COMMUNICATIONS AUTHORITY OF KENYA

APRIL 2022

CYBERSECURITY REPORT

For the period January to March 31, 2022

Prepared by the
National KE-CIRT

Table of Contents

03
Message from the Director General

04
Securing the Vulnerable Online: Child Online Protection

05
Measuring Cyber Readiness and Resilience

06
Cyber Threat Statistics At A Glance

08
Overview of the Local Cyber Threat Landscape

10
Overview of Cyber Threat Response by the National KE-CIRT

11
Cyber Threat Insights

12
Cyber Safety Tips

Message from the Director General

"What if cybersecurity innovation was not playing catch up to technology development? What if we could build technology that people could trust?"

We are living in an exciting period characterized by tremendous technological innovation at a rapid pace. We are constantly being bombarded with technology innovations that are changing the way we do business, and that are transforming the lives of individuals and the society at large. Technological advancements such as Artificial Intelligence, 3D Printing, Block chain, Autonomous Vehicles, 5G, Virtual Reality and Augmented Reality, are but some of the emerging technologies that are having major social, economic and environmental impacts worldwide.

The underlying philosophy in this cutthroat technology space seems to be 'release early and release often". Everyone wants a part of cutting edge tech: consumers want it, shareholders expect it, top executives peg their reputation on how fast they incorporate cutting edge tech to add value and increase revenue.

However, often times, security is not built into new tech from the ground up. In fact, security innovation has lagged behind the development of new technology. So, while the rush is to release early and fast, safety is often times an after thought. Indeed, whatever our thoughts about cyber criminals, we must recognize their innovation and research spirit. Time and again, it is their 'penetration testing' of new tech and subsequent exploitation of the underlying vulnerabilities that have called attention to the conversation on the security of new technology.

What if cybersecurity innovation was not playing catch up to technology development? What if we could build technology that people could trust? We need to revolutionize the place of cybersecurity in the development of new technology. We need to normalize considerations of cybersecurity and in build these from the ground up in the development of new technologies.

Cyber readiness and cyber resilience require that we reassess and interlink tech innovation and cybersecurity innovation as we continue to move into a digitally enabled future. It is only by interlinking innovation and security that we shall be able to harness the revolutionary power of technology for social economic development in a safe and sustainable way.

Ezra Chiloba
Director General
Communications Authority of Kenya

Securing the Vulnerable Online: Child Online Protection

As Kenya continues to accelerate digital adoption towards becoming a digitally transformed nation, children and the youth are increasingly using the internet as a key component towards becoming digital citizens in this digital environment.

However, this has increased the exposure of this vulnerable population to various cyber harms such as exposure to child abuse material, cyber bulling, online fraud, internet addiction, violence, racism, sexual harassment, among many other dangers.

To address this, the Authority in partnership with various stakeholders developed and launched a Child Online Protection campaign dubbed “Be The COP”. This initiative was developed in line with International Telecommunication Union (ITU) renewed focus on Child Online Protection under the Global Cyber Security Agenda (GCA), which is in keeping with the Authority’s Consumer Protection mandate.

The first phase of the Child Online Protection campaign acknowledged the front line role that parents, teachers and guardians play in protecting children online, and therefore sought to increase their level of awareness of the dangers that exist online and to provide them with information on how they can encourage responsible internet usage. The campaign also sought to trigger the development of stakeholder initiatives in Child Online Protection in Kenya.

Following the success of the first phase, the Authority launched the second and current phase of the Child Online Protection programme that is dubbed “Huwezi Tucheza: Tuko Cyber-Smart”. This phase targets children and young people with a view to informing and empowering them with the skills, knowledge, and values on how to stay safe online and how to use the Internet in a productive manner, while making them advocates for responsible and productive use of the Internet.

For more information, please visit: https://cop.ke-cirt.go.ke/?_ga=2.45894180.1868369514.1646900518-1411552063.1645432911

Measuring Cyber Readiness and Resilience

Kenya continues to benefit from the gains made so far in ICTs, with increased digital adoption resulting in significant shifts in how Kenyans operate online. These shifts include remote working, increased adoption of the gig economy, adoption of online and hybrid learning, increased uptake of e-commerce, increased uptake of video conferencing applications, increase in the use of social media, amongst others.

