
# NATIONAL CYBER SECURITY REPORT FOR THE PERIOD JANUARY - MARCH 2020

COMMUNICATIONS AUTHORITY OF KENYA

# MESSAGE FROM THE AG DIRECTOR GENERAL

The Communications Authority of Kenya (CA) is mandated with developing a national framework for cybersecurity management in Kenya. Towards this, the Authority, through the National KE-CIRT/CC, has put in place initiatives covering people, processes and technologies, that are aimed at enhancing the national cybersecurity readiness and resilience to ensure the optimization and sustainability of the gains that Kenya has made in ICT.

Technological advancements in Kenya have resulted in a more open, interconnected nation. On the other hand, cyber threats are continuously evolving at a greater speed than the development of cyber defenses. Indeed, during the period January-March 2020, the National KE-CIRT/CC detected 34.6 million cyber threat events, this being a 6.7% decrease from the 37.1 million cyber threat events detected in the previous period, October - December 2019.

Further, during this period, we observed an increase in the use of phishing emails, fake websites, fake news and email scams.These were linked to the ongoing COVID-19 pandemic, with cyber criminals using a variety of Covid-19 themes lures such as phishing emails, fake news and fake websites to carry out these attacks for purposes of stealing personal information and defrauding unsuspecting Kenyans.

In response to these incidents, the National KE-CIRT/CC issued advisories, best practices guides and created awareness to the public via various platforms in a bid to deter and contain these criminal and fraudulent activities.

Further, the Authority notes the need for the rapid development of a skilled cyber security workforce through training, re-training and up-skilling as a critical component in enhancing Kenya's cyber readiness and resilience. Towards this, the Authority has earmarked cyber security capacity building as a strategic deliverable.

With regards to the ICT consumer, the Authority has enhanced cyber awareness efforts targeting the end user, in cognizance of the fact that a cyber-aware and cyber-vigilant consumer is our best bet in ensuring Kenya's cyber resilience, especially as we move towards becoming a digitally transformed nation. .

## "A Digitally Transformed Nation"

# CYBER THREAT STATISTICS

**33,747,678**

During this period, the National KE-CIRT/CC detected 33,747,678 malware threat events as compared to 34,854,959 in the previous period, October – December 2019.
In response, the National KE-CIRT/CC issued 1,559 cyber threat advisories.

**287,481**

During this period, the National KE-CIRT/CC detected 287,481 botnet attack events, which was a decrease from the previous period October – December 2019, when 346,704 botnet attack events were detected.
In response, the National KE-CIRT/CC issued 111 cyber threat advisories.

**582,281**

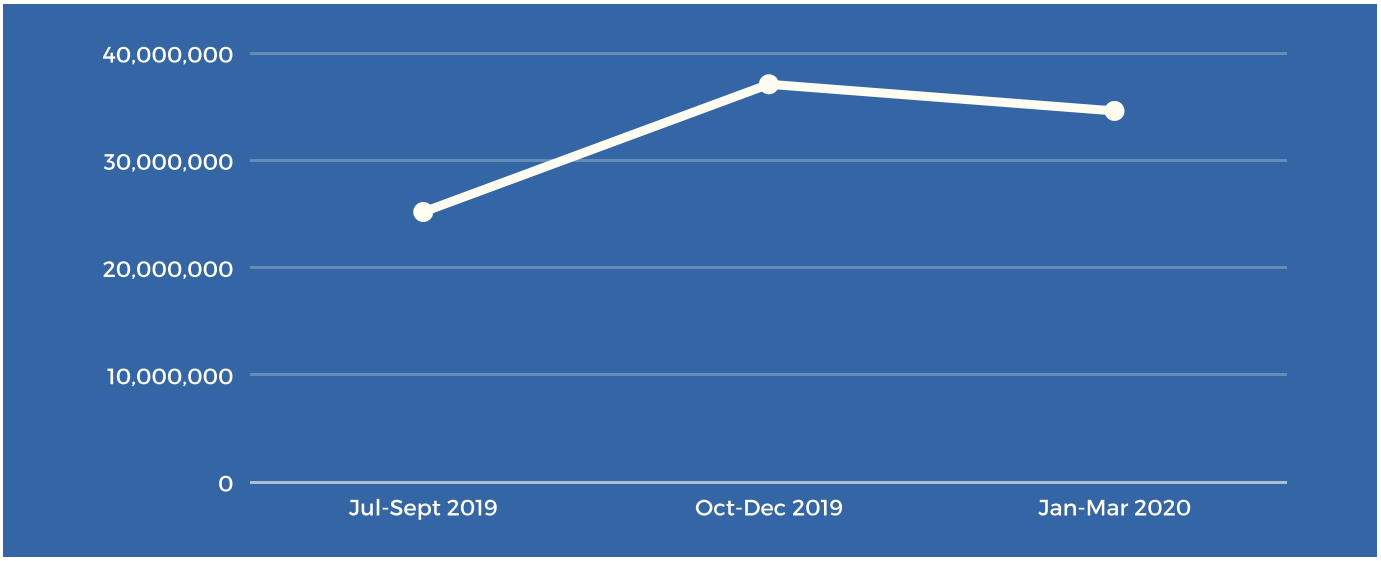
During this period, the National KE-CIRT/CC detected 582,281 web application attacks, which was a decrease from the 1,908,001 detected in the previous period, October – December 2019.
In response, the National KE-CIRT/CC issued 147 cyber threat advisories.

