COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

38th Edition

April - June 2025

A report by:

The National KE-CIRT/CC

☎ +254-703-042700 or
+254-730-172700

✉ incidents@ke-cirt.go.ke

🌐 www.ke-cirt.go.ke

Strategic Direction

Our Vision

Digital Access for All

Our Mission

Enabling a Sustainable Digital Society through Responsive Regulation

Our Core Values

Integrity, Innovation, Excellence, Inclusion, Agility.

Cybersecurity Mandate

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

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

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

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

Director General's Perspective

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

The Authority continued to observe a notable increase in cyber threat activity with the most prevalent threat vectors including ransomware attacks, data breaches, Distributed Denial-of-Service (DDoS) campaigns and social engineering techniques such as phishing and vishing (voice phishing). These trends are consistent with the global threat landscape, illustrating the need for continuous vigilance, enhanced cyber resilience measures and stakeholder collaboration to mitigate potential risks.

Ransomware remained the dominant threat vector globally, with coordinated attacks increasingly targeting both public and private sector entities. Critical sectors such as healthcare, point-of-sale systems and critical information infrastructure experienced significant disruptions. At the same time, data breaches continued to pose a serious and persistent risk, resulting in the compromise of sensitive personal, financial and institutional data, raising serious concerns around data privacy, operational resilience and compliance to regulatory frameworks.

The Authority observed that DDoS attacks surged significantly, with politically motivated hacktivist groups launching large-scale disruptions in the wake of the recent global geopolitical tensions. Social engineering tactics continue to become more sophisticated, with attackers increasingly impersonating technical support personnel and exploiting human trust to gain unauthorised access to diverse systems.

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 threat environment.

Over the period April - June 2025, the National KE-CIRT/CC detected over 4.5 billion cyber threat events which represented an increase of over 80% from the previous period, January - March 2025. In response to these cyber threat events detected, the National KE-CIRT/CC issued over 17 million cyber threat advisories between the period April - June 2025. This represented an increase of about 30% compared to the previous period, January - March 2025.

During the period under review, the majority of cyber threat advisories centred on the critical importance of maintaining up-to-date software through timely patching, enforcing strong password protocols through mechanisms such as multi-factor authentication and deploying secured network firewalls. These priority areas were highlighted as fundamental to strengthening organisational cybersecurity posture in view of the increasingly sophisticated threat landscape.

The prevailing global trends can be largely attributed to the continued proliferation of Internet of Things (IoT) devices, many of which are deployed without adequate security controls. In addition, the sustained exploitation of botnets and Distributed Denial-of-Service (DDoS) techniques continues to shape the global cyber threat landscape. Due to their decentralised nature, botnets remain a tool of choice for threat actors, facilitating highly effective, large-scale and coordinated cyber attacks.

In alignment with the 2023–2027 Strategic Plan, the Authority remains steadfast in its efforts to advance cyber safety and security through the promotion of industry best practices, enhancement of threat detection and response capabilities, and continued public awareness and capacity building initiatives in collaboration with key sector stakeholders. These efforts are intended to empower stakeholders across the cybersecurity value chain with the requisite tools, perspectives and capabilities to proactively manage and respond to the continually evolving cyber threat landscape.

Mr. David Mugonyi, EBS
Director General/CEO

Cyber Threat Landscape Overview

Global Cyber Threat Landscape Overview

1. Ransomware

Ransomware remained a highly leveraged attack vector against local and international manufacturing, healthcare, telecoms and finance sectors. Domestic and international groups including LockBit and Cl0p exploited outdated software and used advanced extortion tactics.

The National KE-CIRT/CC issued advisories to organisations providing prevention guidance such as implementing offline backups, network segmentation, prompt patching and implementing Multi Factor Authentication (MFA) to reduce this impact.

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

The frequency and intensity of DDoS attacks remained prevalent, often leveraging large botnets and infecting IoT devices. Attackers rented DDoS-as-a-Service (DaaS), executed protocol amplification assaults to unauthorisedly access systems through Common UNIX Printing System (CUPS) and Network Time Protocol (NTP) and leveraged botnets of consumer devices for purposes of compromising critical infrastructure such as government systems and telecommunication services.

