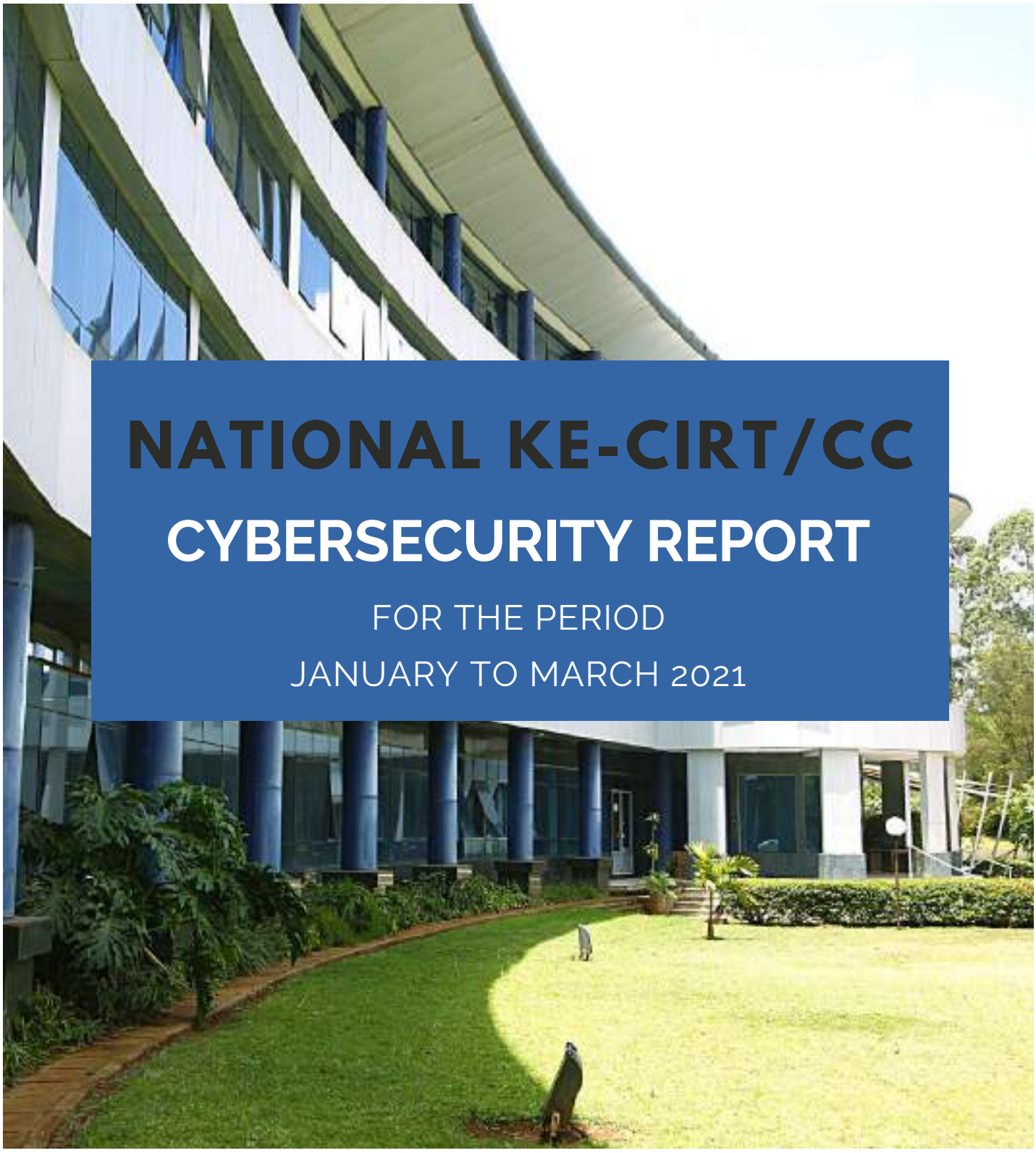
COMMUNICATIONS AUTHORITY OF KENYA



NATIONAL KE-CIRT/CC

CYBERSECURITY REPORT

FOR THE PERIOD

JANUARY TO MARCH 2021

About Us

The Kenya Information and Communications Act, 1998, supported by the Computer Misuse and Cyber Crimes Act, 2018, mandates CA as the regulator of the ICT sector in Kenya to contribute towards the national management of cybersecurity in Kenya along with other appointed Ministries, Departments and Agencies.

It is in this regard that the Government established the National Kenya Computer Incidence Response Team – Coordination Centre (National KE-CIRT/CC), which is based at the Communications Authority of Kenya HQ, the CA Centre.

The National KE-CIRT/CC is a multi-agency collaboration framework responsible for the national co-ordination of cybersecurity, and is Kenya's point of contact on cybersecurity matters.

MISSION

Building a connected society through enabling regulation, partnership and innovation.

VISION

A Digitally Transformed Nation.

VALUES

Integrity

Innovation

Excellence

MESSAGE FROM THE DIRECTOR GENERAL

COVID-19 continued to drive digital transformation by speeding up the adoption of digital technologies by individuals and organizations. From digitizing customer facing as well as internal operations, the pandemic created new opportunities for innovation in products and services, as businesses sought to remain competitive in this economic environment. This digital transformation included the increased uptake of Device-as-a-Service (DaaS) plans. DaaS provides organizations with pre-configured devices that are pre-installed with specific applications and security software, as well as other value-added services at a periodic subscription fee.

This accelerated digital adoption streamlined processes, led to innovative and new ways of doing business, enhanced efficiency, agility and productivity, and allowed businesses to reach new global markets. However, this accelerated digital transformation increased the attack surface, as cybercriminals optimized attack campaigns to increase their success rate.

During this period, the Authority observed an increase in phishing, ransomware, Trojans and botnet attacks globally. This was amidst the global shift towards automation by cyber threat actors for purposes of increasing efficiency and productivity, maximizing profits and scaling operations. This resulted in cybercriminals industrializing malware and social engineering campaigns for malicious purposes.

As working remotely continues to be our new reality amidst measures such as restrictions in movement that are aimed at flattening the curve of new COVID-19 infections, organizations are rapidly adopting the use of cloud services, remote access tools and collaboration applications. This has resulted in an increase in cloud and remote services attacks, due to these tools not being properly vetted or configured. Cyber threat actors exploited these vulnerabilities to carry out attacks leading to data breaches.
As organizations adopted third-party applications from vendors to support existing services amidst this digital transformation, there was a notable increase in third-party application attacks. This was attributed to cybercriminals leveraging on the vulnerabilities in third-party vendors systems to gain access to the organizations' websites and systems to steal data and download malware on the affected systems.

Small, Medium and Micro Enterprises (SMMEs) also continued to face a myriad of cyber threats in the wake of the COVID-19 pandemic. These included sophisticated ransomware attacks, phishing and supply chain attacks. This was attributed to lack of information system infrastructure and information security personnel, lack of awareness of cyber threats and lack of information management frameworks.

Also notable during this period was an increase in the prevalence and complexity of malware. Emotet, one of the most costly and destructive malware variants ever seen, made a resurgence during this period despite global efforts towards take down. Emotet continued to evolve from what was once a banking Trojan to a distributer of other malware or malicious campaigns. Worryingly, Emotet uses multiple methods for maintaining persistence and evasion techniques to avoid detection and can be spread through phishing spam emails containing malicious links or attachments.

As smart phone use increases, there are growing concerns globally over privacy of data held by mobile application developers and how this is shared with third parties. Towards this, various regulators worldwide are working towards developing regulations to secure individuals' personal data. These regulatory trends include requiring informed consent by users, limiting data gathering by mobile applications to minimum necessity and ensuring that terms are presented to users in simple, clear language.

In recognition of the critical role that a safer Internet plays in Kenya's socio-economic transformation, the National KE-CIRT/CC joined the world in celebrating Safer Internet Day. This was in recognition of the key role that cybersecurity plays as a critical enabler of Kenya's digital transformation. Safer Internet Day celebrations were marked by the launch of the interactive Child Online Protection (COP) micro-site, to promote the safe and positive use of digital services and technology by children. The running theme for this year was "Together for a Better Internet".

The National KE-CIRT/CC also continues to collaborate with local and international stakeholders in monitoring, analysis and responding to these cyber threats. Key amongst this is the continued collaboration with local stakeholders through the National KE-CIRT/CC Cybersecurity Committee (NKCC) whose membership entails financial sector players, telecommunication, Internet service providers, law enforcement agencies, and academia amongst other government agencies. In addition, the National KE-CIRT/CC continues to issue cybersecurity technical advisories to the affected organizations and complements these with cyber awareness campaigns, which are geared towards enhancing the national cyber hygiene and cyber readiness levels.

