COMMUNICATIONS
AUTHORITY OF KENYA

CYBERSECURITY REPORT

JULY - SEPTEMBER 2022

PREPARED BY :

The National KE-CIRT/CC

Vision, Mission & Cybersecurity Mandate

VISION

A Digitally Transformed Nation.

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 Authority's 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.

DIRECTOR GENERAL MESSAGE

A thriving digital ecosystem means that the different sectors of an economy leverage the gains realised by the advancements in Information and Communications Technology (ICTs). From E-learning and E-government services to E-health and emerging automated technology. With these exponential advancements, cyber threat actors continue to take-up sophisticated attack techniques to compromise individuals' Personally Identifiable Information (PII) as well as states' Critical Information Infrastructure (CII).

In view of this, the Authority is committed to secure Kenya's Critical Information Infrastructure (CII) and by extension the public's digital assets against the ever-evolving cyber threats. Towards this, the Authority through the National KE-CIRT/CC detects, assesses, prevents, monitors and responds to cybersecurity incidents using its state-of-the-art systems. Further, the Authority shares: technical advisories to critical information organisations; cybersecurity best practices to the public; and leverages its network of partners to share information and critical resources towards securing Kenya's cyberspace.

This year, the Authority joins the global community in commemorating October Cyber Security Awareness (OCSAM) Month. The October Cyber Security Awareness Month (OCSAM) is a collaboration between public and private sectors with the goal of raising awareness of cyber safety through empowering individuals with the knowledge, skills, and values to safeguard themselves online.

The Authority will lead this year's OCSAM 2022 in partnership with key local and international stakeholders under the overarching theme: *'Securing Tomorrow: Collaboration for a Thriving Digital Nation.'* This is in cognisance of the reality that cybersecurity calls for an interplay of collaboration among different stakeholders across the cybersecurity value chain in managing cybersecurity. In addition, through the theme, the Authority seeks to highlight the collaborative approach to enhancing cyber readiness and resilience, which is the cornerstone of the National KE-CIRT/CC.

The Authority seeks to commemorate OCSAM 2022 through three key initiatives; the CA CyberRise Summit that will entail a Bootcamp and Hackathon targeting students, and the annual cybersecurity conference that will be targeted at cybersecurity industry leaders. The Authority appreciates the need for a competent workforce to address the ever-evolving cybersecurity threat landscape. As a result, the authority will hold the Bootcamp in partnership with Huawei Kenya guided by its existing Memorandum of Understanding (MOU) and hold a hackathon in partnership with the Kenya Cyber Security and Forensics Association (KCSFA), a local stakeholder who draw their membership from the National KE-CIRT/CC Cybersecurity Committee (NKCC). Further, the Authority realises the continued need to collaborate with stakeholders towards curbing cybercrime. Consequently, the Authority will host the annual cybersecurity conference that will run initiatives that are geared at encouraging cyber security knowledge exchange, enhancing collaboration and teamwork, enhancing cyber awareness and cyber hygiene, and enhancing information sharing between trusted networks within the cybersecurity community.

This October, even as the Authority recognizes how much work remains to be done to bolster Kenya's cybersecurity, we continue to spearhead the safeguarding of Kenya's digital assets in which Kenyans rely on.

CHILDREN AND THE INTERNET

A focus on Online gaming

ONLINE SAFETY FOR THE WHOLE FAMILY
READY TO FIGHT CYBERCRIME?
CYBER SOLJAS
PLAY
incidents@ke-cirt.go.ke

The digital space has enabled individuals to access critical services such as e-government, e-commerce, e-learning and telehealth among others. Children are an important demographic that also share in the benefits that the advancements in technology have to offer. One such service that children have taken up to is online gaming. Online gaming refers to games played over a computer network. Online gaming has presented children with the opportunity to socialise, where gamers interact with their friends as they enjoy their favourite multiplayer games through online clubs, teams, societies and events thereby cultivating relationships via common experiences while creating an inclusive environment for differently abled children.

