COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

39th Edition

July - September 2025

A report by:

The National KE-CIRT/CC

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

incidents@ke-cirt.go.ke

www.ke-cirt.go.ke

Strategic Direction

Our Vision

Digital Access for All

Our Mission

Enabling a Sustainable Digital Society through Responsive Regulation

Our Core Values

Integrity, Innovation, Excellence, Inclusion, Agility.

Cybersecurity Mandate

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

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

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

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

Director General's Perspective

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

As we step into the new financial year, the Authority observed that the global threat activity remains heightened and is increasingly becoming sophisticated. Organisations continue to face relentless cyber threats from ransomware, Distributed Denial-of-Service (DDoS) attacks and social engineering, largely driven by advanced phishing campaigns. At the same time, new and emerging risks continue to increase, including advanced persistent threats (APTs), supply chain attacks, exploitation of zero-day vulnerabilities and AI-driven attacks, as demonstrated by the growing prevalence of deepfakes.

These attacks continued to target Critical Information Infrastructure (CII) across essential sectors such as e-government, ICT & telecommunications, banking & finance, academia, among others. Threat actors leveraged various exploits to disrupt critical systems and services, thereby threatening business continuity. These trends highlight the need for enhanced cyber hygiene, proactive threat detection and continuous user awareness training to defend against an increasingly complex and adaptive cyber threat landscape.

Over the period July - September 2025, the National KE-CIRT/CC detected over 842 million cyber threat events, most of which exploited system vulnerabilities. In response to this, the Authority issued over 19 million cyber threat advisories during the same period, representing an increase of about 15 per cent compared to the previous period, April - June 2025.

The majority of cyber threat advisories emphasised the critical importance of undertaking system patching of operating systems, software applications and firmware, enforcing strong password policies through mechanisms such as multi-factor authentication (MFA), deploying antivirus and other security utilities, and appropriately configured network firewalls, to mitigate cyber threats. These priority areas were highlighted as foundational to strengthening organisational cybersecurity posture amid an increasingly dynamic cyber threat landscape.

In line with the Authority's 2023 – 2027 Strategic Plan which prioritises strengthening cybersecurity frameworks, enhancing national preparedness, and deepening collaboration with domestic and international partners, the Authority, in partnership with UK's Foreign, Commonwealth & Development Office (FCDO), hosted a Cyber Threat Intelligence (CTI) training programme in August 2025 for members of the National KE-CIRT/CC Cybersecurity Committee (NKCC). The programme was aimed at strengthening national cyber resilience through capacity building, knowledge sharing and exposure to international best practices.

The programme provided a structured forum for participants to assess Kenya's cyber threat landscape, benchmark against global standards and deliberate on measures to enhance national cyber readiness and resilience. Participants were introduced to the fundamentals of CTI and relevant playbooks customised to the Kenyan context, mapped our threat posture against recognised global standards and developed both tactical and strategic knowledge and skills through cybersecurity simulations and guided discussions.

The Authority reaffirms its commitment to continue empowering stakeholders across the cybersecurity value chain with the tools, perspectives and capabilities required to proactively deal with the ever-evolving cyber threat landscape. Through targeted capacity building programmes, the adoption of industry best practice and strategic partnerships, we will continue to strengthen national cyber resilience and the digital-certification and digital-trust value chain.

Mr. David Mugonyi, EBS
Director General/CEO

Cyber Threat Landscape Overview

Global Cyber Threat Landscape Overview

1. Ransomware

Ransomware groups continued to intensify their activity during this period targeting Critical Information Infrastructure (CII) and public services, aiming both for financial gain and reputational damage impact. Attackers used Ransomware-as-a-Service (RaaS) models augmented by Artificial Intelligence Large Language Models (AI/LLM)-assisted extortion, as well as combined Distributed Denial-of-Service (DDoS) and compliance extortion tactics.

The National KE-CIRT/CC issued advisories to organisations to maintain comprehensive offline backups, enforce zero-trust network segmentation and regularly update threat intelligence to better resist and recover from attacks.

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

Cyber threat actors continued to mount volumetric and multi-vector DDoS campaigns, often leveraging Internet of Things (IoT) botnets and exploiting amplification protocols. This involved several campaigns that used protocol amplification vectors such as Network Time Protocol (NTP) to compromise public time servers and Domain Name System (DNS) to exploit weak DNS servers. Adversaries were observed combining these attacks with large botnet fleets and using DDoS as a pressure tool alongside ransomware.

The National KE-CIRT/CC issued advisories to organisations to use scalable cloud scrubbing to provide checkpoints within cloud environments where they can handle large amounts of traffic and keep services online even when attackers try to overwhelm them thereby reducing downtime. The National KE-CIRT/CC also advised organisations to implement AI-based traffic anomaly detection to enhance behavioural traffic analysis, observe and block suspicious traffic in real time.

3. Social Engineering and Phishing

During this period, social engineering attacks became more personalised, with increased use of AI-generated content, voice deepfakes and Business Email Compromise (BEC) campaigns. Attackers used synthetic voice and video impersonation, refined phishing kits tailored to compromise users visiting targeted online shopping stores and service portals, and carried out campaigns on multiple channels, through email, SMS and voice.

