NATIONAL KE-CIRT/CC CYBERSECURITY REPORT

FOR THE PERIOD JULY - SEPTEMBER 2020

COMMUNICATIONS AUTHORITY OF KENYA

MESSAGE FROM THE AG DIRECTOR GENERAL

With data being the most coveted asset in the 21st century, cybersecurity continues to be a forefront measure to secure data and its supporting infrastructure.

During the period July - September, the Authority through the National KE-CIRT/CC observed various cybersecurity threat attempts attributed to COVID-19 vulnerability exploits in the financial sector, healthcare sector, video conferencing platforms, threats targeting infrastructure, mobile malware, data leaks and cyber threat attempts at Government level.

This period was characterized by a wide range of COVID-19 related financial scams. There was also the increased use of social engineering techniques by cyber criminals to acquire credentials for malicious purposes such as the compromise of high profile twitter accounts for purposes of promoting cryptocurrency scams. There was also the use of phishing campaigns impersonating various personalities and organizations, which were used to spread Bitcoin and get-rich-quick scams.

During this period, the National KE-CIRT/CC noted the adoption of a line-up of sophisticated exploitation techniques that targeted video conferencing platforms such as Zoom. These bugs allowed cyber criminals to pose as company employees, invite customers and partners to meetings and extract sensitive information using social engineering techniques.

Other developments during the period included the continued evolution of malware in the mobile arena. This included Android banking malware strains that are designed to steal passwords and credit card data.

The Authority through the National KE-CIRT/CC continues to invest in enhancing the current monitoring, detection and analysis systems, as well as capacity building of front line cybersecurity professionals with the objective of enhancing Kenya's national cyber readiness and resilience.

Further, the Authority through the National KE-CIRT/CC continues to enhance collaborations with local and international partners such as with over 50 National Computer Incident Report Teams (CIRTs) globally, 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 with the objective of leveraging knowledge and infromation sharing as well as levelled-up research and development to further upscale Kenya's cybersecurity standing.

"Towards a Cyber Ready and Cyber Resilient Nation"

CYBER THREAT STATISTICS

31,842,635

The National KE-CIRT/CC detected 31,842,635 malware threat attempts during the period July - September 2020, as compared to the 12,508,275 detected in the previous period April - June 2020.

1,245,451

The National KE-CIRT/CC detected 1,245,451 DDOS/Botnet threat attempts during the period July - September as compared to the 267,931 detected in the previous period April - June 2020.

2,057,369

The National KE-CIRT/CC detected 2,057,369 web application attacks during the period July - September as compared to the 1,102,840 detected in the previous period April - June 2020.

28,482

The National KE-CIRT/CC detected 28,482 system vulnerabilities during the period July - September as compared to the 30,023 detected in the previous period April - June 2020.

35,173,937

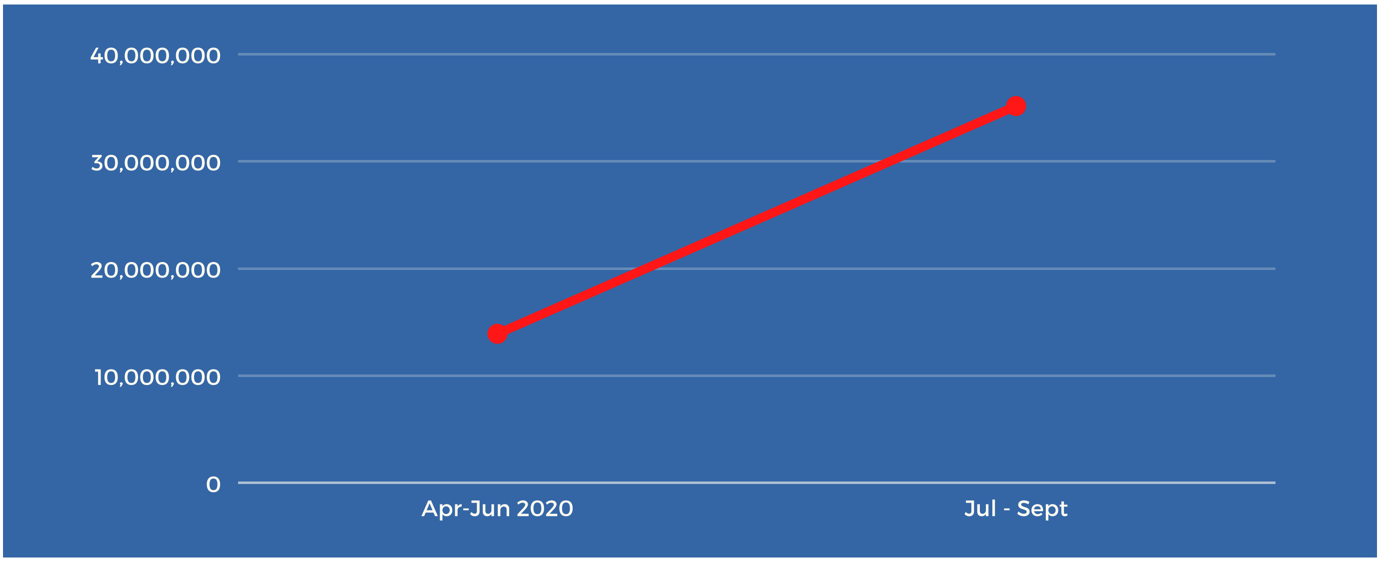
Total number of cyber threat events detected by the National KE-CIRT/CC during the period July - September 2020.

