COMMUNICATIONS AUTHORITY OF KENYA

31ST Cybersecurity Report

July - September 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

Our Vision

A Digitally Transformed Nation.

Our Mission

Building a connected society through enabling regulation, partnership and innovation.

Cybersecurity Mandate

The Kenya Information and Communications Act, 1998, mandates the Communications Authority of Kenya (CA) to develop a framework for facilitating the investigation and prosecution of cybercrime offenses.

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).

The National KE-CIRT/CC is a multi-agency collaboration 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 based at the CA Centre Nairobi, comprises of staff from the Communications Authority and 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 services providers whose platforms are 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 of 2018 has further enhanced the multi-agency collaboration framework.

Director General's Perspective

You will agree with me that in the past two decades, we have witnessed wave after wave of technology transformation that has changed both production and consumption trends, and opened up new horizons in the development of innovative ICT solutions and applications. These developments clearly show that innovation and technology are the drivers of our social and economic development.

Indeed, as the ICT sector regulator, we recognize that ICTs are the cornerstone of our country's social economic development, and we must therefore ensure the accessibility, and sustainability of ICTs towards the attainment of our vision of a digitally transformed nation.

However, we are also cognizant of the underbelly of this digital transformation. Whether this takes the form of cyber attacks targeting critical information infrastructure, or advanced social engineering and online fraud, our citizenry are more exposed to online harms in the digital world.

Indeed, Kenya' s cyberspace is characterized by an increase in the frequency, sophistication and scale of cyber attacks targeted at our country.

In the period between July 2022 to June 2023, the National KE-CIRT/CC detected over 855 million cyber threats targeted at Kenyan critical information infrastructure, ranking Kenya among the top three most targeted countries in the region, alongside South Africa and Nigeria. In response to these threats, the National KE-CIRT/CC issued 23,194,321 cyber threat advisories to CII.

It is in recognition of this that the Authority is this year leading the national commemoration of October Cyber Security Awareness Month (OCSAM), under the theme *'The Paradox of Progress: Securing a Digital Nation'.* Kenya joins jurisdictions across the world in engaging with our stakeholders on solutions to foster a cyber ready and cyber resilient digital nation.

This year, we set out to carry out various activities in the run up to OCSAM 2023, which included the 2023 CA Cybersecurity Bootcamp and Hackathon Series which is a capacity building initiative targeted at students, that seeks to build Kenya's future cybersecurity workforce to power a digitally transformed nation. The series were hosted nationally in Nairobi, Kisumu, Eldoret, Mombasa and Nyeri, through our regional offices. Arising from the level of engagement with academia and the passion we witnessed from students across the country, we are planning to expand this activity further to more counties in the country.

The Authority's investment in building the capacity of Kenya's cybersecurity workforce is aligned to our heightened pursuit of cyber security in the midst of an expanded attack surface. We are also cognizant that in order to secure Kenya's cyber space, capacity building is key, whether this is building the capacity of frontline cybersecurity personnel, cyber awareness of our citizenry, or mentoring the next generation of cyber defenders in collaboration with academia, Counties and our partners. The second leg of the 2023 CA Cybersecurity Bootcamp and Hackathon Series involves study tours amongst CIIs and key players within the industry, as well as mentorship for the top performers in the series. The Authority welcomes organizations in both pubic and public sector to partner in the mentorship and placement of the 2023 cohort.

As we commemorate OCSAM this year, I'd like to reiterate that cybersecurity starts at the individual level, and that we must collaborate if we are to enhance our collective cyber posture.

I hereby extend an invitation to players across public and private sector as well as civil society, to join us this OCSAM in creating awareness on cyber safety.

