COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

APRIL - JUNE 2022

PREPARED BY:
THE NATIONAL KE-CIRT/CC

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 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 INSIGHT

CYBERSECURITY & MURPHY'S LAW

In a digital ecosystem, data is the name of the game.

Indeed, advanced economies leverage on data to provide digital solutions that have a direct and positive impact on development. They use data to understand humanity and humanity's challenges; and thereafter harness this insight towards development of impactful solutions.

With data as the world's most valuable resource, we would rightfully assume that there are a myriad of questions that organizations, and undoubtedly, cyber threat actors, consider when it comes to identifying, collecting, analyzing and ultimately, monetizing data.

These questions include: who provides it, how can we access it, how fast can it be shared, and how much value can be derived from it?

With data being such a valuable resource and currency, it is therefore not surprising that cyber threat actors are also increasingly leveraging on the accelerated digital adoption to harvest data to advance their malicious agenda. Whether this agenda is the crippling of critical infrastructure, or spreading misinformation and disinformation, or even socio-economic sabotage; data is a double-edged sword in the wrong hands.

To bring it home, data security strategies are at the heart of cybersecurity. Cybersecurity is at the crux of data protection. Technically defined, cybersecurity encompasses the strategies, techniques, and controls that are put in place to ensure that data assets are protected. A laissez faire approach to cybersecurity undoubtedly negatively impacts not just the organization, but the socio-economic fabric of society as a whole.

As Murphy's law aptly puts it; while operating in an erratic environment, anything that can go wrong will go wrong, and at the worst possible time. With 92,838,258 cyber threat attempts detected by the National KE-CIRT during the period April to June 2022, and a total of 444,055,806 cyber threat attempts detected in the period July 2021 to June 2022, as compared to 158,404,552 in the previous year; it cannot be business as usual.

The importance of cybersecurity cannot therefore be downplayed. Adoption of cybersecurity practices is critical; whether at the personal or organizational level, or even nationally.

Addressing the myriad of cyber threats in the digital landscape demands that we take up innovative cybersecurity solutions and implement robust cyber readiness and resilience programs. It is also important that we empower end users with the knowledge, values and skills to enable them to thrive in the digital world.

As a parting shot, I wish to emphasize that countering the rise in cyber threats calls for synergized efforts, and for every individual to play their role in safeguarding their part of cyberspace.

EZRA CHILOBA
DIRECTOR GENERAL

National Cybersecurity Strategy

"Cyberspace is the new strategic high ground in the fourth industrial revolution"

Development of the National Cybersecurity Strategy 2022-27

The ICT sector plays a critical role in Kenya's economy. As Kenya laid the groundwork towards a digital economy, the Government recognized the need to provide for cybersecurity at the national level, as a means of enabling economic growth while protecting the interests of the Kenyan people against the rising threat of cybercrime. It is this strategic awareness that led to the development of the National Cybersecurity Strategy 2014-2019.

The inaugural Strategy sought to clearly define Kenya's cybersecurity vision, goals, and objectives towards securing the nation's cyberspace, while continuing to promote the use of ICT to enable Kenya's economic growth. Towards this, the Strategy was anchored on the three pillars of the Vision 2030, while supporting and leveraging on other national initiatives such as the National ICT Master Plan. The strategy also took cognizance of initiatives taken to promote improved cybersecurity. including the Kenya Information and Communications ACT, CAP 411A as amended by The Kenya Information and Communication (Amendment) ACT, 2014 , the formation of the National Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC), and the establishment of the National Certification Authority Framework.

The Strategy sought to support and mature GoK's cybersecurity posture by providing a strategic cybersecurity direction with accompanying implementation actions to secure the nation's critical cyber infrastructure against existing and emerging threats. The successful implementation of this inaugural cybersecurity strategy is evident in enhanced national cyber threat detection and analysis capabilities, enhanced capacity building and cyber awareness, as well as the implementation of the National Public Key Infrastructure, amongst other milestones. With the Strategic period coming to an end in 2019, this necessitated the development of a new strategic document to guide national cybersecurity efforts for the next five years.

The proposed strategy seeks to provide direction towards a unified approach in the implementation of cyber security activities in Kenya. The strategy identifies six key pillars to guide effective interventions towards enhancing Kenya's cyber posture. The proposed strategy envisions a trusted cyberspace for the people of Kenya, with the overarching mission being to build a secure and resilient cyberspace through a coordinated approach that will maximize on the benefits of a digital economy.

