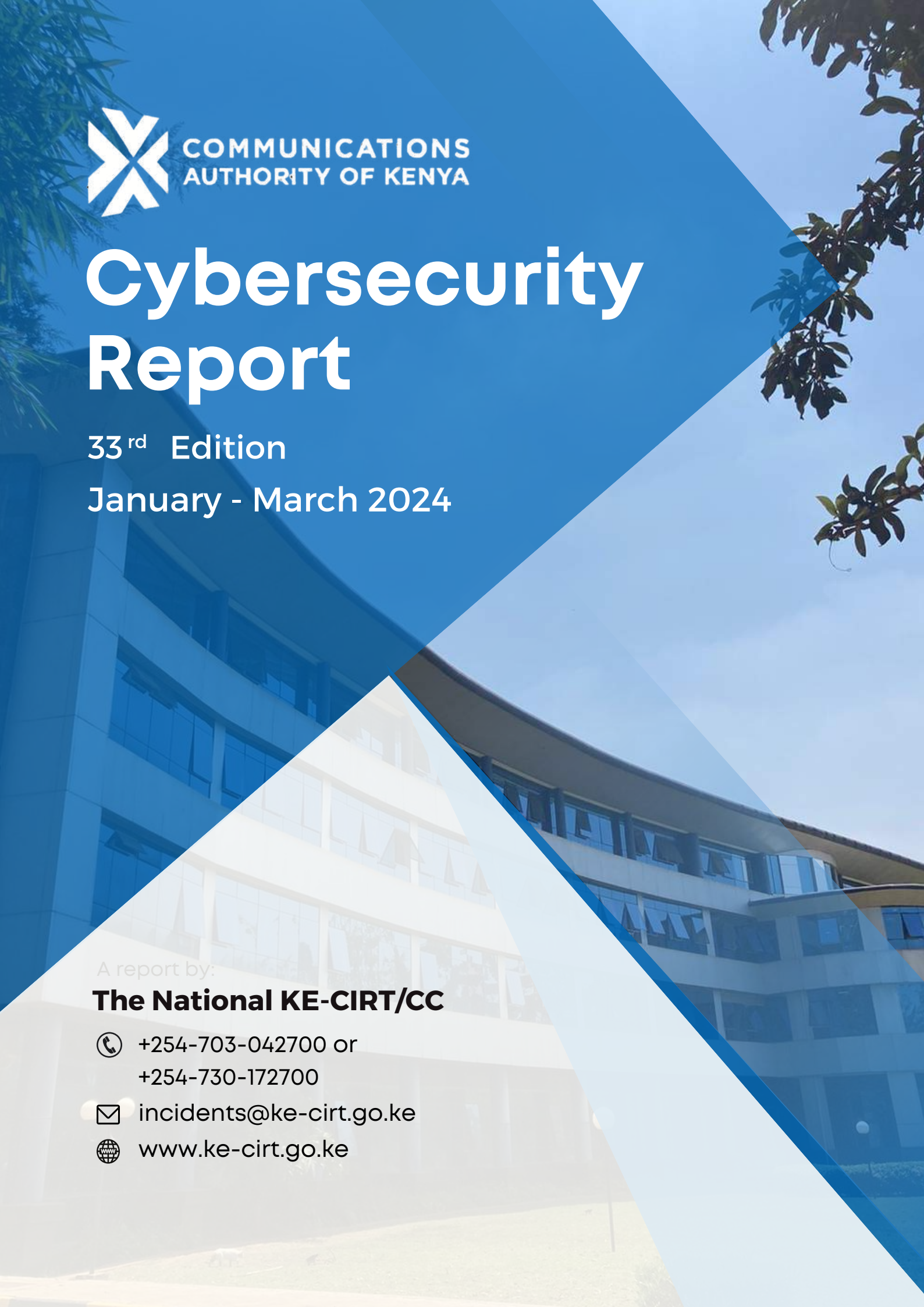
COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

33rd Edition

January - March 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 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) 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).

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, 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) of 2018 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 cyber threat landscape has evolved tremendously over the past few years, driven by rapid technological advancements and global interconnectivity. The threat landscape is the full range of known and potential cybersecurity risks that could impact particular industries, user groups or organisations. As new cyber threats emerge, the threat landscape changes accordingly.

The dynamism in the cyber threat landscape is attributed to various factors including increasingly sophisticated tools and threat vectors, greater reliance on cloud services and related technologies, improved technical skills and finances to drive cyber attacks, ongoing global conflicts and related actions by state actors, faster software releases with added functionality, new hardware development such as Internet of Things (IoT) devices, amongst others.

Over the period January - March 2024, the National KE-CIRT/CC detected over 900 million cyber threats. 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) received over 200 requests for digital forensic investigations. The majority of these requests are attributed to online abuse and online fraud cases.

Online abuse encompasses a range of malicious activities, including cyberbullying and harassment. Similarly, online fraud poses significant financial risks with cybercriminals leveraging diverse threat vectors such as phishing and identity theft to deceive victims and illicitly obtain money or sensitive information. The DFL has been instrumental in the successful prosecution of various cybercrimes and other technology-related offences.