**27,091**

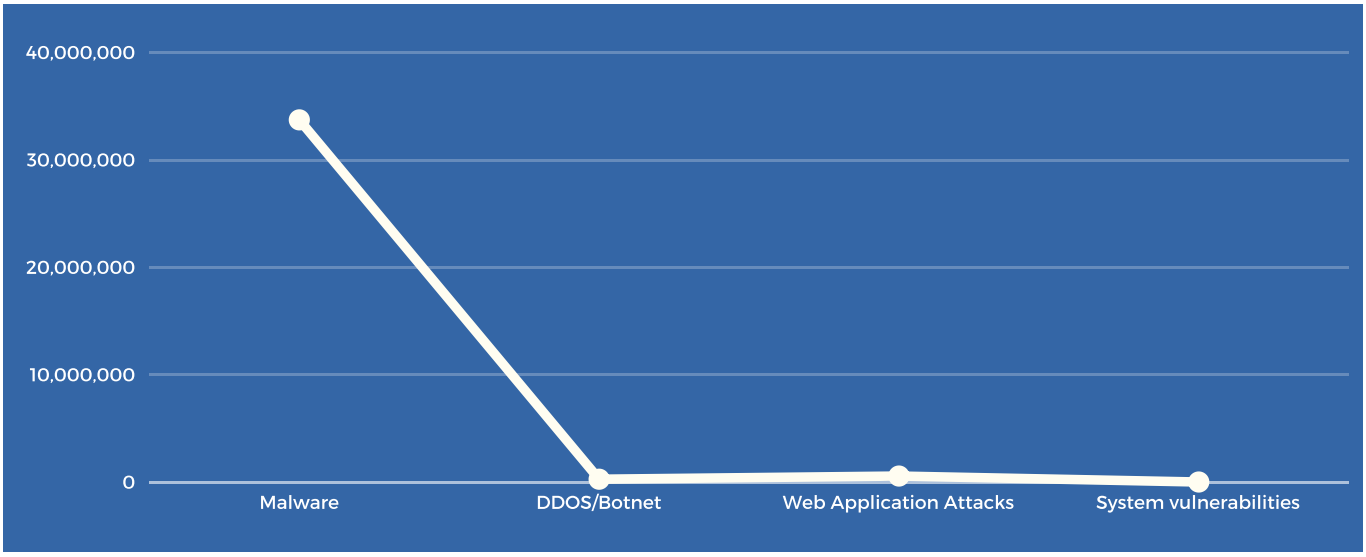
During this period, the National KE-CIRT/CC detected 27,091 system vulnerabilities, which was an increase from the 23,536 detected in the previous period October – December 2019.
In response, the National KE-CIRT/CC issued 15,517 cyber threat advisories.

# CYBER THREAT LANDSCAPE

During the period January – March 2020, the National KE-CIRT/CC detected 34.6 million cyber threats events, which was a 6.7% decrease from the 37.1 million threat events detected in the previous period, October - December 2019. This decline was due to a decline in Malware, DDOS/Botnet and Web Application attacks during the period.




Of the 34,644,531 cyber threat events detected, 33,747,678 were Malware threat events; 287,481 were Botnet/DDOS threat events; 582,281 were Web Application Attack threat events; and 27,091 were System Vulnerabilities threat events.



# CYBER THREAT ADVISORIES ISSUED

## 17,844

In response to the 34,644,531 cyber threat events detected, the National KE-CIRT/CC issued 17,844 advisories during the period January - March 2020.

