COMMUNICATIONS AUTHORITY OF KENYA

NATIONAL KE-CIRT/CC

CYBERSECURITY REPORT

APRIL TO JUNE 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

Digital transformation means that technology is increasingly playing a critical role across sectors. While this has enhanced service delivery and fast tracked innovation, this has also widened our attack surface, and gained the attention of cyber threat actors. Indeed, the top-three cybersecurity threats faced in the region during the reporting period were ransomware, malware, and phishing.

This comes as malicious cyber threat actors take various forms such as insiders, hacktivists, organized cyber criminals, cyber terrorists, and even state sponsored threat agents. Driven by different motivations, these threat actors are increasingly adopting complex and innovative ways of exploiting unsecured segments of different critical systems. These include using fileless attacks targeting various national critical infrastructure, spear-phishing campaigns to compromise systems using downloadable malware attached to emails, or the use of double-extortion tactics by ransomware gangs to steal encrypted files and encrypt networks.

As a result, we are increasingly faced with data breaches and theft of proprietary information, financial loss, reputation loss, destruction of equipment, distributed denial of services through targeted DDoS attacks, unauthorised access to critical systems and theft of Personally Identifiable Information (PII).

"When it comes to enhancing the national cybersecurity readiness and resilience ... we must go far, quickly"

Indeed, in order to enhance cyber incidents reporting, the Authority developed a cybersecurity incident reporting mobile application, which is available on both android and iOS mobile application stores. The application allows easier reporting of cyber crimes, with users also having the option of being able to report cyber crime anonymously.

In addition, the Authority, through the National KE-CIRT/CC continues to support national cybersecurity management efforts through 24/7 cyber threat monitoring, detection and analysis. Further, we continue to support individuals and organizations through daily cybersecurity advisories, cyber awareness and capacity building of cybersecurity personnel manning critical systems. Through the Digital Forensics Laboratory (DFL) that is part of the National KE-CIRT/CC, the Authority supports the investigation and prosecution of cyber crime in collaboration with law enforcement agencies.

When it comes to enhancing the national cybersecurity readiness and resilience, I find the words of Al Gore poignant. He expanded the scope of the saying that goes "If you want to go fast, go alone, but if you want to go far, go together" by adding that "...we have to go far, quickly, and that means we have to quickly find a way to change the world's consciousness about exactly what we are facing and how we have to work to solve it."

Noting the potential devastating impact that cyber threats pose to our digital transformation journey, it is critical that we scale up our collective cybersecurity posture from the individual, organizational and ultimately, national level. We have to simply, "go far, quickly".

MRS. MERCY WANJAU, MBS
AG. DIRECTOR GENERAL

Trends during the period April-June 2021

OVERVIEW OF THE CYBER THREAT LANDSCAPE

COVID-19 continues to accelerate the adoption of technology trends such as online shopping, digital payments, remote work, tele-health, online learning, amongst others. Subsequently, cyber threat actors are evolving and leveraging these trends to launch increasingly complex and organized cyber attack techniques that are harder to detect and prevent.

These attacks take advantage of vulnerabilities resulting from inadequate cyber defences in systems supporting remote working, such as out-of-date Virtual Private Networks (VPNs) and vulnerabilities in remote working tools, to maintain persistent unauthorised access to systems, exfiltrate data and encrypt data for ransom.

Cyber threat actors are also increasingly evolving and adapting new techniques, such as Double Extortion Ransomware, which seeks to optimize ransom payment by first exfiltrating data before encrypting a network, which means that the data can be leaked online or sold to the highest bidder if the victim refuses to pay the ransom. This forces victims to pay the ransom.

In addition, various cyber threat actors, such as hacktivists, state-sponsored groups, organized cyber criminals and cyber terrorists, are increasingly targeting healthcare systems, utility providers, public infrastructure, insurance firms, schools, government organizations, and financial institutions through ransomware, malware and Distributed Denial of Service (DDoS) attacks. These attacks are targeted at crippling critical infrastructure systems, destroying equipment, disrupting services, and exfiltrating sensitive data such as emails, passwords, financial information, intellectual property, among others.

To address these emerging concerns, the National KE-CIRT/CC continued to issue Technical Cybersecurity Advisories to organizations and Cybersecurity Best Practice Guides to the public, which provided detailed insights to assist in cyber threat prevention and detection. These included 26,536 advisories and 26 best practice guides which were shared through various platforms during the period April-June 2021.

CYBER THREAT STATISTICS

26,536

Total number of cyber advisories issued by the National KE-CIRT/CC

38,776,699

Total number of cyber threats detected by the National KE-CIRT/CC during the period Apr-Jun 2021

During the period April - June 2021, the National KE-CIRT/CC detected **38,776,699** cyber threat events, which was a **37.27%** increase from the **28,247,819** threat events detected in the previous period, January - March 2021.