While these changes have accelerated Kenya's digital transformation, these have also increased our vulnerability online, with cyber criminals leveraging on these shifts in behaviour to exploit vulnerabilities in these tools and platforms. This has resulted in an increase in phishing attacks, data breaches, fake news, ransomware, impersonation, false publications, incitement, online fraud, cyber bullying and harassment, child online abuse, amongst others.

Indeed, there has been a continuous upward trajectory of cyber attack attempts detected by the National KE-CIRT in the last five years, with 7,755,498 detected in the fiscal year 2016/17; 23,815,972 in the fiscal year 2017/18; 51,903,286 in the fiscal year 2018/19; 110,903,069 in the fiscal year 2019/20; and 154,404,552 in the fiscal year 2020/21 respectively.

Noting the ever increasing threat posed by the evolving and dynamic cyber threat landscape, the Authority recognized that there is need to evaluate our collective national cyber readiness and resilience as a strategy in mitigating against this rising threat.

Towards this, the Authority developed a Cybersecurity Readiness and Resilience Measurement Tool that assesses both individual and organizational cyber posture in five key domains namely: Governance; Technology and Infrastructure; Capacity and Development; Incidents, Vulnerabilities and Forensics; as well as Risk and Continuity.

The purpose of the tool is to identify the current national cybersecurity posture by assessing the level of cyber security preparedness at both organizational and individual level.

Arising from this assessment, the Authority will be able to identify existing gaps and thereafter develop strategies to address these gaps with the goal of enhancing the collective cyber readiness and resilience.

To participate in the organizational Cyber Readiness and Resilience Self Assessment, send an email to *cse@ca.go.ke*.

