



COMMUNICATIONS
AUTHORITY OF KENYA

Cybersecurity Report

34th Edition

April - June 2024

A report by:

The National KE-CIRT/CC

☎ +254-703-042700 or
+254-730-172700

✉ incidents@ke-cirt.go.ke

🌐 www.ke-cirt.go.ke

Strategic Direction

Our Vision

Digital Access for All

Our Mission

Enabling a Sustainable Digital Society through Responsive Regulation

Our Core Values

Integrity, Innovation, Excellence, Inclusion, Agility.

Cybersecurity Mandate

The 5th Strategic Plan (2023 - 2027) of the Communications Authority of Kenya (CA) aims to build upon past achievements, tackle present challenges and opportunities in the evolving ICT landscape and enhance the Authority's performance in the digital access for all. This plan will guide the Authority's activities and ensure its continued contribution to the growth and development of the ICT sector in Kenya.

The Kenya Information and Communications Act (KICA) of 1998, mandates the Authority to develop a framework for facilitating the investigation and prosecution of cybercrime offences. It is in this regard, and in order to mitigate cyber threats and foster a safer Kenyan cyberspace, that the government established the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC), which was officially launched in 2014.

The National KE-CIRT/CC is a multi-agency framework that coordinates response to cyber security matters at the national level in collaboration with relevant actors locally and internationally. The National KE-CIRT/CC, which is domiciled at the Communications Authority of Kenya, comprises of technical staff from the Authority and various law enforcement agencies.

The enactment of the Computer Misuse and Cyber Crimes Act (CMCA) in 2018 has further enhanced the multi-agency collaboration framework through the establishment of the National Computer and Cybercrimes Coordination Committee (NC4). Under the CMCA, and following the enactment of the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations in 2024, the role of the Authority has been enhanced to include the establishment and operation of the Cyber Security Operations Centre (CSOC) for the ICT and Telcom Sector.

Director General's Perspective



Mr. David Mugonyi, EBS, Director General/CEO, Communications Authority of Kenya (CA)

Cybersecurity is a multifaceted concept that involves people, processes, and policies in addition to technology. Developing a culture of cyber hygiene, establishing robust policies and ensuring that all stakeholders receive ongoing education and training are all necessary for effective cybersecurity. The effective detection and response to cyber threat activity, requires a collaborative effort at both the organisational and national levels. This therefore underscores the importance of the human element in addition to technological measures in safeguarding our digital assets, data and systems.

Over the period April - June 2024, the National KE-CIRT/CC detected over 1.1 billion cyber threat events. Majority of these attacks exploited system vulnerabilities. This is attributed to the continued proliferation of Internet of Things (IoT) devices in the country which are inherently insecure, insecure system configurations and deprecated software, as well as the dynamism occasioned by new and emerging technologies such as Artificial Intelligence (AI).

Cybercriminals have continued to utilise identity theft and phishing to trick victims into disclosing sensitive information, which can result in grave financial losses. Cyber bullying and cyber harassment are some of the activities that comprise online abuse, amongst other malicious activities.

Cyberwarfare is the use of digital attacks by a nation-state to interfere with, destroy or cause harm to another state's networks and information systems

These attacks try to compromise security, economic well-being and public trust by focusing on government networks, private sector assets and military operations. Cyberwarfare poses a serious and dynamic threat that calls for strong cybersecurity defences and cross-national collaboration to lessen its effects.

Kenya continues to seek strategic engagements with various international partners in areas that cut across cybersecurity governance, capacity and capability development, information sharing and cyber incident response.

In recognition of this, collaboration in the field of cyber security was a key agenda during His Excellency President William Ruto's state visit to the United States in May 2024. The two countries agreed to enhance their national cyber security collaborative efforts, in particular, Kenya and the United States agreed to host a regional cybersecurity symposium that would bring together various government and stakeholders from Africa.

As we move into the 2024/2025 financial year, the Authority will continue focusing on building national cyber readiness and resilience that involves a combination of robust strategies, advanced technological defences, comprehensive policy frameworks and a culture of cyber hygiene.

The Authority hosts the National Kenya Computer Incident Response Centre - Coordination Centre (National KE-CIRT/CC), which is a multi-agency collaboration framework that is responsible for the national coordination of cyber security and acts as Kenya's national point of contact on cyber security matters. The Centre has been instrumental in coordinating response to cyber threats in partnership with relevant law enforcement agencies, sector regulators, financial institutions and the private sector.

In conclusion, the management of cybersecurity requires a recognition of the interconnectedness of the digital ecosystem, where the security of one is intertwined with the security of all, and therefore the need for a concerted multi-stakeholder approach.

**Mr. David Mugonyi, EBS
Director General/CEO**

Global Cyber Threat Landscape Overview



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.*

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 this period, cyber threat actors were observed leveraging various malware families to compromise and disrupt systems, carry out data breaches and cause operational downtime and data loss within the education, government, insurance and healthcare sectors. The top malware families include:

- FakeUpdates: Led to widespread system compromises and unauthorised access.
- AndroXgh0st: Resulted in data exfiltration and system vulnerabilities.
- Qbot: Facilitated further attacks through compromised credentials.

Mobile Malware

Mobile devices are increasingly being used for personal and professional activities, making them prime targets for cyber threat actors. During this period, cyber threat actors were observed leveraging mobile malware such as *Anubis*, *AhMyth*, and *Hiddad* to unauthorisedly access sensitive data and carry out financial fraud, compromising user privacy and security.

Social Engineering

Cyber threat actors continue to exploit human psychology for purposes of bypassing technical defences. Notably during this period, phishing and smishing (SMS phishing) attacks were observed being propagated to manipulate users into revealing personal information and installing malware, causing widespread data breaches and financial losses.

