
# NATIONAL CYBERSECURITY REPORT

APRIL - JUNE 2020

COMMUNICATIONS AUTHORITY OF KENYA


# MESSAGE FROM THE AG DIRECTOR GENERAL

The COVID-19 pandemic continues to create new cybersecurity and data privacy challenges for organizations nationally and globally. With Working from Home (WFH) and e-commerce becoming the new norm, organizations globally are struggling with cybersecurity resilience for remote workforces as well as meeting operational goals within these new digital parameters. To address these challenges, the Authority continued to create awareness on cyber security resilience and continuity for organizations.

During the period April to June 2020, we observed that cyber threat actors continued to exploit the work and life shifts brought about by the pandemic to perpetrate cyber crime. These included attacks against teleconferencing and Virtual Private Network (VPN) applications, COVID-19 themed phishing campaigns, online impersonation, fake news, online fraud, Business E-mail Compromise (BEC) scams and registration of malicious COVID-19 themed domains.

We also observed an increase in cyber attacks targeting the education sector, as more institutions adopted online learning as an alternative channel to deliver learning amidst the pandemic. This increased the risk of learners being exposed to inappropriate content, as well as the exploitation of minors by malicious actors online.

To address these and other threats arising during the period, the Authority sensitized organizations and the public on these emerging vulnerabilities through cyber security advisories and awareness on cyber hygiene. Further, through the National KE-CIRT/CC 24/7 cyber incidents hot lines, the Authority was able to respond to cyber incidents in a timely manner.

In addition, under the National KE-CIRT/CC multiagency framework, the Authority collaborates with local and international stakeholders in the management of cybersecurity in Kenya. This includes liaising with law enforcement agencies in the analysis of digital forensics through the Digital Forensics Lab (DFL) towards the prosecution of cyber crime in Kenya.

Furthermore, in order to ensure that front line cyber security workers were better prepared to address these emerging cybersecurity challenges, the Authority sponsored a Certified Information System Manager (CISM) course for information security officers working with critical infrastructure service providers with the objective of enhancing Kenya's national cyber readiness and resilience.

## "Cybersecurity as an Enabler for a Digitally Transformed Nation"

# CYBER THREAT STATISTICS

**12,508,275**

During the period April to June 2010, the National KE-CIRT/CC detected 12,508,275 malware threat events compare to the 33,747,678 detected in the previous period January to March 2020.

**267,931**

During the period April to June 2020, 267,931 DDOS attack events were detected compared to the 287,481 detected in the previous period January to March 2020.

**1,102,840**

The National KE-CIRT/CC detected 1,102,840 web application attack events during the period compared to 582,281 in the previous period January to March 2020.

**30,023**

During the period April to June 2020, the National KE-CIRT/CC detected 30,023 system vulnerabilities compared to 27,091 in the previous period January to March 2020.

**13,909,069**

Total number of cyber threat events detected by the National KE-CIRT/CC during the period April to June 2020.

**20,839**

Total number of cyber threat advisories issued to affected organizations in response to cyber threat events detected by the National KE-CIRT/CC during the period April to June 2020.

# OVERVIEW OF THE CYBER THREAT LANDSCAPE

During the period April – June 2020, cyber threat actors continued to use the pandemic to perpetrate cyber crime using COVID-19 themed lures in phishing campaigns and malware attacks, fake news and impersonation. These included luring victims into downloading malware disguised as legitimate COVID-19 related applications, data breaches through the exploitation of unsecure databases, data leaking sprees by ransomware gangs involved in extortion operations, and the spread of misinformation through Fake News related to the pandemic. The increase in the use of technology in response to the pandemic also resulted in an increase in cyber attacks targeting end users at home, as opposed to attacks on corporate networks. These included attacks targeting mobile device security, Virtual Private Networks (VPNs), teleconferencing applications and theft of private data through installation of malicious software on targeted devices.

As more businesses shifted their operations to online platforms in response to social distancing measures as a result of the pandemic, cyber threat actors upscaled Megacart card skimming attacks targeting online retail stores. The attackers would hide malicious code in these sites to record customers' payment details during online shopping. These attacks, which are designed to steal users' information such as credit card details among others, targeted online retail stores, local government services payment platforms, and even academic institutions.