Cyber Threat Statistics

For the period January to March 2022

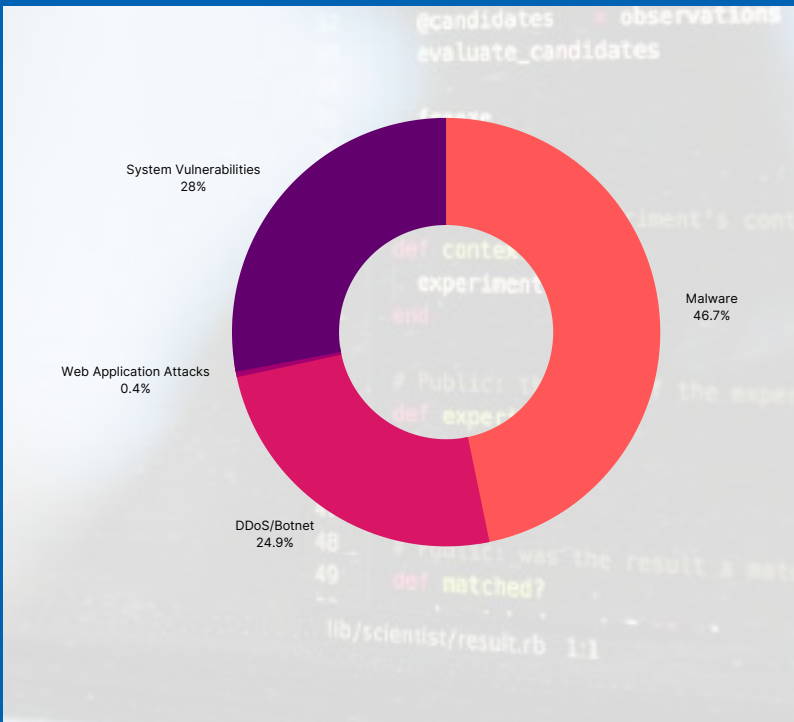
Cyber Threat Statistics at a Glance

Cyber Threat Attempts Detected

79,175,429

Cyber Security Advisories Issued

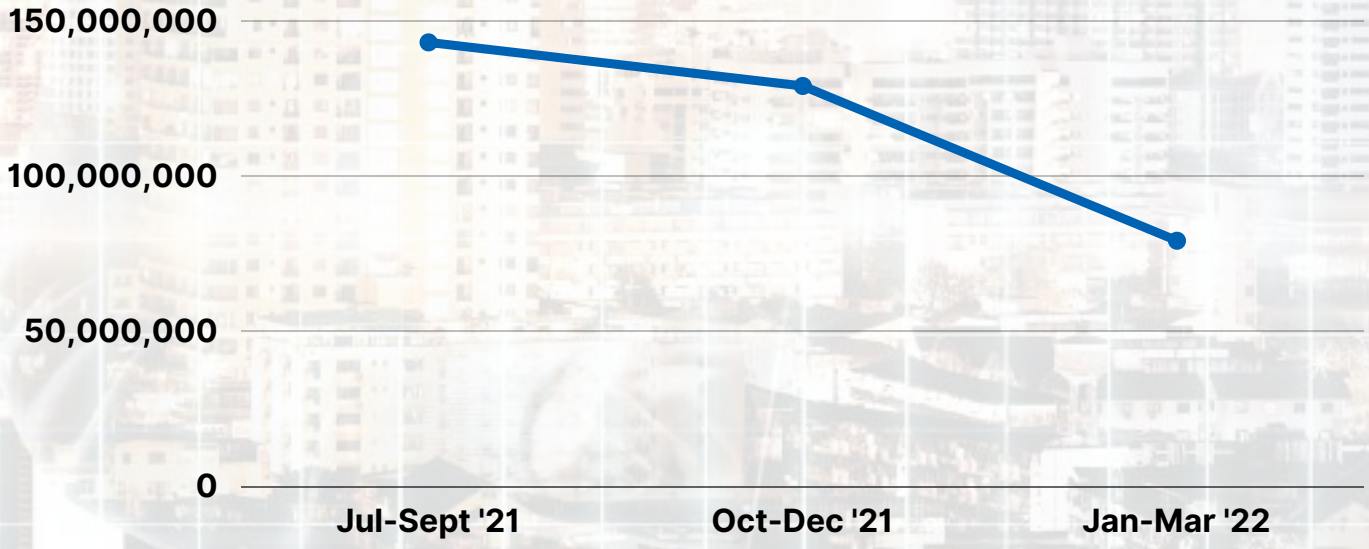
2,908,431



Overview of the Local Cyber Threat Landscape