21,728

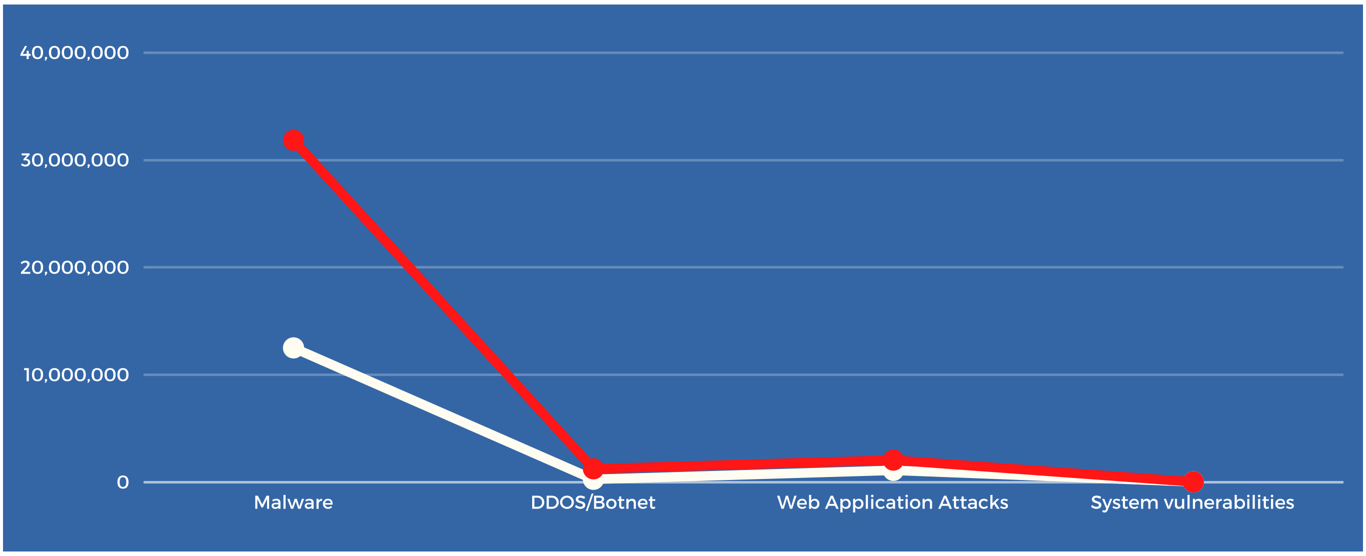
Total number of cyber threat advisories issued to affected organizations in response to cyber threat events detected by the National KE-CIRT/CC during the period July - September 2020.

CYBER THREAT LANDSCAPE

During the period July – September, the National KE-CIRT/CC detected 35.17 million cyber threat events, which was a 153.02% increase from the 13.90 million threat events detected in the previous period, April – June 2020. This increase was attributed to increased attacks targeted at organizations, with an averaged of 1,008 attacks per week locally, as compared to 485 attacks per organization globally. The top malware accounted for 25% impact on organizations locally as compared to 13% of the top impacting malware globally. There was an increase in malicious file types via email and web applications, which leveraged on the increased uptake of working remotely and online learning measures in response to the ongoing Covid-19 pandemic.



In response to the detected cyber threat attempts, the National KE-CIRT/CC issued 21,728 advisories. This was a 4.26% increase compared to the 20,839 advisories that were issued during the period of April – June 2020.



CYBER THREAT ADVISORIES

21,728

In response to the 35,173,937 cyber threat attempts detected locally by the National KE-CIRT/CC during the period July - September 2020, 21,728 advisories were issued to the affected organizations. This was a 4.26% increase from the 20,839 advisories issued during the previous period April - June 2020.

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

SYSTEM VULNERABILITIES

System vulnerabilities are weaknesses exploitable by threat actors who use these to cross privilege boundaries within a computer system. A cyber criminal exploits a system by possessing at least one applicable tool or technique that can connect to a system weakness.