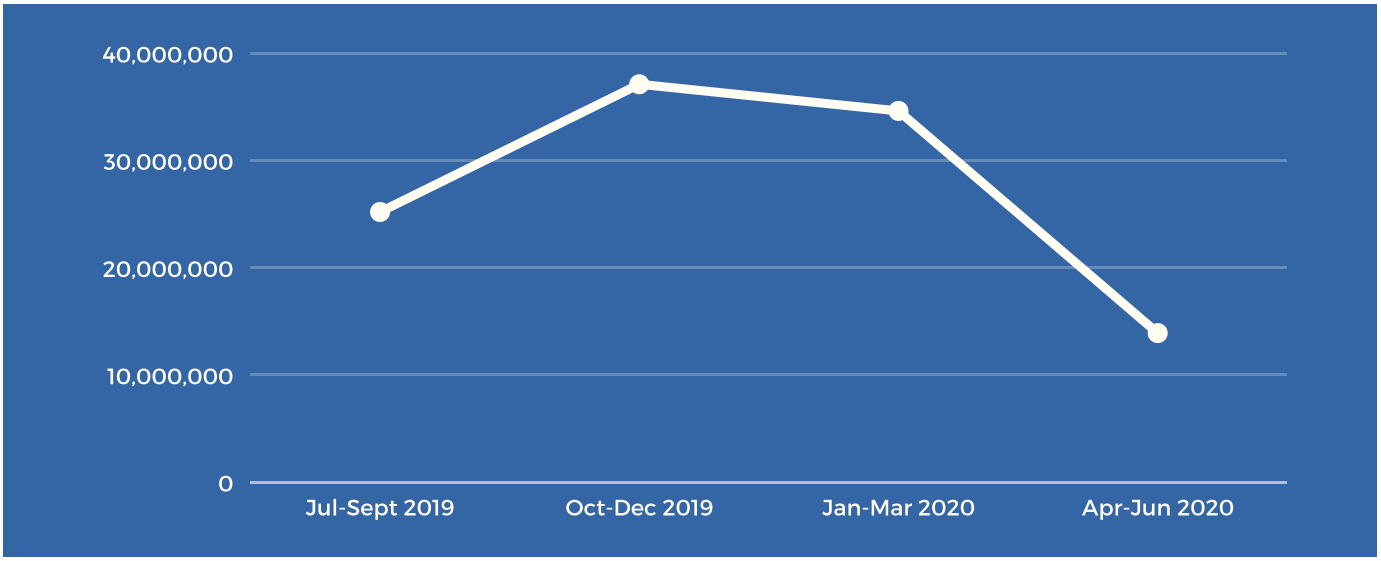
Also notable during this period was the evolution of ransomware, which was characterized by ransomware actors adopting new methods of generating illicit revenue such as partnership with other ransomware gangs, targeted attacks on large organizations, name-and-shame tactics, and the roll out of ransomware-as-a-service model. This evolution and escalation of ransomware included the launch of an auction site set up by ransomware gangs for purposes of selling stolen data.

Malware events accounted for 90% of the total cyber threat events detected locally by the National KE-CIRT/CC during the period April to June 2020. The three top malware infiltrating enterprises and individuals during this period were Trojans, Backdoors and Droppers. Also notable during this period was the evolution of malware into the mobile landscape. This was characterized by an increase in malware types migrating into the mobile arena. This is attributed to the exploitation of vulnerabilities in mobile operating systems, as well as the increasing use of mobile applications to propagate malware.

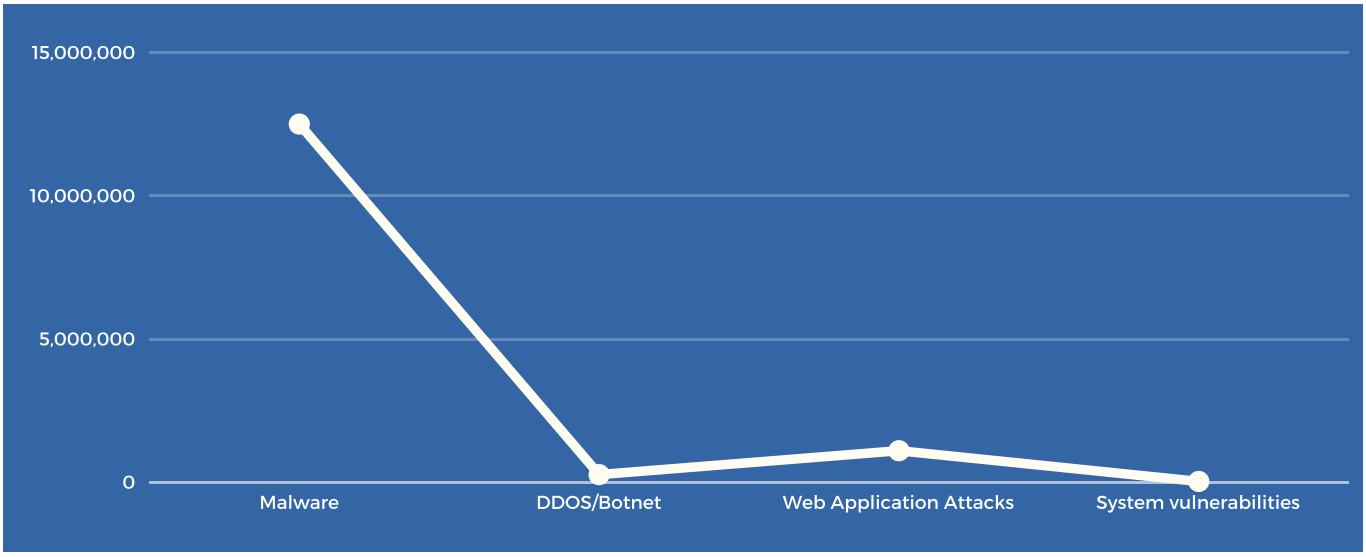
Cyber attacks targeting mobile devices were carried out through banking Trojans and fake banking apps that were used to harvest banking credentials of mobile banking customers; phishing attacks on email, Internet messaging platforms and SMS; and, via malicious software such as spyware. The increased targeting of mobile devices targets to harvest and steal users' Personally Identifiable Information (PII). Attacks targeting mobile devices such as smartphones and tablets are noteworthy because these devices are trusted devices that sit at the intersection of the owner's personal and professional identity, and can thereby be a gateway for compromising corporate networks.

