Report

KENYA
Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

Top Takeaways

Sector-Specific Targeting: The public administration, information, and finance sectors are the primary targets in Kenya's cyber threat landscape, collectively accounting for over 43% of observed incidents. This focus highlights the increasing risk to critical infrastructure and financial systems.

Geographical Focus: Kenya remains a primary target for cybercriminals, with 69.1% of threats directed solely at the country. However, 30.9% of attacks affect Kenya alongside other nations, indicating the regional scope of threat actor operations.

Ransomware Threats: Manufacturing is the top sector targeted by ransomware, representing over a quarter of ransomware incidents. LockBit variants dominate ransomware activities, with a combined share of 22.74%, indicating the sophistication and persistence of these threat actors.

Phishing Attacks: National Security and International Affairs sectors are highly targeted by phishing attacks (50%), reflecting the value of sensitive government information. Banking follows with 21.43%, signaling continued efforts by cybercriminals to exploit financial institutions.

Evolving Phishing Techniques: Phishing pages largely rely on generic or ambiguous titles (61.19%), making it difficult for users to immediately recognize malicious intent. However, titles such as "Sign in to your account" and "Redirecting..." suggest an increasing focus on user credentials and data harvesting.

HTTPS Adoption in Phishing: Despite the growing use of HTTPS (56.7%) in phishing domains, a significant portion (43.3%) still operates on HTTP. This emphasizes the need for users to scrutinize URLs and not rely solely on secure connection indicators.

Diverse Threat Activity: Threat actors are not confined to one type of attack. Data/database compromises are the most prevalent attack type (61.8%), followed by access-related threats (21.1%), and website disruptions (14.5%). This variety reflects the multifaceted nature of the threat landscape and the need for a multi-layered defense strategy.

Technical Details

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around Kenya.

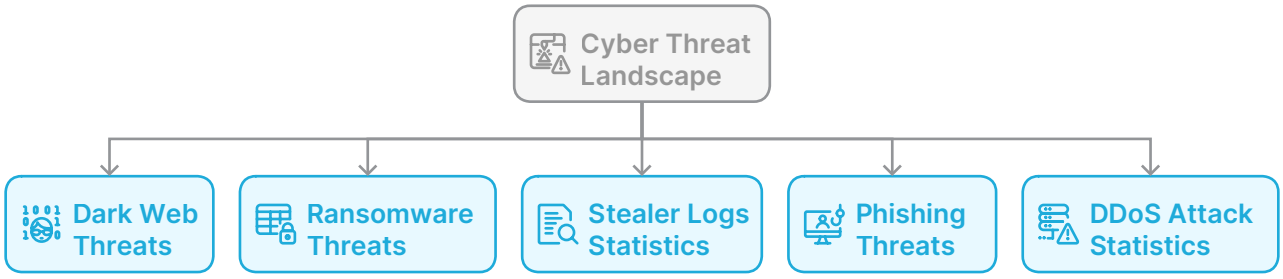
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups and so on. These are areas where threat actors with various skill sets come together, discuss, share tools and publish their alleged cyber attacks.

In the Ransomware Threats chapter you will find detailed information about ransomware actors targeting Kenya, their detailed profiles and the necessary data that summarizes the ransomware activities.

Stealer Logs Statistics chapter is all about stealer malware and the data around leaked credentials. These days, hackers don't hack, they log in. It is important to make sure that employee credentials are not compromised.

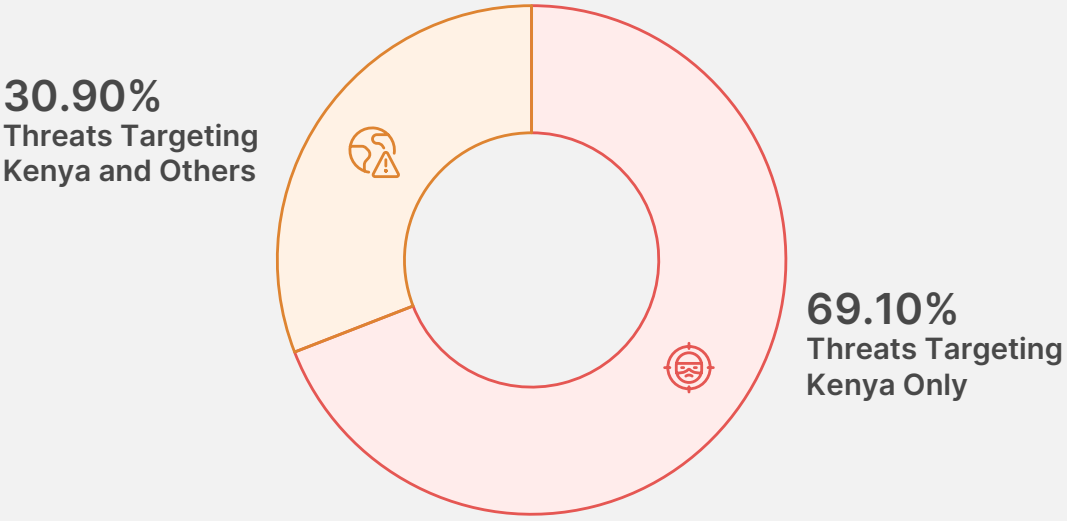
The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

And lastly, the DDoS Attack Statistics shows you the latest information about the intensity of DDoS attacks and how threat actors target organizations to disrupt their operations.



Dark Web Threats

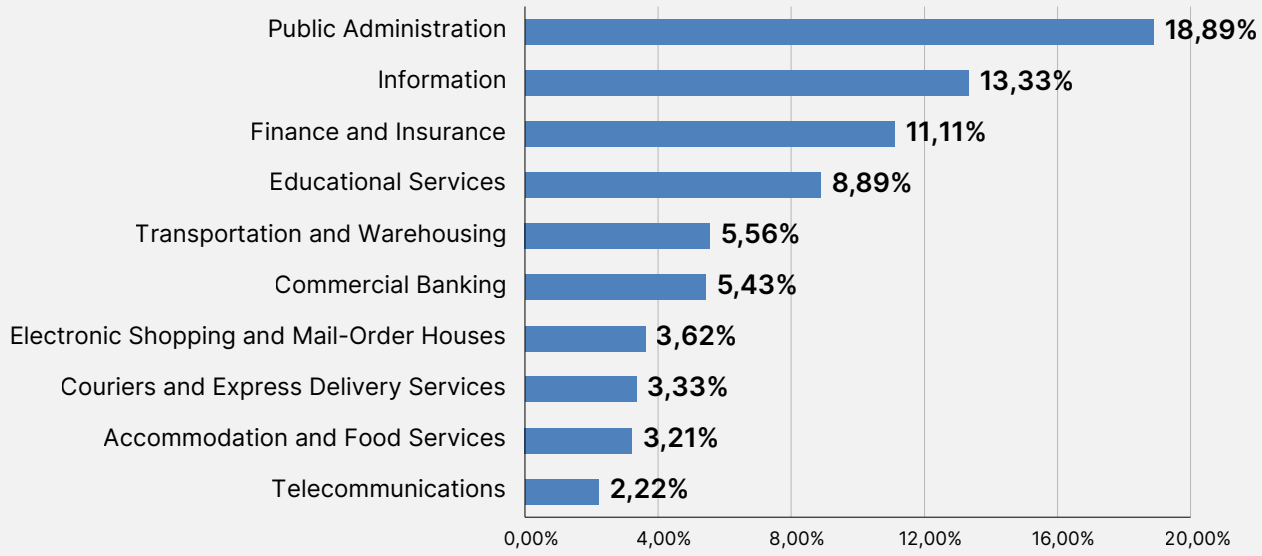
Distribution of Dark Web Threats by Country



A significant majority (69.1%) of observed threats specifically target Kenya, underscoring the country's prominence in the regional cyber threat landscape. This focus likely reflects Kenya's growing role as an economic and technological hub in East Africa.

Meanwhile, 30.9% of threats target Kenya alongside other countries, suggesting coordinated or broad campaigns by threat actors across the region. The high specificity of attacks on Kenya highlights the need for localized threat intelligence and sector-specific security strategies.

