COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

32nd Edition

October - December 2023

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 5th Strategic Plan (2023 - 2027) of the Communications Authority of Kenya (CA), aims to build upon past achievements, tackle present challenges and opportunities in the evolving ICT landscape and enhance the Authority's performance in the 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), 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).

This 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 CA Centre along Waiyaki Way, Nairobi, comprises of technical staff from the Authority and various law enforcement agencies.

The National KE-CIRT/CC detects, prevents and responds to various cyber threats targeted at the country on a 24/7 basis. It also 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 enactment of the Computer Misuse and Cyber Crimes Act (CMCA) has further enhanced the multi-agency collaboration framework through the establishment of the National Computer and Cybercrimes Coordination Committee (NC4).

Director General's Perspective

The Authority, as the regulator for the ICT sector in Kenya, is mandated to develop a national cyber security management framework. We are executing this responsibility through the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC), a multi-agency national collaboration framework that is Kenya's point of contact on cyber security matters.

Since the operationalization of the National KE-CIRT/CC over seven years ago, we have noted that citizens and businesses alike are increasingly being targeted through sophisticated cyber attacks. In that 7-year period alone, we detected over 1.6 billion cyber threat attempts targeted at critical information infrastructure (CII) service providers and subsequently issued over 31 million cyber threat advisories to organisations in both the private and public sectors. Cyber threat activity has grown exponentially, and in the last 3 months alone, the National KE-CIRT/CC detected over 1.2 billion attacks. Most of these attacks exploited system vulnerabilities, which may be attributed to the proliferation of Internet of Things (IoT) devices which are inherently insecure.

Over the same period, the Digital Forensics Lab (DFL) has facilitated the investigation of 9,442 cyber crimes and 560 requests for digital forensics analysis spanning network forensics, disk forensics and mobile forensics. This has enabled the successful prosecution of various cybercrimes and other technology-related crimes. In order to fully respond to the ever-evolving cyber threat landscape, there is an urgent need to build a critical pool of cybersecurity professionals equipped with the necessary skills and tools to be on the frontline in safeguarding our country's digital assets.

This year marked the fourth consecutive year that the Authority has spearheaded activities towards national commemoration of the global October Cybersecurity Awareness Month (OCSAM). Consequently, the Authority rolled out the inaugural "CA Cybersecurity Bootcamp & Hackathon Series" targeting students in universities and other institutions of higher learning. The overarching theme of the series was, "The Paradox of Progress: Securing a Digital Nation".

For the last three years, we have collaborated with relevant stakeholders in diverse sectors, both locally and globally, to foster technical competencies at both individual and organizational levels. This is geared towards bridging the existing cybersecurity skills and capabilities gap within the Kenyan context.

In the spirit of devolution, we broadened the scope of the series this year to cover four other counties (Eldoret, Mombasa, Kisumu and Nyeri) in addition to Nairobi. We were impressed by the level of enthusiasm witnessed this year, with a record over 6,000 students expressing interest to take part in the bootcamp and hackathon competitions. The top teams in the regional bootcamp and hackathon series qualified for the national competition which was held in Nairobi, with the winning teams in the bootcamp and hackathon competition both coming from Nairobi County.

Granted, the management of cybercrime is not the sole responsibility of government. The interconnected nature of our digital world demands a unified front amongst governments, law enforcement agencies, private enterprises, and cybersecurity experts, among others. Collaboration not only enhances cyber threat detection and response capabilities but also facilitates the exchange of best practices and cyber threat intelligence, undertaking joint simulation exercises, conducting vulnerability assessments and penetration testing, all aimed at fostering resilience in the face of dynamic cyber threats.

In alignment with the Authority's 5th Strategic Plan (2023 - 2027), we will continue building our national cybersecurity capacity and capabilities by shifting our focus on emerging and dynamic technologies such as artificial intelligence and machine learning, quantum computing, post-quantum cryptography, cloud security, and cyber risk visibility, amongst others.

Mr. David Mugonyi, MBS
Director General/CEO

Global Cyber Threat Landscape Overview

Malware

Malware propagation has surged, infiltrating systems with harmful software, while phishing attacks have become even more prevalent, targeting unsuspecting users through deceptive emails and websites. Hackers commonly target to steal user logins, credit card credentials and other types of personal and financial information, as well as gain access to private databases.

** 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.*

Ransomware

Ransomware attacks have spiked considerably, leveraging sophisticated techniques to extort valuable data. The rise of cryptocurrencies is credited with helping to fuel ransomware attacks by allowing ransom demands to be paid anonymously. As a result, instances of cryptojacking have seen a sharp rise. Cryptojacking is characterized by cyber criminals hijacking third-party home or work computers to "mine" for cryptocurrency. Because mining for cryptocurrency generally requires immense amounts of computer processing power, hackers can make money by secretly piggybacking on someone else's systems.

Social Engineering

It is often said that the human element is the weakest link in cybersecurity. However, it may well be the most important. Social engineering tactics have evolved, manipulating human psychology to breach security protocols. This can expose sensitive information or lead to the execution of malicious content. Latest social engineering trends globally include business email compromise (BEC), supply chain attacks, and search engine optimization (SEO) poisoning.

Cloud Security

Cloud security attacks have intensified, exploiting vulnerabilities within cloud infrastructures. Securing cloud environments presents unique challenges due to data breaches, misconfigurations and insider threats. Specific security measures and best practices are required for effective cloud security. This may include identity and access management (IAM), data loss prevention (DLP) and incident response and forensics.