# CYBER THREAT LANDSCAPE

During the period April – June 2020, the National KE-CIRT/CC detected 12.9 million cyber threats events, this being a 59.9% decrease from the 34.6-million cyber threat events detected in the previous period, January – March 2020. This decrease was attributed to timely incident response mechanisms and increased endpoint security measures adopted to protect end user devices.




Of the 13,909,069 cyber threat events detected, 12,508,275 were Malware threat events; 267,931 were Botnet/DDOS threat events; 1,102,840 were Web Application Attack threat events; and 30,023 were System Vulnerabilities threat events.



# CYBER THREAT ADVISORIES

# 20,839

In response to the 13,909,069 cyber threat events detected in the period April-June 2020, the National KE-CIRT/CC issued 20,839 advisories compared to the 17,844 advisories issued during the previous period January - March 2020.

# SYSTEM VULNERABILITIES

System vulnerabilities are flaws in a computer system that cyber attackers exploit to carry out cyber attacks. During the period April – June 2020, the National KE-CIRT/CC detected 30,023 system vulnerabilities, which was a 10.8% increase from the 27,091 detected in the previous period, January – March 2020.

This increase was attributed to increased exploitation of systems that support remote working such as cloud resources and Virtual Private Networks (VPNs) as a result of organizations making their systems publicly accessible to remote workers via their home networks.

In response to these detected events, the National KE-CIRT/CC issued 17,364 system vulnerabilities advisories to the affected organizations, which is a 11.9% increase from the 15,517 issued in the previous period, January – March 2020.

Working from home arrangements in response to the Covid-19 pandemic have resulted in the increased use of applications such as video conferencing, cloud computing, and the use of Virtual Private Networks (VPNs) to secure home networks.