The number of advisories issued during this period was a 7.1% increase as compared to the 16,654 advisories that had been issued during the previous period October to December 2019.

# SYSTEM VULNERABILITIES

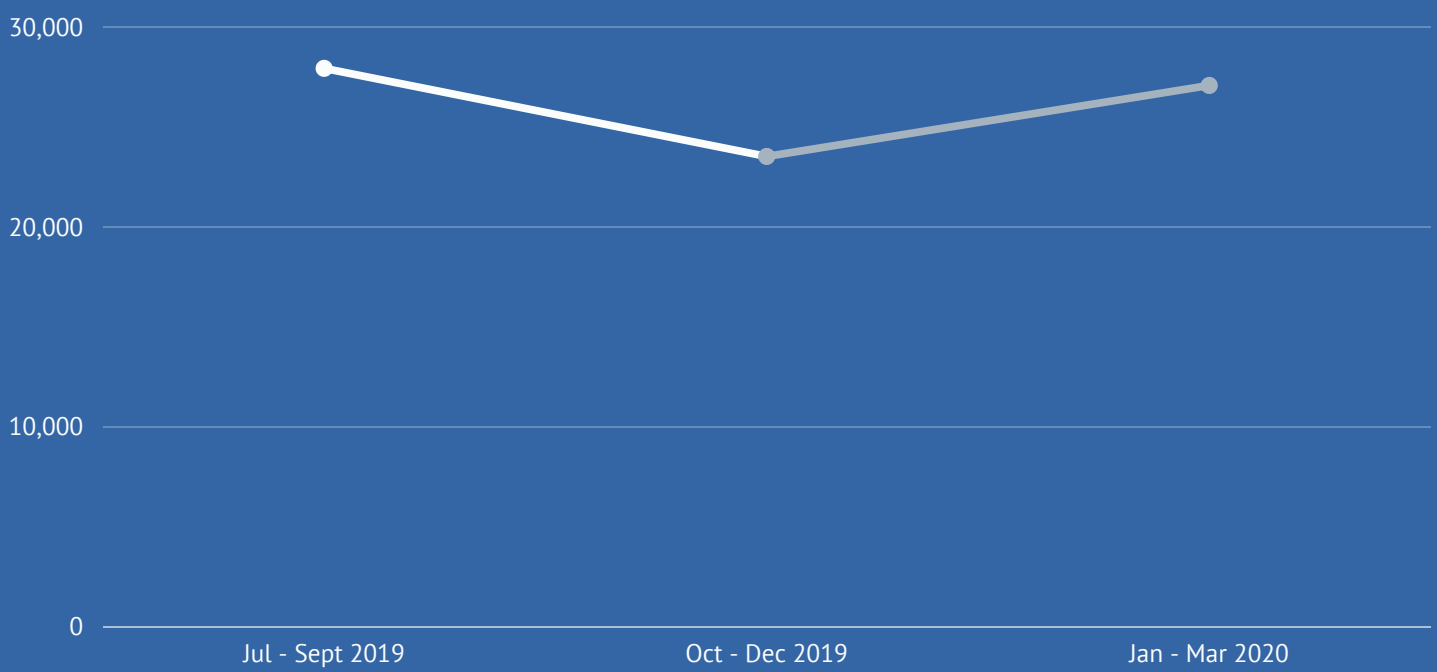
System vulnerabilities are flaws in a computer system that cyber criminals exploit to carry out an attack. During the period January – March 2020, the National KE-CIRT/CC detected 27,091 system vulnerabilities, which was a 15.1% increase from the 23,536 detected in the previous period October – December 2019.
In response to these detected events, the National KE-CIRT/CC issued 15,517 system vulnerabilities advisories to the affected organizations, which was a 12.3% increase from the 13,815 issued in the previous period, October – December 2019.

Notable system weaknesses observed by the National KE-CIRT/CC during the period included: the 'BlueKeep' flaw that plagued more than 55% of medical imaging devices such as MRIs, X-rays, and ultrasound machines that affect Remote Desktop Services (RDP) services running on outdated Windows versions; the 'Cable Haunt flaw' that affected cable modems and which allowed attackers to compromise a modem and gain full control over the inbound and outbound traffic and that allowed attackers to eavesdrop on browsing activity, re-route traffic to malicious domains, or even zombify devices to use them in botnet attacks; the 'CryptoAPI' spoofing flaw that allowed attackers to spoof digital certificates to perform Man-in-the-Middle (MITM) attacks, amongst other system weaknesses.