The following is an overview of cyber attack attempts detected by the National KE-CIRT during the period July 2021 to March 2022.

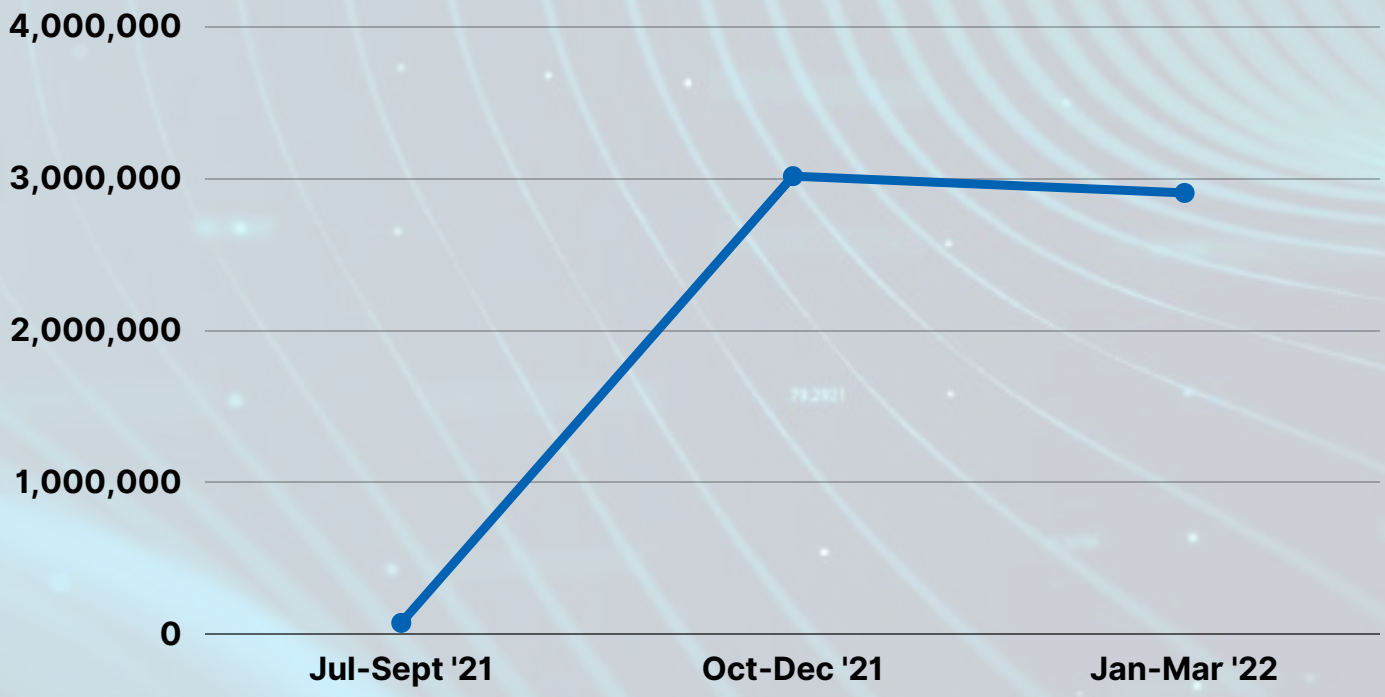
JULY - SEPTEMBER 2021	OCTOBER - DECEMBER 2021	JANUARY - MARCH 2022
143,040,599	129,001,520	79,175,429