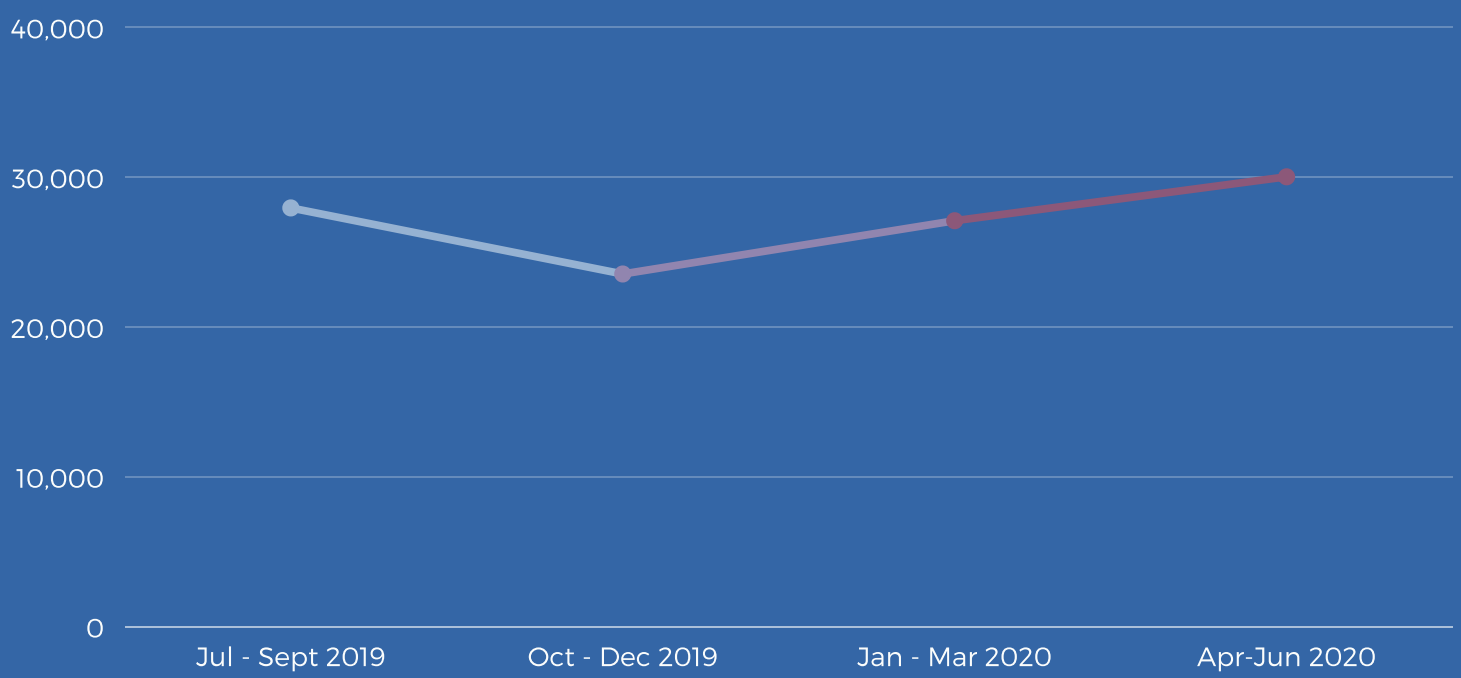
Cyber threat actors are in turn exploiting these vulnerabilities to steal users credentials and distribute malware.

The leading vulnerability exploit type that impacted organizations in Kenya was Remote Code Execution (RCE) followed by Information Disclosure, Authentication Bypass and Denial of Service (DoS).

**30,023**

Detected system vulnerabilities events during the period

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



# MALWARE

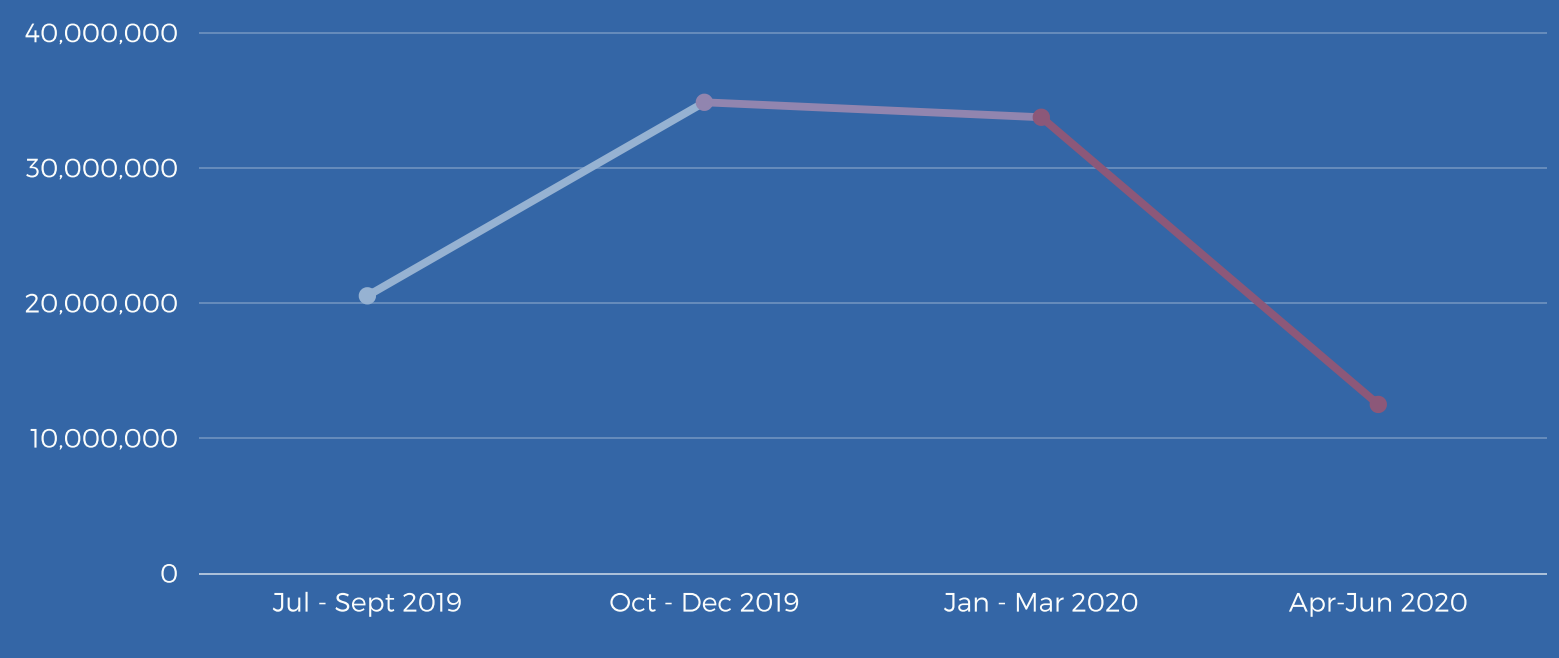
During the period April – June 2020, the National KE-CIRT/CC detected 12,508,275 malware threat events. This was a 62.9% decrease from the previous period where 33,747,678 malware threat events had been detected.
In response to these detected cyber threat events, the National KE-CIRT/CC issued 2,398 cyber threat advisories, which was a 53.8% decrease compared to those issued in the previous period January – March 2020.

