COMMUNICATIONS
AUTHORITY OF KENYA

OCTOBER - DECEMBER

Cybersecurity REPORT

PREPARED 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 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).

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 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.

Message from the Director General

The digital ecosystem continues to flourish in the advancements realised by emerging technology. Equally, cyber threat actors are hard at work developing novel advanced sophisticated cyber attack techniques with the objective of scaling cyber attacks while maintaining a low profile to avoid drawing the attention of law enforcement agencies. The reality of operating in an erratic environment such as this where cyber threat actors are constantly evolving therefore means that the most important defence we have against them is active collaboration.

This has been a recurring theme throughout the year and particularly this quarter that featured the October Cyber Security Awareness Month (OCSAM). The Authority commemorated this year's OCSAM through the theme '*Securing Tomorrow: Collaboration for a Thriving Digital Nation*'. This is in realisation of the reality that cybersecurity is borderless and faces evolving cyber threats that therefore call for collaboration among various stakeholders across the cybersecurity value chain.

During OCSAM, the Authority hosted cybersecurity initiatives targeted at the youth specifically students in higher learning institutions through the *CA Bootcamp* in partnership with Huawei Kenya that registered 1,719 students from whom the top 9 students were determined from a technical hands-on training; and the *CA CyberRise Hackathon* run in partnership with the Kenya Cyber Security and Forensics Association (KCSFA) that registered 118 students where the top three teams comprising of 5 members emerged as winners.

The Authority further hosted the national cybersecurity conference that brought together industry leaders in the cybersecurity value chain from across the country where they engaged in conversations encouraging cyber security knowledge exchange; enhanced collaboration and teamwork; enhanced cyber awareness and cyber hygiene; and enhanced information sharing between trusted networks within the cybersecurity community. This was delivered through keynotes and panel sessions as well as immersive and interactive table-top cybersecurity simulation exercises that were jointly facilitated with the Kenya Bankers Association (KBA). In addition, the best performing students from the Bootcamp and Hackathon were then awarded during the national cybersecurity conference awards and gala ceremony where they also got to interact with industry leaders in the cybersecurity value chain.

This period also featured Kenya's re-election to the council of the International Telecommunications Union (ITU) during the 2022 Plenipotential Conference that garnered 146 votes, the highest in the African region, to secure a seat on the 48-member council where the Authority in collaboration with the Ministry of Foreign and Diaspora Affairs and the the Ministry of Information, Communication and Digital Economy spearheaded the campaigns. This re-election enables Kenya to continue enjoying the trust and confidence of the international community to provide meaningful leadership in the digital economy as well as enable the Authority to enhance cybersecurity initiatives that align with the UN specialised agency for Information and Communication Technologies (ICTs) such as Child Online Protection (COP) and building confidence and security in the use of ICTs towards enhancing Kenya's cybersecurity readiness and resilience.

The Authority's National KE-CIRT/CC continues to collaborate with local and international stakeholders towards management of Kenya's cybersecurity. This is a critical strategy to building Kenya's national cyber readiness and resilience by leveraging the synergies that these partnerships afford in the cybersecurity management process.

Even as we cast our anticipation for a prosperous year in 2023, it is important to bear in mind that building a secure digital superhighway calls for concerted efforts across all sectors to enhance collaboration within cyberspace thereby benefiting from the collective power of the digital economy.

EZRA CHILOBA
DIRECTOR GENERAL, COMMUNICATIONS AUTHORITY OF KENYA

The digital environment continues to offer tremendous opportunities to children thereby creating new channels for learning, innovation and social interaction among others. Social media platforms embody these aspects in a delightful and relatable manner to children therefore contributing to forming a huge part of their pre-teen and teenage years where they share interests; explore their identities as well as make, develop and maintain relationships. However, social media platforms are also hosts to countless cyber threats such as cyberbullying, sextortion, identity theft, online fraud, online grooming, invasion of privacy among others. The risks of these cyber threats have become particularly acute, as the surge in screen time among children has precipitated.