**15.1%**

Increase in detected system vulnerabilities events as compared to the previous period

An analysis of System Vulnerabilities threat events detected during the period July 2019 to March 2020



# MALWARE

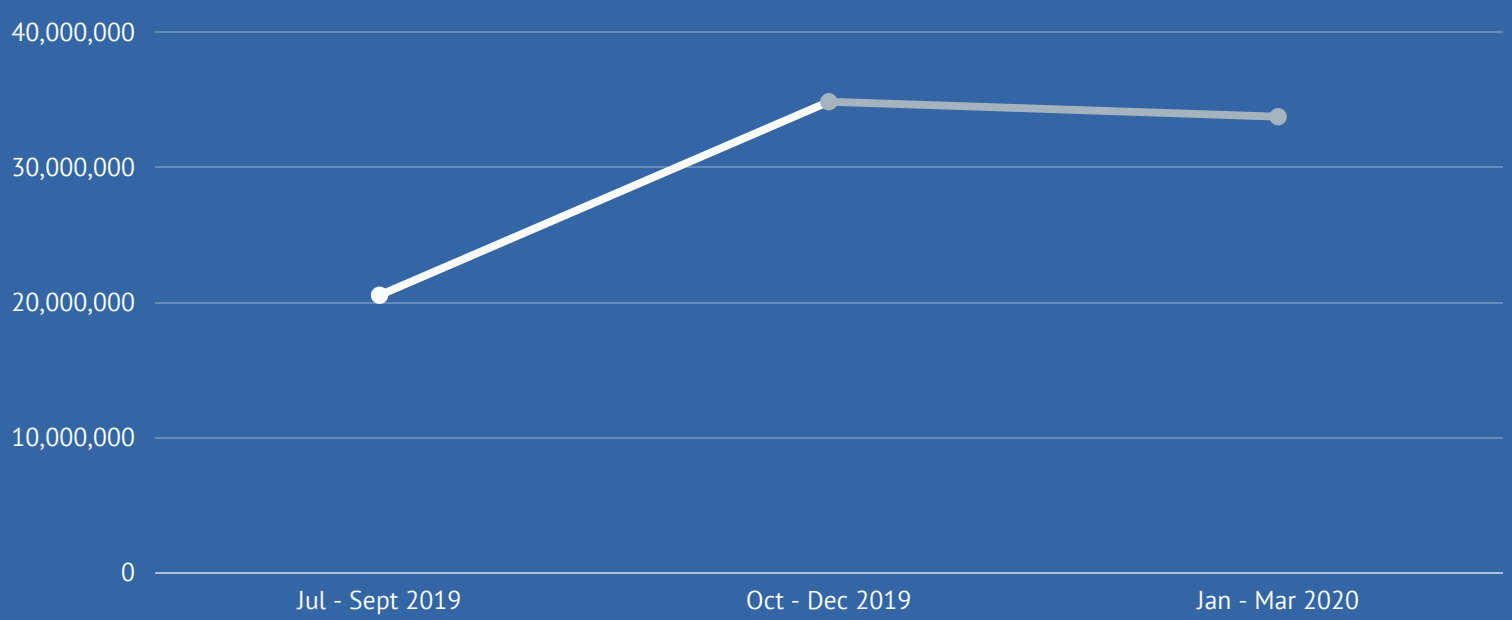
During the period January – March 2020, the National KE-CIRT/CC detected 33,747,678 malware threat events. This was a 3.2% decrease from the previous period where 34,854,959 malware threat events had been detected.
In response to these detected cyber threat events, the National KE-CIRT/CC issued 1,559 cyber threat advisories. The number of advisories issued during the period January-March 2020 slightly decreased by 2.6% as compared to those issued in the previous period October – December 2019.

During the reporting period, the most notable malware incidents included: the new version of the 'Cerberus' android banking trojan which accessed 2FA-protected accounts by stealing one-time codes generated by the Google Authenticator app; the 'AZORult' trojan that made a comeback in a campaign where it disguises itself as fake ProtonVPN installers which once installed, collected the infected machine environment data and sent it back to an attacker's C2 server; the new malware 'Dustman', which is designed to wipe data on infected computers; and, the remote access trojan (RAT) named 'Parallax' which was widely distributed through malicious spam campaigns and when installed, allowed attackers to gain full control over an infected system.

