resilience and support the development of a secure and trusted digital ecosystem.

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

# Cyber Threat Landscape Overview

# Global Cyber Threat Landscape Overview

During the period July - September 2026, the cybersecurity landscape continued to be characterised by persistent ransomware activity, phishing and social engineering, exploitation of system vulnerabilities and the increasing use of Artificial Intelligence (AI) to support cybercrime. Threat actors continued to exploit weaknesses in identity, remote access, system configuration and user awareness, while organisations faced growing risks to the confidentiality, integrity and availability of information and digital services.

## *1. Ransomware*

Ransomware remained a persistent threat, with attackers increasingly combining system disruption with data theft and extortion. Global threat intelligence continued to identify groups such as Qilin, The Gentlemen, Cl0p, Orova and Dire Wolf among active ransomware operations. Kenyan organisations also remained exposed, with some identified among organisations targeted or listed by ransomware groups. Initial access was commonly obtained through phishing, compromised credentials, exposed remote-access services and exploitation of vulnerabilities in systems facing the Internet. Attackers then sought to escalate privileges, move laterally and exfiltrate sensitive information before disrupting systems.

In response, the National KE-CIRT/CC issued advisories urging organisations to implement Multi-Factor Authentication (MFA), secure remote access, apply timely security updates, segment networks, monitor privileged accounts, maintain isolated backups and regularly test recovery procedures.

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

Distributed Denial-of-Service (DDoS) attcks remained a concern for organisations providing publicly accessible digital services. Attackers continued to use large volumes of traffic to overwhelm targeted systems and disrupt service availability. Attacks involved compromised devices and botnets, as well as reflection and amplification techniques that generated large volumes of traffic towards targeted services. Internet-facing infrastructure and connected devices remained potential sources of exposure where security controls were inadequate.

In response, the National KE-CIRT/CC issued advisories encouraging organisations to implement DDoS monitoring and protection, maintain appropriately configured firewalls and intrusion detection controls, secure network devices and collaborate with Internet Service Providers (ISPs) and other relevant partners to support rapid detection and traffic mitigation.

## *3. Social Engineering*

Phishing and other social engineering scams remained among the most common methods used to obtain user credentials, perpetrate financial fraud and gain initial access to organisational systems. Threat actors increasingly used convincing messages, impersonation and trusted digital services to make malicious activity appear legitimate. Attackers used fraudulent emails, messages, links and login pages to capture credentials or redirect users to malicious content. Social engineering was also used to manipulate users into approving requests, disclosing information or bypassing security procedures.

In response, the National KE-CIRT/CC issued advisories urging organisations to strengthen phishing-resistant authentication, conduct regular staff awareness training, verify unusual requests through independent channels, and implement email and endpoint security controls to detect malicious content.

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

## *4. Exploitation of System Vulnerabilities and Misconfigurations*

Exploitation of vulnerabilities in public-facing systems continued to present a significant risk. During the period July - September 2026, the disclosure and observed exploitation of vulnerabilities affecting Citrix NetScaler demonstrated the risks associated with delayed patching of exposed infrastructure. Threat actors scanned for vulnerable or poorly configured systems and exploited weaknesses to gain unauthorised access, execute malicious activity or establish a foothold within affected environments. Misconfigured services and unnecessary exposure of management interfaces further increase the attack surface.

In response, the National KE-CIRT/CC issued advisories cautioning organisations to maintain accurate asset inventories, conduct regular vulnerability assessments, prioritise timely patching, securely configure systems and remove unnecessary internet exposure. Continuous monitoring of critical internet-facing services was also important for identifying and addressing weaknesses promptly.

## *5. Emerging Threats: AI-Enabled Cybercrime*

Artificial Intelligence (AI) continued to influence the cyber threat landscape during the quarter, with bad actors increasingly using AI to support phishing, social engineering, credential harvesting and other cybercrime activities. Regional threat reporting also highlighted the growing use of AI alongside Cybercrime-as-a-Service (CaaS). AI tools enabled attackers to produce more convincing communications, automate elements of malicious activity and increase the scale and speed of campaigns. This reduced some of the technical and operational barriers previously associated with conducting cyberattacks.