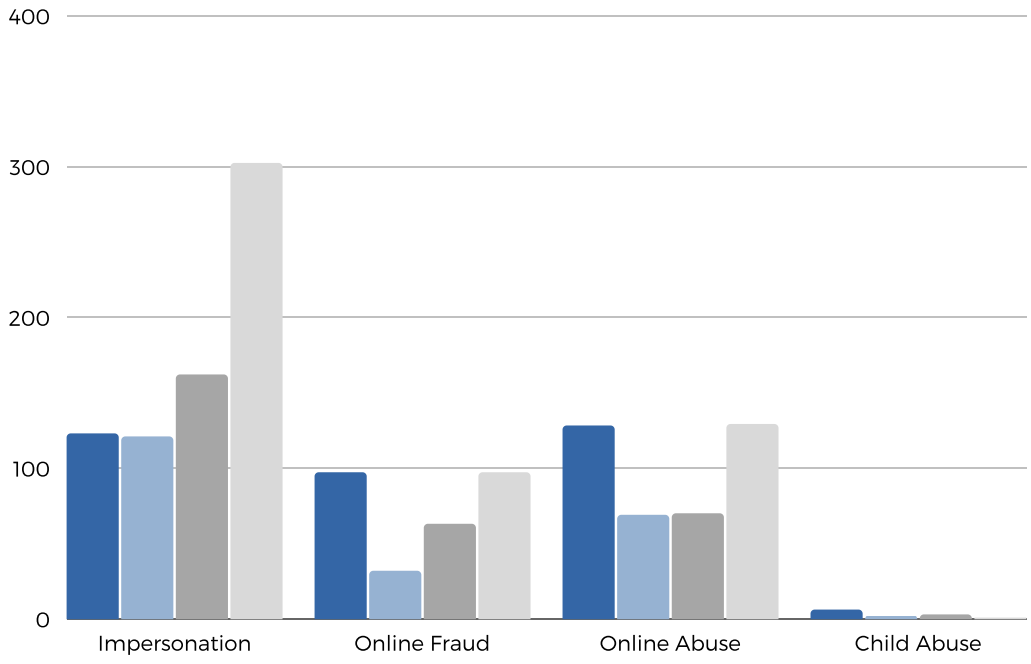
DIGITAL FORENSICS & INVESTIGATIONS

529

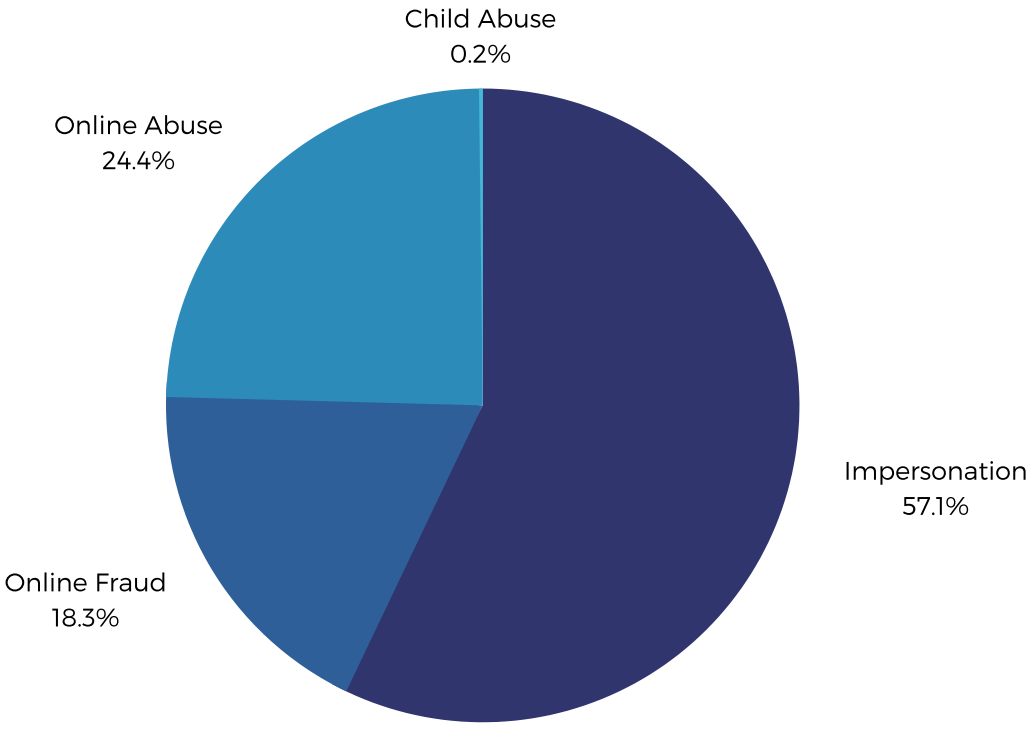
Number of digital investigations facilitated by the National KE-CIRT/CC Digital Forensics Lab

36

Number of Digital Forensics facilitated by the National KE-CIRT/CC Digital Forensics Lab