Business Email Compromise (BEC)

Business Email Compromise (BEC) is a type of cyberattack where threat actors use email to lure individuals within organisations into transferring money or sensitive information. Cyber threat actors leverage BEC to target critical communication channels within organisations with the aim of causing operational disruptions by exploiting trusted email communications to carry out fraud and steal sensitive information.

Mapping the Global Threat Landscape

The similarities in attack vectors, tactics, and vulnerabilities impacting both individuals and organisations demonstrates how the cyber threat landscape in Kenya and across the rest of the world align. This convergence highlights the universal nature of cyber threats, as global trends and techniques tend to materialize and adapt within particular geolocations.

Cyber Threat Landscape Roundup

Total Cyber Threats Detected

1,131,696,878



16.50%

During the three-month period between April and June 2024, the National KE-CIRT/CC detected **1.1 billion** cyber threat events, which represented a **16.50%** increase from the 971,440,345 threat events detected in the previous period (January to March). In response to the increasing frequency of cyber threats, we enhanced the dissemination of cyber threat advisories to critical information infrastructure sectors. In line with global trends, the ongoing exploitation of "system vulnerabilities" may be associated to the continued proliferation of Internet of Things (IoT) devices which are inherently insecure, insecure system configurations and deprecated software, as well as the dynamism occasioned by new and emerging technologies such as Artificial Intelligence (AI).



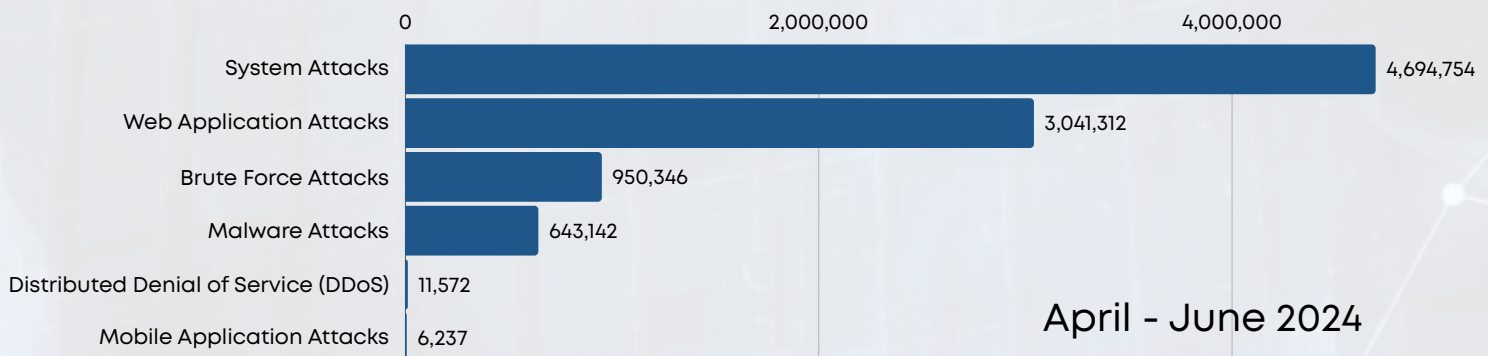
Total Cyber Threat Advisories Issued

9,347,542



9.66%

In response to the detected cyber threat events, the National KE-CIRT/CC issued **9,347,542** advisories between the period April to June 2024, which represented a **9.66%** increase compared to the 8,524,407 advisories that were issued during the previous period, January to March 2024. During the period, there was a significant increase in the number of advisories on system attacks. These advisories were aimed at advising users to patch vulnerable systems on a regular basis, utilising multi-factor authentication, strong passwords, and hardening network switches and firewall configurations.