The National KE-CIRT/CC issued advisories to organisations to adopt phishing-resistant authentication such as passkeys and hardware tokens, enforce Multi-Factor Authentication (MFA) on all possible entry points and increase user training to reduce success rates.

Global Cyber Threat Landscape Overview... cont'd

4. System Misconfiguration Exploits

Misconfigurations in cloud services, Application Programming Interfaces (APIs) and default settings continued to be a major factor in breaches and data exposure. Attackers exploited open API endpoints, poorly secured cloud storage, default credentials, and weak access control settings. The speed of cloud adoption left many gaps in secure configuration hygiene.

The National KE-CIRT/CC issued advisories to organisations to apply secure-by-default settings, enforce least privilege access, conduct frequent configuration audits, and use Infrastructure-as-Code (IaC) Scanning to scan for security misconfigurations such as weak passwords, disabled encryption, or publicly open databases thereby reducing exposure.

5. Emerging Threats

During this period, Advanced Persistent Threats (APTs) continued to target critical infrastructure and government systems across Africa, including Kenya. These groups quietly infiltrated networks with the goal of long-term espionage and data theft. Attackers used spear-phishing emails, exploitation of zero-day vulnerabilities and supply chain compromises to gain access. These APTs stayed hidden for long periods of time, moving laterally across systems to collect intelligence.

The National KE-CIRT/CC issued advisories to organisations to strengthen their defences with network segmentation, carry out regular system updates and adopt threat intelligence sharing with emphasis on early detection through behavioral monitoring, since traditional antivirus tools alone often miss these stealthy operations. In addition, the National KE-CIRT/CC continued to enhance its threat intelligence sharing to its constituents and hosted capacity building initiatives aimed at equipping constituents with the knowledge, skills and mindset required to respond to cyber threats effectively.

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

842,320,667 | **81.64%**

The National KE-CIRT/CC detected over **842 million** cyber threat events during the three-month period between **July - September 2025**, which represented an **81.64% decrease** from the threat events detected in the previous period, April - June 2025. The Authority continued to enhance the dissemination of cyber threat advisories to critical information infrastructure sectors as part of its proactive response to the evolving cyber threat landscape.

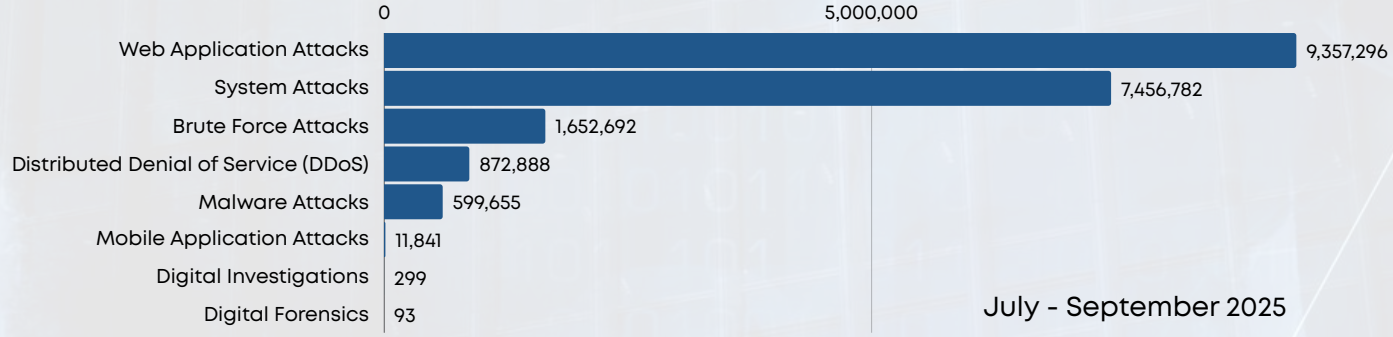
The detected cyber threats can be attributed to several factors, including inadequate system patching, limited user awareness of threat vectors such as phishing and other social engineering techniques, as well as the growing adoption of AI-driven attacks and machine learning technologies by malicious actors.

Total Cyber Threat Advisories Issued

19,951,546 | **15.53%**

The National KE-CIRT/CC issued **19,951,546** advisories between the period **July - September 2025**, which represented a **15.53%** increase compared to the advisories that were issued during the previous period, April - June 2025, in response to the detected cyber threat events.

During the period under review, the Authority enhanced the dissemination of advisories with an emphasis on regular patching of systems and applications, implementing multi-factor authentication (MFA) and robust password policies, properly configured network firewalls and antivirus software, to mitigate emerging cyber threats.