Notably, the Authority observed a rise in child online abuse cases where offenders recorded and shared audio visual content of children in compromising situations such as partaking in alcohol and substances, dressing and dancing provocatively among others.

In addition, the Authority observed an increase in the number of children participating in dangerous viral social media trends as a way of commanding attention from viewers, gaining popularity, and maintaining a sense of belonging with their online connections.

Children ON SOCIAL MEDIA

> **"A third of children aged between 8 and 17 with a social media profile have an adult user age."**
>
> *According to a report by the Office of Communications (Ofcom), United Kingdom*

Online predators leverage such trends to masquerade as peer social media accounts for purposes of forming private online spaces where they normalise sharing of inappropriate content within the space preying on children's assumption that what is shared in private means safe.

Moreover, a study by the United Kingdom’s Office of Communications commonly referred to as Ofcom worryingly cites that a third of children aged between 8 and 17 with a social media profile sign up with false dates of birth thereby ageing their online profiles. This then affords them access to unfiltered social media content such as content promoting violence; negative body image content that includes pro-anorexia content among others; sexual content; pro-self harm content among others.

In view of this alarming trend, the Authority through the National KE-CIRT/CC investigates and prosecutes cybercrimes targeted at children; works closely with Child Online Protection (COP) specialised agencies such as the International Telecommunications Union (ITU), Childline Kenya, Watoto Watch Network among others to promote COP awareness, educate the public and establish hotlines that support reporting offences as well as provide counselling to victims.

Protecting children online is a global concern that requires concerted efforts of parents, guardians, the government and COP specialised agencies. As we work towards enabling a secure digital space for children, it is also important to bear in mind that the most effective and durable measures are those that build on adopting cybersecurity best practices as a behavioural change within the family and community thus empowering children to make informed choices as they benefit from the generative power of the digital space.

For more information on cybersecurity best practices, please visit: https://cop.ke-cirt.go.ke/

To play the CA games: https://www.ca.go.ke/play-cyber-soljas/

National Cybersecurity Simulation Insight

October Cyber Security Awareness Month (OCSAM) continues to enable governments, the public and private sectors to engage in initiatives geared towards empowering consumers with the knowledge, skills and values to safeguard themselves online. This year, the Authority organised cyber security training and awareness programs that included the national cybersecurity conference under the theme *"Securing Tomorrow: Collaboration for a Thriving Digital Nation"*. Through the national cybersecurity conference, the Authority was able to reach industry leaders in the cybersecurity value chain.

The national cybersecurity conference featured keynotes and panel sessions as well as immersive and interactive table-top cybersecurity simulation exercises jointly facilitated with the Kenya Bankers Association (KBA). These table-top cybersecurity simulations highlighted real-world cybersecurity scenarios that enabled the delegates representing various critical information organisations across the country to immerse themselves in deliberative conversations on the implications of cybersecurity incidents to every aspect of an organisation.

The conference delegates were grouped into ten (10) working groups of twelve (12) members and the outcomes of the table-top cybersecurity simulation exercises were as follows:

Lessons Learnt	Application to Working Environment	Looking Forward
Cybersecurity crisis management impacts every aspect of a business. Therefore; monitoring, responding and resolving cybersecurity incidents requires continued preparedness efforts at the inter-departmental level to counter cyber threats.	Incorporate cybersecurity incident response plans that can easily be cascaded at the inter-departmental level in the event of a cybersecurity incident.	Implement cybersecurity crisis management strategies and policies that guide inter-departmental cybersecurity crisis post-recovery.
Cybersecurity executive decision making requires insight from representatives of the different operational units within an organisation to enable informed allocation of resources and investment to respond to cybersecurity threats.	Include representatives of the different organisational units within the executive decision making arm to enable informed allocation of resources and investment to respond to cybersecurity threats.	Implement continuous inter-departmental focus groups that review their digital assets health to provide their executive level representatives with the current outlook of the department's security posture.
Cybersecurity management requires collaborative efforts among different stakeholders given the reality of the borderless and ever-evolving cyber threat landscape.	Incorporate secure channels of information sharing among different stakeholders across the cybersecurity value chain to expedite resolution of cybersecurity incidents.	Engage in collaborative efforts that seek to enhance knowledge sharing among different stakeholders across the cybersecurity value chain thus enhancing cybersecurity readiness and resilience.