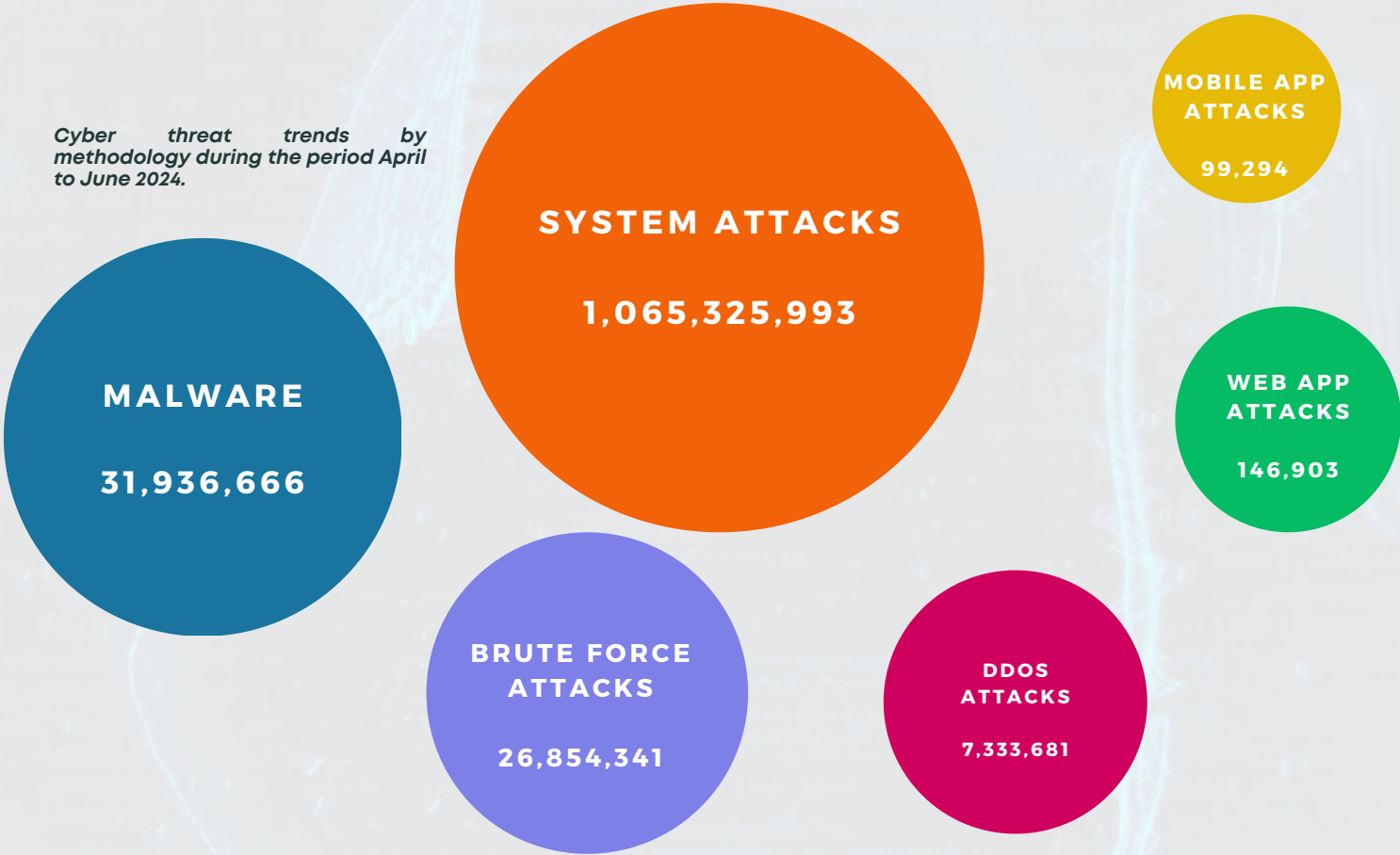


Cyber Attack Vector Trends

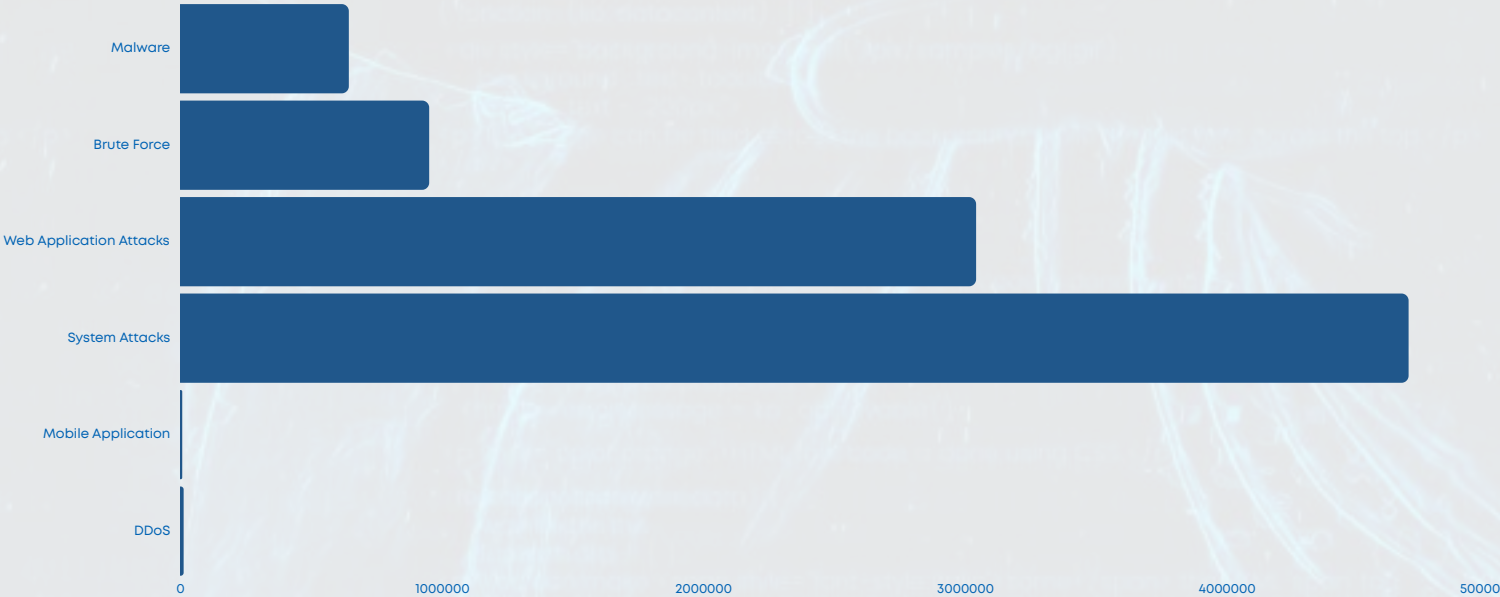
During the quarter under review, system misconfiguration attacks were the most prevalent. This aligns with the global cyber threat landscape where malware attacks, and more specifically ransomware, was most common.

Cyber attacks occasioned by system misconfiguration may be linked to inadequate investment in technical infrastructure, use of legacy systems, default login credentials, and low levels of cyber risk awareness. These factors all contribute to increased susceptibility of the critical infrastructure sectors to cyber threats.

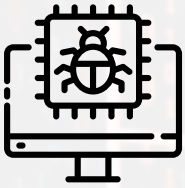
Cyber threat trends by methodology during the period April to June 2024.



Comparison of cyber threat advisories (per vector) issued during the period April to June 2024.



Malware Trends



Threats Detected

31,936,666

3.77%

Advisories Issued

643,142

45.61%

During the three month period between April to June 2024, the National KE-CIRT/CC detected **31,936,666** malware threat attempts targeting at the critical information infrastructure sector. This represented a **3.77%** decrease from the previous period, January to March 2024.