Mapping the Global Threat Landscape

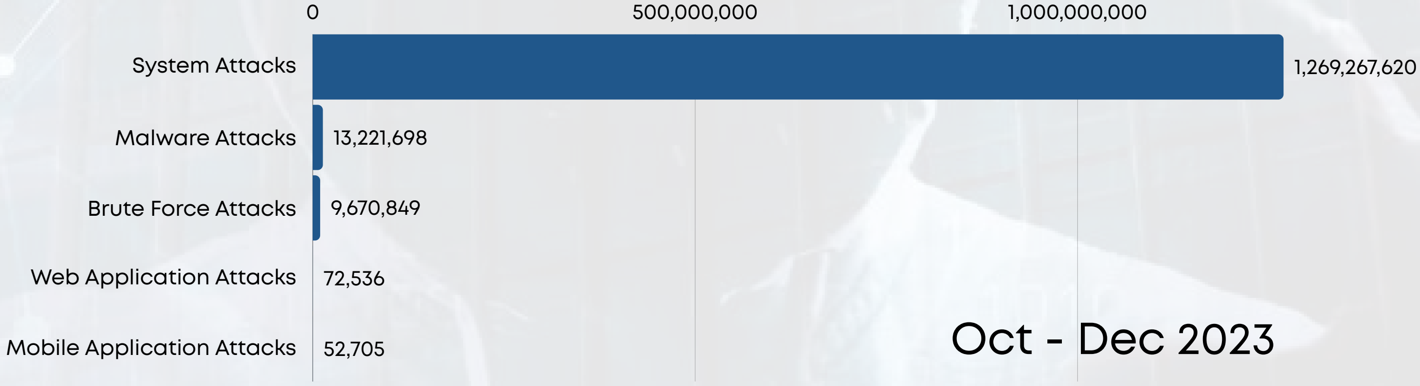
The alignment between the global cyber threat landscape and Kenya's cyber threat landscape is evident in the similarities in attack vectors, tactics and vulnerabilities affecting both individuals and organizations. This convergence underscores the universal nature of cyber threats, where trends and techniques observed on a global level are manifested and adapted within specific geolocations.

Cyber Threat Landscape Roundup

Total Cyber Threats Detected

1,292,285,408 | **943.01%**

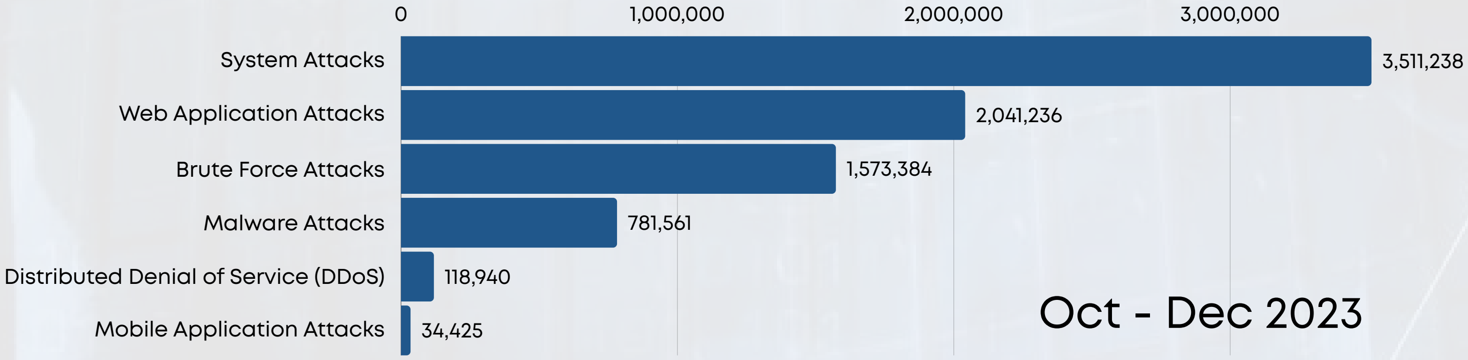
During the three month period between October and December 2023, the National KE-CIRT/CC detected over 1.2 billion cyber threat events, which represented a 943.01% increase from the 123 million threat events detected in the previous period (July to September 2023). This exponential increase is attributed to enhancement of our cyber threat monitoring capabilities and the existence of vulnerable systems due to system misconfigurations. Further, the increased exploitation of "system vulnerabilities" is also aligned to global trends, and relates to the global surge in the deployment and use of Internet of Things (IoT) devices which are inherently insecure.



Total Cyber Threat Advisories Issued

8,061,267 | **44.44%**

In response to the detected cyber threat events, the National KE-CIRT/CC issued 8,061,267 advisories between the period October to December 2023, which represented a 44.44% increase compared to the 5,580,972 advisories that were issued during the previous period, July to September 2023. There was a significant increase in the number of advisories related to system attacks during this period, with the advisories aimed at guiding users on keeping system software up to date, including regular patching of vulnerable systems, using strong passwords and multi-factor authentication, and hardening of firewall configurations.