**3.2%**

Decrease in detected malware events as compared to the previous period

An analysis of Malware threat events detected during the period July 2019 to March 2020



# PHISHING

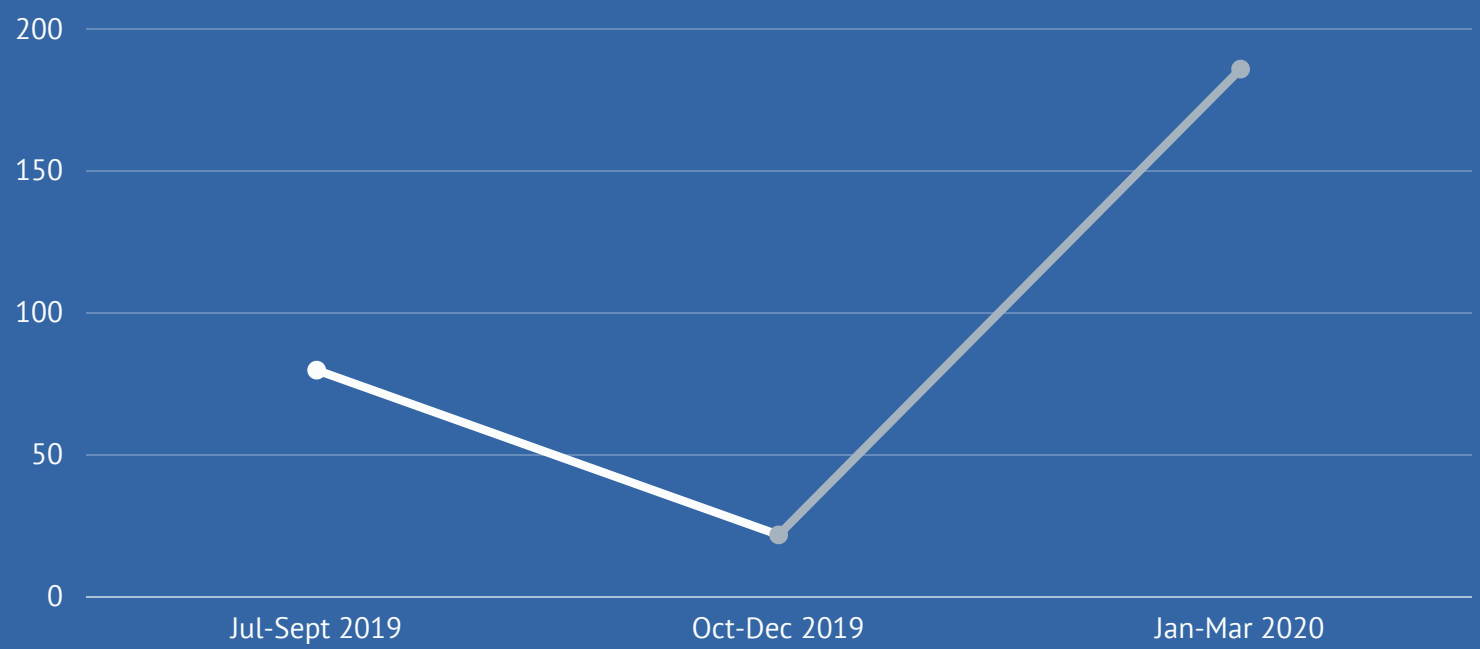
The most notable phishing trend observed by the National KE-CIRT/CC during the reporting period was the Ksh. 10 billion Evil Corp phishing campaign, carried out by the TA505 threat actor group, that delivered malicious payloads through Excel documents. The phishing campaign, which was detected by the Microsoft Corporation, uses HTML redirectors attached to emails that when opened, lead to the download of 'Dudear', a malicious macro-laden Excel file that drops the payload.

During the period January – March 2020, the National KE-CIRT/CC issued 186 phishing advisories. This was a 745.5% increase in advisories issued as compared to 22 issued in the previous period October – December 2019.
There was a marked increase in the use of phishing as a cyber attack method during the reporting period, which was attributed to the shifting working patterns as more people work remotely in an effort to flatten the curve in regard to the Covid-19 pandemic.

