COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

35th Edition

July - September 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)

Artificial intelligence (AI) technologies have become an integral component to enhancing cybersecurity systems through automation, machine learning and threat detection. However, they also present challenges as cybercriminals leverage AI technologies to perpetrate sophisticated attacks. With the rise of mobile devices, cybersecurity risks are increasing, particularly in mobile banking and personal data. The growth of cloud services demands stronger security protocols to prevent breaches, while data protection regulations enforce stricter data protection standards.

The Authority hosts the National KE-CIRT/CC, which 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 detects, prevents and responds to various cyber threats targeted at the country, and acts as the interface between local and international ICT service providers whose platforms may be used to perpetrate cybercrimes, and our Judicial Law and Order Sector which investigates and prosecutes cybercrimes.

The National KE-CIRT/CC detected over 650 million cyber threat events over the period July - September 2024. Majority of these attacks exploited system vulnerabilities. This trend is further attributed to the continued adoption of AI-enabled attacks, continued attacks targeted at system misconfigurations, and continued adoption of botnets and Distributed Denial of Service (DDoS) attack techniques.

Cybercriminals are increasingly using AI-enabled attacks to enhance the efficiency and magnitude of their operations. They leverage AI and machine learning to automate creation of phishing emails and other types of social engineering. Further, they are increasingly targeting system misconfigurations to exploit security weaknesses. These include open ports, insufficient access controls, amongst others, enabling cybercriminals to gain unauthorized access to systems, steal sensitive data or even deploy malware.

Threat actors are also using botnets and Distributed Denial of Service (DDoS) attacks to disrupt services and overwhelm networks. Botnets are networks of compromised devices controlled remotely by attackers, which are used to flood a target system with traffic during a DDoS attack. This overwhelming volume of requests renders the targeted system or website unable to handle legitimate user traffic, resulting in outages or degraded performance. These attacks are often used for extortion, causing financial loss and reputational damage to organizations. Botnets can also spread malware and other malicious software to expand the attacker’s reach.

The Global Cybersecurity Index (GCI) is a ranking system developed by the International Telecommunication Union (ITU) to assess and measure countries' commitment to cybersecurity. The GCI survey conducted for Kenya assessed a range of cybersecurity indicators aligned with the five pillars of the ITU’s Global Cybersecurity Agenda (GCA).

Kenya, through the Authority's National KE-CIRT/CC, earned the prestigious Tier 1 ranking in the GCI, marking the highest level of recognition for its commitment, readiness and resilience in cybersecurity. This achievement reflects Kenya’s advanced capabilities across the five key pillars - legal frameworks, technical measures, organisational structures, capacity-building initiatives and international collaboration.

As a Tier 1 country, Kenya joins the ranks of global cybersecurity leaders such as the United States, the United Kingdom, Japan, and Germany, showcasing its leadership in digital transformation and cybersecurity.

Mr. David Mugonyi, EBS
Director General/CEO

Global Cyber Threat Landscape Overview

Malware

**** Malware refers to any malicious code or program such as viruses, bugs, worms, bots, rootkits, spyware, adware, Trojans, and even ransomware that gives a cyber threat actor explicit control over your system.***

Ransomware is an advanced sub-type of malware that enables cyber threat actors to gain control of a system and limit users' access to files unless a ransom is paid.

Cyber threat actors continued to leverage various malware categories to compromise and disrupt systems, carry out data breaches and cause operational downtime and data loss within the education, government, insurance and healthcare sectors. The top malware categories include:

- BugSleep: Steals files and executes commands on compromised systems.
- ViperSoftX: Steals sensitive data, including crypto.
- Macma Backdoor and Nightdoor: Deployed by *Evasive Panda/StormBamboo* threat group to intercept and modify victims' DNS requests and infect them with malicious IP addresses without any detection.

Notably, the ransomware trend observed was as follows:

- Volcano Demon: Targets manufacturing and logistics industries, encrypting files with *.nba* extension.
- Lockbit3: The Ransomware-as-a-Service (RaaS) based malware resurfaced, attacking large scale enterprises and government entities.
- New play Ransomware: The malware deploys a dedicated Linux locker for encrypting VMware ESXi virtual machines. The locker can evade detection on Linux systems.