The top malware in Kenya during this period included: Lotoor, a mobile hacking tool that targeted android operating systems in order to gain root privileges on compromised mobile devices; XMRig, an open sourced Monero CPU Cryptominer that targeted Windows and Linux servers and which would hijack the full power of the servers CPUs; the Glupteba botnet, a router exploiter that targeted MikroTik routers vulnerability to relay malicious traffic and initiate widespread spam attacks; and Vidar Infostealer that was delivered to Windows OS devices via phishing, and which is also capable of exfiltrating a variety of data such as system information, browser data, and user credentials.

**12,508,275**

Malware threat events detected by the National KE-CIRT/CC during the period April-June 2020

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



# PHISHING

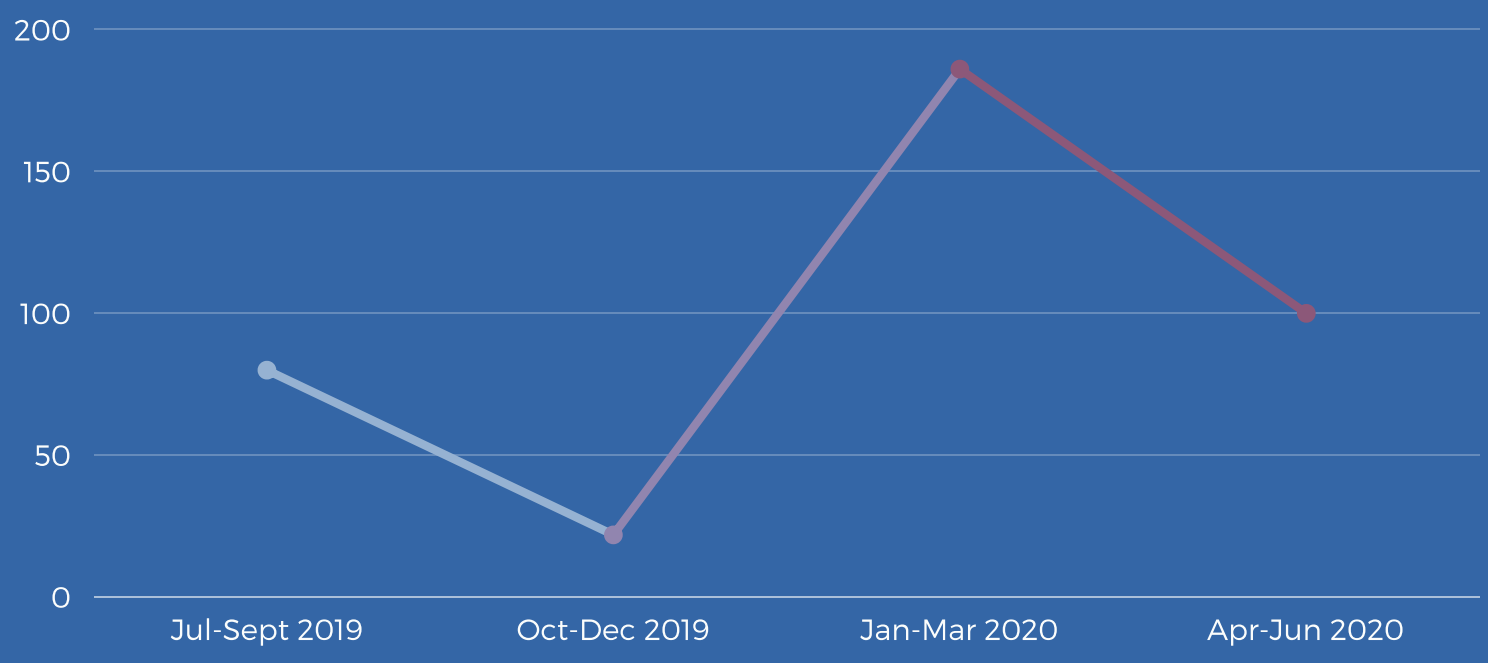
Cyber threat actors continued to use COVID-19 themed phishing lures to trick unsuspecting users into opening emails containing malicious attachments that install malicious software onto the victim's devices, or clicking on malicious links that would redirect the victim to a spoofed domain that would harvest the victim's Personally Identifiable Information (PII).
In the period April – June 2020, the top malicious file type for E-mail in Kenya was xlsx, which is an excel document that contains malicious code called macro, that when enabled installs malware into a device.

