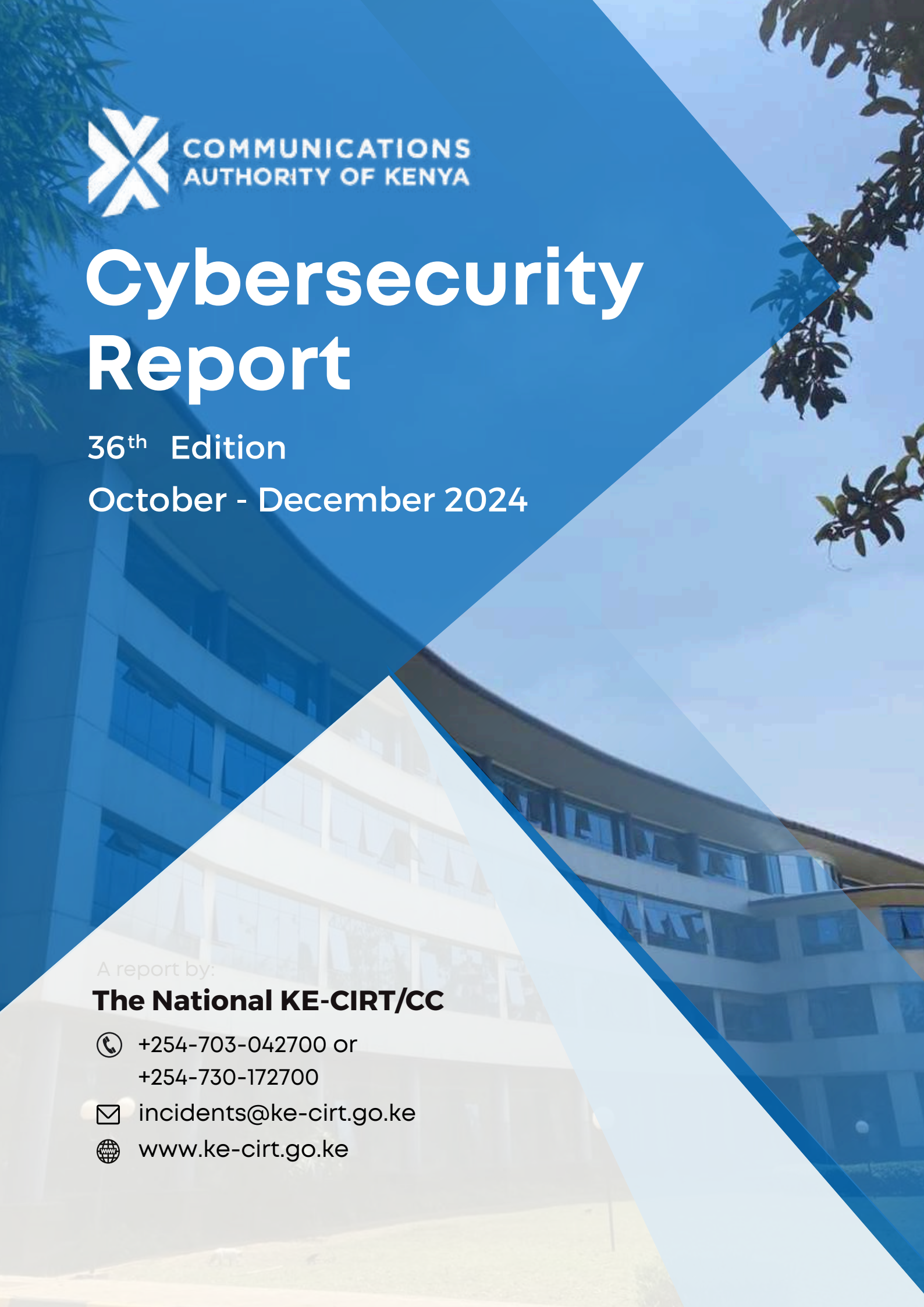
COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

36th Edition

October - December 2024



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)

As we draw towards the close of the year, we observed that ransomware, Distributed Denial-of-Service (DDoS), and social engineering attacks including phishing, continued to evolve and have remained pervasive on the global cyber threat landscape. Ransomware attacks continued to target critical information infrastructure including ICT and telecommunications, banking & finance, health, manufacturing, among other sectors. Cybercriminals continue to deploy sophisticated techniques aimed at disrupting critical systems by encrypting data while demanding exorbitant sums of money.