Christopher Wambua
Ag. Director General

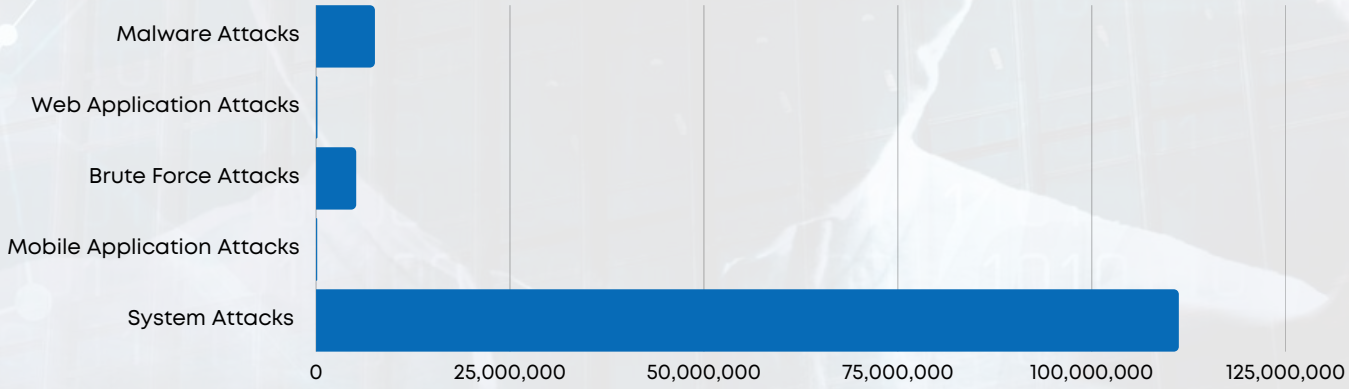
Cyber Threat Landscape Roundup

Total Cyber Threats Detected

123,899,936 | **11.36%**

During the three month period between July to September 2023, the National KE-CIRT/CC detected 123,899,936 cyber threat events, which was a 11.36% decrease from the 139,775,123 threat events detected in the previous period, April to June 2023. This decrease is attributed to the ongoing cyber awareness and capacity building efforts by the National KE-CIRT/CC, as well as the uptake in the adoption of digital signatures in the country, which was facilitated by the licensing of four additional accredited Electronic Certification Service Providers (E-CSPs).

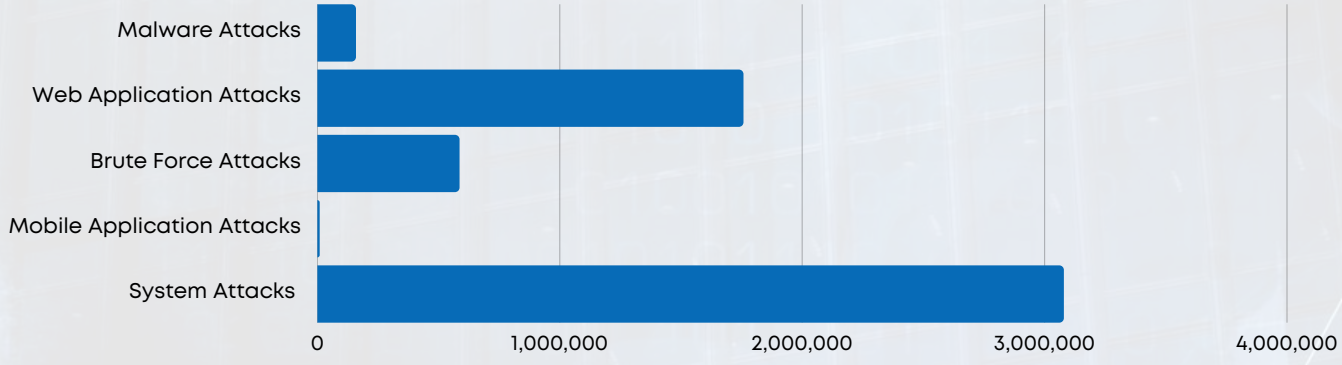
While the web application attacks were relatively minimal as compared to other attack vectors, their impact was very significant as was the case with the eCitizen DDoS attack, which led to the unavailability of online public services.