The National KE-CIRT/CC issued advisories to organisations to scale up security mitigations with AI-powered DDoS protection, cloud-based scrubbing, traffic filtering, disabling vulnerable services and using firewall rules.

3. Social Engineering & Phishing

Social engineering attacks, including phishing, vishing, smishing and AI-generated deepfake scams, intensified globally and within Kenya. Cybercriminals used AI-generated emails and voice impersonations of executives to facilitate fraud and Business Email Compromise (BEC). Phishing kits were also adapted for emerging African brands and services.

In response to this, the National KE-CIRT/CC promoted widespread adoption of phishing-resistant authentication such as passkeys and biometrics, increased security awareness training focused on voice deepfakes and distributed technical advisories to organisations.

Global Cyber Threat Landscape Overview

4. *System Misconfiguration Exploits*

Misconfigured servers, cloud environments, outdated software, weak access controls and default credentials continued to drive breaches. Attackers exploited unpatched services such as OpenSSH, Windows Remote Desktop Protocol (RDP) and cloud platforms to gain unauthorised access in both private enterprises and public bodies.

The National KE-CIRT/CC issued advisories recommending security audits, prompt patching, disabling default setups, and enforcing Zero-Trust architectures in organisations.

5. *Emerging Threats*

Nation-state and AI-powered cyber attacks grew more sophisticated, with IoT devices increasingly targeted. State-sponsored espionage campaigns and AI-enhanced malware were increasingly aimed at government, telecom and financial sectors. Poorly secured IoT devices were also leveraged for reconnaissance and botnet activity.

The National KE-CIRT/CC issued advisories to organisations recommending the deployment of AI-driven threat detection systems, enforcement of cybersecurity regulations and engaging in collaborative efforts to help mitigate these threats.

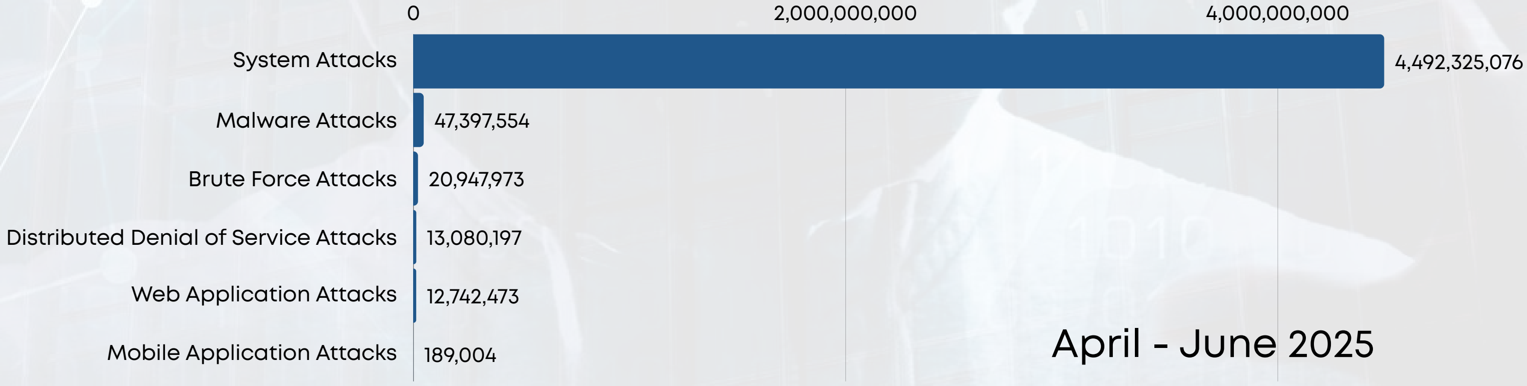
Cyber Threat Landscape Roundup

Total Cyber Threats Detected

4,586,682,277 | **80.70%**

The National KE-CIRT/CC detected over **4.5 billion** cyber threat events during the three-month period between **April - June 2025**, which represented an **80.70% increase** from the threat events detected in the previous period, January - March 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 sharp rise in 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.