The Authority continued to witness growth in the magnitude and complexity of DDoS attacks with threat actors leveraging botnets and exploiting vulnerabilities in connected devices such as smartphones and other household appliances to disrupt online services and other critical operations. Social engineering remains a significant threat vector, with cybercriminals employing tactics such as impersonation and pretexting, to manipulate individuals into disclosing sensitive information or to gain unauthorised access to information systems.

Phishing attacks, enhanced by the use of artificial intelligence (AI) and automation, have become more targeted and convincing, in exploiting human vulnerabilities to steal account credentials, sensitive financial information and other critical information.

Over the period October - December 2024, the National KE-CIRT/CC detected over 840 million cyber threat events whereby most of these attacks exploited system vulnerabilities. In response to the detected cyber threat events, the National KE-CIRT/CC issued over 11.5 million advisories between the period October - December 2024, which represented a 20.90% increase compared to the advisories that were issued during the previous period, July - September 2024.

This trend continued to be attributed to the proliferation of Internet of Things (IoT) devices which are inherently insecure, the continued adoption of botnets and other Distributed Denial of Service (DDoS) attack techniques, and also the continued adoption of AI-enabled attacks by threat actors. Botnets continue to be used for malicious purposes and their distributed nature makes them a powerful tool for threat actors, especially when conducting large-scale operations. DDoS attacks can disrupt critical services, cause financial losses and reputational damage to organisations. AI-enabled cyber threats leverage artificial intelligence technologies to enhance the sophistication, magnitude, and effectiveness of cyberattacks. Threat actors continued to utilise AI technologies to automate and refine attacks, making them more adaptive and difficult to detect.

Going into 2025, the Authority will continue to focus on key thematic areas that are poised to continue dominating the cyber threat landscape and will require proactivity and possible regulatory interventions. Artificial Intelligence (AI) will remain at the forefront, with its dual-use nature presenting both great opportunities and serious challenges. Quantum computing cryptography remains a significant area of concern, as advancements in quantum computing continue to pose a challenge to traditional encryption methods. Supply chain and third-party application security also remains a critical area of focus as organisations increasingly rely on third-party vendors and service providers to support their operations.

In alignment with the Authority's 5th Strategic Plan (2023 - 2027), the Authority will continue to support the implementation of cybersecurity measures and best practices, enhance threat detection capabilities, and continue investing in awareness and education programmes to assist in navigating the ever-changing cyber threat landscape.

Mr. David Mugonyi, EBS
Director General/CEO

Cyber Threat Landscape Overview

Global Cyber Threat Landscape Overview

1. Ransomware

- New groups such as RansomHub, Sarcoma, and Interlock have emerged, showcasing evolving tactics. Sarcoma documented over 40 incidents in October 2024. The emergence of groups like Hellcat and PlayBoy Locker further underscores the dynamic nature of the ransomware landscape.
- The healthcare sector was particularly hard-hit, experiencing a staggering 95% increase in ransomware incidents, escalating from 20 to 39 cases in October alone. Other sectors like manufacturing and finance also faced significant threats, with manufacturing attacks rising by 37.9%.
- The average ransom demand reached unprecedented levels, with some reports indicating demands exceeding $5.2 million per incident. Many organisations faced repeated attacks shortly after paying ransoms, highlighting a troubling cycle of victimisation.
- Ransomware groups have increasingly adopted sophisticated data exfiltration methods, utilizing tools like Azure Storage Explorer to transfer large volumes of sensitive data to cloud storage before encryption. This trend emphasizes the dual threat of data theft and operational disruption.

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

- DDoS attacks continue to increase in frequency and intensity, with cybercriminals using more powerful botnets and leveraging Internet of Things (IoT) devices to amplify their attacks.
- There has been a rise in multi-vector DDoS attacks, which combine different attack techniques (e.g., volumetric, application-layer, and protocol-based attacks) to overwhelm targets.
- Reports from 2024 suggest that the number of DDoS attacks increased by around 20-30% compared to previous years, with a notable surge in attacks against critical infrastructure and financial sectors. Some attacks have exceeded 1Tbps in volume.