Total Cyber Threat Advisories Issued

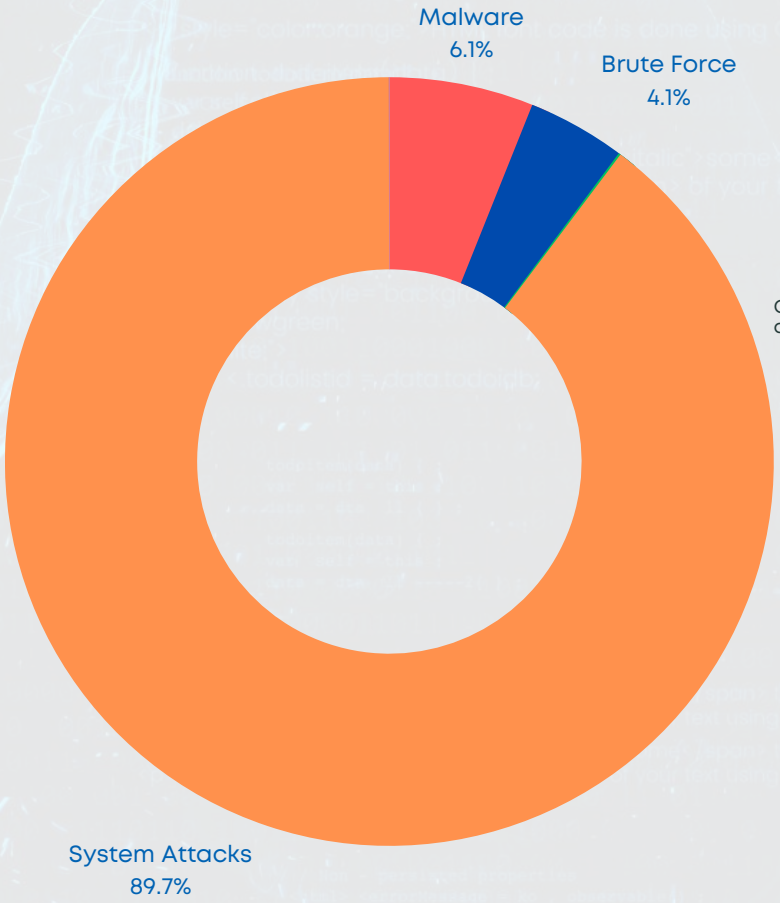
5,581,354 | **48.05%**

In response to the detected cyber threat events, the National KE-CIRT/CC issued 5,581,354 advisories between the period July to September 2023, which was a 48.05% decrease compared to the 10,742,859 advisories that were issued during the previous period April to June 2023. There was a significant increase in the number of advisories related to Brute Force attacks during this period, with the advisories serving to caution against the continued use of default and weak passwords on sensitive systems, such as IoTs & internet enabled CCTV systems. In addition, the National KE-CIRT/CC issued advisories on Zero trust, anti-DDoS, update of info security policies, the need for regular backups, cyber awareness, as well as on the need to update software to patch known vulnerabilities.



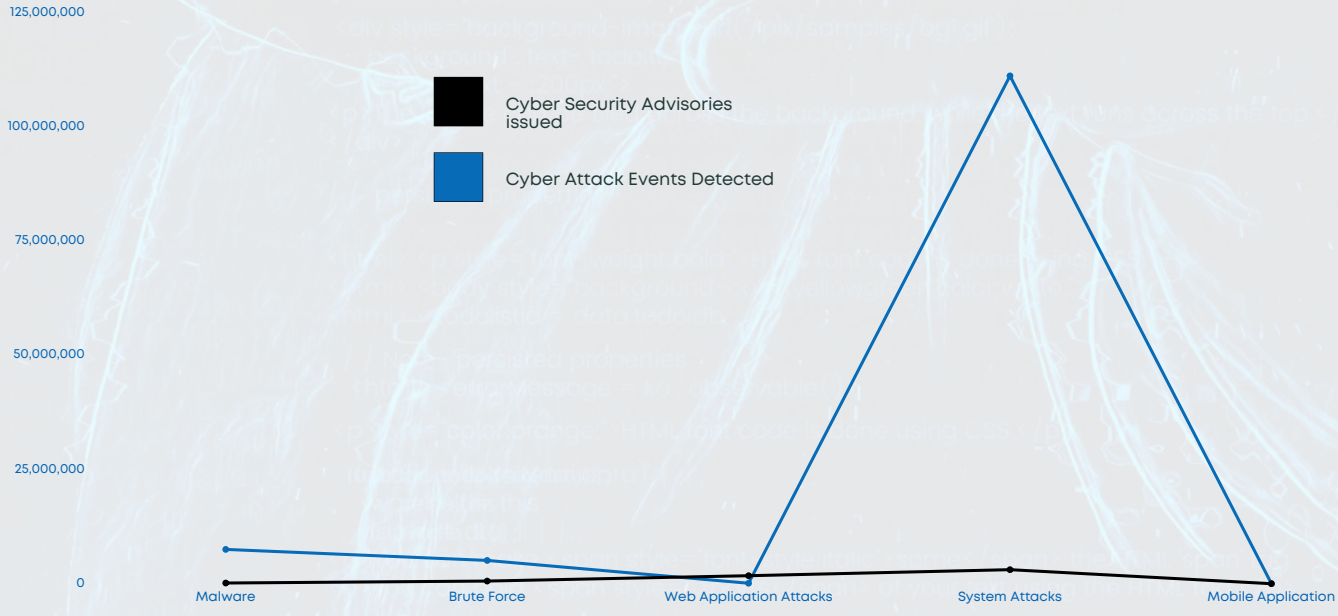
Cyber Attack Vector Trends

A comparison of the local cyber threat landscape to the global trends suggests that Kenyan CIIs are more vulnerable to system attacks compared to the global average. This can be attributed to lower levels of cybersecurity investment by CIIs, which coupled with outdated systems, raises the risk of system attacks by both local and international cyber criminal rings.