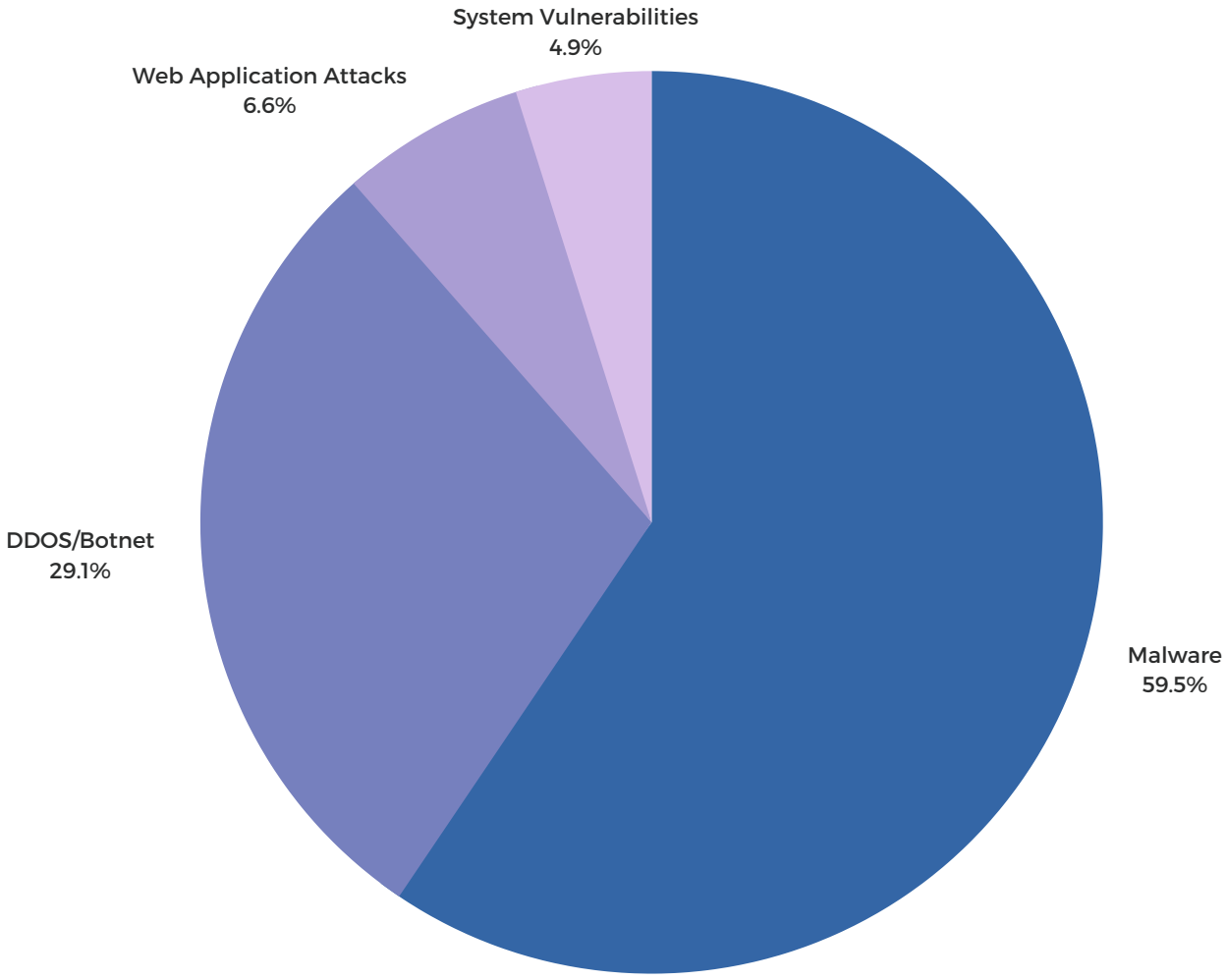
Digital investigations facilitated by the National KE-CIRT/CC during the period July 2020 to June 2021



Digital investigations facilitated by the National KE-CIRT/CC during the period April to June 2021

Apr-Jun 2021

OVERVIEW OF THE LOCAL CYBER THREAT LANDSCAPE



The National KE-CIRT/CC continued to spearhead the protection of the Kenyan cyberspace 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 monitoring, analysis and response to cyber incidents on a 24/7 basis.

During the period April - June 2021, the National KE-CIRT/CC detected 38,776,699 cyber threat events, which was a 37.27% increase from the 28,247,819 threat events detected in the previous period, January - March 2021.

This increase in cyber threat events detected is attributed to the significant increase in targeted attacks at Internet of Things (IoT) devices; increased activity by organized cybercrime groups; adoption of more sophisticated tools by ransomware gangs; increased targeted attacks at critical systems and services; increased exploits of mobile application vulnerabilities; increased targeted attacks at cloud-based supported services and unsecured infrastructure; and increased adoption of botnet and Distributed Denial of Service (DDoS) attack techniques.

