



COMMUNICATIONS
AUTHORITY OF KENYA

Cybersecurity Report

April - June
2023

PREPARED BY

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



The ICT industry is a very vibrant and evolving sector and this calls for us to have a proactive approach in safeguarding our digital ecosystem even as we move towards embodying a digitally transformed nation.

For instance, In the last six (6) years, we have been able to detect an upward trajectory in cyber threats from 7,755,437 in the FY 2016/2017 to 444,055,806 in the FY 2021/2022.

Recognizing the concerning increase in attacks by threat actors, the importance of safe-guarding the digital landscape and nurturing the next generation of cybersecurity professionals against the backdrop of a widening attack surface, the Authority has taken significant strides in the last two (2) years to enhance capacity building initiatives, particularly in academia. The Authority continues to work closely with universities and educational institutions to equip students with the necessary knowledge and skills through the CA Bootcamp and Hackathon Series.

This year, the Bootcamp and Hackathon Series will be held in line with the overarching OCSAM 2023 theme: *'The Paradox of Progress: Securing a Digital Nation'*.

The Authority seeks to extend the Bootcamp and Hackathon Series reach even further by engaging a larger number of students across the country through the regional offices in Nairobi, Nyeri, Kisumu, Eldoret and Mombasa.

This is in cognizance of the power in collective empowerment where empowering more individuals with cybersecurity expertise, contributes not only to personal growth but also to the overall cybersecurity resilience of the nation. We have received over 6,000 participants for the Bootcamp and Hackathon Series representing a drastic growth from last year's 1,500+ participants.

In addition, the Authority's commitment extends beyond knowledge transfer and skill development. The Authority recognizes the need to guide and enable an ethical community of practice. Therefore, the Authority seeks to incorporate a mentorship aspect into this series. By pairing students with experienced professionals and industry leaders, the Authority aims to foster a culture of ethical behavior, responsible use of technology, and continuous learning. This mentorship component will play a crucial role in shaping Kenya's future cybersecurity workforce.

As we embark on this journey of empowerment and innovation, let us not forget the underlying purpose of our efforts—to build a cyber-ready and resilient nation. Building a secure digital superhighway is not an isolated goal; it is an essential part of our national agenda. This involves ensuring that Kenyans, businesses, and institutions can leverage technology with confidence, knowing that their digital assets are protected, and their privacy is respected.

In conclusion, let us embrace this Bootcamp and Hackathon Series as a catalyst for change that propels Kenya towards a future where we are cyber-ready and resilient. Together, let us build a secure digital ecosystem that not only safeguards our interests but also propels us towards progress and prosperity.

Ezra Chiloba
Director General



Cyber Threat Roundup

“The hacker didn't succeed through sophistication. Rather he poked at obvious places, trying to enter through unlocked doors. Persistence, not wizardry, let him through.”

— Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*

Info Stealers

Info stealers, also known as data stealers are a type of malicious software designed to secretly gather and steal sensitive information from a targeted user or system. Info stealers operate by secretly infiltrating a computer or network and accessing various types of data without the user's knowledge or consent.

Cyber threat actors use info stealers for purposes of stealing users' sensitive data such as usernames, passwords, bank account details, phone numbers, and email addresses to perpetrate online identity theft and financial fraud.

Under the "Malware-as-a-Service" (MaaS) business model, cyber threat actors are able to obtain different types of info stealer malware at a fee from malicious actors who offer the malware to subscribers.

To address this rising threat, users are advised to adopt the following cyber hygiene practices: use verified and updated antivirus software; regularly patch operating systems and applications; always verify online communication before acting on it; and use strong and unique passwords for all online accounts.



What is targeted?

- Usernames and passwords
- Bank account details
- Email address
- Phone number

Top Cyber Threat Concerns around the Globe

Bandit Stealer

Bandit stealers are a type of information stealing malware that targets web browsers and cryptocurrency wallets. Cyber threat actors use Bandit Stealer to compromise web browsers and cryptocurrency wallets for purposes of propagating identity theft, financial fraud, data breaches, credential stuffing attacks, and account takeovers.