MRS. MERCY WANJAU, MBS
AG. DIRECTOR GENERAL
COMMUNICATIONS AUTHORITY OF KENYA

MOBILE

Increased smartphone use has led to convergence of work and personal life functionalities in a single device. This has led to increasing data and privacy concerns over data collected by mobile application developers and how this data is shared with third parties. These concerns have led to some countries developing regulations to address personal data held by mobile application developers. These regulations touch on issues relating to informed consent, the presentation of terms of use in simple and clear language, as well as guidelines on data gathering and minimum necessity.

During this period, there was an increase in mobile phishing attacks with the majority of successful attacks taking place via gaming, messaging and social media applications. These attacks are designed to steal data, install spyware and carry out Denial of Service (DDoS) attacks, with scammers leveraging on device-centric social engineering to widen the attack surface. To address this growing trend, the National KE-CIRT/CC issued Cybersecurity Best Practice Guides advising the public not to click on links in emails and messages from unknown senders.

As smart phones become more powerful, there is a tremendous increase in malware targeting these mobile devices. This explosion of malware targets smartphones and tablets via banking malware, mobile ransomware, MMS malware, mobile adware, mobile spyware, and SMS Trojans. These malicious applications are designed to completely avoid detection; with the most common method being through malicious applications and downloads. Mobile devices become infected when cyber threat actors exploit vulnerabilities in their Operating Systems (OS), when users open suspicious emails and texts and click on the embedded links, when users access insecure websites and WI-FI networks, or when users download applications from less legitimate sources “Pirated” apps. To address this, the National KE-CIRT/CC issued Cybersecurity Best Practice Guides advising end-users to avoid jail-breaking devices, use Virtual Private Networks (VPN), download apps only from reputable sources and regularly update their device software.

Also notable during this period was the increase in cyber romance scams. Cyber romance scams occur when cybercriminals adopt a fake online identity for purposes of gaining the victim’s affection and trust, and then use the illusion of a romantic relationship to manipulate or steal from the victim. The cybercriminal thereafter devises a fake cause such as a medical expense or family emergency that requires the victim to send them money. To address this, the National KE-CIRT/CC issued Cybersecurity Best Practice Guides advising end-users to conduct due diligence to verify the identity of online love interests and to avoid sharing Personal Identifiable Information (PII) that may make them a target for such scams.

CHILDREN AND THE INTERNET

The Covid-19 pandemic has resulted in the rapid adoption of digital technologies, with more households adopting digital solutions for learning, entertainment and socialization. This has resulted in an increase in screen time amongst children as well as increased unsupervised access to the Internet by minors.

During this period, there was a notable increase in child online sexual exploitation and grooming, as well as cyber bullying and cyber harassment targeting children. There was also an increase in the number of downloads and uploads of indecent photos and videos of children. Also worrying was the increased manipulation of Internet content popularly accessed by children with inappropriate content. This has led to calls for more stringent measures to protect children online such as the use of Artificial Intelligence by social media platforms to protect children online, as well as calls for internet service providers to consider incorporating mechanisms to protect children online in their packages.

As more children operate social media accounts, there has also been an increase in child Personal Identifiable Information (PII) that is available on social media sites, which makes them vulnerable to online predators. To counter this, some social media platforms have announced changes to their account settings, automatically setting accounts of users aged between 13 and 15 to private, in an effort to shield minors from potentially inappropriate interaction with online predators. This move will limit who can view and comment on any content posted by this age group of users. Other social media platforms have increased their efforts to crack down on child online abuse on their platforms by restricting account creation of children below 13 years, monitoring account activity for children aged between 13 and 18 years, implementing child friendly parameters on its plugins, improving child online abuse detection capabilities, and updating tools to prevent sharing of content that victimizes children.

In an effort to ensure that parents and children have the necessary knowledge, skills and values to safely navigate the Internet, the Authority in partnership with local telecommunications service providers, launched an interactive portal aimed at creating a safer online environment for children. The micro-site, which was developed in collaboration with Safaricom, Airtel, Telkom Kenya, Jamii Telecommunication Ltd and the Global System for Mobile Communications (GSMA), provides online safety tips for children and guardians. The gaming component of the microsite enables both parents and children to measure their level of awareness on online risks such as cyber bullying, identity theft and online sexual harassment through an immersive learning experience.

To find out more about how to protect children online, go to: https://cop.ke-cirt.go.ke/

EMERGING TECHNOLOGIES

Deepfakes are videos, photos, or audio recordings that seem real but which have been manipulated with computers using machine-learning (artificial intelligence) software. Deepfake technology can create convincing but entirely fictional photos, videos or even audios from scratch. Deep fakes, so-named because they use deep learning technology, are a branch of machine learning that apply neural net simulation to massive data sets in order to create a fake version of the identified target. The underlying technology can replace faces, manipulate facial expressions, synthesize faces, and synthesize speeches. Advances in the application of Generative Adversarial Networks (GANs) have made it possible for AI algorithms to continuously learn and update dynamically to make better forgeries.

Deepfake technology can be used in the film industry such as in Computer-Generated Imagery (CGI) footage, in gaming, or even for corporate training purposes. However, there have been worries that the technology could be abused to create realistic doctored videos for malicious purposes.

Deepfakes could be used to generate blackmail materials that falsely incriminate a victim. Audio deepfakes are increasingly being used as part of social engineering scams for purposes of misleading people into thinking they are receiving instructions from a trusted individual. They can also be used to misrepresent well-known public figures in videos and can be used to defame, impersonate, and spread disinformation. In addition, majority of deepfakes on the Internet feature pornography using the likeness of celebrities and public personalities without their consent.

While it is becoming increasingly difficult to detect deep fakes from genuine content, there are proposals suggesting the use of the same AI solutions to detect deep fakes. Another proposed solution is the use of media literacy campaigns targeting the public, which create awareness on the existence of deep fakes and how to spot them. To address this locally, the National KE-CIRT/CC issued Cybersecurity Best Practice Guides educating end-users on deepfakes and how to spot them.

E-COMMERCE

The COVID-19 pandemic resulted in more businesses providing their goods and services through online platforms. This was largely in response to measures that have been put in place to flatten the curve such as the restrictions in movement in certain areas of the country and the curfew. This increased uptake of e-commerce has enabled Small, Medium and Micro Enterprises (SMMEs) to expand and tap into new markets. The shift to the digital space has also enabled businesses to reduce costs by closing down physical stores, spurred innovation and enabled businesses to remain competitive in the changing business environment. This shift has widened the attack surface, with cyber threat actors using more sophisticated arsenal of methods to exploit vulnerabilities in these platforms.

During this period, the top cyber threats in e-commerce were Distributed Denial of Service (DDoS) attacks, credit card fraud, malware, bad bots, SQL injections, phishing attacks and e-skimming. Attackers targeted customer data for purposes of stealing personal information such as credit card numbers as well as login credentials, which were subsequently sold on the black market. The increase in these threats amongst sites owned by SMMEs is attributed to poor cyber hygiene practices, lack of information system infrastructure and information security personnel, lack of awareness on cyber threats and lack of information management frameworks.

To protect against these rising cyber threats targeting e-commerce platforms, it is important that these sites have at least one level of encryption in place. In addition, in order to ensure that your business does not become a victim of credit card and debit card fraud, it is important that you ensure that your payment gateway is secured. Securing your website with an SSL certificate protects sensitive user data that is submitted to your website and makes it difficult for cyber threat actors to eavesdrop on your website. It is also important that you use reliable antivirus software to protect your computer and those using the backend of your e-commerce site. Lastly, it is essential that you install a firewall on your e-commerce server to monitor traffic and protect your e-commerce site from DDoS attacks.

NPKI

The National Public Key Infrastructure system is considered a critical element of securing Kenya's cyber space as it assures the safety of electronic transactions and online services such as e-Government, Financial, Health, Tax, Insurance, among others.

A Public Key Infrastructure (PKI) refers to a system for the creation, storage and distribution of digital certificates, which are used to verify that a particular public key (online identity) belongs to a certain entity. A PKI is a technical infrastructure that comprises a Root Certification Authority (RCA) and a Certification Authority (CA).

The PKI creates a framework for protecting communications and stored information from unauthorized access and disclosure, by addressing the fundamentals of cybersecurity, which are - confidentiality, integrity, authentication and non-repudiation. As such, the PKI is key to the rollout of e-transaction services.