During the period July – September 2020, the National KE-CIRT/CC detected 28,482 system vulnerabilities, which was a 5.13% decrease from the 30,023 detected in the previous period April – June 2020. This decrease was attributed to increased security measures taken by organizations to safeguard their systems that support remote working including cloud resources and Virtual Private Networks (VPNs), as organizations continued to make their systems publicly accessible to workers operating remotely via their home networks amidst the Covid-19 pandemic. Top national vulnerability exploits accounted for 62.1% locally compared to 64.7% globally through remote code execution exploit.

In response to these detected cyber threat attempts, the National KE-CIRT/CC issued 19,674 system vulnerabilities advisories to the affected organizations. This was a 13.30% increase from the 17,364 issued in the previous period, April -June 2020

During this period, the National KE-CIRT/CC observed the critical automatic propagating exploit bug SigRed, with the tracking identifier CVE-2020-1350, in Microsoft's Windows Domain Name System (DNS) Server. Prior to its patch, SigRed enabled an attacker to gain remote domain administrator privileges and compromise the entire corporate infrastructure, receiving a severity score of 10 out of 10 owing to the critical DNS server breach status. Also noted prior to Cisco releasing software updates, was the exploitation of the Cisco Small Business RV340 Series Routers for the purpose of conducting Remote Code Execution (RCE) and privilege escalation attacks on Cisco's Small Business Wireless VPN Firewall routers.

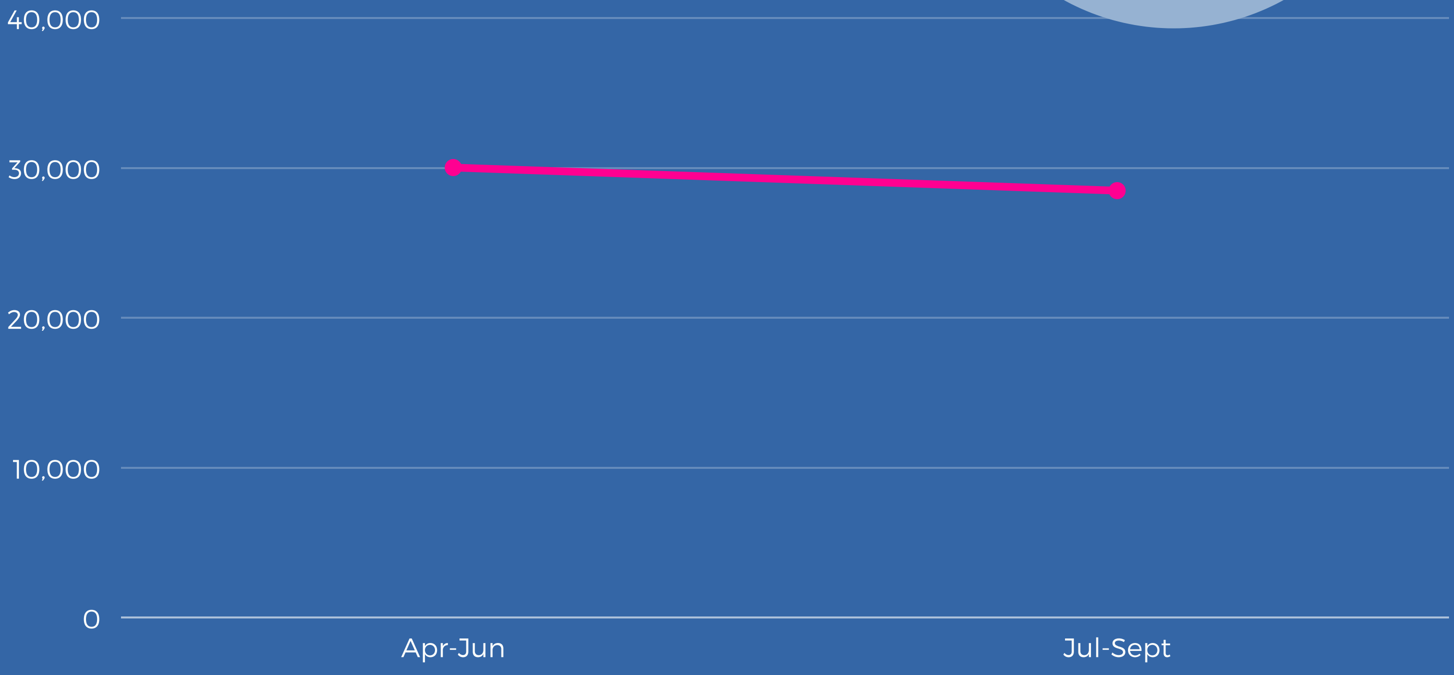
Another notable vulnerability during this period was the vulnerability in the GRUB2 bootloader, a popular bootloader for all major Linux distributors that is sometimes used for Windows and macOS. The vulnerability with the tracking identifier CVE-2020-10713 dubbed BootHole, allowed attackers to tamper with the boot-loading process that precedes starting up the actual Operating System (OS) thus potentially enabling full control of systems.