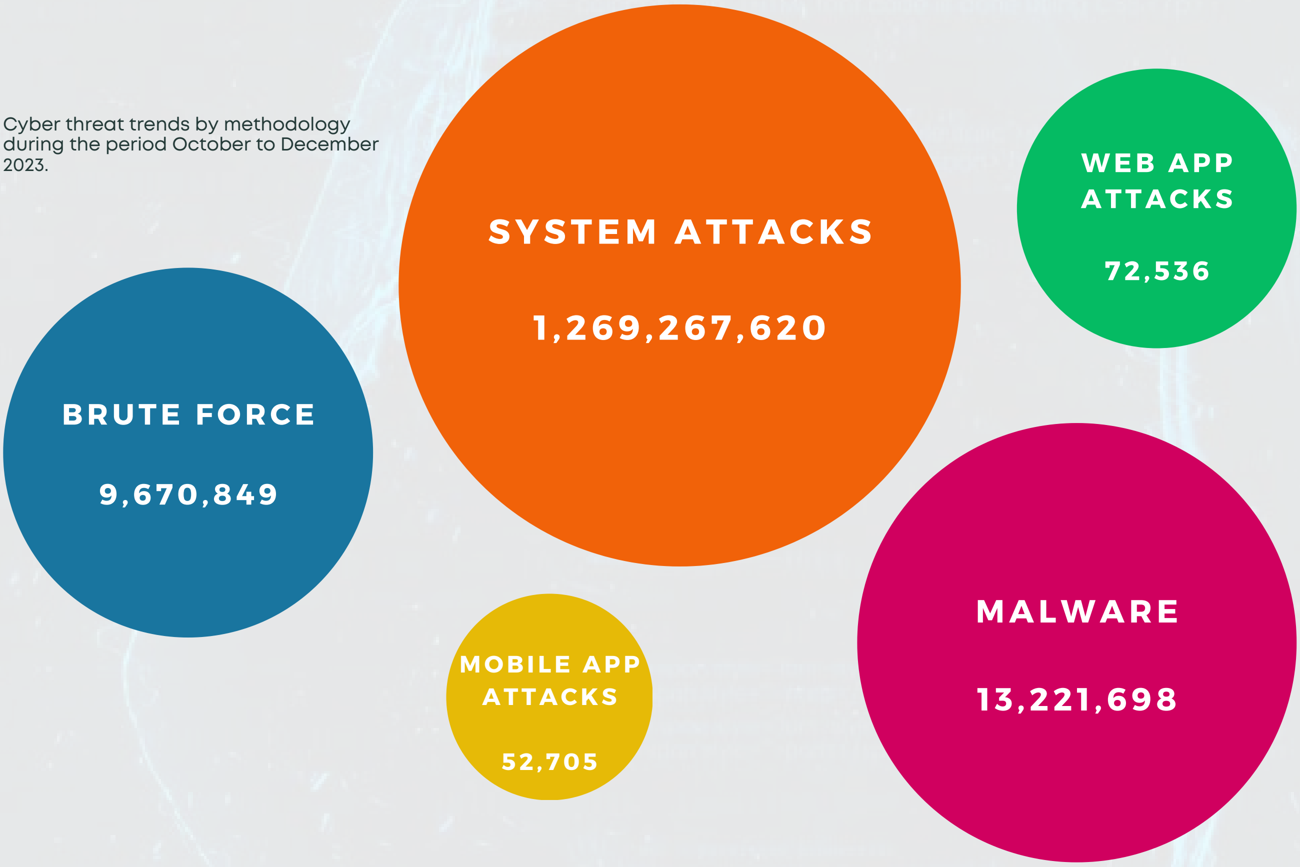


Cyber Attack Vector Trends

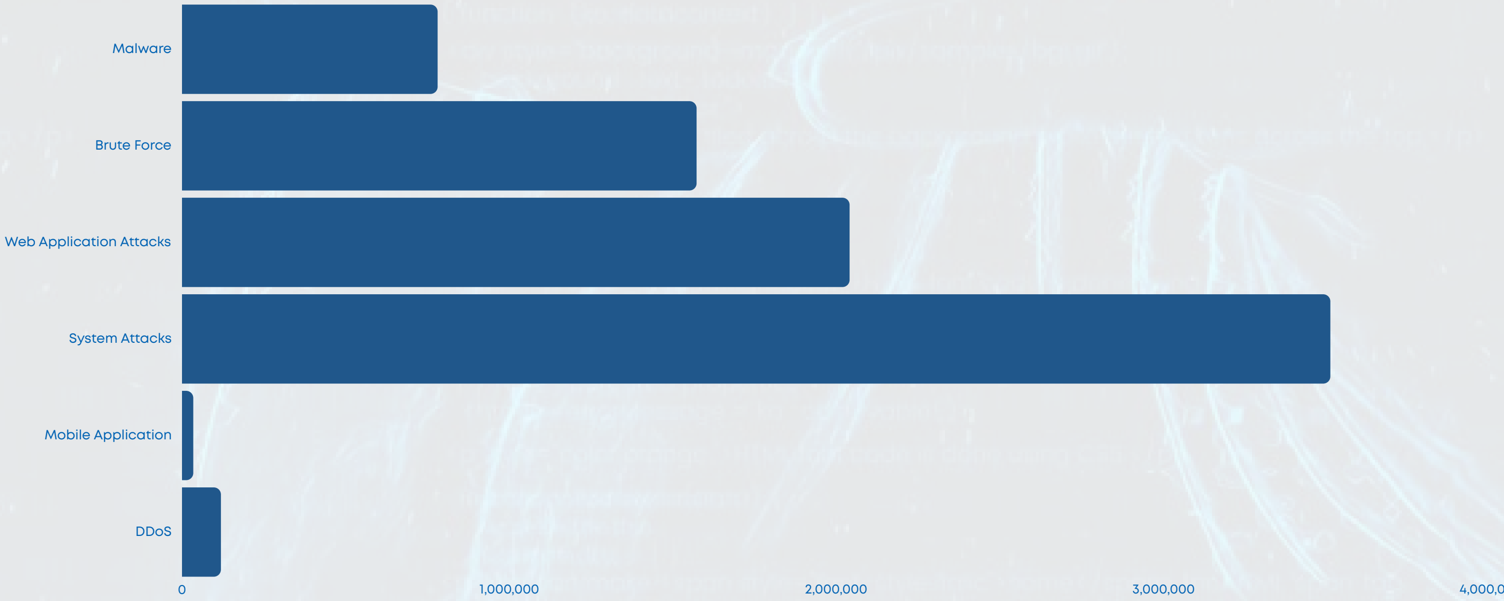
During the quarter, system misconfiguration attacks were the most prevalent, which aligns with global trends in cyber threat activity where malware attacks, and more specifically ransomware, were most rampant.

Misconfiguration attacks can be attributed to limited investment in cybersecurity, outdated systems, default system login credentials, and limited cyber risk visibility, thereby raising the susceptibility of CIIs to cyber attacks.

Cyber threat trends by methodology during the period October to December 2023.



Comparison of cyber threat advisories (per vector) issued during the period October to December 2023.



Malware Trends

Threats Detected

13,221,698

75.94%

Advisories Issued

781,561

397.87%

During the three month period between October to December 2023, the National KE-CIRT/CC detected 13,221,698 malware threat attempts targeting critical infrastructure service providers. This represented a 75.94% increase from the previous period, July to September 2023.

Majority of the attacks were targeted at organisations within the ICT sector. Attackers targeted end-user devices, web applications and networking devices belonging to Internet Service Providers (ISPs) and cloud-based services. Most attackers exploited phishing campaigns and worms which is a type of computer virus

Top Targeted Systems

- End-User Devices
- Web Applications
- Networking Devices
- Email Systems

Top Affected Industries

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

Top Targeted Exploits

- Spam email campaigns with malicious attachments
- Worm Infections
- Lockscreen Encryption Ransomware
- Critical Remote Code Execution Vulnerability

During the period, malware attacks were targeted at systems deemed to hold sensitive data such as personal and financial information. The attack objectives were mainly to steal sensitive information such as personal financial information, disrupt and sabotage systems and take control of entire networks for malicious purposes.

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

- Security by design, that is, developing software and hardware systems that are inherently secure.
- Consider deploying asset management software for managing hardware and software inventories.
- Deploying Domain-based Message Authentication, Reporting and Conformance (DMARC).
- Improve end-user cyber hygiene and awareness in organizations, through capacity building of staff.

Web Application Attack Trends

Threats Detected

72,536

31.96%

Advisories Issued

2,041,236

16.28%

During the three month period between October to December 2023, the National KE-CIRT/CC detected 72,536 web application attack attempts targeting critical infrastructure service providers. This represented a 31.96% decrease from the previous period, July to September 2023.