Kenya's National PKI comprises of a Root Certification Authority (RCA), which is managed by the Communication Authority of Kenya (CA) as a regulatory function. Under the Electronic Certification Service Providers (E-CSPs) license regime, CA oversees the technical accreditation and licensing process of players in the NPKI system, that are referred to as Certification Authorities (CAs). The licensing process includes review and approvals of the Business Plans, Technical Proposals, Technical Compliance to the x.509 ITU Standards, creation of the algorithms and scripts to facilitate the propagation of the first Certificate.

The NPKI is instrumental towards the effectiveness of the licensing of Electronic Certification Service Providers (E-CSPs), since a licensed E-CSP must be accredited by the RCA for its digital certificates to be globally recognized and trusted.

To facilitate the successful rollout of the NPKI, the Authority during the period January to March 2021 hosted a series of preparatory workshops with key stakeholders to guide operationalization of the NPKI in the public sector. Legal, supply chain, technical and communication were the main thematic areas considered towards the operationalization of the NPKI during this period. In an effort to create awareness on the NPKI, the National KE-CIRT/CC continued to carry out consumer education and awareness on the benefits of e-signatures and digital signatures brought on by NPKI.

GLOBAL CYBER THREAT LANDSCAPE

Cyber threat actors continued to leverage on system and network vulnerabilities to unveil even more aggressive cyber attacks. These included malware and ransomware attacks targeted at cloud services, Internet of Things (IoT) devices, mobile devices and web browser applications supporting schools, enterprise infrastructure, healthcare systems and facilities, and consumer services. This period also saw cyber threat actors compromising remote access software to gain unauthorized access into public-sector utilities with the aim of remotely manipulating critical systems thereby compromising public safety.

Accelerated digital adoption as a result of the pandemic has widened the web applications attack surface. During the period, cyber threat actors increasingly used automated tools to launch attacks targeted at web applications vulnerabilities through fuzzing attacks, injection attacks, fake bots and application Distributed Denial of Service (DDoS) attacks. Cyber threat actors leveraged on these automated attacks to avoid detection thereby enabling them to subtly overload website resources and crash them.

With the rollout of COVID-19 vaccines, there was a notable move by cyber threat actors to compromise Information Technology (IT) applications of healthcare, pharmaceuticals, universities and other organizations involved in the COVID-19 vaccine development and distribution. This is being carried out for purposes of spreading disinformation campaigns designed to undermine trust in the vaccines.

Jan - Mar 2021

OVERVIEW OF THE LOCAL CYBER THREAT LANDSCAPE

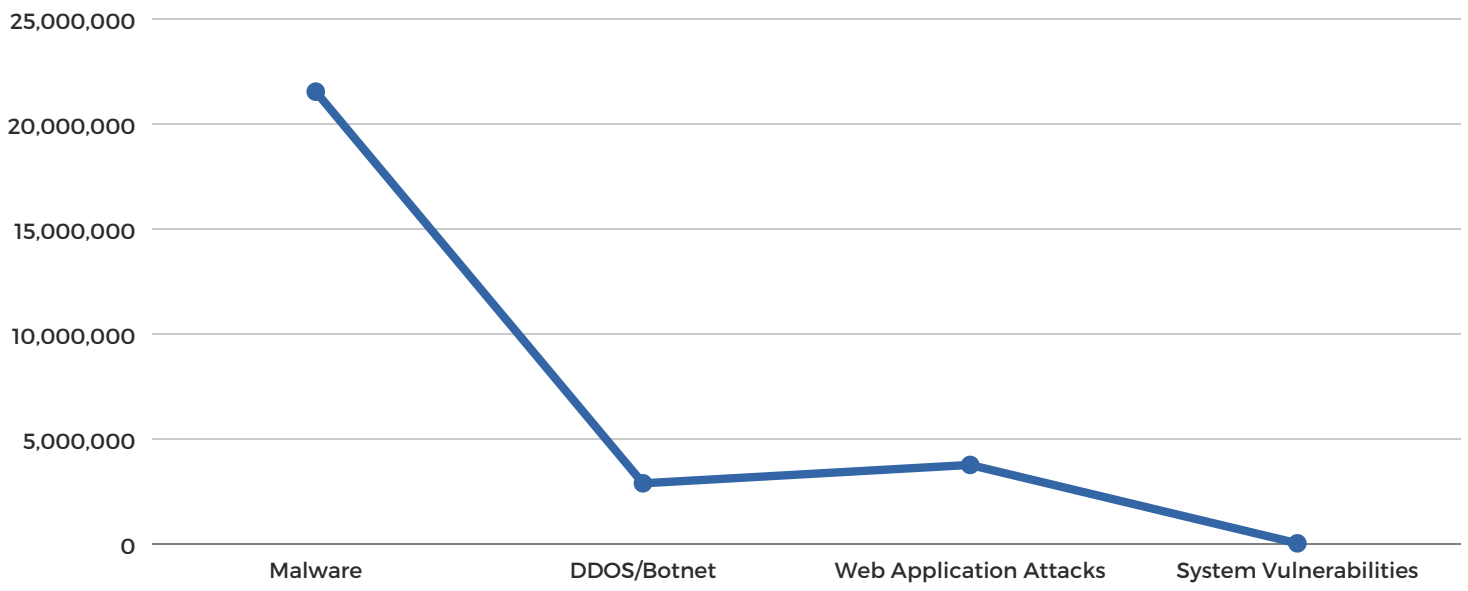
During the period January to March 2021, the National KE-CIRT/CC detected **28,247,819** cyber threat attempt events as compared to the **56,206,097** detected in the previous period October to December 2020.

28,247,819

Total Cyber threat attack attempts during the period

49.74%

% Decrease from the last period



The National KE-CIRT/CC continued to spearhead the protection of the Kenyan cyber space against various emerging and persistent cyber threats such as system vulnerabilities, malware, phishing, web application attacks and Botnet/Distributed Denial of Service (DDoS) attacks through 24/7 monitoring, analysis and response.

During the third period January to March 2021, the National KE-CIRT/CC detected 28,247,819 cyber threat events, which was a 49.74% decrease from the previous period October to December 2020, where 56,206,097 cyber threat events were detected.

The decline in cyber threat events detected during this period is attributed to a metamorphosis in the type and manner of attacks by cyber threat actors, which were optimized to circumvent current cyber threat detection systems. Cyber threat actors are increasingly developing and adopting sophisticated tools and methods that are designed to avoid detection while maximizing harm. In recognition of this trend, the National KE-CIRT/CC is upgrading its detection systems.

In response to the detected cyber threat event attempts, the National KE-CIRT/CC issued 25,506 advisories. This was an 18.56% increase compared to the 21,513 advisories that were issued during the period of October - December 2020.

CYBER THREAT STATISTICS

21,559,181

The number of malware threat event attempts detected during the period

2,890,847

The number of DDOS/Botnet threat event attempts detected during the period

3,767,588

The number of Web Application attacks threat events detected during the period

30,203

The number of System Misconfiguration threat event attempts detected during the period

CYBER THREAT ADVISORIES

25,506

In response to the 28,247,819 cyber threat attempts detected locally during the period January to March 2021, the National KE-CIRT/CC issued 25,506 advisories to the affected organizations.
This was a 18.56% increase from the 21,513 advisories issued during the previous period October - December 2020.
The advisories provide timely information on emerging and current cyber threats thereby enhancing the cyber readiness of critical organizations in Kenya.

SYSTEM VULNERABILITIES

30,203

JAN - MAR '21

Number of system vulnerabilities detected in the period January to March 2021

29,079

OCT - DEC '20

Number of system vulnerabilities detected in the previous period October to December 2020

INSIGHTS

System vulnerabilities are weaknesses exploitable by threat actors who use these weaknesses to cross privilege boundaries within a computer system. Cyber threat actors exploit system vulnerabilities to breach systems, manipulate data or take control of computers for malicious purposes.

During this period, targeted attacks at the Hypertext Transfer Protocol Secure (HTTPS) interface of the vCenter plugin exposed VMware vCenter servers, which are used to manage virtual machines, thereby allowing cyber threat actors to take over unpatched devices and organizations' entire networks. This system vulnerability allowed cyber threat actors to elevate access privileges on the victim devices without having to authenticate by executing malicious code. To counter this, organizations running the vCenter software are advised to apply the rolled out software patch.

The use of zero-day vulnerabilities to attack on-premise versions of Microsoft Exchange Server by state-sponsored groups was also a notable trend during this period. Threat actors used these vulnerabilities to access email accounts and install malware to facilitate long-term access to the victim's environments.