Most of the attacks were targeted at the ICT sector and cloud services. Threat actors targeted end-user devices, Internet of Things (IoT), web applications and networking devices belonging to Internet Service Providers (ISPs), cloud-based services and government systems. Most attackers exploited zero-day vulnerabilities and supply-chain attacks.

Top Targeted Systems

- End-User Devices
- Internet of Things (IoT)
- Web Applications
- Networking Devices

Top Affected Industries

- Internet Service Providers
- Cloud Service Providers
- Government
- Academia/Education

Top Targeted Exploits

- CVE-2024-3400 in Palo Alto Networks PAN-OS: A zero-day vulnerability exploited by threat actors to execute code with root privileges, leading to full device control and significant security risks.
- CVE-2024-4978: A supply chain attack on JAVS courtroom software led to the distribution of RustDoor malware via a backdoored installer, compromising affected systems with full remote access capabilities.
- CVE-2024-24919: A zero-day vulnerability in CheckPoint VPNs is being exploited, allowing remote attackers to execute arbitrary code and gain unauthorized access to affected systems.

These malware attacks were mainly targeted at systems that were deemed as being vulnerable or holding valuable or sensitive data. The objectives of these attacks was to conduct backdoor deployments, perform data exfiltration, affect brand reputation and to encrypt or damage user data.


To mitigate this risk, the National KE-CIRT/CC recommended the following actions to affected organisations:

- Security by design, include security during development of software.
- Asset management with patch management.
- Deployment of DMARC and spam filters.
- Improve end-user cyber hygiene and awareness.

Web Application Attack Trends



Threats Detected
146,903
 **26.34%**

Advisories Issued
3,041,312
 **13.40%**

During the three month period between April to June 2024, the National KE-CIRT/CC detected **146,903** web application attack attempts targeted at the critical information infrastructure sector. This represented a **26.34%** decrease from the previous period, January to March 2024.

Most of these attacks were targeted at government systems and the ICT sector. Attackers targeted user login credentials, vulnerable web browsers and database servers belonging to government and Internet Service Providers (ISPs). Most attackers exploited vulnerabilities in SSL/TLS security misconfigurations.

Top Targeted Systems

- Widely used libraries like Log4J to exploit and compromise web applications.
- APIs with limited security features.
- Insecure configurations in serverless functions.
- Vulnerabilities in open-source libraries.

Top Affected Industries

- Government
- Internet Service Providers
- Cloud Services
- Academia/Educa

Top Targeted Exploits

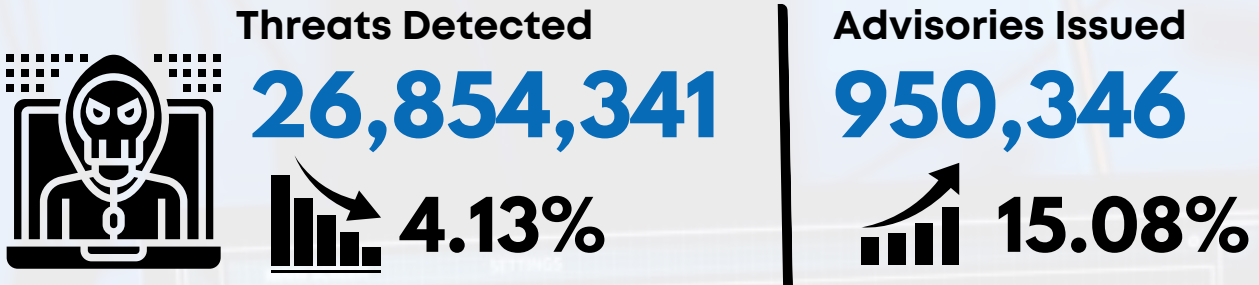
- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication

During the period, web application attacks were targeted at systems regarded to contain valuable data and provide functionality that can be exploited by attackers. The attack objectives were mainly to make services unavailable, manipulate databases and release sensitive data for purposes of damaging organisations' reputations.

To mitigate this risk, the National KE-CIRT/CC recommended the following actions to affected organisations:

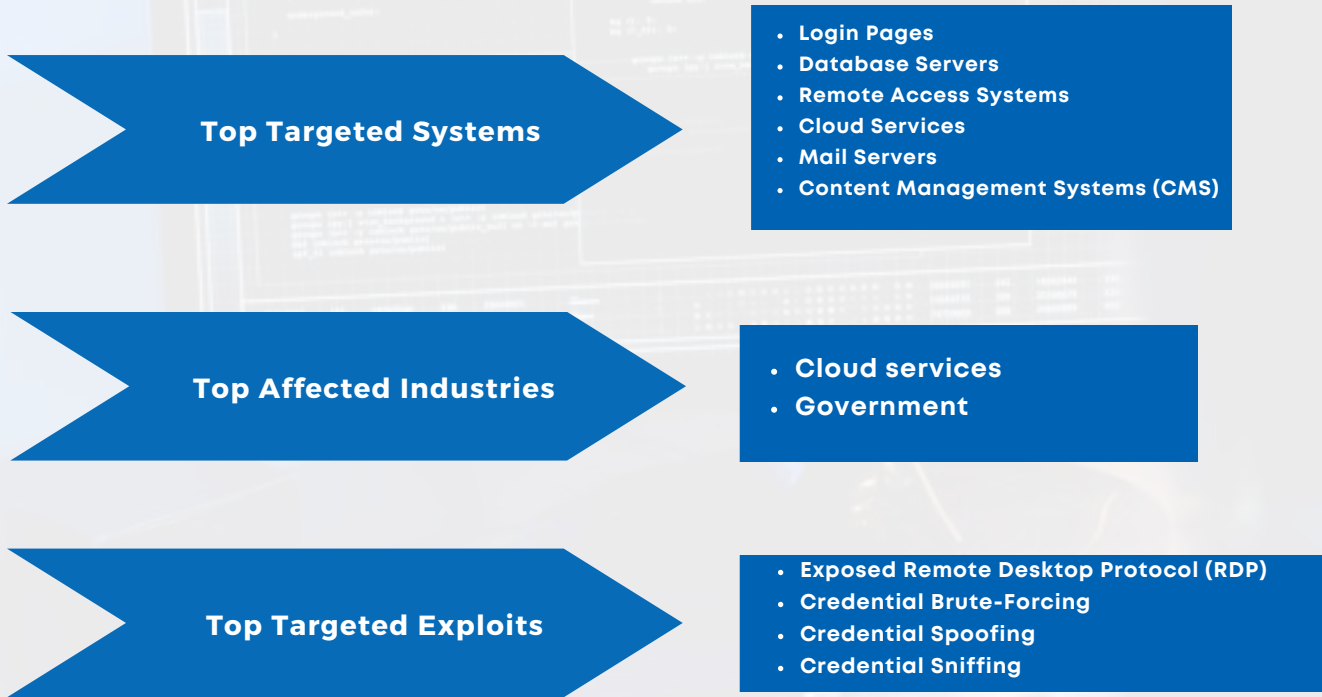
- Disabling SSL 3.0 support in system/ application configurations.
- Upgrading end-of-life (EOL) products.
- Apply the relevant patches and updates as provided.

