OCTOBER - DECEMBER 2020
COMMUNICATIONS AUTHORITY OF KENYA
NATIONAL KE-CIRT/CC
CYBERSECURITY REPORT

COMMUNICATIONS AUTHORITY OF KENYA

EXECUTIVE SUMMARY

This report is a perspective of the Communications Authority of Kenya with respect to the National Cyber Security landscape during the period October – December 2020. The Communications Authority of Kenya (CA) is mandated with implementing the National framework for cybersecurity management in Kenya. Towards this, the Government of Kenya through the Authority established the National Kenya Computer Incident Response Centre – Coordination Centre (National KE-CIRT/CC) as the point of contact on cybersecurity matters. To achieve this mandate and safeguard Kenya's cybersecurity readiness and resilience, the Authority through the National KE-CIRT/CC has put in place initiatives covering people, processes and technologies to ensure the optimization and sustainability of the gains Kenya has so far realized in ICTs.

During the period October to December 2020, the National KE-CIRT/CC continued to carry out monitoring and receive incident reports from organizations and the public regarding cyber threat events. During this period there was continued use of social media platforms as a means for social interaction amidst the Covid pandemic. However, the increased use of social media platforms provided a wider attack surface to propagate various cyber incidents such as hate speech, incitement, cyber bullying, online trolling, social media impersonation and misinformation. To counter the rising trend in the use of social media platforms to propagate fake news and misinformation, social media service providers incorporated fact-checking warnings into their platforms.

This period was also characterized by an increase in cybercrime targeting remote workers with cybercriminals taking advantage of the lack of corporate firewalls and other location binding cybersecurity measures amongst remote workers. This included exploitation of vulnerabilities on systems that support remote working such as Virtual Private Networks (VPNs), video conferencing applications, among others. Further, cyber criminals continued to capitalize on the Covid pandemic through Covid themed phishing attacks.

The National KE-CIRT/CC also observed a continued spike in ransomware attacks during the period October – December 2020. This is amidst a growing trend where organizations are taking up cyber insurance to mitigate the financial impact of ransomware. However, this has elicited concerns that ransomware demands by ransomware gangs are being guided by these cyber insurance policies, and that these policies are a guiding element for the intensified ransomware extortion campaigns.

With the holiday season falling during the period under review, there was a marked increase in time spent online by consumers purchasing gifts and searching for the best deals. In anticipation of a possible increase in fraud targeting e-commerce platforms through the harvesting of user credentials and credit card skimming during the holiday shopping season, the National KE-CIRT/CC carried out an intense end user awareness to increase end-user vigilance on online fraud. The campaigns were mostly done on the online platforms.

Information sharing and collaboration is key in managing cyber security risks and enhancing the collective ability to achieve cyber readiness and resilience. Towards this, the National KE-CIRT/CC continues to work closely with local and international partners and build local cybersecurity capacity, increase awareness, and strengthen information sharing networks. Key amongst the local collaboration networks is the quarterly meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC), which was held virtually on 30th December 2020. In addition, the National KE-CIRT/CC supported the local cybersecurity community through various fora, amongst them the launch of the TAI Security Operations Centre (TAI SOC), which is a Security Operations Centre based at Strathmore University.

As Kenya strives towards being a digital economy, there is need to empower end users with the skills, knowledge and values necessary to thrive in the digital environment. Towards this, the National KE-CIRT/CC continued to carry out end user cybersecurity awareness through various initiatives and platforms. Amongst the initiatives during this period was the October Cybersecurity Awareness Month (OCSAM). This year, the Authority through the National KE-CIRT/CC sought to empower individuals and organizations to own their role in safeguarding their part of cyberspace through the theme 'Do Your Part #BeCyberSmart'. OCSAM incorporated various activities such as virtual Cyber Security Town Halls, a National Cyber Security Webinar, social media cyber awareness campaigns and engagements using the National KE-CIRT/CC official twitter handle.

"Towards a Cyber Ready and Cyber Resilient Nation"

CYBER THREAT STATISTICS

46,069,525

The number of malware threat events detected during the period October - December 2020.

2,260,036

The number of DDoS/Botnet threat events detected during the period October - December 2020.

7,847,457

The number of Web Application attack threat events detected during the period October - December 2020.

29,079

The number of System Vulnerabilities threat events detected during the period October - December 2020.