CYBER THREAT TRENDS DURING THE FY YEAR 2021/21

A snapshot the cyber threat trends during the period July 2020 to June 2021

158,405,656

Total number of cyber threat detected by the National KE-CIRT/CC during the FY 2020/21

95,390

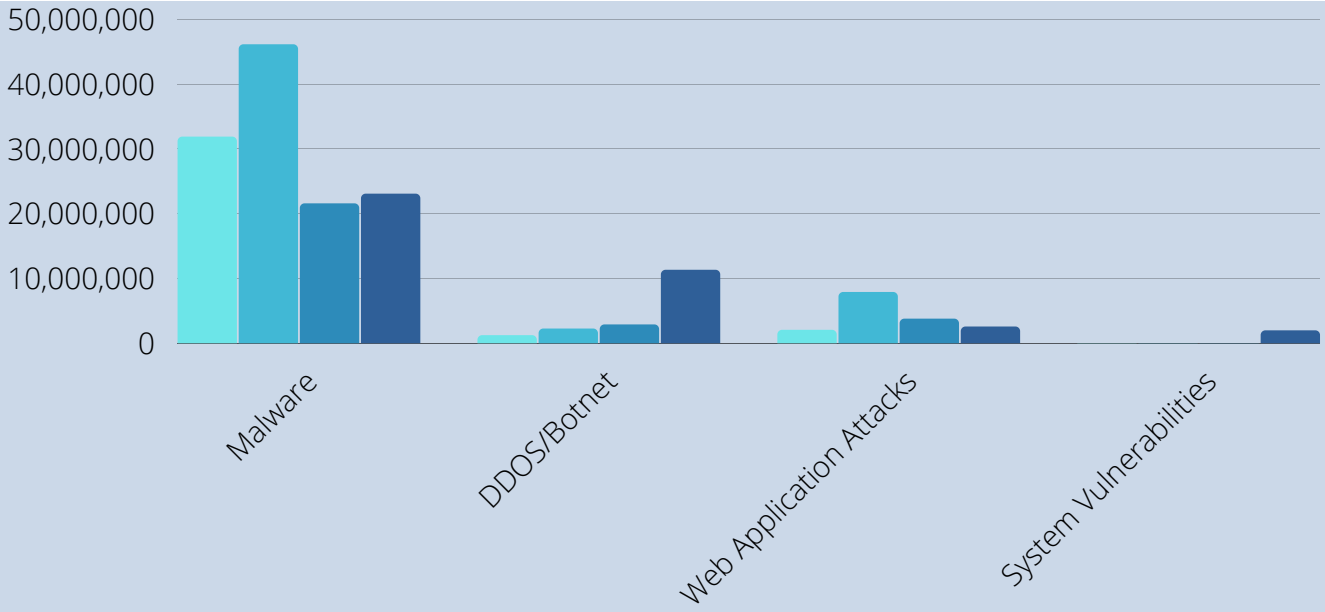
Total number of advisories issued by the National KE-CIRT/CC during the FY 2020/21

CYBER THREAT ADVISORIES

The advisories provide timely information on emerging and current cyber threats thereby enhancing the cyber readiness of critical organizations in Kenya.

CYBER THREATS ANALYSIS BY ATTACK MECHANISM

Cyber threats detected by the National KE-CIRT/CC during the period July 2020 to June 2021



TRENDS IN SYSTEM VULNERABILITIES

An overview of System Vulnerabilities trends detected by the National KE-CIRT/CC during the period July 2020 to June 2021

1,886,934

TOTAL SYSTEM VULNERABILITIES DETECTED DURING THE PERIOD APRIL - JUNE 2021

6,147.51%

INCREASE FROM THE LAST PERIOD JAN-MAR 2021

1,974,698

TOTAL DETECTED DURING THE PERIOD JULY 2020 TO JUNE 2021

MOBILE THREAT LANDSCAPE

The adoption of remote work and hybrid workforces has accelerated the dependency on mobile devices for collaborative workplaces. Mobile devices are becoming increasingly capable of integrating with networks and infrastructure that are embedded with sensors, software, and other technologies that are used to connect and exchange data with other devices and systems over the Internet. This comes as organisations embrace Bring Your Own Device (BYOD) policies to enable their employees' access corporate networks with personal devices as organisations continue to move away from on premise infrastructure to remote working.

In response to this trend, cyber threat actors are leveraging on unsecured mobile devices and compromised mobile applications to carry out sophisticated attacks on enterprise networks.

Cyber threat actors propagate these attacks by spreading Trojanized applications that disguise themselves as legitimate apps in official app stores such as popular games, phone layout themes and phone utility apps. These applications are then used to distribute malware and spyware capable of infiltrating networks, stealing data, infecting devices into botnets to carry out Distributed Denial of Service (DDoS) attacks, and carry out spam email campaigns.

Malicious software developers are able to bypass security protection in app stores by using various evasion techniques that prevent their code from being detected by antivirus software, code reviewers, or from being analysed when run in a sandbox environment. Further, cyber threat actors mimic human activity and use delayed execution tactics to hide the malware's true functionality, thereby allowing these applications to pass inspection by official app stores. To successfully effect these schemes, cyber threat actors also create fake profiles on popular application development sites such as Github, providing a layer of legitimacy for these applications.

What can we do?