The proposed strategy pillars are as follows:
Cybersecurity governance which seeks to enhance Kenya's institutional framework for cybersecurity governance and coordination.
Cybersecurity policies, laws, regulations and standards which seeks to strengthen cybersecurity policies, laws, regulations and standards.
Critical information infrastructure protection (CIIP) which seeks to enhance the protection and resilience of CIIs.
Cybersecurity capability and capacity building which seeks to strengthen cybersecurity capability and capacity.
Cyber risks and cyber crimes management which seeks to minimize cyber risks and cyber crimes.
Cooperation and collaboration which seeks to foster national and international cooperation and collaboration.

Children & the Internet

"Top targeted spaces by predators include: Online gaming platforms, instant messaging social platforms, and social media"

Kenya's digital ecosystem enables individuals to access critical services while also providing them with the opportunity to leverage on global resources for socio-economic development. In this digital eco-system, the Internet is a key component, and children have not been left out. Indeed, children are increasingly using the Internet for learning, networking, and entertainment. Consequently, children are increasingly being targeted and negatively influenced in this digital space.

Digital platforms that provide entertainment, collaborative spaces, and networking channels such as online gaming, instant messaging, and social media, remain the top preferred online spaces for children to interact. Worryingly, predators are increasingly infiltrating these platforms for malicious and criminal purposes suck as perpetrating cyberbullying, cyber stalking, child pornography, sexual harassment, recruiting and grooming children into terrorist affiliation groups, online fraud, spreading fake news and online propaganda, among others.

Indeed, there has also been a rise in reports of children participating in social media trends and challenges that endanger their safety, and increase incidents of violence and suicide amongst children. In addition, these social media challenges are increasingly used to spread misinformation and disinformation amongst children, as well as harvesting of Personally Identifiable Information (PII) linked to children for malicious purposes.

During this period, the Authority continued to roll out the Child Online Protection program that seeks to empower children, parents, guardians, and educators with the skills, knowledge and values to enable the safe and positive use of the Internet.

In addition, the Authority continues to leverage on the power of collaboration with various stakeholders towards enhancing the effectiveness and reach of Child Online Protection initiatives.

Parents, and care givers are encouraged to assess resources on child online protection by visiting: https://cop.ke-cirt.go.ke/ .

Social Media & Fake News

Unpacking Misinformation and Disinformation

Social media platforms are an attractive playing ground for cyber threat actors. With millions of users, the temptation to stir the waters for malicious purposes is too hard to resist. According to the USIU-Africa Kenya Social Media Landscape Report 2020, Kenyans on average spend more than one hour daily on social media. This increased use of social media offers an attractive playing ground for cyber threat actors. Consequently, cyber threat actors are increasingly using sophisticated tools such as synthetic media, which include Deepfakes and malicious bots to spread misinformation, disinformation, and fake news campaigns.

While misinformation and disinformation are both wrong/false information, the distinction between the two lies in the intent. Misinformation is false or misleading information that is unwittingly shared. Disinformation on the other hand is false information that is shared deliberately to mislead, deceive and manipulate the target audience. Disinformation is a subset of propaganda, and is intentionally and carefully crafted and targeted so as to influence the behavior and ultimately, the decision of the target audience.

Be cyber smart, report cyber incidents to the National KE-CIRT/CC through the KECIRT Mobile application or through incidents@ke-cirt.go.ke.

Global Cyberthreat Concerns

The cyber threat landscape continues to rapidly evolve, with cyber security solutions often times playing catch-up to the sophisticated and agile cyber threat actors.

Cyber threat actors continued to carrying out large-scale targeted attacks by leveraging on cryptocurrency scams, carrying out sophisticated ransomware attacks and running automated malware campaigns targeting critical infrastructure systems such as the energy and healthcare sectors, financial services, supply chains, and government services. These attacks compromised sensitive information and public safety. This trend has led to a rise in collaborative efforts between countries, that are geared at cyber awareness and capacity building.