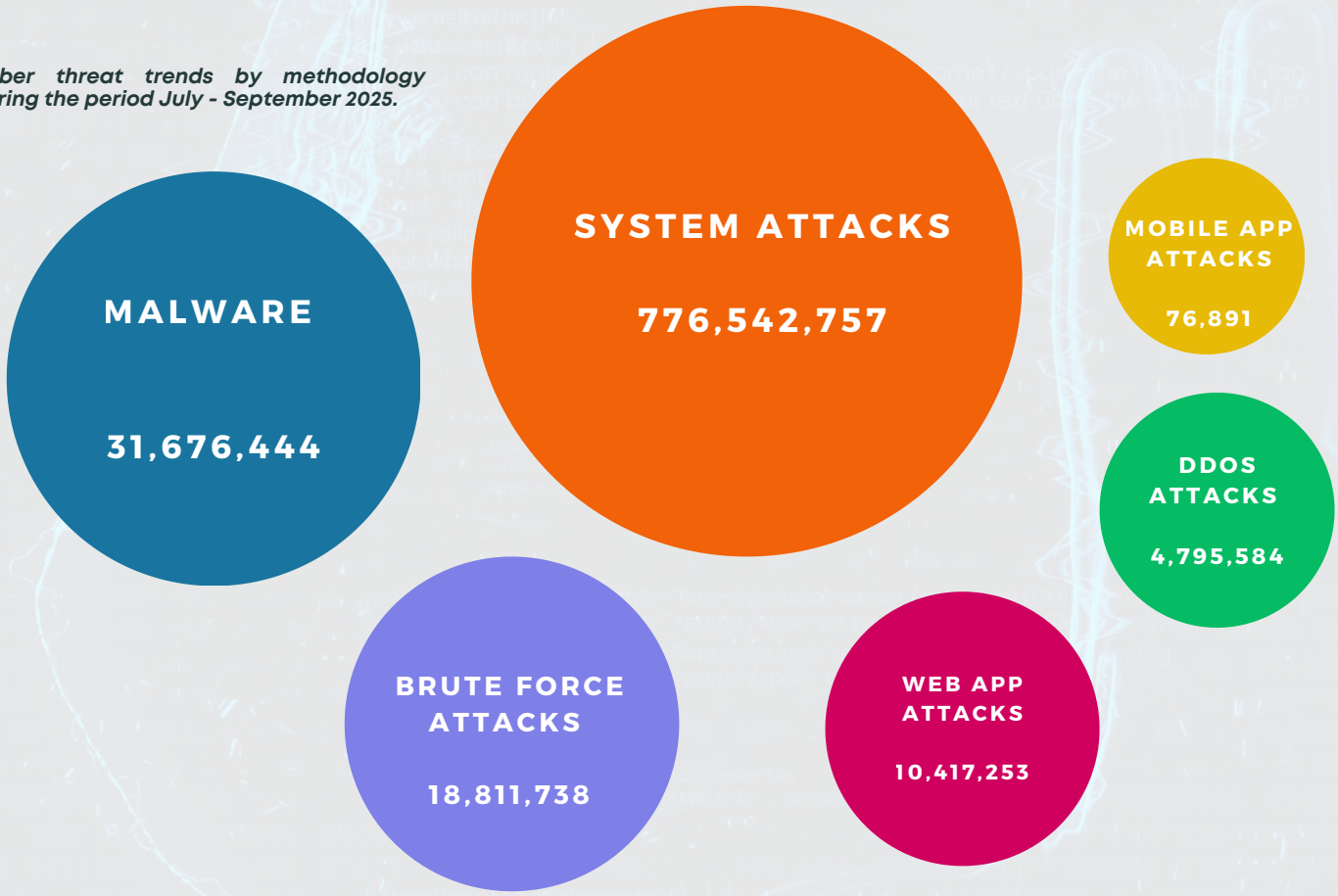


Cyber Attack Vector Trends

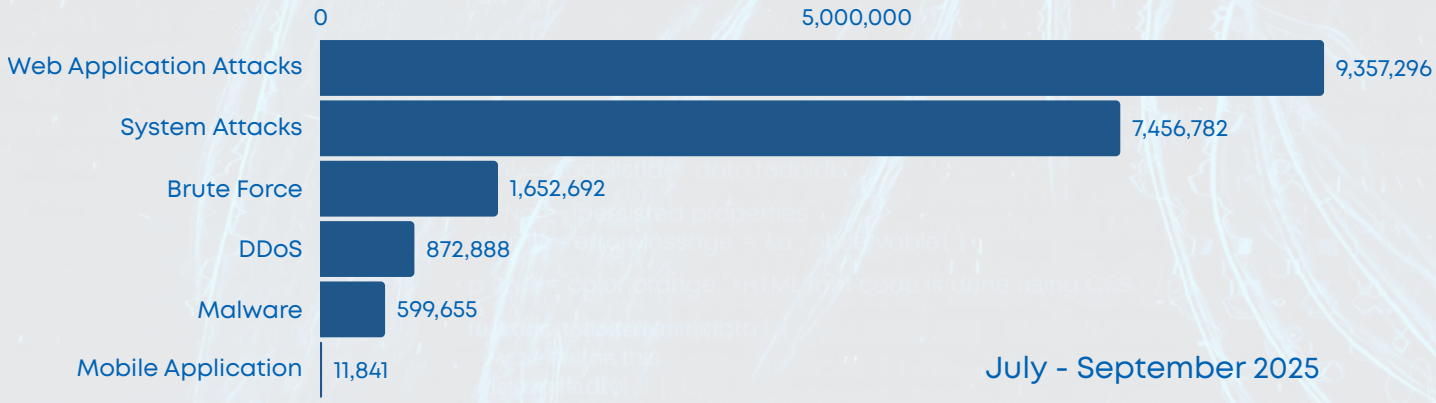
During the period under review, system vulnerabilities and malware attacks emerged as the most prevalent threat vectors, consistent with global cyber threat trends. Key contributing factors to incidents related to misconfiguration included inadequate cyber risk awareness, reliance on deprecated systems, use of default credentials and limited investment in modern infrastructure.