3. Social Engineering

- Social engineering tactics have become more sophisticated, with attackers leveraging psychological manipulation to bypass technical defences. Global trends indicate a rise in Business Email Compromise (BEC) schemes where attackers impersonate trusted contacts to deceive individuals into transferring funds or sensitive information.
- A significant percentage of organisations have reported experiencing social engineering attacks, with many acknowledging that these tactics have led to substantial financial losses and/or operational disruptions.

Global Cyber Threat Landscape Overview... cont'd

4. Phishing

- Phishing remains a dominant threat vector in Kenya, with a significant rise in incidents attributed to the exploitation of AI technologies. Attackers are increasingly using sophisticated phishing emails that mimic legitimate communications to deceive users into revealing sensitive information.
- Phishing attacks are often used as a precursor to ransomware incidents, making them critical to understanding the broader threat landscape. Approximately 90% of cyberattacks begin with phishing attempts, underscoring the need for comprehensive email security measures.

5. System Misconfiguration Attacks

- **Cloud Security Risks -** As more businesses adopt cloud-based systems, misconfigured cloud settings and insecure APIs have been a major attack vector.
  - Cloud breaches remain a top concern. Data shows that cloud security incidents have risen by about 18-25% in 2024, making cloud systems a top target for attackers.
- **IoT Vulnerabilities -** The increase in connected devices (smart devices, sensors, etc.) has led to a rise in IoT-related attacks. These devices often have poor security measures, making them easy to exploit.
  - Reports estimate that IoT-related attacks have surged by 30-35%, particularly in sectors like smart cities and manufacturing.
- **Zero Trust Implementation -** In response to internal threats and advanced cyberattacks, many organisations are adopting zero-trust models to limit access and minimise the impact of breaches.
  - Around 45-50% of organisations have accelerated the implementation of zero-trust architectures in the last quarter of 2024.

6. Emerging Threats

- **AI-Powered Attacks -** Cybercriminals have been increasingly utilising artificial intelligence (AI) to enhance their cyberattack capabilities, such as automating sophisticated phishing schemes and AI-driven malware.
  - AI-related cybercrime is expected to account for 40-50% of all cyberattacks by 2025, with 2024 marking an initial increase in AI-driven phishing and social engineering.
- **Ransomware Evolution -** Ransomware attacks are evolving, with attackers now incorporating double extortion techniques (threatening to leak stolen data) and targeting more sectors beyond traditional industries (e.g., healthcare and energy).
  - Ransomware attacks increased by 15-20% year-over-year, with 60-70% of organisations experiencing a data breach as part of the attack.
- **Supply Chain Attacks -** These attacks remain a significant threat, with cybercriminals exploiting vulnerabilities in third-party vendors to breach larger organizations.
  - The share of attacks targeting supply chains has grown by 25%, with organizations now accounting for 30% of incidents related to third-party vulnerabilities.

Cyber Threat Landscape Roundup

Total Cyber Threats Detected

840,921,998 | **27.83%**

The National KE-CIRT/CC detected over **840 million** cyber threat events during the three-month period between **October to December 2024**, which represented a **27.82% increase** from the threat events detected in the previous period, July - September 2024. We continued to enhance the dissemination of cyber threat advisories to critical information infrastructure sectors, in response to the cyber threats observed.