ESTIMATED COST OF CYBERCRIME IN 2021

$6.9 Billion*

According to the FBI annual Internet Crime Report

Cyber Updates

Ransomware

Ransomware gangs accelerated the adoption of Ransomware-as-a-Service (RaaS) to run highly customizable ransomware executables that support multiple encryption methods to compromise corporate environments.

In addition, cyber threat actors continued to take up automated and Artificial Intelligence (AI)-enabled attack techniques for purposes of automating and scaling their attacks. These attacks were primarily targeted at supply chain, government services, manufacturing and healthcare sectors, Information Technology/Operational Technology (IT/OP) enterprise and industrial operations.

Insider Threats

A significant number of cyber threats are attributed to insider threats.

However, the vast majority of insider threats are unintentional, and are as a result of negligent behavior ranging from leaving devices unattended in public spaces, acting on digital communication before verifying them, poor password hygiene, negligence of organization's security protocols, or lack of top-bottom security controls that enable a gateway for potential breaches.

The Year in Numbers

444,055,806

Cyber Threats Detected by the National KE-CIRT/CC during the period July 2021 - June 2022

During the FY 2021/22 (July 2021 - June 2022), the National KE-CIRT/CC detected 444,055,806 cyber threat events.

This was a 180.3% increase from the 158,404,552 threat events detected in the previous FY 2020/21 (July 2020 to June 2021).

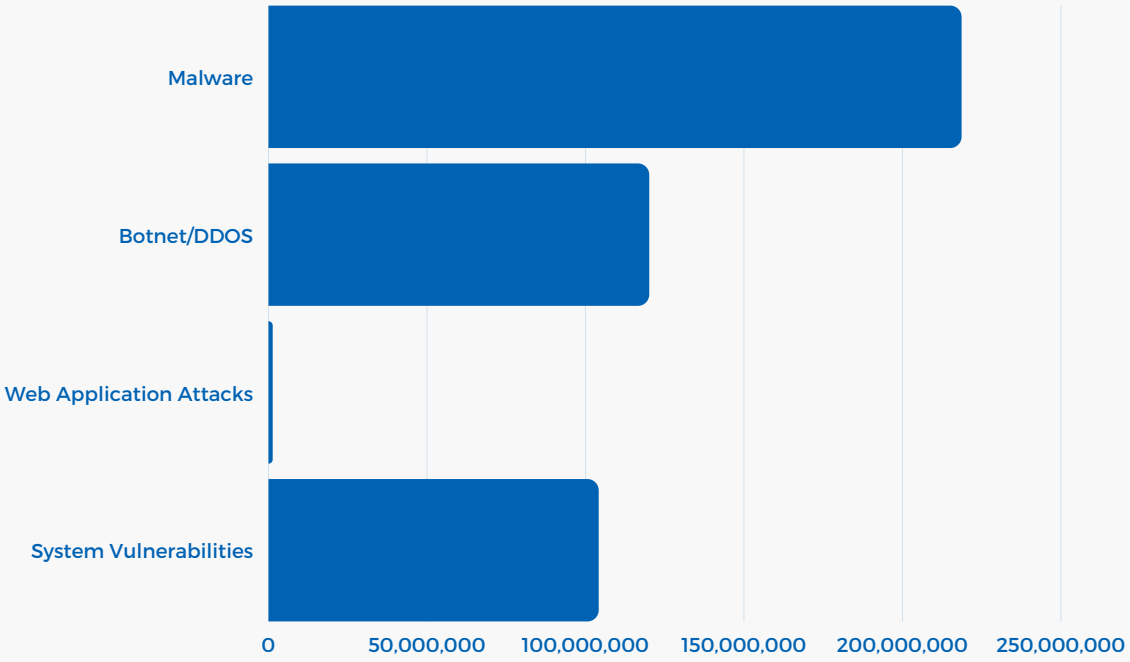
7,973,129

Cyber Advisories issued by the National KE-CIRT/CC during the period July 2021 - June 2022

In response to the detected cyber threat attempts, the National KE-CIRT/CC issued 7,973,129 technical cybersecurity advisories to affected organizations.

This was a 8,409.6% increase from the 93,696 advisories which were shared in the previous period, July 2020 to June 2021.