The Authority hosted the 2024 Annual National Public Key Infrastructure (NPKI) Forum which brought together stakeholders from across the digital certification and digital trust services value chain. The forum was aimed at enhancing awareness on the digital certification and digital trust ecosystems, and to explore how digital trust services can be applied towards the realization of Kenya's national digital transformation agenda. This year, the forum was held on 19th - 20th March, 2024 at the Safari Park Hotel & Casino, Nairobi under the theme, "Building Trust in a Digital World: The Future of the NPKI".

As a key outcome of the forum, delegates had the privilege of witnessing, "The Nairobi Declaration on the Formation of the Africa Public Key Infrastructure (PKI) forum". This was a collective resolve by select African countries that included South Africa, Uganda, Ivory Coast, Ghana and Kenya, to advance the implementation and utilization of PKI in Africa. This will lay the foundation for a secure, inclusive, and prosperous digital future for all Africans. Going into the future, it is proposed that hosting of the forum be held on rotational basis from country-to-country. As a follow up to this, Ghana graciously offered to host the inaugural African PKI Forum in Accra, in 2025.

The 2024 edition of the Safer Internet Day took place on 6th February 2024 under the slogan, "Together for a better Internet.". The Authority joined the rest of the world in marking this day through various social media campaigns and initiatives. The Safer Internet Day is an annual event that is commemorated globally to promote safer and more responsible use of online technology and mobile devices, especially amongst children and the youth. It aims to raise awareness about online safety concerns such as cyberbullying, identity theft, privacy risks, and the proliferation of inappropriate content.

In alignment with the 5th Strategic Plan (2023 - 2027), the Authority will continue building our national cybersecurity capacities and capabilities by shifting our focus on emerging cybersecurity concerns such as ransomware-as-a-service (RaaS), AI-driven cyber attacks, supply chain attacks, amongst others.

Given the cross-border nature of cyber threats, the Authority will continue to foster frameworks for collaboration to facilitate sharing of threat intelligence and technical assistance, thus mitigating cyber threats on a local and global scale.

Mr. David Mugonyi, EBS
Director General/CEO

Global Cyber Threat Landscape Overview

Ransomware-as-a-Service (RaaS)

** 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 as a service (RaaS) enables individuals to purchase or rent ransomware software, tools, and infrastructure to carry out cyberattacks without needing advanced technical skills. The increased adoption of RaaS is attributed to the continued evolution and sophistication of ransomware techniques, attracting more actors into the cybercrime ecosystem seeking financial gain through extortion.

AI-Driven Attacks

AI-driven attacks utilise artificial intelligence techniques to automate and enhance various stages of cyberattacks, such as reconnaissance, exploitation, and evasion. Cyber threat actors have been observed leveraging AI-driven attacks to extend their social engineering efforts, spread malware, carry out adversarial attacks, and compromise critical information infrastructure and Internet of Things (IoT) devices by leveraging the following:

- Increased sophistication: AI-powered attacks are more intricate, bypassing traditional security measures through techniques such as sophisticated social engineering techniques and exploiting zero-day vulnerabilities. These attacks involve creating deepfakes to impersonate executives or tailoring phishing emails with higher personalisation, making them harder to detect.
- Automation and speed: AI is being used to automate tasks in cyberattacks, enabling rapid execution and wider reach. This involves quicker identification of targets, deployment of malware, and data exfiltration.
- Evolving techniques: AI is being employed to develop new types of malware that can learn and adapt to security defences. This involves techniques such as self-replication or mutation, making them harder to contain and eradicate.
- Emerging threats: The development of adversarial AI is being used to specifically target and defeat other AI-powered security systems.

**Adversarial AI refers to the technique of intentionally manipulating AI systems by introducing carefully crafted input data. That is often imperceptible to humans but can cause AI models to make incorrect predictions or classifications.*

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

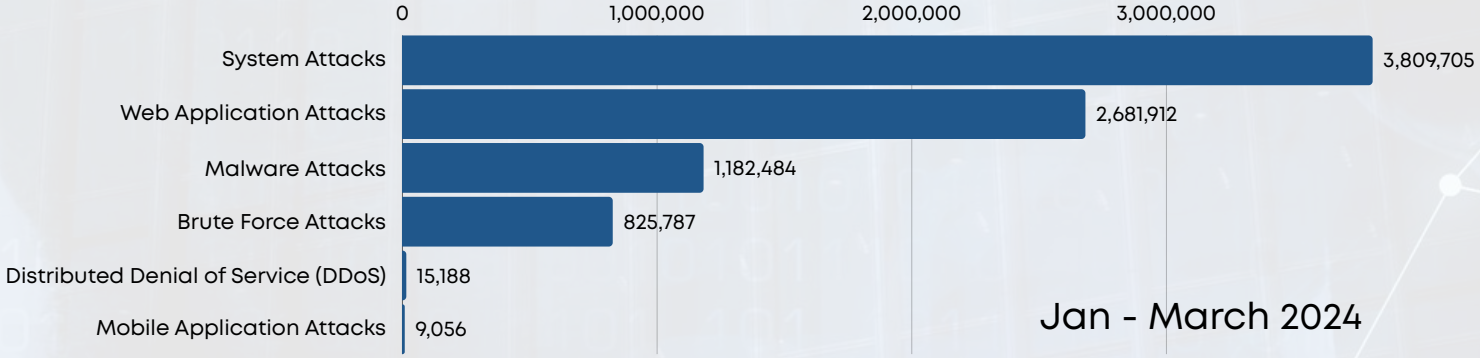
971,440,345 | **- 24.83%**

During the three-month period between January and March 2024, the National KE-CIRT/CC detected over 900 million cyber threat events, which represented a 24.83% decrease from the 1.2 billion threat events detected in the previous period (October to December 2023). In response to the increasing frequency of cyber threats, we enhanced the dissemination of cyber threat advisories to critical information infrastructure sectors. The continued 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