Distribution of Dark Web Threats by Industry



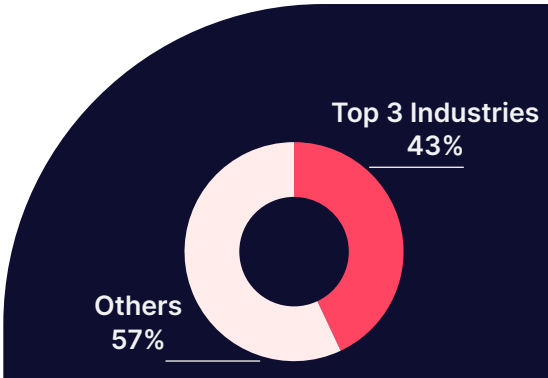
Public Administration emerges as the most targeted industry, accounting for 18.89% of the threats, highlighting the increasing interest of threat actors in critical government operations and data.

The Information sector follows at 13.33%, likely due to the digital transformation and data-centric services it offers.

Finance and Insurance sectors rank third at 11.11%, reflecting the persistent focus on financial gains through fraud, data theft, or ransomware campaigns.

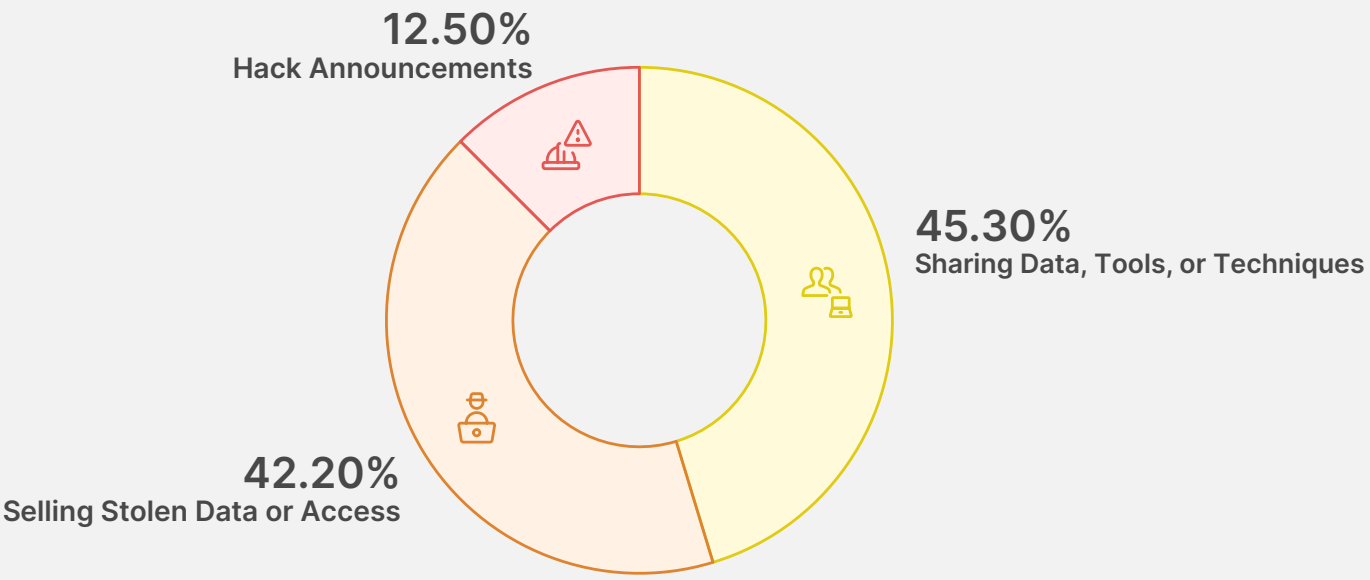
Together, these top three sectors account for over 43% of observed threats, indicating the concentration of risk in areas critical to national stability and economic development.

Lower, yet still notable, threats are seen in Educational Services (8.89%) and Transportation and Warehousing (5.56%), possibly driven by the rising use of digital systems for learning and supply chain logistics. Threat actors may also be pivoting toward commercial sectors, such as Electronic Shopping (3.62%) and Couriers (3.33%), as e-commerce continues to grow in the region.



Together, these top three sectors account for over **43%** of observed threats, indicating the concentration of risk in areas critical to national stability and economic development.

Distribution of Dark Web Threats by Threat Categories



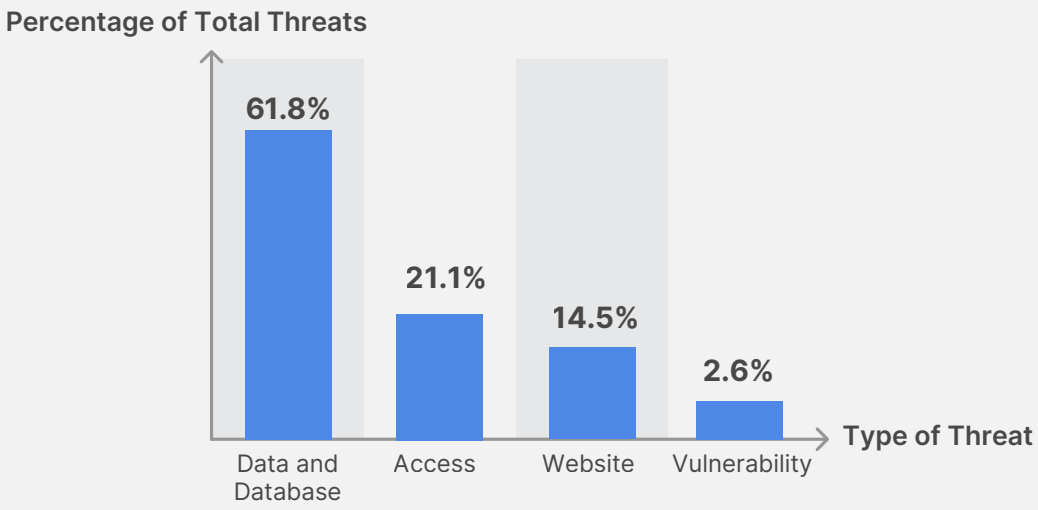
The majority of threat actor activities (45.3%) involve sharing data, tools, or techniques, potentially fueling further attacks by other malicious actors.

Closely following, 42.2% of the threats involve the selling of stolen data or access, indicating a thriving underground market targeting Kenyan entities.

Hack announcements account for 12.5%, often signaling recent breaches and serving as a warning for possible follow-up exploitation.

The dominance of sharing and selling highlights the dynamic and collaborative nature of the cybercriminal ecosystem.

Distribution of Dark Web Threats by Threat Types

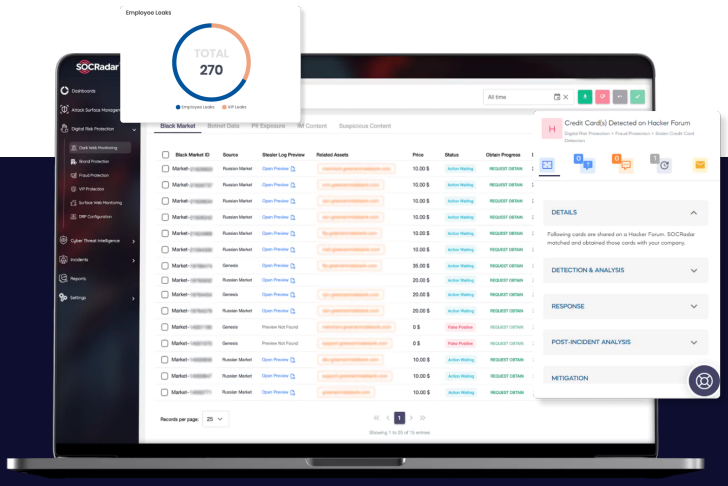


Data and database compromises dominate at 61.8%, indicating a strong attacker focus on exfiltrating sensitive information from Kenyan organizations.