During the period April – June 2020, the National KE-CIRT/CC issued 100 phishing advisories, which was a 46.2% decrease compared to the 186 issued in the previous period January – March 2020.
This decrease was attributed to the take down of malicious domains by domain registrars with the objective of curbing the spread of phishing attacks.

**100**

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 June 2020



# WEB APPLICATION ATTACKS

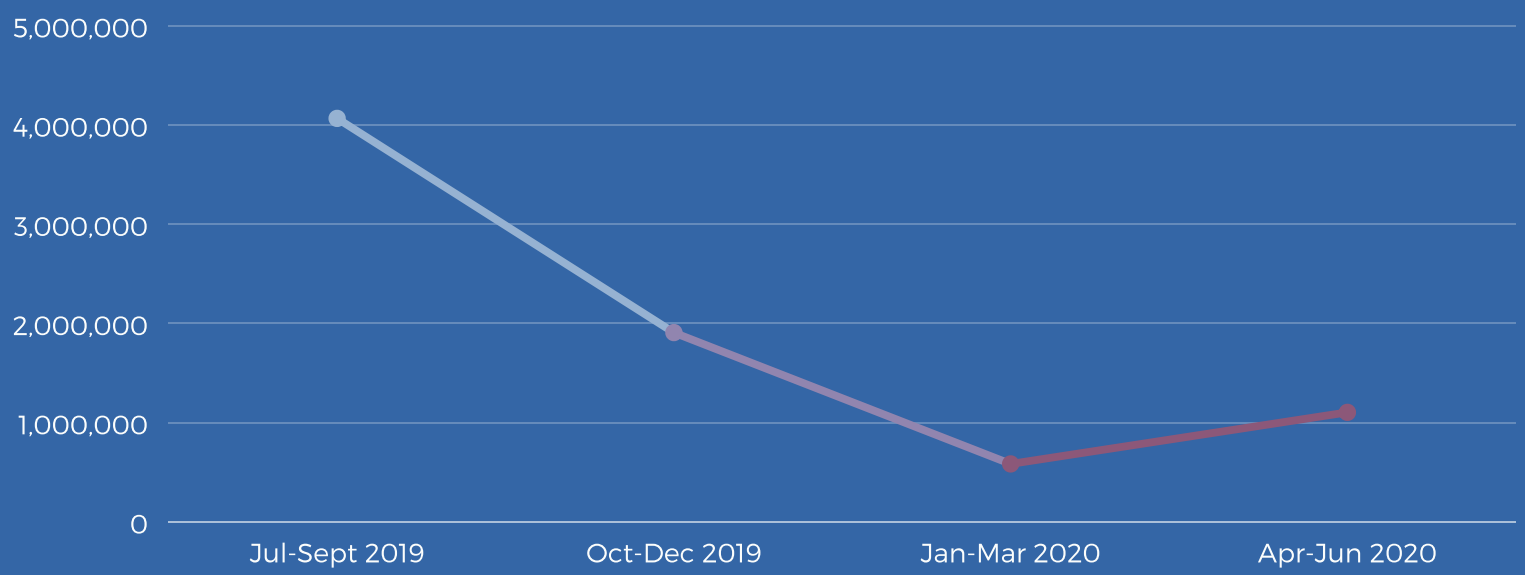
During the period April – June 2020, the National KE-CIRT/CC detected 1,102,840 web application attack events, which was a 84.9% increase from the 582,281 detected in the previous period, January – March 2020.
This increase was attributed to attacks targeted at e-commerce websites as more businesses leveraged on online services in response to the pandemic, as well as the newly registered COVID-19 driven domains that were hosted on unsecured public cloud platforms such as Amazon Web Services (AWS) and Google Cloud Platform.