Vulnerabilities in data file transfer services affecting the healthcare sector, finance sector, telecommunications and government organizations, enabled attackers to breach organization systems and exploit existing unpatched zero-day flaws. These vulnerabilities were as a result of ransomware attacks by Clop ransomware actors. To address this, organizations using file transfer applications are advised to temporarily isolate or block Internet access to and from systems hosting the software, and regularly review the system for suspicious activity.

The National KE-CIRT/CC also noted a significant increase in supply-chain attacks during this period. These attacks were carried out through compromise of information resources used for the circulation of documents, by distributing documents embedded with macros. When opened, these documents downloaded malicious code to control the compromised systems remotely and further carry out Distributed Denial of Service (DDoS) attacks.

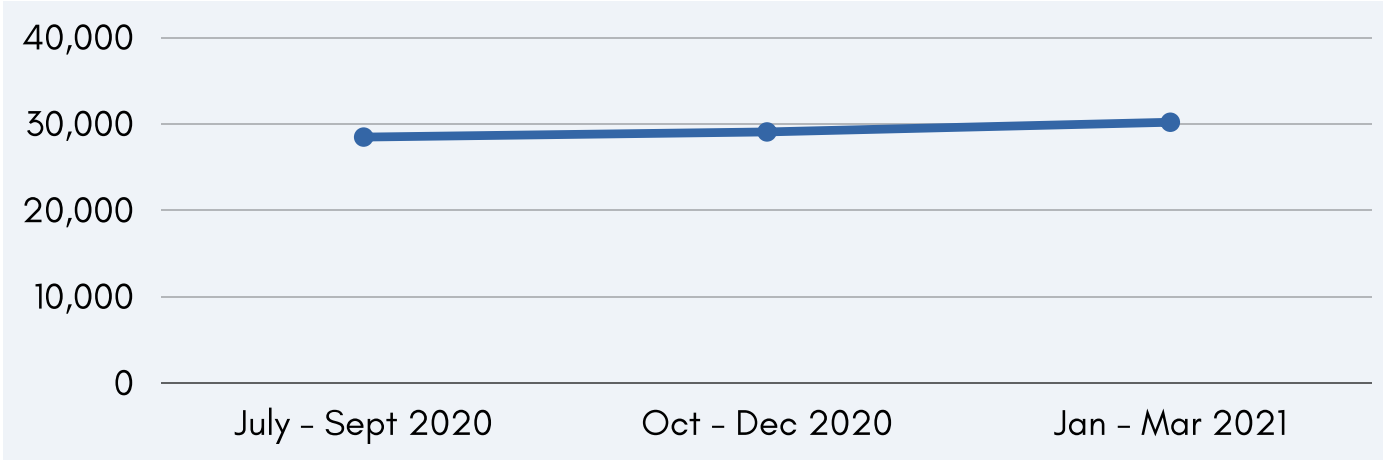
A notable trend during this period was an increase in third party vendor vulnerabilities. This involves cyber threat actors targeting software providers who serve as vendors for organizations (both public and private), allowing the attackers to compromise software that is installed on the systems running the tools offered by the vendors. As such, any system that comes into contact with the affected software is compromised thereby creating a domino effect. These attacks involved the cyber threat actors embedding hack code into the software updates being offered by the third party vendors to client organizations, thereby providing a backdoor to end-user's systems. This enabled them to install malware that was used to spy on organizations, allow unauthenticated user access to critical systems, enable remote code execution with high privileges, enable remote control of systems, as well as access to passwords for the backend databases from where they exfiltrated data and created new accounts with administrator rights to propagate further attacks. The National KE-CIRT/CC issued advisories to affected organizations as well as Cybersecurity Best Practice Guides on addressing this vulnerability

WHAT CAN WE DO?

If you suspect a system misconfiguration attack, isolate or block Internet access to and from systems that are hosting data file transfer services, and review the system for any evidence of malicious activities.

Apply rolled out software patches to protect your organization against system vulnerabilities in the VMware vCenter plugin.

Patch and upgrade your systems and devices to protect your organization against system vulnerabilities in third-party managed platforms.



21,559,181

JAN - MAR '21

Number of malware threat attempts detected in the period January to March 2021

46,069,525

OCT - DEC '20

Number of malware threat attempts detected in the previous period October to December 2020

INSIGHTS

Malware refers to any malicious code or program such as viruses, bugs, worms, bots, rootkits, spyware, adware, Trojans, and even ransomware that gives a cyber threat actor explicit control over your system.
During the period there was an increase in malicious third-party browser add-ons that were configured to steal mail and browser data and download malware on the infected systems. Cyber threat actors leveraged on the ScanBox malware in this attack to track visitors to specific websites, perform keylogging and collect user data to leverage in future intrusion attempts.

There was a sharp increase in malware strains programmed in Go language during the period. This was as a result of E-crime malware developers taking up this programming language due to the fact that Go-based binaries are hard to analyze and reverse engineer. As a result Go-based malware are hard to detect. Go-based malware families propagated botnets targeting Linux and Internet of Things (IoT) devices to install crypto miners and enroll the infected machine into DDoS botnets.

An increase in the use of cloud applications to support remote information system infrastructure with the continued shift to remote work and adoption of digital services, resulted in a considerable increase in malware being delivered via cloud applications. In addition, cyber threat actors continued to evade legacy security defenses thereby exposing enterprise data to increased risks such as web and cloud-enabled threats as well as unauthorized cloud data migrations and file transfers.

Notable malware trends during this period included Emotet, Trickbot and Phorpiex malware families spreading phishing spam emails containing malicious attachments and links, which fueled large-scale Sextortion campaigns. Hiddad, an Android malware that repackages legitimate apps and then releases them to third-party stores, was noted enabling unauthorized access to critical security details built into the Android Operating System (OS). xHelper, which leverages its capability to hide itself from users and reinstall itself in case it was uninstalled, was also used to stealthily download malicious applications. Further, mobile crime perpetrators used Triada, a modular backdoor for Android that grants superuser privileges, to download malware.

RANSOMWARE

Ransomware is an advanced sub-type of malware that enables cyber threat actors to gain control of a system and limit users' access to files unless a ransom is paid.

Ransomware-as-a-Service (RaaS) is a growing concern globally, with the monetary value of the average ransom significantly increasing and ransomware remaining as the top tool for cyber crime. The RaaS model is gaining popularity amongst crime gangs, who are supporting the development of ransomware variants for purposes of carrying out ransomware attacks. This model allows cyber threat actors to sponsor the development of tools to execute ransomware attacks, with the ransomware developers earning a commission on successful ransom payments. This has led to the development of sophisticated ransomware variants that use anti-forensic techniques to cover their footprint making them difficult to detect.

The systematic return to on-premise information systems amidst efforts of returning to post-COVID normalcy, has resulted in a notable increase in ransomware attacks targeted at schools, the healthcare sector and enterprises. This comes as organizations grapple with the after effects of the pandemic, such as job cuts that affected information system personnel, and budget cuts that affect the maintenance and update of critical information systems security.

WHAT CAN WE DO?

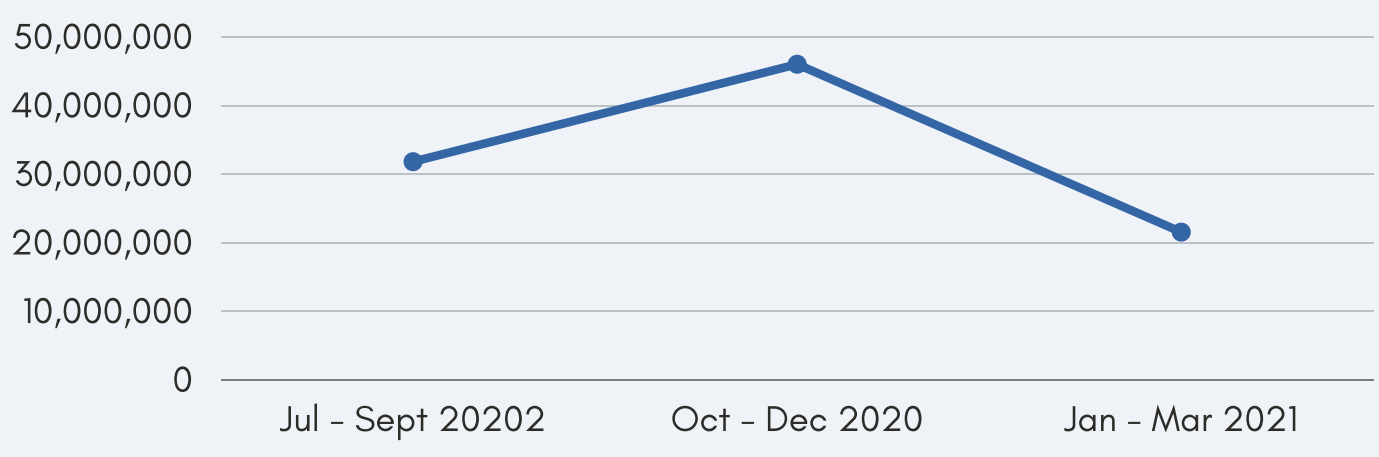
Install anti-malware software to protect your organization against malicious third-party browser add-ons and mobile malware.