56,206,097

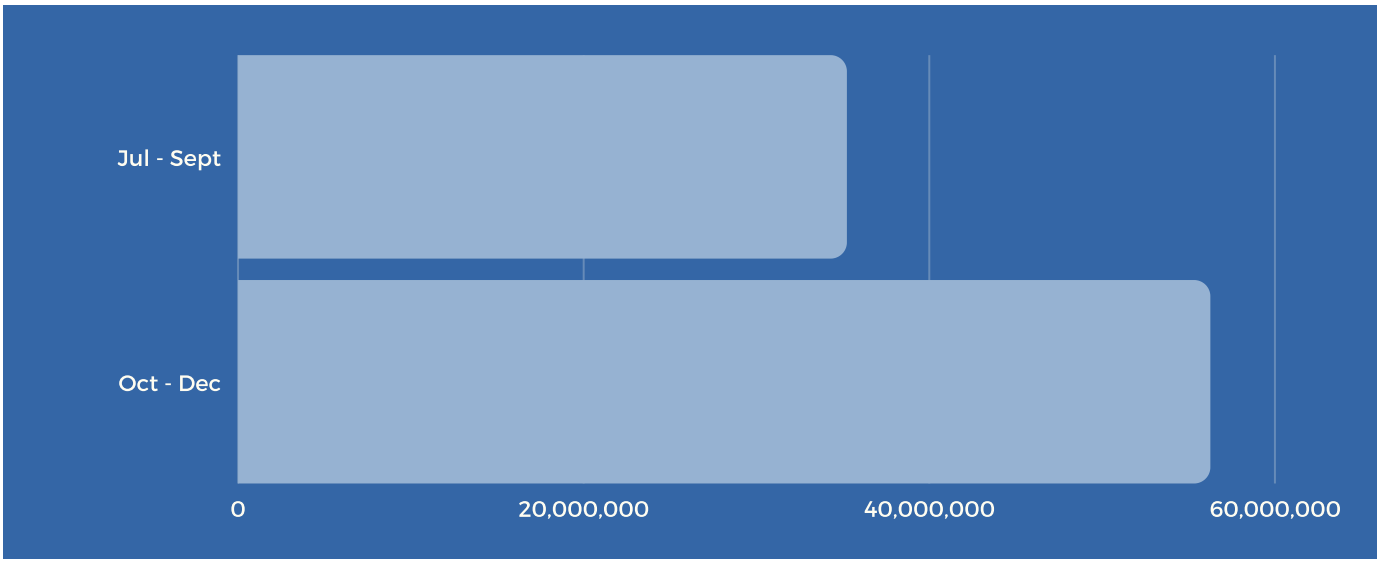
Total number of cyber threat events detected by the National KE-CIRT/CC during the period October - December 2020.

21,513

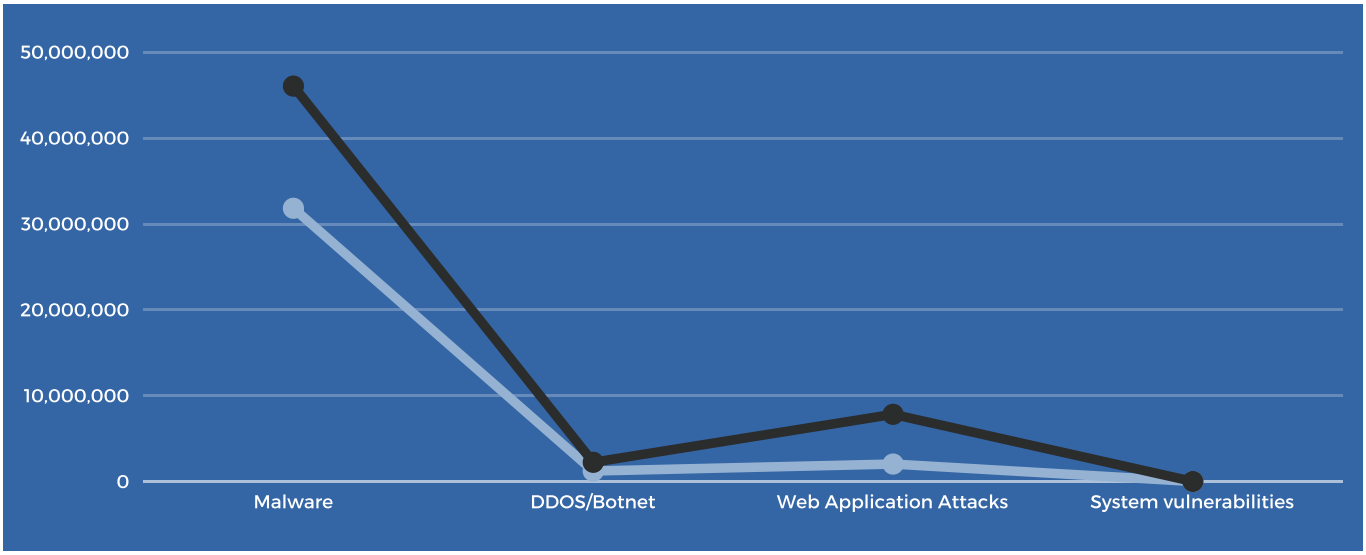
Total number of cyber threat advisories issued to affected organizations in response to cyber threat events detected by the National KE-CIRT/CC during the period October - December 2020.

CYBER THREAT LANDSCAPE

The National KE-CIRT/CC operates on a 24/7 basis carrying out monitoring, analysis and responding to cyber threats targeting Kenya. During the period October – December 2020, the National KE-CIRT/CC detected 56,206,097 cyber threat events. This was a 59.8% increase from the previous period July to September, where 35,173,937 cyber threat events had been detected. There was a significant increase in Malware, DDoS/Botnet and Web Application attacks during the period. This increase in cyber threat events detected is attributed to the systematic resumption to normalcy amongst sectors and services that were previously dormant due to the restrictions surrounding the Covid-19 pandemic. This is illustrated below.



In response to the 56,206,097 cyber threat events detected, the National KE-CIRT/CC issued 21,513 advisories, which was a decrease compared to the 21,728 advisories issued in the previous period. This is illustrated below.



CYBER THREAT ADVISORIES

21,513

In response to the 56,206,097 cyber threat events detected, the National KE-CIRT/CC issued 21,513 advisories, which was a decrease compared to the 21,728 advisories issued in the previous period.
The advisories provide timely information on emerging and current vulnerabilities and cyber threats thereby enhancing the cyber readiness of critical organizations in Kenya.

SYSTEM VULNERABILITIES

System vulnerabilities are weaknesses exploitable by cyber criminals who use these to cross privileged boundaries within a computer system. Cyber criminals exploit a system by possessing at least one applicable tool or technique that can connect to a system weakness. They focus on customer-facing assets and attack surfaces, as well as on weaknesses in third-party systems or applications that organizations use on a regular basis.

The common services exploited include web access services, authentication services, database services, network services, domain name systems, and remote access services.