On the contrary, malware attacks may be attributed to exploitation of unpatched vulnerabilities, increased social engineering and phishing attacks, cybercrime-as-a Service (CaaS) models and the widespread use of AI and automation by attackers.

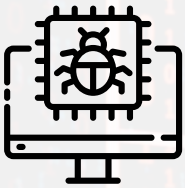
Cyber threat trends by methodology during the period July - September 2025.



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



Malware Trends



Threats Detected

31,676,444

33.17%

Advisories Issued

599,655

7.72%

During the three-month period between July - **September 2025,** the National KE-CIRT/CC detected **31,676,444** malware threat attempts targeted at the critical information infrastructure sector. This represented a **7.72%** increase from the previous period, April - June 2025.

Internet Service Providers (ISPs) and cloud service providers remained key targets, with threat actors focusing on end-user devices, Internet of Things (IoT) components, web applications and network infrastructure. Other sectors that were targeted included government institutions and academia.

Top Targeted Systems

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

Top Affected Industries

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

Top Targeted Exploits

- SharePoint-Deser (CVE-2025-53770 — RCE via unsafe deserialization): Installs remote backdoors by abusing unsafe deserialization in SharePoint, enabling RCE, credential harvesting and forged ViewState attacks against enterprise servers.
- Chrome-ANGLE-Esc (CVE-2025-6558 — Sandbox escape / RCE): Escapes the browser sandbox via ANGLE/GPU calls to run arbitrary code from crafted pages, used to drop loaders and persistent web-based implants.
- Citrix-NetScaler-Overflow (CVE-2025-7775 — Unauthenticated RCE): Unauthenticated memory overflow allowing attackers to execute commands on gateways, implant persistent backdoors and pivot into internal networks.

Malware attacks mostly targeted systems with known vulnerabilities and those containing sensitive information. The objectives of these attacks included data encryption or corruption, reputational damage, the deployment of backdoors for 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

10,417,253

18.25%

Advisories Issued

9,357,296

33.39%

The National KE-CIRT/CC detected **10,417,253** web application attack attempts targeted at the critical information infrastructure sector, during the three-month period between **July - September 2025**, This represented an **18.25%** decrease from the previous period, April - June 2025.

The main targets were government systems and Internet Service Providers (ISPs), with threat actors prioritising compromising user login credentials, vulnerable web browsers and database servers. A significant number of attacks exploited weaknesses in SSL/TLS security configurations to gain unauthorised access and intercept 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**

Top Targeted Exploits

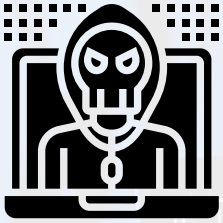
- **FortiWeb-SQLi (CVE-2025-25257 — SQLi → RCE): Installs web shells and remote backdoors by exploiting pre-auth SQL injection in FortiWeb, enabling full server compromise and lateral pivoting.**
- **CodeIgniter-CmdInj (CVE-2025-54418 — Command injection): Executes arbitrary OS commands via a vulnerable endpoint in CodeIgniter apps, used to drop loaders, escalate privileges and deploy ransomware.**
- **LaRecipe-SSTI (CVE-2025-53833 — Server-side template injection): Injects templates to execute server code, resulting in data exfiltration, web shells and complete application takeover.**

Web application attacks were directed at systems deemed vulnerable and holding valuable data. These attacks aimed to disrupt service availability, manipulate or compromise databases and expose sensitive information, ultimately undermining the affected organisation's reputation.

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

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

Brute Force Attack Trends



Threats Detected

18,811,738

10.20%

Advisories Issued

1,652,692

11.18%

The National KE-CIRT/CC detected **18,811,738** brute force attack attempts majorly targeting the critical information infrastructure sector during the three-month period from **July - September 2025**. This represented a **10.20%** decrease from the previous period, April - June 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)

Top Affected Industries

- Cloud Service Providers
- Government

Top Targeted Exploits

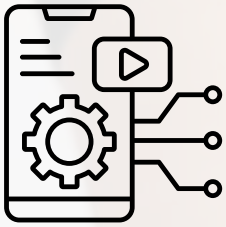
- Drupal-MailLogin (CVE-2025-7393 — Missing rate-limit / brute-force): Allows unlimited login attempts against Mail Login modules, enabling automated password spraying and account takeover on Drupal sites.
- Grandstream-UCM-Auth (CVE-2025-28172 — No auth attempt limits): API/login endpoints permit unlimited password guesses against UCM devices, enabling remote brute-force to obtain admin access and pivot into voice networks.