8,524,407 | **5.75%**

In response to the detected cyber threat events, the National KE-CIRT/CC issued 8,524,407 advisories between the period January to March 2024, which represented a 5.75% increase compared to the 8,061,267 advisories that were issued during the previous period, October to December 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.

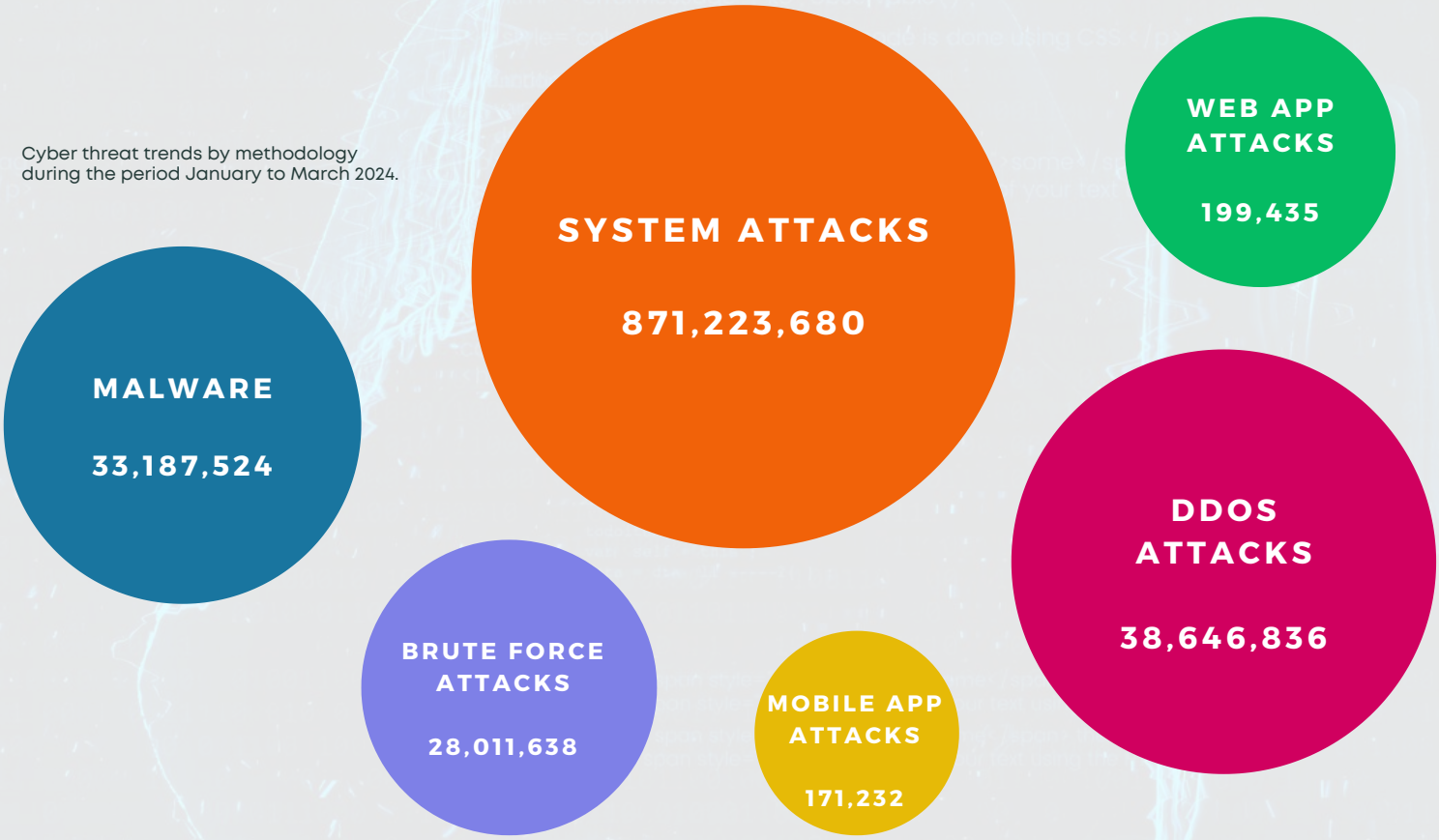


Cyber Attack Vector Trends

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.

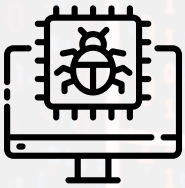
Misconfiguration attacks can be attributed to limited investment in cybersecurity, outdated systems, default system login credentials, and limited cyber risk visibility, thereby raising the susceptibility of the critical information infrastructure sectors to cyber attacks.