During this period, Microsoft issued an emergency out-of-band security update for Windows 8.1 and Windows Server 2012 R2 vulnerabilities in the Remote Access Service (RAS), that had prior to the patch release, allowed attackers to remotely gain elevated privileges.

28,482

Detected system vulnerabilities events during the period

An analysis of System Vulnerabilities threat attempts detected during the period April - September 2020



MALWARE

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

During the period July - September 2020, the National KE-CIRT/CC detected 31,842,635 malware threat attempts locally. This was a 154.57% increase from the previous period April-June where 12,508,275 malware threat attempts had been detected locally. This increase was attributed to the extended impact malware had on organizations locally at 25% compared to 13% globally via the Lucifer and Emotet malware families respectively. The Lucifer malware was observed abusing critical vulnerabilities on Windows machines to further perpetrate Remote Code Execution (RCE) attacks.

In response to these detected malware attack attempts, the National KE-CIRT/CC issued 1,003 cyber threat advisories to affected organizations. The number of advisories issued during the period July - September 2020 decreased by 58.17% as compared to those issued in the previous period April - June 2020.

During this period, the National KE-CIRT/CC observed a malware family application named xHelper that impacted 20% of local organizations. The malicious application downloaded additional malicious applications and had the ability of reinstalling itself even after being uninstalled. Further, the Emotet malware continued to affect 19% of Kenya's cyber space as compared to its 13% impact globally. Emotet continues to distribute additional malware and malicious campaigns through phishing spam emails containing malicious links and attachments.

The XMRig miner malware exploited vulnerable Windows, Internet Information Services (IIS) and Linux servers for purposes of mining Monero cryptocurrency. This malware impacted 14% of Kenyan organizations as compared to 2% globally. An information stealer and backdoor malware, Floxif was observed in malware campaigns targeting the Windows Operating System (OS) cleanup utility CCleaner free version, impacting 13% of local organizations as compared to 1% globally. A

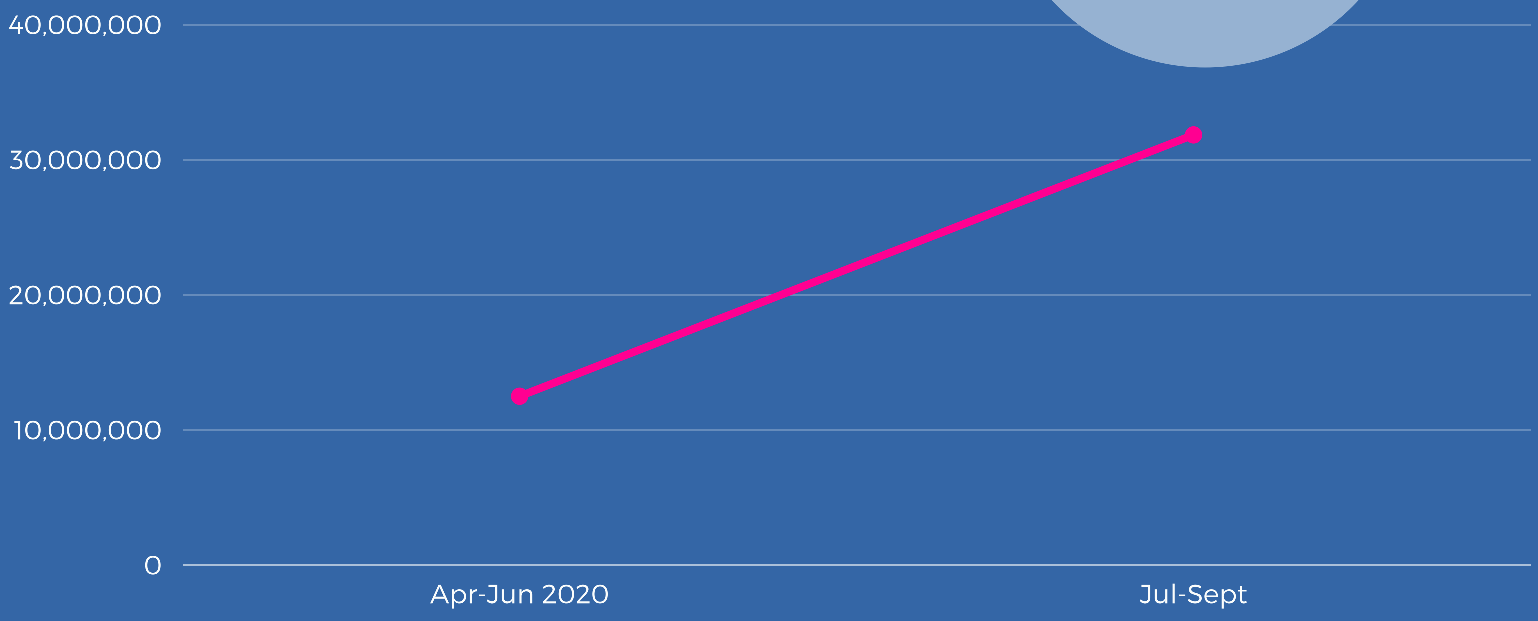
gentTesla malware, a Remote Access Trojan (RAT) was observed monitoring and collecting users keystrokes entered for a variety of software including Google Chrome, Mozilla Firefox and Microsoft Outlook email client. This malware impacted 9% of organizations locally as compared to 3% globally.