Brute Force Attack Trends



During the three month period from April to June 2024, the National KE-CIRT/CC detected **26,854,341** brute force attack attempts majorly targeting the critical information infrastructure sector. This represented a **4.13%** decrease from the previous period, January to March 2024.

Majority of the attacks were targeted at organisations within the ICT sector and government systems. Attackers targeted user login credentials and database servers belonging to government organisations and cloud-based services. Most attackers exploited vulnerabilities in the remote desktop protocol, database servers and user login credentials.

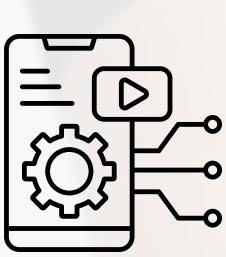


During the period, brute force attacks were targeted at systems deemed to hold sensitive data such as login credentials and financial information. The objective of these attacks was mainly to gain elevated privileges, gain unauthorized access and exfiltrate sensitive data for financial gain.

To mitigate this risk, the National KE-CIRT/CC recommended the following actions to the affected organisations:

- Implement patch management on devices running network-based services.
- Implement appropriate access management with strong password management.
- Disconnect devices from the network if not in use.
- Update softwares to the latest versions.

Mobile Application Attack Trends



Threats Detected

99,294

42.01%

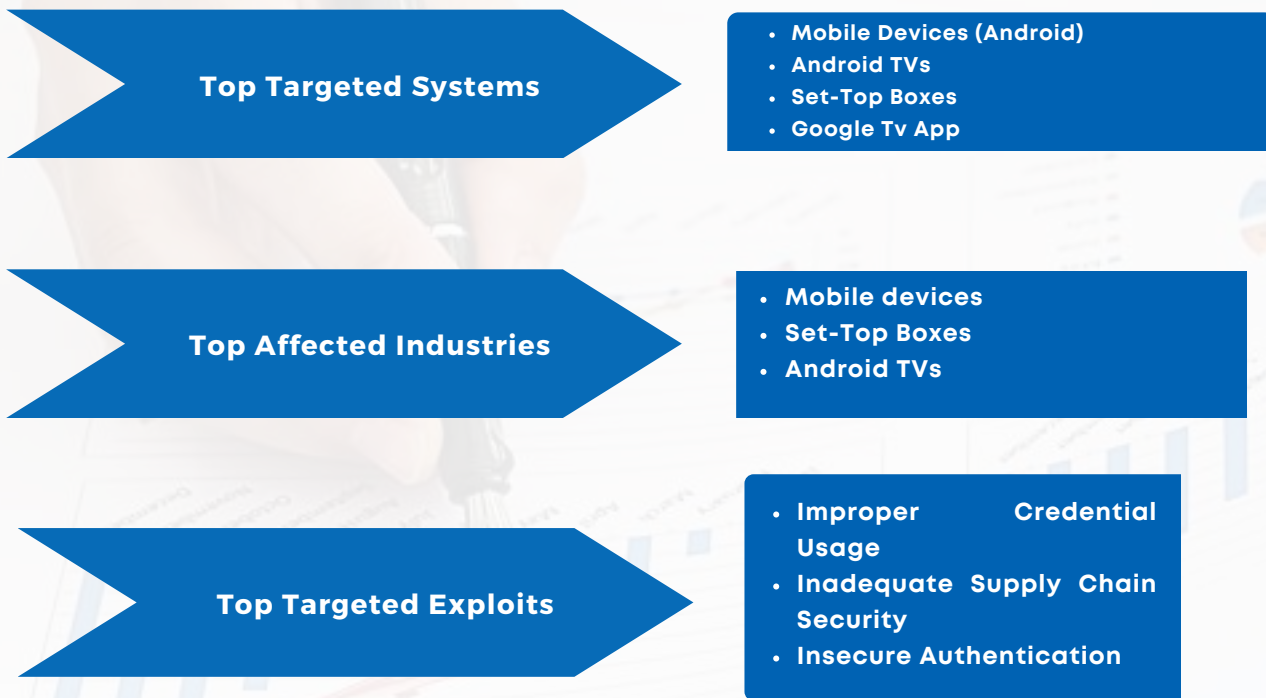
Advisories Issued

6,237

31.13%

During the three month period April to June 2024, the National KE-CIRT/CC detected **99,294** mobile application attack attempts targeting end-user devices. This represented a **42.01%** decrease from the previous period, January to March 2024.

Majority of the attacks were targeted at endpoint devices. Attackers targeted mobile devices and Android TVs and leveraged mostly malware to compromise these devices.