Mobile Malware

Mobile devices continue to be used for both personal and professional activities. This makes them prime targets for cyber threat actors. During this period, cyber threat actors were seen to leverage the following mobile malware:

- Joker: Android spyware stealing SMS messages and contact lists.
- Anubis: Android banking Trojan with additional ransomware features.
- AhMyth: Android Remote Access Trojan (RAT) that steals sensitive device information.

Phishing and Social Engineering

The human element remains the weakest link in cybersecurity due to human error, lack of awareness, but also human intellect, amongst other reasons. During this period, cyber threat actors used advanced techniques like Natural Language Processing (NLP) to craft convincing phishing and smishing (SMS phishing) attacks. These tactics were used to lure users into revealing personal identifiable information and installing malware, leading to data breaches and financial losses.

Global Cyber Threat Landscape Overview

System Attacks

During this period, cyber threat actors targeted database servers, operating systems, web applications and email servers, Industrial Control Systems (ICS), and networking infrastructure of organisations within government and the healthcare sectors in order to deliver malware and ransomware. The increased number of IoT devices also led to a surge in increased system attacks given most devices are rarely updated and use default login credentials.
To mitigate these risks, the National KE-CIRT/CC recommends applying regular operating system and application updates, using strong passwords and multi-factor authentication, and hardening firewall configurations.

DDoS Attacks

During this period, Microsoft experienced a significant disruption across its cloud services due to a Distributed Denial-of-Service (DDoS) attack that disrupted global cloud services for nearly 10 hours. This impacted a range of services including Azure Application Services, Application Insights, and the Azure portal, among others, causing widespread disruption of business processes and customer services globally.

The attack primarily targeted Azure Front Door (AFD) and Azure Content Delivery Network (CDN) components. Despite having DDoS protection mechanisms in place, an error in their implementation amplified the attack's impact rather than mitigating it. Towards this, Microsoft's team implemented networking configuration changes and failovers to alternate paths to mitigate the impact and thereafter rolled out a revised mitigation strategy.

Mapping the Global Threat Landscape

The similarities in attack vectors, tactics, and vulnerabilities impacting both individuals and organisations demonstrates how the cyber threat landscape in Kenya and across the rest of the world are aligned.

This convergence highlights the universal nature of cyber threats, as global trends and techniques tend to manifest within local and regional geolocations.

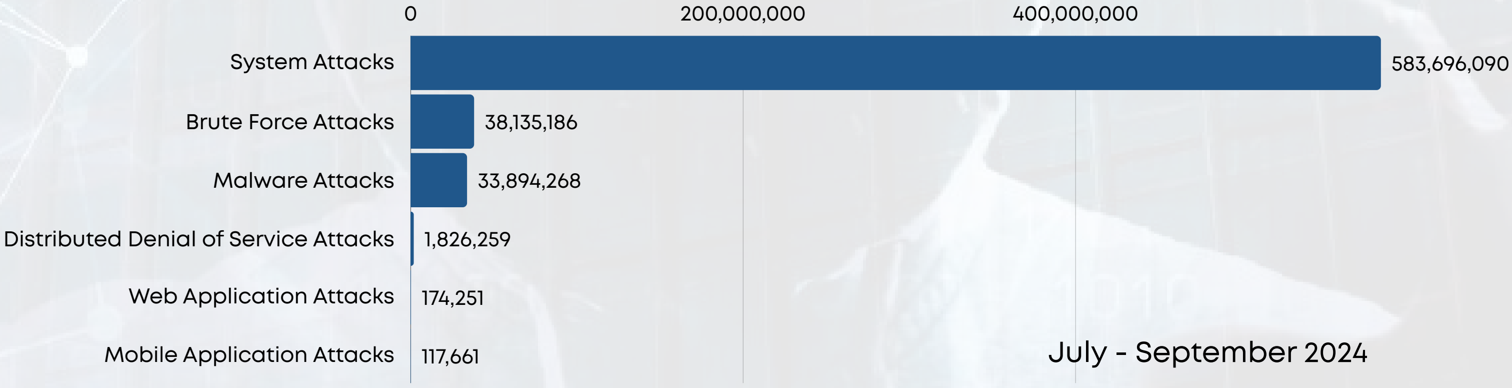
Cyber Threat Landscape Roundup

Total Cyber Threats Detected

657,843,715 | **41.87%**

During the three-month period between **July and September 2024**, the National KE-CIRT/CC detected over **657.8 million** cyber threat events, which represented a **41.87%** decrease from the **1,131,696,878** threat events detected in the previous period, April - June 2024. In response to the cyber threats observed, we continued to enhance the dissemination of cyber threat advisories to critical information infrastructure sectors.