In response, the National KE-CIRT/CC issued advisories urging organisations to strengthen identity and access controls, improve staff awareness of AI-enabled scams, maintain effective monitoring and threat intelligence capabilities, and establish appropriate governance for the secure use of AI tools. Security controls should also be regularly reviewed as AI-enabled attack techniques continue to evolve.

## *6. Overall Perspective*

The period July to September 2026 demonstrated that cybersecurity risks continued to be driven by a combination of established attack techniques and emerging technologies. Ransomware, phishing, Distributed Denial-of-Service (DDoS) attacks and exploitation of system vulnerabilities remained persistent threats during the period.

At the same time, the increasing use of Artificial Intelligence (AI) created additional opportunities for threat actors to enhance the scale and sophistication of cyber attacks. In response, strengthening cyber hygiene, identity security, vulnerability management, monitoring, user awareness and incident-response preparedness remained critical to enhancing organisational cyber resilience.

# Cyber Threat Landscape Roundup

## *Total Cyber Threats Detected*

**2,696,335,021** | **14.45%**

The National KE-CIRT/CC detected over **2.6 billion** cyber threat events during the period between **July - September 2026**. This represented a **14.45%** increase from the threat events detected during the previous period, April - June 2026. The Authority continued to enhance the dissemination of cyber threat advisories to the Critical Information Infrastructure (CII) sector, as part of its broader commitment to enhancing national cybersecurity resilience in response to the evolving cyber threat landscape.

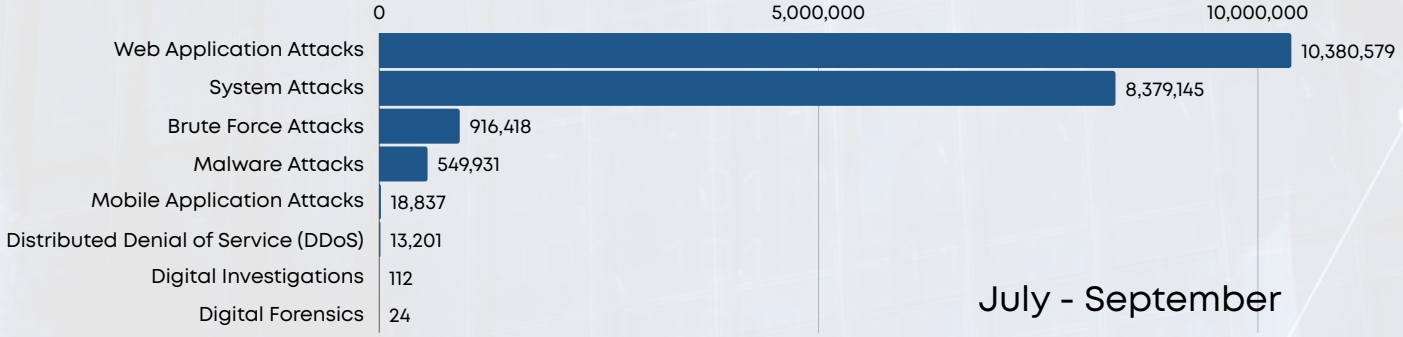
These threats were largely attributed to inadequate system patching, insufficient user awareness of phishing and other social engineering attacks, and the increasing exploitation of AI technologies by malicious actors to execute more sophisticated cyberattacks.

## *Total Cyber Threat Advisories Issued*

**20,258,111** | **2.36%**

The National KE-CIRT/CC issued **20,258,111** advisories between the period **July - September 2026**, in response to the detected cyber threat events. This represented a **2.36%** decrease compared to the advisories that were issued during the previous period, April - June 2026.