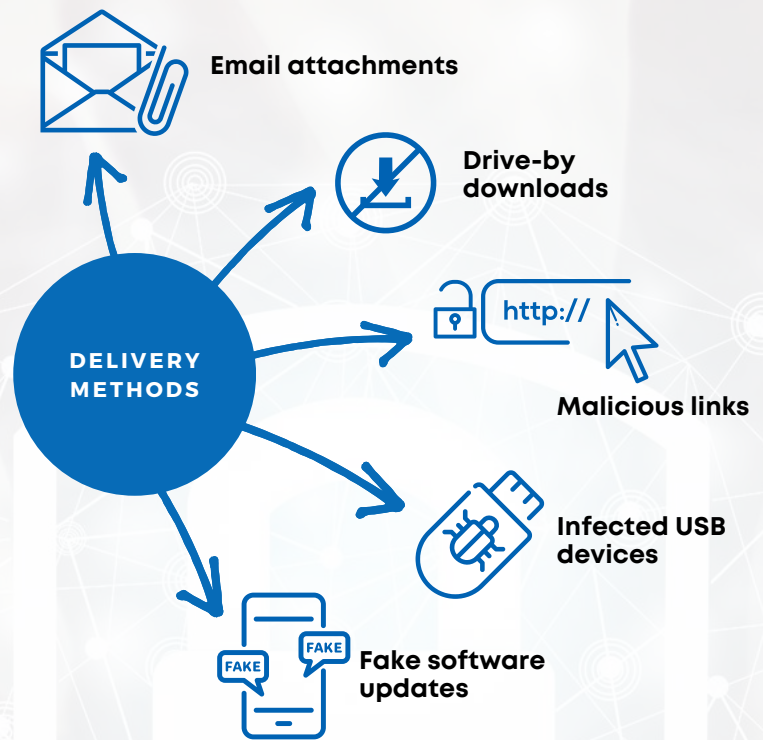
Bandit stealer is written in the Go programming language, which has become very popular with malware developers, with this choice of language meaning that it can potentially expand to other platforms due to its flexible codebase. Indeed, Bandit Stealer has been marketed and sold as a service on underground criminal forums since April 2023.

Once the bandit stealer malware has penetrated into the user's computer, it implements various checks to determine if it's running in a sandbox or virtual environment, whereafter it terminates a list of processes to conceal its presence on the infected system, and sends stolen information to a command and control server via Telegram.

By establishing persistence by means of Window Registry modifications, Bandit Stealer ensures that it is executed every time the infected system starts up. This way, even after a system shutdown, the malware can still operate and steal data from the victim's system.

What is being targeted?

- Personally Identifiable Information (PII)
- Corporate credentials
- Financial data
- Intellectual property



Users are advised to adopt the following cyber hygiene practices as a protective measure against bandit stealers: keep software up to date; use strong and unique passwords; verify online communication before acting on it; regularly scan systems with reputable antivirus and anti-malware software; apply multi-factor authentication on all digital accounts; and encrypt sensitive data.

Ransomware-as-a-service

Ransomware-as-a-Service (RaaS) is a business model that enables cyber threat actors to develop and provide ransomware tools and infrastructure as a business service to individuals who wish to conduct their own ransomware attacks.

RaaS systems include an easy-to-use interface that enables non-technical users to develop and launch ransomware campaigns.

Ransomware-as-a-Service (RaaS) has transformed the threat landscape and contributed to the proliferation of ransomware attacks by lowering the entry barrier for potential cybercriminals.

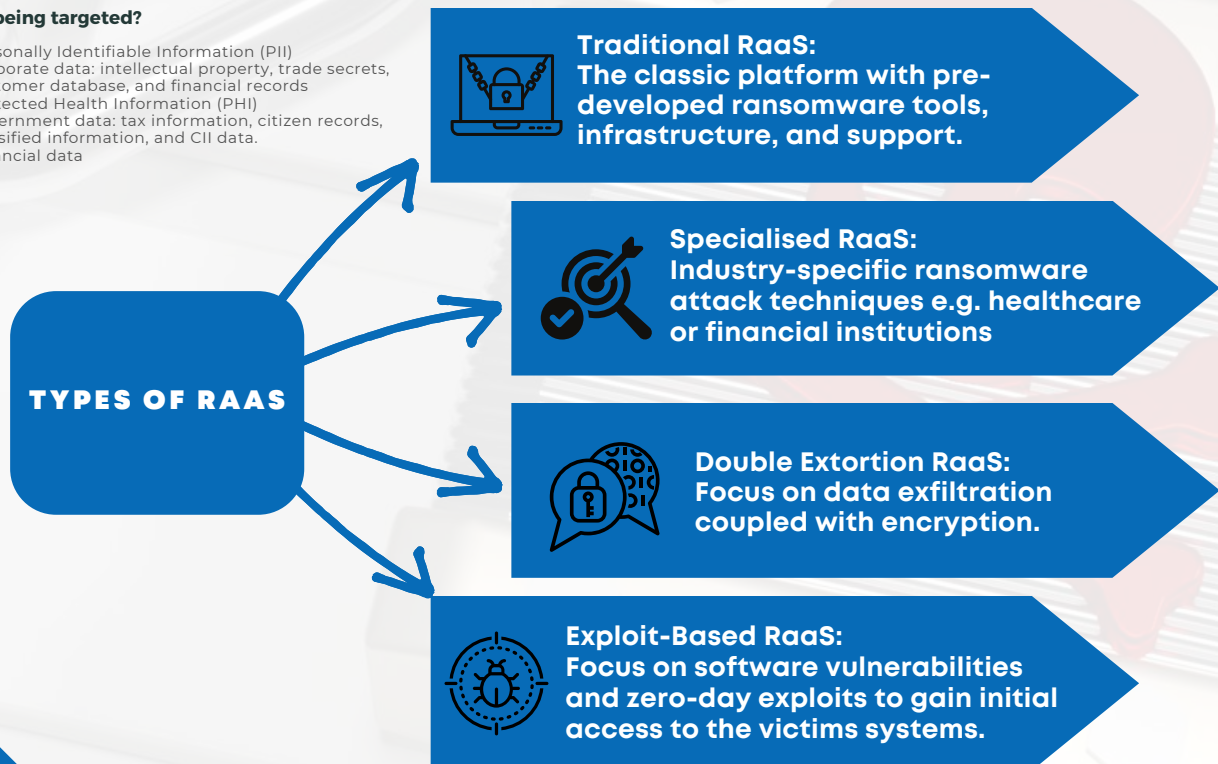
Cyber threat actors handle the development, maintenance, and support of the ransomware software, while the affiliates distribute the malware and conduct the actual attacks. For every ransomware attack launched through the RaaS model, cyber threat actors receive a percentage of the ransom payments.