Cyber Threat Vectors



Cyber Threat Events Detected by the National KE-CIRT/CC during the period July 2021 - June 2022

444,055,806

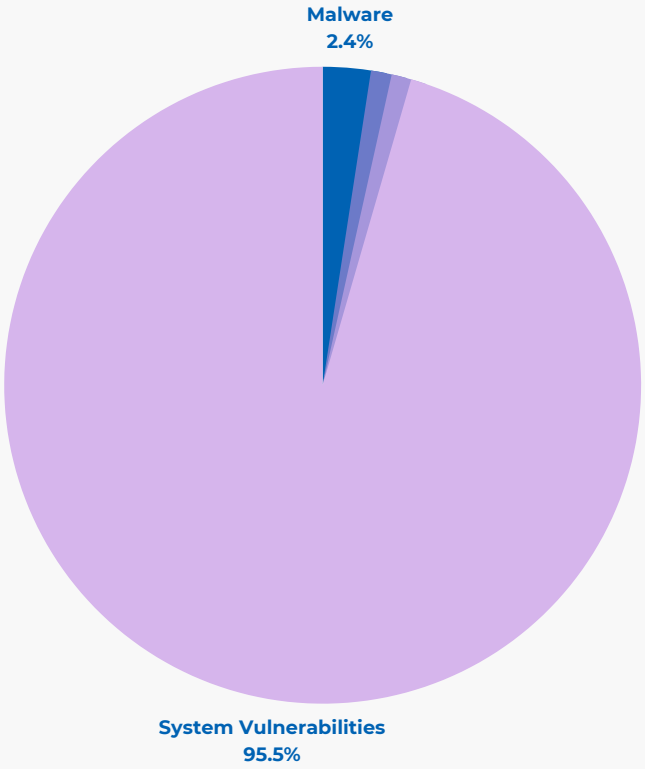
Technical Cyber Advisories Issued by the National KE-CIRT/CC during the period July 2021 - June 2022

7,973,129

Percentage annual change in the number of cyber threat attempts detected by the National KE-CIRT/CC

180.3%

Cyber Advisories



The National KE-CIRT/CC continued to issue Technical Cybersecurity Advisories to organizations. These technical advisories provide detailed insights to assist in cyber threat response.

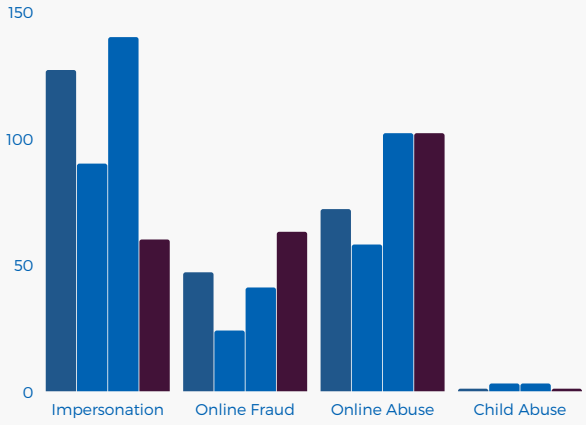
July 2020 - June 2021	July 2021 - June 2022
93,696	7,973,129

% Change

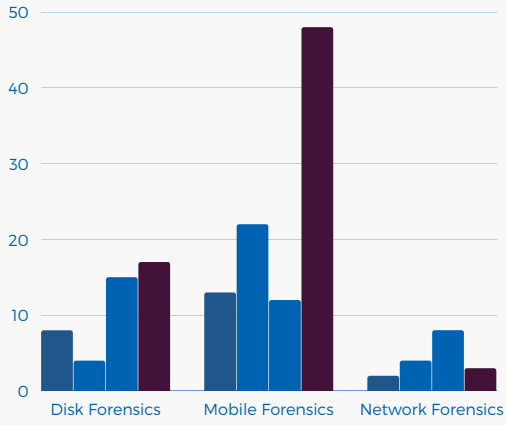
8,409.6%

Digital Forensics & Investigations

Digital Investigations



Digital Forensics



Digital Investigations facilitated by the National KE-CIRT/CC Digital Forensics Lab during the period July 2021- June 2022

947

Digital forensics facilitated by the National KE-CIRT/CC Digital Forensics Lab during the period July 2021- June 2022