**186**

Number of phishing advisories issued by the National KE-CIRT/CC during the reporting period

An analysis of Phishing threat events detected during the period July 2019 to March 2020



# WEB APPLICATION ATTACKS

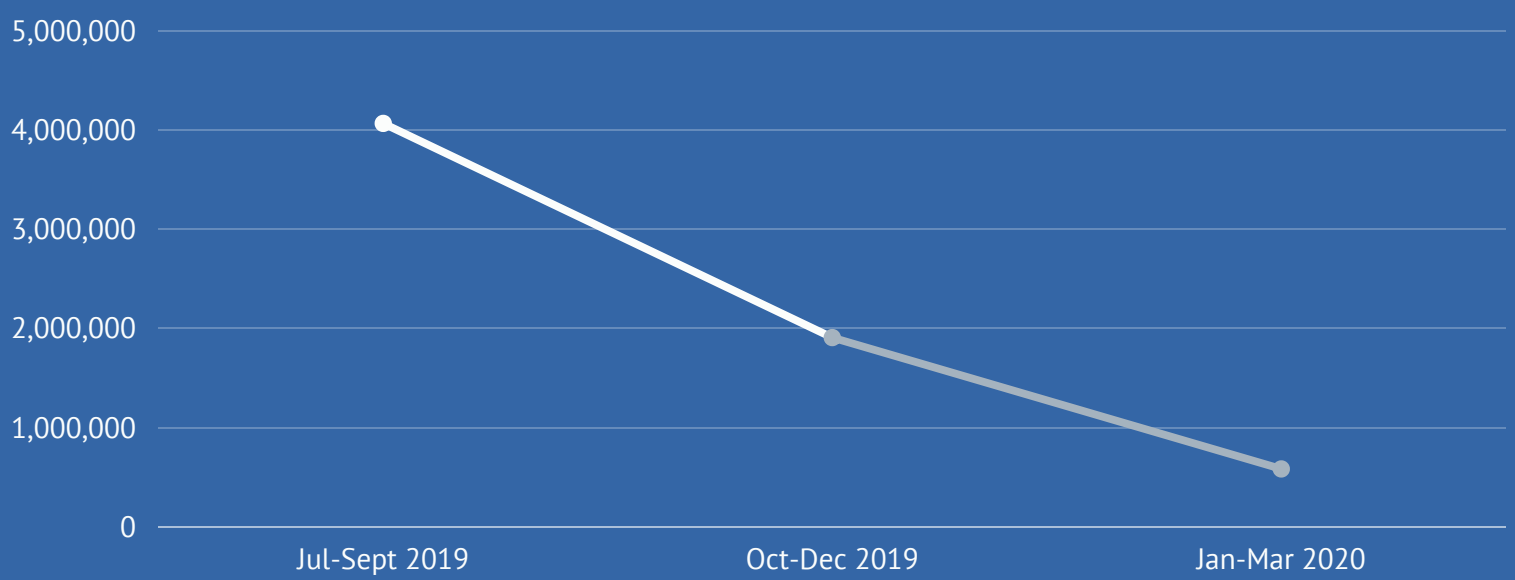
During the period January - March 2020, the National KE-CIRT/CC detected 582,281 web application attack events, which was a 69.5% decrease from the 1,908,001 detected in the previous period October – December 2019.
In response, the National KE-CIRT/CC issued 147 advisories to the affected organizations, which was an increase compared to the 45 advisories issued in the previous period October – December 2019.
Notable web application attacks observed globally during the period include the exposure of more than 200 million records related to USA residents which were on an unsecured database hosted on Google Cloud.

The exposed data included the names, addresses, email addresses, age, gender, ethnicity, employment, credit rating, and property information of victims. An unprotected 'Elasticsearch' database also exposed over 5 billion records including domains, sources, contact email addresses, and passwords. Also notable was the attack on the online platform 'Rallyhood', which exposed nearly 4.1 Terabytes of files via an unprotected Amazon Web Services (AWS) S3 bucket, which had the effect of giving anyone access to a decade's worth of user files such as passwords lists, contracts, and other permission slips and agreements. These scenarios illustrate the impact that web application attacks have on corporations and individuals, and calls for enhanced capacity building of cyber security professionals to adequately bridge these cyber security gaps.

**69.5%**

Decrease in detected Web Application Attack events as compared to the previous period

An analysis of Web Application Attack threat events detected during the period July 2019 to March 2020



# BOTNET/ DDOS

Botnets are networks of devices such as computers, smartphones or IoT devices which perform a number of repetitive tasks to maintain heavy web traffic. These can be hijacked by cyber attackers to carry out distributed denial of service (DDoS) attacks as well as spamming and phishing attacks.

During the period January – March 2020, the National KE-CIRT/CC detected 287,481 botnet attack events, which was a 17.1% decrease from those detected in the previous period, October – December 2019.