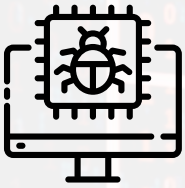


Cyber threat trends by methodology during the period July to September 2023.

Comparison of cyber threat events detected by the National KE-CIRT/CC vis a vis cyber threat advisories issued during the period July to September 2023.



Malware Trends



Threats Detected

7,514,964

39.11%

Advisories Issued

156,982

81.94%

During the three month period between July to September 2023, the National KE-CIRT/CC detected 7,514,964 malware threat attempts targeting critical infrastructure service providers. This represented a 39.11% decrease from the last period April to June 2023.

Top Targeted Systems

- **Operating Systems**
- **Serves and Workstations**
- **IoT Devices**

Top Affected Industries

- **ISPs**
- **Cloud Service providers**
- **Government**
  Academia/Education

Top Targeted Exploits

- **Stealer/broken access controls**
- **Social Engineering**
- **Vulnerable O/S**

During the period, malware attacks were targeted at systems deemed to hold sensitive data such as financial information. The attackers objectives were to steal sensitive 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:

- Adoption of Security by design during development and purchase of software.
- Implement zero trust security architecture to secure their infrastructure and data.
- Use strong authentication methods, including digital certification services, biometrics and multi-factor authentication.
- Maintain regular backup of systems and keep offline backups.
- Develop and implement business continuity plans.
- Update software and apply software patches as soon as they are released to resolve specific software vulnerabilities.
- Deploy anti-DDoS tools.
- Cyber awareness amongst organizational staff on phishing emails and on clicking on links on emails and websites to avoid automatic installation of Malware

Web Application Attack Trends

Threats Detected

106,603

35.95%

Advisories Issued

1,755,467

2,374.86%

During the three month period between July to September 2023, the National KE-CIRT/CC detected 106,603 web application attack attempts targeting critical infrastructure service providers. This represented a 35.95% increase from the last period April to June 2023.

Top Targeted Systems

- Authentication portals
- Databases
- Web servers

Top Affected Industries

- Government
- ISP's
- Cloud Services
- Academia

Top Targeted Exploits

- Vulnerable HTTP
- Remote Code Execution (RCE)
- Broken Authentication and Session Management
- Vulnerable Kubernetes
- Vulnerable SSL/TLS
- Open TFTP

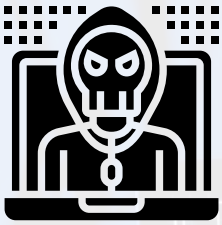
During the period, web application attacks were targeted at systems deemed to hold sensitive data and services such as s authentication data, financial data, and public services as was the case with the DDoS attack on the eCitizen platform.

The attack objectives were to make services unavailable, manipulate databases and release sensitive data for purposes of damaging organizations' reputation.

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

- Use strong authentication methods, including digital certification services, biometrics and multi-factor authentication.
- Maintain regular backup of systems and keep offline backups.
- Develop and implement business continuity plans.
- Update software and apply software patches as soon as they are released to resolve specific software vulnerabilities.
- Deploy anti-DDoS tools.
- Implement zero trust security architecture to secure their infrastructure and data.
- Use a web application firewall to filter, monitor, and block malicious traffic.
- Sensitize employees about web application security.
- Perform regular vulnerability assessments and periodic penetration tests to identify and address system and organizational weaknesses that may be exploited by cyber threat actors .

Brute Force Attack Trends



Threats Detected

5,101,538

32.93%

Advisories Issued

584,166

1,558.06%

During the three month period July to September 2023, the National KE-CIRT/CC detected 5,101,538 brute force attack attempts targeting critical infrastructure service providers. This represented a 32.93% decrease from the last period April to June 2023.

Top Targeted Systems

- Database servers
- Remote access systems
- Cloud-based systems
- Email systems
- Content Management Systems
- Identification Management Systems
- VPN Systems
- Point of Sale systems (POS)
- Content Delivery Networks

Top Affected Industries

- ISPs
- Academia
- Cloud Service
- Government

Top Targeted Exploits

- Authentication vulnerabilities
- Dictionary attacks
- Credential stuffing

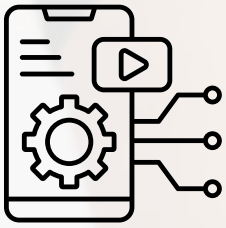
During the period, brute force attacks were targeted at systems deemed to hold sensitive data such as login credentials and financial information.