RaaS has allowed a broader spectrum of individuals to participate in ransomware attacks without requiring substantial technical knowledge or resources.

This strategy has resulted in a surge in the volume and sophistication of ransomware attacks, making it a rising concern for individuals, businesses, and organisations globally.

What is being targeted?

- Personally Identifiable Information (PII)
- Corporate data: intellectual property, trade secrets, customer database, and financial records
- Protected Health Information (PHI)
- Government data: tax information, citizen records, classified information, and CII data.
- Financial data



Children & the Internet:

Gaming Safety

As technology advances and online gaming becomes increasingly popular, cyber threat actors are also increasing their presence on these platforms with the aim of infiltrating systems and compromising children who are a primary audience on online gaming platforms.

Online gaming involves creating digital identities and communicating with other players to enhance both collaborative and competitive gaming that happen in both public and private spaces.

Creating these digital identities means giving up personal information such as full name, age, residence, and contact information.

Cyber threat actors hop onto gaming platforms counting on children's vulnerability and blind trust that other players on the platform are only in it for friendly gaming.

However, cyber threat actors masquerade as peer gamers to befriend children and leverage the chat functions on these platforms to gather private information for purposes of propagating identity theft, cyberbullying, child pornography, online grooming and other forms of exploitation.

Worryingly, cyber threat actors extend the online threats to the physical world where they establish online connections that lead up to offline meet-ups with children masked as meetings with a friend or confidant for purposes of recruiting them into illegal activities such as drug trafficking and organised crime, as well as carrying out child trafficking, exploitation, and abuse among others.

In view of prioritising online gaming safety against this trend, the Authority continues to assist in the investigation and prosecution of cybercrimes targeted against children, as well as collaborate with agencies involved in different elements of Child Online Protection (COP). Further, parents, teachers, and guardians are advised to monitor children's online activity, as well as establish open communication with children to encourage sharing of their online experiences.

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

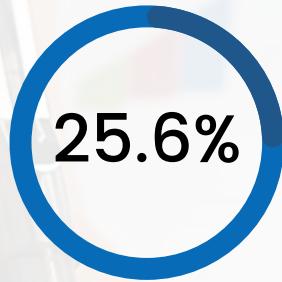


Cyber Threat Landscape in Numbers

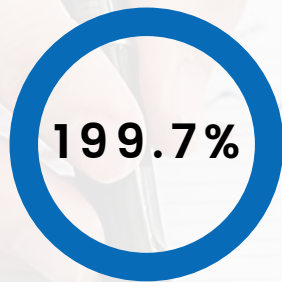
“Threat is a mirror of security gaps. Cyber-threat is mainly a reflection of our weaknesses. An accurate vision of digital and behavioural gaps is crucial for a consistent cyber-resilience.”

— Stephane Nappo

April - June 2023 Cyber Threat Landscape Roundup



During the period April to June 2023, the National KE-CIRT/CC detected 139,775,123 cyber threat attempts targeting critical infrastructure service providers. This represented a 25.6% change from the last period.



During the period April to June 2023, the National KE-CIRT/CC issued 10,742,859 cyber threat advisories to critical infrastructure service providers. This represented a 199.7% change from the last period.