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

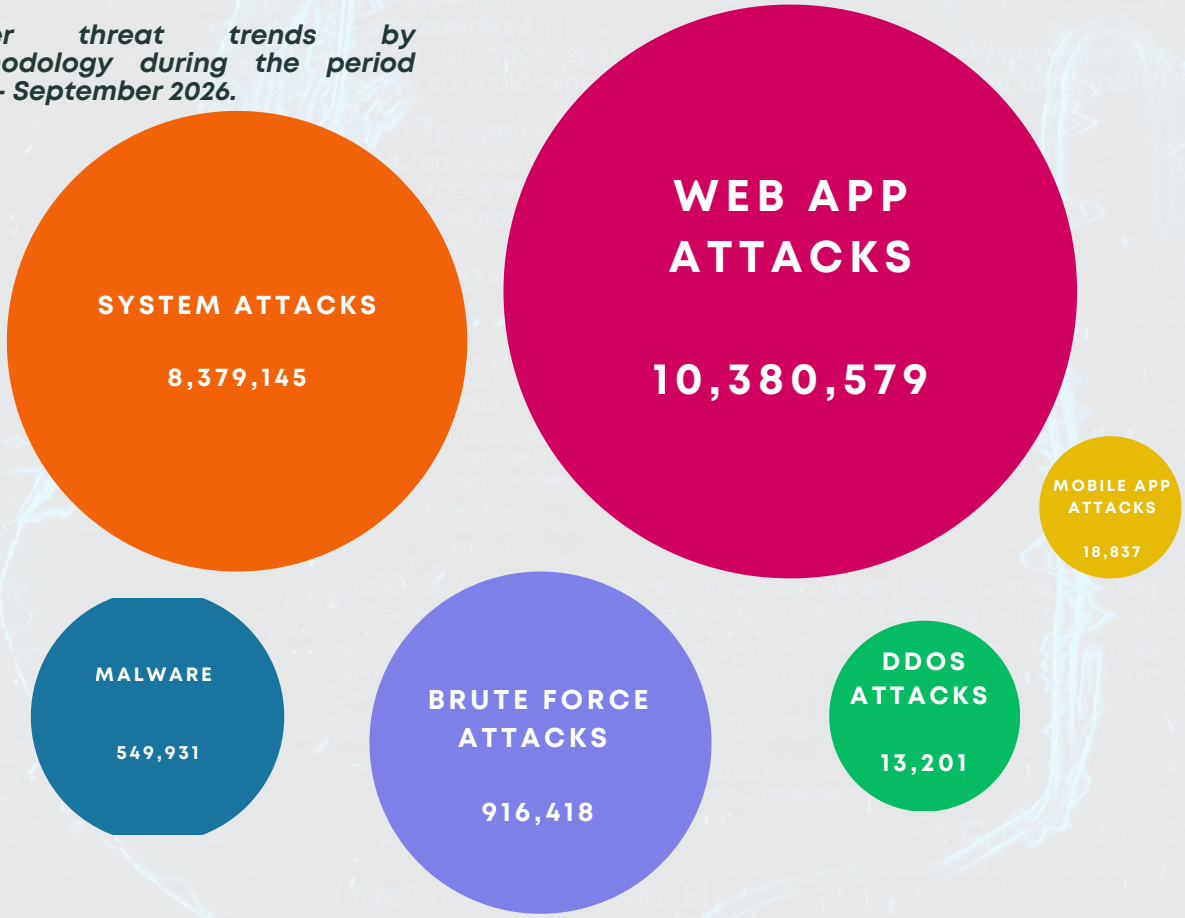


# Cyber Attack Vector Trends

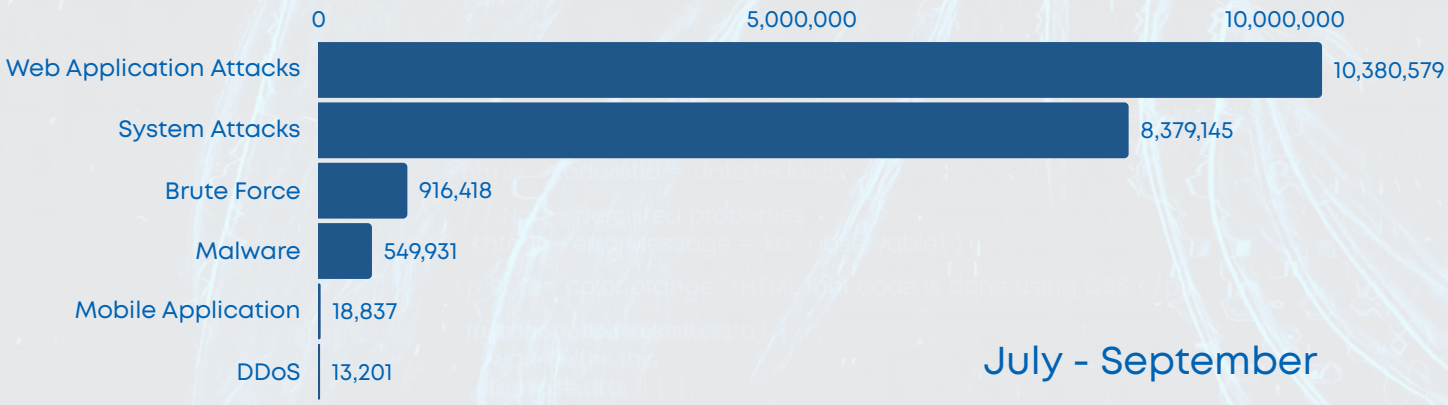
Web application attacks and system attacks remained the most prevalent cyber threat vectors during the period under review. Web application attacks were primarily associated with the exploitation of vulnerable third-party libraries, inadequately secured Application Programming Interfaces (APIs), insecure serverless configurations and weaknesses within open-source software dependencies.

System attacks, on the other hand, were largely attributed to credential-stealing malware, weak access controls, information leakage, continued use of outdated and vulnerable operating systems, and user interaction with malicious links, among other attack techniques.

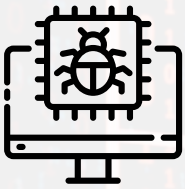
***Cyber threat trends by methodology during the period July - September 2026.***




Comparison of cyber attack vector trends (per vector) issued during the period **July - September 2026.**



# Malware Trends



**Threats Detected**

**70,800,154**

**20.01%**

**Advisories Issued**

**549,931**

**0.47%**

During the period between **July - September 2026,** the National KE-CIRT/CC detected **70,800,154** malware threat attempts targeted at the Critical Information Infrastructure (CII) sector. This represented a **20.01%** increase from the previous period, April - June 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 the deployment of Remote Access Trojans (RATs). Other targeted sectors included academia, individual users and the financial sector, particularly banks, cryptocurrency platforms, foreign exchange 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**

**27,435,527**

**57.62%**

**Advisories Issued**

**10,380,579**

**2.02%**

During the three-month period between **July - September 2026**, the National KE-CIRT/CC detected **27,435,527** web application attack attempts targeted at the critical information infrastructure sector. This represented a **57.62%** increase from the previous period, April - June 2026.