During the period under review, the National KE-CIRT/CC detected 29,079 system vulnerabilities, which was a 2.1% increase from the 28,482 detected in the previous period July – September 2020.

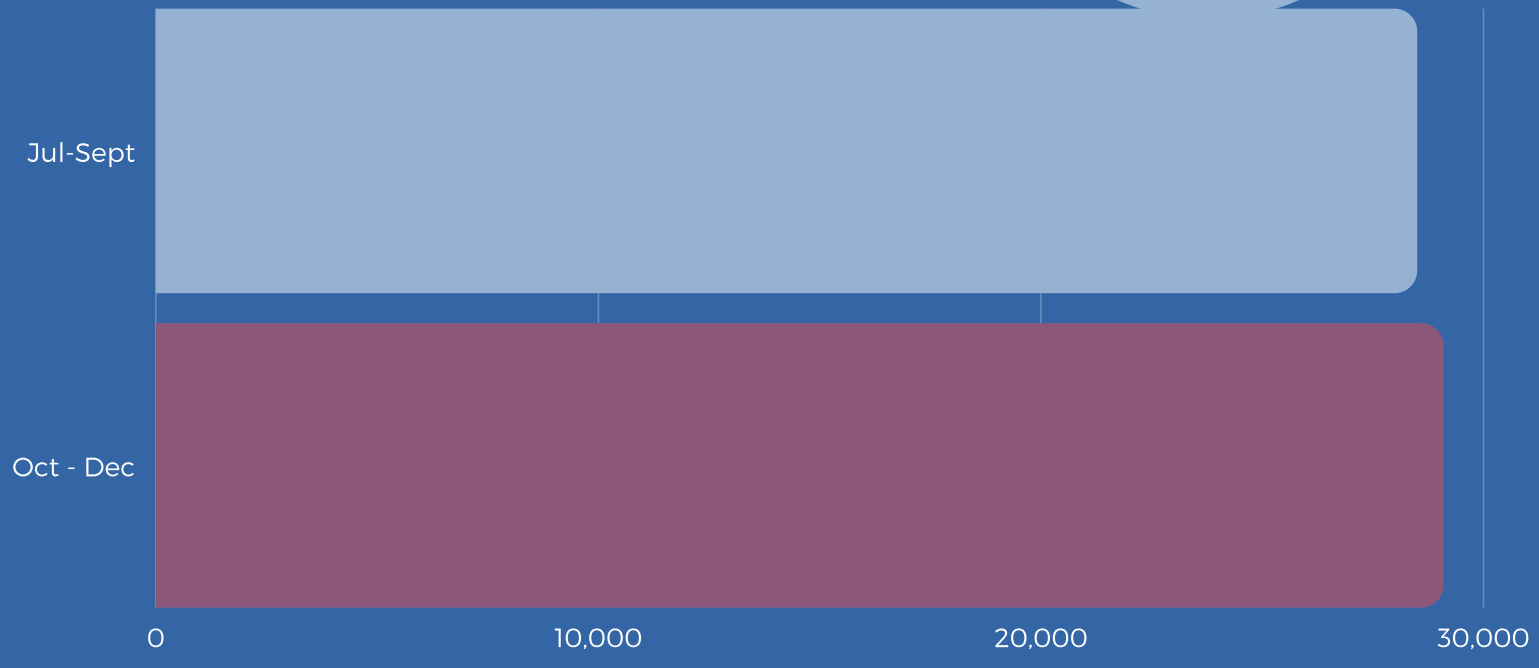
In response to these detected system misconfiguration events, the National KE-CIRT/CC issued 19,521 cyber threat advisories, which was a slight decrease from the last period July to September 2020.

Cyber criminals exploited system vulnerabilities during this period to breach systems for purposes of compromising and stealing personal and financial data such as usernames, passwords and email addresses.

29,079

Detected system vulnerabilities events during the period

An analysis of System Vulnerabilities threat attempts detected during the period October - December 2020



MALWARE

Malware refers to any malicious code or program such as viruses, bugs, worms, bots, rootkits, spyware, adware, Trojans, and even ransomware that gives a cybercriminal explicit control over your system.

During the period October to December 2020, the National KE-CIRT/CC detected 46,069,525 malware threat events, which was a 44.7% increase compared to 31,842,635 in the previous period July – September 2020. This is attributed to an increase in distribution of malware on the mobile arena as well as the increase in attacks targeting corporate networks amidst the systematic resumption to normalcy from the Covid-19 restrictions.

In response to these malware threat events, the National KE-CIRT/CC issued 850 malware advisories, which is a 15.3% decrease as compared to the 1,003 that were issued in the previous period, July – September 2020.