- Review organizational Bring Your Own Device (BYOD) policies;
- Introduce Corporate issued devices which will separate work data from personal data;
- Adopt Device-as-a-Service (DaaS) model, which provides employees with preconfigured devices with essential security software.

CHILDREN AND THE INTERNET

The Internet is an increasingly important part of today's culture, especially for children and youth. From schoolwork, online gaming, and social networking, children and the youth are constantly engaged online. This constant online exposure comes with risks such as cyber predators, or even negative use of these platforms that could have lasting, severe, costly, and even tragic, consequences. Cyber bullying can happen at any time of the day or night, anywhere there's internet or mobile access.

One of the most prevalent and prolific challenges facing children online is cyber bullying. Cyber bullying is when a person uses digital technology to deliberately and continuously harass, humiliate, embarrass, torment, threaten, pick on or intimidate another person. Cyber bullying can take place on email, messaging, gaming & social media platforms.

Cyber bullying usually involves: posting or sending messages that threaten people or put people down; leaving people out of online games or social forums; spreading nasty rumors online about people; setting up unkind or unpleasant fake social media accounts using real photos and contact details; impersonating someone and sending mean messages to others on their behalf; trolling or stalking someone online; sharing or forwarding someone's personal information; posting insulting or embarrassing photos or videos of someone; harassing someone in virtual environments or online games; and sending hurtful messages or threats via messaging platforms.

To protect your child from cyber bullies it is important that you teach your child responsible online behavior such as the proper way to interact with people online; including the kind of language to use online, whether they are addressing a friend or a stranger. It is also important to report cyber bullying, which is recognized as criminal behavior in Kenyan law. In reporting or escalating cyber bullying to the school or to the bully's parents, please keep the mean or threatening pictures, messages or texts as evidence so that the matter can be addressed.

For more information on cyber bullying, please visit: https://cop.ke-cirt.go.ke/index.php/pillars/cyber-bullying/.

E-COMMERCE

As businesses continue to expand their presence online, the growth in e-commerce has resulted in more and more innovative products and services being launched on online platforms. Online stores are proving to be convenient channels for businesses as customers can access a wider market variety, extensively compare quality and prices, and receive prompt feedback from sellers.

This growth and increased uptake of e-commerce has resulted in a notable increase in e-skimming and credit card fraud. E-skimming, otherwise known as mega cart, occurs when cyber threat actors infect e-commerce websites with malicious codes for purposes of intercepting shoppers' credit card details when they make purchases on the affected sites.

Cyber threat actors target online payment platforms through malicious code injection which allows them to gain unauthorised access to websites for purposes of stealing critical user information such as credit card details, usernames and passwords. The malicious code captures users' information such as credit card details, username and password which is either sold or used to make fraudulent purchases.

What can we do?

- Secure e-commerce sites using Transport Layer Security (TLS) certificates which authenticate and encrypt data over the Internet;
- Implement secured firewalls;
- Apply available patches as soon as they are released;
- Implement multilevel factor authentication;
- Implement strong encryption mechanisms on e-commerce platforms.

NPKI

As we move towards digital transformation, digital transactions are our new normal. This transformation necessitates the move from physical documents to digital documents. This transition however requires that we are able to authenticate and verify digitaldocuments to avoid tampering and impersonation. Digital signatures are the solution to tampering and impersonation in digital communications, as they provide evidence of the origin, identity and status of digital communications.

A digital signature is a type of e-signature based on the (Public Key Infrastructure) PKI standards that enables users to authenticate the identity of the signing party. They entail a mathematical algorithm that is used to validate the authenticity and integrity of digital communications such as emails, credit card transactions or the validity of a digital document. In many countries, including Kenya, digital signatures are considered legally binding in the same way as traditional hand written document signatures.

A digital signature solution provider follows a specific protocol, called the PKI, where they use a mathematical algorithm to generate two long numbers - called keys. One key is a public key and the other is a private key. The Public key infrastructure(PKI) standard ensures that generated keys are made and stored securely as per international standards. This is important as more countries are accepting digital signatures as legally binding.

A private key is only known to the person it belongs to and should always be kept securely by the signer, while the public key can be shared with anyone who needs to access the digital message. When a signing party electronically signs a document, the signature is created using the signer's private key.

The mathematical algorithm acts like a cryptograph that encrypts the data, and the resulting encrypted data is the digital signature. This signature is marked with a timestamp of when the document was signed, and if the document changes after signing, the digital signature is invalidated.

The main benefit of digital signatures is security. Digital signatures ensure that a document is not altered and is genuine. Digital signatures also simplify the time consuming processes of physical documents signing, storage and exchange; thereby enabling businesses to quickly transact, sign and access documents. This greatly enhances the ease of doing business in the digital economy.

Going paperless also has a positive environmental impact, as digital signatures cut down on physical waste generated by paper, as well as the negative environmental impact of transporting paper documents. Traceability of digital signatures is also a key benefit as digital signatures create an audit trail which makes record keeping easier for organizations.