The objective of these attacks was 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:

- Use strong authentication methods, including digital certification services, biometrics and multi-factor authentication.
- Maintain regular backup of systems and keep offline backups.
- Develop and implement business continuity plans.
- Implement zero trust security architecture to secure their infrastructure and data.
- Perform regular vulnerability assessments and periodic penetration tests to identify and address system and organizational weaknesses that may be exploited by cyber threat actors .

Mobile Application Attack Trends



Threats Detected

27,147

53.65%

Advisories Issued

7,193

331.23%

During the three month period July to September 2023, the National KE-CIRT/CC detected 27,147 mobile application attack attempts targeting end user devices. This represented a 53.65% decrease from the last period April to June 2023.

Top Targeted Systems

- Mobile payment applications
- Online payment gateways
- Cloud-based services

Top Affected Industries

- Telcom/ISPs
- Cloud Service providers
- End user devices

Top Targeted Exploits

- Accessible Android Debug Bridge (Provide access to OS)
- Broken Authentication and Session Management
- Malicious Application Downloads
- Malvertising
- Outdated applications and operating systems
- Remote Code Execution
- Social Engineering Attacks

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

The perpetrators of these attacks sought to steal sensitive user data such as Personally Identifiable Information (PII), login credentials and financial details for malicious purposes.

To mitigate this risk, the National KE-CIRT/CC carried out cyber awareness to end users recommending the following actions:

- Only download applications from authorized sources.
- Regularly review mobile application permissions.
- Keep device security software up to date.
- Use strong authentication methods, including digital certification services, biometrics and multi-factor authentication.
- Maintain regular backups and keep offline backups.

System Attack Trends

Threats Detected

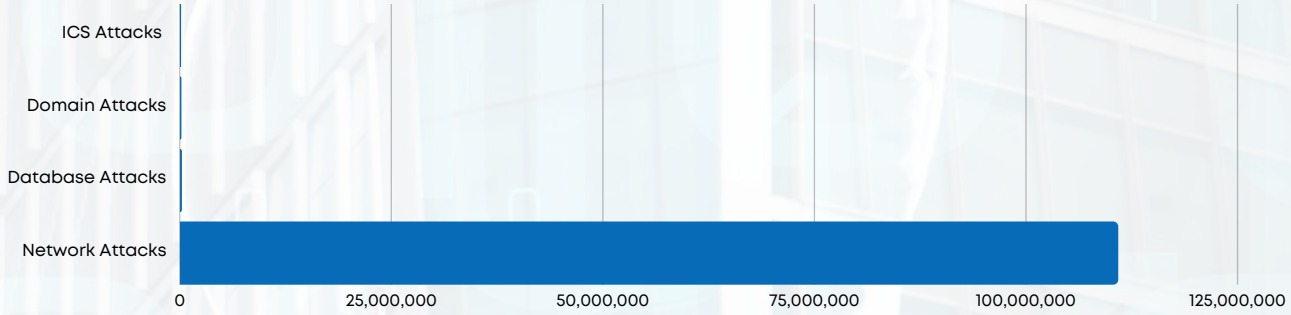
111,149,684

7.18%

Advisories Issued

3,077,164

70.83%



Top Targeted Systems

- Database Servers
- Operating Systems
- Network devices
- Web Applications
- Remote access systems.
- Mailing Servers
- Backup systems
- Operational Technology (OT)
- IP-based printers
- IP-based CCTV systems

Top Affected Industries

- ISPs
- Cloud Service providers

Top Targeted Exploits

- Stealer/broken access controls
- Vulnerable O/S
- Malicious links
- HTTP Vulnerable
- Vulnerable databases
- Zero-day exploits
- Remote code execution (RCE)
- Denial-of-service (DoS)

System attacks were targeted at Critical Information Infrastructure (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:

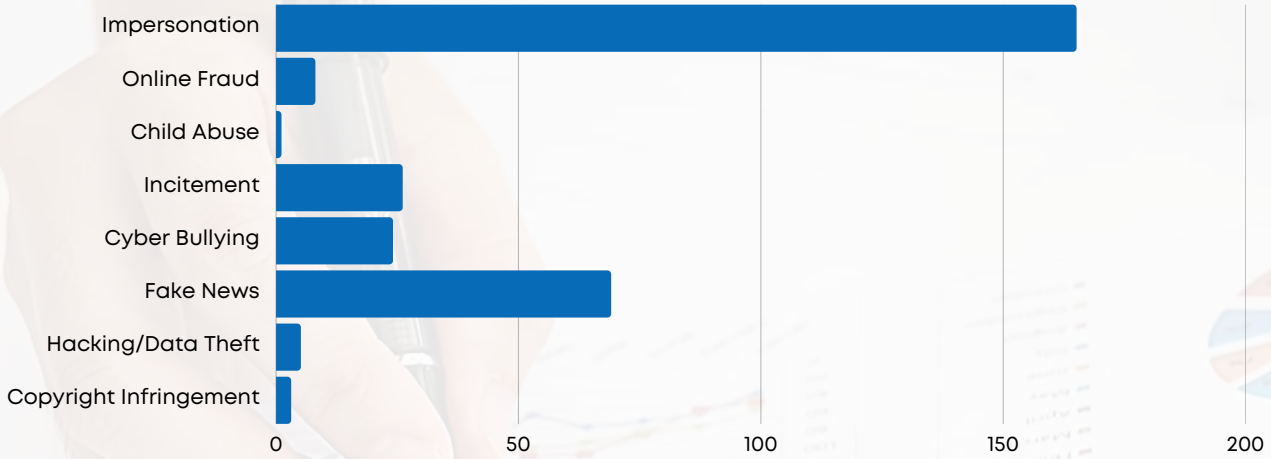
- Keep software up to date and apply patches as soon as they are released.
- Deploy anti-DDoS tools.
- Use a firewall to filter, monitor, and block malicious traffic.
- Use strong authentication methods, including digital certification services, biometrics and multi-factor authentication.
- Maintain and test regular backups, including keeping an offline copy.
- Develop and implement business continuity plans.
- Implement zero trust security architecture to secure their infrastructure and data.
- Perform regular vulnerability assessments and periodic penetration tests to identify and address system and organizational weaknesses that may be exploited by cyber threat actors .

Digital Forensics and Investigations Trends

Digital Investigations

301 | **90.51%**

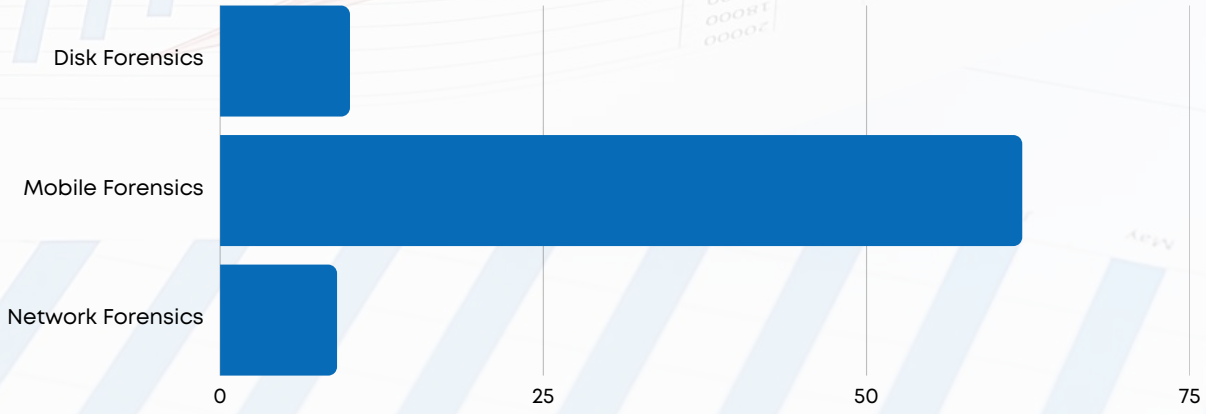
During the three month period July to September 2023, the National KE-CIRT/CC received 301 digital investigation requests. This represented a 90.51% increase from the last period April to June 2023.