The higher than global average trend in malware impact calls for enhanced detection, analysis and recovery processes amongst Kenyan organizations. Further, there is need to continually upscale the skills of frontline cyber security professionals in the country as a measure towards enhancing the collective cyber readiness and resilience across sectors nationally.

31,842,635

Malware threat events detected by the National KE-CIRT/CC during the period July - September 2020

An analysis of Malware threat events detected during the period April - September 2020



PHISHING

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

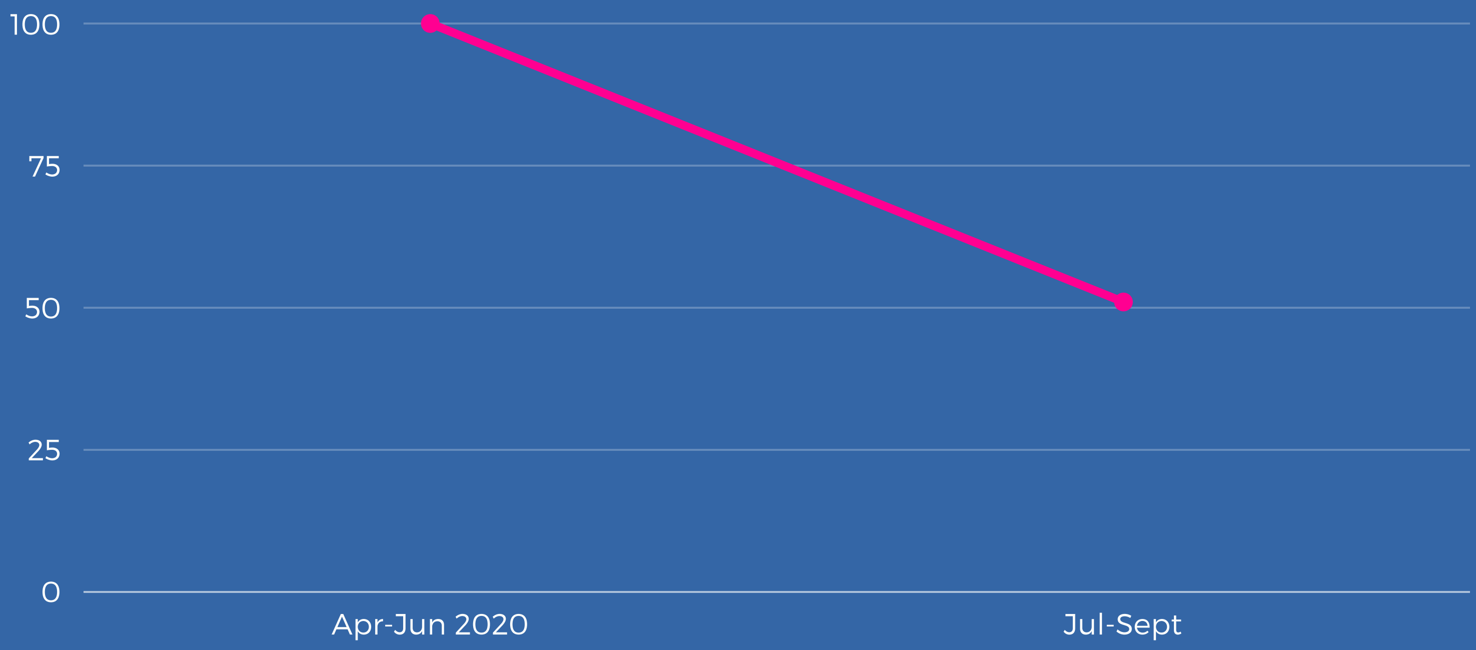
During the period July – September, the National KE-CIRT/CC noted a phishing campaign where attackers impersonated the Office 365 platform from Microsoft by bypassing the Proofpoint email security feature. The phishing campaign asked recipients to renew their Microsoft Office subscription through the malicious links provided with the objective being to steal sensitive user information from approximately 15,000 to 50,000 mailboxes.

Also notable was the phishing scam affecting cPanel, an industry leader for turning standalone servers into fully automated point-and-click hosting platform. The phishing scam spread a fake security advisory of a critical vulnerability in their web hosting management panel and redirected users to a credential-stealing page.