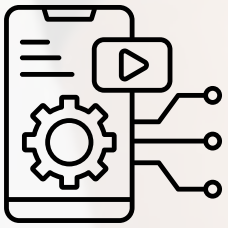


During the period, the perpetrators of mobile application attacks mainly sought to steal sensitive user data such as personally identifiable information, login credentials and financial details for malicious purposes.

To mitigate this risk, the National KE-CIRT/CC carried out cyber awareness for end-users recommending the following actions:

- Disable Android Debug Bridge (ADB) on mobile devices.
- Only download applications from trusted sources.
- Check application permissions.
- Keep device and utilities software up to date.

Distributed Denial-of-Service Attacks



Threats Detected

7,333,681

81.02%

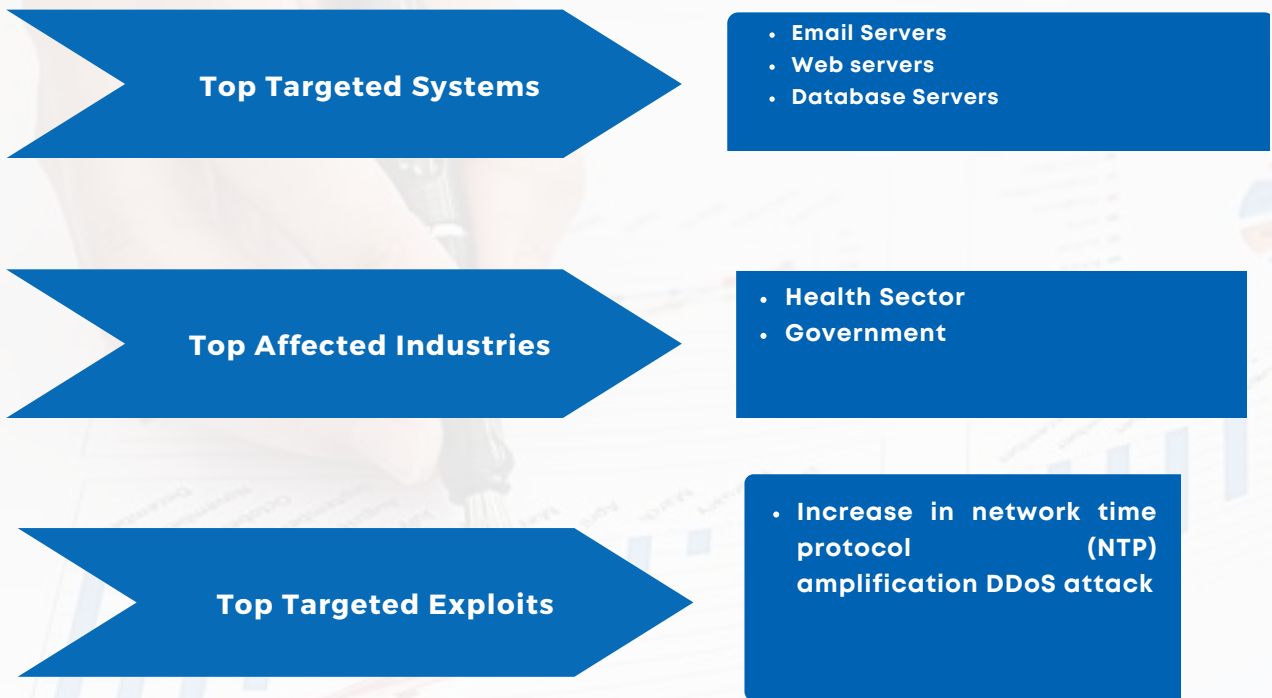
Advisories Issued

11,572

23.81%

During the three month period April to June 2024, the National KE-CIRT/CC detected **7,333,681** Distributed Denial-of-Service (DDoS) attacks compromising access to critical public ICT infrastructure. This represented an **81.02%** decrease from the previous period, January to March 2024.

Majority of the attacks were targeted at government systems and the health sector. Attackers exploited vulnerabilities in insecure protocols to amplify requests to legitimate servers with the aim of exhausting them such that users were unable to access services.

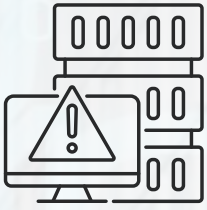


During the period, the perpetrators of the DDoS attacks mainly sought to degrade the quality of services and also to render critical services inaccessible to system users.

To mitigate this risk, the National KE-CIRT/CC carried out cyber awareness for end users and organizations recommending the following actions:

- Implement appropriate out-of-band DDoS detection systems.
- Implement firewalls and intrusion detection systems to detect and mitigate suspicious traffic.
- Use strong passwords for your devices to prevent them from being compromised and used in botnets.
- Keep devices and utilities software up-to-date.

System Attack Trends



Threats Detected

1,065,325,993

22.28%

Advisories Issued

4,694,754

23.23%



April - June 2024

Majority of the attacks were targeted at organisations within the ICT sector. Attackers targeted database servers and operating systems belonging to Internet Service Providers (ISPs) and cloud-based services. Most attackers exploited vulnerabilities in outdated operating systems and leaked user login credentials. The continued prevalence of system vulnerabilities, which is a vector that has long been used by cyber threat actors, may be attributed to the proliferation of Internet of Things (IoT) devices which are inherently insecure.

Top Targeted Systems

- Database Servers
- Operating Systems
- Network Devices
- Web Applications
- Remote Access Systems

Top Affected Industries

- Internet Service Providers
- Cloud Service providers
- Health care sector

Top Targeted Exploits

- Stealer/ Broken Access Controls
- Leakage of Information
- Outdated OS
- Malicious Links
- HTTP Vulnerability
- Remote Code Execution (RCE)

System attacks were targeted at the critical information infrastructure sector that holds sensitive data such as financial information. The objectives of these attacks were to disrupt, compromise and sabotage essential systems and services on a large scale.