In addition, online gaming enhances children's concentration and analytical skills through engaging their planning and problem-solving skills to solve challenges and attain goals within the games. Moreover, gaming equips children with skills that are critical in Science Technology Engineering Arts and Mathematics (STEAM) careers.

It further provides an avenue for children to venture into professional online gaming and content creation where gamers can stream their gameplays via Twitch and YouTube to generate income. Highly talented players in the gaming industry are in high demand.

However, with these benefits, children remain a vulnerable group in society more so in the digital space where they are left vulnerable to a myriad of boundless threat actors. Online gaming platforms continue to face challenges of cyber-attacks that are further extended to children. Notably, the Authority observed the Log4Shell vulnerability on the Minecraft gaming platform enabling cyber threat actors to access the web server without a password thereby exposing internal networks and further allowing threat actors to compromise users' data and install malware. In addition, the Authority observed the MitD attack in the Fortnite android application as well as other android gaming apps. Threat actors leverage this vulnerability to crash the apps and inject malicious code as well as monitor apps external storage area and tamper with the data. The Authority further observed threat actors leveraging the Discord Injector to inject malware into discord tokens using a JavaScript code for purposes of relaying user's credentials and unauthorizedly scanning their credit information.

In view of this, the Authority continues to share Child Online Protection (COP) cybersecurity best practices to the public and further rolled out the CA games to impart knowledge and values on children.

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

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

Mis/Dis/Mal-information

Insight during the 2022 electioneering period in relation to social media management

The electioneering period is often characterised by the different parties involved sharing extreme amounts of information, be it true or false, for purposes of garnering the highest support. The recently concluded election was no exception. With digital platforms such as social media enabling the rapid sharing of information, social media amplified the mis/dis/mal-information and fake news voices thereby misleading and or shaping individuals' opinions surrounding the election processes and period. Cyber threat actors were observed leveraging synthetic media such as deep fakes for purposes of manipulating videos and images to appear as though the targeted personalities spoke to given subject matters for purposes of misleading the public and causing harm.

Towards this, the Authority continued to share technical advisories on a 24/7 basis, publish cybersecurity reports on notable concerns during the period, share cybersecurity best practices with the public, collaborate with social media and fact-checking entities towards verifying information as well as collaborate with critical information infrastructure technical teams towards monitoring of digital assets and addressing domain impersonation concerns.

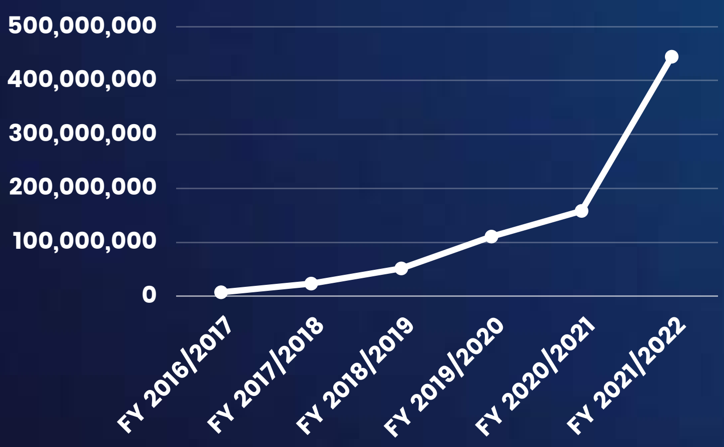
As the Authority continues to implement security measures towards safeguarding Kenyans from mis/dis/mal-information and fake news, we call on every individual to perform due diligence when consuming content on digital platforms as well as perform due diligence before acting on any digital communication.

Be cyber astute and report cyber incidents to the National KE-CIRT/CC through the KECIRT mobile application or incidents@ke-cirt.go.ke incident reporting email or https://www.ke-cirt.go.ke web portal or our hotlines on +254-703-042700 or +254-730-172700.