51

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

An analysis of Phishing threat attempts detected during the period April - September 2020



WEB APPLICATION ATTACKS

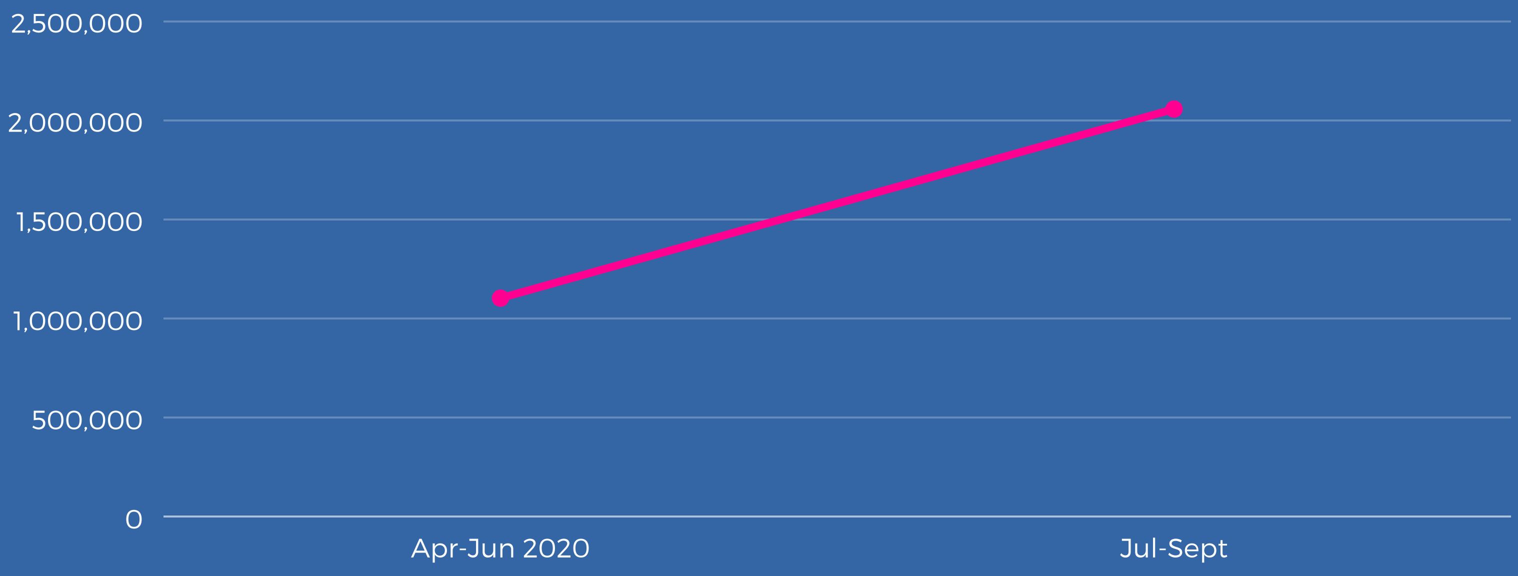
Web Application attacks are executed by leveraging on web application vulnerabilities. Website vulnerabilities are weakness or misconfiguration in websites application code that allow cyber criminals to gain some level of control of the website, including the hosting server.
During the period July - September 2020, the National KE-CIRT/CC detected 2,057,369 web application attack attempts. This was a 86.55% increase from the 1,102,840 detected in the previous period April - June 2020.
This rise was attributed to increased data theft attacks, privilege escalation attacks enabling unauthorized data access, and Man-in-the-Middle (MitM) attacks on existing web facing applications such as WordPress, Adobe and its variants, and Google Chrome browser.

In response to the detected web application attack attempts, the National KE-CIRT/CC issued 305 advisories to the affected organizations. This was a 49.50% increase from the 204 advisories that were issued in the previous period, April - June 2020.
During this period, misconfiguration of public clouds, unsecured platforms and account hijacking ranked globally at 68%, 52% and 50% in security impact severity by organizations. Notable during the period were the four critical vulnerabilities across five different platforms in Adobe which were later addressed: Creative Cloud Desktop, Media Encoder, Download Manager, Genuine Service, and ColdFusion.
Vulnerability on the Google Chrome browser during the period exposed users to data theft by allowing attackers to bypass the Content Security Policy (CSP) protection to steal data and execute rogue code.
Also notable was the high severity bug in Facebook's official chat plugin which allowed WordPress website owners to embed a chat pop-up to communicate, in real-time with visitors, and which allowed attackers to intercept messages sent by visitors to the vulnerable sites' owner.

2,057,369

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

An analysis of Web Application Attack threat attempts detected during the period April - September 2020



BOTNET/ DDOS

Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding IT infrastructure with a flood of Internet traffic.