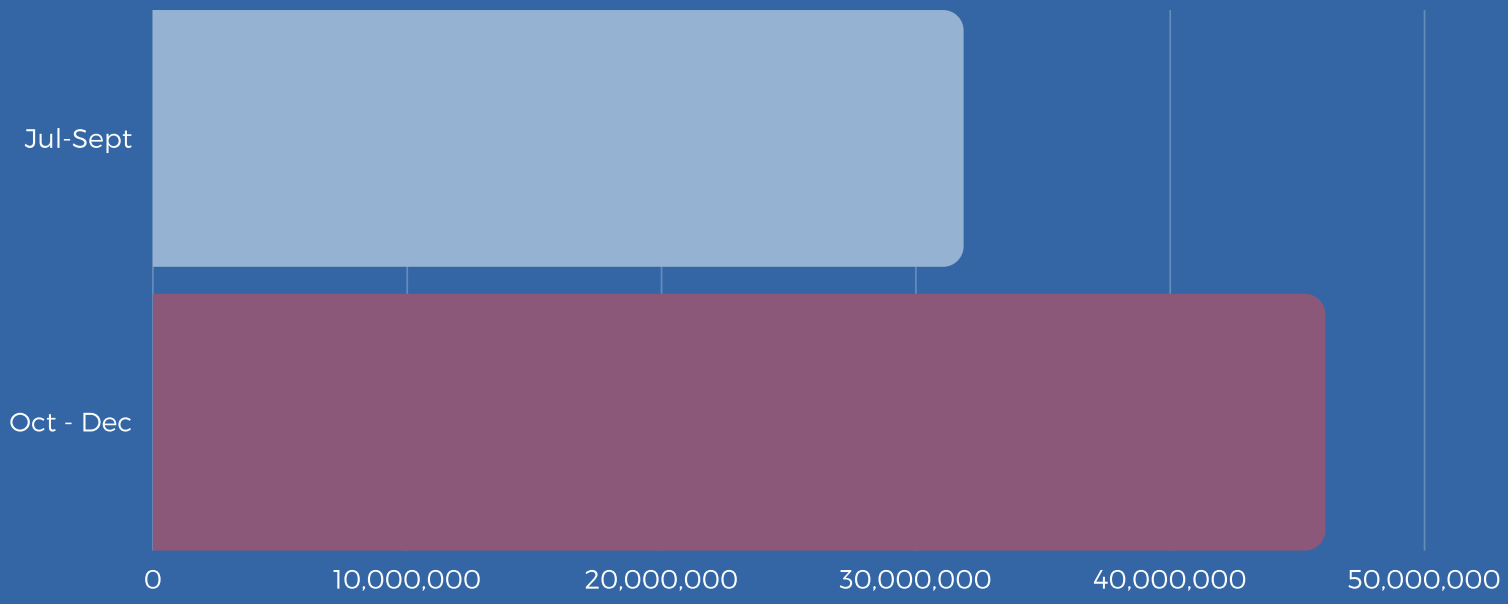
The National KE-CIRT/CC noted the continued migration of malware to the mobile arena during the period under review, with malicious applications masquerading as legitimate applications in official application stores.

Also notable during this period was the continued evolution of Emotet from a banking Trojan to its current capabilities of delivering a collection of malware such as information stealers, email harvesters, self propagation mechanisms and ransomware to devices and systems

46,069,525

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

An analysis of Malware threat events detected during the period October - December 2020



PHISHING

Phishing is the fraudulent attempt by a cybercriminal to obtain sensitive data by posing as a trustworthy party. Spam is the unsolicited sharing of messages with the intention of broadcasting unwanted or malicious content. Spam can be used to spread phishing campaigns. The National KE-CIRT/CC continued utilizing existing monitoring systems to gather reports on spam and phishing threat attempts locally.

During the period October – December 2020, the National KE-CIRT/CC noted a large-scale phishing campaign that targeted 200 million Microsoft 365 users globally across the financial services, healthcare, insurance, manufacturing, utilities, and telecom sectors. These attackers are said to have leveraged on a domain spoofing technique to create emails that appear to have come from Microsoft Outlook (no-reply@microsoft.com), which duped unsuspecting victims into clicking the link on a fake authentication page.

The National KE-CIRT/CC also noted a surge in malicious phishing campaigns targeting online shoppers in the form of "special offers" that capitalized on the holiday shopping season to hook unsuspecting online shoppers. The fraudsters would use spoofed email addresses and share a link that leads to a newly registered domain that spoofs a legitimate website.

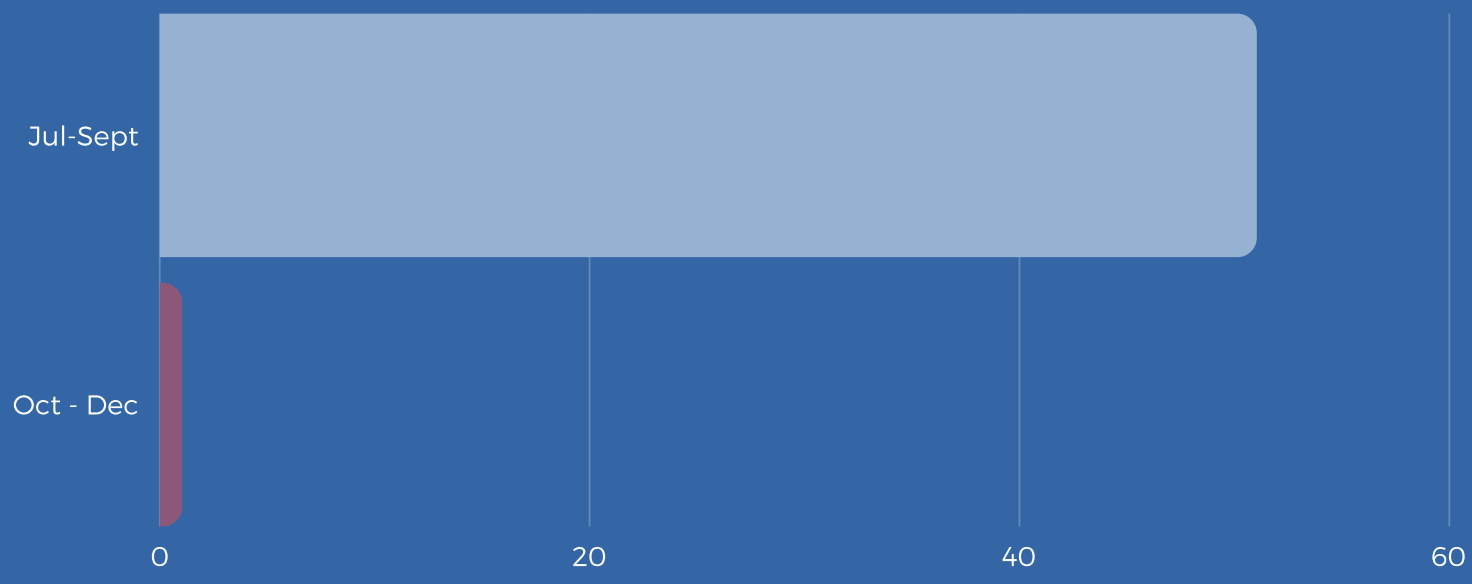
To counter this growing trend, the National KE-CIRT/CC published a cybersecurity best practice guide about Holiday Sales Scams on our social media platforms to create awareness.