% Change in cyber threat attempts detected by the National KE-CIRT/CC from the previous period (Jan to March 2023)



25.6%

% Change in cyber threat advisories issued by the National KE-CIRT/CC from the previous period (Jan to March 2023)

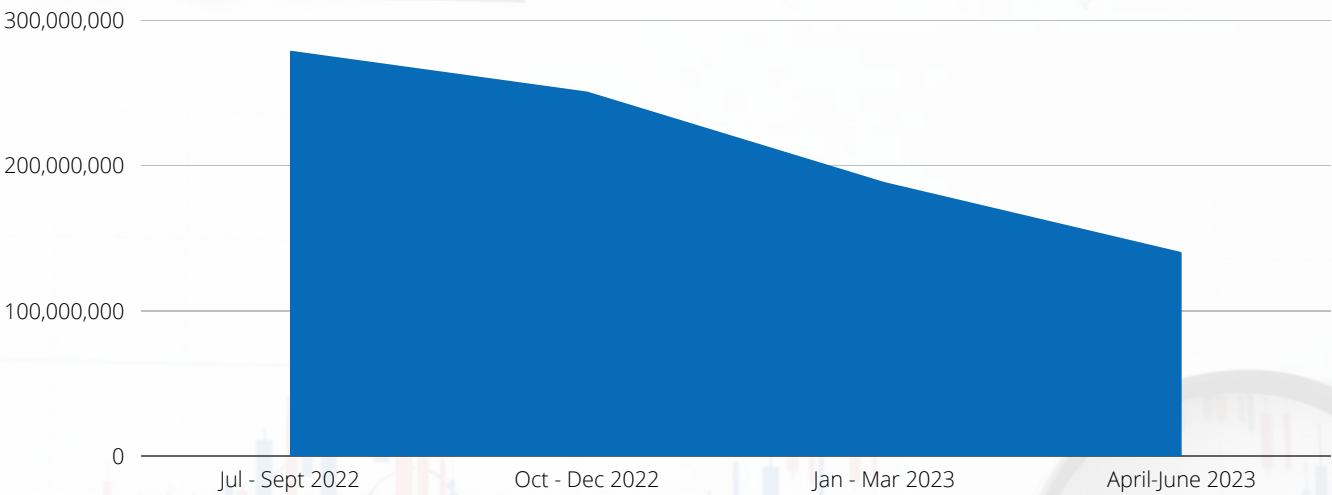


199.7%

12 Months Cyber Threat Trends Analysis

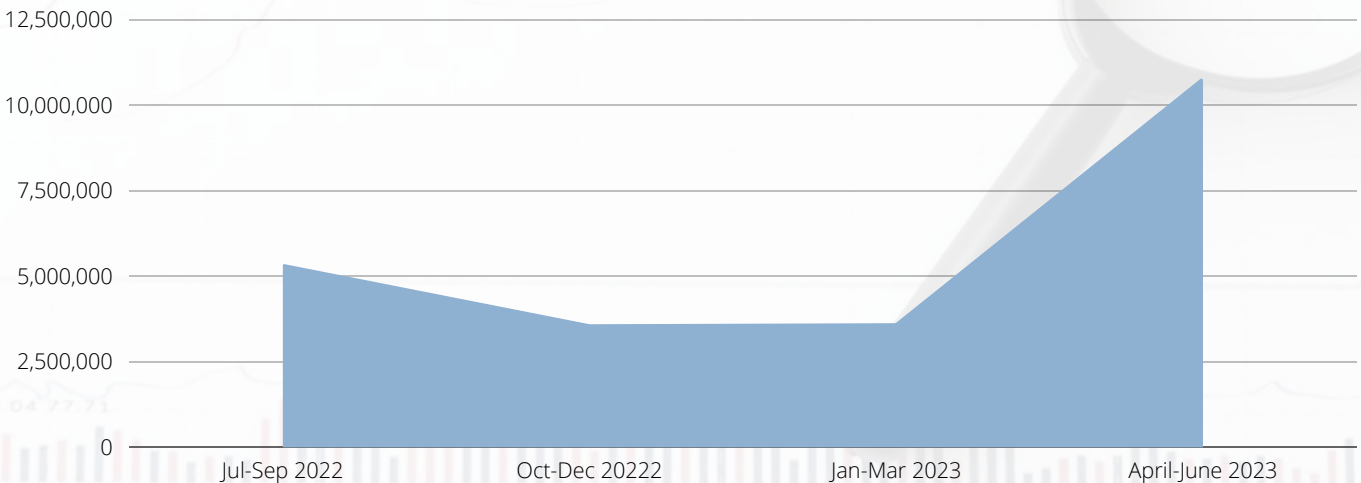
During the period April to June 2023, the National KE-CIRT/CC detected 139,775,123 cyber threat events, which was a 25.6% decrease from the 187,757,659 threat events detected in the previous period, January to March 2023.

This trend in cyber threat events detected is attributed to the continued activity by organised cybercrime groups; adoption of more sophisticated tools by ransomware gangs; continued targeted attacks at critical systems and services; adoption of sophisticated phishing and malware kits by threat actors; continued targeted attacks at cloud-based supported services and unsecured infrastructure; continued network misconfiguration attacks; and continued adoption of botnet and Distributed Denial of Service (DDoS) attack techniques.