Use anti-malware software to scan email attachments before downloading them.

Do not trust pop-up windows that ask you to download software.

Perform due diligence before opening email links.

Download third-party browser add-ons and applications from trusted stores.



WEB APPLICATION ATTACKS

3,767,588

JAN - MAR '21

Number of malware threat attempts detected in the period January to March 2021

7,847,457

OCT - DEC '20

Number of web application attack attempts detected in the period October to January 2020.

INSIGHTS

Web Application attacks are executed by exploiting web application vulnerabilities, such as misconfiguration in website application code. These allow cyber threat actors to gain control of the website, including the hosting server, for purposes of gaining access to databases in order to compromise data and services, spread spam email, launch attacks against other servers running critical services, and launch phishing attacks.

Cyber threat actors continued to target public-facing web applications and externally accessible servers by taking advantage of existing code and configuration vulnerabilities. These allowed them to compromise servers running a host of services, including synchronization, backup, and other applications, thereby exposing organization resources. Also notable during this period was the use of Search Engine Optimization (SEO) techniques to compromise websites. Cyber threat actors used carefully crafted message boards that redirected users to malicious links containing malware variants.

There was also increased adoption of bots and automation tools to propagate automated attacks on web applications through Distributed Denial of Service (DDoS) attacks, which overwhelmed organizations web application services. In response to this trend, the National KE-CIRT/CC issued advisories to organizations recommending the application of Web Application Firewalls (WAF)-as-a-Service or Web Application & API Protection (WAAP) solutions that include bot mitigation, DDoS protection, Application Programing Interface (API) security, and credential stuffing protection. In addition, the National KE-CIRT/CC also recommends that organizations ensure proper configuration of web application services.

WHAT CAN WE DO?

Use an automated configuration-monitoring tool to regularly verify the effectiveness of your web application settings and configurations.

Further, purge unused features and frameworks in your web applications to prevent web application vulnerabilities.

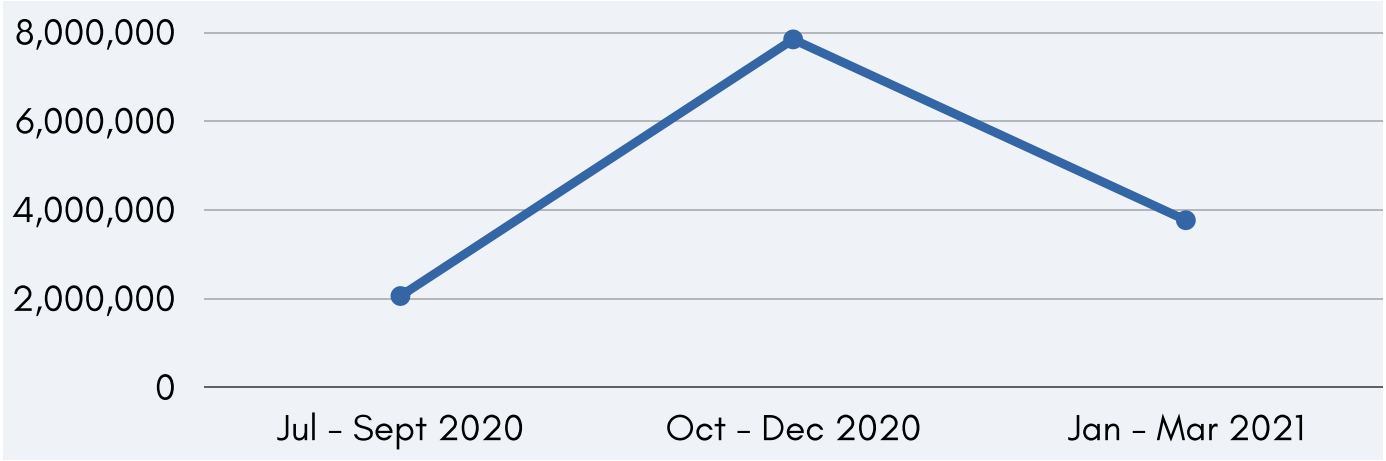
Define permissions for approved third-party vendors that access your website data or block them from receiving specific types of data.

Block formjacking and payment card skimming by enabling control over third-party JavaScript, which is permitted to operate within the user's browser.

Use encrypted Hypertext Transfer Protocol Secure (HTTPS) connections to transfer data and information.

Perform all remote tasks through secured channels such as Virtual Private Networks (VPNs) to minimize web application vulnerabilities.

Regularly conduct file integrity checks to prevent unauthorized changes to critical files through file integrity checking tools.



PHISHING AND SPAM

3

JAN - MAR '21

Number of phishing threat attempts detected in the period January to March 2021

1

OCT - JAN '21

Number of phishing threat attempts detected in the period October to December 2020

INSIGHTS

Phishing is the fraudulent attempt to obtain sensitive data such as passwords or credit card details by posing as a trustworthy party. On the other hand, spam is the sharing of messages with the intention of broadcasting unwanted or malicious content. Spam can be used to spread phishing campaigns. Phishing and spam campaigns are often used by cyber threat actors to distribute malware, ransomware, spyware and other cyber attacks.

As Small, Medium and Micro Enterprises (SMMEs) moved to cloud-based services in response to restrictions brought on by the pandemic, cyber threat actors increased attacks targeted at cloud services. These attacks included spear phishing, ransomware, smishing and supply chain attacks. Cyber threat actors leveraged on cybersecurity challenges faced by SMMEs, such as lack of technical resources, poor information system security policies, and inadequate cyber defense and incident response. To address this, the National KE-CIRT/CC continues to support SMMEs through Cybersecurity Best Practice Guides addressing cyber threats targeting them.

There was a notable increase in vishing scams, where threat actors lure victims into giving up personal information and financial details such as account numbers and passwords over the phone. These stolen credentials enable the scammers to access victim financial accounts including mobile wallets.

Cyber threat actors continued to propagate COVID-19 themed phishing campaigns embedded with malware, viruses, spyware, ransomware and a host of other cyber attack vectors. Phishing campaigns luring victims with promises of financial bonuses were also used to distribute new variants of the Bazar Trojan. The Bazar Trojan provides cyber threat actors with a backdoor into compromised Windows systems. This allows cyber threat actors to control devices and gain access to networks for purposes of collecting sensitive information and delivering malware, including ransomware. Holiday sale scams related campaigns, such as the valentine's day-themed phishing campaigns, are also increasingly being used to steal credentials to perform account takeovers and spread malware. To counter these trends, the National KE-CIRT/CC continues to carry out public awareness through Cybersecurity Best Practice Guides that are published on our social media platforms and website.

WHAT CAN WE DO?

Isolate critical components and services in your network to limit the impact of breaches from successful credential harvesting in phishing attacks.

In addition, implement a centralized network protection solution that filters potentially malicious sites and prevents users from accessing them.