Cyber threat trends by methodology during the period January to March 2024.



Comparison of cyber threat advisories (per vector) issued during the period January to March 2024.

Malware Trends



Threats Detected

33,187,524

151.01%

Advisories Issued

1,182,484

51.30%

During the three month period between January to March 2024, the National KE-CIRT/CC detected 33,187,524 malware threat attempts targeting at the critical information infrastructure sector. This represented a 151.01% increase from the previous period, October to December 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, 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

- Critical Remote Code Execution Vulnerabilities:
  - CVE-2017-0199: Remote code execution bug in Microsoft Office often used by banking and spyware trojans such as Dridex.
  - CVE-2019-0604: A SharePoint remote code execution flaw.
  - CVE-2017-0143: A remote code execution vulnerability in Microsoft SMB
  - CVE-2017-8759: A remote code execution vulnerability in the Microsoft .NET Framework.
  - CVE-2018-4878: A vulnerability in early versions of Adobe Flash Player.

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 organisations, through capacity building of staff.

Web Application Attack Trends

Threats Detected

199,435

174.95%

Advisories Issued

2,681,912

31.39%

During the three month period between January to March 2024, the National KE-CIRT/CC detected 199,435 web application attack attempts targeting at the critical information infrastructure sector. This represented a 174.95% increase from the previous period, October to December 2023.

Majority of the attacks were targeted at 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 and 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**
- **ISPs**
- **Cloud Services**
- **Academia**

Top Targeted Exploits

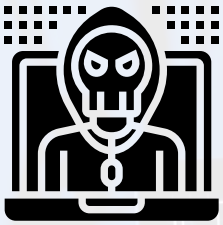
- **Broken access control**
- **Cryptographic failures**
- **Injection**
- **Insecure design**
- **Security misconfiguration**
- **Vulnerable and outdated components**
- **Identification and authentication**

During the period, web application attacks 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

28,011,638

189.65%

Advisories Issued

825,787

47.52%

During the three month period from January to March 2024, the National KE-CIRT/CC detected 28,011,638 brute force attack attempts majorly targeting CII providers. This represented a 189.65% increase from the previous period, October to December 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

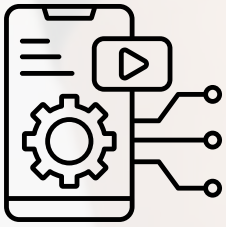
- Exposed Remote Desktop Protocol (RDP)
- Credential Brute-Forcing
- Credential Spoofing
- Credential Sniffing

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

171,232

224.89%

Advisories Issued

9,056

73.69%

During the three month period January to March 2024, the National KE-CIRT/CC detected 171,232 mobile application attack attempts targeting end-user devices. This represented a 224.89% increase from the previous period, October to December 2023.

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

Top Targeted Systems

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

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

871,223,680

31.36%

Advisories Issued

3,809,705

8.50%

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 continued prevalence 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 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 to affected organizations:

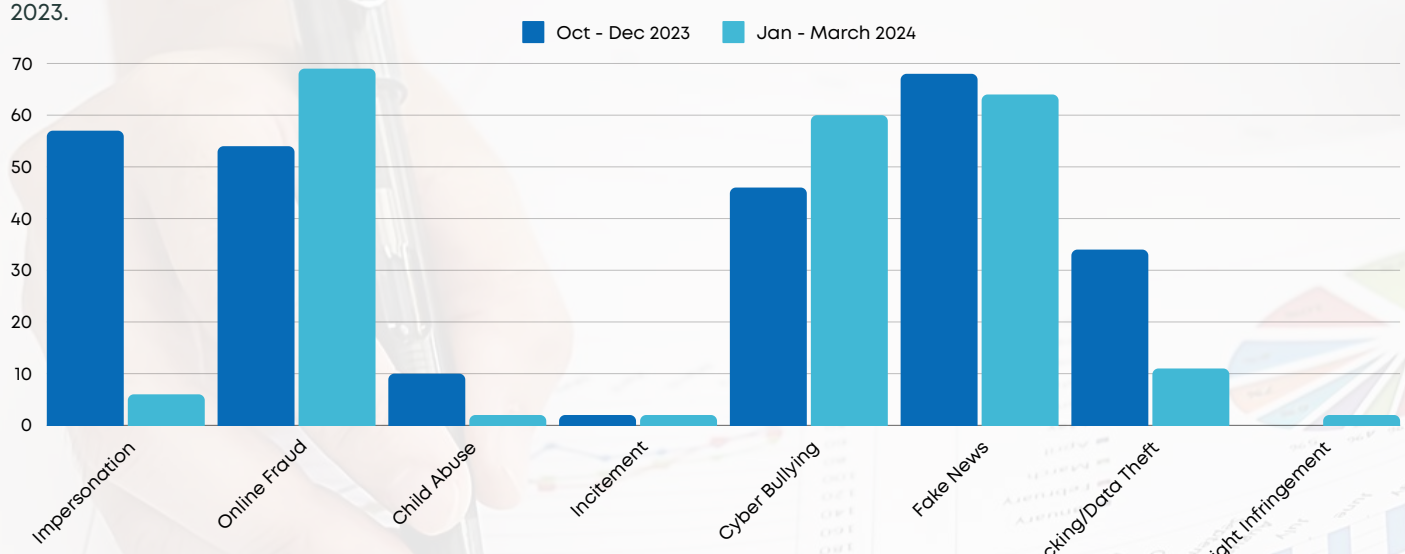
- Keep software up to date and apply patches as soon as they are released.
- Use of strong passwords and multi-factor authentication.
- Hardening of firewall configurations.