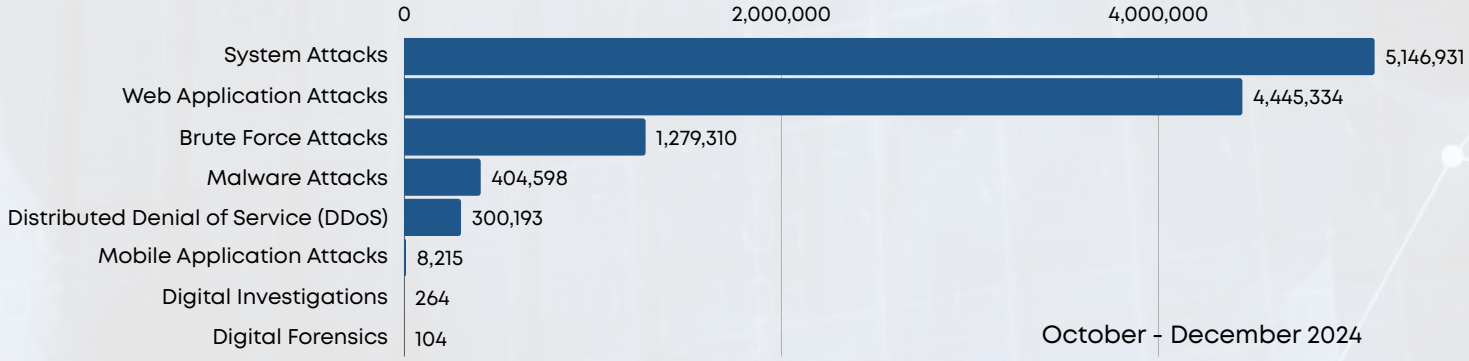
The increase in detected cyber threats can be attributed to the increase in use of artificial intelligence (AI) and machine learning (ML) technologies, inadequate patching of information systems, low levels of awareness about different threat vectors such as phishing and other types of social engineering attacks, hacktivism, among others.

Total Cyber Threat Advisories Issued

11,584,949 | **20.90%**

In response to the detected cyber threat events, the National KE-CIRT/CC issued **11,584,581** advisories between the period **October - December 2024**, which represented a **20.90%** increase compared to the advisories that were issued during the previous period, July - September 2024.

During the period, there was a significant increase in the number of advisories on regularly updating systems, implementing organizational access controls, hardening the anti-virus and firewalls, patching vulnerable systems on a regular basis, and utilising multi-factor authentication and strong passwords.



Cyber Attack Vector Trends

During the quarter under review, system misconfiguration and brute force attacks continued to be the most prevalent in alignment with the global cyber threat landscape. Cyber attacks occasioned by system misconfigurations may be linked to inadequate investment in technical infrastructure, use of legacy or deprecated systems, use of default login credentials, and low levels of cyber risk awareness.

On the other hand, attacks occasioned by brute force may be linked to poor password management, increased automation such as the use of cloud services as well as poor security configurations.

Cyber threat trends by methodology during the period October - December 2024.

SYSTEM ATTACKS

752,441,233

MOBILE APP ATTACKS

138,175

BRUTE FORCE ATTACKS

34,784,028

WEB APP ATTACKS

4,542,939

MALWARE

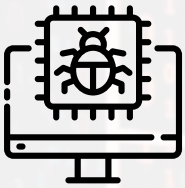
33,920,406

DDOS ATTACKS

15,030,358

Comparison of cyber threat advisories (per vector) issued during the period **October to December 2024**.

Malware Trends



Threats Detected

33,920,406

0.08%

Advisories Issued

404,598

41.9%

During the three-month period between **October to December 2024**, the National KE-CIRT/CC detected **33,920,406** malware threat attempts targeted at the critical information infrastructure sector. This represented a **0.08%** increase from the previous period, July to September 2024.

Majority of the attacks targeted Internet Service Providers (ISPs) and Cloud Service Providers whereby threat actors targeted end-user devices, Internet of Things (IoT) devices, web applications and networking devices belonging to ISPs, cloud-based services and government systems. Attackers also exploited zero-day and supply-chain vulnerabilities.

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

- FortiManager Missing Authentication (CVE-2024-47575): This vulnerability enables attackers to bypass authentication, potentially allowing them to deploy malware or malicious scripts on compromised systems.
- Oracle WebLogic Server Vulnerability (CVE-2024-21260):Attackers exploiting this vulnerability can gain unauthorized access to deploy malware, such as ransomware or cryptominers, on affected systems.
- CWindows Common Log File System Zero-Day (CVE-2024-49138):This zero-day vulnerability allows attackers to execute arbitrary code. Malware often exploits zero-day vulnerabilities for persistence and further infiltration.