SYSTEM VULNERABILITIES

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 the period April - June 2021, the National KE-CIRT/CC detected 1,886,934 cyber threat events, which was a 6,147.51% increase from the 30,203 threat events detected in the previous period, January - March 2021. In response to the detected cyber threat attempts, the National KE-CIRT/CC issued 23,253 advisories. This was a 0.92% increase compared to the 23,039 advisories that were issued during the period of January - March 2021.

Cyber threat actors continued to target organizations through zero-day vulnerability exploits, with threat actors exploiting these flaws to propagate credential harvesting and data exfiltration attacks on public facing applications. Some of the targeted organizations during this period included government and financial sectors.

There was also an increase in attacks targeting Windows, Linux and MacOS users. These attacks compromisedvarious security tools, firewall rules, and system security settings. This enabled cyber threat actors to gain remote access and maintain persistent unauthorized access to vulnerable applications and compromised networks.

Also notable during this period was the increase in Common Vulnerabilities and Exposures (CVEs), resulting in increased targeted attacks at VMware vCenter Server management interface for VSphere environments. Cyber threat actors exploited this flaw to execute commands with elevated privileges on the operating system hosting the vCenter Server. The vulnerability was also exploited using the Necro malware for purposes of carrying out DDoS attacks, network traffic exfiltration, and crypto currency mining.

WHAT WE CAN DO

TIPS ON BEST PRACTICES

Keep systems up-to-date by implementing patch management as soon as these are released;

Implement the principle of least privilege as a means of protecting against lateral movement of cyber threat actors within systems;

- Implement updates on all versions of vCenter Server immediately;
- Disable the Virtual Storage Area Network (SAN) Health Check Plugin and ensure that the vCenter Server is not exposed to the Internet;
- Upgrade the on-premise exchange server environment to the latest version;
- Implement the Internet Information Service (IIS) Rewrite Rule to filter malicious https requests.

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 cyber threat actor explicit control over your system.

During the period April - June 2021, the National KE-CIRT/CC detected 23,053,190 cyber threat events, which was a 6.92% increase from the 21,559,181 threat events detected in the previous period, January - March 2021.In response to the detected cyber threat attempts, the National KE-CIRT/CC issued 2,215 advisories. This was a 51.40% increase compared to the 1,463 advisories that were issued during the period of January - March 2021.

The adoption of digital technology by news channels attracted the attention of cyber threat actors, with a significant surge in News Malware attacks. Cyber threat actors impersonate news channels to spread links and attachments embedded with malware, which on clicking them, would copy users' files and steal personal information.

Cyber threat actors continued to target banking and financial services using malicious software that was used to spread spam emails embedded with malicious links and attachments. These were used to infect users' systems and inject key-loggers that enabled the threat actors to steal banking credentials.

Threat actors optimised the use of modular botnets and banking Trojans to steal credentials using spoofed financial institution websites. Info stealers were also used to harvest credentials from various web browsers, collect screenshots, monitor and log keystrokes. To avoid detection, cyber threat actors increased the use of malicious applications capable of hiding from users and reinstalling themselves after being uninstalled, as well as the use of modular variants that grant them super user privileges.

WHAT WE CAN DO

TIPS ON BEST PRACTICES

Regularly update systems and devices to benefit from updated security features;

Develop contingency plans such as regularly securing your backups;

- Establish security protocols and policies to mitigate external threats;
- Implement multi-factor authentication on systems and devices for an added layer of security;
- Conduct multi-layered simulated malware drills as a way of raising awareness and training staff;
- Perform due diligence when responding to digital communication, and where possible, call the sender to confirm the requests.

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.

During the period April - June 2021, the National KE-CIRT/CC continued to monitor and analyse ransomware threat vectors occurring in the global cybersecurity landscape, towards the protection of the Kenyan cyberspace.

There was a global upsurge in ransomware trends, as cyber threat actors exploited vulnerabilities in systems to launch sophisticated ransomware attacks. These attacks were carried out by a variety of cyber threat actors such as hacktivists, state sponsored actors, organized cyber criminals as well as cyber terrorists.

The attackers exploited the vulnerabilities to access sensitive data, which they steal and encrypt; and threatened to publish on data leaks sites or sell to highest bidders, unless the victims agreed to pay the ransom, usually in crypto currencies. During this period, there was a significant increase in attacks targeted at mobile network operators, File Transfer Appliance (FTA) products, and the banking sector.

In addition, cyber threat actors also continued to evolve and adapt their ransomware attack techniques to optimize ransom payments. This included the adoption of tactics such as the Double Extortion Ransomware, where attackers first exfiltrate an organization's data before encrypting the network. This tactic forces victims to pay the ransom as there is the added threat that as the attacker already has a copy of the data, they can leak this data online or sell it to the highest bidder.

Also notable during this period was the rise in the deployment of ransomware using Virtual Machines (VM), with ransomware gangs leveraging Virtual Machines' (VMs) ability to run separately from their hosting machines while still having access to the host computer files and directories through shared folders. This method enables attackers to hide ransomware payloads and encrypt files in the host computer, thereby masking ransomware and malware attacks and avoiding detection by security solutions.