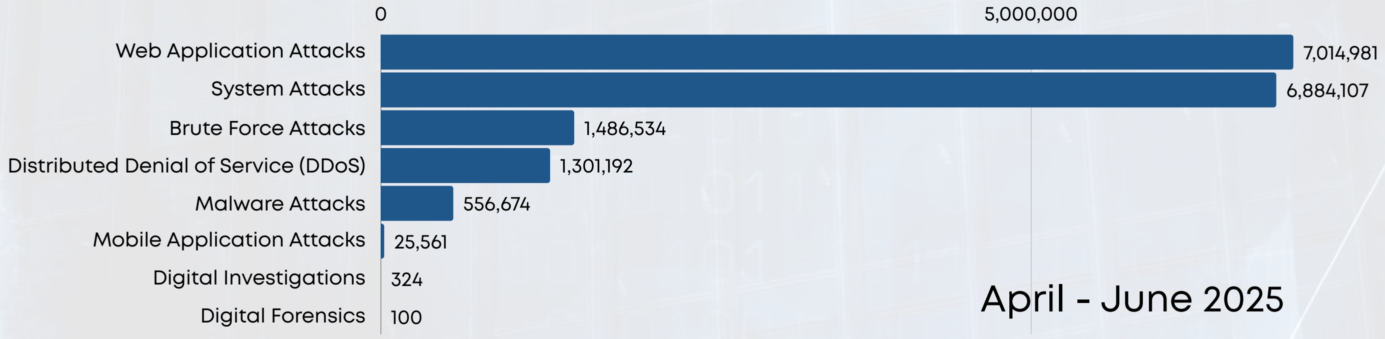


Total Cyber Threat Advisories Issued

17,269,473 | **30.55%**

The National KE-CIRT/CC issued **17,269,473** advisories between the period **April - June 2025**, which represented a **30.55%** increase compared to the advisories that were issued during the previous period, January - March 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, implementing multi-factor authentication and strong password policies, hardening firewalls and antivirus software and maintaining up-to-date system software to mitigate emerging cyber threats.