Malware attacks majorly targeted vulnerable systems or those systems holding financial or sensitive data. These attacks were aimed at undertaking data exfiltration, backdoor deployments, perform impact brand reputation and to encrypt or damage user 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

4,542,939

29.04%

Advisories Issued

4,445,334

31.36%

During the three-month period between **October to December 2024**, the National KE-CIRT/CC detected **4,542,939** web application attack attempts targeted at the critical information infrastructure sector. This represented a **29.04%** increase from the previous period, July to September 2024.

These attacks majorly targeted government systems and ISPs whereby attackers targeted user login credentials, vulnerable web browsers and database servers belonging to government and Internet Service Providers (ISPs). Most attackers exploited vulnerabilities in SSL/TLS security misconfigurations.

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/Educa**

Top Targeted Exploits

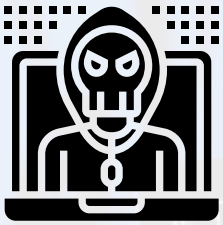
- **Broken access control**
- **Injection**
- **Insecure design**
- **Security misconfiguration**
- **Identification and authentication**

During the period, web application attacks targeted systems deemed vulnerable and containing valuable data. The objectives of the attack were mainly to make services unavailable, manipulate databases and release sensitive data for purposes of damaging organizational 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

34,784,028

8.79%

Advisories Issued

1,279,310

20.81%

During the three-month period from **October to December 2024**, the National KE-CIRT/CC detected **34,784,028** brute force attack attempts majorly targeting the critical information infrastructure sector. This represented a **8.79%** decrease from the previous period, July to September 2024.

Majority of the attacks targeted government systems and cloud service providers whereby attackers targeted user login credentials and database servers belonging to government organisations and cloud-based services. Attackers mostly exploited vulnerabilities in the remote desktop protocol, database servers and user login credentials.

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

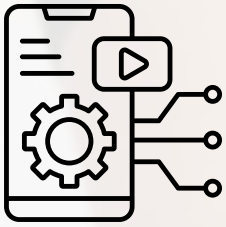
- Exposed Remote Desktop Protocol (RDP)
- Credential Brute-Forcing
- Credential Spoofing
- Credential Sniffing

Over the three month-period, brute force attacks were targeted at systems perceived to hold sensitive data such as financial information and login credentials. These attacks were aimed at mainly gaining elevated privileges, unauthorized access and exfiltrating sensitive data for financial gain.

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

138,175

17.43%

Advisories Issued

8,215

24.49%

During the three-month period from **October to December 2024**, the National KE-CIRT/CC detected **138,175** mobile application attack attempts targeting end-user devices. This represented an **17.43%** increase from the previous period, July to September 2024.

Most of the attacks targeted portable devices such. Attackers targeted mobile devices and Android TVs and leveraged mostly malware to 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

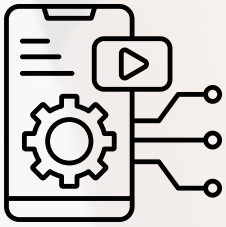
- Improper Credential Usage
- Inadequate Supply Chain Security
- Insecure Authentication
- Insufficient Input/Output Validation

During the period, the perpetrators of mobile application attacks mainly sought to steal sensitive user data such as personally identifiable information, login credentials and financial details for malicious purposes.

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

15,095,217

726.57%

Advisories Issued

300,193

39.19%

During the three-month period **October to December 2024**, the National KE-CIRT/CC detected **15,095,217** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure. This represented a **726.57%** increase from the previous period, July to September 2024.

Most of the attacks targeted the health sector and government systems whereby attackers exploited vulnerabilities in insecure protocols and remote desktop service, with the aim of amplifying requests to legitimate servers thus denying legitimate users access to services.

Top Targeted Systems

- Email Servers
- Web servers
- Database Servers

Top Affected Industries

- Health Sector
- Government

Top Targeted Exploits

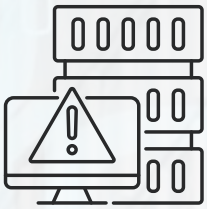
- Increase in network time protocol (NTP) amplification DDoS attack
- Windows Remote Desktop Services Denial of Service Vulnerability
- Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability

Over the three month period, attackers mainly aimed to degrade the quality of services or render critical services unavailable for system users.