CYBERSECURITY COLABORATION INSIGHTS

Cybersecurity is not a stand alone function in view of this, the National KE-CIRT/CC collaborates 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 on the synergies that these partnerships afford in the cybersecurity management process. Globally, the National KE-CIRT/CC leverages partnerships with 51 other National Computer Incident Report Teams (CIRTs), the global 24/7 G7 Cybercrime Network, the International Telecommunication Union (ITU), the Forum for Incident Response and Security Teams (FIRST), Internet Corporation for Assigned Names and Numbers (ICANN), Facebook, Twitter, TikTok, Google and GoDaddy. Locally, the National KE-CIRT/CC Cybersecurity Committee (NKCC) continues to support the National KE-CIRT/CC in addressing cybersecurity concerns. The NKCC members represent Kenya's critical information infrastructure organisations, Mobile Network Operators (MNOs), academia as well as government.

Cyber Threats Detected for the Last 5 Years



In an effort to enhance the national cyber readiness and resilience in the face of the ever-increasing cyber threats, the National KE-CIRT/CC continues to operate on a 24/7 basis monitoring and responding to cyber threats; issues cyber threat advisories to organisations; builds capacity of critical information infrastructure service providers (CIIPs); collaborates with local and external stakeholders in cybercrime investigation and prosecution; offers technical support to affected organisations; and creates cybersecurity awareness that is geared at enhancing individual and organisational cyber hygiene.

The National KE-CIRT/CC hosts quarterly NKCC meetings to share information and address notable cybersecurity concerns in the Kenyan cybersecurity landscape. During the 40th quarterly NKCC meeting that was held on 28, September 2022, the National KE-CIRT/CC run an assessment that entailed responses from members representing over 20 organisations who provided insight into the National KE-CIRT/CC's efforts in securing Kenya's cybersecurity and further tabled suggestions on ways to better serve stakeholders at large.

- Participants reported that the National KE-CIRT/CC's technical advisories and cybersecurity reports provided their organisations with visibility on the threat landscape thereby enabling them to resolve cyber threats in a timely and more informed manner.
- Participants reported that the continued increase in complexity of training rolled out by the National KE-CIRT/CC enabled their organisations to address the matuaring cyber threat landscape.
- Participants pointed out the need to run curated training for organisations that may otherwise not have mature Security Operation Centres (SOC) as well as implement frameworks that analyse security infrastructure at an organisational level.
- Participants pointed out the need to run several table-top simulation exercises highlighting real-life cybersecurity challenges being faced by stakeholders within Kenya's ecosystem as a measure of enabling organisations to adequately address the ever-evolving cyber threats.

NPKI

Insights & Updates

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). During the quarter, 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 three (3) entities as E-CSPs namely: the ICT Authority as the GCA, TendaWorld Ltd. as a local E-CSP and eMudhra Technologies Ltd. as the second licensed Foreign E-CSP.

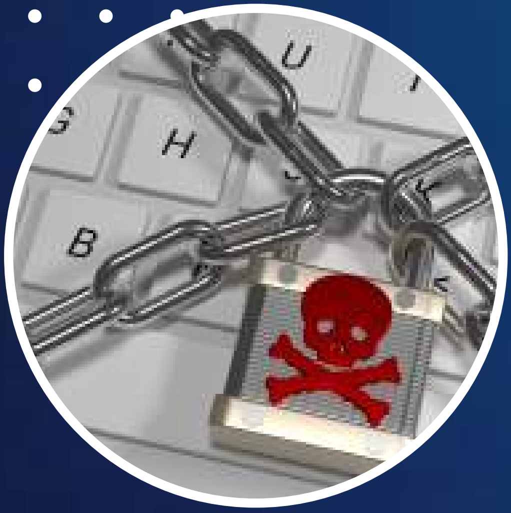
For more information, please visit our website: https://ke-cirt.go.ke/licensed-accredited-e-csps-2/