WHAT WE CAN DO

TIPS ON BEST PRACTICES

Implement intrusion detection and prevention technologies which give detailed insight into the traffic on your network and identify anomalies;

Regularly update your software and operating systems to mitigate against cyber threat actors exploiting vulnerabilities in operating systems and common applications to deploy ransomware;

- Maintain secure backups;
- Implement multi-factor authentication on your systems and devices for an added layer of security;
- Conduct multi-layered simulated ransomware drills as way of raising awareness and training staff;
- Use software inventory and restriction tools to control the installation software;
- Use enterprise versions of VM software that restrict creation of new unauthorized VMs;
- Perform due diligence when responding to digital communication, and where possible, call the sender to confirm the requests.

DDOS/BOTNET

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.

During the period April - June 2021, the National KE-CIRT/CC detected 2,564,173 cyber threat events, which was an 11.30% decrease from the 2,890,847 threat events detected in the previous period, January - March 2021. In response to the detected cyber threat attempts, the National KE-CIRT/CC issued 278 advisories. This was a 33.80% decrease compared to the 420 advisories that were issued during the period of January - March 2021.

The increased adoption of technology has resulted in more interconnected devices that are handling, sharing and storing sensitive data. Cyber threat actors are leveraging on Internet of Things (IoT) devices' ability to connect with various systems and easy-to-access features to log into unsecured user accounts. This allows the threat actors to spy on users and steal sensitive information; while targeting vulnerable groups of users, such as children, through Internet-based cameras, gaming microphones, and even smart baby monitors. Cyber threat actors are also exploiting vulnerabilities in unsecured Internet-connected servers, Android devices, and smart TV ecosystems, for purposes of infecting them with crypto mining botnets.

DDoS attacks on gaming targets were carried out through IoT nodes, with cyber crime groups targeting gamers through sophisticated attack variants run on crypto-mining campaigns. These attacks were carried out by exploiting BTC block chain transactions as a means of avoiding detection by security systems.

Also notable during this period was the rise in DDoS attacks targeting banking institutions and Government IT networks. These attacks, which resulted in high service latency and financial loss, sought to compromise critical financial services and disrupt public services that depend on Government IT services.

WHAT WE CAN DO

TIPS ON BEST PRACTICES

Create redundant network resources that prevent downtime of entire network services;

- Implement advanced intrusion prevention and threat management systems which combine firewalls, Virtual Private Networks (VPNs), anti-spam solution, content filtering, load balancing, and other layers of DDoS defense techniques.

PHISHING & SPAM

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.

During the period April - June 2021, the National KE-CIRT/CC continued utilizing its Darknet Monitoring System to gather reports on spam and phishing threats.

The move to remote working as a result of the COVID-19 pandemic has fast tracked the shift to remote working, with organizations moving from on-premise infrastructure to the cloud. This means that substantial business activities are increasingly being conducted online and remotely, more so with personal smart devices.

This shift has resulted in a surge in phishing attacks targeting various platforms and tools, with the objective of stealing confidential information.

Notably, there was an increase in phishing attacks targeted at video conferencing software, with cyber threat actors impersonating trusted video conferencing software. The attackers used false domains to impersonate legitimate video conferencing domains such as Zoom, Google Meet and Skype, and used these to fabricate online meeting notifications and create fake COVID-19 themed email alerts. These malicious links and email alerts were then used to deliver malware, exfiltrate user data, and steal login credentials.

There was also a notable increase in phishing attacks targeted at e-commerce platforms through search engine phishing; emails, through email phishing; voice, through vishing; and text communication, through smishing attacks. Cyber threat actors leveraged these attacks to harvest login credentials, steal Personally Identifiable Information (PII), compromise search engine searches, and gain unauthorised access to personal and corporate resources.

WHAT WE CAN DO

TIPS ON BEST PRACTICES

Perform due diligence when responding to digital communication, and where possible, call the sender to confirm the requests;

- Do not to click on links embedded in unverified digital communication threads;
- Do not to share Personally Identifiable Information (PII);
- Do not do open file attachments associated with unverified digital communication;
- Implement phishing security to filter phishing attempts.

WEB APPLICATION ATTACKS

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.

During the period April - June 2021, the National KE-CIRT/CC detected 11,272,402 cyber threat events, which was a 199.19% increase from the 3,767,588 threat events detected in the previous period, January - March 2021. In response to the detected cyber threat attempts, the National KE-CIRT/CC issued 223 advisories. This was a 16.47% decrease compared to the 267 advisories that were issued during the period of January - March 2021.

From web-hosted video conferencing applications, banking services, e-commerce sites, e-government services, web-hosted document editing applications, to file sharing services amongst others; more and more services and web applications are being hosted by web servers. This means that the cyber threat attack surface continues to expand, thereby attracting cyber threat actors who are drawn to the data held in these services and applications. In fact, web application attacks account for nearly 90% of cyber attacks in the cyber threat landscape.