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

752,441,233

28.91%

Advisories Issued

5,146,931

11.13%

Most attacks were targeted at the ICT sector whereby attackers targeted database servers and operating systems belonging to ISPs and Cloud Service Providers. Attackers mostly exploited vulnerabilities in outdated operating systems and leaked user login credentials. The continued prevalence of system vulnerabilities may be attributed to the proliferation of Internet of Things (IoT) devices which are inherently insecure.

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

System attacks targeted the critical information infrastructure sector that holds sensitive data such as financial information. The objectives of these attacks were to disrupt, compromise and sabotage essential systems and services on a large 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

2024 Africa Cyber Sector Collaboration Symposium

October is internationally recognized as the cyber security awareness month. The Authority, on behalf of the Kenyan government, spearheads the October Cybersecurity Awareness Month (OCSAM) series. This is a collaboration between the public and private sectors with the objective of raising awareness on cyber safety and security by empowering industry and consumers with the requisite knowledge, skills and values to safeguard themselves online. This aligns with the Authority's Strategic Goal on empowerment and protection of consumers of ICT services as outlined in the Authority's 2023 - 2027 Strategic Plan.

During His Excellency President Dr. William Ruto's visit to the United States in May 2024, Kenya and the United States agreed to co-host a regional forum to be the highlight of the October cybersecurity awareness month activities. The main objective of the forum was to build the technical capacity and knowledge of cybersecurity incident response teams, and to enhance information sharing between them, thus enabling a more resilient cyberspace in Africa.

It is in this regard that the Authority, through the National KE-CIRT/CC, hosted the 2024 Africa Regional Cyber Sector Collaboration Symposium from 22nd to 25th October, 2024 in Nairobi. The symposium was hosted in collaboration with the U.S. State Department's Bureau of Cyberspace and Digital Policy (CDP). Carnegie Mellon University's Software Engineering Institute (SEI) and the Forum of Incident Response and Security Teams (FIRST) facilitated a managerial training program and a technical training program, respectively.

This year's theme was *"Human-Driven Innovation: Empowering Minds, Enhancing Cyber Defences."* Throughout the month of October, the theme highlighted the power of human intellect, problem-solving capabilities, and collaborative efforts in shaping advanced cyber security solutions thereby facilitating discussions that addressed the following key areas:

- Bridging the cybersecurity skills gap and enhance the cyber security awareness levels in the African region;
- Enhancing innovation, trust networks, information sharing and collaboration amongst diverse cybersecurity constituents across Africa;
- Enhancing the resilience and security of the critical information infrastructure sector; and,
- Strengthening and expanding Public-Private Partnerships (PPPs) across all sectors.

Two separate training programmes were conducted for three days each, from 22nd to 24th October, 2024 as part of the pre-conference programme. The training programmes were conducted as follows:

- Track 1: This comprised technical personnel who handle day-to-day operations of organisations in the Critical Information Infrastructure (CII) sector. This track was facilitated by the Forum of Incident Response and Security Teams (FIRST).

- Track 2: This comprised managerial personnel that directly influence decision making processes as relates to operations of organisations in the Critical Information Infrastructure (CII) sector. This track was facilitated by the CERT Division (CERT/CC) of Carnegie Mellon University's Software Engineering Institute (SEI).

Over 80 trainees participated in the training programmes. Based on deliberations and feedback from participants, the training programme was highly effective and beneficial and imparted practical skills that could be applied immediately in their work environment.

In particular, and based on the Authority's strategic direction, participants recommended that the National KE-CIRT/CC constituents be trained on the development of sector CIRTs/SOCs as an immediate need.

The main conference was conducted on 25th October, 2024 with over 155 delegates participating in the conference. Based on deliberations and feedback from participants, there is a need to upscale cybersecurity training programmes in academic institutions across Africa by collaborating with public and private entities to bridge the skills gap. Additionally, there is a need to develop regional information-sharing frameworks that prioritise trust-building, transparency, and structured collaboration between stakeholders. Implementing emerging technologies for CII security, including AI and machine learning for proactive threat detection, focusing on cost-effective solutions for wider adoption was also discussed. Finally, there's need to strengthen and sustain Public-Private Partnerships (PPPs) by formulating policies that promote regulatory alignment across sectors, encouraging private sector innovation while ensuring cybersecurity compliance.