In line with global trends, the ongoing exploitation of "system vulnerabilities" may be associated to the continued proliferation of Internet of Things (IoT) devices which are inherently insecure. Other weaknesses include system misconfigurations and deprecated software, and the dynamism occasioned by new and emerging technologies such as Artificial Intelligence (AI).

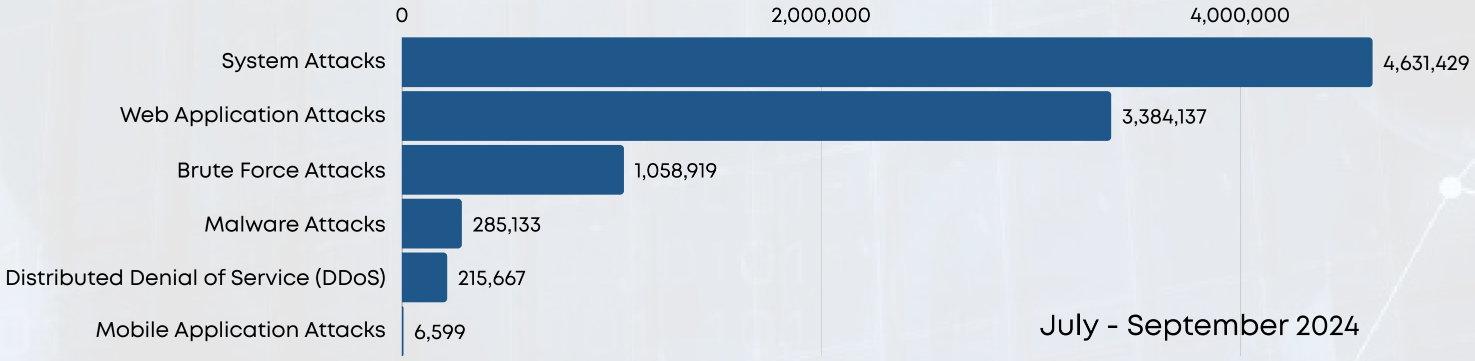


Total Cyber Threat Advisories Issued

9,582,347 | **2.51%**

In response to the detected cyber threat events, the National KE-CIRT/CC issued **9,582,347** advisories between the period **July - September 2024**, which represented a **2.51%** increase compared to the **9,347,363** advisories that were issued during the previous period, April - June 2024.

During the period, there was a significant increase in the number of advisories on system attacks. These advisories were aimed at advising users to patch vulnerable systems on a regular basis, utilising multi-factor authentication, strong passwords, and hardening systems and networks.



Cyber Attack Vector Trends

During the quarter under review, system misconfiguration attacks were the most prevalent. This aligns with the global cyber threat landscape where malware attacks, and more specifically ransomware, was most common.

Cyber attacks occasioned by system misconfiguration may be linked to inadequate investment in technical infrastructure, use of legacy systems and default login credentials, and low levels of cyber risk awareness. These factors all contribute to increased susceptibility of the critical information infrastructure sectors to cyber threats.

Cyber threat trends by methodology during the period July to September 2024.