During the period under review, the National KE-CIRT/CC also noted the persistence of COVID-19 themed phishing campaigns. This was targeted at harvesting user credentials, delivering malware and carrying out financial fraud through fake charity donations. There was also an increase in incidents of spoofing of login and download pages for popular web conferencing applications such as Zoom, Skype, and WebEx.

1

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

An analysis of Phishing advisories issued during the period October - December 2020



WEB APPLICATION ATTACKS

Web Application attacks are executed by leveraging on web application vulnerabilities such as misconfiguration in websites application code, that allow cyber criminals to gain control of the website.

During the period October - December 2020, the National KE-CIRT/CC detected 7,847,457 web application attacks, which was a 281.4% increase from the 2,057,369 detected in the previous period July – September 2020.

The increase is attributed to the increased adoption of unsecured online platforms, failure to updated plugins, and lack of technical capacity to secure these platforms amongst users. Some of the targeted platforms include banking, government services and working from home platforms.

In response to the 7,847,457 web application attack events detected, the National KE-CIRT/CC issued 625 advisories during this period.

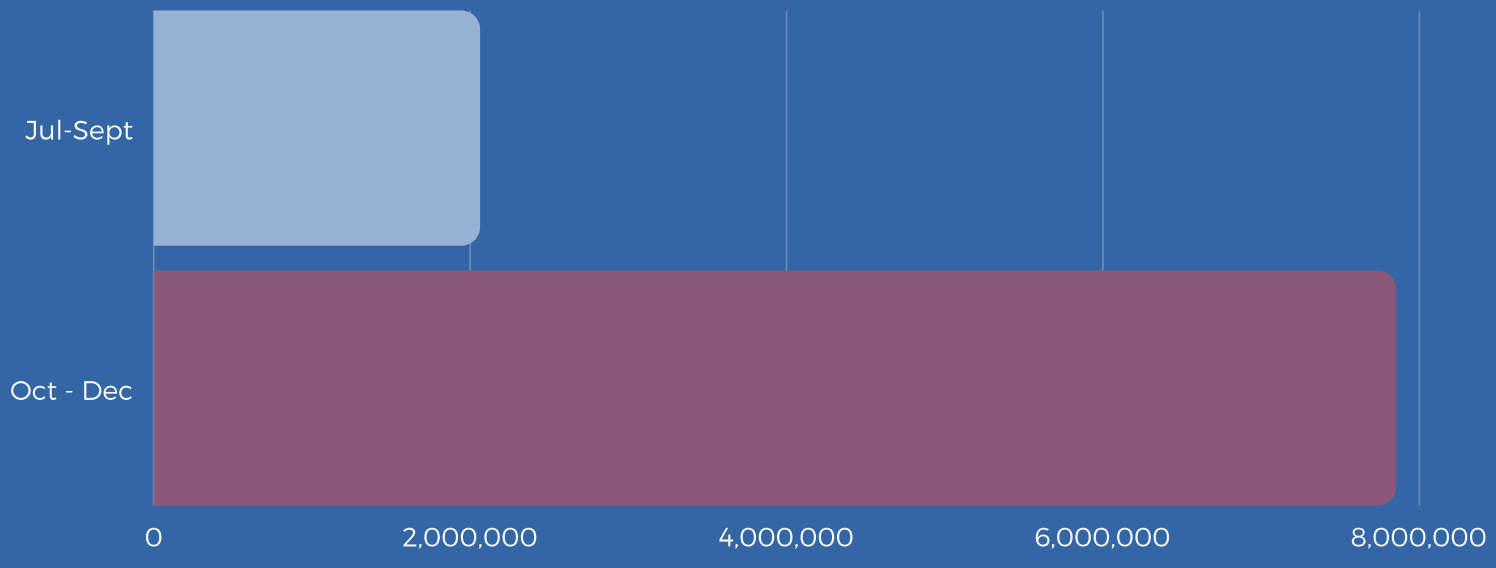
Notable web application attacks during the period under review include the code injection attacks to WordPress sites via Welcart e-commerce vulnerability. Welcart is a WordPress plugin that allows site owners to add online shopping to their sites. The vulnerability in the plugin allows cyber criminals to install payment skimmers, to crash the site, or retrieve information via SQL injection. Site admins were advised to upgrade after a patch was developed by its publisher.

Also notable was the discovery of a Two-Factor Authentication (2FA) bypass in cPanel that potentially exposed tens of millions of websites to hackers. Researchers stated that the 2FA implementation of cPanel & WebHost Manager (WHM) software was vulnerable to brute-force attacks that allowed attackers to guess URL parameters and bypass 2FA thereby manage the associated websites. The vulnerability was later patched and website administrators were urge to confirm that their hosting provider has updated the patch.