In response to these threat events, the National KE-CIRT/CC issued 204 advisories to the affected organizations, which is a 38.8% increase from the 147 advisories issued in the previous period January – March 2020.
Notable web application attack incidents during the period included the vulnerable plugin for e-commerce platforms, unsecured databases belonging to remote learning platforms, and a misconfigured Amazon Web Services (AWS) S3 bucket that leaked 845GB of data including explicit photos, private chats and recordings belonging to various dating applications.

**1,102,840**

Web Application Attack events detected by the National KE-CIRT/CC during the period

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



# BOTNET/ DDOS

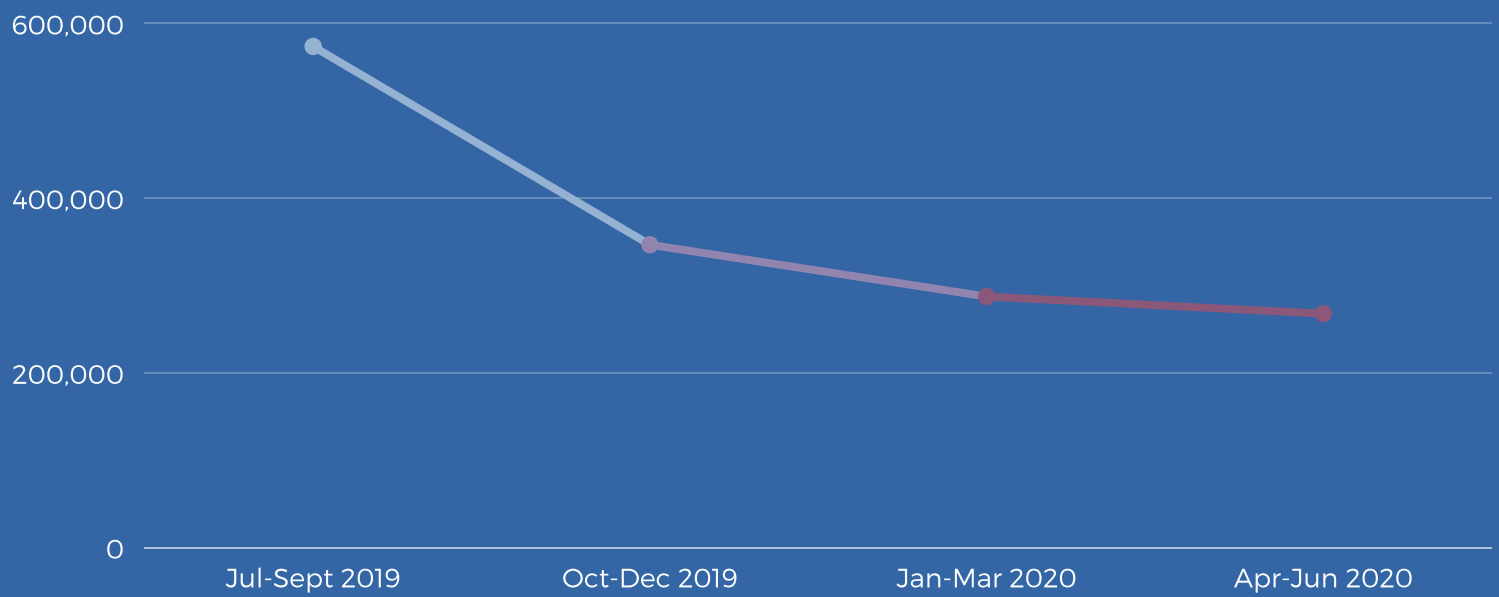
During the period April – June 2020, the National KE-CIRT/CC detected 267,931 Botnet attack events, which was a 6.8% decrease from those detected in the previous period January – March 2020. This decrease is attributed to the adoption of DDoS protection services in response to the rising demand for uninterrupted online services.
In response, the National KE-CIRT/CC issued 457 advisories during the period, compared to 111 advisories issued in the previous period.

Notable Botnet/DDOS events observed during this period included: the successfully exploit of vulnerable Netlink home fiber routers in a bid to spread its IoT controlling network infrastructure through MooBot botnet; and the Hoaxcall botnet that exploited unpatched vulnerabilities of a network management appliance known as Zyxel Cloud CNM SecuManager, in a bid to widen its spread to a list of targeted devices and expand its IoT controlling network infrastructure.