SYSTEM ATTACKS
583,696,090

MOBILE APP ATTACKS
117,661

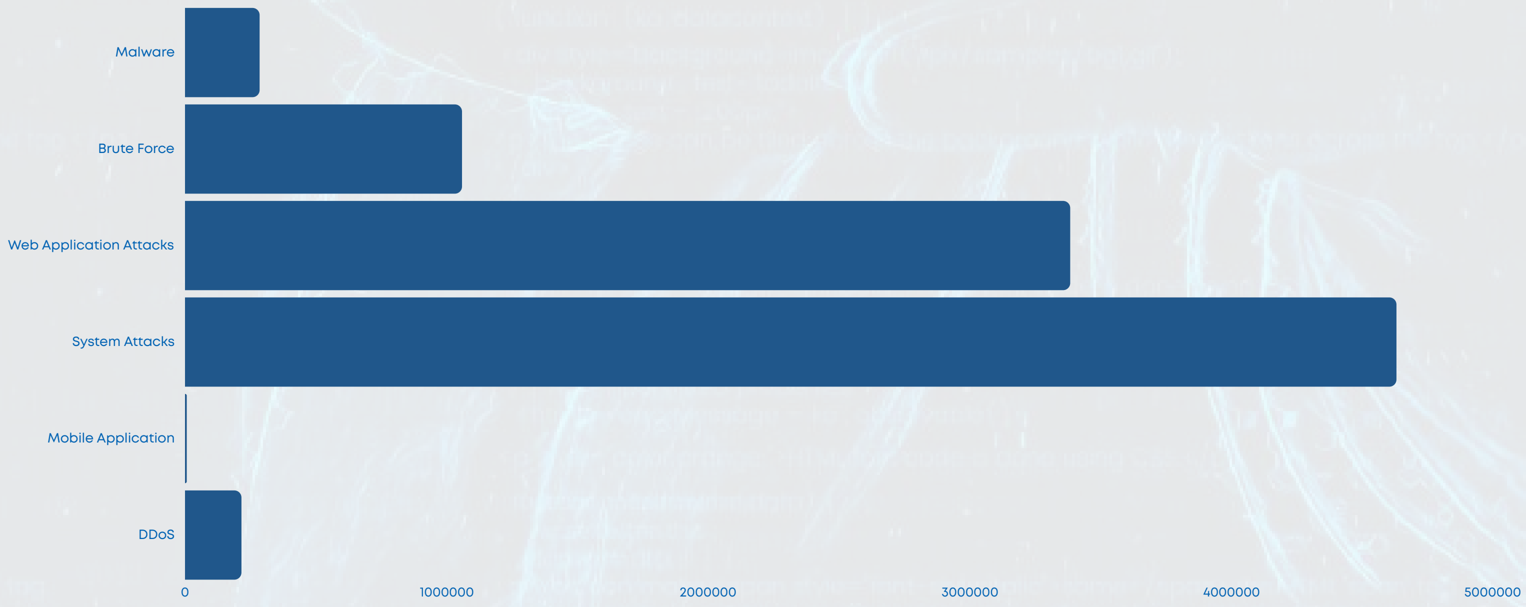
BRUTE FORCE ATTACKS
38,135,186

WEB APP ATTACKS
174,251

MALWARE
33,894,268

DDOS ATTACKS
1,826,259

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



Malware Trends

Threats Detected

33,894,268

6.13%

Advisories Issued

285,133

55.67%

During the three-month period between **July to September 2024**, the National KE-CIRT/CC detected **33,894,268** malware threat attempts targeted at the critical information infrastructure sector. This represented a **6.13%** increase from the previous period, April to June 2024.

Most of the attacks targeted the ICT sector and Cloud Service Providers. Threat actors targeted end-user devices, Internet of Things (IoT) devices, web applications and networking devices belonging to Internet Service Providers (ISPs), cloud-based services and government systems. Most attackers 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

- **CVE-2024-20399: Cisco patched a zero-day vulnerability in NX-OS exploited to install unknown malware as root on vulnerable switches.**
- **CVE-2024-6387: An unauthenticated remote code execution vulnerability in OpenSSH, dubbed "regreSSHion," allows root access on glibc-based Linux systems.**
- **CVE-2024-39929: A critical bug in Exim mail transfer agent allowing threat actors to bypass security filters on over 1.5 million mail servers.**
- **CVE-2024-5441: A vulnerability in the Modern Events Calendar WordPress plugin, affecting over 150,000 sites, allows hackers to upload arbitrary files and execute code remotely.**

These malware attacks were mainly targeted at systems that were deemed as being vulnerable or holding valuable or sensitive data. The objective of these attacks was to conduct backdoor deployments, perform data exfiltration, 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, include security during development of software.
- Asset management with patch management.
- Deployment of domain protection tools such as Domain-Based Message Authentication Reporting and Conformance (DMARC) and spam filters.
- Improve end-user cyber hygiene and awareness.