Over the three-month period, brute force attacks mostly targeted systems perceived to store sensitive information such as user login credentials and financial data. The primary intent of these attacks was to escalate access privileges, obtain unauthorised entry and extract confidential data for financial exploitation.

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

- Implement patch management on devices running network-based services.
- Implement appropriate access management with strong password management.
- Disconnect devices from the network if not in use.
- Update softwares to the latest versions.

Mobile Application Attack Trends



Threats Detected

76,891

59.32%

Advisories Issued

11,841

53.68%

The National KE-CIRT/CC detected **76,891** mobile application attack attempts targeting end-user devices, during the three-month period from **July - September 2025**. This represented a **59.32%** decrease from the previous period, April - June 2025.

Most attacks targeted mobile devices and Android TVs, with threat actors primarily exploiting improper credential use to gain unauthorised access and compromise these devices.

Top Targeted Systems

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

Top Affected Industries

- Mobile devices
- Set-Top Boxes
- Android TVs

Top Targeted Exploits

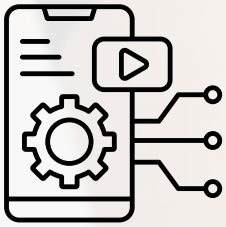
- Improper Credential Usage
- Inadequate Supply Chain Security
- Insecure Authentication
- Insufficient Input/Output Validation

Threat actors targeting mobile applications typically seek to compromise sensitive user information, including financial data, user account credentials and personally identifiable information (PII), for unlawful exploitation or criminal gain.

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

4,795,584

63.34%

Advisories Issued

872,888

32.92%

The National KE-CIRT/CC detected **4,795,584** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure during the three-month period, **July - September 2025**. This represented a **63.34%** decrease from the previous period, April - June 2025.

The majority of attacks targeted healthcare and government systems, primarily exploiting vulnerabilities in remote desktop services and insecure communication protocols.

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, attackers predominantly sought to disrupt public services delivery and compromise the availability of critical systems, thereby disrupting access for legitimate users and degrading overall service quality.

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

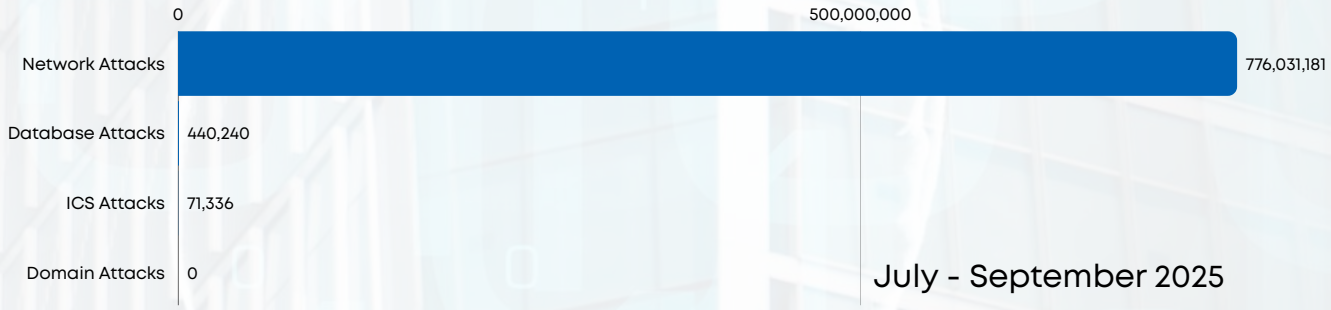
776,542,757

82.71%

Advisories Issued

7,456,782

8.32%



The majority of attacks targeted the ICT sector, with a focus on operating systems and database servers managed by Internet Service Providers (ISPs) and cloud service providers. Threat actors primarily exploited outdated system vulnerabilities and exfiltrated user login credentials. The persistence of such vulnerabilities is largely attributed to the rapid proliferation of Internet of Things (IoT) devices, many of which lack comprehensive security protocols.

Top Targeted Systems

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

Top Affected Industries

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

Top Targeted Exploits

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

System attacks predominantly targeted the critical information infrastructure sector, which holds sensitive assets. These attacks aimed to disrupt operations, compromise system integrity and sabotage critical services at scale.

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

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

Capacity Development & Partnerships

Training Programme on Cyber Threat Intelligence (CTI)

The Authority, in partnership with the UK's Foreign, Commonwealth & Development Office (FCDO), hosted a four-day training programme on Cyber Threat Intelligence (CTI) from 18th to 21st August, 2025, in Nairobi. It was targeted at members of the National KE-CIRT/CC Cybersecurity Committee (NKCC) and was facilitated by KPMG UK.

The training programme was aimed at strengthen national cyber resilience through capacity building, knowledge sharing and exposure to international best practices. It provided a platform for members of the NKCC to assess Kenya's cyber landscape, benchmark against global standards and deliberate on strengthening national preparedness and response mechanisms. 87 trainees from 25 organisations took part in this programme.