Overview of Cyber Threat Response by the National KE-CIRT

The following is an overview of the number of cyber threat advisories issued by the National KE-CIRT to various organizations in response to detected cyber attack attempts during the period July 2021 to March 2022.

JULY - SEPTEMBER 2021	OCTOBER - DECEMBER 2021	JANUARY - MARCH 2022
73,578	3,018,545	2,908,431

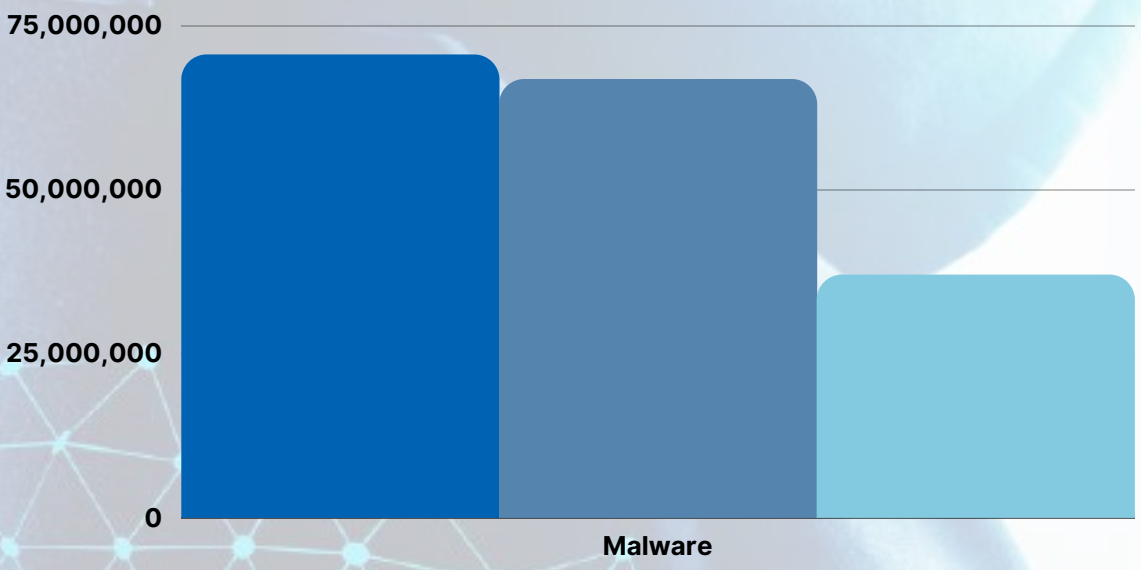


An Overview of Cyber Threat Trends over the Last FY

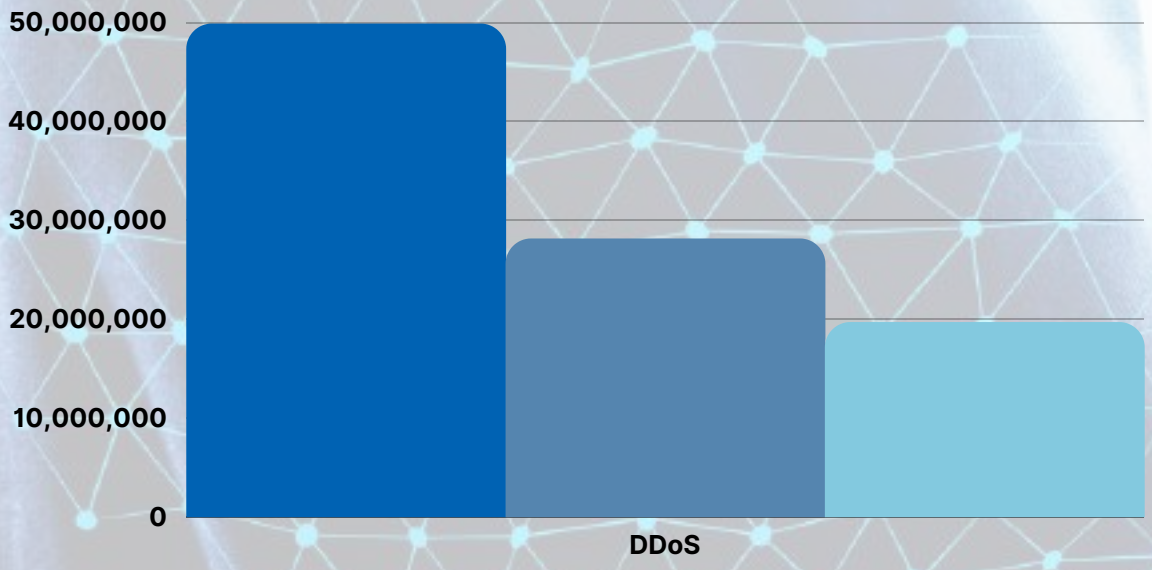
	January - March 2022	October - December 2021	July - September 2021
Overall Cyber Attack Attempts Detected	**79,175,429**	**129,001,520**	**143,040,599**
Overall Cyber Threat Advisories Issued	**2,908,431**	3,018,545	73,578
Malware	37,012,510	**66,765,638**	**70,501,144**
Advisories	**54,643**	63,165	17,896
DDoS/Botnet	19,695,287	**28,128,957**	**49,816,062**
Advisories	**25,252**	35,675	3,300
Web Application Attacks	324,836	**223,720**	**478,123**
Advisories	**28,848**	27,415	603
System Vulnerabilities	22,142,796	**33,883,205**	**22,245,270**
Advisories	**2,799,688**	2,892,290	51,779

An Overview of Cyber Threat Trends over the Last FY

The following is an overview of attempted malware attacks that were detected by the National KE-CIRT during the period July 2021 to March 2022.