Government systems and Internet Service Providers (ISPs) remained the primary targets, with threat actors focusing on the compromise of user authentication credentials, vulnerable web browsers and database servers. A significant proportion of these attacks exploited weaknesses in SSL/TLS security configurations, facilitating unauthorised system access and interception of sensitive information 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**

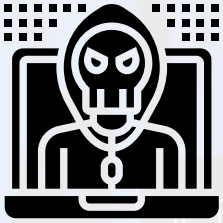
- **Government**
- **Internet Service Providers (ISPs)**
- **Cloud Service Providers**
- **Academia**

These attacks exploited vulnerabilities such as unauthenticated remote code execution, privilege escalation and reflected cross-site scripting to gain unauthorised access, elevate system privileges and compromise sensitive information, potentially resulting in data breaches and reputational impact on affected organisations.

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**

**44,949,518**

**85.41%**

**Advisories Issued**

**916,418**

**14.12%**

During the three-month period from **July - September 2026**, the National KE-CIRT/CC detected **44,949,518** brute force attack attempts majorly targeting the critical information infrastructure sector. This represented a **85.41%** increase from the previous period, April - June 2026.

These attacks primarily targeted cloud service providers and government systems, with threat actors focusing on the compromise of database servers and user authentication credentials. Successful compromises were largely attributed to vulnerabilities within database infrastructure, weak authentication controls and insecure Remote Desktop Protocol (RDP) configurations, which facilitated unauthorised access to critical systems and 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**

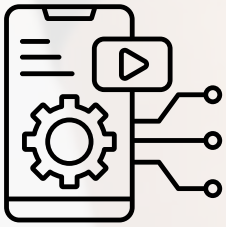
- Cloud Service Providers
- Government

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 Multi-Factor Authentication (MFA) 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**

**177,732**

**3.08%**

**Advisories Issued**

**18,837**

**34.43%**

During the three-month period from **July - September 2026,** the National KE-CIRT/CC detected **177,732** mobile application attack attempts targeting end-user devices. This represented a **3.08%** decrease from the previous period, April - June 2026.