Access-related threats follow at 21.1%, reflecting attempts to sell or exploit unauthorized access to systems, often facilitating further malicious activities.

Website-related threats account for 14.5%, targeting the digital presence of businesses for defacement, phishing, or malware distribution.

Vulnerability-related threats are minimal (2.6%), suggesting a lower emphasis on exploit development but underscoring the importance of proactive patch management to mitigate risks.



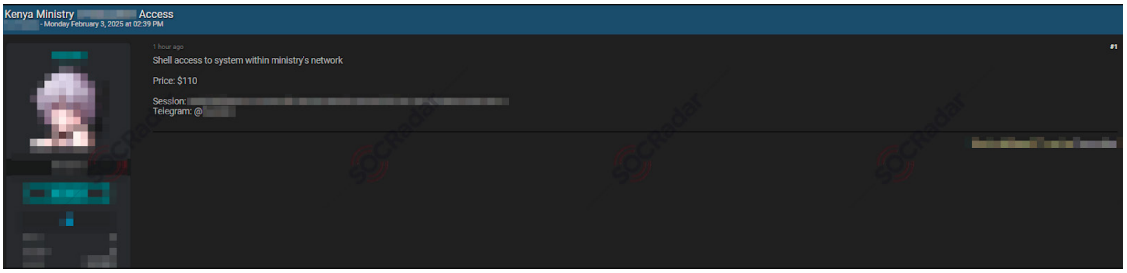
SOCRadar's Advanced Dark Web Monitoring

SOCRadar's Advanced Dark Web Monitoring provides Kenyan organizations with critical insights into hidden threats targeting their sectors, including Retail Trade, finance, and Insurance, which have faced significant risks over the past year. With real-time tracking of underground chatter and sensitive data exposure, SOCRadar enables proactive defense against Dark Web threats.

Activate your *free demo today* to safeguard your organization's most valuable assets.

Recent Dark Web Activities Targeting the Entities in Kenya

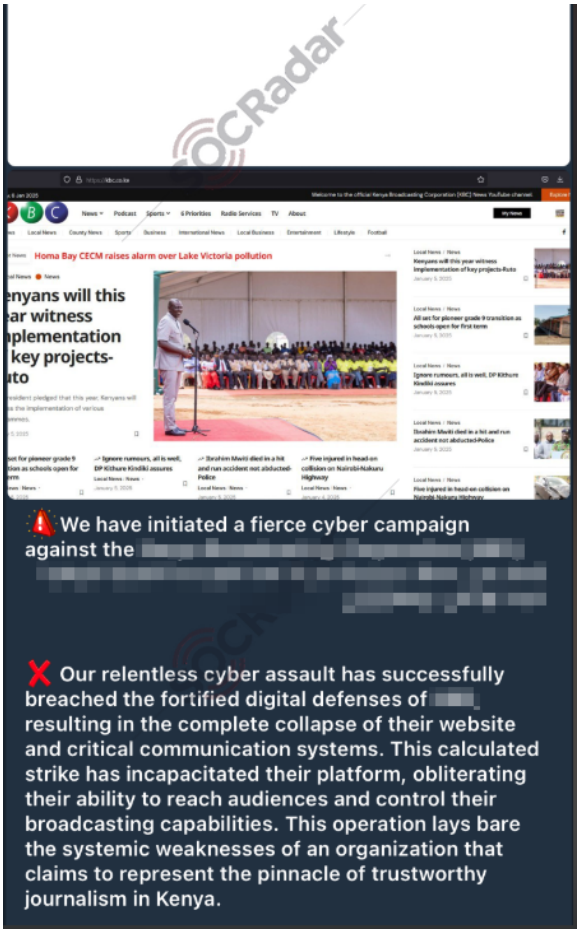
Alleged Unauthorized Access to a Network of a Ministry from Kenya Listed for Sale



SOCRadar has identified a concerning listing on a hacker forum, where unauthorized shell access to a network of a Ministry in Kenya is being offered for sale. The seller claims to have access to a system embedded in the ministry's infrastructure, raising potential cybersecurity risks for sensitive government data.

The asking price for the shell access is $110, a relatively low cost that could attract a wide range of buyers with malicious intent. The nature of the access and the specific system compromised have not been disclosed, but such breaches can lead to data theft, espionage, or further exploitation of government networks.

Anonymous Sudan Conducted DDoS Attack on a Broadcasting Company

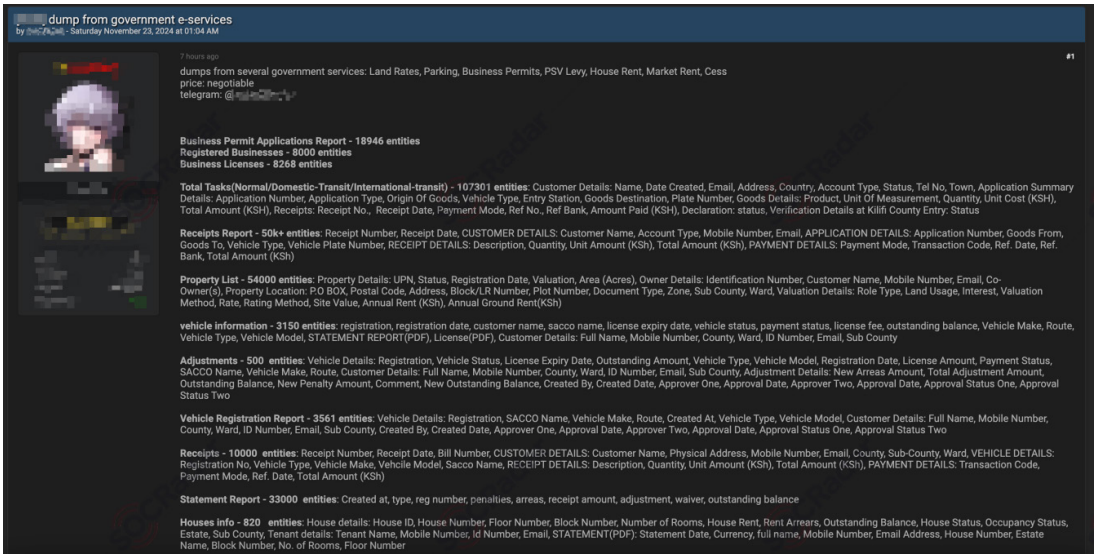


SOCRadar has detected an announcement on Anonymous Sudan's Telegram channel claiming responsibility for a Distributed Denial-of-Service (DDoS) attack targeting a broadcasting company in Kenya. The group declared the launch of a "fierce cyber campaign" against the company, stating that their assault successfully breached the organization's digital defenses.

According to the statement, the attack led to the collapse of the company's website and critical communication systems, severely disrupting its broadcasting capabilities. Anonymous Sudan described the operation as a calculated effort to expose what they allege are systemic vulnerabilities within the company's infrastructure.

The group provided multiple links as proof of the attack, showing the service disruptions. They also issued a warning, demanding accountability for any repercussions on Kenya's network integrity and potential collateral damage from the operation.

Alleged Data of a Government E-Service is on Sale



SOCRadar has identified a data breach incident on a hacker forum, where an alleged data dump from a county government's e-services is being offered for sale. The listing includes sensitive information from several government services, such as land rates, parking, business permits, PSV levies, house and market rents, and vehicle registrations.

The seller has not specified a fixed price, labeling it as negotiable, and has provided a Telegram contact for potential buyers.

The leaked data reportedly contains detailed records, including:

Business Information: Over 18,000 business permit applications, 8,000 registered businesses, and 8,200 business licenses, with customer names, contact details, application summaries, and financial transactions.

Property Records: A database of 54,000 properties, including owner identification numbers, property valuations, and registration details.