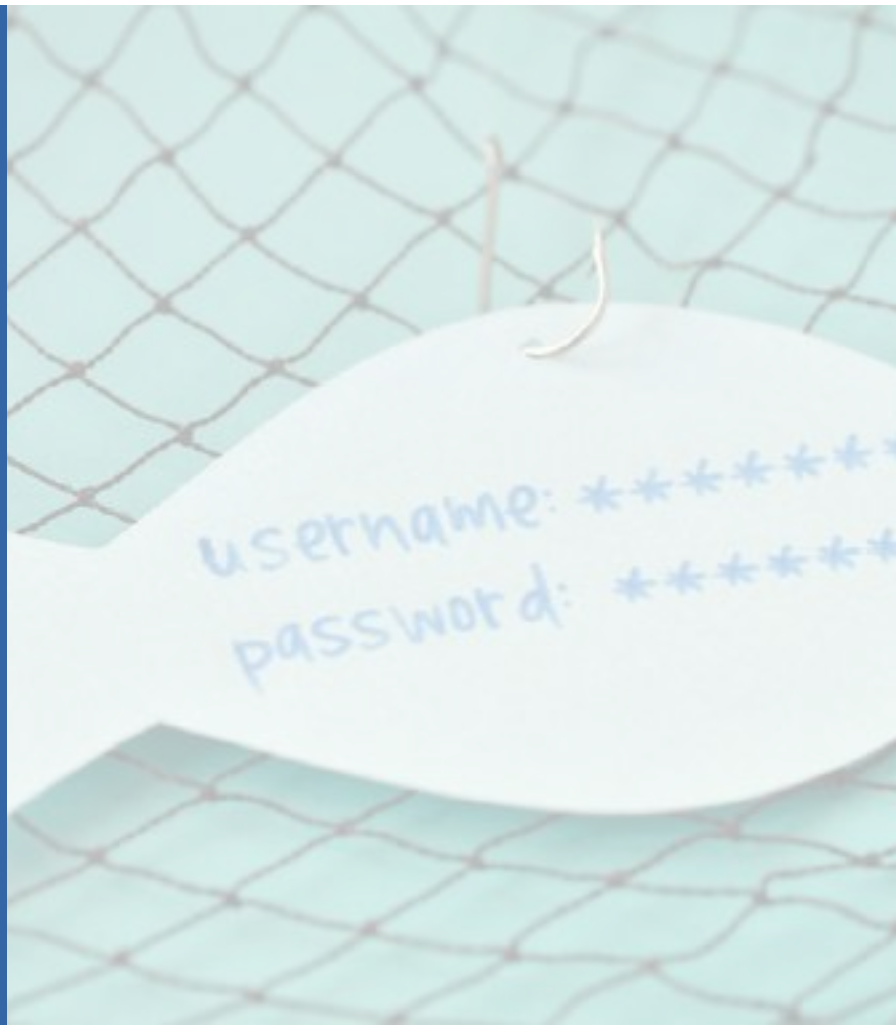
Update your devices, anti-virus, firewalls, and software regularly to avoid falling victim to targeted phishing attacks that rely on outdated software.

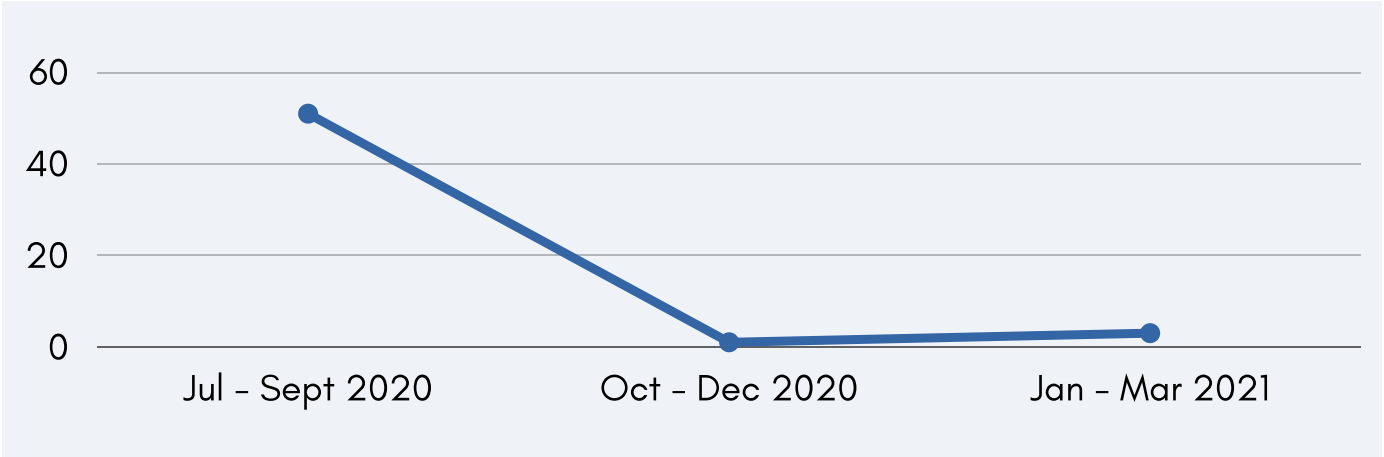
Enforce good password policies to ensure that similar passwords cannot be used to grant cyber threat actors access to other systems or accounts on successful phishing attacks.

Do not share Personal Identifiable Information (PII) over the phone.

Always verify phone requests before acting on them.

Avoid clicking on unverified links in emails, social media posts, and messages.





BOTNET/DDOS

2,890,847

JAN - MAR '21

Number of Botnet/DDOs threat attempts detected in the period January to March 2021

2,260,036

OCT - DEC '20

Number of Botnet/DDOs threat attempts detected in the previous period October to December 2021

INSIGHTS

Distributed Denial of Service (DDoS) attack, is the 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. On the other hand, a botnet is a group of Internet connected devices running automated tasks over the Internet. Botnets can be used to perform DDoS attacks.

Matryosh botnet and malware developers continued to target Android devices through the Android Debug Bridge (ADB) interface, allowing the malware developers to communicate with devices directly. This enabled them to execute commands on targeted devices and take control of them remotely, for purposes of carrying out DDoS attacks. In response to this, the National KE-CIRT/CC issued advisories recommending that administrators block the use of ADB on corporately managed devices, and install mobile threat defense software on these devices.

DDoS threat groups amplified DDoS attacks through the abuse of vulnerable Virtual Private Network (VPN) infrastructure, which exposed data transmission ports thereby leaking user data. To address this, the National KE-CIRT/CC issued advisories recommending that users perform patch management for VPN software and implement secure VPN configurations.

WHAT CAN WE DO?

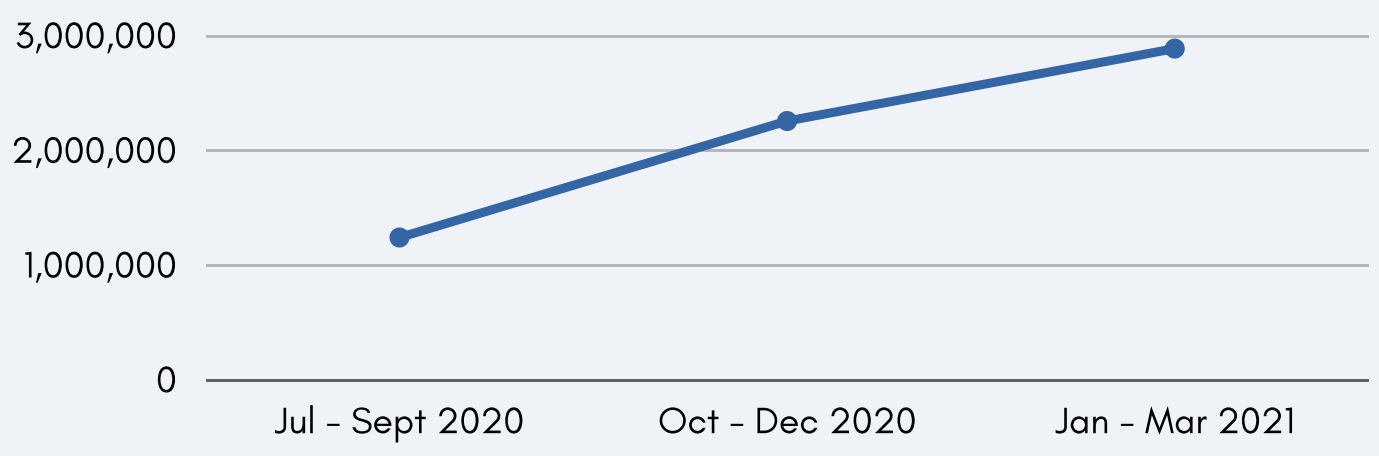
Implement an advanced bot-detection solution to protect your website and web server from botnet attacks.

In addition, in order to prevent account takeover (ATO), regularly monitor unusual failed login attempts, which are usually a sign of a botnet attack.

Implement secure Virtual Private Network (VPN) configurations to mask your Internet Protocol (IP) address and prevent cyber threat actors from targeting your network.

Update your software and Operating System (OS) regularly to prevent malware infection by botnets and the enrollment of infected devices into DDoS botnets.

Implement a Zero Trust Security Model to protect against DDoS attacks. This ensures that only authorized users gain access to critical applications and services.