Participants were drawn from both local and international cybersecurity stakeholders, bringing together representatives from national CIRTs across Africa, industry players, CEOs, CISOs, academia, legal and compliance professionals, technology vendors, government regulators, among others. The international delegates who attended the conference were drawn from several African countries that included Botswana, Ethiopia, Malawi, Mauritius, Mozambique, South Africa, Tanzania, Uganda, and Zambia.

Moments in Motion – Capturing the Essence of the 2024 Africa Regional Cyber Sector Collaboration Symposium

Moments in Motion – Capturing the Essence of the 2024 Africa Regional Cyber Sector Collaboration Symposium

49th Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

The National KE-CIRT/CC Cybersecurity Committee (NKCC) draws its membership from over 50 public and private sector critical information infrastructure (CII) organisations across various sectors 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.

State-sponsored threat actor groups are increasingly leveraging ransomware attacks to target industries with complex supply chain processes, exploiting vulnerabilities during system updates to disrupt critical operations. Notably, the aviation industry reported a surge in drone-initiated attacks, which compromised critical signals and frequencies essential for seamless flight operations.

A significant increase in Distributed Denial of Service (DDoS) and phishing attacks was observed in sectors that process personal data and Personal Identifiable Information (PII) such as the health sector. In response, various sector players conducted comprehensive risk assessment exercises to identify vulnerabilities in their security frameworks and developed strategies to mitigate risks. Key initiatives focused on enhancing cybersecurity best practices, improving incident response plans, and enhancing collaboration between industry players and regulators.

NKCC members reiterated the importance of collaboration, including information sharing and training opportunities, to enhance the capacity of organisations in addressing the ever-evolving cyber threats. By pooling resources and expertise, sectors can better prepare for, and respond to emerging threats, ultimately safeguarding critical infrastructure and protecting sensitive customer data.

The 49th Meeting of the NKCC was held on 5th December, 2024, on the sidelines of the training programme on Cybersecurity Governance, in Nairobi.

Members pose for a photo during the 49th meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC). Eng. Leo Boruett, Director, Multimedia Services (centre in tie), represented the Authority's Director General during the event.

Training Programme on Cyber Security Governance

The Authority hosted a training programme on Cyber Security Governance for members of the National KE-CIRT/CC Cybersecurity Committee (NKCC) from 2nd – 5th December, 2024, in Nairobi. The programme was held in line with the Strategic Goal on empowerment and protection of consumers of ICT services as outlined in the Authority's 2023 - 2027 Strategic Plan.

The four-day programme explored aspects of data security governance, covering risk assessment, mitigation strategies, and data protection mechanisms such as encryption and secure access controls. Additionally, the programme explored the legal and regulatory considerations of cybersecurity including compliance with the Data Protection Act, 2019. Over 40 trainees took part in the training, bringing together key stakeholders from diverse sectoral CIRTs, such as, e-government, ICT and telecoms, banking & finance and academia.

The programme also emphasised the importance of enterprise cybersecurity strategies, including incident response, business continuity planning, and disaster recovery plans. Participants learned about the benefits of adopting zero trust architectures, which prioritise strict access controls and trust verification to minimise risks within organisational networks.

Throughout the training programme, participants were encouraged to take proactive roles in promoting a security-first culture within their organisations.

Trainees drawn from the NKCC during a training programme on Cyber Security Governance that was held from 2nd to 5th December 2024, in Nairobi.

Updates from the National KE-CIRT/CC

The Kenya Information and Communications Act (KICA) of 1998 mandates the Authority to develop a national cybersecurity management framework. Towards this end, the government of Kenya established the Kenya Computer Incident Response Centre - Coordination Centre (National KE-CIRT/CC). This is a multi-agency collaboration framework that is responsible for the national coordination of cyber security and acts as Kenya's national point of contact on cyber security matters.

The National KE-CIRT/CC has been instrumental in coordinating response to cyber threats in partnership with relevant law enforcement agencies, sector regulators, financial institutions and the private sector.

The following is an update on the National KE-CIRT/CC's cybersecurity management activities between October and December 2024:

National Credit Market Convention

The Authority participated in the inaugural National Credit Market Convention from 21st to 22nd November, 2024 at Lake Naivasha Resort, Naivasha. The convention was organised by Metropol Credit Reference Bureau Limited and brought together key players in finance, strategy, risk, credit and operations, from across the banking and financial sector in Kenya.