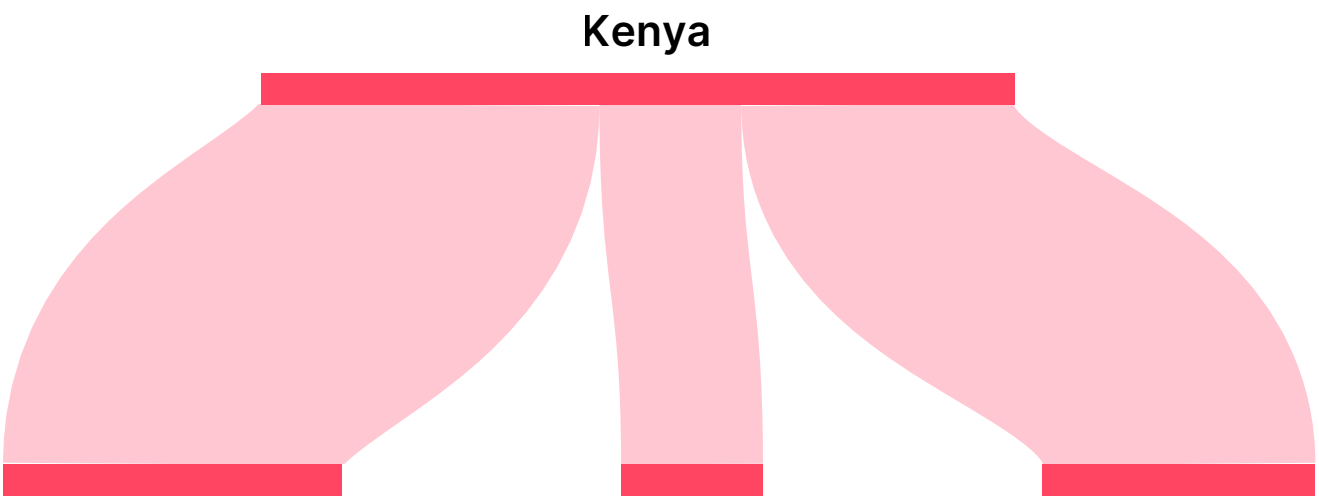
Vehicle Data: Information on more than 3,500 registered vehicles, including ownership details, license statuses, payment records, and route data.

Financial Reports: Over 50,000 receipt entries with transaction details, payment methods, and customer information.

Housing and Market Data: Details on over 800 housing units and 4,000 market stalls, including rent arrears, tenant information, and payment statuses.

Ransomware Threats

Distribution of Ransomware Attacks by Country



44.93%

Interestingly, in 44.93% of incidents, Kenya was not the main target but still affected, showing the spillover effects of global ransomware operations.

18.84%

In 18.84% of cases, Kenya was the primary target alongside other nations, indicating coordinated regional campaigns.

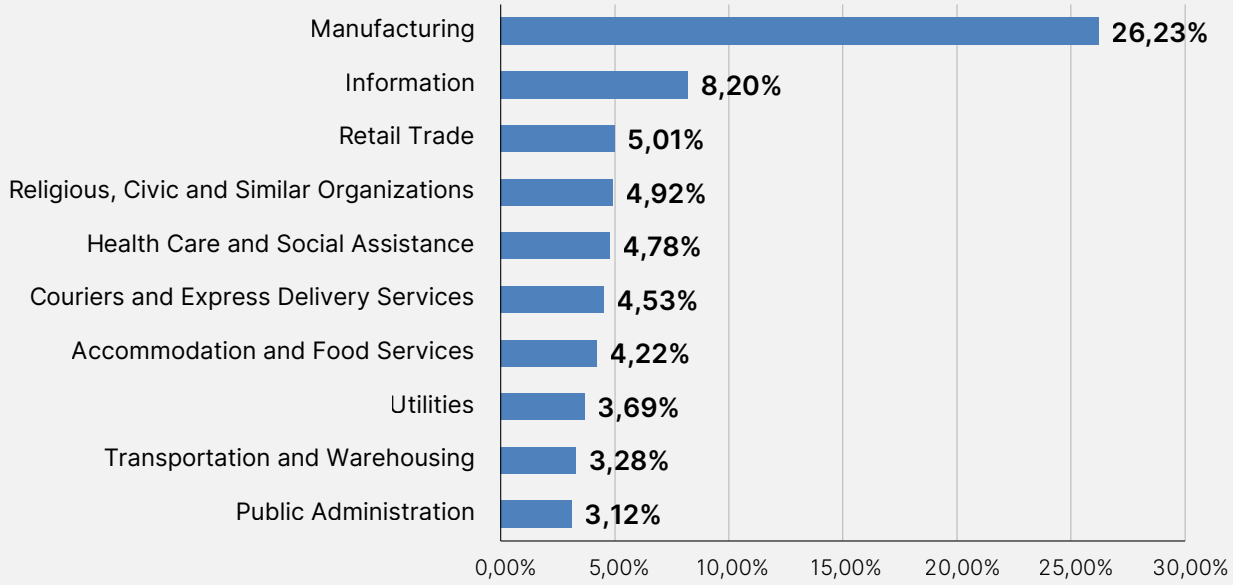
36.23%

Kenya was the exclusive target in 36.23% of ransomware incidents, highlighting the country's direct appeal to attackers.

The collateral impact of shared vulnerabilities stemming from the use of similar technologies and systems is a serious threat for organizations worldwide. Threat actors might not be after your organization specifically but as soon as they find a vulnerability, they will target every organization they can.

This underscores the importance of threat monitoring and collaboration in defending against ransomware campaigns.

Distribution of Ransomware Attacks by Industry



Manufacturing is the most targeted sector for ransomware attacks, accounting for 26.23% of incidents.

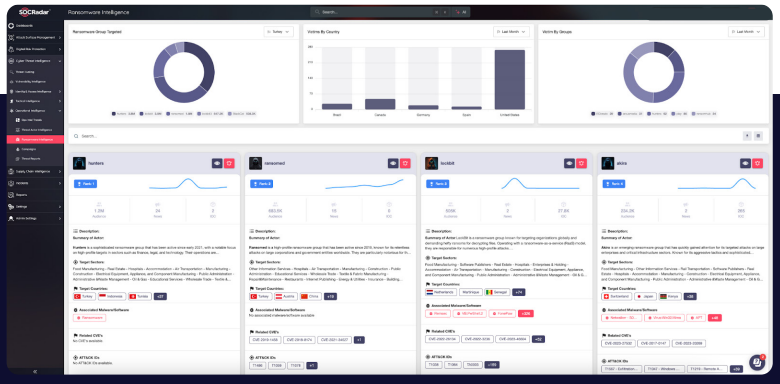
This aligns with global trends where attackers exploit the sector's reliance on operational continuity.

The Information sector ranks second at 8.20%, reflecting attackers' interest in disrupting or monetizing data-driven operations.

Retail Trade follows at 5.01%, likely due to the financial incentives associated with transactional data.

Notably, sectors such as Religious and Civic Organizations (4.92%) and Health Care (4.78%) are increasingly being targeted, highlighting a concerning trend where essential services and non-profits face operational and reputational risks.

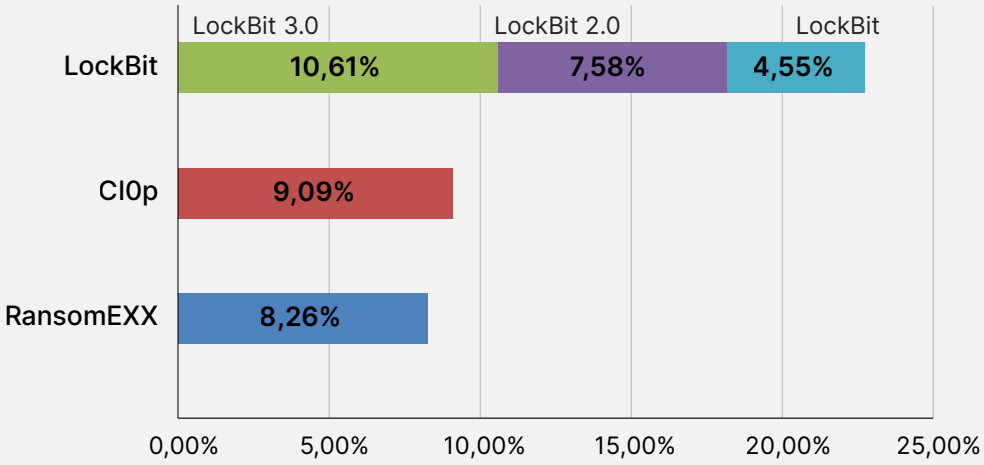
The broad spread of attacks across multiple industries underscores the need for ransomware-specific defenses across diverse sectors.