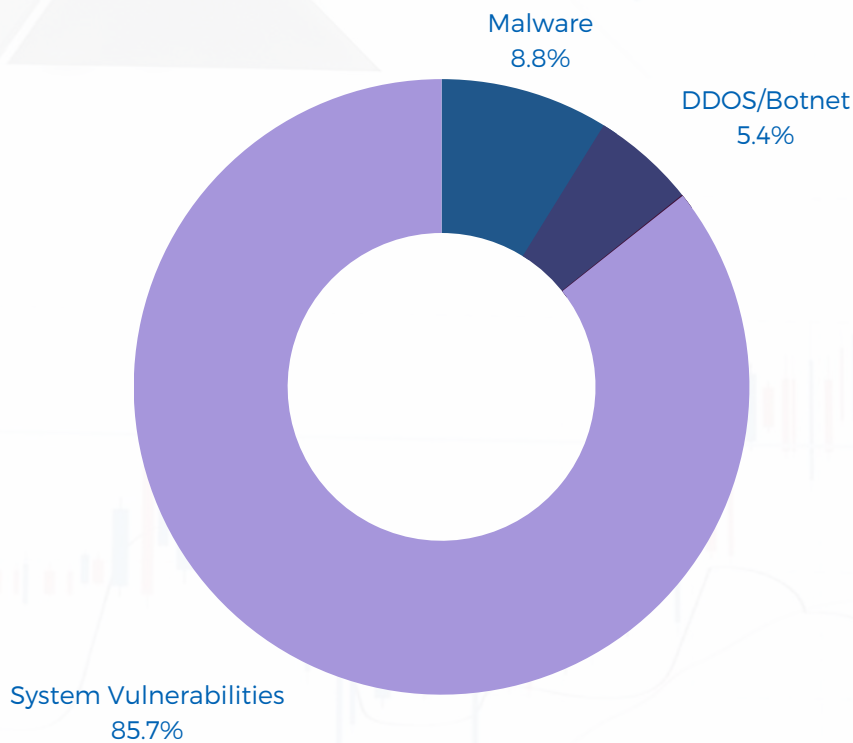
To address these emerging concerns, the National KE-CIRT/CC continued to issue Technical Cybersecurity Advisories to organisations and Cybersecurity Best Practice Guides to the public, which provided detailed insights to assist in cyber threat prevention and detection.

These included 10,742,859 advisories marking a 199.7% increase from the 3,584,966 advisories, which were shared during the period January to March 2023.



April - June 2023 Cyber Attack Vector Trends

Insight into cyber threat vector trends during the period April to June 2023:

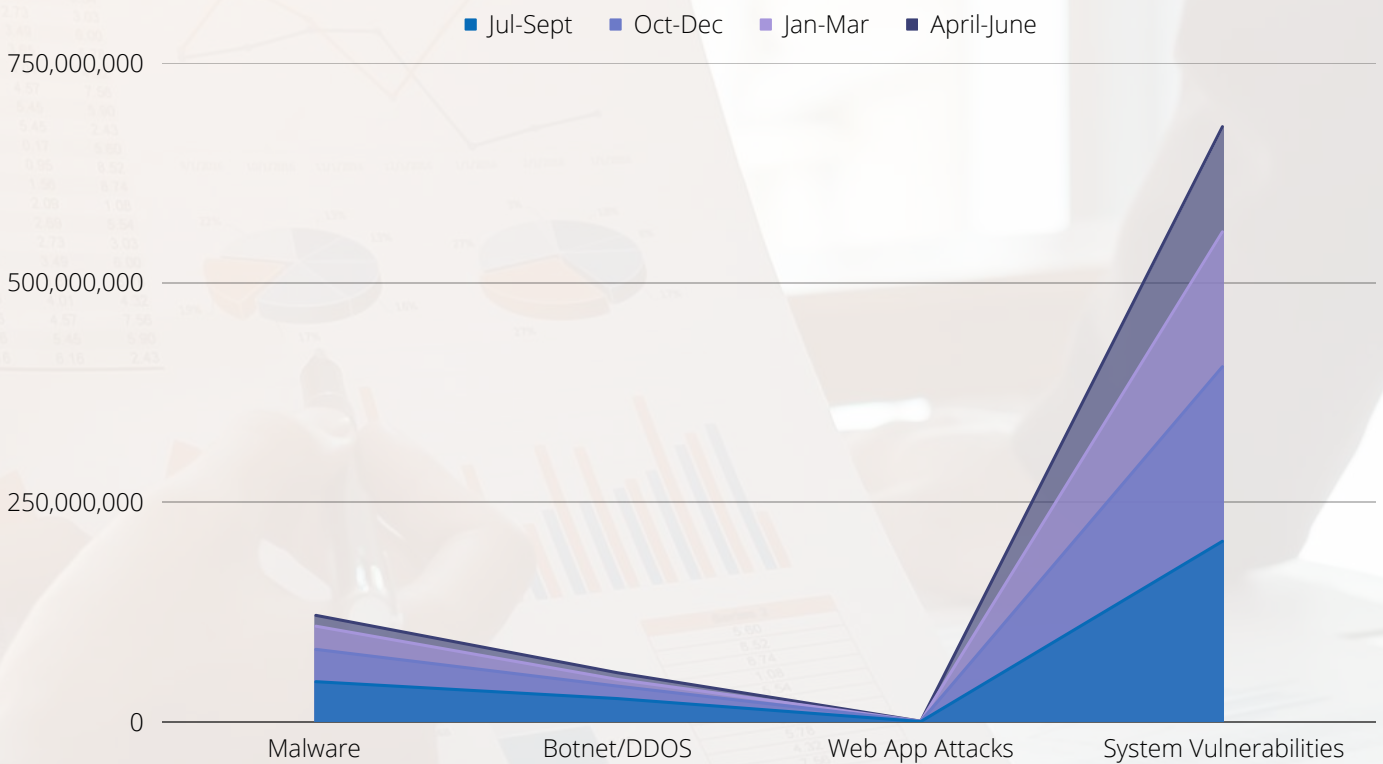


During this period, the following were notable cyber attack vector trends:

- Persistent targeted attacks at critical information infrastructure (CII)
- Decrease in DDoS attacks

12 Months Overview of Cyber Attack Vector Trends

Trend analysis of cyber attack vectors used to target critical information infrastructure service providers as detected by the National KE-CIRT/CC from July 2022 to date.

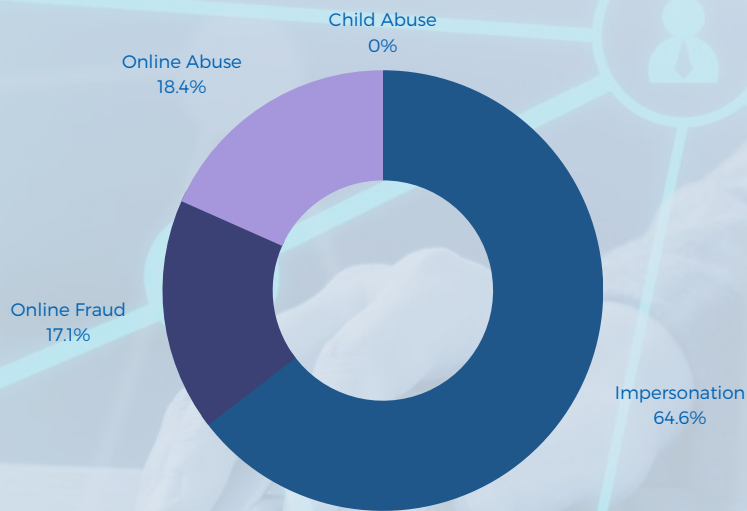


The following are the cyber threat vector trends over the past 12 months:

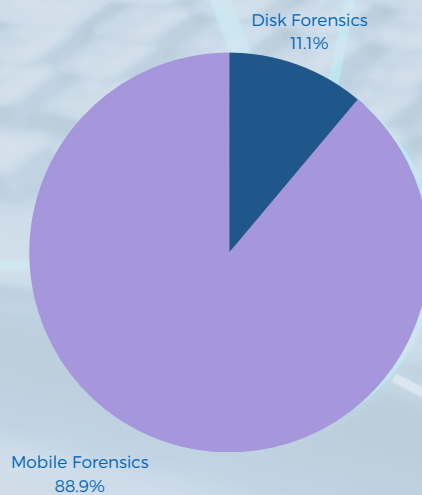
- Malware and system misconfiguration attacks continued to top the threat vectors over the past 12 months as cyber threat actors adopted sophisticated techniques to extend their attacks.

April - June 2023 Digital Forensics & Investigations Trends

During the period April to June 2023, the National KE-CIRT/CC received 158 digital investigation requests, which was a 57.9% decrease as compared to 375 requests in the previous period.