Mobile devices and Android TVs remained key targets, with threat actors exploiting weak credential management practices, particularly the continued 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**

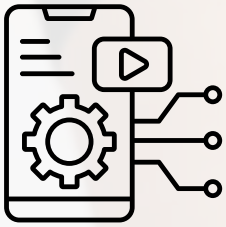
- Improper Credential Usage
- Inadequate Supply Chain Security
- Insecure Authentication
- Insufficient Input/Output Validation
- Insecure Communication
- Inadequate Privacy Controls
- Insufficient Binary Protections
- Security Misconfiguration
- Insecure Data Storage
- Insufficient Cryptography

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**

**23,124**

**97.18%**

**Advisories Issued**

**13,201**

**90.92%**

During the three-month period from **July - September 2026,** the National KE-CIRT/CC detected **23,124** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure. This represented a **97.18%** decrease from the previous period, April - June 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**

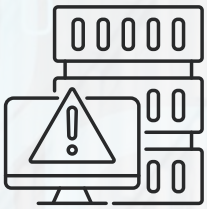
- Reflection/Amplification UDP Abuse: attackers leveraged spoofed UDP services (DNS/NTP/SSDP) to amplify traffic into Tbps floods.
- Missing Source Address Validation (No ISAV): networks allowing IP spoofing enabled large reflection/amplification attacks.
- IoT/Router Botnets: compromised consumer devices 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**

**2,552,948,966**

**13.25%**

**Advisories Issued**

**8,379,145**

**0.05%**

July - September

Most system attacks targeted operating systems and database servers of Internet Service Providers (ISPs) and cloud service providers, exploiting vulnerabilities associated with inadequate patch management, legacy systems and poorly secured Internet of Things (IoT) devices, thereby expanding the attack surface.

During this period, the National KE-CIRT/CC detected over **2.5 billion** attacks, resulting in the issuance of about **8.3 million** cyber threat advisories. The disparity between detected events and advisories issued reflects the aggregation of multiple related threat events into consolidated reports to facilitate targeted communication of actionable threat intelligence and recommended mitigation measures to affected stakeholders.

**Top Targeted Systems**

- Database Servers
- Operating Systems
- Network Devices
- Web Applications
- Remote Access Systems
- Critical Infrastructure
- Mailing Servers
- User Accounts
- Backup system printers

**Top Affected Industries**

- Internet Service Providers
- Cloud Service Providers
- Health Sector

**Top Targeted Exploits**

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

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 (MFA).
- Enhancing firewall configurations.

# Capacity Development & Partnerships

# The Africa PKI Consortium (AfPKIC) Annual General Meeting (AGM) 2026

***Dr. Vincent Ngundi, Director of Cyber Security and Head of the National KE-CIRT/CC, delivering his remarks during the Africa PKI Consortium (AfPKIC) Annual General Meeting (AGM) 2026 on 25th August 2026, in Abuja, Nigeria.***

The Authority participated in the Africa PKI Consortium (AfPKIC) Annual General Meeting (AGM) 2026, held from 25th - 26th August 2026 in Abuja, Nigeria, under the theme, *"Building Africa's Digital Trust Ecosystem: Harmonization, Capacity and Interoperability."* The meeting was hosted by Nigeria through the National Identity Management Commission (NIMC) and brought together thought leaders and delegates from several African countries.

The Authority was represented by Dr. Vincent Ngundi, the Director of Cyber Security and Head of the National KE-CIRT/CC. In his address to delegates, Dr. Ngundi highlighted Kenya's progress in strengthening the National Public Key Infrastructure (NPKI) as a foundation for secure electronic transactions and digital trust. He outlined Kenya's policy, legal and regulatory frameworks supporting electronic certification services and observed that the Authority has licensed and accredited six Electronic Certification Service Providers (E-CSPs). He further explained the role of the NPKI in supporting secure e-government services and in enhancing interoperability.