HIGHLIGHT OF THE GLOBAL CYBER THREAT INSIGHT

New and emerging technologies have greatly influenced the rapid technological advances realised in Digital Financial Services (DFS). This has further resulted in the proliferation of digital identity systems, data driven financial services, crypto-currencies, blockchain applications, automated e-government financial services and compliance processes, and improved financial regulatory industry standards. With this shift, cyber threat actors continue to adopt sophisticated attack techniques to compromise critical financial information infrastructure and by extension individuals' sensitive information.

There was a notable rise in crypto-currency scams being propagated through synthetic identity fraud where cyber threat actors leverage Artificial Intelligence (AI) to impersonate users' biometrics for purposes of bypassing verification controls as well as generate synthetic profiles with cloned documents for purposes of carrying out financial fraud. Cybercriminals were also observed turning to Fraud-as-a-Service (FaaS) where cyber threat actors develop automated attacks tools and offer their services for hire making it easy for novice threat actors to deploy mass fraudulent real-time payment fraud. In response to this, several nations shared in collaborative efforts towards educating the public on cybersecurity best practices to take up and implement strong security solutions.

CYBER UPDATES



RANSOMWARE

Ransomware continues to be a major cybersecurity challenge affecting organisations and individuals across different sectors. Ransomware gangs, Conti and LockBit being the two most active, were observed targeting Small, Medium and Micro Enterprises (SMMEs), the healthcare sector, and government critical infrastructure owing to the quantity of confidential information that they handle. Threat actors leverage on organisations' and SMMEs poor cyber defence as well as susceptibility to pay ransom following pressure to restore operations. In addition, cyber threat actors were observed adopting advanced and automated ransomware attack techniques such as Ransomware-as-a-Service (RaaS) for purposes of destroying data at ransom using destructive malware. This method makes it impossible for victims to bypass paying ransom if they successfully decrypt the retrieved encrypted data.

In view of this, it is important for organisations to perform regular backup processes; keep software up to date; implement multi-factor authentication across their network; and adopt zero-trust network access.

PHISHING

Humans are the weakest link in relation to the cybersecurity chain due to our imperfect nature, and cyber threat actors are fully aware of this. Cyber threat actors leverage phishing attacks to launch advanced attacks for purposes of exploiting human behaviour. During this period, there was a rise in financial phishing targeted at e-commerce and e-payment platforms where threat actors send fake alerts from financial institutions and e-payment systems for purposes of obtaining unsuspecting victims' credentials and data. Further, cyber threat actors were observed using new attack tactics to deepen authenticity and minimise suspicion by composing phishing emails as replies in existing email threads for purposes of compromising users' information.

To mitigate phishing attacks, it is important that individuals perform due diligence before acting on any digital communication.

CYBER UPDATES

DDOS

Critical information infrastructure and organisations' systems being online means that cyber threat actors are hard at work searching for vulnerabilities or low hanging fruits to compromise. Cyber threat actors were observed investing resources to expand and add features to botnets by secretly infecting more interconnected devices such as Internet of Things (IoT) with malware for purposes of exploiting them to launch larger DDoS attack campaigns. Moreover, cyber threat actors were observed overwhelming a wide range of services and devices of a target with smaller portions of traffic with the aim of evading detection from mitigation systems that focus on individual IP addresses as opposed to entire subnets.

In view of this, organisations should implement IP stresser services to test bandwidth capabilities, and implement DDoS mitigation services.

VULNERABLE IOT

Increased penetration and adoption of Internet of Things (IoT) devices has enabled a seamless interconnected digital ecosystem. However, with this, the attack surface possibility only extends further. Cyber threat actors were observed taking up Ransomware for IoT (R4IoT) attack technique, which is a convergence of ransomware and IoT attacks, for purposes of compromising Information Technology (IT) and Operational Technology (OT) networks at a large scale, exfiltrating data, and installing crypto mining software in IT environments.