Web Application Attack Trends

Threats Detected

174,251

18.62%

Advisories Issued

3,384,137

11.27%

During the three-month period between **July to September 2024**, the National KE-CIRT/CC detected **174,251** web application attack attempts targeted at the critical information infrastructure sector. This represented a **18.62%** increase from the previous period, April to June 2024.

Most of these attacks targeted government systems and the ICT sector. 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
- Cloud Service Providers
- Academia/Educa

Top Targeted Exploits

- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication

During the period, web application attacks targeted systems deemed to contain valuable data and critical information services. 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

38,135,186

42.01%

Advisories Issued

1,058,919

11.42%

During the three-month period from **July to September 2024**, the National KE-CIRT/CC detected **38,135,186** brute force attack attempts majorly targeting the critical information infrastructure sector. This represented a **42.01%** increase from the previous period, April to June 2024.

Majority of the attacks targeted government systems and cloud service providers. Attackers targeted user login credentials and database servers belonging to government organisations and cloud-based services. Most attackers 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

During the period, brute force attacks were targeted at systems deemed to hold sensitive data such as login credentials and financial information. The objective of these attacks was mainly to gain elevated privileges, gain unauthorized access and exfiltrate 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

117,661

18.50%

Advisories Issued

6,599

5.80%

During the three-month period from **July to September 2024**, the National KE-CIRT/CC detected **117,661** mobile application attack attempts targeting end-user devices. This represented an **18.50%** increase from the previous period, April to June 2024.

Majority of the attacks targeted portable devices. Attackers targeted mobile devices and Android TVs and leveraged mostly on 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

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

1,826,259

75.10%

Advisories Issued

215,667

1,763.70%

During the three-month period **July to September 2024**, the National KE-CIRT/CC detected **1,826,259** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure. This represented a **75.10%** decrease from the previous period, April to June 2024.

Majority of the attacks targeted government systems and the health sector. Attackers exploited vulnerabilities in insecure protocols to amplify requests to legitimate servers with the aim of exhausting them such that users were unable to access 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

During the period, the perpetrators of the DDoS attacks mainly sought to degrade the quality of services or render critical services inaccessible to system users.

To mitigate this risk, the National KE-CIRT/CC carried out cyber awareness activities targeting 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

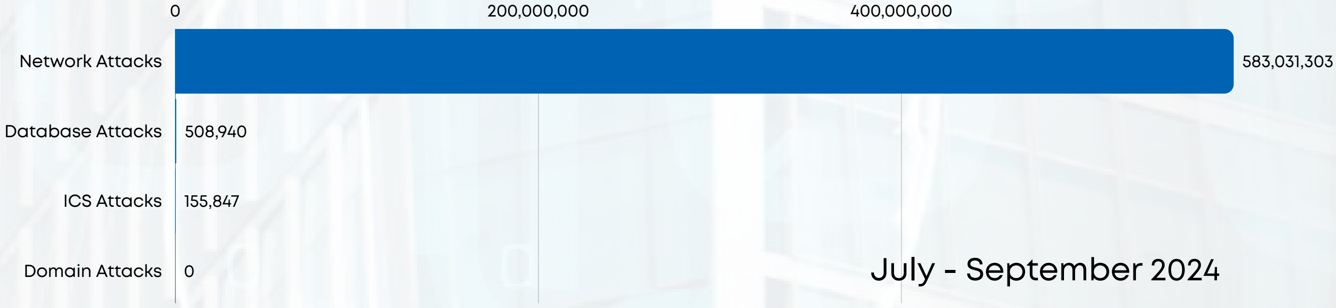
583,696,090

45.21%

Advisories Issued

4,631,429

1.35%



July - September 2024

Majority of the attacks targeted organisations within the ICT sector. Attackers targeted database servers and operating systems belonging to Internet Service Providers (ISPs) and cloud-based services. Most attackers 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
- Remote Code Execution (RCE)

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.
- Use of strong passwords and multi-factor authentication.
- Hardening of firewall configurations.

48th 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.