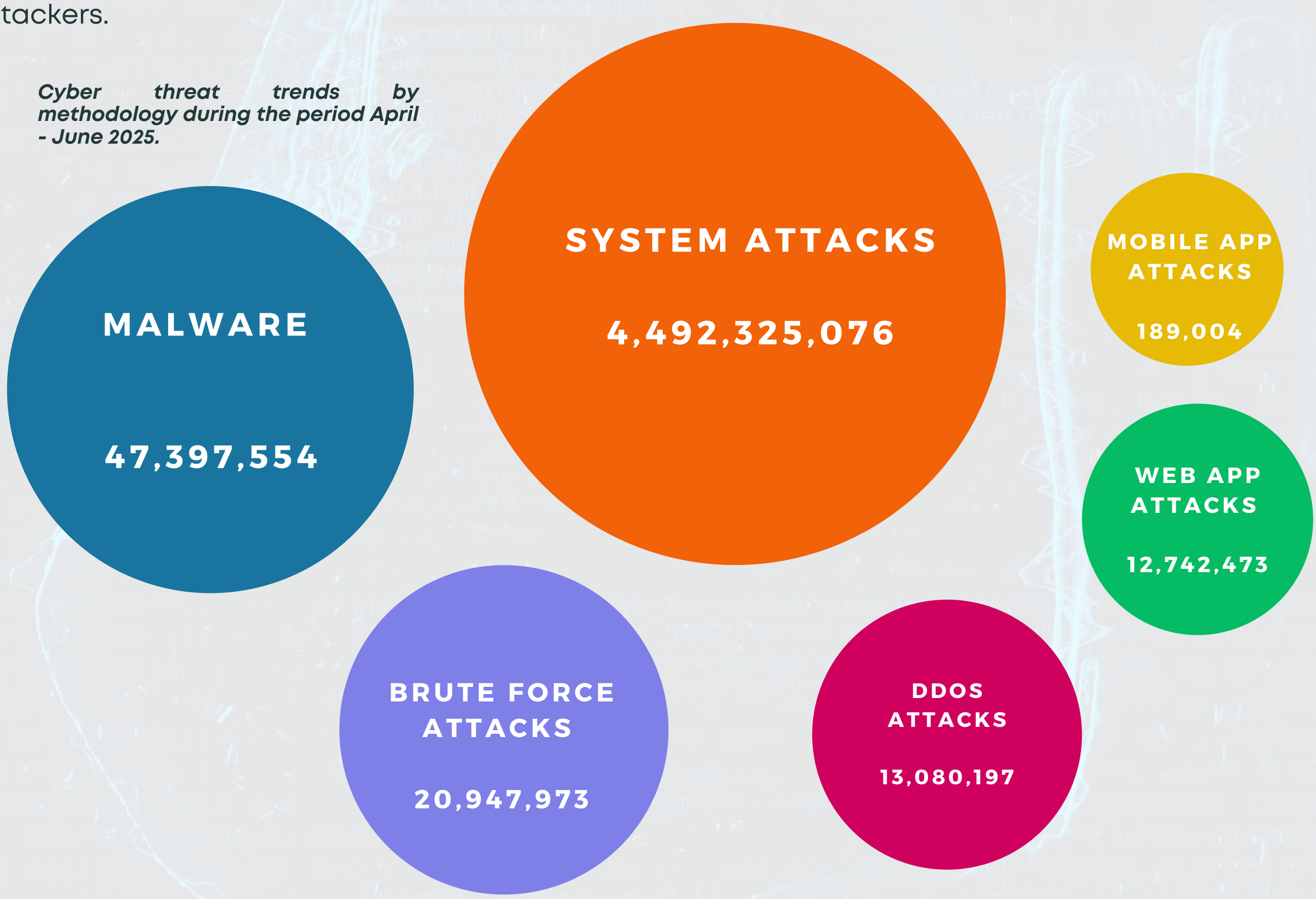


Cyber Attack Vector Trends

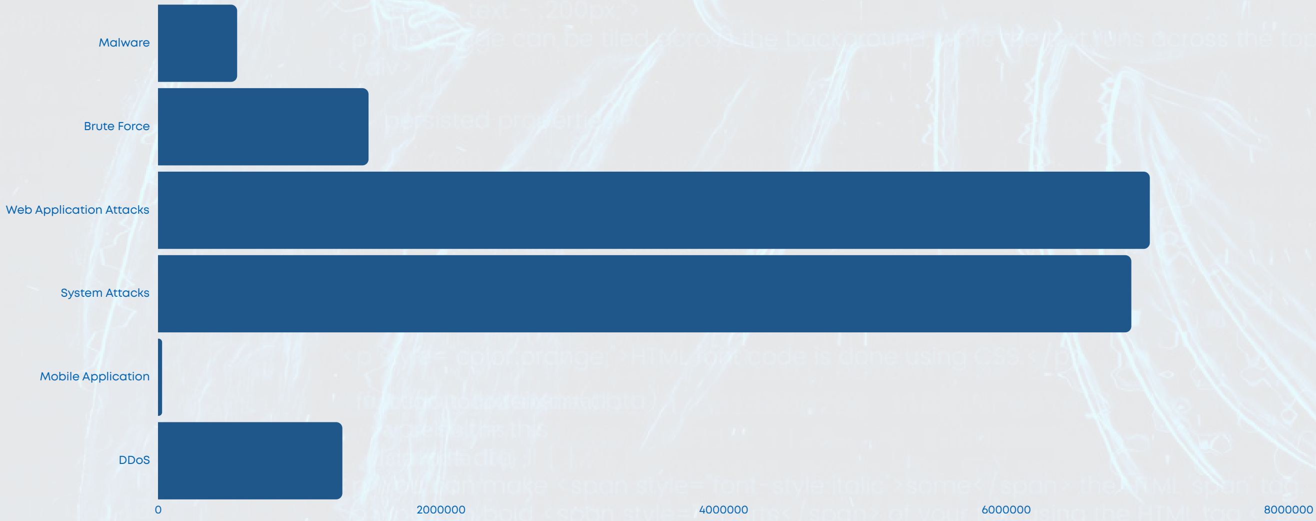
During the period under review, system vulnerabilities and malware attacks emerged as the most prevalent threat vectors, consistent with global cyber threat trends. Key contributing factors to misconfiguration-related incidents included inadequate cyber risk awareness, reliance on outdated systems, use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

On the other hand, malware attacks may be attributed to exploitation of unpatched vulnerabilities, increased social engineering and phishing attacks, cybercrime monetisation models such as infostealers and cryptojackers, and the widespread use of AI and automation by attackers.

Cyber threat trends by methodology during the period April - June 2025.