Majority of the attacks were targeted at government systems. 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 and TLS security misconfigurations.

Top Targeted Systems

- **Login Pages**
- **Session Cookies**
- **Database Systems**
- **Cross-site requests forgery**
- **File upload vulnerabilities**

Top Affected Industries

- **Government**
- **ISPs**
- **Cloud Services**
- **Academia**

Top Targeted Exploits

- **SSL & TLS security misconfiguration (Accessible SSL IPv4)**
- **Sinkholev4 HTTP Events**
- **Servers/Clients still support SSL 3.0 - SSLv3/Poodle**
- **CVE-2017-17215 - Honeypot HTTP Scanners**

During the period, web application attacks were targeted at systems regarded to hold sensitive data such as user credentials used to authenticate systems, financial data, and public services.
The attack objectives were mainly to make services unavailable, manipulate databases and release sensitive data for purposes of damaging organizations' reputations.

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

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

Brute Force Attack Trends

Threats Detected

9,670,849

↗ 89.57%

Advisories Issued

1,573,384

↗ 169.34%

During the three month period from October to December 2023, the National KE-CIRT/CC detected 9,670,849 brute force attack attempts majorly targeting CII providers. This represented a 89.57% increase from the previous period, July to September 2023.

Majority of the attacks were targeted at organisations within the ICT sector and government systems. 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 and user login credentials.

Top Targeted Systems

- Login Pages
- Database Servers
- Cloud Services
- Mail Servers
- Point-of-Sale (PoS) Systems
- Remote Access Systems

Top Affected Industries

- Cloud services
- 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 organizations:

- 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

52,705

94.15%

Advisories Issued

34,425

378.59%

During the three month period October to December 2023, the National KE-CIRT/CC detected 52,705 mobile application attack attempts targeting end-user devices. This represented a 94.15% increase from the previous period, July to September 2023.

Majority of the attacks were targeted at end-user devices. Attackers targeted mobile devices and Android TVs. Most attackers leverages malware to compromise end-user devices.

Top Targeted Systems

- **Mobile Devices (Android)**
- **Android TVs**
- **Set-Top Boxes**
- **Google Chromecast**

Top Affected Industries

- **Mobile devices with significant traffic emanating from China and Vietnam**
- **Set-Top Boxes**
- **Android TVs**

Top Targeted Exploits

- **Mobile Cryptominer Trojan**

During the period, there was an increase in mobile application attacks targeted at end-user devices.

The perpetrators of these attacks mainly sought to steal sensitive user data such as PII, 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 up to date.