Digital Forensics and Investigations Trends

Digital Investigations

216 | **20.00%**

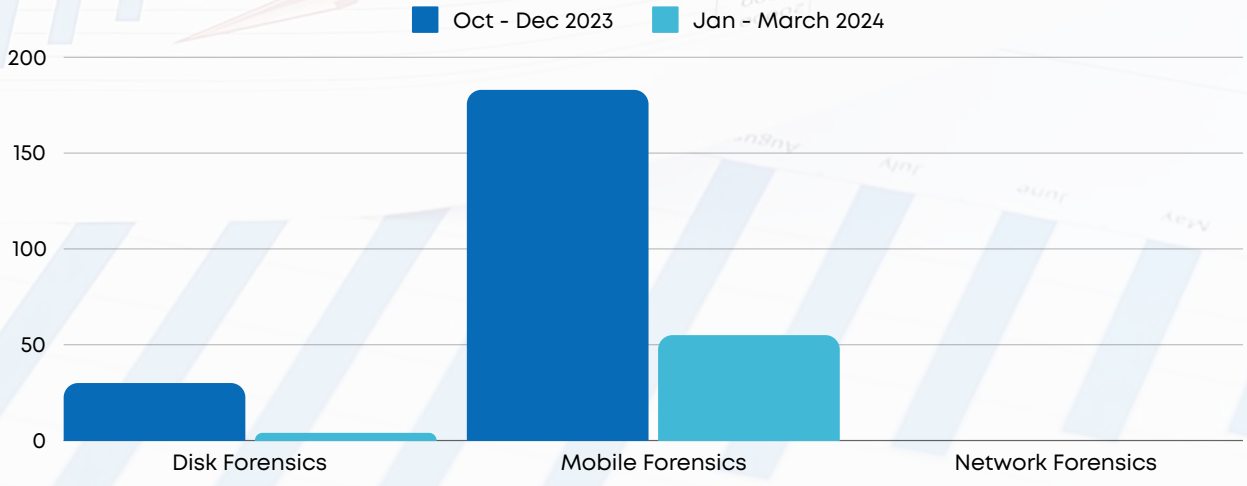
During the three month period January to March 2024, the National KE-CIRT/CC received 216 digital investigation requests. This represented a 20.00% decrease from the last period, October to December 2023.



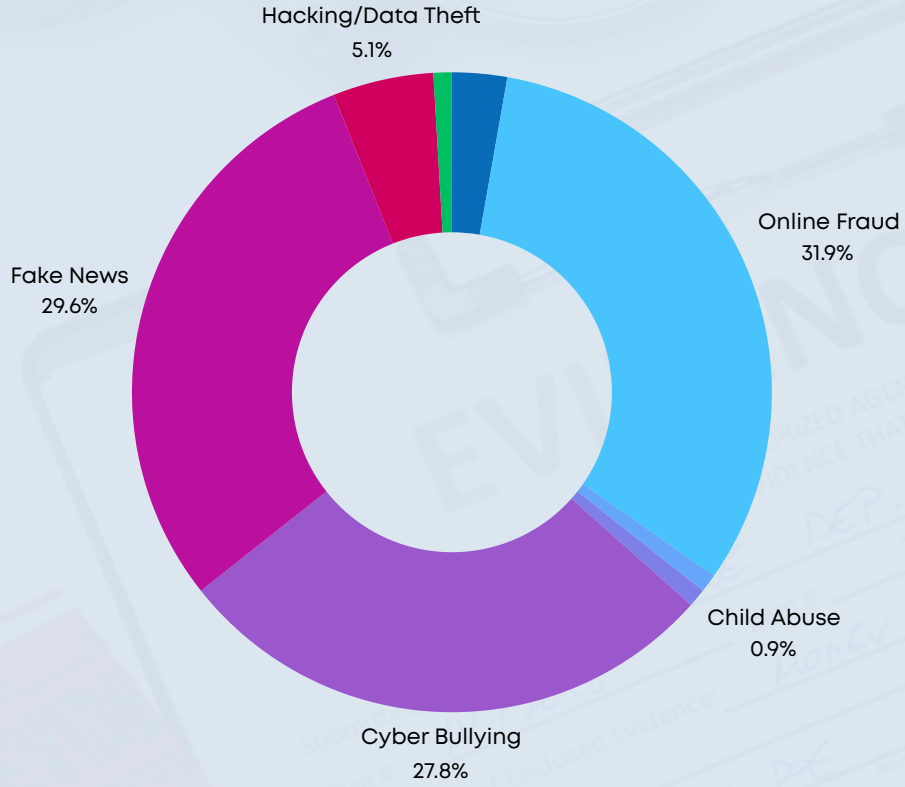
Digital Forensics

59 | **72.30%**

During the three month period January to March 2024, the National KE-CIRT/CC received 59 forensic requests. This represented a 72.30% decrease from the previous period, October to December 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.