156

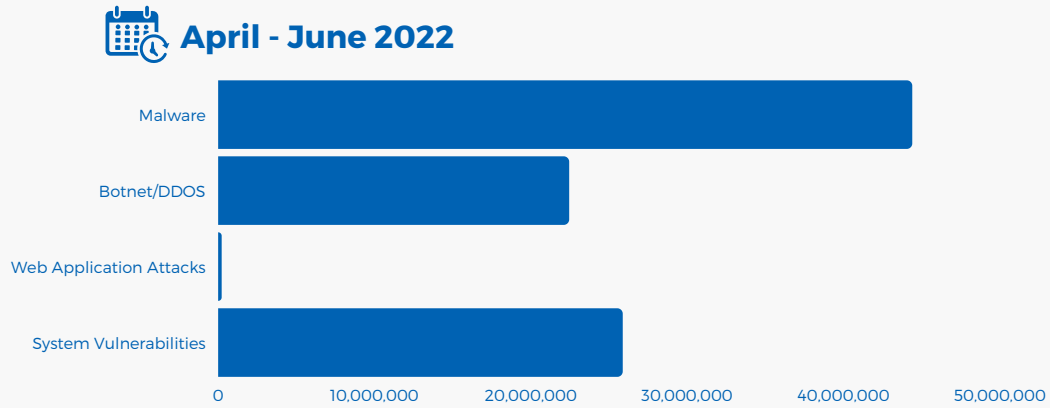
Annual % Change in Digital Investigations facilitated by the National KE-CIRT/CC Digital Forensics Lab

32.6%

Annual % Change in Digital forensics facilitated by the National KE-CIRT/CC Digital Forensics Lab

24.8%

April - June Cyberthreat Landscape



Cyber threat events detected by the National KE-CIRT/CC during April - June 2022

92,838,258

% Change from the previous period Jan - Mar 2022

17.3%

FY 2021/22 Cybersecurity SWOT Analysis

Strengths

- Implementation of Kenya's Computer Misuse and Cybercrimes Act 2018 (CMCA);
- Enhanced local and international collaborative efforts on cybersecurity management
- Enhanced capacity building efforts
- Development of a new national cybersecurity strategy
- A robust and well positioned National KE-CIRT/CC

Weaknesses

- Slow adoption of cybersecurity security measures in both public and private sector
- Low cyber hygiene practices amongst end users
- Low budgetary allocation for cybersecurity in both public and private sector
- Low cybersecurity professional capacity

Opportunities

- Collaboration amongst public and private sector in cyber awareness initiatives and capacity-building programs
- Collaboration in research and innovation with academia
- Government support towards cybersecurity efforts through an enabling policy and legal framework

Threats

- Rise in the adoption of sophisticated tools and automated attack techniques, by cyber threat actors
- Increase in the spread of fake news on social media
- Rise in coordinated cybercrimes groups (cybergangs)

Cyber Readiness

Understanding Organizational Cyber Readiness

Cyber readiness is variously defined as the process of integrating cyber security measures for purposes of being able to detect and effectively respond to cyber security incidences from both inside and outside the network. Cyber readiness encompasses the ability to identify, prevent, and respond to cyber threats.

Cyber Readiness Plan

A cyber readiness plan specifies the mandatory cyber security policies, procedures, and controls required to protect an organization against cyber threats and cyber risks.
It also includes elements of prevention, business continuity and recovery strategies.

Cyber Awareness

According to the IBM Cyber Security Intelligence Index Report, 95% of cyber security breaches are primarily caused by human error.
Cyber awareness training therefore assists employees to understand what cyber threats look like, how they work, and how they should respond when they encounter a threat.
Cyber awareness targeting both internal and external stakeholders such as employees, customers, as well as third party contractors is recommended.

Cyber Advocacy & Partnerships

Cybersecurity Policy: The National KE-CIRT/CC is dedicated to the development of enabling policy environment towards enhancing Kenya's cyber readiness and resilience.

Enabling partnerships: The National KE-CIRT/CC leverages on collaboration frameworks with local and international stakeholders to build Kenya's national cyber readiness and resilience.

Educating a digital citizenry: The National KE-CIRT/CC issues cyber threat advisories to affected parties and creates cybersecurity awareness that is geared at enhancing individual and organizational cyber hygiene.

Reinforcing knowledge: The National KE-CIRT/CC builds the capacity of critical information organizations and the public through fireside chats, bootcamps and county cyber clinic training.

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