System Attack Trends

Threats Detected

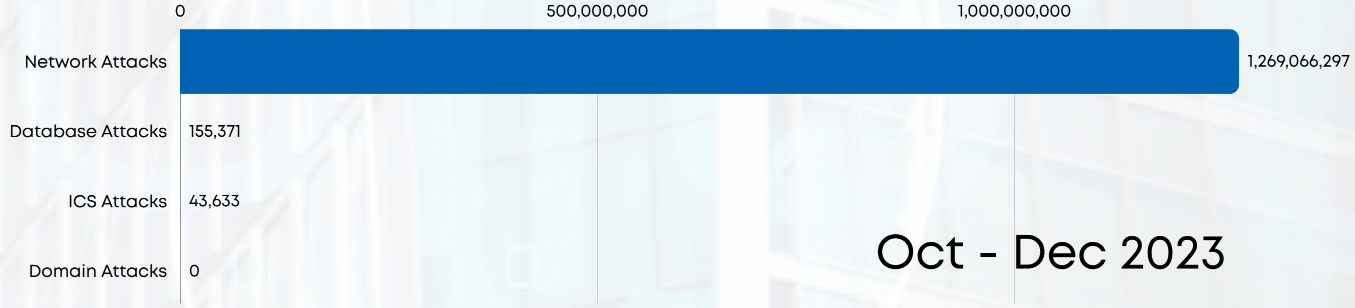
1,269,267,620

1041.94%

Advisories Issued

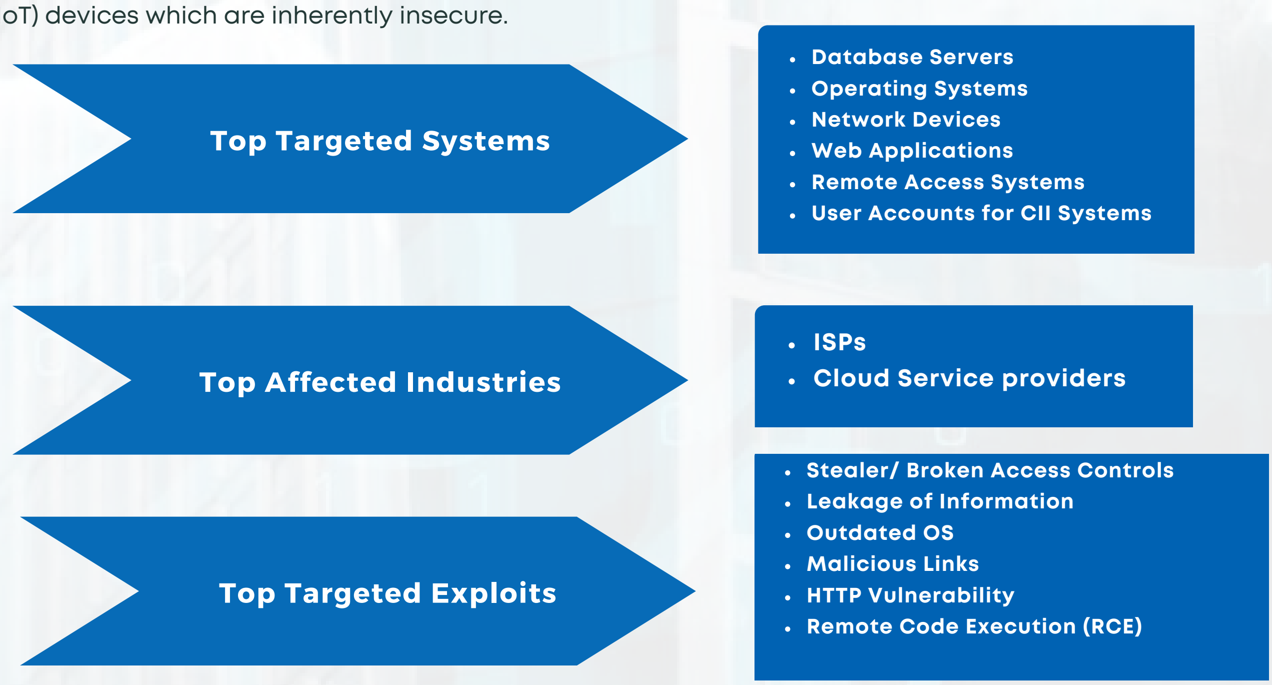
3,511,238

14.11%



Oct - Dec 2023

Majority of the attacks were targeted at organisations within the ICT sector. Attackers targeted database servers, operating systems and infrastructure belonging to various Internet Service Providers (ISPs) and cloud-based services. Most attackers exploited vulnerabilities in outdated operating systems and leaked user login credentials. The exponential growth in the exploitation of system vulnerabilities, which is a vector that has long been used by cyber threat actors, 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
- User Accounts for CII Systems

Top Affected Industries

- ISPs
- Cloud Service providers

Top Targeted Exploits

- Stealer/ Broken Access Controls
- Leakage of Information
- Outdated OS
- Malicious Links
- HTTP Vulnerability
- Remote Code Execution (RCE)

System attacks were targeted at CII systems that hold 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 to affected organizations:

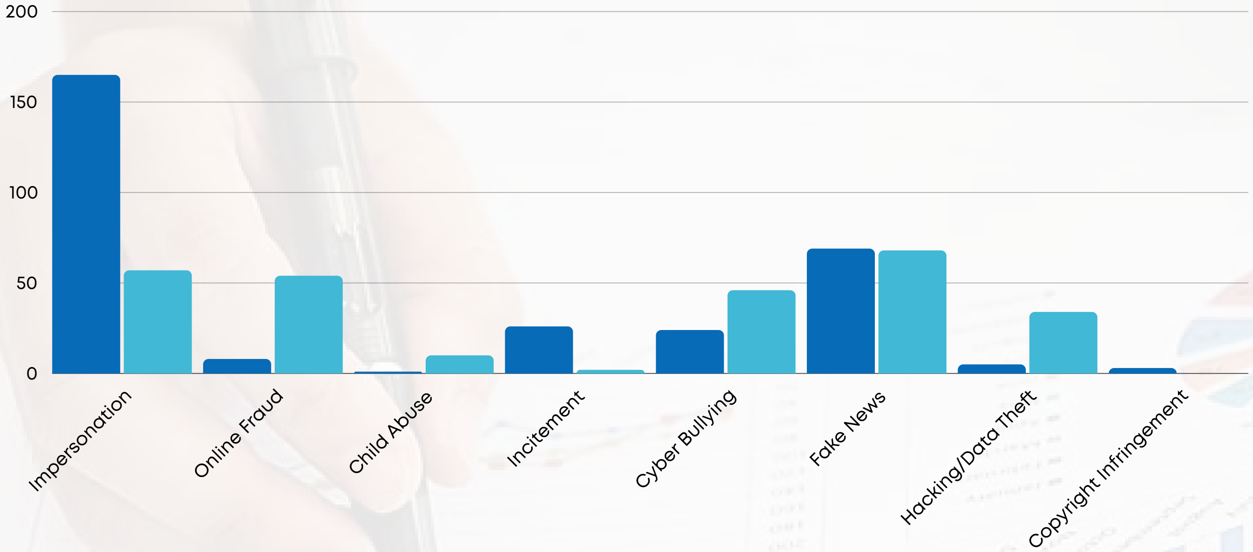
- Keep software up to date and apply patches as soon as they are released.
- Use of strong passwords and multi-factor authentication.
- Hardening of firewall configurations.

Digital Forensics and Investigations Trends

Digital Investigations

270 | **10.30%**

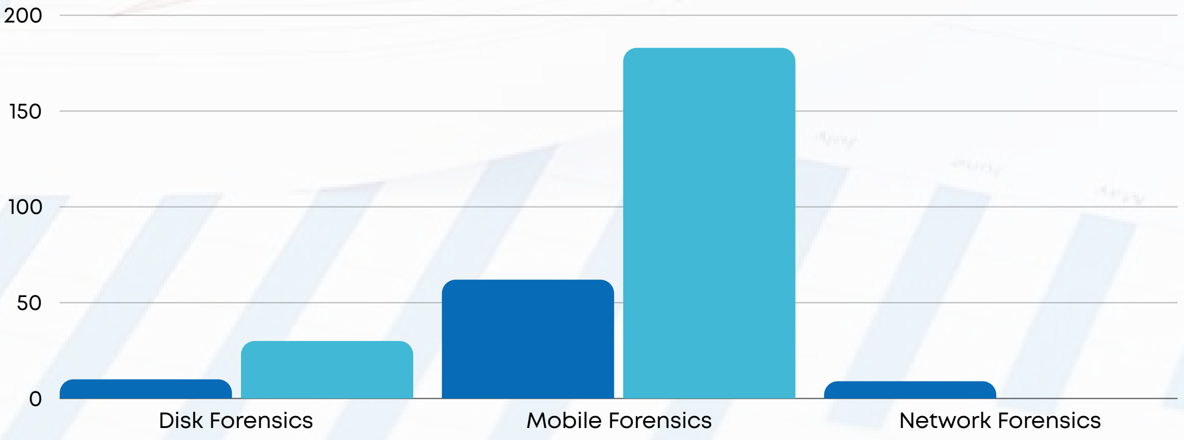
During the three month period October to December 2023, the National KE-CIRT/CC received 270 digital investigation requests. This represented a 10.30% decrease from the last period, July to September 2023.