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



Malware Trends

Threats Detected

47,397,554

93.07%

Advisories Issued

556,674

29.77%

During the three-month period between **April - June 2025,** the National KE-CIRT/CC detected **47,397,554** malware threat attempts targeted at the critical information infrastructure sector. This represented a **93.07%** increase from the previous period, January - March 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 academic organisations.

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

- **Android Vo1d2 (Root-level backdoor via supply chain tampering): Installs persistent malware on uncertified Android TV boxes, turning them into proxy nodes for ad fraud and illicit traffic. Gains root by replacing system binaries and communicates with C2 servers using encryption.**
- **Play Ransomware – Windows CLFS Vulnerability (CVE-2025-29824): This vulnerability in the Windows Common Log File System allows attackers to escalate privileges to SYSTEM level, enabling them to deploy ransomware payloads with full system control.**

Malware attacks predominantly 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

12,742,473

150.78%

Advisories Issued

7,014,981

59.33%

The National KE-CIRT/CC detected **12,742,473** web application attack attempts targeted at the critical information infrastructure sector, during the three-month period between **April - June 2025**, This represented a **150.78%** increase from the previous period, January - March 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

- **OttoKit WordPress Plugin (CVE-2025-27007):This vulnerability allows unauthenticated attackers to elevate privileges by exploiting insecure authorization, enabling creation of admin users on WordPress sites.**
- **SAP NetWeaver (CVE-2025-31324): This vulnerability allows unauthenticated users to upload malicious JSP files, enabling remote shell access and malware deployment on SAP web servers.**
- **Apache Tomcat (CVE-2025-24813):This vulnerability allows path traversal through crafted URLs, leading to unauthenticated remote code execution on Apache Tomcat instances.**

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

20,947,973

38.01%

Advisories Issued

1,486,534

10.12%

The National KE-CIRT/CC detected **20,947,973** brute force attack attempts majorly targeting the critical information infrastructure sector during the three-month period from **April - June 2025**. This represented a **38.01%** decrease from the previous period, January - March 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) settings, 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

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

Over the three-month period, brute force attacks predominantly 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

189,004

177.69%

Advisories Issued

25,561

93.07%

The National KE-CIRT/CC detected **189,004** mobile application attack attempts targeting end-user devices, during the three-month period from **April - June 2025**. This represented a **177.69%** increase from the previous period, January - March 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, authentication 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

13,080,197

255.56%

Advisories Issued

1,301,192

67.51%

The National KE-CIRT/CC detected **13,080,197** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure during the three-month period, **April - June 2025**. This represented a **255.56%** increase from the previous period, January - March 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

- Adyen Payment Platform (April 2025): This attack exploited insufficient rate-limiting on payment APIs, overwhelming backend infrastructure and causing widespread transaction failures.
- Internet Archive (April–May 2025): This attack leveraged botnets to flood archive.org with HTTP requests, exploiting its open archival endpoints to exhaust bandwidth and server resources.

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

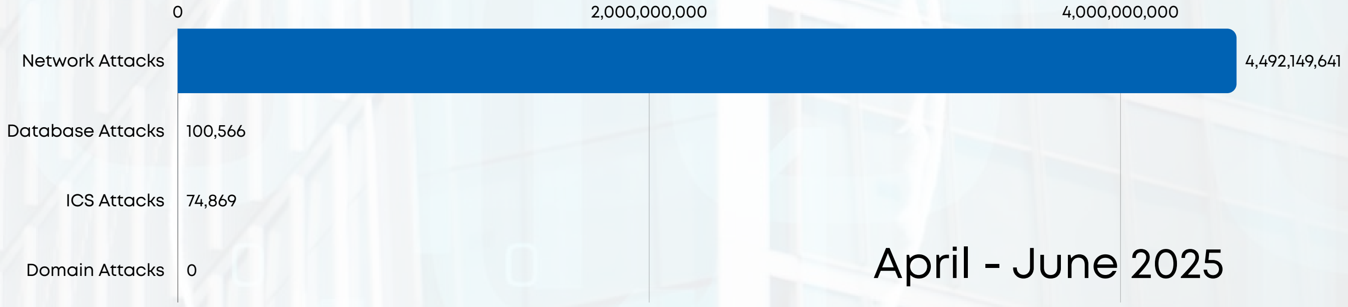
4,492,325,076

81.86%

Advisories Issued

6,884,107

16.66%



April - June 2025

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

Enhancing Kenya's Digital Transformation: Highlights from the 2025 Digital Trust Forum

A section of the panelists is pictured posing for a group photo during the 2025 Digital Trust Forum held on 1st April 2025, in Nairobi.