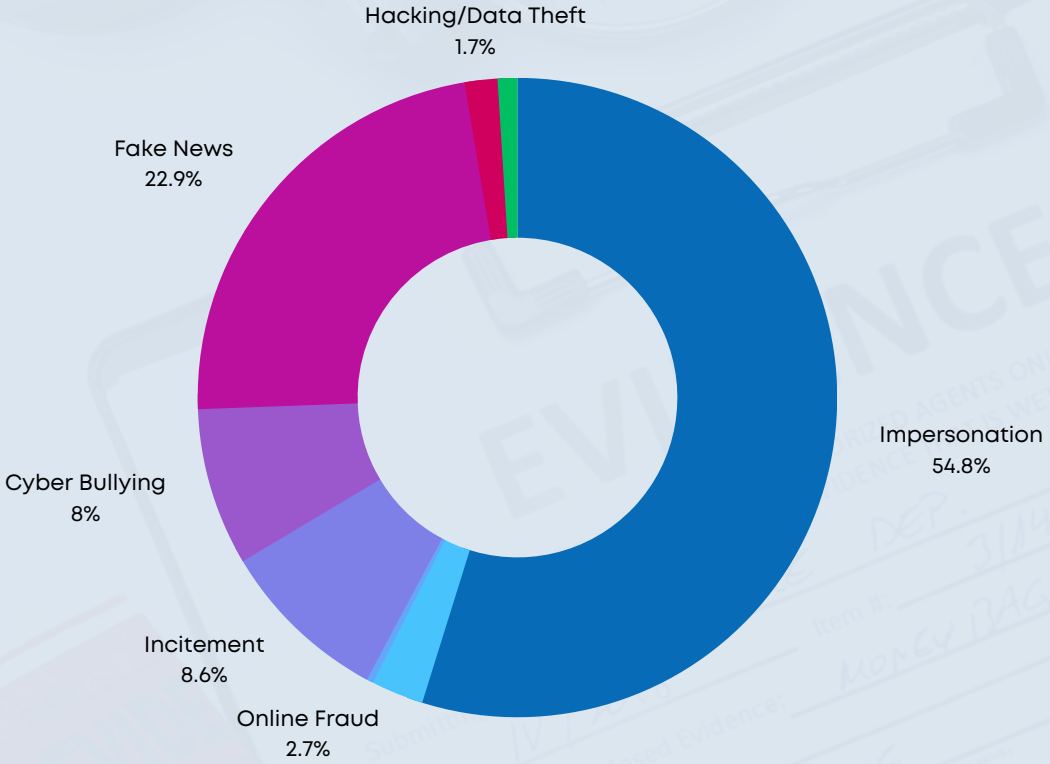
Digital Forensics

81 | **350%**

During the three month period July to September 2023, the National KE-CIRT/CC received 81 forensic requests. This represented a 350% increase from the last period April to June 2023.



Digital Investigations Trends



During the period, Facebook, X, telegram, Instagram, YouTube, TikTok, Google, WhatsApp and blogs, were the top platforms that cyber threat actors leveraged to carry out various online harms whose objectives were to steal data, radicalize youth, damage individuals reputation, carry out online revenge and for financial gain.

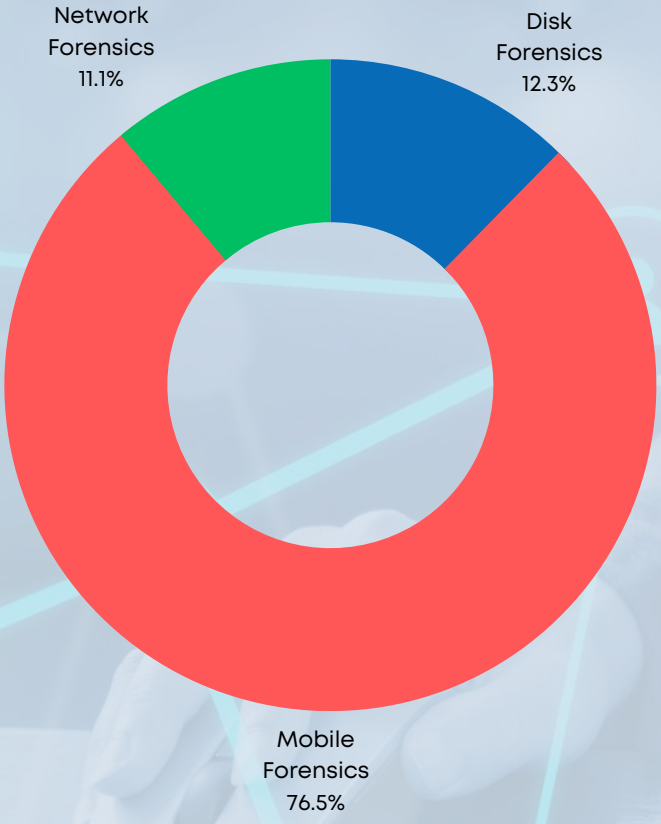
The majority of Impersonation cases reported to the National KE-CIRT/CC during the period were majorly committed on Facebook, X, Telegram, Instagram and TikTok, with the motive being mainly politically motivated, revenge and for purposes of propagating fraud. Victims reported to have lost money and assets through these impersonating accounts. Also notable during this period was the use of Telegram by kidnappers to demand ransom after kidnapping children.