The convention was aimed at formulating strategies to ensure the stability and prosperity of the credit market, by benefiting all stakeholders involved. It brought together industry leaders, policymakers, financial institutions, and regulators to address pressing challenges such as the surge in cybercrime and other forms of technology misuse, explore innovative solutions, and develop actionable frameworks aimed at promoting sustainable financial practices.

During the convention, the Authority delivered a presentation on its cybersecurity mandate through the National KE-CIRT/CC, highlighting its functions and services. The Authority also highlighted its collaboration frameworks that includes the banking and financial sector, and further outlined how this partnership has been instrumental in addressing various cross-sector and cross-border cybersecurity challenges affecting the sector such as phishing and other types of social engeering scams .

A section of delegates during the inaugural National Credit Convention that was held from 21st - 22nd November, 2024 at Lake Naivasha Resort, Naivasha.

TV Interview on Artificial Intelligence (AI) and Cyber Harassment

Dr. Vincent Ngundi, Director, Cyber Security, Communications Authority of Kenya (CA) and Head of the National KE-CIRT/CC, during an interview on AI and Cyber Harassment on Citizen TV on 13th December, 2024.

In a televised interview on *Citizen TV* on 13th December 2024, Dr. Vincent Ngundi, Director, Cyber Security and Head of the National KE-CIRT/CC, speaking on the subject of AI and cyber harassment, informed viewers that AI has significantly altered the dynamics of cyber harassment, both as a tool for mitigation and as a mechanism for amplification. He further stated that AI-driven attacks, just like conventional threat vectors, are considered cybercrimes within the context of the Computer Misuse and Cybercrimes Act (CMCA 2018).

Dr. Ngundi observed that, since threat actors exploit the same infrastructure that supports telecommunications and other critical business operations, this makes them in direct violation of Kenyan cybersecurity laws and regulations. Further, he affirmed that the Authority collaborates with the various agencies of government that includes the military, the Directorate of Criminal Investigations (DCI) and the Judiciary, to effectively combat these new and emerging cybercrimes. This multi-stakeholder approach ensures a comprehensive response by integrating expertise in investigation, enforcement, and the adjudication of cyber-related offences.

Acknowledging that the social media platforms used by Kenyans are predominantly foreign-owned, the Authority has established partnerships with various global technology companies such as Meta, Telegram, and TikTok to address the linkage between local concerns and global challenges. These frameworks facilitate the building of synergies to assist in mitigating cyber threats, combating harmful and inappropriate content, and ensuring the safety and security of Kenyan users while aligning with international best practices.

On data privacy, Dr. Ngundi asserted that the cornerstone of the Data Protection Act (DPA 2019) lies in safeguarding individuals' personal data and ensuring the acceptable use of Personally Identifiable Information (PII) by data controllers and data processors. This principle outlines the need to protect individuals' rights while at the same time strengthening trust in our digital infrastructure.

In closing, he reiterated the need to raise public awareness on Kenya's cybercrime laws and regulations, as there remains a significant level of laxity among citizens in understanding and adhering to the legal frameworks. Educating the public on their rights, responsibilities, and the consequences of cybercrime is essential to promote a culture of accountability and promoting safer digital practices.

Future Insights on Cybersecurity

The Authority, in partnership with the African Union Commission, the European Union and the Council of Europe (GLACY-e project), the Ministry of Interior and National Administration, the Kenya Judiciary Academy (KJA) and other local and international stakeholders and partners, will host the 3rd African Forum on Cybercrime in Nairobi.

The forum, that is slated to be held in March 2024, will focus on addressing emerging cybersecurity threats by identifying comprehensive mechanisms to combat cybercrime. The forum is expected to provide a platform for sharing of Information on new threats, trends and responses to the challenges of cybercrime and electronic evidence to enable more consistent approaches to these challenges across the African continent.

Additionally, delegates from participating countries will have the opportunity to better understand the strategies, policies, legislation and tools in order to engage more effectively in domestic, regional and international criminal justice responses to cybercrime and electronic evidence.

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