On 1st April 2025, the Authority in collaboration with Evrotrust Technologies AD, hosted the Digital Trust Forum 2025 in Nairobi. This event marked a key milestone in advancing the adoption of trusted digital services in Kenya. Bringing together policymakers, business leaders, fintech innovators, journalists and technology enthusiasts, the forum outlined the country's readiness to embrace advanced digital trust solutions that align with global security standards. The Authority was represented at the forum by Mr. Dennis Loyatum.

The five pillars of digital trust formed the central theme of the forum, with each pillar addressing a key component in the development of a secure and reliable digital ecosystem. *e-Identification* was presented as a means of enabling secure, remote verification for both individuals and businesses, thereby eliminating the need for physical presence. *e-Signatures* were highlighted for their ability to provide legally binding digital authentication, streamlining processes and significantly reducing reliance on paper-based transactions.

The role of *e-Seals* was emphasised in preserving the authenticity and integrity of documents, ensuring that organisations can maintain accountability and trust in their communications. *e-Timestamps* were recognised for their value in certifying the precise timing of digital actions, contributing to transparency and traceability across systems.

Finally, *e-Delivery* was showcased as a secure and legally recognised method for the electronic transmission of documents, offering verifiable proof of receipt and content integrity. Together, these services constitute a comprehensive foundation for building confidence in digital services and digital transactions.

The forum showcased how these widely adopted European digital trust services can be effectively integrated into Kenya's digital ecosystem, aligning with the government's agenda to digitise and build trust and confidence in digital services. By enhancing the security and efficiency of business processes, these innovations have the potential to reduce operational costs, streamline service delivery and enable seamless cross-border digital trade, thus eliminating the inefficiencies associated with traditional paper-based systems.

The Cyber Carnival 2025

The Authority alongside members of the National KE-CIRT/CC Cybersecurity Committee (NKCC) participated in the *Cyber Carnival 2025*, held from 11th – 13th June 2025, in Nairobi, under the banner of the *Africa Cyber Defense Forum*. The event convened cybersecurity professionals, the youth, regulators and community leaders across Africa, with a focus on threat intelligence, policy dialogue and hands-on skills development. This event aligned with the Authority's 2023 – 2027 Strategic Plan, particularly in the areas of stakeholder engagement, cybersecurity awareness and youth capacity building.

The three-day cybersecurity carnival focused on three key thematic areas. The first theme, *Threat Intelligence and Regional Resilience*, featured live demonstrations by various vendors showcasing real-time perspectives into cybersecurity trends such as ransomware campaigns, cyber espionage and infrastructure vulnerabilities both within the country and globally. These sessions outlined the critical need for enhanced cross-border intelligence sharing and the establishment of collaborative Computer Emergency Response Team (CERT) mechanisms to strengthen regional preparedness and response to emerging threats.

Discussions were centred around leveraging advanced threat intelligence platforms and promoting public-private partnerships to ensure a coordinated, proactive approach to cyber risk management. The discussions also highlighted the growing importance of regional cyber diplomacy in addressing cross-border cyber threats.

Secondly, the *Cyberlympics Qualification Rounds* provided an interactive platform for youth and university teams to participate in Capture-the-Flag (CTF) competitions, assessing their hands-on expertise in ethical hacking, malware analysis and cryptanalysis. This initiative supports the Authority's broader strategic goal of cultivating a strong national cybersecurity talent pipeline through practical, skills-based engagement. By nurturing early interest and technical proficiency among young professionals, the competition also contributes to bridging the cybersecurity skills gap in the region and enhancing national resilience against evolving digital threats.

Lastly, the carnival facilitated *Policy and Industry Collaboration* through stakeholder engagements with mobile network operators, financial institutions and academia. These discussions reaffirmed the Authority's commitment to nurturing a secure and innovation regulatory environment that balances technological advancement with cyber readiness and resilience. The sessions provided a platform for sharing best practices, aligning regulatory priorities and identifying areas for public-private collaboration.