Members discussed the critical role that e-government platforms play in driving Kenya's national digital transformation agenda, in enhancing public service delivery, promoting transparency and accountability, and also improving accessibility to public services for citizens and businesses alike. Through cyber threat monitoring, issuance of advisories, capacity development, user awareness, and collaboration with our various stakeholders, the National KE-CIRT/CC continues to facilitate and enhance the protection of CIIs, and therefore advance national cyber resilience.

The telecommunications and ICT sector continues to grapple with numerous cases of identity theft, online impersonation and social engineering, with cybercriminals exploiting vulnerabilities especially on social media platforms. It was observed that that these threats pose significant risks to both individuals and organisations, highlighting the need for stronger security measures and public awareness to protect individuals' Personally Identifiable Information (PII).

The dot ke country code top-level domain (.ke ccTLD) is a critical asset to Kenya's digital identity, playing a key role in promoting local online presence, supporting electronic services and electronic commerce, amongst other roles. Members agreed that in order for the country to derive its full benefits, there's a pressing need to sensitize the public on the need for its adoption by all relevant stakeholders, highlighting the strategic advantages of using the .ke ccTLD in building a trusted national digital ecosystem.

The 48th Meeting of the NKCC was held on 16th August 2024, in Nairobi.

Participants pose for a photo during the 48th meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC) on 16th August 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 July and September 2024:

Capability and Capacity Development

The Authority, in collaboration with Huawei Technologies Kenya, hosted a training programme on Cloud Computing Security for members of the National KE-CIRT/CC Cybersecurity Committee (NKCC) on August 15th & 16th, 2024. Such capacity building initiatives support the empowerment and protection of consumers as one of the strategic objectives in the Authority's 5th strategic plan.

The focus of the two-day programme, which targeted cybersecurity professionals in the critical information infrastructure sector, was on cloud computing security, understanding the inherent cyber risks and how to manage them, exploring governance frameworks, and trends that shape modern approaches to cloud computing security.

The programme was interactive, and included post-module Q&A sessions, information and experience sharing sessions, and knowledge exchange sessions by subject matter experts. Case studies were used to provide real-world examples of cloud security breaches and how they could be mitigated. Participants had the opportunity to take part in a certification exam at the end of the training thereby validating the skills and knowledge gained during the training.

Seventy (70) trainees took part in the training, bringing together key stakeholders from various sectors that included e-government, telecommunications, health, energy, the banking & finance sectors, law enforcement agencies, the civil society, and standards bodies, amongst others.

Participants pose for a photo during the training programme on Cloud Computing Security that was held on 15th and 16th August 2024 in Nairobi.

CyberWeek Africa 2024 Conference & Expo

The Authority took part in the CyberWeek Africa 2024 Conference & Expo in Nairobi, Kenya. The conference, which took place from September 23rd to 27th, 2024, was organised by the Kenya School of Government (KSG), the University of Nairobi (UoN), the Ministry of State and Industry of the State of Israel, and the National Computer and Cybercrimes Committee (NC4), amongst others.

The objective of the conference was building resilience for Africa's cyberspace by emphasising the importance of collaboration, technological innovation, security by design, workforce development, risk management and security awareness. The conference highlighted the collaborative effort between government, industry and academia to build the capacity of Africa's cybersecurity workforce and leverage new and emerging technologies.

During the conference, the Authority delivered a presentation on its cybersecurity mandate through the National KE-CIRT/CC, highlighting its core functions and services. Additionally, the Authority highlighted its strategic partnerships and collaborations with both local and international stakeholders, which are crucial in addressing cross-sector and cross-border cybersecurity challenges. Moreover, the ongoing capacity-building initiatives aimed at enhancing skills and expertise in the cybersecurity workforce were highlighted.

These efforts are central to advancing the National digital transformation agenda through enhancing the security and resilience of our national digital ecosystem.

Top 100 Cybersecurity Women to Watch Africa (T1CWWA) 2024 Awards

The Authority participated in the Acyberschool's Top 100 Cybersecurity Women to Watch in Africa (T1CWWA) 2024 Awards that was held on September 27th, 2024 at the Kenya School of Government (KSG) in Nairobi. The event's key objective was to celebrate outstanding women in the cybersecurity field with discussions centred on the role women play in shaping the future of cybersecurity.