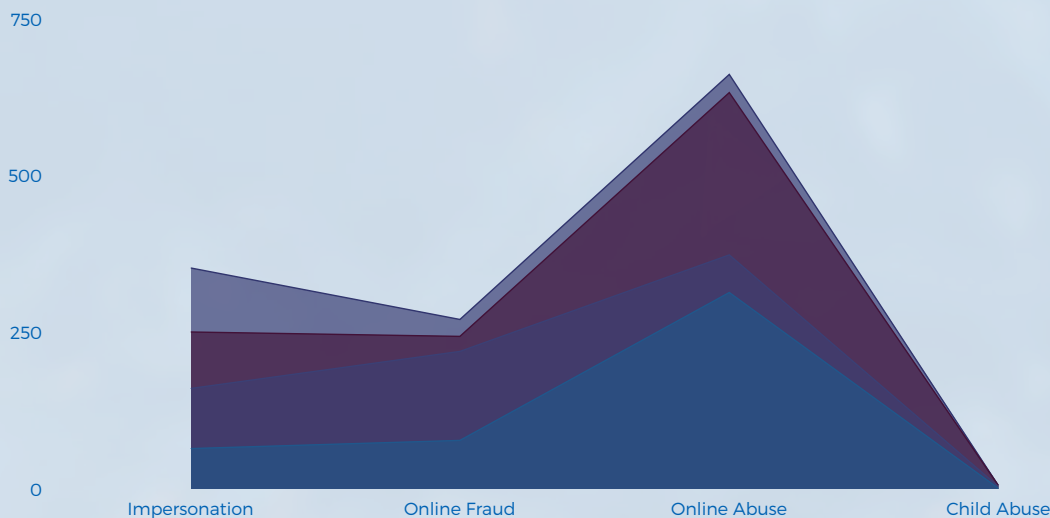


The National KE-CIRT/CC Digital Forensics Lab (DFL) carries out mobile forensics, disk forensics, and network forensics. In the period April to June 2023, the National KE-CIRT/CC Digital Forensics Lab received 18 forensic requests, which was a 52.6% decrease compared to 38 requests received in the previous period January to March 2023.