The AGM provided a platform for advancing continental priorities on the harmonisation of PKI standards, strengthening governance frameworks, enhancing technical capacity and promoting cross-border interoperability. Through its specialised working groups, the Consortium continues to bring together government, industry and academia to address priorities across the technical, policy, capacity building, innovation and sustainability thematic areas.

The meeting further highlighted the importance of strengthening PKI governance, developing scalable digital trust infrastructure and promoting harmonised standards to support Africa's growing digital economy. Continuous collaboration among the AfPKIC leadership, Member States and international partners will be critical to advancing the Consortium's objectives.

# Courtesy Call by the United Kingdom National Cyber Security Centre (NCSC-UK)

***Group photo during the visit by Mr. Ollie Whitehouse, Chief Technology Officer at the United Kingdom's National Cyber Security Centre (NCSC-UK) (third from right), to the Authority's National KE-CIRT/CC on 29th September 2026 at the CA Centre in Nairobi. Mr. Whitehouse was received by Dr. Vincent Ngundi, Director, Cyber Security and Head of the National KE-CIRT/CC (third from left). Also present were Eng. Dennis Chepkwony, Director, Universal Service Fund (extreme left), and CS. Lydia Sitienei, Director, Legal Services and Corporation Secretary (extreme right). Mr. Whitehouse was accompanied by Mr. Matt Jowett, Head of Cyber - Africa (second from right) and Ms. Clarian Makungu, Africa Cyber Programme Project Manager (second from left), both from the British High Commission in Nairobi.***

The Authority hosted Mr. Ollie Whitehouse, Chief Technology Officer at the United Kingdom's National Cyber Security Centre (NCSC-UK), for a courtesy visit on 29th September 2026 at the CA Centre in Nairobi. The visit formed part of ongoing engagements aimed at strengthening the longstanding Kenya–UK cybersecurity partnership and enhancing institutional cooperation on shared priorities relating to cyber resilience, digital trust and the protection of Critical Information Infrastructure (CII) sector.

The engagement provided a platform for strategic dialogue on the evolving cyber threat landscape, emerging risks affecting government systems, the CII sector and approaches to strengthening national cyber resilience. The discussions also explored opportunities for enhanced cooperation between the NCSC-UK and the Authority's National KE-CIRT/CC in areas of mutual interest, including information sharing, capacity building, technical collaboration, and institutional readiness and resilience.

Held within the broader framework of the 2025–2030 Kenya–UK Strategic Partnership, the meeting reiterated the commitment of both countries to advancing cybersecurity cooperation, strengthening digital resilience and supporting the development of a safer, secure and trusted digital environment.

# Benchmarking and Study Visit by the South Sudan Computer Incident Response Team (SS-CIRT)

*The delegation from the South Sudan Computer Incident Response Team (SS-CIRT) led by Eng. Vukeni Innocent Joseph (foreground), during the visit on 3rd September 2026, in Nairobi.*

*Mr. Rodgers Mumelo from the Authority's National KE-CIRT/CC, engages with the South Sudanese delegates during the benchmarking exercise.*

The South Sudan Computer Incident Response Team (SS-CIRT) conducted a benchmarking and study visit to the Authority's National KE-CIRT/CC on 3rd September 2026. The SS-CIRT is established under the National Communication Authority (NCA), the regulatory agency for the ICT sector and serves as the national focal point for coordinating responses to cybersecurity incidents and cyber threats in South Sudan.

The visit sought to provide the delegation with an understanding of Kenya's cybersecurity management framework, including the supporting policy, legal and regulatory regime, as well as the institutional structures, processes and governance mechanisms that support national cybersecurity coordination and oversight. The engagement also provided an opportunity to share best practices on cybersecurity strategy implementation and regulatory compliance, while exploring opportunities to strengthen institutional capacity, enhance collaboration and improve preparedness in addressing evolving cyber threats.