During this period, the National KE-CIRT/CC noted a significant increase in web application attacks targeted at healthcare and utility industry databases. In these attacks, cyber threat actors deployed malicious code into unsecured web-server hierarchies and also submitted malicious code into website forms through Structured Query Language (SQL) injection attacks. These attacks sought to steal user credentials, provide unauthorized database access, as well as provide access to critical configuration files.

The increased migration to cloud based infrastructure has also resulted in a significant increase in web application attacks targeted at cloud-based servers. Cyber threat actors utilize malicious automated scripts and botnets to steal credentials, disrupt services, and carry out double brute force intrusion attempts at critical systems and organizations.

Also notable during this period was the continued Distributed Denial of Service (DDoS) attacks targeted at web-based applications. These attacks were carried out using networks of compromised computers and bots, which were used to mount attacks on organization servers by overwhelming them with server requests thereby disrupting services. The threat actors also used local file intrusion techniques to force web-based applications to execute malicious files remotely.

WHAT WE CAN DO

TIPS ON BEST PRACTICES

Apply security patches as soon as they are released;

- Automate vulnerability scanning and security testing;
- Implement secured firewalls that restrict access to applications.

COLLABORATION & INFORMATION SHARING

The future of cybersecurity is collaboration. In fact, collaboration in cyber threat information sharing has been proven as an effective means of enhancing the collective cyber resilience and readiness. In this cybersecurity management approach, cybersecurity is a shared responsibility amongst multiple stakeholders spanning both the public and private sector, through the establishment and nurturing of trusted information sharing frameworks.

These frameworks may be formal or informal, regulatory driven or sector driven. These trust networks are important, as they allow stakeholders to strengthen their collective resilience and reactivity to potential threats. This comes as cyber criminals are continuously innovating, evolving and adapting their techniques to exploit vulnerabilities for malicious purposes. In light of this, cybersecurity experts are faced with the daunting challenge to keep up. Oftentimes, this keeping up with cyber threat actors requires budget intensive resources in the form of new skill sets, infrastructure and systems. Simply put, it is unsustainable for organizations to try and keep up with cyber threat actors. It is this perspective that informs the need for proactive information sharing – also known as intelligence sharing.

In carrying out our mandate of national cybersecurity management, the Authority, through the National KE-CIRT/CC, leverages on collaboration frameworks with local and international stakeholders. This is a critical strategy to building Kenya's national cyber readiness and resilience.

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.

An often-overlooked critical stakeholder in national cybersecurity management is the consumer or end user. This is because end users can define the success, or lack thereof, in complex, well designed cybersecurity systems. To incorporate this critical stakeholder in our national cybersecurity management value chain, the National KE-CIRT/CC developed a cyber incident reporting mobile application - KeCirt App. The application, which is available on android and iOS versions, will enhance seamless cybersecurity incident reporting, incident response, information sharing, as well as enable monitoring of key areas of intervention and support. This is geared at promoting collaboration with the public in cybersecurity management, by encouraging end users to own their role in securing their part of cyberspace.

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

CYBERSECURITY PREDICTIONS

Digital transformation in Kenya has cut across sectors. From agriculture, education, healthcare, manufacturing, amongst others, technology is influencing and shaping our social economic fabric. Indeed, as Kenya moves towards an election year, it is against the backdrop of increased use of the Internet including social media, which has largely been fast tracked by the COVID-19 pandemic.

Social media is no longer just a platform to check up on friends or make new friends. It is increasingly being used for e-commerce, to share interests and hobbies, as a tool to exercise democratic freedoms, civic activism, radicalization, propaganda, and even political campaigning. Already, even as Kenya inches towards the elections, these platforms are awash with dissenting political voices, political propaganda influencers, and peddlers of fake news and disinformation.

However, what many social media users are not aware of is that a majority of these conversations are being driven by social media botnets. Whereas traditional botnets directly infect computers to create networks, social botnets use social media platforms to generate a network of fake profiles that are linked together to spread malicious links and content such as fake news, propaganda, misinformation, or even defamation campaigns.

These are able to mimic the interactions of normal social media users to reduce the risk of being detected by social media platforms. Cyber criminals do this by either creating hundreds of profiles themselves or by using specially designed software programs to create and multiply false personalities.

These social media botnets are found across all social media platforms, and cyber threat actors are increasingly using them to disseminate malicious links, collect intelligence on high profile targets, steal Personally Identifiable Information (PII), propagate cyber propaganda, and spread misinformation, not only about the COVID-19 pandemic, but also about the upcoming electoral processes. This has the potential of causing serious and harmful consequences that could lead to undermining of our electoral processes, through the spread of harmful conspiracy theories, hate speech, ethnic incitement, among others.

To mitigate against this, the Authority, through the National KE-CIRT/CC, has identified the need for cyber education to end-users that focuses on how to identify fake news, social bots, disinformation and cyber propaganda. In addition, the launch of the cyber incident reporting application will enhance reporting of these incidents by the general public for quicker response and action. However, a multi stakeholder approach is necessary in creating awareness and responding to the risks arising from the continued use of social bots to influence voter behaviour especially in electoral processes.

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