Insights & Updates

NPKI

Enabling Kenya's National Public Key Infrastructure (NPKI) across all sectors

The National Public Key Infrastructure (NPKI) refers to a system for the creation, storage and distribution of digital certificates, which are used to verify that a particular online identity belongs to a certain entity or individual. The NPKI system is considered a critical element for securing Kenya's cyberspace as it assures the safety and integrity of electronic transactions and online services such as e-government, e-commerce, e-health, e-tax, e-insurance, e-learning among others.

The NPKI project is well stipulated in the Vision 2030 Mid-Term Plan (MTP), Under MTP II, the Key Flagship Programs and Projects identified in upgrading ICT infrastructure. Part VIA of the KICA Act of 1998 mandates the Communications Authority of Kenya (CA) to licence and regulate Electronic Certification Service Providers (E-CSPs).

The NPKI comprises the Root Certificate Authority (RCA) and the Government Certificate Authority (GCA) with the provision for onboarding private E-CSPs. The Authority is mandated under Section 83(c) of KICA to be the RCA while the ICT Authority under Section 4 of Legal Notice No. 183 is mandated to be the Government Certificate Authority (GCA). The Authority licensed two (2) entities namely: Idently Systems Ltd. and DigiCheti Ltd., as Electronic Certification Service Providers (E-CSPs).

The Authority as the regulator and the Root CA, is required to technically accredit an entity as an E-CSP within one (1) year upon issuance of the E-CSP Licence. For the accreditation to happen, the Authority conducts an inspection and compliance audit of the infrastructural establishment of the entity, which will host the equipment for the E-CSP. Upon accreditation, the entity can therefore commence the issuance of digital certification services to the end-user as required.

In view of this, the Authority accredited four (4) entities as E-CSPs namely:

1. The ICT Authority as the GCA,
2. TendaWorld Ltd. as a local E-CSP,
3. Evrotrust Technologies AD as a Foreign E-CSP and
4. eMudhra Technologies Ltd. as the second licensed Foreign E-CSP.

For more information, please visit our website: https://ke-cirt.go.ke/licensed-accredited-e-csps-2/

Cyber Updates

The digital space continues to experience rapid technological advancements enabling individuals and organisations across the world to access digital services more conveniently as well as scale and optimise their business operations respectively. This means that more and more critical information is held in the digital space thereby becoming increasingly attractive to cyber threat actors. In view of this, the Authority's National KE-CIRT/CC continues to operate on a 24/7 basis, monitoring and responding to cyber threats; issuing cyber threat advisories to affected parties; and creating cybersecurity awareness that is geared at enhancing individual and organisational cyber hygiene. Our cyber updates seek to highlight trends as observed globally during the period October to December 2022.

Malware

Cyber threat actors continue to leverage malicious software capability to compromise and gain unauthorised access to individuals' and organisations' computer systems. During the period in review, the Authority observed a rise in cyber-espionage groups, notably the *Worok* group that was observed using sophisticated steganography techniques to hide information-stealing malware within PNG image files for purposes of compromising high-profile individuals within government agencies and private companies to further steal data by exploiting unpatched vulnerabilities called *ProxyShell* in Microsoft Exchange servers. Cyber threat actors were also observed advancing their tactics to distribute malware through phishing campaigns; fake forum pages; embedding malicious links in Ads such as Google Ads; infected software; and fake updates of apps masked as legitimate apps such as Teamviewer, Any Desk, Adobe Flash Player and Zoom among others. The Android malware dubbed *RatMilad* was significantly observed being distributed through fake apps advertised over messaging apps such as Telegram for purposes of stealing data and listening in to victim's conversations. Moreover, cyber threat actors were observed engineering novel ways of hiding malware in software packages in the open source *Python Package Index (PyPi)* library for purposes of compromising software using the Python programming language.