To mitigate this, it is important that organisations obtain visibility into their digital assets and communications inventory to monitor threats and vulnerability indicators; implement network segmentation to minimise the radius of initial threat access to digital assets; and implement automated risk mitigation measures.

CLOUD SECURITY

Rapid adoption of cloud-based services has resulted in a sharp rise in the dependency of digital services as digital transformation continues to take shape. Cyber threat actors, just like organisations and businesses continue to realise the potential of the cloud infrastructure. More and more threat actors were observed exploiting critical vulnerabilities in cloud providers and cloud-based supply chains for purposes of gaining unauthorised access to corporate environments, running large scale remote attacks, compromising authentication processes, and compromising open-source software code used by supply chains. In addition, cyber threat actors were observed leveraging DDoS and crypto jacking attacks to compromise container-based systems running in the cloud for purposes of restricting access to services, spreading malicious images that contain crypto miners, carrying out backdoor attacks and spreading threat vectors disguised as legitimate software applications, which are used by supply-chains.

In view of this, organisations are advised to create multiple overlapping layers of security to reduce exposure to risks.

CYBER THREAT NUMBERS

Our Numbers for the Period July - September 2022; FY2022/2023 Cybersecurity Landscape

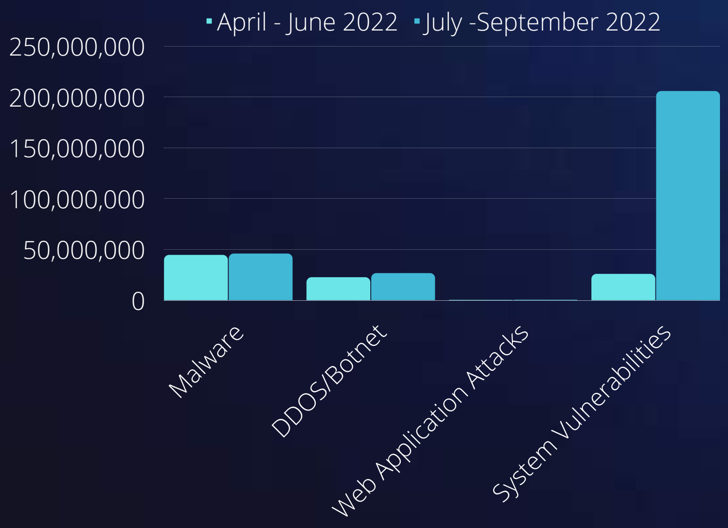
278,030,354
TOTAL THREATS DETECTED

5,313,512
TOTAL ADVISORIES SHARED

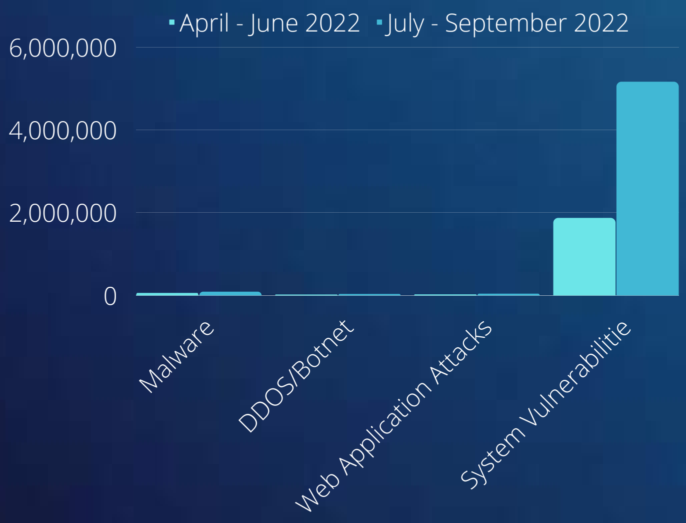
199.478%
% INCREASE FROM THREATS DETECTED BETWEEN APRIL - JUNE 2022