The key objectives of the training programme were to:

- Familiarise members of the NKCC with deliverables and knowledge products to inform cyber threat intelligence in the Kenyan context.
- Scope the Kenyan cyber threat landscape against best practice models.
- Build both technical and managerial capacity through practical simulations and discussions.
- Enhance understanding of cyber crisis communication at organizational, stakeholder, and national levels.
- Provide a platform for post-incident review, reflection and development of an actionable roadmap for national cyber resilience.

The opening session focused on socialising and contextualising cyber threat-intelligence deliverables, with participants mapping Kenya's threat landscape against international best practice to establish a common baseline. For the integrated exercises, participants were organised into two complementary groups: a *Bronze Team* of technical personnel responsible for hands-on incident response and penetration testing and a *Gold Team* of personnel at managerial level providing strategic oversight, governance and decision-making during periods of crisis.

Building on this foundation, hands-on penetration-testing labs developed participants' proficiency in identifying and exploiting vulnerabilities, enabling them to emulate real-world attack paths and enhancing detection, containment, and remediation. Breakout sessions brought together smaller groups to evaluate key thematic areas such as incident coordination, stakeholder engagement and resource allocation. This was instrumental in promoting peer learning and cross-sector collaboration.

These workstreams culminated in a national-level cyber crisis simulation that assessed end-to-end coordination between the tactical and strategic teams, including technical detection and containment, executive decision-making, inter-agency communication and recovery planning. Crisis-communication modules addressed internal messaging and staff preparedness, engagement with partners, sector regulators and service providers, and information sharing at the national level, with an emphasis on coherent, accurate and timely communications to maintain public confidence and trust.

The programme concluded with a structured post-incident review, during which participants identified strengths, gaps and lessons learned from the labs and simulations, producing actionable recommendations to improve preparedness, response coordination, and governance.

Training Programme on Cyber Threat Intelligence (CTI)... cont'd

The CTI programme improved participants' understanding of Kenya's cyber threat landscape in line with international benchmarks and strengthened their technical skills in penetration testing and incident handling. It also enhanced crisis-time decision-making and outlined the importance of strategic communication across organisational, stakeholder and national levels.

Participants agreed to prioritise an update of Kenya's National Crisis Communication Plan for cyber incidents.

Highlights from the training programme on Cyber Threat Intelligence (CTI) that was held from 18th to 21st August, 2025, in Nairobi.

2025 Cybersecurity Youth Forum

Dr. Vincent Ngundi (centre, in yellow tie), Director of Cyber Security & Head of the National KE-CIRT/CC, strikes a pose with enthusiastic youth participants during the 2025 Cybersecurity Youth Forum on 11th September 2025, in Nairobi.

The Authority, in collaboration with the Kenya Cyber Security and Forensics Association (KCSFA), hosted the inaugural 2025 Cybersecurity Youth Forum under the theme, "Unpacking Misinformation and Disinformation in the Cyberspace." The event, which took place on 11th September, 2025 in Nairobi, brought together 107 participants that included the youth, academia, cybersecurity experts, policymakers and civil society, and served as a strategic platform to engage young people on issues of digital responsibility, misinformation and cyber threats. The forum aligns with the Authority's 2023 – 2027 Strategic Plan, specifically the strategic goal on empowerment and protection of consumers of ICT services.

IIn his welcoming remarks, Mr. Keniz Agira, Chairman of the KCSFA, raised concerns about the increasing involvement of youth in cybercrime, attributing it to the fast-paced evolution of technology outpacing policy development. Citing the shift to online platforms during the COVID-19 pandemic and the emergence of robust AI tools, he noted that while the youth are quick adopters of technology, their curiosity can sometimes lead to criminal activities. Mr. Agira emphasized the vulnerability of sectors such as banking & finance and education, and warned of rising cyber threats due to institutional and regulatory delays. He highlighted the need for structured mentorship to guide young talent toward innovation rather than exploitation.

The keynote address was issued by the Authority's Director General/Chief Executive Officer, Mr. David Mugonyi, EBS, and was delivered on his behalf by Dr. Vincent Ngundi, Director of Cyber Security and Head of the National KE-CIRT/CC. In his speech, the DG/CEO stressed the importance of empowering the youth with critical thinking skills and digital responsibility, noting that 75 per cent of Kenya's population is under 35, according to the 2019 census. "The youth are not just the future, they are the present. We must empower them to make informed digital decisions today," he reiterated.

The DG/CEO also highlighted existing initiatives including the annual Cybersecurity Bootcamps and Hackathons, the October Cybersecurity Awareness Month (OCSAM) series and the annual Africa Public Key Infrastructure Forum (PKI) Forum, as key pillars in building digital resilience. Additionally, the DG/CEO reaffirmed the Authority's commitment to advancing digital trust through progressive policy and regulatory mechanisms, targeted capacity building and public awareness campaigns, investment in research and innovation and enhanced international cooperation and collaboration.