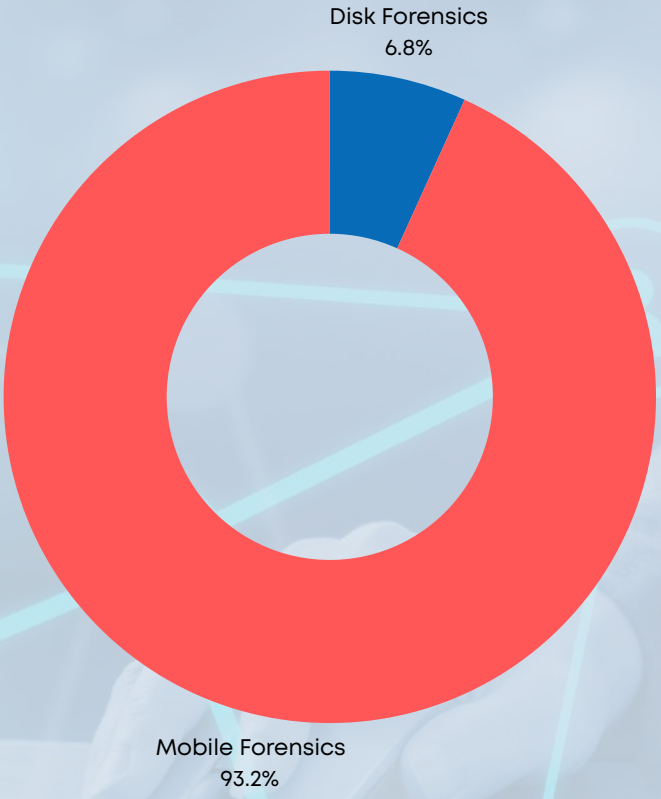
Most of the cases of impersonation reported to the National KE-CIRT/CC during the period were majorly committed on Facebook, X, Telegram, Instagram and TikTok, with the motive being mainly political, revenge attacks and for purposes of propagating fraud. Victims reported to have lost money and consumer 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

Updates from the National KE-CIRT/CC

The Kenya Information and Communications Act 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 from January to March 2024:

The Computer Misuse & Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations

On 9th February 2024, the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations came into effect, vide Gazette Notice Number 44. The Authority played a pivotal role in the development of these regulations, providing logistical support and technical expertise to ensure the formulation of a comprehensive regulatory framework.

The enactment of these regulations reinforces the Authority's critical role as a member of the National Computer and Cybercrimes Co-ordination Committee (NC4) and will go a long way in building the capacity of both public and private sector institutions, including the telecommunications, banking & finance, transportation and energy sectors. This will enhance the safeguarding of critical information infrastructure from cyber threats therefore improving national cybersecurity readiness and resilience. The regulations effectively operationalize provisions of the Computer Misuse and Cybercrimes Act of 2018.

Capability and Capacity Development

During the month of March, the Authority hosted a training programme on cyber threat intelligence (CTI). The programme was aimed at equipping technical officers within the critical information infrastructure (CII) sector with the necessary skills to identify and counter evolving cyber threats in a rapidly evolving digital landscape.

The CII sector refers to various systems, networks and assets that are essential for the functioning of Kenya's economy, security and public welfare such as energy, transportation, finance, healthcare, telecommunications and government services.

Trainees during the Cyber Threat Intelligence (CTI) training programmes in Nairobi, pose for a photo

2024 Annual National Public Key Infrastructure (NPKI) Forum

The Authority hosted the 2024 Annual National Public Key Infrastructure (NPKI) Forum which brought together stakeholders from across the digital certification and digital trust services value chain. The forum was aimed at enhancing awareness on the digital certification and digital trust ecosystems, and to explore how digital trust services can be applied towards the realization of Kenya's national digital transformation agenda. This year, the forum was held on 19th - 20th March, 2024 at the Safari Park Hotel & Casino, Nairobi under the theme, *"Building Trust in a Digital World: The Future of the NPKI"*.

Amongst the attendees included African ICT regulators, the Asian and European PKI consortiums, critical infrastructure sector representatives, local standards bodies and training institutions, various industry regulators, innovators and researchers, the civil society, law enforcement agencies, amongst others. The forum was attended by over 200 delegates.

Here's a glimpse into the insightful conversations and collaborative spirit that defined the 2024 Annual NPKI Forum:

Prof. Edward Kisiang'ani, CBS, Ph.D, Principal Secretary, State Department for Broadcasting & Telecommunications, Ministry of Information, Communications and the Digital Economy, delivering the keynote address on behalf of the Cabinet Secretary.

Ms. Mary Mungai, CBS, Chairperson of the Board of Directors, Communications Authority of Kenya, delivering her statement.

Mr. David Mugonyi, EBS, Director General/CEO, Communications Authority of Kenya, making his remarks.

Mr. Christopher Wambua, Director, Corporate Communications, Communications Authority of Kenya, welcoming delegates during the official opening ceremony.

Dr. Vincent Ngundi, Ag. Director, Cyber Security, Communications Authority of Kenya, making his presentation on the role of the NPKI in the government's digital transformation agenda.