**267,931**

BOTNET/DDOS threat events detected by the National KE-CIRT/CC during the period

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



# DIGITAL FORENSICS AND INVESTIGATIONS

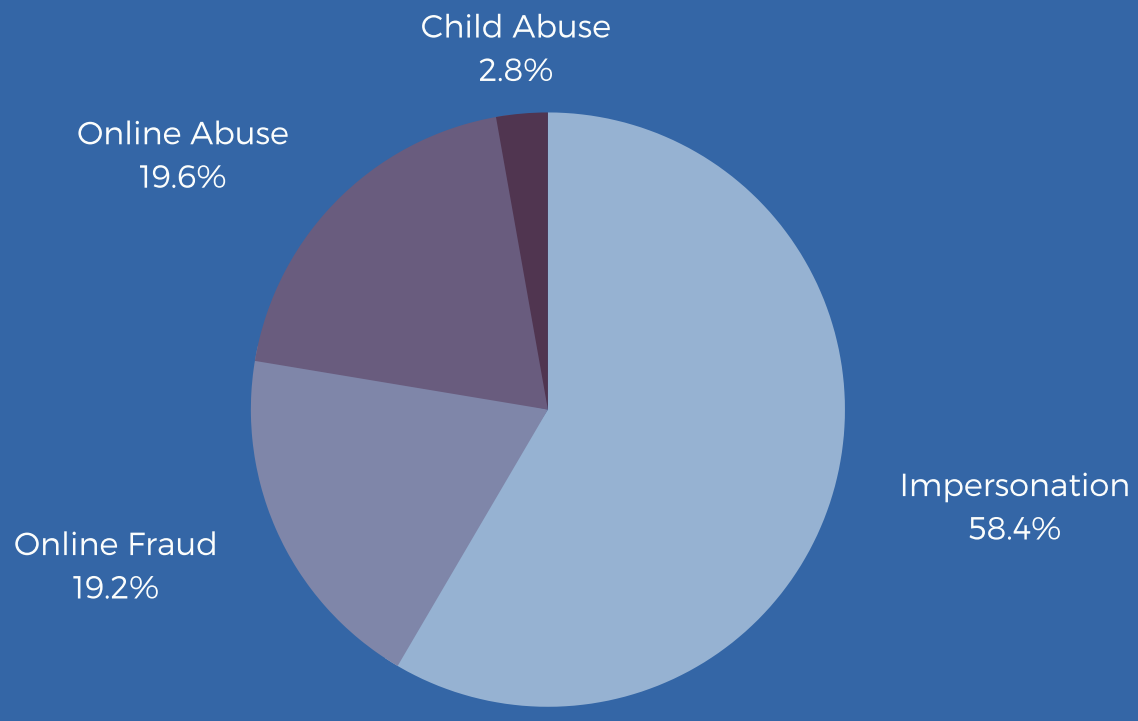
The National KE-CIRT/CC is a multiagency collaboration framework for the management of cybersecurity in Kenya. In executing this role, the National KE-CIRT/CC works closely with law enforcement agencies, by facilitating digital forensics and investigations through the Digital Forensics Lab (DFL).
Digital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

During the period April – June 2020, the National KE-CIRT/CC received 260 requests for facilitation from law enforcement agencies, which was an 8.1% decrease from the previous period January – March 2020.
There was an increase in online abuse and online fraud cases during this period, while there was a decrease in impersonation and child abuse cases as compared to the previous period, January – March 2020.
The increase in online abuse and online fraud cases is attributed to the increased reliance on digital tools and platforms as more people work remotely and shop online as a result of the pandemic. There was also a marked increase in online misinformation and Internet trolling across domains and social media platforms.

**260**

Digital forensics and investigations requests facilitated by the National KE-CIRT/CC during the period April to June 2020

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



# COLLABORATION AND CYBERSECURITY

As Kenya leverages on ICTs for education, healthcare, commerce and social interaction amidst the Covid-19 pandemic, the National KE-CIRT/CC continues to operate on a 24/7 basis in close collaboration with local and international partners in order to mitigate cyber threats and foster a safer Kenyan cyberspace.

As a multiagency framework, the National KE-CIRT/CC is responsible for the national coordination of cybersecurity as Kenya's national point of contact on cyber security matters.

Indeed, the continued successful execution of this mandate hinges on the leveraging of synergies between the agencies and stakeholders involved in the multiagency framework.

The Authority wishes to recognize and appreciate all our local and international partners for their contribution towards enhancing Kenya's cyber readiness and resilience.

**MERCY WANJAU, MRS**
AG DIRECTOR GENERAL

Report cyber incidents to the National KE-CIRT/CC via:

Email: incidents@ke-cirt.go.ke

Hotlines: **+254 703 042700, +254 730 172700**