2025 Cybersecurity Youth Forum... cont'd

Overall, the forum emphasised the urgency of equipping youth with cybersecurity knowledge, recognising Kenya's young population as a vital force in combating online threats. Speakers highlighted the dangers of misinformation, ethical concerns around AI use and the importance of mentorship in steering young talent toward innovative ideas. Interactive sessions provided practical tools for verifying online content, while panel discussions highlighting the need for responsible digital behaviour, stronger regulation and cross-sector collaboration.

The event strengthened dialogue between youth and decision-makers, raised awareness of digital risks, and mobilised young people as champions of truth, ethics and innovation in the digital space. It concluded with a reaffirmed commitment to secure Kenya's digital ecosystem through continued youth engagement, partnerships and empowerment. Key resolutions included institutionalizing the forum as an annual event, expanding digital literacy efforts, promoting responsible AI adoption and increasing public awareness around content verification and domain authenticity.

Moments captured during the inaugural 2025 Cybersecurity Youth Forum that was held on 11th September, 2025, in Nairobi.

Cybersecurity Bootcamp for Professionals

The Authority, in collaboration with Huawei Technologies Kenya, conducted a two-week Cybersecurity Bootcamp for Professionals from 28th July to 8th August, 2025, in Nairobi. This training programme reinforces the Authority's commitment to strengthening national cybersecurity resilience, enhancing incident response capabilities, promoting collaboration among critical information infrastructure organisations and developing local cybersecurity expertise to address new and emerging cyber threats. The programme also aligns with the Authority's 2023–2027 Strategic Plan, which aims to empower and protect consumers of ICT services while advancing Kenya's digital transformation and regulatory compliance.

The bootcamp brought together 52 technical officers from the Authority's National KE-CIRT/CC and from the Ministry of Information, Communications and The Digital Economy (MICDE). Participants undertook Huawei's HCIP-Security V4 curriculum, covering firewall policy design and hardening, site-to-site and remote-access VPNs, intrusion prevention and DDoS mitigation, penetration-testing workflows, content/URL filtering, network access control with identity-based policies and end-to-end enterprise security deployment.

The programme combined instructor-led theory with extensive hands-on labs, building and tuning policies, configuring VPNs, analysing logs in simulated attack traffic and troubleshooting real-world fault scenarios, to enable participants to translate concepts into operational skills. Scenario-based exercises and tabletop exercises (TTXs) were aimed at enhancing incident-response fundamentals (detect, contain, eradicate, recover) and emphasised secure configuration, change control and documentation.

Participants concluded with practical artefacts, baseline configurations, hardening checklists and mini playbooks, ready to adapt within their respective environments.

Participants pictured during the Cybersecurity Bootcamp for Professionals that was held from 28th July to 8th August, 2025, in Nairobi.

Benchmarking Tour by the Communications Regulatory Authority of Namibia (CRAN)

The delegation from CRAN led by the Board Chaiperson, Mr. Jose Van Vyk (far right).

Ms. Stella Kipsaita (left) and Ms. Jane Kinyanjui from Corporate Communications, look on.

Mr. Francis Sitati (left) from Cyber Security, makes his presentation.

Ms. Banchale Gufu (right) from Cyber Security, engages Mr. Van Vyk.

The Communications Regulatory Authority of Namibia (CRAN) conducted a benchmarking tour to the Authority's National KE-CIRT/CC on 13th August 2025. The visit sought to get more insights into Kenya's National Public Key Infrastructure (NPKI) including the enabling policy, legal and regulatory frameworks that support digital trust services. The visit examined the role of the Root Certification Authority in relation to Certification Authorities and Registration Authorities, among other dependencies within the digital trust value chain.

The delegation was also briefed on the accreditation process for electronic certification service providers (E-CSPs), covering areas such as incident, security and risk management, personnel controls, business continuity planning (BCP), among other critical areas. Rounding out the programme, the delegation explored capacity building, public awareness, and other strategies to accelerate the adoption of electronic certification services. These included targeted outreach programmes for banking and finance, insurance, and the judicial and legislative sectors, among others.

Key takeaways from the tour are expected to inform CRAN's implementation roadmap for digital trust services, strengthen policy, legal and regulatory frameworks, and identify opportunities for continued cooperation between the two countries on areas of mutual interest. The visit also established mechanisms for continous information sharing, including expert exchanges and periodic progress reviews.

Study and Benchmarking Tour by the Insurance Regulatory Authority (IRA)

Part of the delegation from IRA led by Ms. Joan Kirika, Director, Internal Audit (far right).

Mr. Christopher Wambua, Director, Corporate Communications, engaging the delegates.

Mr. Francis Sitati (left) from Cyber Security, articulates a point.

Mr. Mark Kilonzo (right) from Cyber Security, making his presentation.

The Insurance Regulatory Authority (IRA) conducted a study and benchmarking tour to the Authority's National Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC), as part of its ongoing efforts to strengthen cybersecurity oversight within the insurance sector. The engagement, which took part on on 23rd July 2025, familiarised the insurance sector regulator with the governance frameworks, operational processes and tools required to establish and operate a Cyber Security Operations Centre (CSOC). The scope of the engagement included incident detection and response workflows, threat-intelligence integration and reporting practices.