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, blogs, as well as WhatsApp platforms. The motives behind these were: revenge and retaliation, radicalization of youths, financial gain, politics, as well as clickbait. These had the impact of inciting ethnic tensions, insecurity, riots and violence that caused injuries and even loss of life, as well as reputation damage and financial loss to the victims.

The National KE-CIRT/CC also received cases 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 a cyber awareness campaign to raise awareness on these online harms and empower Kenyans with the skills and resources needed to stay safe online.

Digital Forensics Trends



Top crimes for which digital forensics investigations are requested

- Fraud
- Robbery
- Fraud
- Murder
- Impersonation
- Incitement theft
- Child abuse
- Data breach
- Cyberbullying

Top forensic analysis areas

- Mobile
- Disk
- Network

Sector CIRT Updates

One of the critical roles of the National KE-CIRT/CC is to support, coordinate and collaborate with sector Computer Incident Response Teams (CIRTs). This includes technical support, information sharing as well as capacity building of sector CIRT teams. The following is an update of the cybersecurity management efforts by the various sector CIRTs in the country during the period between July and September 2023.

Government Sector CIRT

- Continued commitment to securing government networks;
- Commitment to advancing digital literacy among civil servants;
- Expansion of the public Wi-Fi services to more counties.

Telcom Sector CIRT

- Awareness creation for their membership and the general public, such as on the protection of infrastructure to address vandalization of CII, as well as to enhance cyber resilience.
- Capacity building of their members on new and emerging cyber threats.
- Nurturing of information sharing networks amongst their members to enhance cyber threat prevention and response.

Financial Sector CIRT

- Ongoing cyber resilience capacity building within the banking sector;
- Enhancing security practices within SACCOs;
- Partnership between banking industry and the government on efforts to enhance financial digital literacy in the workforce.

Academia Sector CIRT

- Currently supporting security initiatives within academic institutions nationwide;
- Capacity building of front line cyber security officers in academic institutions to better safeguard their networks and data;
- Ongoing collaborative endeavors between the sector CIRTs and academic institutions for purposes of enhanced prevention and response measures.

Dot KE CCTLD

- Continued takedown of domains perpetrating impersonation and fraudulent activities.

44TH Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

The National KE-CIRT/CC Cybersecurity Committee (NKCC) draws membership from over 50 public and private sector organizations across various sectors in the country. The main objective of the NKCC is to nurture trust networks amongst stakeholders, so as to facilitate the sharing of information on emerging cyber trends, and identify a collective strategy to address these emerging issues.

The NKCC holds quarterly meetings through which the National KE-CIRT/CC updates members on emerging cyber issues, and through which sector CIRTs also update members on emerging cyber trends within the various sectors. The 44th Meeting of the NKCC was held on September 20th, 2023 at the Safari Park Hotel & Casino, Nairobi.

During the meeting, members noted that Kenya's continued accelerated digital adoption calls for innovative and collaborative approaches to cybersecurity management. Towards this, members discussed the various essential technical, policy, and best practice measures that are needed to protect critical systems, so as to foster trust among users, customers, and stakeholders in the digital environment.

The meeting also included various key note presentations on the evolving cybersecurity landscape within the Kenyan context, including the emergence of Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks as a means of disrupting service delivery in the country, and ways of combating these attacks. The meeting also included discussions on the adoption of IPv6 technology, including its relevance and applications in enhancing network security. These engagements serve to empower the Committee with a deeper understanding of emerging cyber security challenges and the strategies and technologies available to mitigate them, thereby fostering a proactive cybersecurity management approach within the Kenyan context.

Building Tomorrow's Cybersecurity Workforce: Bootcamp & Hackathon Series

The Authority successfully completed the regional series of the 2023 CA Bootcamp and Hackathon Series, which was held in partnership with Huawei and the Kenya Cybersecurity and Forensics Association (KCSFA), under the overarching theme: *'The Paradox of Progress: Securing a Digital Nation'*.

The aim of this initiative is to support the development of relevant local cybersecurity capabilities as a way of enhancing our collective cyber readiness and resilience towards advancing Kenya's digital transformation agenda. The 2023 Series brought together students in tertiary institutions from across the country, with competitions held in Nairobi, Kisumu, Eldoret, Mombasa and Nyeri.

Nairobi Edition in Pictures

Kisumu Edition in Pictures

Eldoret Edition in Pictures

Mombasa Edition in Pictures

Nyeri Edition in Pictures

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