In view of this, organisations are advised to fully patch their Exchange servers; keep their systems up to date; and implement a security solution to automatically and regularly scan their systems and networks for malicious signatures. It is also important that developers using open source libraries scan their code before downloading and inserting them into applications.

System Vulnerabilities

During the period in review, Microsoft Exchange vulnerabilities continued to plague enterprise mail servers through vulnerabilities such as *Proxy Logon*, *ProxyOracle* and *ProxyShell*. Cyber threat actors were observed leveraging these vulnerabilities that are based on an architectural flaw in Exchange server for purposes of carrying out *Server-Side Request Forgery (SSRF)* attacks that enable them to unauthorisedly access and tamper with organisations' digital assets. HealthCare systems also suffered an increased amount of data breaches where cyber threat actors were observed unauthorisedly accessing critical systems for purposes of encrypting and demanding ransom over patients' Personally Identifiable Information (PII). The Authority also observed cyber threat actors targeting Mobile Network Operators' (MNOs) mobile wallet to bank services where they gained unauthorised access to the MNOs' mobile wallet central systems for purposes of carrying out financial fraud.

To mitigate these threats, organisations are advised to implement security patches as soon as they are available; implement Internet Information Services (IIS) URL Rewrite rule as well as disable remote PowerShell for non-admins.

Cyber Updates

Elementary and advanced phishing attacks result in an alarming rate of successful theft of user credentials and account takeovers.

Phishing

Several phishing attacks result in successful theft of user credentials and account takeovers as a cyber threat actors continue to leverage individuals' negligent behaviour towards observing cybersecurity best practices when it comes to acting on unverified digital communication. Cyber threat actors were observed overwhelming enterprise IT teams with targeted phishing email attacks for purposes of gaining privileged access to organisations' networks and compromising their data. The Authority also observed cyber threat actors advancing their phishing attack campaigns by leveraging sophisticated automation tools to develop informed social engineering message scams for purposes of stealing individuals' sensitive information. Cyber threat actors were further observed paying for 'https' and '.com' domains for purposes of stealing individuals' sensitive information by redirecting them to websites that appear legitimate.

In view of this, individuals and organisations are advised to verify all forms of digital communication before acting on them.

Web Application Attacks

A large percentage of digital services are web-based hosted this means that they receive an overwhelming amount of targeted attacks. During the period in review, cyber threat actors were observed leveraging vulnerabilities in web application framework software such as *Apache, dotCMS, Drupal, FortiOS, GLPI, Grafana, OpenSSL, PHP, SAP NetWeaver, WordPress,* and *WS02* for purposes of gaining unauthorised access to organisations' servers; running malicious code on victim's devices remotely; injecting malicious scripts into trusted websites among others. Cyber threat actors were also observed exploiting the application mode feature that is available in Chromium-based browsers such as Google Chrome, Microsoft Edge and the Brave Browser for purposes of stealing users' passwords through launching spoofing attacks.

To mitigate these cyber threats, organisations are advised to perform regular audits of their networks; apply security patches as soon as they are available as well as keep their software up to date to prevent cyber attacks that cyber threat actors may leverage from vulnerabilities in outdated software.

Cyber Updates

Ransomware attacks continued to top the threat vectors quarter-over-quarter as cyber threat actors adopted sophisticated techniques to extend their attacks.