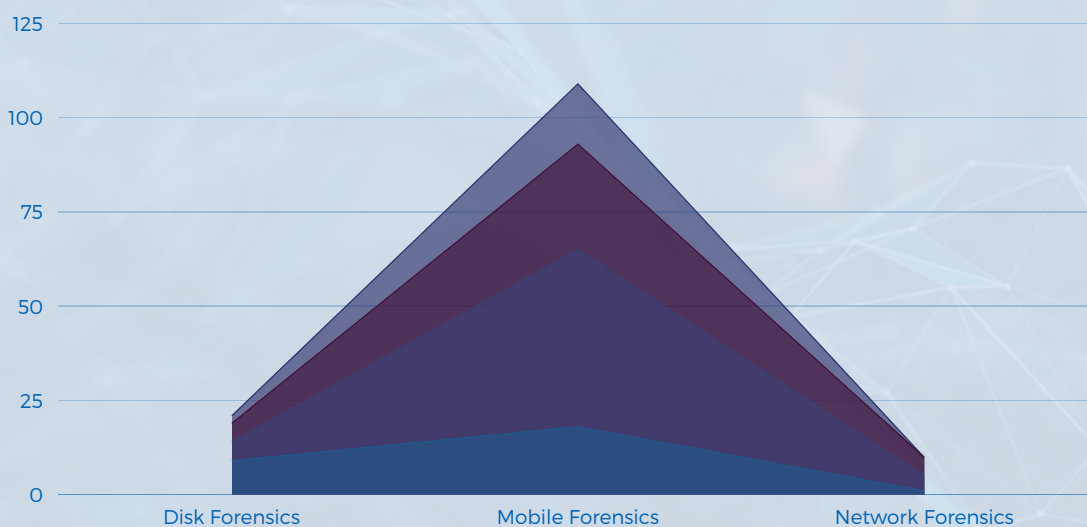


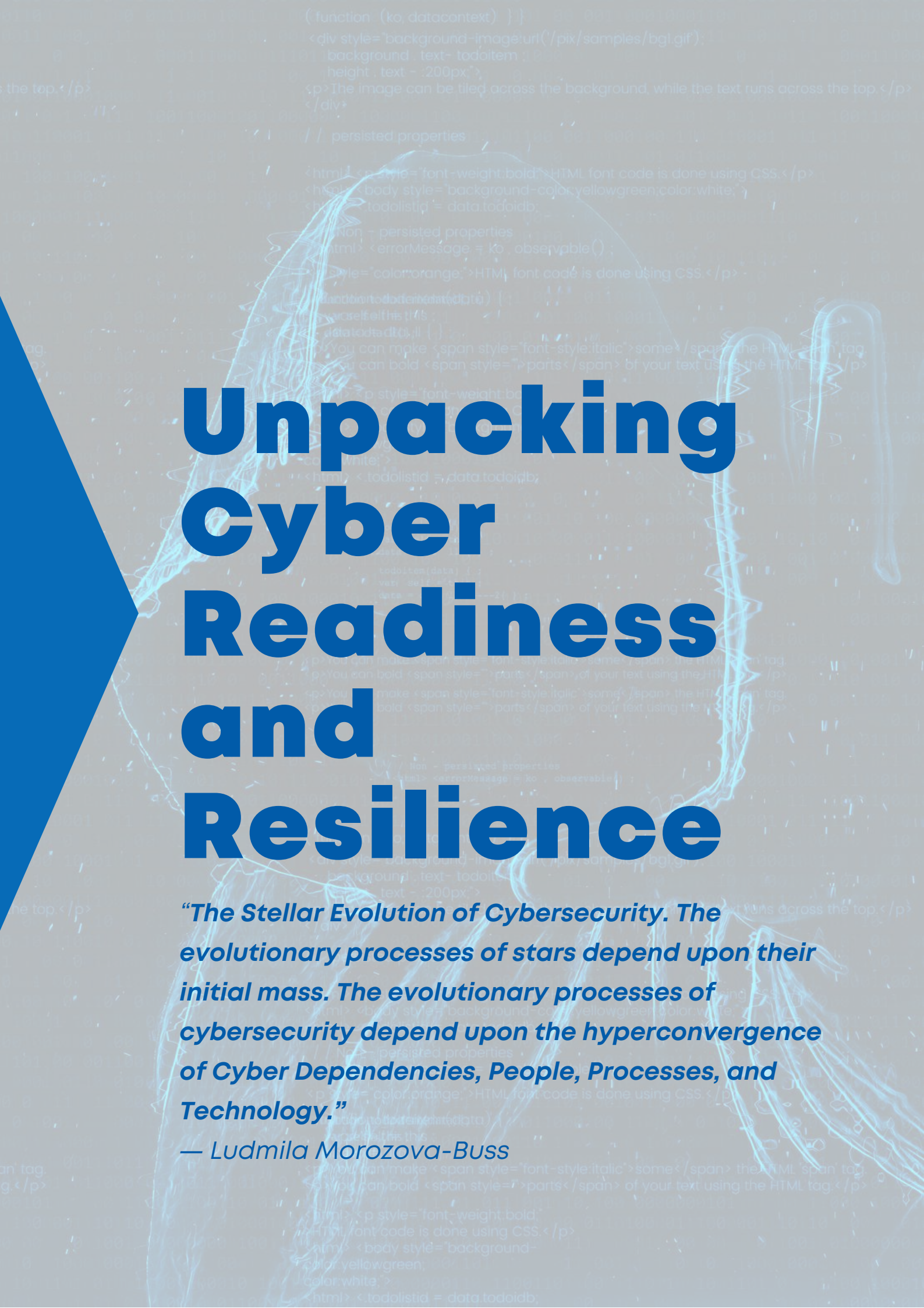
12 Months Overview of Digital Forensics & Investigations

The National KE-CIRT/CC has facilitated 1,293 digital Investigations through the Digital Forensics Lab over the last 12 months starting July 2022 to June 2023.



The National KE-CIRT/CC has facilitated 140 digital forensics through the Digital Forensics Lab over the last 12 months starting July 2022 to June 2023.





Unpacking Cyber Readiness and Resilience

“The Stellar Evolution of Cybersecurity. The evolutionary processes of stars depend upon their initial mass. The evolutionary processes of cybersecurity depend upon the hyperconvergence of Cyber Dependencies, People, Processes, and Technology.”

— Ludmila Morozova-Buss

Cyber Threats Impact Analysis



01 Financial Loss

Cyber attacks result in considerable financial loss for organisations, which can be through direct costs from cyber attack incident response, forensic investigation, data recovery, legal processes, regulatory fines, and loss of business due to compromised client trust.

02 Regulatory Compliance Issues

Cyber attacks result in non-compliance of regulatory frameworks and standards such as data protection laws and industry-specific regulations leading to fines and penalties.



03 Damage to Business Relationships

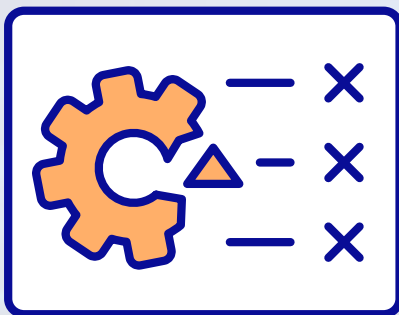
Cyber attacks disrupt critical operations causing operational delays as well as financial losses, which may result in business partners losing confidence in an organisation's ability to safeguard their data. This may affect collaborative efforts and may even result in termination of business partnerships.

Cyber Resilience in an Expanding Attack Surface



Multi-factor Authentication (MFA)

Implementing MFA adds an extra layer of security by requiring users to provide two or more forms of identification, such as a password, a unique code sent to their device, or biometric data before accessing a system or application. This helps protect against unauthorised access, even if passwords are compromised.



Incident Response Planning

Developing and regularly testing an incident response plan is crucial for cyber resilience. This plan outlines the steps to be taken in case of a cyber incident, ensuring a timely and coordinated response to minimise the impact and facilitate recovery.



Regular Backup & Recovery Procedures

Comprehensive backup and recovery protocols guarantee that organisations' vital data is backed up on a regular basis and can be recovered in the event of a cyber attack. This reduces the effect of data loss or system unavailability.

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