SOCRadar's Ransomware Intelligence Module

Explore *SOCRadar's Ransomware Intelligence module* and gain comprehensive insights with detailed group profiles, MITRE Visualizer, and actionable IOCs. These insights will empower you to stay ahead of evolving threats and enhance your cybersecurity strategy.

Top Ransomware Groups Targeting Kenya



In total, these three threat actors are equal to the 40% of ransomware attacks targeting Kenya.

LockBit remains the dominant ransomware operator, with its variants (LockBit 3.0, LockBit 2.0, and LockBit) collectively accounting for 22.73% of observed incidents.

Cl0p follows at 9.09%, known for high-profile data extortion campaigns.

RansomEXX ranks third at 8.26%, indicating its growing presence and targeting capabilities.

These top three operators collectively highlight the evolving sophistication of ransomware threats targeting Kenyan organizations.

A Closer Look into The Top 3 Ransomware Groups

LockBit

LockBit 3.0, succeeding LockBit and LockBit 2.0, functions as a Ransomware-as-a-Service (RaaS) entity.

Since January 2020, LockBit has transitioned to an affiliate-based model, employing diverse methodologies to target businesses and critical infrastructure entities. Noteworthy tactics include double extortion and the utilization of initial access broker affiliates, alongside recruitment efforts involving insiders and hacker recruitment competitions.

With over 1,500 victim disclosures on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's cessation. As of the first quarter of 2023, they retain their position as the most prolific group, with over 300 disclosed victims.

You can visit our *blog post* for more detailed Lockbit 3.0 Ransomware Group information.

Cl0p

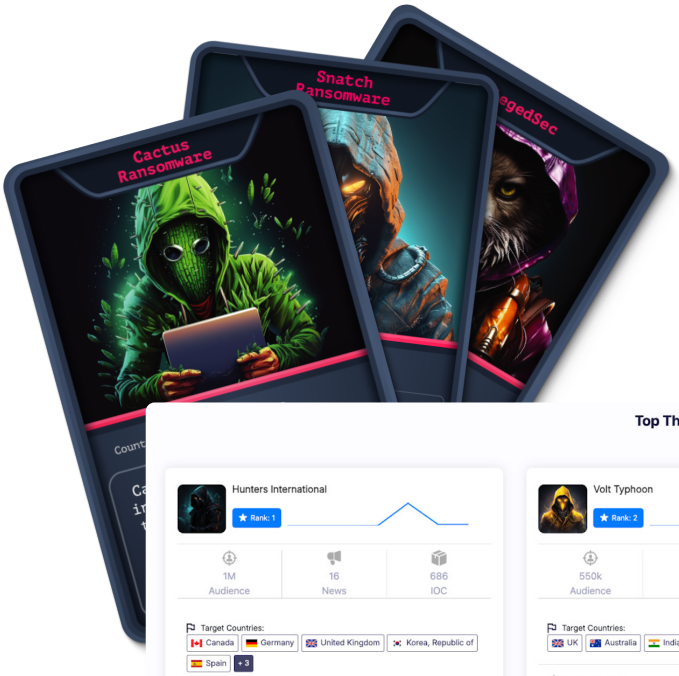
Cl0p, a member of the well-known Cryptomix ransomware family, is a dangerous file-encrypting malware that intentionally exploits vulnerable systems and encrypts saved files with the ".Clop" extension. The name of the threat actor comes from the Russian word "klop," which means "bed bug," a Cimex-like insect that feeds on human blood at night (mosquito). A distinguishing feature of Cl0p is the string "Don't Worry C|0P" found in the ransom notes.

On June 16, 2021, in a coordinated international effort involving law enforcement agencies from various countries, authorities arrested numerous individuals suspected of affiliation with the Cl0p ransomware gang. Despite this operation, the ransomware group grabbed attention a few days later by releasing data acquired from new victims.

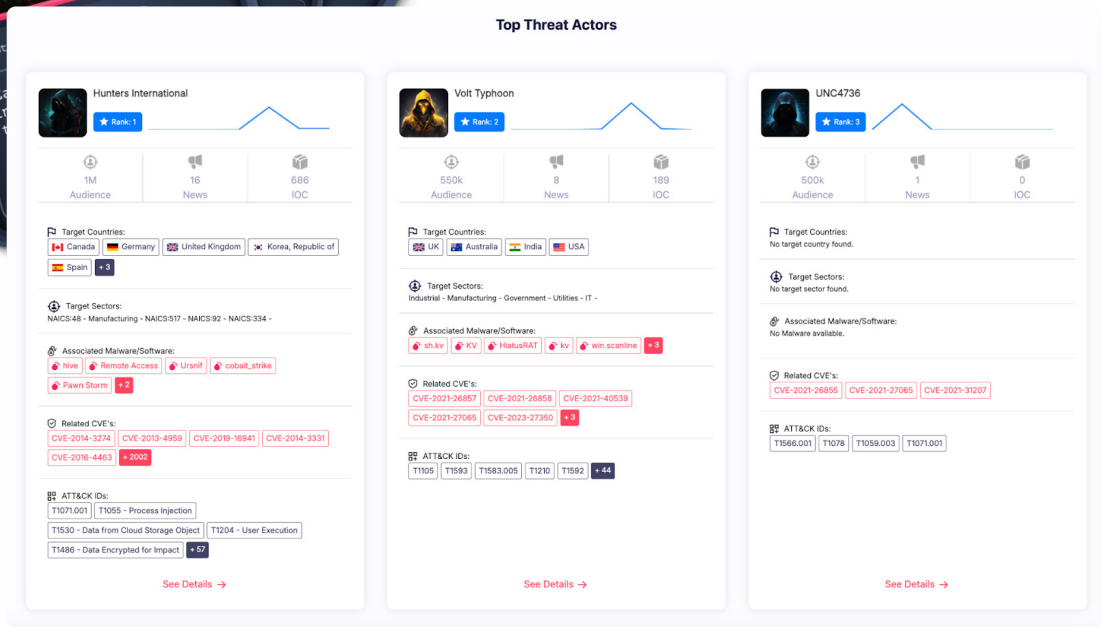
You can visit our *blog post* for more detailed information about the Cl0p Ransomware Group.

RansomEXX

Since late 2020, security researchers have tracked RansomEXX, also known as Defray or Defray777. This threat actor has successfully attacked major organizations including the Texas Department of Transportation and Groupe Atlantic. The malware comes in two versions - one for Windows systems and another for Linux systems. Unlike some ransomware groups that attack indiscriminately, RansomEXX is known for carefully selecting a limited number of specific targets.