The delegates were also briefed on the roles of other key institutions within Kenya's cybersecurity ecosystem. These include the Ministry of Information, Communications and the Digital Economy, which provides policy leadership and strategic direction for the ICT sector, as well as on digital transformation and cybersecurity governance, and the Technology Service Providers of Kenya (TESPOK), which supports industry coordination, manages national critical infrastructure such as the Kenya Internet Exchange Point (KIXP) and facilitates incident response through the TESPOK iCSIRT.

The engagement forms part of the Authority's ongoing initiatives, through the National KE-CIRT/CC, to strengthen regional collaboration, promote information sharing and enhance collective readiness and response to the dynamic cyber threat landscape.

# 56th Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

***Members pose for a group photo during the 56th meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC) that was held on 23rd September 2026, in Nairobi.***

The 56th meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC) was held on 23rd September 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 meetings, the NKCC continues to strengthen collaboration, build cybersecurity capacity, facilitate information sharing on emerging cyber threats and coordinate collective response efforts, to enhance the country's cyber resilience.

During the meeting, members provided updates on initiatives across sectors aimed at strengthening cybersecurity resilience. The e-government sector stressed the need for stronger protection of information assets and the adoption of a more proactive approach to data security following a breach earlier in the year, while working to address audit requirements raised by the Office of the Data Protection Commissioner (ODPC). The National KE-CIRT/CC highlighted its role in stakeholder coordination, the dissemination of threat advisories, regulatory compliance, among other responsibilities.

Members were also apprised on emerging risks in the aviation sector, that includes credential theft, third-party software compromise and exploitation of known vulnerabilities. The sector called for stronger implementation of the National Information Sharing Framework, increased focus on Identity and Access Management (IAM) and AI-related cybersecurity training. It also reported progress towards establishing a Security Operations Centre (SOC) and proposed a forum for knowledge sharing on SOC operations.

Private sector and civil society stakeholders highlighted ongoing initiatives in cybersecurity capacity building, vulnerability management, awareness on AI, digital literacy and cyber hygiene. Members also emphasised the need to expand such programmes beyond Nairobi to strengthen national outreach and impact.

In conclusion, members reiterated the importance of continued collaboration, information sharing and coordinated implementation of cybersecurity initiatives across all sectors.

# Bilateral Exchange on Cybersecurity Best Practices with the Tanzania Communications Regulatory Authority (TCRA)

On 28th August 2026, the Authority's National KE-CIRT/CC, hosted a bilateral exchange on cybersecurity best practices with the Tanzania Communications Regulatory Authority (TCRA). The Tanzania Computer Emergency Response Team (TZ-CERT), which serves as the national Computer Incident Response Team (CIRT), is established and operates within the TCRA, providing an institutional framework for coordinating national cybersecurity incident response and related functions.

TCRA expressed interest in gaining a deeper understanding of the tools, technologies and operational processes required to support an effective Cyber Security Operations Centre (CSOC). Discussions also centred around approaches to cyber incident detection and response, Cyber Threat Intelligence (CTI) sharing and coordination mechanisms for strengthening collaboration among relevant partners and stakeholders.

The engagement provided a platform for knowledge exchange and regional cooperation, with the National KE-CIRT/CC sharing its experience in coordinating national cybersecurity operations and supporting sectoral CSOCs. The engagement is expected to contribute to stronger regional collaboration, enhanced operational coordination and improved preparedness and response to emerging cyber threats.

# Benchmarking Visit by Kenya Navy Students from the Kenya Defence Forces (KDF)

On 19th August 2026, the Authority's National KE-CIRT/CC hosted Kenya Naval Communications Students, Class 035/24, from the Kenya Navy of the Kenya Defence Forces (KDF). The visit provided the students with practical insights into the Authority's cybersecurity mandate and the role of the National KE-CIRT/CC in coordinating national cyber incident response, strengthening cyber resilience and supporting the protection of the Critical Information Infrastructure (CII) sector. The engagement also highlighted the strategic importance of secure, reliable and resilient communications systems in enhancing national security, situational awareness and operational effectiveness.

The engagement further highlighted the complementary roles of the Authority and the KDF in strengthening the security and resilience of Kenya's communications and digital ecosystem. Discussions covered cybersecurity, secure communications, data governance, emerging technologies and evolving cyber threats, while emphasizing the importance of continuous capacity building, specialised technical skills development and enhanced inter-agency collaboration. Such engagements strengthen national readiness, cyber awareness and the protection of the CII sector.