The event incorporated panel discussions and hands-on learning and demonstrations that featured micro-workshops addressing topics such as home network security, blockchain security and phishing prevention. Participants were exposed to real-world scenarios, including social engineering challenges and cloud security hacks. This segment provided practical knowledge on detecting AI-driven threats, an essential skill in today's cyber threat landscape.

The day's highlight was the awards ceremony, which honoured the top 100 cybersecurity women across Africa. The ceremony included recognition of in-person attendees and virtual awardees, ensuring inclusivity across the continent. The final session involved a fireside chat with the key speakers of the day discussing the role, challenges and opportunities for women in the cybersecurity field.

The Authority's Ms. Jessica Wanjohi and Ms. Cynthia Rotich were recognized among the top 100 cybersecurity women to watch in Africa, a fete attributed to their dedication in raising awareness and building cybersecurity capacity in Kenya.

Kenya Ranked in Tier 1 in the ITU Global Cybersecurity Index (GCI) Ranking

The Global Cybersecurity Index (GCI), which is an initiative of the International Telecommunication Union (ITU), is a ranking system that is used to measure countries' global commitment to cybersecurity. It aims to assist countries in improving their cybersecurity readiness and resilience by establishing a comparative baseline and encouraging cybersecurity cooperation and capacity-building. The purpose of the GCI is to measure countries' commitment to strengthen cybersecurity, promote best practices, foster international cooperation, encourage capacity building highlight gaps in national strategies and encourage improvement, support global cybersecurity resilience, amongst others.

The GCI survey looks at a variety of cybersecurity indicators based on the five pillars of ITU's Global Cybersecurity Agenda (GCA). These include legal measures, technical measures, organisational measures, capacity building and cooperation. The main objective of these pillars is to measure the type, levels and evolution over time of countries' cybersecurity commitments, the progress in cybersecurity commitment from a global perspective, the progress in cybersecurity commitment from a regional perspective, and the cybersecurity commitment divide which is the difference between countries in terms of their level of engagement in cybersecurity initiatives.

Kenya, which is represented by the Authority in the ITU GCI initiative, was ranked as Tier 1, which is the highest ranking awarded in the ITU GCI report. This ranking indicates that a country has demonstrated the highest level of cybersecurity commitment, readiness and resilience. Tier 1 countries are acknowledged as global cybersecurity leaders with advanced legal frameworks, technical measures, organisational structures, capacity-building initiatives, and strong international collaboration in cybersecurity. These countries are typically at the forefront of global cybersecurity efforts and often play a key role in shaping international cybersecurity policies, initiatives and frameworks.

This recognition highlights Kenya's growing role as a leader in digital transformation on the global stage. This remarkable achievement was realised through collaborative efforts with both local and international partners and stakeholders.

The detailed GCI 2024 report can be accessed at the following link: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

Future Insights on Cybersecurity

The Authority, in its effort to commemorate the October Cyber Security Awareness Month (OCSAM), will host the *African Regional Cyber Sector Collaboration Symposium*. This symposium represents a pivotal effort in strengthening national cyber readiness and resilience, under the theme *"Human-Driven Innovation: Empowering Minds, Enhancing Cyber Defences"*. The theme underscores the vital role of human intellect, problem-solving capabilities, and collaboration in developing innovative and effective cybersecurity solutions.

The symposium is designed as a comprehensive four-day event, featuring three days of intensive managerial and technical training sessions followed by a full-day plenary conference, culminating in a formal gala dinner. This structure not only fosters the exchange of knowledge but also provides a platform for networking and partnership-building among participants.

The symposium, which will be held in collaboration with the United States government, will be feted with local and international industry players. This emphasizes the global nature of cybersecurity threats and the critical importance of cross-border collaboration in combatting increasingly sophisticated cyber crimes.

As part of our ongoing commitment to capacity building, particularly among the next generation of cybersecurity professionals, the Authority will also host a bootcamp competition targeted at tertiary, college, and university students. This bootcamp is designed to immerse students in real-world cybersecurity scenarios, equipping them with practical skills, broadened perspectives, and enhanced problem-solving capabilities beyond the traditional classroom environment.

This symposium and bootcamp are integral steps in our broader mission to fortify our national cybersecurity posture, recognizing that a well-prepared workforce is essential to maintaining strong, adaptable cyber defenses.

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