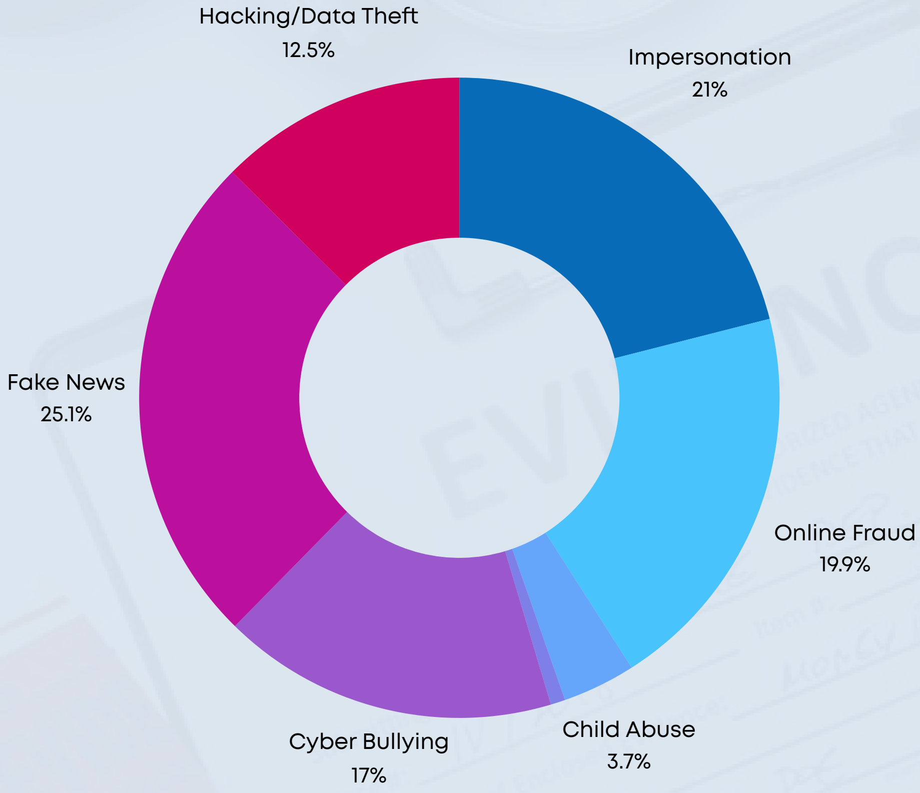
Digital Forensics

213 | **162.96%**

During the three month period October to December 2023, the National KE-CIRT/CC received 213 forensic requests. This represented a 162.96% increase from the previous period, July to September 2023.



Digital Investigations Trends



During the period, Facebook, X (formerly Twitter), Telegram, Instagram, YouTube, TikTok, Google, WhatsApp and various blogs, were the top platforms that cyber threat actors leveraged to carry out diverse online harms whose objectives included stealing sensitive data, youth radicalization, reputational damage to individuals, revenge attacks and for financial benefit.

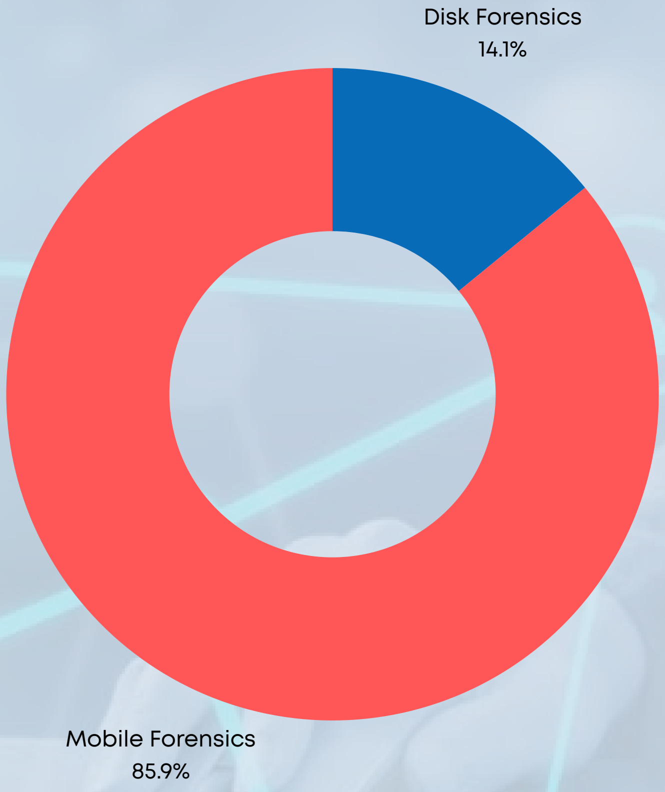
Most of the cases of impersonation reported to the National KE-CIRT/CC during the period were majorly committed on Facebook, X, Telegram, Instagram and TikTok, with the motive being mainly political, revenge attacks and for purposes of propagating fraud. Victims reported to have lost money and consumer goods through these impersonating accounts. Also notable during this period was the use of Telegram by kidnappers to demand ransom, in an attempt to force the victims' families to pay.

During this period, there was an increase in cases of incitement, cyber bullying and fake news, which were primarily carried out on Facebook, X, Telegram, Instagram, YouTube, TikTok, various blogs, and WhatsApp. The motives behind these included revenge and retaliation, youths radicalization, financial benefit, political incitement and clickbait. These had the impact of fanning ethnic tensions, political riots and violence that caused injuries to individuals, loss of life, reputation damage and financial loss to the victims.

The National KE-CIRT/CC also received reports of hacking of personal accounts such as Gmail, YouTube, X, Facebook, and WhatsApp, for purposes of data theft. There were also cases of copyright infringement, which were associated with blogs and domains, as well as Facebook, X, Telegram, Instagram, YouTube, TikTok, Google, and WhatsApp platforms.

To address these trends, the National KE-CIRT/CC has developed and rolled out a cyber awareness campaign programme to raise the level of understanding about these online harms and to empower Kenyans with the skills and knowledge needed to stay safe online.

Digital Forensics Trends



Top crimes for which digital forensics investigations are requested

- Fraud
- Robbery
- Theft
- Murder
- Impersonation
- Incitement
- Child Abuse
- Data Breach
- Cyberbullying

Main types of forensic analysis conducted

- Mobile
- Disk
- Network

National KE-CIRT/CC Updates

The National KE-CIRT/CC's mandate includes providing technical support and incident response to CIIs in the public and private sectors, as well as developing laws and regulations to improve the safety of Kenya's cyber space, thereby supporting the government's agenda of a Digitally Transformed Nation.

The following is an update on the National KE-CIRT/CC's cybersecurity management activities from October to December 2023:

Computer Misuse and Cybercrimes Act:

During the quarter, the Authority facilitated public and stakeholder consultations to gather input on the draft regulations under Computer Misuse and Cybercrimes Act, 2018

Capacity & Capability Development:

The Authority organized a training on cyber incident response, crisis management and digital forensics to enhance the level of cyber readiness and resilience amongst organizations operating critical information infrastructure. The training included simulations on response to potential cyber incidents based on the current threat landscape.