# Training Programme on a Threat Intelligence Sharing Platform (TISP)

The Authority participated in a Threat Intelligence Sharing Platform (TISP) training programme held from 13th - 17th July, 2026 in Nairobi. The programme was undertaken as part of the Kenya Cyber Resilience (KCR) initiative, that is being coordinated by the Ministry of Information, Communications and the Digital Economy. The training brought together 16 participants drawn from key institutions within Kenya's cybersecurity ecosystem, comprising representatives from the Authority's National KE-CIRT/CC, the National Computer and Cybercrimes Coordination Committee (NC4), the ICT Authority, the Directorate of Criminal Investigations (DCI), the Ministry of Information, Communications and the Digital Economy (MICDE).

The TISP training programme focused on strengthening national capacity to develop and operationalise a trusted cyber threat intelligence sharing platform. Key areas included team formation, trusted sharing of indicators, alerts and advisories, development of a national CTI dashboard, and identification of priority technical requirements. The programme also supported pilot planning and culminated in an initial Action Plan to guide the TISP development team in enhancing information sharing, situational awareness and coordinated cyber threat detection and response.

The KCR initiative is aimed at strengthening Kenya's national cybersecurity capabilities, improving coordination among relevant stakeholders and enhancing resilience across the digital ecosystem. Funded by the European Union (EU) and implemented by Expertise France in partnership with the Estonian Centre for International Development (ESTDEV), the three-year initiative is expected to contribute to a safer, more inclusive and trusted cyberspace in Kenya.

# Study Tour by the General Service Unit (GSU) of the National Police Service (NPS)

The Authority recently hosted officers from the General Service Unit (GSU) of the National Police Service (NPS) for a study tour to the National KE-CIRT/CC on 4th September, 2026 at CA Centre, in Nairobi. The engagement provided the officers with an overview of Kenya's cybersecurity management framework, including the policy, legal and regulatory environment that supports national cybersecurity coordination.

The visit also exposed the GSU Station Commanders, who are undertaking the Ordinary Subordinate Officers to Inspector of Police Course, to the operations of the National KE-CIRT/CC, including cyber threat monitoring, incident coordination, information sharing and stakeholder collaboration. The engagement provided an opportunity to exchange knowledge and best practices on cybersecurity governance and operational preparedness.

The visit further reinforced the longstanding collaboration between the Authority and the NPS and forms part of ongoing efforts to strengthen inter-agency cooperation, institutional capacity and coordinated responses to emerging cyber threats in support of national security objectives.

# Outlook for the Next Quarter

In collaboration with the Africa Cyber Defense Forum (ACDF) and other strategic partners, the Authority will host the 7th Africa Cyber Defense Forum 2026, scheduled to take place from 2nd to 5th November 2026 in Nairobi. The Forum, themed *"Africa's Cyber Sovereignty: From Vision to Action in a Fragmented World,"* will bring together cybersecurity leaders, policymakers, industry players and technical experts to advance dialogue and practical solutions towards strengthening Africa's cyber resilience and digital sovereignty. The programme will include capacity building workshops on 2nd and 3rd November 2026, followed by the main conference on 4th and 5th November 2026.

The Forum will provide a platform for multi-stakeholder engagement on key areas including capacity building and local talent development, regional cooperation among CIRTs/CERTs/CSIRTs, development of home-grown solutions, secure cloud and digital infrastructure, cybersecurity policy frameworks, AI and emerging technologies. The engagement is expected to strengthen collaboration, the sharing of Cyber Threat Intelligence (CTI), institutional readiness and collective capacity to prevent, detect, respond to and recover from evolving cyber threats.

The Forum will bring together senior government officials, cybersecurity thought leaders and practitioners, the CII sector, policymakers and regulators, academia, technology service providers, innovators and start-ups, investors, researchers, students and other diverse stakeholders within Africa's cybersecurity ecosystem. This broad representation is intended to enhance partnerships, knowledge exchange and coordinated approaches towards building a secure, resilient and trusted digital environment across Kenya and the wider African continent.

# 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