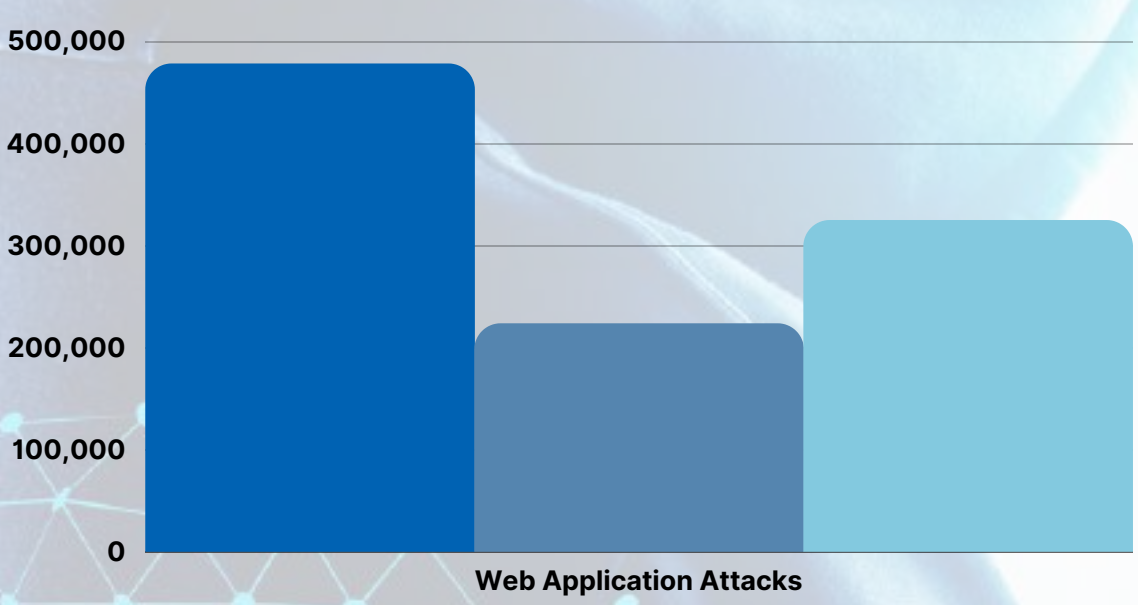


The following is an overview of attempted Distributed Denial of Service(DDoS)/Botnet attacks that were detected by the National KE-CIRT during the period July 2021 to March 2022.



An Overview of Cyber Threat Trends over the Last FY

The following is an overview of attempted Web Application attacks that were detected by the National KE-CIRT during the period July 2021 to March 2022.



The following is an overview of System Vulnerabilities that were detected by the National KE-CIRT during the period July 2021 to March 2022.

Cyber Threat Landscape Insights

01 Gig Economy

The gig economy allows workers flexibility with their schedules and workload, while allowing them to engage in projects of their interest as side hustles, freelancers and contractors. On the other hand, it allows organizations to access top talent in an increasingly competitive and global marketplace.

However, this comes with unique security concerns, such as how to keep proprietary information safe in freelancer's own devices that are not subject to company policies and statutory requirements.

Interestingly, the gig economy has also been behind the success of ransomware attacks, with criminal gangs using this strategy to recruit or contract 'hackers for hire'.

02 Pay-Now-Or-Get-Breached

Cyber criminals continue to evolve and use sophisticated tactics to maximize payout. Unlike standard ransomware attacks, double extortion ransomware gangs infiltrate a target's networks, steal sensitive data and deploy ransomware to encrypt files.

They then threaten to publish the exfiltrated data if the victim fails to pay a ransom within the specified time frame. These threats are some times accompanied by publishing of some of the victim's stolen data as a warning, or to damage their reputation and therefore increase pressure on the victim to pay ransom.

It is important to note that since the victim's data is already in the hands of the ransomware actors, paying the ransom does not guarantee the victim that their data will not be published or sold to other cybercrime actors.

Cyber Safety Tips

Just-In-Time Access

This is a fundamental security practice that involves limiting access to systems or applications on an as-needed basis and for a limited period of time. This allows organizations to minimize the threat of exposure of their systems or data to unauthorized users.

Patch Management

Patches are updates offered by a developer to fix identified flaws in software. Patch management is an essential component in organizational cybersecurity management, and entails applying updates to software as part of preventative maintenance.
Patch management ensures that an organization's software is up-to-date, stable, and secure from vulnerabilities or 'bugs'.

Principle of Least Privilege

This concept is considered best practice in information security, and entails limiting the privileges of users, programs and processes to the bare minimum necessary to carrying out their functions.
This is characterized by limiting the access to the resources necessary to enable users or programs to perform a task. This serves to reduces the risk of unauthorized access to an organization's critical systems and sensitive data.

Questions? Contact us

Website

www.ke-cirt.go.ke

Email

incidents@ke-cirt.go.ke

Hotlines

254-703-172-700
254-730-172700