7,847,457

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

An analysis of Web Application Attack threat events detected during the period October - December 2020



BOTNET/ DDOS

Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding IT infrastructure with a flood of Internet traffic. A botnet is a group of Internet connected devices running automated tasks over the Internet and which can be used to perform DDoS attacks.

During the period October - December 2020, the National KE-CIRT/CC detected 2,260,036 events as compared to the 1,245,451 events detected during the previous period, representing an 81.5% increase. This increase is attributed to the increase in malicious attacks by cybercriminal who are using these hijacked devices to disrupt online systems that are supporting remote working.

In response to these detected Botnet/DDOS attack attempts, the National KE-CIRT/CC issued 243 advisories which represent a 28.2% decrease from the 326 advisories issued in the previous period July – September 2020.

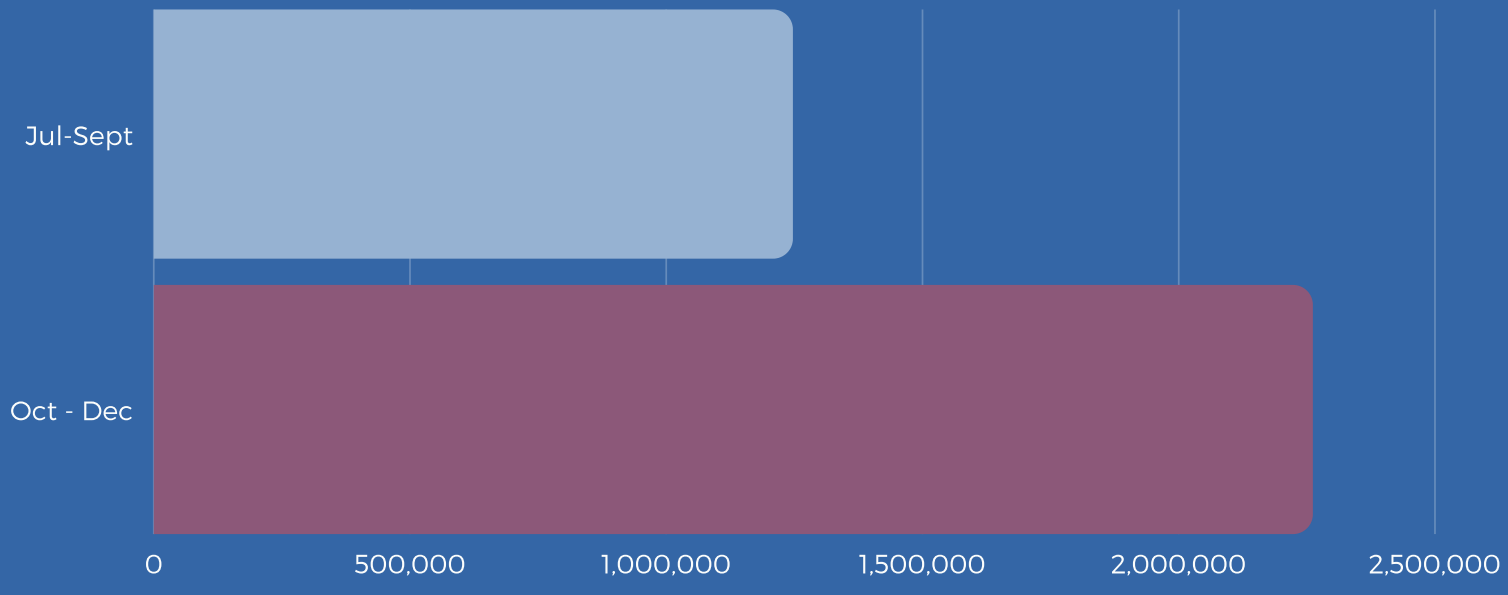
Notable during the period was the revelation by Google of the largest DDoS attack recorded to date, which clocked at 2.54 Tbps and that targeted Google services in 2017. A state-sponsored threat actor reportedly carried out this attack. This revelation was part of Google's awareness campaign about the increased use of state-sponsored threat actors to disrupt systems through DDoS attacks, with Google claiming that these state-sponsored DDoS attacks are likely to intensify in the coming years as internet bandwidth also increases.

Also notable was the evolution of the Gitpaste-12 botnet to hijack more devices by targeting web applications, IP cameras, and routers. Gitpaste-12 propagates through GitHub and Pastebin platforms by exploiting vulnerabilities related to Apache Struts, Asus routers, Webadmin plugin for opendreambox, and Tendo routers. The botnet also features commands allowing it to run a cryptominer that targets the Monero cryptocurrency and install backdoors.

2,260,036

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 October - December 2020



DIGITAL INVESTIGATIONS

The National KE-CIRT/CC continues to secure and analyze digital evidence and conduct research and development through the Digital Forensic Lab (DFL). Exhibits relating to criminal matters are conveyed to the DFL by law enforcement agencies while requests for preservation, identification, extraction and documentation of digital evidence relating to civil matters are accompanied by court orders.

Some of the cases received by the National KE-CIRT/CC digital forensics and investigations team include impersonation, online fraud, online abuse and child abuse. Impersonation is the act of presenting oneself as some else with the ultimate goal of falsely obtaining private information, access to a person, access to systems information or even carrying out financial fraud; Online fraud entails the use of Internet services or software to defraud victims or to otherwise take advantage of them; Online abuse entails cyber bullying and incitement; and online child abuse entails the physical, sexual, and/or psychological abuse of children on online platforms. The National KE-CIRT/CC continues to carry out cyber awareness in an effort to counter these harmful online practices.

During the period October - December 2020, the National KE-CIRT/CC received 224 investigation related requests as compared to 354 requests received in the previous period.