Ransomware

Ransomware continued to be a major cybersecurity challenge affecting organisations and individuals across different sectors. Cyber threat actors were observed taking up *Ransomware-as-a-Service (RaaS)* attack techniques for purposes of executing automated ransomware attacks. Notably, the Authority observed cyber threat actors exploiting three ransomware strains namely *AXLocker* a ransomware variant that targets file extensions with Advanced Encryption Standard (AES) encryption for purposes of encrypting victim's files and stealing Discord users' credentials by enabling a Discord Account TakeOver (ATO) to further propagate malware and fraud. Cyber threat actors were also observed exploiting *OctoCrypt* and *Alice* otherwise known as *Alice in the Land of Malware* ransomware variants that are RaaS offerings for purposes of running large-scale automated file encryption of victim's files. The Authority also observed cyber threat actors running the *Venus* ransomware variant over unsecured instances of HealthCare Windows Remote Desktop Protocol (RDP) for purposes of spreading ransomware over their networks. Cyber threat actors were further observed running a malicious campaign delivering the *Magniber* ransomware for purposes of luring unsuspecting users of the Windows home version to opt into running fake security Windows 10 updates embedded with file-encrypting malware.

To mitigate these cyber threats, individuals and organisations are advised to perform regular backup processes; keep software up to date; implement multi-factor authentication across their networks; implement automated security solutions that scan the dark web for early warning signs of new ransomware variants as well as compromised credentials and vulnerability exploits; and adopt zero trust network access.

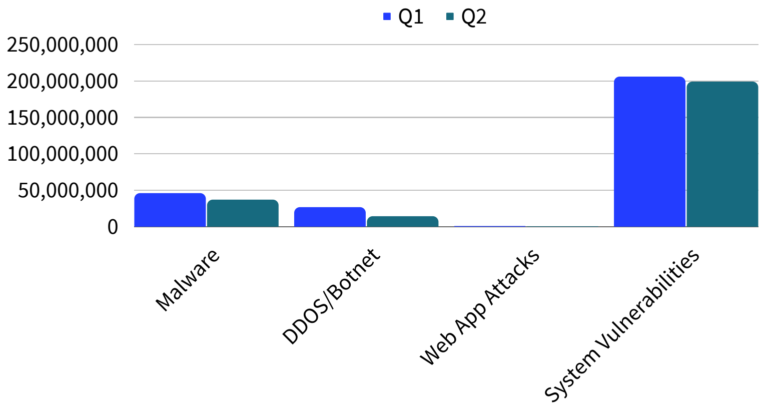
Distributed Denial of Service (DDoS)

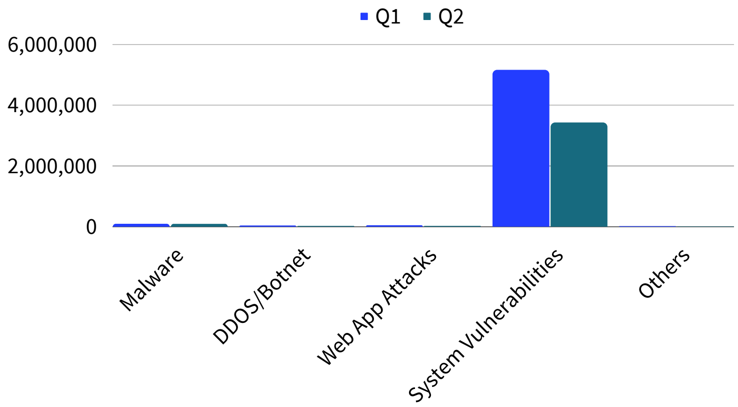
Critical information systems seamless performance depends on uninterrupted availability to enable continued access to supported services. Cyber threat actors expressly understand the value of uninterrupted system availability and the ripple effects of disrupting it, hence the continued efforts to compromise organisations' systems. The Authority observed a spike in attacks generated by the *Mirai* botnet targeting online gaming platforms such as the Wynncraft Minecraft for purposes of disrupting their website service infrastructure that includes servers and network resources availability thereby affecting multiple users' access to the platform. DDoS attacks continued to expand in magnitude and frequency at an exponential rate as cyber threat actors were observed leveraging *DDoS-as-a-Service* attack techniques for purposes of launching automated and wide-reaching DDoS attacks.

To mitigate these cyber threats, organisations are advised to continuously analyse their network traffic for malicious patterns; and implement an automated anti-DDoS hardware and software for efficient detection and mitigation of DDoS attacks.