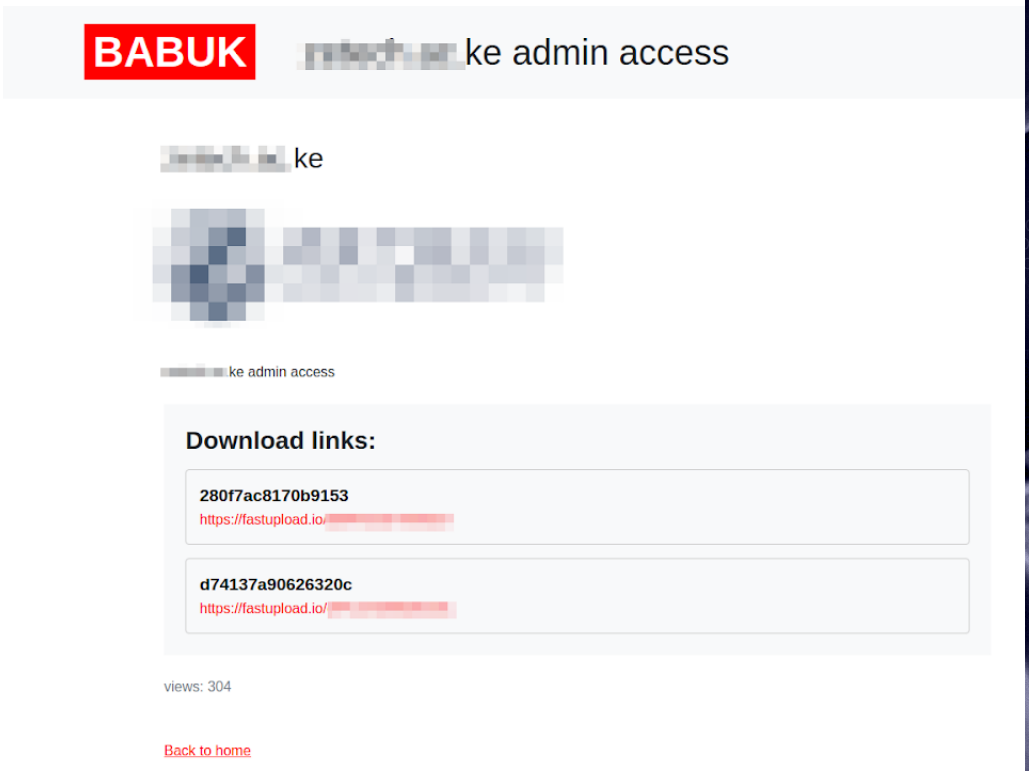
SOCRadar enhances cybersecurity measures with its *Threat Actor Intelligence Module*, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.



SOCRadar Labs - Threat Actor Page

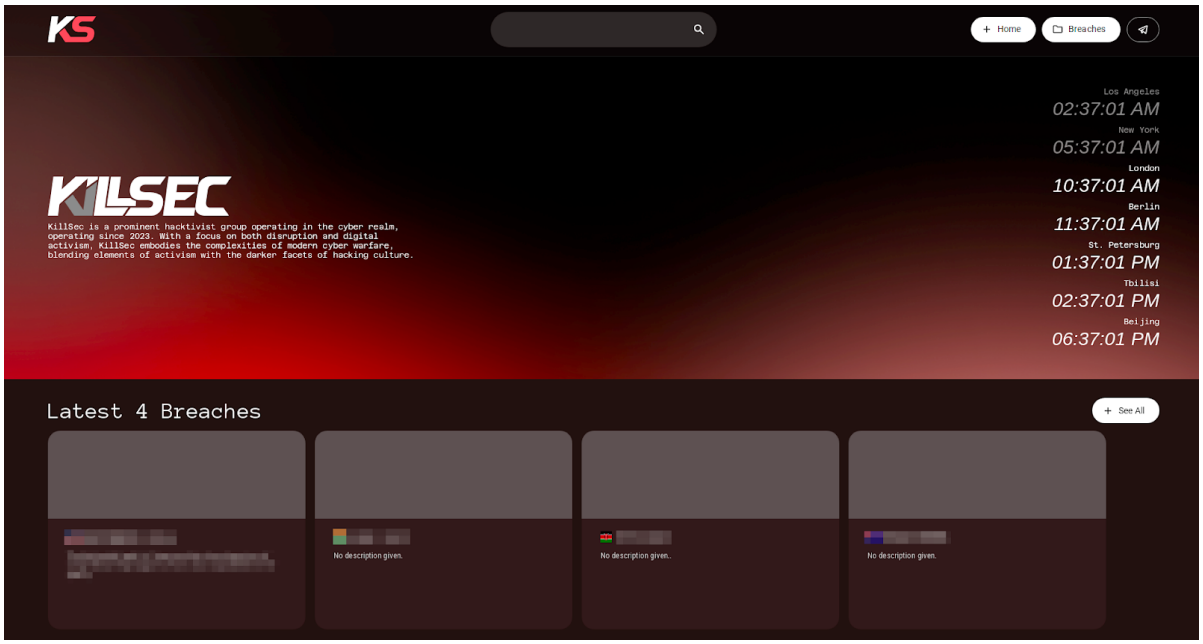
Recent Ransomware Attacks Targeted Entities in Kenya

babuk Ransomware Targeted a University in Kenya



In the babuk ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as a higher education institution.

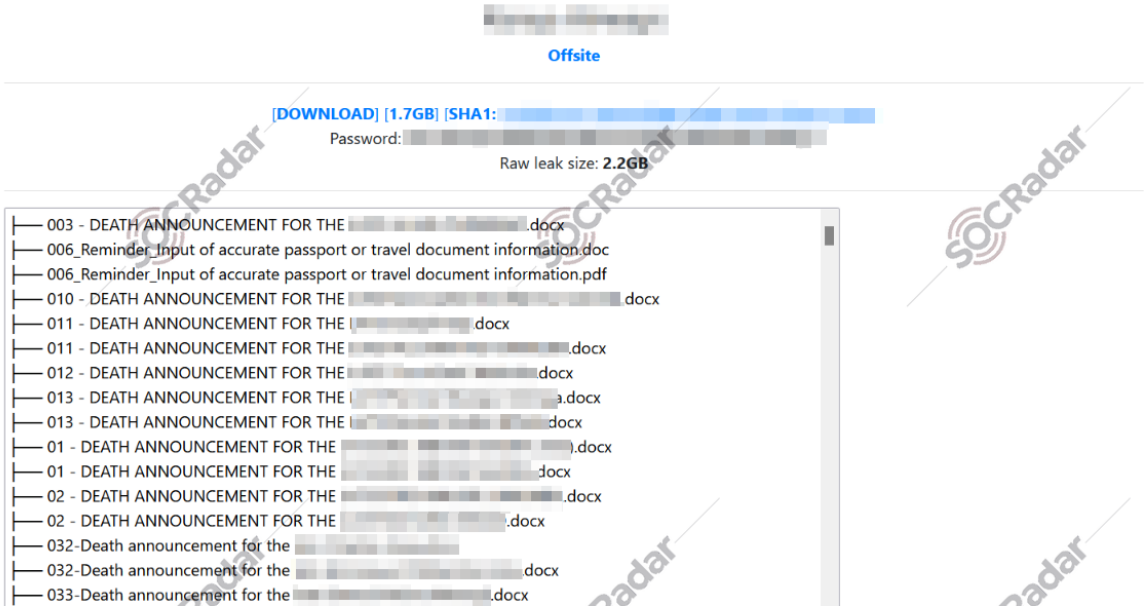
One of KillSec's Victims is Allegedly an IT Company from Kenya



In the killsec ransomware group website monitored by SOCRadar, a ransomware victim from Kenya was announced. The allegation is about an IT firm located in Kenya.

The threat actor didn't share any additional information about their allegation.

RansomExx Ransomware Group Leaked the Data of an Airline Company from Kenya



In the RansomEXX ransomware group website monitored by SOCRadar, a data leak detected allegedly belongs to an airline company from Kenya.

The leak, which was published on December 30, 2023, reportedly contains sensitive information related to the airline, including accident reports, identification documents, case files, passport details, and records concerning staff incidents and deaths.

The leaked data is available for download, with a compressed file size of 1.7 GB and a raw leak size of 2.2 GB. The post includes a password for access.