A botnet is a group of Internet connected devices running automated tasks over the Internet and which can be used to perform DDoS attacks.

During the period July - September 2020, the National KE-CIRT/CC detected 1,245,451 botnet attack events, which was a 364.84% increase from those detected in the previous period April - June 2020.

This increase was attributed to increased botnet aided malspam campaigns, malware and ransomware aided attacks. Botnet attacks impacted an average of 27.0% organizations locally compared to 6.95% globally.

In response to these detected Botnet/DDOS attack attempts, the National KE-CIRT/CC issued 326 advisories. This was a 28.66% decrease from those issued in the previous period April - June 2020.

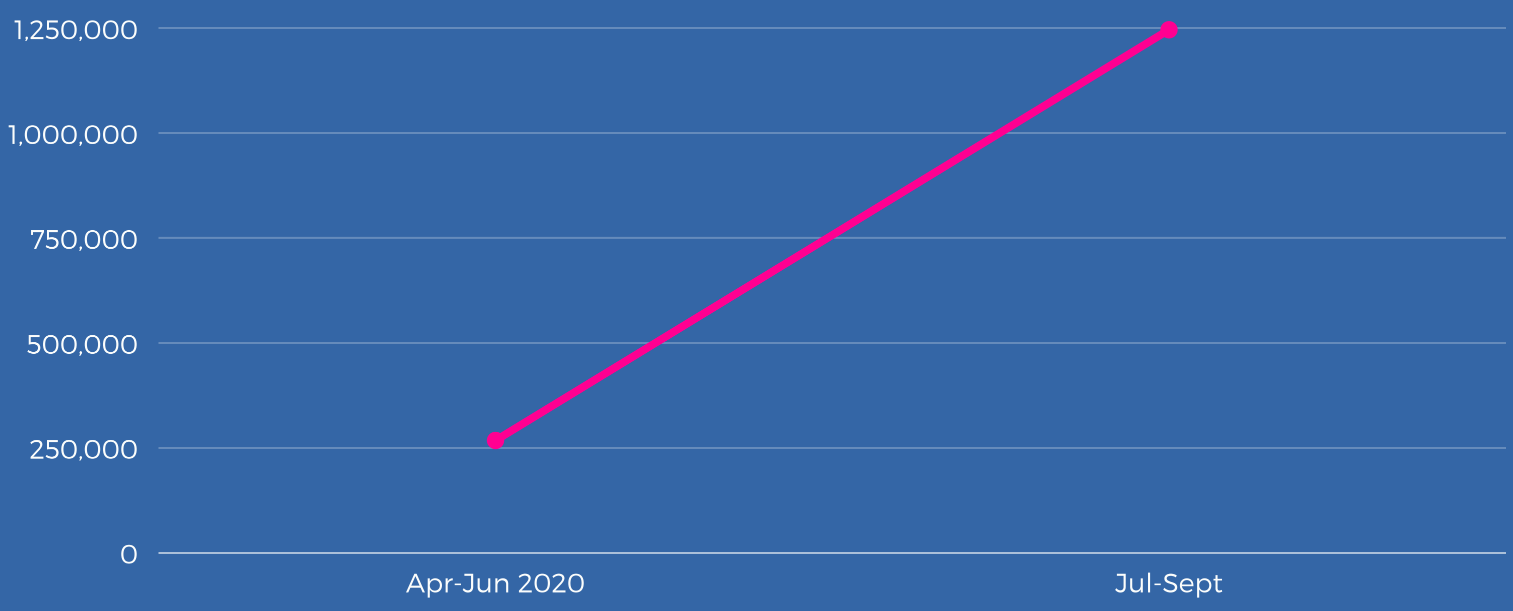
During the period, the Dridex botnet leveraged macros in Microsoft Office with the objective of infecting banking and financial systems to gain access to users financial records and Personal Identifiable Information (PII). This strain of botnet malware accounted for 23% of the botnet attacks experienced in the Europe, the Middle East and Africa (EMEA) region.,

Other notable attacks during the period included the attack by the cyber criminal gangs known by the alias *Armada Collective* and *Fancy Bear actors*, which targeted financial service providers such as PayPal, Venmo, money transfer service MoneyGram, among others. The gang demanded Bitcoin payments as extortion. Also notable were DDoS attacks targeted at European Internet Service Providers (ISPs) routers and DNS infrastructure, and which accounted for 300 Gigabit per second (Gbit/s) in volume and which were part of an extortion attempt.

An analysis of Botnet/DDOS threat events detected during the period April - September 2020

1,245,451

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



DIGITAL FORENSICS AND INVESTIGATIONS

Digital forensics is the process of preservation, identification, extraction and documentation of computer evidence that is admissible in court for cyber crime prosecution.