Cyber Threat Numbers

Our Numbers for the Period October - December 2022; FY2022/2023 Cybersecurity Landscape At A Glance



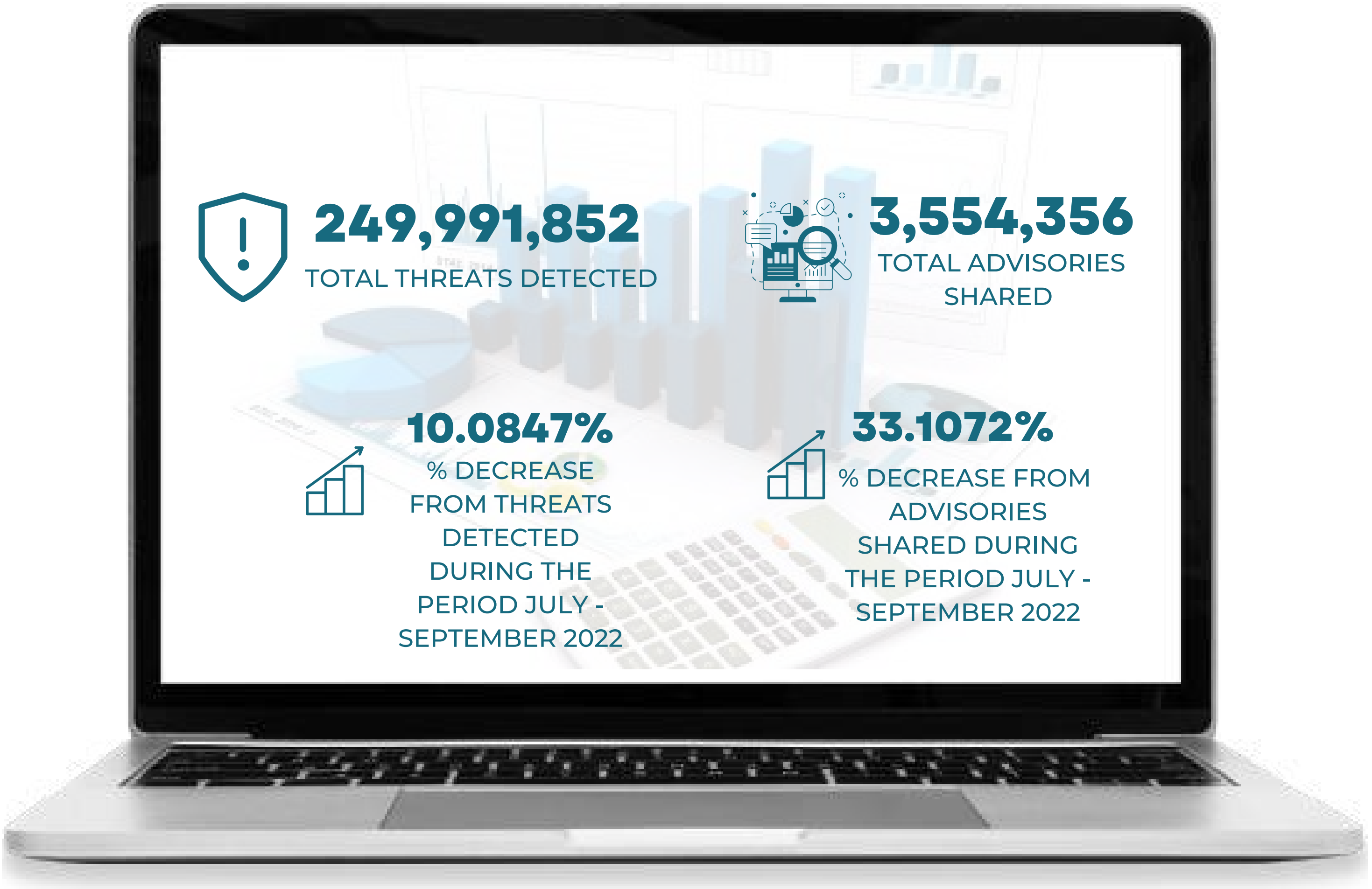


Threat Vectors

- The National KE-CIRT/CC detected *249,991,852* cyber threat vectors making up a *10.0847%* decrease from the previous *278,030,354* threat events.