169.369%
% INCREASE FROM ADVISORIES SHARED BETWEEN APRIL - JUNE 2022

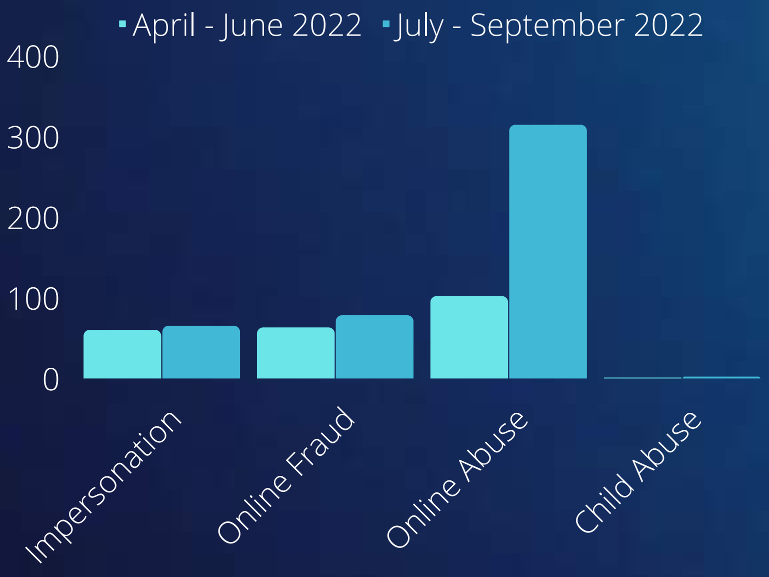
THREAT VECTORS

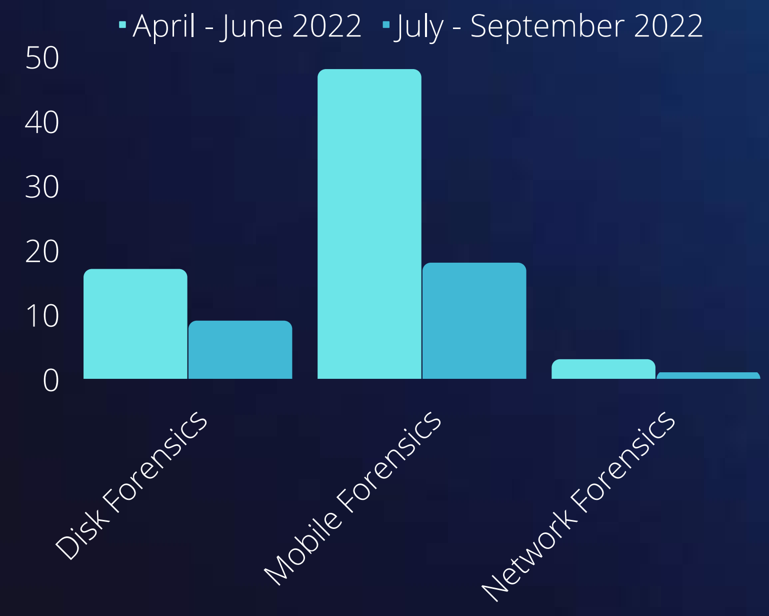


ADVISORIES



DIGITAL FORENSICS & INVESTIGATIONS





Total Digital Investigations

459 digital investigation requests received compared to 239 requests between April - June 2022.

92.05 %

Total Digital Forensics

28 forensic investigation requests received compared to 68 requests between April - June 2022.

58.8235 %

THANK YOU

Report an incident to:
www.ke-cirt.go.ke | incidents@ke-cirt.go.ke |
+254-703-042700; +254-730-172700

Working Round the Clock to Safeguard Kenya's Cybersecurity Landscape