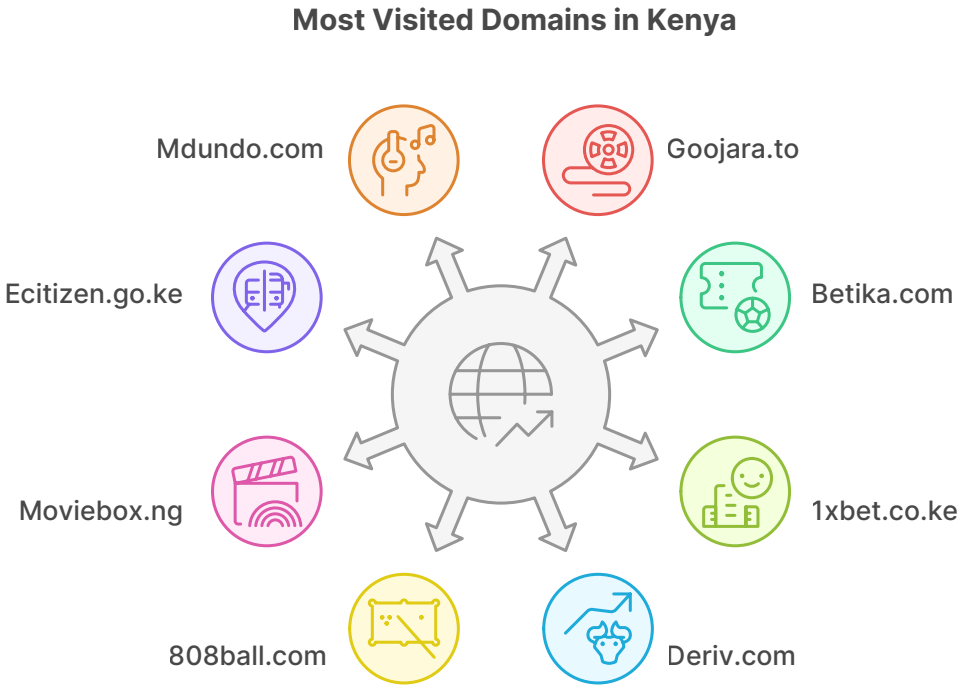
Stealer Log Statistics

Stealer Log Statistics: Top Domains in Kenya

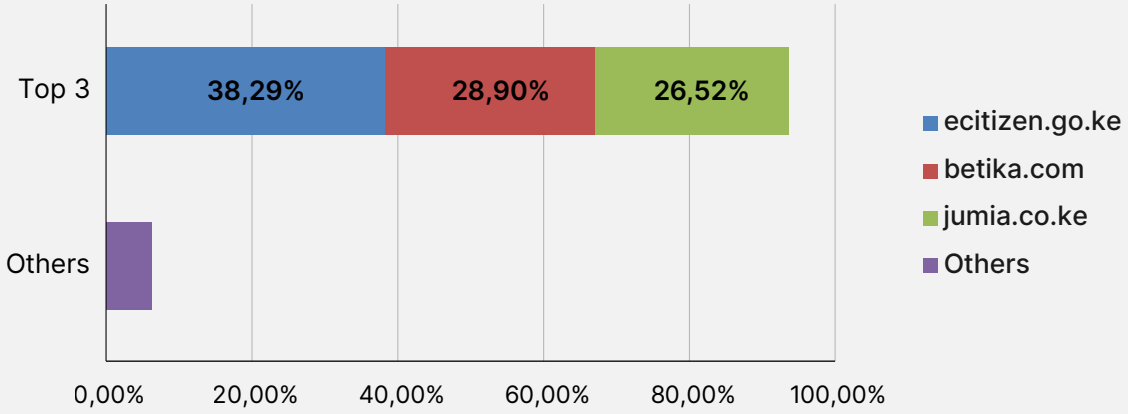
Stealers are a type of tool that collects sensitive data from victims' systems, primarily targeting login credentials, session tokens, and personal information. These logs, often produced by malicious software such as info stealers or keyloggers, can contain detailed information about the websites users visit, their login activities, and the credentials they input. Attackers use stealer logs to harvest credentials, gain unauthorized access to accounts, and orchestrate further attacks, including fraud, identity theft, or lateral movement within a network.

Monitoring and analyzing stealer logs is critical for identifying active threats and understanding attacker behavior, as these logs reveal which platforms are being targeted and how attackers are exploiting victims' data. By tracking these logs, organizations can gain valuable insight into high-risk domains, detect compromised accounts early, and implement targeted defensive measures to mitigate damage.

In order to detect these logs, it is useful to check the most visited domains in a specific country or industry. We analyzed the logs from the following domains in order to identify the leaked credentials that can be used to attack organizations in Kenya.



Stealer Logs - Distribution of the Compromised Data by Domains



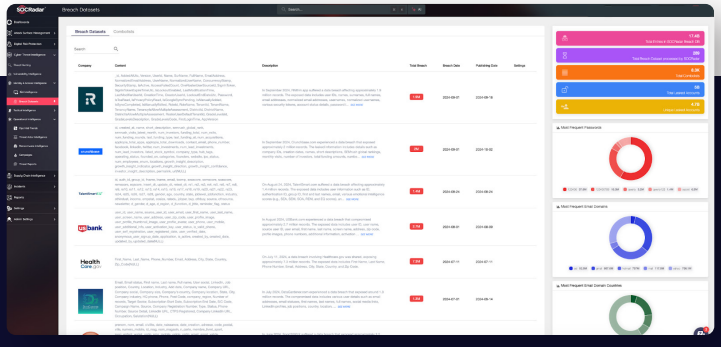
The data reveals that ecitizen.go.ke holds the largest share of stealer logs at 38.29%, followed closely by betika.com and jumia.co.ke, with 28.90% and 26.52%, respectively.

This concentration suggests a targeted focus on high-traffic platforms—betting, e-government services, and e-commerce—where compromised credentials hold significant value.

The remaining 6.29% is distributed across various other domains, indicating a broader but less intensive targeting strategy. The prominence of ecitizen.go.ke highlights potential risks to sensitive governmental data, while the targeting of betika.com and jumia.co.ke reflects the appeal of financial and personal user information.

The top three most visited domains in Kenya account for more than 90% of the stealer logs data collected from the country's ten most visited domains.

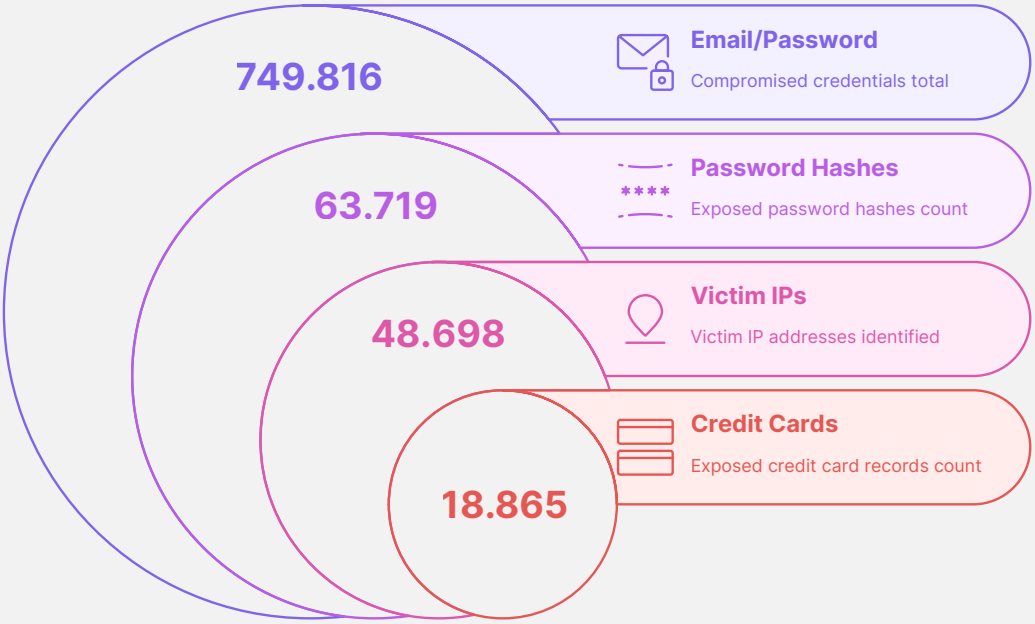
It's important to note that stealer logs are collected from compromised user devices, not from the websites or companies behind those domains. This data should not be interpreted as a breach of these domains. Instead, it indicates that user devices were infected, and threat actors harvested the exposed data from those compromised systems.



SOCRadar's Identity & Access Intelligence Module

SOCRadar's Identity & Access Intelligence Module can detect stealers on your devices and identify their location, facilitating a secure working environment. Changing passwords without eliminating stealers is insufficient to secure your organization, as it will only provide new passwords to threat actors.