Advisories

- The National KE-CIRT/CC issued *3,554,356* technical cybersecurity advisories to organisations and Cybersecurity Best Practice Guides to the public, which provided detailed insights to assist in cyber threat prevention and detection.



249,991,852
TOTAL THREATS DETECTED

3,554,356
TOTAL ADVISORIES SHARED

10.0847%
% DECREASE FROM THREATS DETECTED DURING THE PERIOD JULY - SEPTEMBER 2022

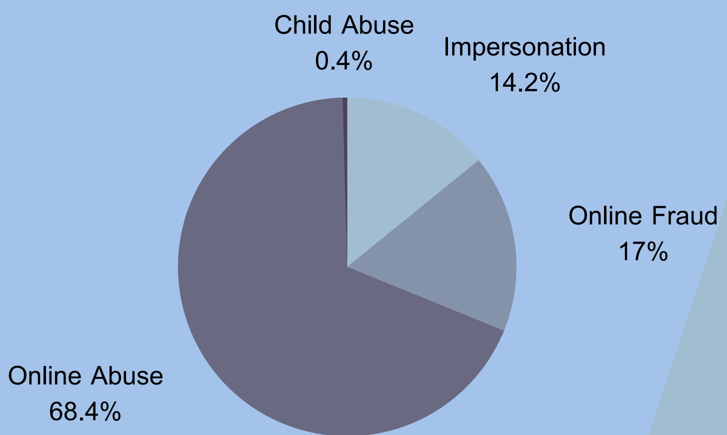
33.1072%
% DECREASE FROM ADVISORIES SHARED DURING THE PERIOD JULY - SEPTEMBER 2022

Digital Forensics & Investigations

34.4227

Total Digital Investigations

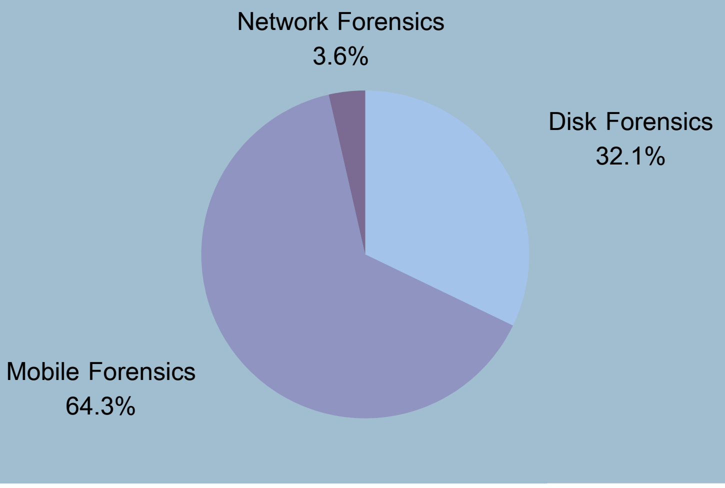
301 digital investigation requests received compared to 459 requests from July - September 2022.



100

Total Digital Forensics

56 forensic investigation requests received compared to 28 requests from July - September 2022.



Key Successes

Sophisticated Digital Forensics Lab (DFL) & exceptionally trained workforce

Successful digital forensics investigations and court prosecutions

Continued cybersecurity awareness to the public

The National KE-CIRT/CC, Kenya's Cybersecurity Command Centre

Working Round the Clock to Safeguard Kenya's Cybersecurity Landscape

Be Cyber Smart | Report Cyber Incidents

Contact

Communications Authority of Kenya
Waiyaki Way, Opposite Kinada School
P.O. Box 14448
NAIROBI 00800

www.ke-cirt.go.ke
incidents@ke-cirt.go.ke ✉
@nationalkecirt
@KeCIRT
@kecirt
@National KE-CIRT
@nationalkecirt