Speakers emphasised the need for adaptive policy frameworks to accommodate emerging and new technologies while safeguarding digital trust. Participants also highlighted the value of continuous dialogue between regulators and industry players to promote responsive and inclusive cybersecurity governance frameworks.

The *Cyber Carnival 2025* reaffirmed the Authority's role in advancing a more resilient and secure digital ecosystem, strengthening national cybersecurity skills capacities, promoting multi-stakeholder cooperation and advocating for socially responsible and ethical engagements online. It provided a platform for key industry actors to align on emerging regulatory priorities and share practical experiences in safeguarding digital infrastructure. The event further facilitated the sharing of innovative strategies and best practices focused on enhancing national cyber capabilities. These engagements demonstrate the Authority's dedication to a knowledge-based, inclusive model of cybersecurity governance.

The Cyber Carnival 2025... cont'd

Highlights from the Cyber Carnival 2025, where participants engaged in a series of enlightening presentations and live demonstrations centred around emerging cyber threats, modern cyber defence strategies and proactive intelligence solutions. The event was held from 11th - 13th June, 2025 in Nairobi.

International Girls in ICT Day

The International Girls in ICT Day, which was commemorated on 24th April 2025 this year, is a global initiative that aims to inspire and empower girls and young women to pursue careers in ICT. The day emphasises the importance of gender inclusion in the digital economy and serves as a platform to promote equal access to opportunities in the technology sector. As digital transformation continues to redefine Kenya's socio-economic landscape, empowering girls and women with ICT skills is critical to nurturing innovation, bridging the digital divide and advancing a more inclusive and equitable digital economy.

The 2025 commemoration featured a wide range of activities globally, including coding workshops, mentorship forums, innovation challenges and interactive sessions with women professionals in the ICT sector. These initiatives aim to build confidence, enhance digital literacy and expose young women to the vast career pathways available in technology and innovation. In Kenya, a collaborative effort by government, academic institutions, private sector stakeholders and civil society organisations was undertaken to advance these initiatives and ensure broad, meaningful participation.

During this year's commemoration, the Authority was honoured by the British High Commission in Nairobi in recognition of Ms. Donna Owiti's outstanding contribution to the UK-funded UN Women in Cybersecurity and Cyberspace Fellowship Programme. Ms. Owiti, who serves within the Cybersecurity Department that also hosts the National KE-CIRT/CC, was celebrated for her dedication and impact in advancing cyber diplomacy and inclusion. This recognition highlights the Authority's ongoing commitment to promoting gender equity and empowering women in the cybersecurity and digital policy arena.

The Fellowship was created to improve the representation of women in UN negotiations on cyberspace. It has supported women diplomats and public officials involved in cyber policy, enabling active participation in the UN Ad Hoc Committee on cybercrime. This effort led to the adoption of the UN Cybercrime Convention on 24th December 2024, the first binding global treaty on cybercrime. The Convention is set for ratification on 25th October 2025 in Hanoi, Vietnam. It is expected to strengthen international cooperation and legal frameworks to combat cybercrime.

Ms. Donna Owiti (left) pictured alongside Her Excellency Leigh Stubblefield, Deputy High Commissioner at the British High Commission on 24th April, 2025 in Nairobi.

Huduma Contact and Tele-Counselling Centre Staff Sensitization on Services Offered by MDAs

Participants pose for a group photo during the two-day sensitization exercise held for staff at the Huduma Contact and Tele-Counselling Centre (HCTC) that was held from 16th - 17th June, 2025 in Nairobi.

The Authority convened a two-day sensitisation exercise for staff of the Huduma Contact and Tele-Counselling Centre (HCTC), held from 16th - 17th June 2025, in Nairobi. The initiative was designed to enhance staff capacity in addressing citizen inquiries on government services, in alignment with the Authority's 2023–2027 Strategic Plan objective of empowering and protecting ICT service consumers. The forum featured representatives from various Ministries, Departments and Agencies (MDAs), who provided perspectives into their respective mandates and service delivery frameworks. The National KE-CIRT/CC was represented at the forum by Ms. Cynthia Chebet.