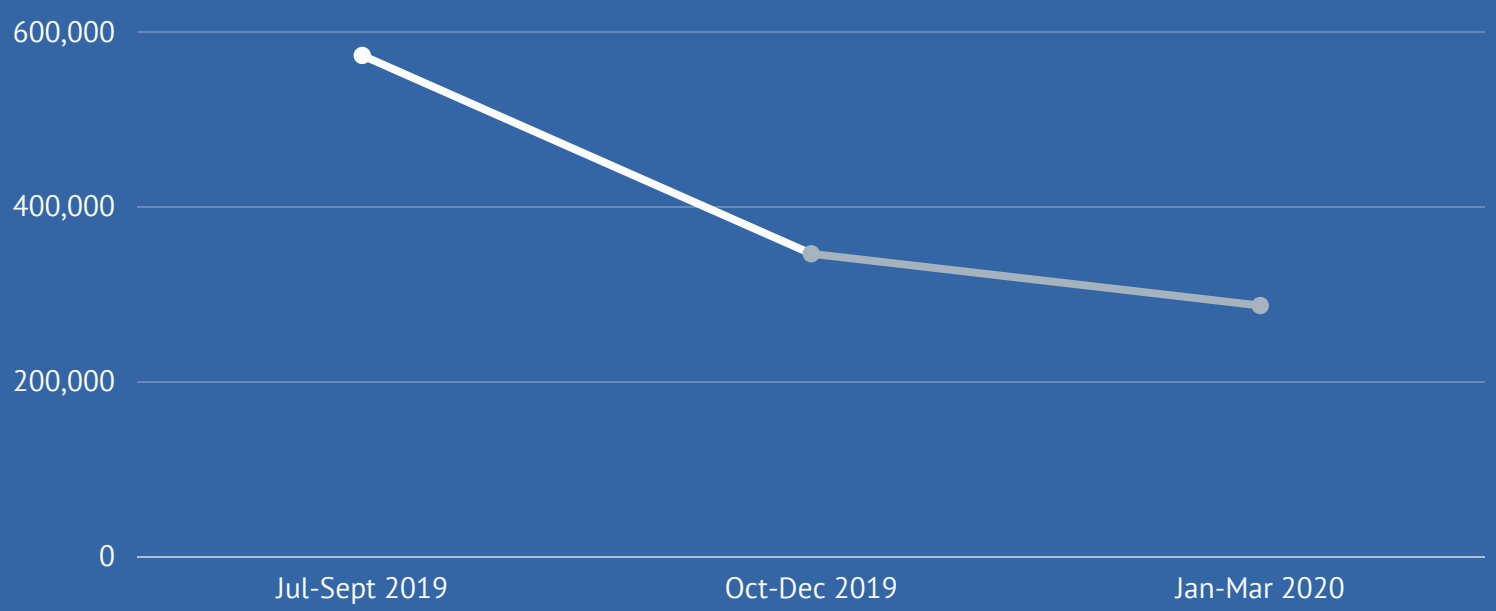
In response, the National KE-CIRT/CC issued 111 advisories, which was a 88.2% decrease from those issued in the previous period.

Notable Botnet/DDOS activity observed by the National KE-CIRT/CC during the reporting period included: the use of a version of the 'njRAT' Trojan by a group of Vietnam hackers to infect the hacking tools of fellow hackers, who thereafter used the hijacked machines to carry out Distributed Denial of Service (DDoS) attacks and steal sensitive data; the new 'Mirai' malware variant dubbed 'Mukashi', which targeted the uncovered critical vulnerability in the Zyxel network-attached storage products, exploiting them to rope the machines into an Internet of Things (IoT) botnet which could then be used to launch Distributed Denial of Service (DDoS) attacks.

**17.1**

Decrease in detected BOTNET/DDOS threat events as compared to the previous period

An analysis of Botnet/DDOS threat events detected during the period July 2019 to March 2020