To mitigate this risk, the National KE-CIRT/CC recommended the following actions to affected organisations:

- Keep software up to date and apply patches as soon as they are released.
- Use of strong passwords and multi-factor authentication.
- Hardening of firewall configurations.

47th Meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC)

The National KE-CIRT/CC Cybersecurity Committee (NKCC) draws its membership from over 50 public and private sector organisations across various sectors in the country. All NKCC member organisations operate critical information infrastructure (CII). The main objective of the NKCC is to nurture trust networks amongst stakeholders, so as to build capacity and facilitate the sharing of information on new and emerging cybersecurity trends, and to identify a collective strategy to address these emerging issues. The NKCC holds quarterly meetings during which the National KE-CIRT/CC provides updates on emerging threats, tactics, techniques and procedures (TTPs) utilised by diverse threat actors. During these meetings, the various sectoral computer incident response teams (CIRTs) are also granted an opportunity to apprise members on the trends and patterns observed within their respective domains.

During the meeting, members discussed the increased adoption of private cloud services to control critical workloads from cyber threats within the private sector. It was observed that there is an increased uptake of artificial intelligence (AI) technologies to promote business efficiency. Recognising that the private sector controls majority of the critical information infrastructure, members deliberated and agreed that there's need to enhance the sector's cyber readiness and resilience as cybercriminals are now leveraging AI-driven tactics and techniques to compromise systems. As such, collaboration between government entities and private organizations is crucial for protecting and securing these vital assets against cyber threats and other disruptions.

Members were informed that the energy sector continues to work closely with various law enforcement agencies and other industry players to monitor and respond to cyber threats. This multi-agency framework has resulted in the development of sector guidelines and best practices that seek to address specific concerns to inform both reactive and proactive measures to be taken in strengthening the sector's cyber readiness and resilience.

The telecommunications sector reported that the widespread Internet outage recorded in May 2024, which was occasioned by a deep-sea fiber optic cable cut, had a negative impact on the Kenya Internet Exchange Point (KIXP), especially from a cyber security standpoint. Members deliberated and agreed that preventing future recurrence will necessitate the involvement of both preventive measures and effective response strategies. These include enhanced redundancy, proactive maintenance efforts, accurate mapping and enhanced collaboration with all the relevant stakeholders. The 47th Meeting of the NKCC was held on 29th May 2024 at the Safari Park Hotel & Casino, Nairobi.



Participants pose for a photo during the 47th meeting of the National KE-CIRT/CC Cybersecurity Committee (NKCC) in Nairobi.

Updates from the National KE-CIRT/CC

The Kenya Information and Communications Act mandates the Authority to develop a national cybersecurity management framework. Towards this end, the government of Kenya established the Kenya Computer Incident Response Centre - Coordination Centre (National KE-CIRT/CC). This is a multi-agency collaboration framework that is responsible for the national coordination of cyber security and acts as Kenya's national point of contact on cyber security matters.

The National KE-CIRT/CC has been instrumental in coordinating response to cyber threats in partnership with relevant law enforcement agencies, sector regulators, financial institutions and the private sector.

The following is an update on the National KE-CIRT/CC's cybersecurity management activities from April to June 2024:

10th Africa Working Group on Cybercrime for Heads of Units

The Authority took part in the 10th Africa Working Group on Cybercrime for Heads of Units in Abuja, Nigeria. The meeting, which took place from 29th April to 3rd May 2024, was organised by INTERPOL under the Africa Joint Operations Against Cybercrime (AFJOC) Project of the United Kingdom's Foreign, Commonwealth & Development Office (FCDO).

The objective of the meeting was to enhance synergies amongst African countries in order to leverage the opportunities presented by ICTs and to address the challenges facing the continent by mitigating the threats to our communities posed by cybercrime. Participants included the heads of cybercrime units and representatives from national computer incident response teams (CIRTs) drawn from across the continent.

During the meeting, Kenya was lauded as a trailblazer in Africa with regard to the advancement of the cybersecurity considering that many other countries on the continent are yet to establish national Computer Incident Response Teams (CIRTs) and are also yet to enact cybersecurity and data privacy laws and regulations.

Commonwealth Telecommunications Organisation (CTO) Digital Week 2024

The Authority took part in the 3rd edition of the Commonwealth Telecommunications Organisation (CTO) Digital Week, that was held from 20th to 24th May 2024 in London, UK. This forum is aimed at supporting the digital transformation goals of member states. The CTO Digital Week 2024 brings together members from across the Commonwealth and stakeholders in the technology sector to assist in establishing an enabling environment for and effectively adopting ICTs for global socio-economic development.

The focus for Digital Week 2024 was on cybersecurity, as espoused in the theme, "Building a Secure Digital Future". The main objective of the forum was to increase cybersecurity awareness in a world that is undergoing rapid digital transformation. Participants at the forum were drawn from senior government officials, international organisations, ICT regulators, law enforcement officers, amongst others.

The CTO also provides capacity building and policy development assistance to member states to enhance their telecommunications infrastructure and regulatory frameworks.

Judicial Dialogue on Mobile Technology and Emerging Jurisprudence in the Digital Arena

The Authority in its Strategic Plan (2023 - 2027), has committed to undertake capacity building exercises to enhance consumer protection and empowerment, by creating awareness on the ICT regulatory framework. In furtherance to this objective, the Authority in conjunction with the Kenya Judiciary Academy (KJA), the Lawyers Hub, Safaricom PLC and Airtel Kenya Ltd., hosted a capacity building programme themed, "Judicial Dialogue on Mobile Technology and Emerging Jurisprudence in the Digital Arena," targeted at judicial officers.