During the session, several key regulatory and consumer protection areas were addressed. On broadcasting regulations, participants received clarification on the Authority's role in licensing and content oversight, particularly in handling public complaints related to media ethics, misinformation and compliance with broadcasting codes. In the area of telecommunications services, staff from the HCTC were guided through common public concerns such as mobile network quality, SIM registration procedures, service outages and available mechanisms for consumer redress. The discussion on postal and courier services focused on creating awareness of licensed service providers, consumer rights and the complaint escalation processes in accordance with established service standards.

Cybersecurity awareness and protection were key focus areas during the engagement, outlining the increasing importance of safeguarding our data and digital infrastructure. Participants received comprehensive perspectives into emerging threats such as phishing, SIM swap fraud, social engineering and the spread of digital misinformation. The Authority highlighted the critical role of good cyber hygiene practices, including the use of multi-factor authentication, regular software updates and staying vigilant while using online platforms. The need for timely reporting of cyber incidents was also emphasised to enable effective response and containment.

Additionally, the Authority reaffirmed the critical support offered through the National KE-CIRT/CC, encompassing advisory services, public awareness initiatives and incident response coordination. This reaffirms the Authority's commitment to building a secure, resilient and digitally aware cybersecurity landscape across the country.

51st Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

Proceedings during the 51st meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC) that was held on 25th June 2025, in Nairobi.

The National KE-CIRT/CC Cybersecurity Committee (NKCC) draws its membership from over 50 public and private sector organisations from the critical information infrastructure (CII) sector in the country. The main objective of the NKCC is to nurture trust networks amongst stakeholders, so as to build capacity and facilitate the sharing of information on new and emerging cybersecurity trends, and to identify a collective strategy to address these emerging issues. The NKCC holds quarterly meetings during which the National KE-CIRT/CC provides updates on emerging threats, tactics, techniques and procedures (TTPs) utilised by diverse threat actors. During these meetings, the various sectoral Computer Incident Response Teams (CIRTs) apprise members on the trends and patterns observed within their respective domains.

During the meeting, it was agreed that cybersecurity remains a key element in the ongoing digitilisation of government services. To ensure the secure delivery of digital platforms, the government has implemented comprehensive security mechanisms including Internet gateway firewalls at strategic entry points, regular vulnerability assessments and robust email security gateways, among others.

The public utilities sector reported a rise in cyberattacks on IT systems and raised concerns about potential threats to critical Operational Technology (OT) infrastructure. Members called for greater collaboration in developing OT-specific incident response plans. They also noted increasing identity theft, phishing attacks and accidental exposure of authentication keys, all posing risks to secure service delivery.

Members were briefed on the growing cyber threats facing government systems, including AI-driven intrusions and phishing campaigns targeting public sector staff. The rising demand for solutions like IDS/IPS and Zero Trust Architecture was highlighted. Notably, increased collaboration between the private sector and government on threat intelligence sharing is significantly strengthening national cybersecurity preparedness. The 51st Meeting of the NKCC was held on 25th June 2025, in Nairobi.

Future Insights on Cybersecurity

The Authority, in collaboration with the Ministry of Information, Communications and The Digital Economy, is scheduled to host a cybersecurity bootcamp targeting professionals from both the public and private sectors. This initiative aims to build capacity among cybersecurity personnel by enhancing both their technical and strategic skills in dealing with evolving cyber threats. The bootcamp will equip participants with hands-on skills and knowledge in critical areas such as network security, digital forensics, cyber threat intelligence, incident response and secure systems design.

In collaboration with the UK's Foreign, Commonwealth & Development Office (FCDO), the Authority is scheduled to host an integrated cyber crisis simulation exercise. This initiative is intended to assess the capacity of institutions to effectively manage complex cyber incidents. By simulating real-world attack scenarios, the exercise will provide an opportunity to evaluate crisis response strategies, improve coordination and communication mechanisms, and strengthen institutional readiness under high-pressure conditions.

In addition, the exercise will include tailored penetration testing and vulnerability assessment exercises. These activities will assist participants to identify weaknesses within their digital infrastructure and learn best practices for mitigating potential risks. The collaboration highlights the importance of strengthening Kenya's cybersecurity posture through proactive testing, strategic partnerships and continuous professional development.

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
X ◎ in f @KeCIRT

Download the KE-CIRT App
▷ *PlayStore* *AppStore*