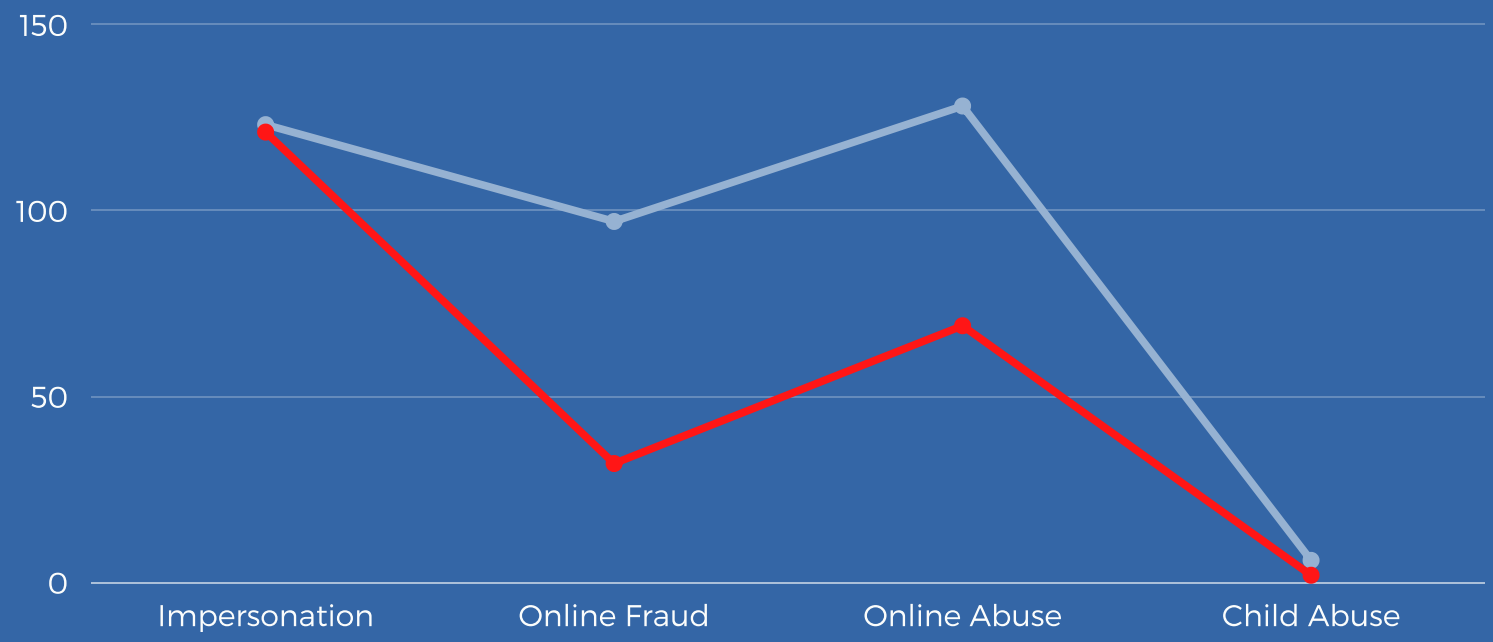
As a result of these concerted consumer awareness and capacity building efforts, there was a decrease in impersonation, online fraud, online abuse and child abuse cases reported to the National KE-CIRT/CC.

The decrease in child abuse cases is attributed to the ongoing child online protection awareness efforts by the Authority coupled with collaborative efforts between the National KE-CIRT/CC and the Directorate of Criminal Investigation's Child Protection Unit (DCI CPU) in responding to reports relating to child online abuse.

224

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

An analysis per category of the number of digital forensics and investigations cases facilitated by the National KE-CIRT/CC during the period October - December 2020



DIGITAL FORENSICS

The Digital Forensics Lab (DFL) within the National KE-CIRT/CC is tasked with carrying out digital forensics which includes: mobile forensics which is the recovery of digital evidence or data from a mobile device under forensically sound conditions; Disk forensics which is the extraction of forensics information from digital storage media; and, Network Forensics which is the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection.

The digital forensics team at the National KE-CIRT/CC is made up of law enforcement officers who carry out forensics and produce expert reports for court purposes after carrying out examination of the various digital exhibits received. During the period October - December 2020, law enforcement officers based at the National KE-CIRT/CC attended court proceeding to give evidence or participate as expert witnesses in on-going cases requiring digital forensics.

Exhibits relating to criminal matters are brought to the lab by law enforcement agencies while those on civil matters are accompanied by court orders. During the period October – December 2020, the National KE-CIRT/CC Digital Forensics Lab received 58 forensic requests. This was an increase compared to the 15 requests received in the previous period July-September 2020.