Mr. Tito Alai, Chairman at Tendaworld (Kenya) Limited, a licensed and accredited electronic certification service provider (E-CSP) in Kenya, speaking at the forum.

Mr. Arvind Srinivasan, Senior Vice President, International Sales & Strategy at eMudhra Technologies Limited (India), a licensed and accredited electronic certification service provider (E-CSP) in Kenya, delivering his remarks.

Prof. George Dimitrov, Chairman of the Board of Directors & Founder at Evrotrust Technologies AD (Bulgaria), a licensed and accredited electronic certification service provider (E-CSP) in Kenya, making his keynote address.

Mr. Philip Irode, Deputy Director, Information Security at ICT Authority - the Government Certification Authority (GCA) in Kenya, delivering his presentation.

Ms. Mutheu Khimulu, Cybersecurity Lawyer and Google Women Techmakers Ambassador, speaking about governance and policy considerations in implementing of the NPKI.

As a key outcome of the forum, delegates had the privilege of witnessing, "The Nairobi Declaration on the Formation of the Africa Public Key Infrastructure (PKI) forum". This was a collective resolve by select African countries that included South Africa, Uganda, Ivory Coast, Ghana and Kenya, to advance the implementation and utilization of PKI in Africa. This will lay the foundation for a secure, inclusive, and prosperous digital future for all Africans. Going into the future, it is proposed that hosting of the forum be held on rotational basis from country-to-country. As a follow up to this, Ghana graciously offered to host the inaugural African PKI Forum in Accra, in 2025.

Overview of the panel sessions: Snapshots of the discussions.

46th 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 organisations across various sectors in the country. All NKCC member organisations operate critical information infrastructure. 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 used by diverse threat actors. During these meetings, the various sectoral computer incident response teams (CIRTs) are also granted an opportunity to apprise members on the trends and patterns observed within their respective domains. The 46th Meeting of the NKCC was held on 20th March 2024 at the Safari Park Hotel & Casino, in Nairobi.

During the meeting, members discussed the rising frequency of attacks on critical systems. The academia sector reported a surge in distributed denial-of-service (DDoS) attacks specifically targeted at the domain name system (DNS) and local area network (LAN) management systems. The criticality of the DNS to the proper functioning of the Internet and vulnerabilities in DNS protocols were highlighted as key contributors to the DNS remaining an attractive target for threat actors seeking to disrupt online services or to exfiltrate data.

The telecommunications sector also reported an increase in DDoS attacks, emphasizing the need for organisations to implement a zero-trust network architecture. Further to this, members deliberated and agreed that there's need for continued user awareness training on common cyber threat vectors such as phishing, business email compromise, and other forms of social engineering.

The academia sector further informed members about an ongoing capacity building programme targeted at law enforcement officers. This programme is tailored for frontline officers who receive cyber incident reports at police stations, and is aimed at equipping them with the necessary skills and knowledge that will assist in the investigation and prosecution of cybercrime offences, such as the handling of digital evidence and collaborating with relevant stakeholders.

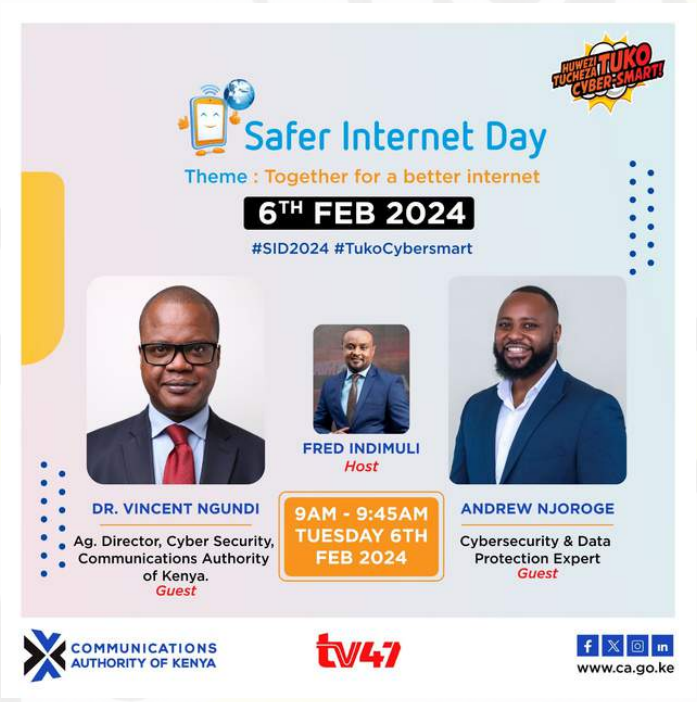
The 46th NKCC meeting was held on the sidelines of the 2024 Annual NPKI Forum.

2024 Safer Internet Day

The Safer Internet Day is an annual event that is commemorated globally to promote safer and more responsible use of online technology and mobile devices, especially amongst children and the youth. It aims to raise awareness about online safety concerns such as cyberbullying, identity theft, privacy risks, and the proliferation of inappropriate content. Through various activities, campaigns and initiatives, the Safer Internet Day encourages individuals, parents, educators, policymakers and industry stakeholders to work together to create a safer and better Internet for all users. It is usually celebrated on the second Tuesday of February each year under the slogan, "Together for a better Internet."