DIGITAL INVESTIGATIONS

298

JAN - MAR '21

Number of digital investigations facilitation requests handled by the National KE-CIRT/CC during the period January to March 2021

224

OCT - DEC '20

Number of digital investigations facilitation requests handled by the National KE-CIRT/CC during the previous period October to December 2020

INSIGHTS

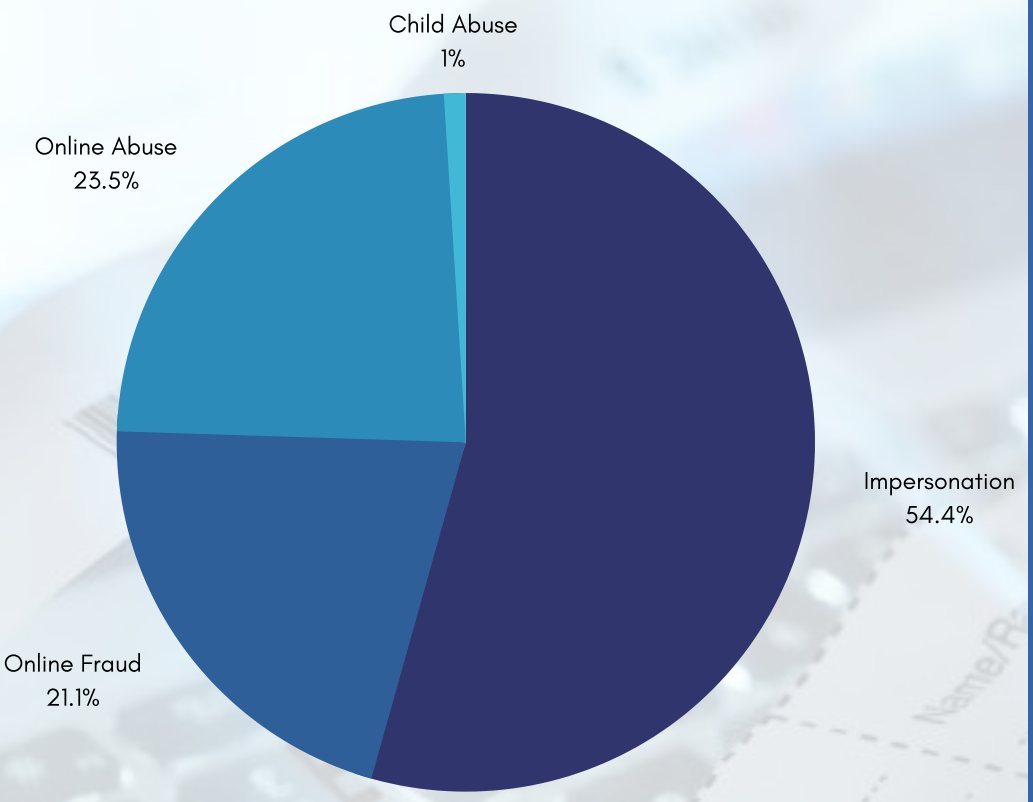
The accelerated uptake of digital devices as part of digital transformation has enhanced communications, learning, socialization, and ease of access to services. However, this has proven to be a double-edged sword, as cyber threat actors use these sophisticated digital devices for criminal purposes. Digital evidence can be found on a computer hard drive, a mobile phone, a tablet, among others. From identity theft, cyber bullying, data leakage, DDoS attacks, malware attacks, fake news and cyber propaganda, to online fraud, cyber attacks are propagated through digital devices. In addition, digital devices can sometimes hold evidence that can be used in the prosecution of other crimes.

Further, incident response approaches usually focus on the containment of the incident for purposes of minimizing harm and launching a swift response and recovery. As such, these are not normally concerned with the preservation and/or collection of data for purposes of investigations and prosecution. As a result, vital evidence is often lost, which would otherwise have aided investigations and possible successful prosecution of the cyber criminals behind the attack.

In handling digital evidence, digital examiners must be conscious of the volatility and fragility of digital evidence. They must ensure that the access, collection, packaging, transfer, and storage of digital evidence follows protocols that maintain the integrity and admissibility of digital evidence in court.

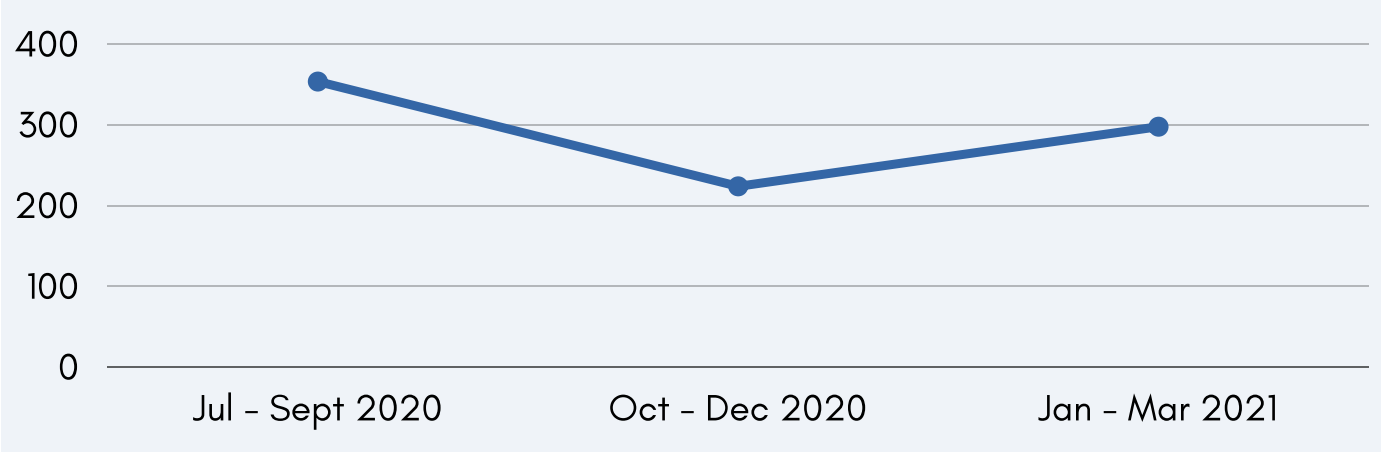
WHAT CAN WE DO?

Carry our consumer education and awareness on the various types of cyber crime, the current regulatory provisions addressing this, as well as on cyber crime reporting mechanisms.



Carry out regular cyber education and cyber awareness of end users as a first line of defense against cyber crimes.

Empower consumers on their rights and responsibilities online, and on how to report cyber crime.



DIGITAL FORENSICS

16

JAN - MAR '21

Number of digital forensics facilitation handled by the National KE-CIRT/CC during the period January to March 2021

58

OCT - DEC '20

Number of digital forensics facilitation handled by the National KE-CIRT/CC during the period October to December 2020

INSIGHTS

Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence, majorly in order to present this evidence in a court of law.

Cybersecurity and digital forensics work hand in hand, with digital forensics handling the investigation, analysis, and recovery of digital assets affected by a cyber incident, while digital forensics can be used to support an organization's defense and offense after a cyber incident.

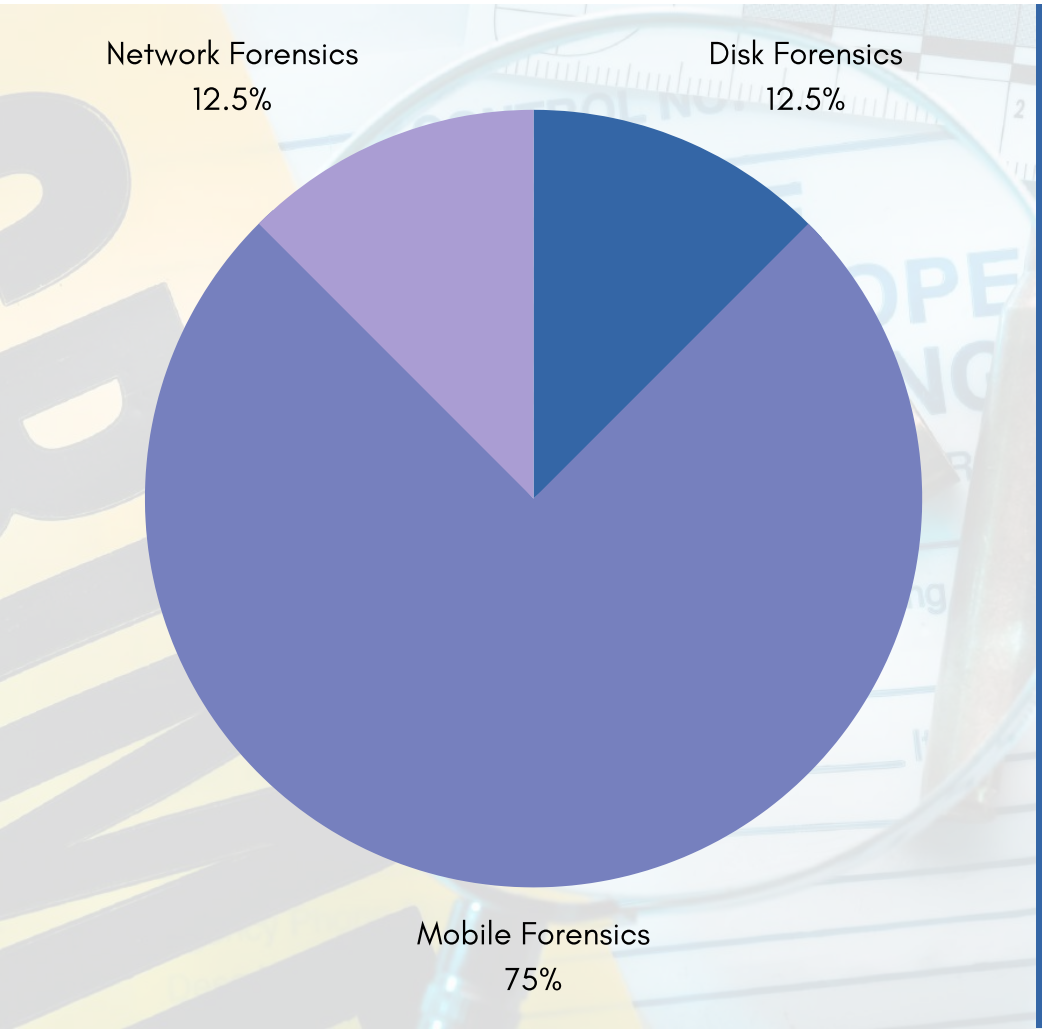
Incident response approaches involving digital forensics allow active monitoring of the cybersecurity incident using digital forensic applications. These allow investigators to gather evidence of and information about the incident for purposes of investigations and prosecution of cyber crimes.