The National KE-CIRT/CC continues to secure and analyze digital evidence and conduct research and development through the Digital Forensic Lab (DFL).

The National KE-CIRT/CC also accords the Directorate of Criminal Investigation (DCI) and other law enforcement agencies support by facilitating the analysis and preservation of digital evidence to aid in the prosecution of cyber related crimes.

Accredited digital forensic examiners working with the DFL are involved in the examination of digital exhibits from different agencies within the country and subsequently generate Expert reports for court purposes, and attend court as Expert Witnesses during the hearing of the said cases.

During the period July - September 2020, the National KE-CIRT/CC received 354 requests for facilitation from investigative agencies. This was a 36.15% increase in requests received as compared to 260 in the previous period April - June 2020.

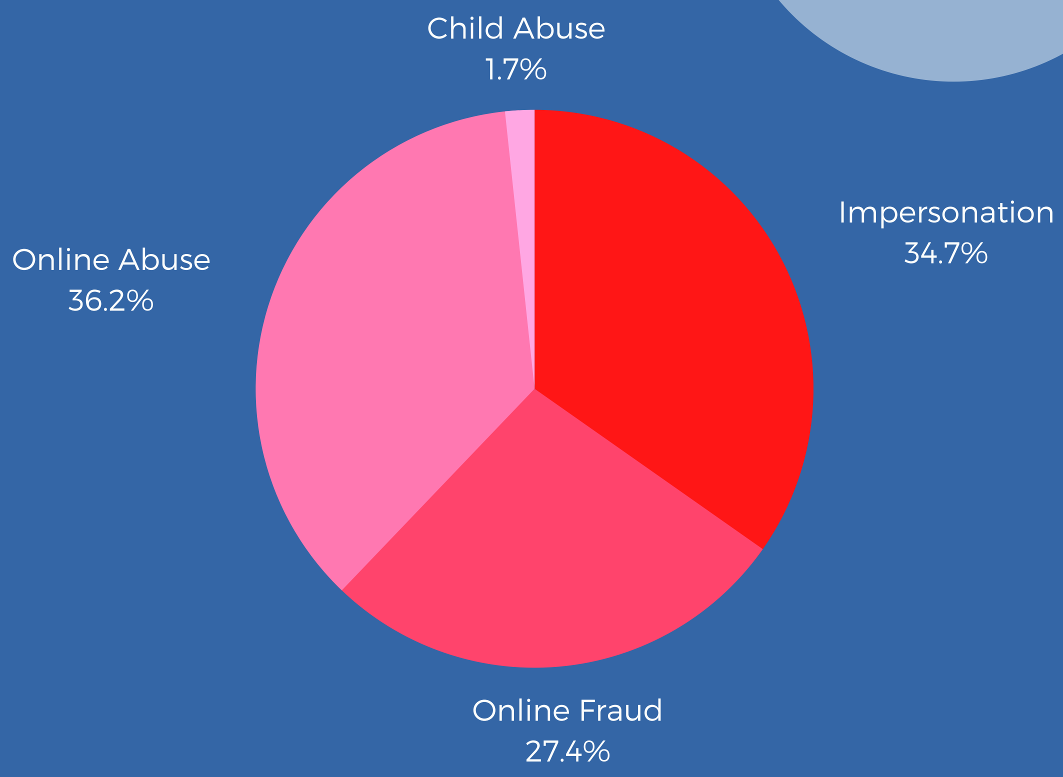
There was an increase in requests for facilitation in investigations relating to online abuse and online fraud cases, while there was a decrease in requests relating to impersonation cases as compared to the previous period.

The overall increase in investigative requests during the period was attributed to the rise in online abuse and online fraud as a result of increased reliance on digital tools and online platforms amidst the Covid-19 pandemic. In addition, the National KE-CIRT/CC observed an increased in cyber bullying and Internet trolling across domains and social media platforms during the reporting period.

The National KE-CIRT/CC continues to carry out cyber awareness in an effort to counter these harmful online practices. .

354

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



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

COLLABORATION AND CYBERSECURITY

The National KE-CIRT/CC continues to collaborate with various cybersecurity stakeholders locally and globally with the aim of enhancing the national cyber readiness and resilience.

Globally, the National KE-CIRT/CC continued to partner with over 50 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 to leverage on knowledge sharing and levelled-up research and development to further upscale the nation's cybersecurity standing.

Locally, the National KE-CIRT/CC Cybersecurity Committee (NKCC), addresses various national sector cybersecurity concerns. Drawing its membership from telecommunications companies, financial sector stakehodlers, academia, law enforcement agencies, public utility companies, professional association among others, the committee is one of the critical collaborative efforts at enhancing Kenya's national cybersecurity posture.

MERCY WANJAU, MRS
AG DIRECTOR GENERAL

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

Email: incidents@ke-cirt.go.ke

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