This strategic initiative aligns with the designation of the National KE-CIRT/CC as the CSOC for the ICT and Telcoms sector, pursuant to the Computer Misuse and Cybercrimes Act, 2018. Similarly, the IRA is mandated to establish a sectoral CSOC to safeguard systems that support the provision of insurance services in Kenya. Alongside its engagement with the IRA, the Authority collaborates with other sectoral SOCs across critical domains such as the Central Bank of Kenya (CBK), the ICT Authority (ICTA), the Sacco Societies Regulatory Authority (SASRA), and the Kenya Civil Aviation Authority (KCAA), among others.

Bilateral Exchange on Cybersecurity Best Practices with Malawi Computer Emergency Response Team (mwCERT)

On 3rd September 2025, the Authority's National KE-CIRT/CC, with facilitation by the Forum of Incident Response and Security Teams (FIRST), hosted the Malawi Computer Emergency Response Team (mwCERT) to a virtual, bilateral knowledge-sharing session.

Discussions were centred around practical experiences in responding to major cyber threats such as distributed denial-of-service (DDoS) and ransomware attacks. The session highlighted best practices and lessons learned towards strengthening mwCERT's crisis readiness and explored opportunities for collaboration during periods of heightened cybersecurity risk.

The Authority welcomed the engagement as timely and strategic, observing that it will advance cyber resilience, promote structured threat intelligence sharing and enhance capacity for coordinated incident response.

The Authority also appreciated the recognition of its regional leadership, through FIRST, and affirmed its commitment to continued collaboration through sharing practical experiences, exchanging lessons learned and identifying further areas for collaboration.

Inaugural Webinar on Data Privacy and Cybersecurity Awareness

Official promotional poster for the inaugural Data Privacy and Cybersecurity Awareness webinar, conducted on 25th September 2025.

On 25th September 2025, the Authority through the National KE-CIRT/CC, participated in the Inaugural Webinar on Data Privacy and Cybersecurity Awareness, convened by the University of Nairobi (UoN). The Authority was represented at the forum by Mr. Dennis Loyatum.

The session brought together diverse stakeholders, including the Office of the Data Protection Commissioner (ODPC) and the County Government of Kisumu, to discuss emerging cyber threats, compliance requirements and practical approaches to enhancing cyber safety and security in an increasingly digital economy.

Continuous data privacy and cybersecurity awareness programmes are central to the Authority's role and mandate, as they could result in improved national cyber hygiene, timely incident reporting and enhanced threat intelligence sharing.

52nd Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

Proceedings during the 52nd meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC) that was held on 18th August 2025, in Nairobi.

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

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

During the meeting, members deliberated on establishing a national, publicly accessible repository of malicious domains to enhance threat intelligence and user protection. The National KE-CIRT/CC welcomed the proposal and suggested partnering with the .KE country code top-level domain (ccTLD) registry. Through this collaboration, stakeholders will oversee the onboarding and publication of reported malicious .KE domains, maintaining a centrally managed list with comprehensive validation processes, takedown and appeals mechanisms, and strict adherence to relevant legal and privacy regulations.

Members also highlighted limited capacity within civil society organisations to respond effectively to cyber incidents and to utilise cyber threat intelligence. Suggestions focused on making threat intelligence more accessible and relevant to such groups, while improving public engagement and trust.

In conclusion, members deliberated and agreed on the need to strengthen Operational Technology (OT) capacity and emphasised that training and collaboration opportunities, within the framework of the NKCC, should be actively considered and pursued. The 52nd meeting of the NKCC was held on 18th August 2025, in Nairobi.

Outlook for the Next Quarter

In collaboration with UK's Foreign, Commonwealth & Development Office (FCDO) and the Forum of Incident Response and Security Teams (FIRST), the Authority will host the 2025 Annual Cyber Security Conference & Forum of Incident Response and Security Teams (FIRST) Technical Colloqiuim on 17th October, 2025. As part of the pre-conference agenda, the Authority will also be hosting a training programme on Mastering Proactive Cyber Defence and Threat Analysis & Tabletop Exercise (TTX) from 13th to 16th October, 2025 in Nairobi. The event aims to promote multi-stakeholder cooperation to strengthen Kenya's collective capacity and capability to prevent, detect and respond to cyber threats.

This year's event target audience includes operators of critical information infrastructure, Chief Executive Officers (CEOs), Chief Information Security Officers (CISOs), academia, legal and compliance practitioners, technology vendors, government regulators, start-ups and innovators, the civil society, county governments, cybersecurity associations, students and the general public.

Separately, the Authority, together with the National Computer and Cybercrimes Coordination Committee (NC4) and other strategic partners, will participate in the 3rd African Forum on Cybercrime, that is scheduled for 25th to 27th November, 2025 in Nairobi. The forum provides a platform to exchange knowledge and advance more effective domestic, regional and international justice responses to cybercrime and electronic evidence. The Council of Europe (CoE) has conferred on the Republic of Kenya the honour of serving as host for this year's event.

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