The 2024 edition of Safer Internet Day took place on 6th February 2024. The Authority joined the rest of the world in marking this day through various social media campaigns and participation in a live television interview on *tv47*. The Authority was represented in the day's discussions by Dr. Vincent Ngundi, Ag. Director, Cyber Security and the Head of the National KE-CIRT/CC.

Dr. Ngundi explained that the human element remains the weakest link in cyber safety and security matters, thus there's need for concerted efforts by organisations in both the public and private sectors, in creating awareness and building the capacity of consumers of ICT services.



He noted that data privacy concerns are not only a problem within the Kenyan context but have evolved into a global one. This is particularly so because businesses have prioritised profit-oriented strategies whereby the collection and use of personal data has become essential to commercial operations.

Addressing these challenges therefore requires a balanced approach that respects individual privacy rights as stipulated under our Kenyan laws, while also supporting innovation and socioeconomic development.

Dr. Ngundi informed viewers that the government of Kenya is actively engaged in securing critical systems through public-private partnerships (PPPs) since a vast majority of systems that are deemed critical in nature, are privately-owned and managed. By acknowledging the challenges posed by the ever-evolving cyber threat landscape and the interconnected nature of our digital infrastructure, collaboration between government agencies, the private sector and other stakeholders is essential to effectively safeguarding critical systems.

In his concluding remarks, Dr. Ngundi stated that the Authority's Child Online Protection (COP) programme is aimed at bringing together various stakeholders to equip children, parents, guardians, and teachers with the necessary skills and knowledge to enable safe use of the Internet, and to minimise or eliminate exposure to online risks and vulnerabilities. He added that the government is proactively addressing the protection of children and youth through legislative approaches. These approaches are aimed at empowering the relevant authorities such as the law enforcement agencies, to address emerging challenges, enforce accountability and provide the necessary protection to mitigate risks faced by children and youth as they navigate the cyberspace.

Empowering Women in Cybersecurity

The cybersecurity sector is facing a significant gender gap, with women being underrepresented in various roles within the industry. Despite efforts to promote diversity and inclusion, women remain underrepresented in cybersecurity professions, including technical roles, leadership positions and decision-making roles.

To address this gap, the Authority has partnered with Acyberschool in supporting the “Top 100 Cybersecurity Women to Watch in Africa”. This initiative aims to bridge this gender gap through spotlighting women's achievements in cybersecurity as practitioners, students, educators, amongst others, thus enriching the field with diverse perspectives for a more resilient cybersecurity ecosystem and to inspire the next generation of female cybersecurity professionals.

Nominations for the awards kicked off on 30th January 2024, marking the beginning of an exciting journey to recognise the outstanding contribution by women in cybersecurity. The nominations were reserved for Africans but non-Africans were eligible to nominate their preferred candidates. After an intense period, nominations officially closed on 1st March 2024. The unveiling of this year's nominees took place during a special media event on 8th March 2024, at Strathmore University, Nairobi, coinciding with the International Women's Day.

The Authority was represented at the event by Ms. Jessica Wanjohi and Ms. Cynthia Rotich from the Cyber Security department. The event marked a significant collaboration amongst government, industry and academia with representation from the University of Nairobi, Strathmore University, University of Rwanda, University of Lagos, University of Witwatersrand, University of Simad, various ICT regulators from Africa, Konza Technopolis Development Authority, the African Advanced Level Telecommunications Institute, Liquid Intelligent Technologies, Kenya Private Sector Alliance (KEPSA), amongst others. It was a bold statement of our shared vision for a more inclusive cybersecurity landscape in the region. The event will culminate in an awards ceremony scheduled to take place on 8th June 2024. This will be a fitting celebration of the remarkable contributions of women to cybersecurity.

A peek into the thought-provoking discussions that shaped the 2024 International Women's Day:

Ms. Jessica Wanjohi from the Communications Authority of Kenya (CA) speaking in a panel session during the Acyberschool "Top 100 Women to Watch in Cybersecurity in Africa" launch, that was held at Strathmore University, Nairobi.

Future Insights on Cybersecurity

Going into 2024, the effective management of risks remains attainable even amidst the unpredictability of the evolving cyber threat landscape. While the cyber threat landscape continues to evolve, organisations can implement proactive risk management strategies to mitigate potential risks and enhance cybersecurity resilience. This can be summed up in three broad areas:

Firstly, gaining a comprehensive understanding of different cyber threat vectors improves the capacity of organisations to defend against cyber threats. Some of the common threats include malware including ransomware attacks, advanced persistent threats (APTs), social engineering attacks such as phishing scams, zero-day vulnerabilities, human fault, amongst others.

Secondly, the most effective way of understanding the current risks affecting your organisation is by having visibility over them. A properly managed attack surface area enables the development of a better tailored cyber threat intelligence programme.

Lastly, implementing a robust information security policy that includes effective mitigation strategies is critical to minimising an organisation's cyber risk. Common strategies may include utilising multi-factor authentication (MFA), regular patching of software, deploying anti-virus software, amongst others.

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