Enhancing Digital Service Provision:

In order to enhance Kenya's digital sovereignty, the Authority held discussions with various Parliamentary committees, to explore various legislative proposals and interventions that would enhance the provision of digital services.

Critical Information Infrastructure Protection:

The Authority, through the National KE-CIRT/CC, continues to facilitate the protection of critical information infrastructure by conducting information security assessments, issuing cyber threat advisories, capacity and capability development, and supporting the response to cyber incidents

45th 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 organizations across various sectors in the country. All NKCC member organisations operate CIIs. 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 emerging cyber trends, and identify a collective strategy to address these emerging issues.

The NKCC holds quarterly meetings during which the National KE-CIRT/CC updates members on emerging cyber security matters. During these meetings, the various sector CIRTs are also given an opportunity to apprise members on the emerging trends within their respective sectors. The 45th Meeting of the NKCC was held on 29th November, 2023 at the African Advanced Level Telecommunications Institute (AFRALTI), in Nairobi.

During the meeting, members discussed the rising frequency of attacks on critical systems. The transport sector alerted members of a surge in Distributed Denial of Service (DDoS) and Supply Chain Attacks mainly due to organisations having different contracts with diverse service providers. The sector also reported the attempted spoofing attacks on satellite communication systems.

The 45th NKCC meeting coincided with a training on, "Cyber Incident Response, Crisis Management and Digital Forensics" that was held from 20th November to 1st December 2023, during which over 60 members were taken through a rigorous, hands-on programme geared towards enhancing their technical skills and knowledge.

2023 October Cybersecurity Awareness Month Conference

The management of cybercrime requires the cooperation of all stakeholders in the cybersecurity value chain, in both the public and private sectors. As the ICT sector regulator, the Authority is cognizant of the critical role that collaboration plays, especially with regard to capacity building and awareness creation. It is against this background that the Authority hosted the Annual National Cyber Security Conference 2023 titled, “Building Tomorrow’s Cybersecurity Workforce” on 31st October 2023, in Nairobi.

The focus of the conference was on capacity building amongst Kenya’s cybersecurity workforce. This theme was mainly informed by the fact that an inadequate cybersecurity workforce is not only a local challenge, but also a global one. The Authority brought together diverse sectors that included academia, finance, telecommunications, energy, health, transportation, manufacturing, amongst others. Discussions at the forum centred around effective, efficient and sustainable ways of building a critical pool of local cybersecurity personnel, equipped with the skills, expertise and tools necessary to safeguard Kenya’s digital transformation.

The following are some snapshots capturing the moments and discussions from the conference:

Mr. Christopher Wambua, Ag. Director General, Communications Authority of Kenya, addressing delegates

Dr. Vincent Ngundi, Ag. Director, Cyber Security, Communications Authority of Kenya, making his remarks

Mr. Victor Guo, Huawei, President, Sub-Saharan Africa Enterprise Business Group

Mr. Keniz Agira, Chairman, Kenya Cyber Security & Forensics Association (KCSFA)

Diverse stakeholders during the 2023 October Cyber Security Awareness Month (OCSAM) Conference

Staff members of Communications Authority of Kenya follow proceedings during the event

Panel session on Cyber Security in Practice: Innovative Approaches to Develop and Identify Cyber Security Capabilities

Panel session on Navigating the Cyber Security Talent Landscape: Cyber Security Skills Needed Now and in the Future

Mr. Andy Chadwick, Head of Africa Cyber Network, at the UK's Foreign Commonwealth and Development Office (FCDO), during a panel session

Mr. Matano Ndaro (right), Director, Postal and Telecommunications Services, Communications Authority of Kenya, awards a student during the national competition

Mr. Steven Zhang (right), Deputy CEO, Huawei Kenya awards a student during the national competition

Mr. Ndaro and Mr. Zhang share a light moment during the event

Mr. William Baraza (right), Director, AFRALTI, presents a student with an award

Mr. Baraza poses for a photo with the winning team from the Mombasa bootcamp competition

Mr. Jack Zhao (right), Huawei Kenyas, awards a student during the national competition

Mr. Zhao celebrates with the winning team from the Nyeri bootcamp competition

Celebrating Excellence in Cybersecurity: 2023 Bootcamp and Hackathon Series Finale

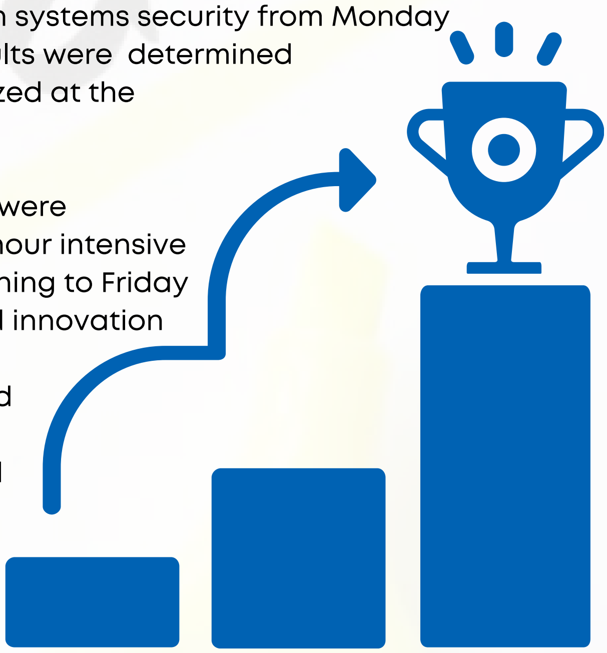
This year marked the fourth consecutive year that the Authority has spearheaded national commemorations of the October Cybersecurity Awareness Month (OCSAM) activities. Consequently, we rolled out the inaugural "CA Cybersecurity Bootcamp & Hackathon Series 2023," targeting students in universities and in other institutions of higher learning.

The bootcamp competition was an intense and hands-on learning programme, aimed at imparting core competencies and knowledge that are geared towards bridging the existing cybersecurity skills and capabilities gap within the Kenyan context. The hackathon competition, on the other hand, brought together cybersecurity enthusiasts and ethical hackers in an event featuring curated challenges in a gaming format.