There are significant challenges affecting digital forensics locally. These include the continued increase in the volume of digital evidence, the rise in the use of full disk/memory encryption software, the increasing use of anti-forensic techniques, as well as emerging technologies that cause digital evidence to become increasingly evanescent.

In addition, challenges such as availability of trained and experienced digital examiners, concerns relating to the acquisition, storage, and processing of large amounts of data for forensic purposes, as well as high costs of digital forensic tools, continue to affect the exercise of digital forensics and the successful prosecution of cyber crime in Kenya.

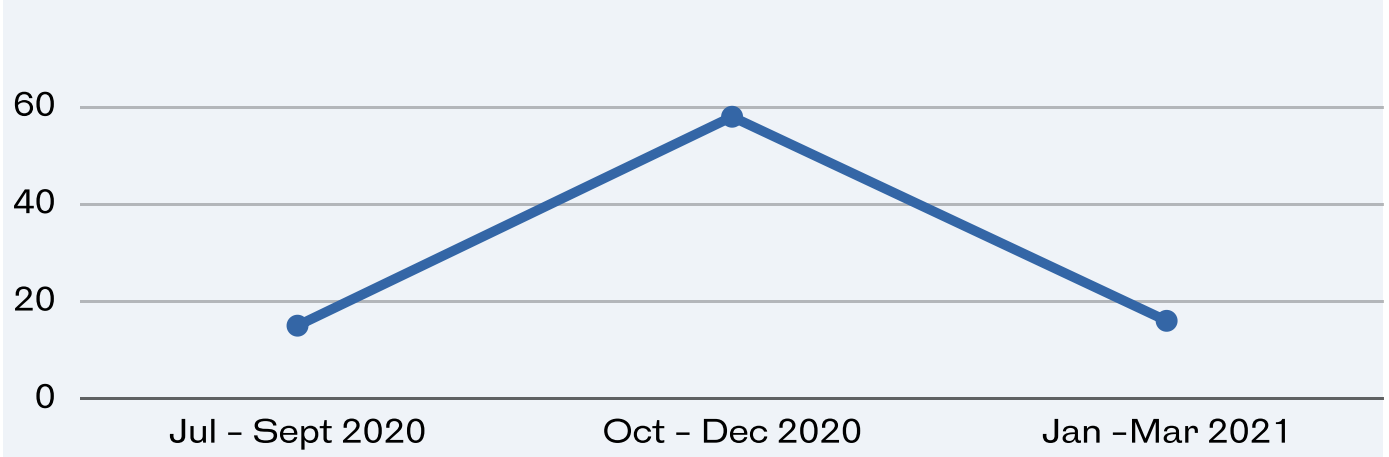
WHAT CAN WE DO?

Invest in capacity building of digital forensics examiners to address the increasing requests for digital forensics.



Rapid changes in the quantity and complexity of cyber attacks requires increased investment in digital forensics equipment.

There is also need to regularly retrain digital forensics examiners on emerging trends in cyber threat distribution and execution, in order to address these rising trends.



COLLABORATION & INFORMATION SHARING

As Kenya makes strides towards becoming a digitally transformed nation, more of her critical infrastructure operates in the digital environment. This digital adoption has widened the attack surface for cyber threat actors. Indeed, as the number and complexity of cyber threats targeting critical infrastructure increases, the potential disruption and impact of these threats is an issue of national concern. From disruption of essential services, loss of trust, to negatively impacting the socio-economic development of communities, the protection of critical infrastructure is a growing concern.

This comes as critical infrastructure increasingly becomes the preferred target for cyber crime and cyber warfare in the digital ecosystem. The National KE-CIRT/CC noted an increase in attacks targeted at critical infrastructure from various cyber threat actors such as organized criminals, terrorists and even nation state actors. These groups used sophisticated tools to launch attacks that breached critical systems, exfiltrated user information, extracted intellectual property and maintained persistent access to networks for purposes of carrying out future offensive operations.

As such, critical infrastructure cybersecurity is a shared responsibility among multiple stakeholders in both the public and private sector. It requires layered vigilance, readiness and resilience strategies, as well as timely and trusted information sharing among stakeholders. In recognition of this, the National KE-CIRT/CC works closely with various local and international stakeholders.

Globally, the National KE-CIRT/CC leverages on partnerships with various other 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. Locally the National KE-CIRT/CC Cybersecurity Committee (NKCC), continues to support the National KE-CIRT/CC in addressing these cybersecurity concerns.

To further enhance its capacity to protect critical infrastructure, the National KE-CIRT/CC undertook an assessment of its Security Incident Management Maturity in line with the forty-four parameters of the Security Incident Management Maturity Model (SIM3), as part of the certification process. In addition, the National KE-CIRT/CC developed a Cybersecurity Readiness Measurement Tool that will be used to assess the level of cyber readiness and resilience among critical infrastructure in the country. The tool will be used to identify key areas of intervention and support, towards enhancing the national cyber readiness and resilience.

MRS MERCY WANJAU, MBS
AG DIRECTOR GENERAL
COMMUNICATIONS AUTHORITY OF KENYA

CYBERSECURITY PREDICTIONS

Kenya's Digital Economy Blueprint recognizes cybersecurity as a key enabler of Kenya's digital transformation. Against the background of the COVID-19 pandemic, Kenya has experienced accelerated digital adoption that has transformed work and life realities for Kenyans. From working remotely, online learning, to increased adoption of e-government and e-commerce, Kenya's digital transformation is here with us.

As Kenya seeks to optimise these gains for socio-economic development, she will have to contend with a dynamic and rapidly evolving cyber threat landscape. Indeed, with the rollout of the COVID-19 vaccine, and the full return to normalcy, global reports indicate that there will be an uptick in ransomware attacks targeted at on-premise information system infrastructure. Further, predictions indicate an increase in attacks on remote infrastructure, an increase in attacks targeting smart devices, an increase in malware, fake news, cyber propaganda, online fraud, as well as increased attacks targeting critical infrastructure. Amidst this, Kenya's cyber resilience will be put to the test.

This comes against the backdrop of poor adoption of cybersecurity policies by organizations, dwindling cybersecurity budgets, reduced investment in robust information systems infrastructure, inadequate capacity building of information security personnel, as well as low levels of cyber hygiene and cyber awareness amongst the general populace.

To mitigate against these, it is important that Kenya prioritizes cyber awareness and cyber education as part of the key strategies towards enhancing national cyber readiness. Further, closer collaboration and cyber threat information sharing amongst stakeholders is an important first line of defence. To complement these, there is need for enhanced support towards the implementation of deterrence measures such as the operationalization of the Computer Misuse and Cyber Crimes Act (CMCA), 2018.

HEAD OF THE NATIONAL KE-CIRT/CC
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

www.ke-cirt.go.ke