# DIGITAL FORENSICS AND INVESTIGATIONS

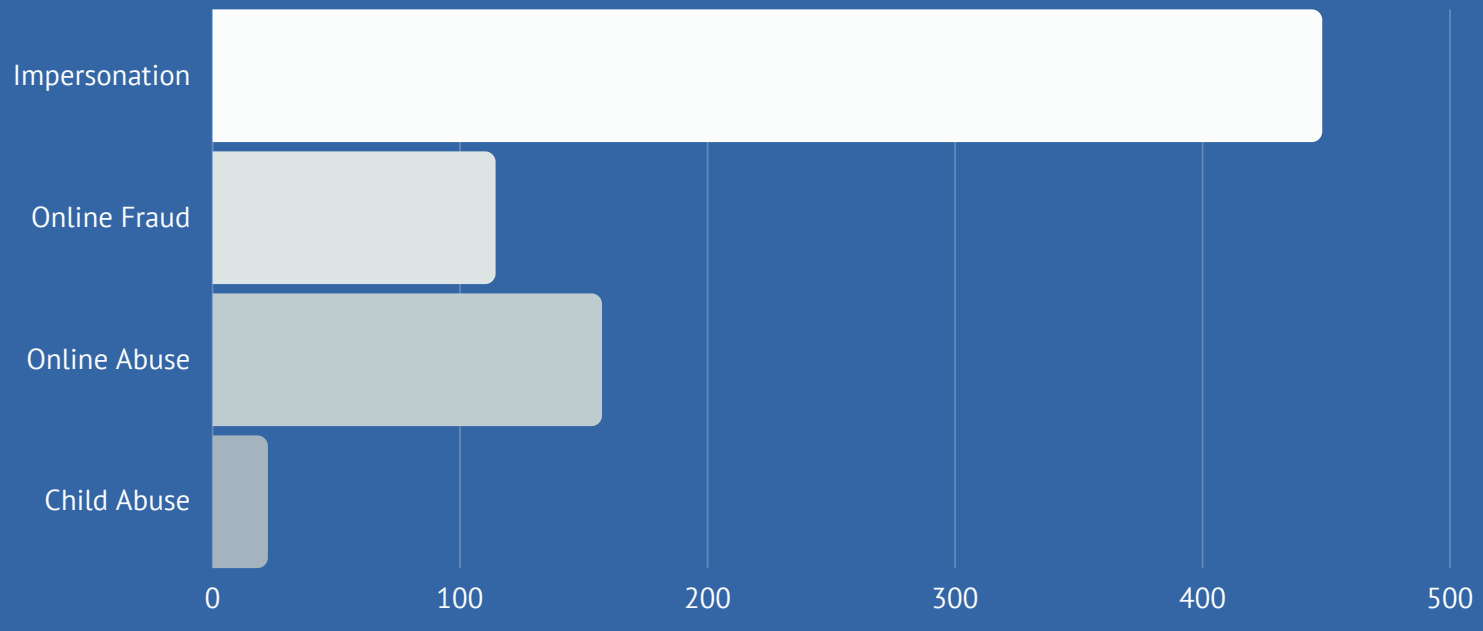
During the period January – March 2020, the National KE-CIRT/CC received 283 requests for digital forensics facilitation from investigative agencies, which was a 45.1% increase from the previous period October – December 2019. During this period, there was an increase in cases reported to the National KE-CIRT/CC regarding online impersonation, online fraud and child abuse cases as compared to the previous quarter. However, there was a 67.1% decrease in online abuse cases as compared to the previous period, October – December 2019.

As a multiagency collaboration framework for the management of cybersecurity in Kenya, the National KE-CIRT/CC works closely with law enforcement agencies by facilitating digital forensics and investigations through its Digital Forensics Lab (DFL).
Digital forensics is the process of identifying, extracting, preserving, analyzing, and presenting digital evidence in a manner that is legally admissible in a court of law. Accredited digital forensics examiners at the National KE-CIRT/CC Digital Forensics Lab are involved in the examination of digital evidence to support the investigation and prosecution of cyber crime cases in Kenya.

**283**

Digital forensics and investigations cases facilitated by the DFL at the National KE-CIRT/CC during the period Jan-Mar 2020

An analysis per category, of the number of digital forensics and investigations cases facilitated by the DFL at the National KE-CIRT/CC during the period July 2019 to March 2020




# CYBER SECURITY AMIDST COVID-19

As Kenya's national trusted point of contact on cybersecurity matters, the National KE-CIRT/CC continues to work 24/7 in close collaboration with local and international partners to detect, monitor and respond to various cyber threats affecting Kenya.
As we continue to work remotely in an effort to flatten the curve with regard to the Covid-19 pandemic, we urge individuals and corporations to remain cyber vigilant and observe cyber hygiene practices so as to safeguard your devices, systems and processes.

Further, we urge individuals and organizations to report cyber incidents to the National KE-CIRT/CC via the email **incidents@ke-cirt.go.ke** or via the hotlines **+254 703 042700** and **+254 730 172700.**

**MERCY WANJAU, MRS**
AG DIRECTOR GENERAL

COMMUNICATIONS AUTHORITY OF KENYA

WWW.KE-CIRT.GO.KE