The objective of the capacity was to: enhance the understanding and appreciation of judges and judicial officers on GSM technology; provide technical insights and case studies that illustrate the intricacies of prosecuting tech-related fraud within the Kenyan legal framework; provide insights into cyber security, cryptocurrency, emerging technologies and data protection; discuss emerging jurisprudence in the mobile money and digital arena; and to facilitate the sharing of knowledge and experiences amongst judges and judicial officers involved in the mobile technology and digital arena on identification of challenges that affect service delivery and areas of collaboration.

The programme was conducted in two cohorts. The first cohort, targeting magistrates, was held from 6th to 8th June, 2024 in Naivasha. The second cohort, targeting judges, was held from 19th to 21st June 2024 in Mombasa. Over 100 judges and judicial officers were trained during the programme.



Participants from the first cohort that consisted of magistrates pose for a photo at the Lake Naivasha Sawela Lodge, Naivasha, following the official opening on 6th June 2024.



Participants from the second cohort that consisted of judges pose for a photo at the Sarova Whitesands Beach Resort & Spa, Mombasa, following the official opening on 19th June 2024.

Kenya Set to Benefit in Cyber Security Collaboration with the United States



His Excellency President William Ruto (second right) responding to questions from journalists during a joint press conference with President Joe Biden (extreme right) of the United States on 23rd May 2024, at the White House in Washington DC.

Kenya continues to seek strategic engagements with various international partners in areas that cut across cybersecurity governance, capacity and capability development, information sharing and cyber incident response. In recognition of this, collaboration in the field of cyber security was a key agenda during His Excellency President William Ruto's state visit to the United States in May 2024.

The United States and Kenya, in collaboration with the Software Engineering Institute (SEI), plan to hold a regional event in October 2024 dubbed, "The Kenya Regional Cyber Sector Collaboration Symposium". The event is aimed at enhancing information sharing between cybersecurity incident response teams to enable a more resilient cyberspace in East Africa. These trust networks will help countries within the region to better anticipate, identify and mitigate potential cyber threats by facilitating the exchange of information about vulnerabilities, attack patterns and threat intelligence. The SEI is based at the Carnegie Mellon University (CMU) in Pittsburgh, Pennsylvania, United States.

Similarly, the U.S. Trade and Development Agency (USTDA) also announced two upcoming reverse trade missions to introduce public and private sector representatives from Kenya and Tanzania to the latest U.S. technologies, services and financing solutions for last-mile connectivity and cybersecurity. Both reverse trade missions are focused on expanding internet access and improving cybersecurity governance, while increasing the likelihood that these digital transformation projects are implemented using U.S. technologies and services.

Future Insights on Cybersecurity

Cyber security researchers predict that the global cost of cybercrime could surge to over \$25 trillion over the next 3 years. The impact of even one security breach could be mission critical, causing massive financial loss and reputational damage. To alleviate the effects of data breaches, organisations should focus on the development of standards on data protection, disclosure requirements for data breaches, cybersecurity risk assessments, amongst others.

Social engineering is an attempt to trick a user into revealing information, such as a username and password, that can be used to attack systems or networks. One concern attributed to the increasing sophistication of phishing attacks is the use of artificial intelligence (AI) technologies by threat actors. For instance, AI technologies can generate more credible phishing emails to deceive unsuspecting users. On the other hand, cyber security teams could leverage AI technologies in conducting risk assessment to assist in the discover of system vulnerabilities.

Ransomware is a type of malicious attack where attackers encrypt an organisation's data and demand payment of ransom to restore access. The average ransomware demand globally is estimated to be approximately \$2 million, with some demands exceeding \$10 million. Afflicted organisations are estimated to lose an average of 21 days of operations whether or not they pay the ransom. Other costs include financial losses and regulatory sanctions. To counter the threat of ransomware, organisations should implement proactive measures such as regular data backups, employee capacity building, antivirus and anti-malware software solutions, timely software updates and patching, network segmentation and the adoption of robust access controls and authentication protocols.

Over the next 3 years, it is predicted that close to 8 billion smartphones will be in use worldwide. Fake apps have infiltrated app stores and other online repositories, such that when downloaded onto devices, can compromise mobile devices thus giving criminals control of accounts and access to sensitive data. Besides reporting these suspicious apps, users should only download apps from official app stores, inspect the permissions before installing any app, review the apps privacy policy, keep their devices updated, etc.

The COVID-19 pandemic saw a rise in remote work globally. Employees at remote locations may be using outdated routers and personal devices that may be vulnerable or connecting to unsecured Wi-Fi networks. Device management at scale is a significant challenge for organisations. Organisations therefore need to implement policies to manage personal devices in the workplace to enhance productivity while protecting sensitive information.

Public cloud services may be more secure than on-premise services, given that the reputable cloud service providers have invested heavily on security infrastructure, training of support personnel, and research and development. Nevertheless, cloud-security technology alone may not provide adequate protection since attackers may target the identity holder rather than the service provider to steal log-in credentials or other sensitive data. Organisations can therefore deploy a hybrid cloud service model that combines on-premises infrastructure with public cloud services, to provide greater flexibility, allowing them to optimise their existing infrastructure while taking advantage of the scalability and cost-effectiveness of public cloud services.

In conclusion, the threats that cybersecurity risks pose to organisations are not static. Rather, they evolve over time, becoming more prevalent and increasingly sophisticated. Since these risks are ever present and changing, more can always be done to minimise vulnerabilities and strengthen defences including review of existing legal and regulatory frameworks that always seem to lag behind technological advancements.

Thank You

We're here to help. Report an incident.

Working round the clock to safeguard Kenya's cybersecurity landscape.



Email

incidents@ke-cirt.go.ke



Hotlines

+254 703 042700

+254 730 172700



Website

www.ke-cirt.go.ke

Social Media



@KeCIRT