In the spirit of devolution, we broadened the scope of the series this year to cover four other counties that included Eldoret, Mombasa, Kisumu and Nyeri, in addition to Nairobi. We were impressed by the level of enthusiasm witnessed this year, with a record of over 6,000 students expressing an interest to take part in the competitions.

The competition comprised two phases. The first, following closure of registration, entailed a two-week session of online classes. At the end of the two weeks, participants took an online exam. The top 30 students from the bootcamp and the top 100 students from the hackathon in each region qualified for the second phase – the onsite competition. The onsite classes for the bootcamp competition involved grouping the top 30 students in each region into teams of three. These teams attended classes on information systems security from Monday to Thursday, culminating in an exam on Friday. Results were determined collectively, and the top three groups were recognized at the regional awards ceremonies.

In the hackathon competition, the top 100 students were organized into groups of five. The hackathon, a 24-hour intensive "hacking marathon", took place from Thursday morning to Friday midday. The diverse test areas included coding and innovation challenges, security testing, database, networking, data protection, digital forensics, written exams and interpersonal and presentation skills. Similar to the bootcamp, group evaluations were conducted, and the top groups from each region progressed to the third and final phase – the national competition.



The national competition brought together the winning teams from Nairobi, Nyeri, Kisumu, Eldoret, and Mombasa in Nairobi. Held over two days, the event featured a rigorous, hands-on programme that tested the students' technical skills and knowledge, that culminated in an examination. Throughout the competition, the students showcased exceptional zeal and teamwork in their pursuit of the coveted first prize.

The following are some photos of the students from the National Bootcamp and Hackathon Competitions:

Cybersecurity experts in the making: Students fully engaged in the national bootcamp, honing their skills to defend our digital infrastructure against the ever-evolving cyber threats

Unlocking cybersecurity solutions: Engaged in the national hackathon, students strategizing, coding, and fortifying our defences in the journey towards Kenya's digital transformation

Unveiling the Champions: Hackathon and Bootcamp Winners

NAIROBI

Mr. Adam Lane (centre), Deputy CEO, Huawei Kenya, awards the bootcamp winners

Mr. Ndaro (third left), poses for a photo with the hackathon winners

KISUMU

His Excellency Dr. Mathew Owili (extreme left), Deputy Governor, Kisumu County, honours the bootcamp winners

Ms. Rosalind Muriithi (extreme left), Director, Internal Audit and Risk Assurance, Communications Authority of Kenya, lauds the hackathon winners

ELDORET

Mr. Ezra Chiloba (second left), former Director General, Communications Authority of Kenya, commends the bootcamp winners

Ms. Bhoke Christina Nchama (second left), Board Member, Communications Authority of Kenya, fetes the hackathon winners

MOMBASA

Dr. Mbwarali Kame (second right), CEC, Education and Digital Transformation, Mombasa County, applauds the bootcamp winners

Mr. Mahmud Noor (third left), Founder, Swahili Pot Hub, poses for a photo with the hackathon winners

NYERI

Mr. Victor Maina (second left), Principal Officer, Central and Eastern Regional Office, Communications Authority of Kenya, poses for a photo with the bootcamp winners

Ms. Esther Muthoni Ndung'u (centre), CEC, Gender, Youth and Social Services, Nyeri County, congratulates the hackathon winners

Youth Mentorship in Cybersecurity

The final component of the 2023 Bootcamp and Hackathon Series involved study tours for the 35 regional finalists from Nairobi, Mombasa, Eldoret, Nyeri and Kisumu, who had competed in both the Bootcamp and Hackathon competition of the series. This phase was carried out in partnership with various organizations in both public and private sector.

The study tour served as a mentorship opportunity for the finalists, and involved study visits to partnering organizations. This gave the students first-hand practical experience on cybersecurity operations as a way of translating theory to practice. The partnering organizations for the 2023 series included the ICT Authority (ICTA), Konza Technopolis Development Authority (KoTDA), Kenya Network Information Centre (KENIC), African Advanced Level Telecommunications Institute (AFRALTI), Technology Service Providers of Kenya (TESPOK), Kenya Bankers Association (KBA), Safaricom PLC, Huawei Technologies Kenya, Liquid Intelligent Technologies and Airtel Networks Kenya.

The winning teams from the regional bootcamp and hackathon at the Authority's premises

Students from the national competition at the National KE-CIRT/CC Monitoring Room

Staff from Safaricom PLC mentoring the students

Mr. George Njuguna, CIO at Safaricom PLC, giving students life lessons about the corporate world

The students on a study tour at Safaricom PLC's IT Security Operation Center (SOC) along Waiyaki Way, Nairobi

Mr. Njuguna, Safaricom PLC, takes a question from a student

Students at the Kenya Network Information Centre (KeNIC) offices in Nairobi

A brief talk on the history of Konza Technopolis Development Authority (KoTDA) in Machakos County

Ms. Jessica Wanjohi (right), from Communications Authority of Kenya, with a staff member from KoTDA

The students from the national competition pose for a photo in front of the KoTDA offices

Staff members from CA and and Huawei Kenya pose for a photo with the students at the Huawei Training Center, at AFRALTI, Nairobi

A staff member from Huawei Kenya performs a demo of an equipment at the Huawei Training Center

Mr. Fidelis Muia, Director of Technical Services, Kenya Bankers Association (KBA), counselling the students

Mr. Muia poses for a group photo with students at the KBA offices in Nairobi

Mr. Emmanuel Emurugat from ICT Authority (ICTA), explaining to the students about the Presidential DigiTalent Programme (PDTP)

Staff from CA and AFRALTI pose for a group photo with the students at AFRALTI grounds

Future Insights on Cyberecurity

In enhancing our national cybersecurity readiness and resilience capabilities, we shift our focus on leveraging the new frontier of emerging trends, going into 2024 and beyond.

Artificial intelligence and machine learning technologies possess immense transformative capabilities in cyber threat detection and response. Simultaneously, the development of quantum computing has resulted in post-quantum cryptography becoming a necessity in order to protect sensitive data from the possible interruption in encryption techniques.

Cloud security remains an ever-evolving landscape. As a result, we must remain vigilant and adaptable in protecting data as it moves across the current countless digital spheres. To support these efforts, there is an urgent need for increased cyber risk visibility, which is a crucial component that enables proactive cyber threat mitigation.

These domains are the centre of our strategic focus as we move forward, bringing our cybersecurity initiatives into a new era defined by innovation, versatility, and unrelenting resilience.

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