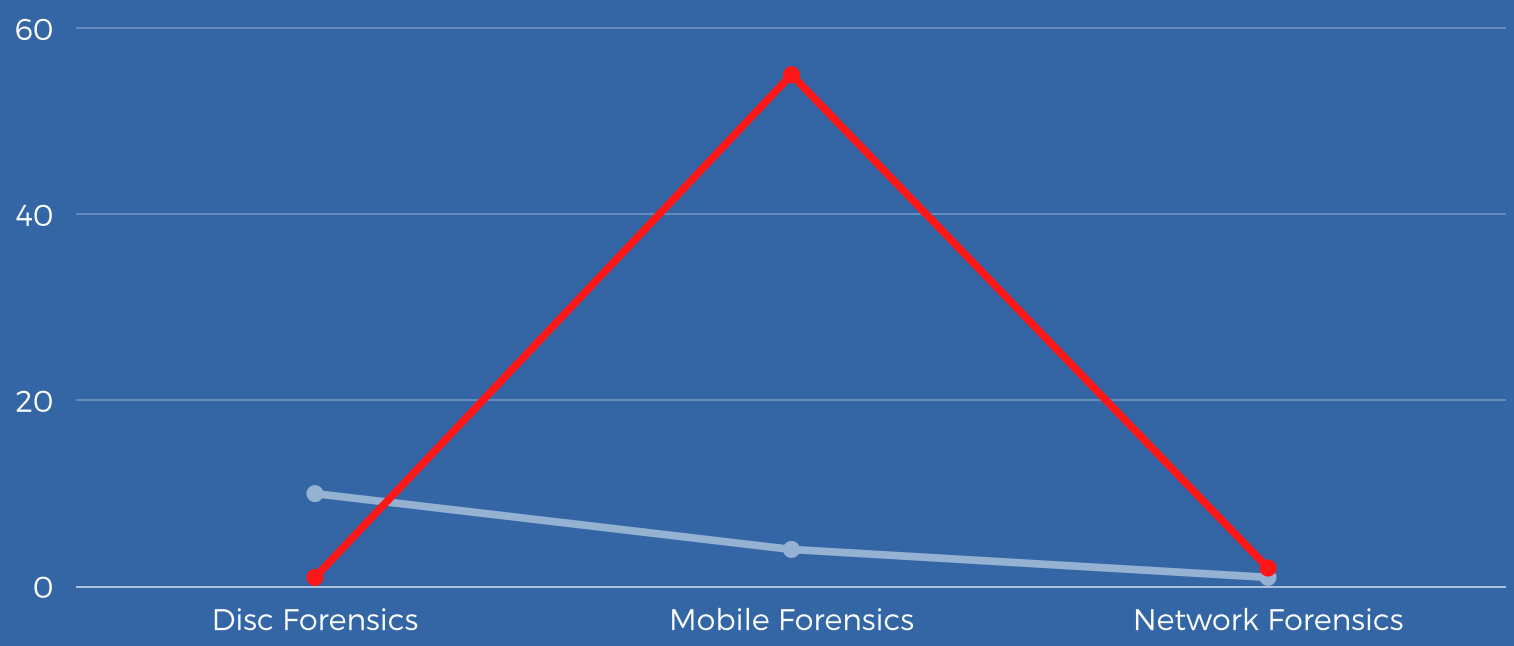
The increase in forensic cases was attributed to an upsurge of mobile forensic requests to facilitate investigations into child online sexual exploitation cases during the holiday season. Schools closure due to the Covid-19 pandemic saw students having more unsupervised exposure to mobile devices and the Internet. As a result, there was an increase in requests for mobile forensics to investigate possible child online abuse cases.

To mitigate against the threat of child online abuse during this period where schools were closed, the National KE-CIRT/CC shared awareness information to parents and guardians on how to safeguard children online. Further, the National KE-CIRT/CC held a Virtual Cyber Townhall on 'Child Online Protection in the Age of Digital Learning' during the month of October.

58

Digital forensics requests facilitated by the National KE-CIRT/CC during the period

An analysis per category of digital forensics requests facilitated by the National KE-CIRT/CC Digital Forensics Lab during the period October - December 2020



COLLABORATION AND CYBERSECURITY

The National KE-CIRT/CC continues collaborate with various critical cybersecurity stakeholders locally and globally with the aim of enhancing the national cyber readiness and resilience. Towards this, the National KE-CIRT/CC continued to partner with various National Computer Incident Report Teams (CIRTs), the global 24/7 G7 Cybercrime Network, the International Telecommunication Union (ITU), the Forum for Incident Response and Security Teams (FIRST), Internet Corporation for Assigned Names and Numbers (ICANN), Facebook, Twitter, Google and GoDaddy to leverage on knowledge sharing and levelled-up research and development to further upscale the nation's cybersecurity standing.

Through the National KE-CIRT/CC Cybersecurity Committee (NKCC), the National KE-CIRT/CC addresses various national and sector cybersecurity concerns. Drawing its membership from telecommunications companies, financial sector stakeholders, academia, law enforcement agencies, public utility companies, professional associations, among others, the committee is one of the critical local collaborative efforts at enhancing Kenya's national cybersecurity posture. The NKCC held its 33rd virtual quarterly meeting on 30th December 2020.

During the period under review, the Authority through the National KE-CIRT/CC participated in the October Cybersecurity Awareness Month (OCSAM). This year's OCSAM global focus was to empower individuals and organizations to own their role in safeguarding their part of cyberspace, with the theme 'Do Your Part #BeCyberSmart'. During the month of October, the National KE-CIRT/CC successfully carried out cyber awareness and engagement on various social media platforms, hosted a Virtual Cyber Town Hall on "Child Online Protection in the Age of Online Learning", and, hosted the Annual National Cybersecurity Conference as a Webinar on the topic "E-government in a Digital Economy ~ Securing and Transforming Government Services". These activities offered an opportunity to carry out awareness on the National KE-CIRT/CC, the NPKI and the Dot KE.

Further, throughout the period under review, the National KE-CIRT/CC continued to engage in cybersecurity awareness, sensitization and capacity building to the Authority's staff and to the public through daily cybersecurity incident advisories, bi-weekly cybersecurity best practice guides, daily cybersecurity updates, press statements on emerging cybersecurity concerns, and through social media. The National KE-CIRT/CC also continues to avail channels for 24/7 reporting and response for organizations and individuals seeking assistance on various cybersecurity concerns.

MERCY WANJAU, MBS
AG DIRECTOR GENERAL
COMMUNICATIONS AUTHORITY OF KENYA

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

Email: incidents@ke-cirt.go.ke

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