Stealer Logs - Distribution of the Compromised Data



The data indicates a significant exposure of credentials, with nearly 750,000 e-mail/password combinations compromised, highlighting the primary focus of stealers on account takeover opportunities.

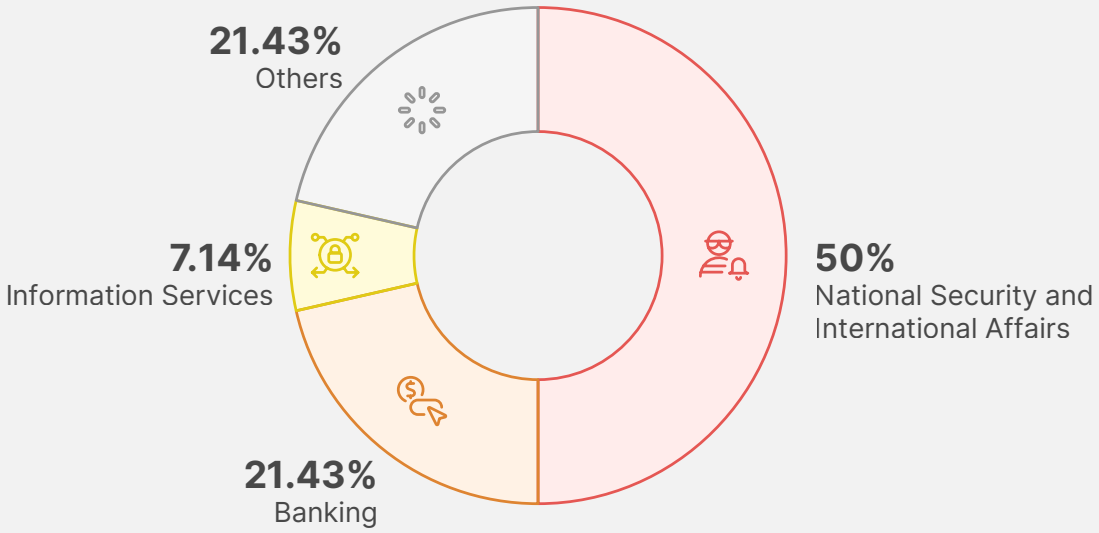
In comparison, 63,719 password hashes were exposed, suggesting that while some platforms implement hashing, plaintext credentials remain a major vulnerability.

The presence of over 48,000 victim IP addresses provides attackers with valuable context for further exploitation, such as geolocation tracking or tailored phishing campaigns.

Additionally, the exposure of 18,865 credit card records underscores the financial motivation behind many of these attacks, though it represents a smaller share compared to credential theft.

Phishing Threats

Phishing Attacks - Distribution by Industry



National Security and International Affairs sectors bear the brunt of phishing attacks, accounting for 50% of incidents.

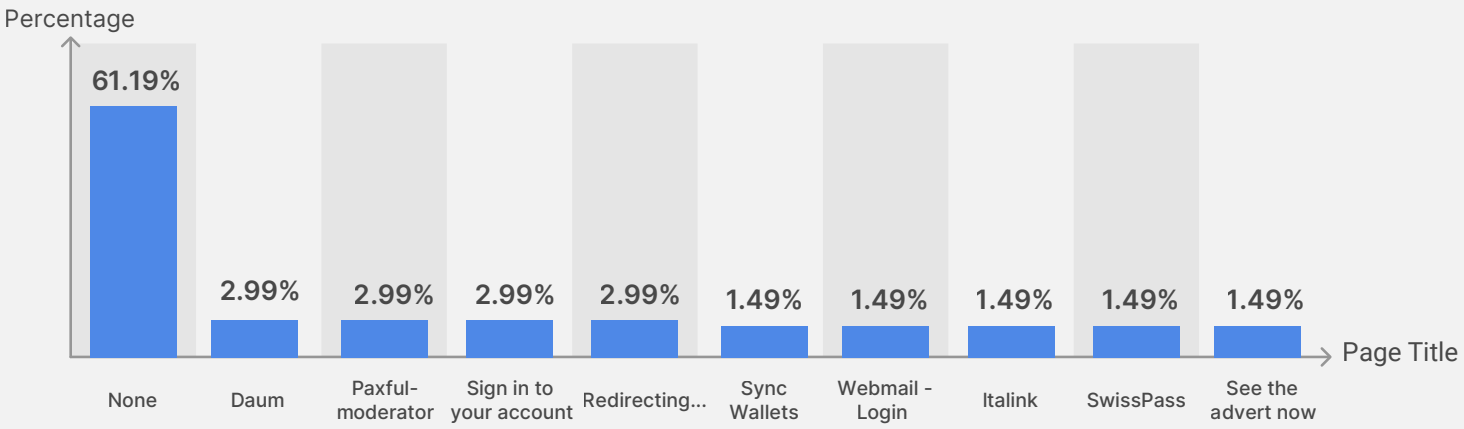
The Banking sector follows at 21.43%, driven by the financial rewards from credential theft and fraud.

Information Services (7.14%) is also targeted, likely due to its role as a data gateway for other sectors.

These trends highlight the need for robust email security and user awareness training across critical industries.

This heavy targeting suggests threat actors' interest in sensitive governmental communications and classified information.

Phishing Attacks - Distribution by Phishing Page Title



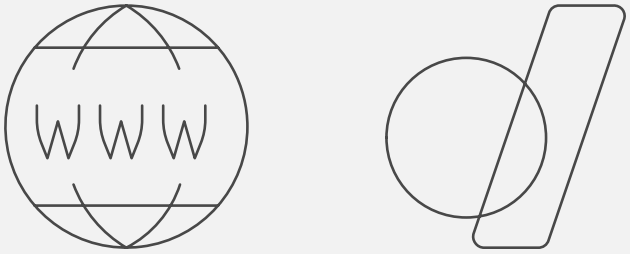
A majority (61.19%) of phishing pages used “None” as their title, likely indicating attempts to obscure malicious intent or evade detection.

Among other titles, "Sign in to your account" (2.99%) and "Redirecting..." (2.78%) were the most common, reflecting strategies aimed at luring victims into credential theft.

Notable targeted services include Paxful (2.63%) and Daum (2.49%), suggesting phishing campaigns tailored toward cryptocurrency users and international service providers.

The diversity of page titles underscores the need for vigilant user awareness and adaptive threat detection.

Phishing Attacks - Distribution by SSL/TLS Protocol



56.7%
HTTPS Domains

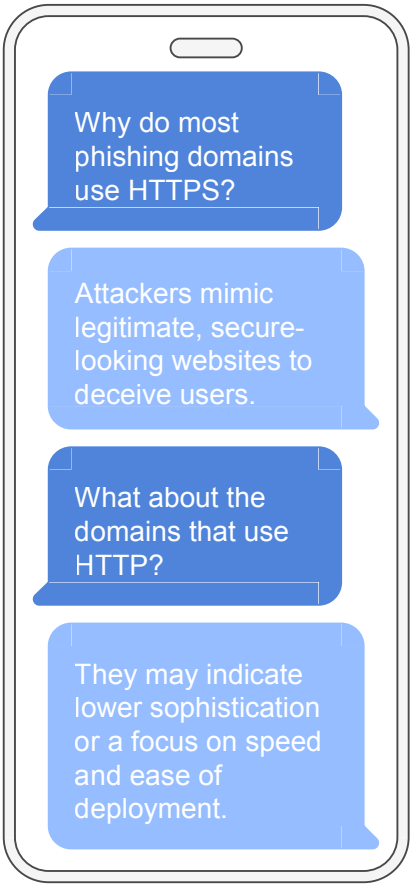
Majority use HTTPS for deception

43.3%
HTTP Domains

Significant portion still uses HTTP

The majority of phishing domains (56.7%) use HTTPS, highlighting a common tactic where attackers mimic legitimate, secure-looking websites to deceive users. However, a significant portion (43.3%) still employs HTTP, which may indicate lower sophistication or a focus on speed and ease of deployment.

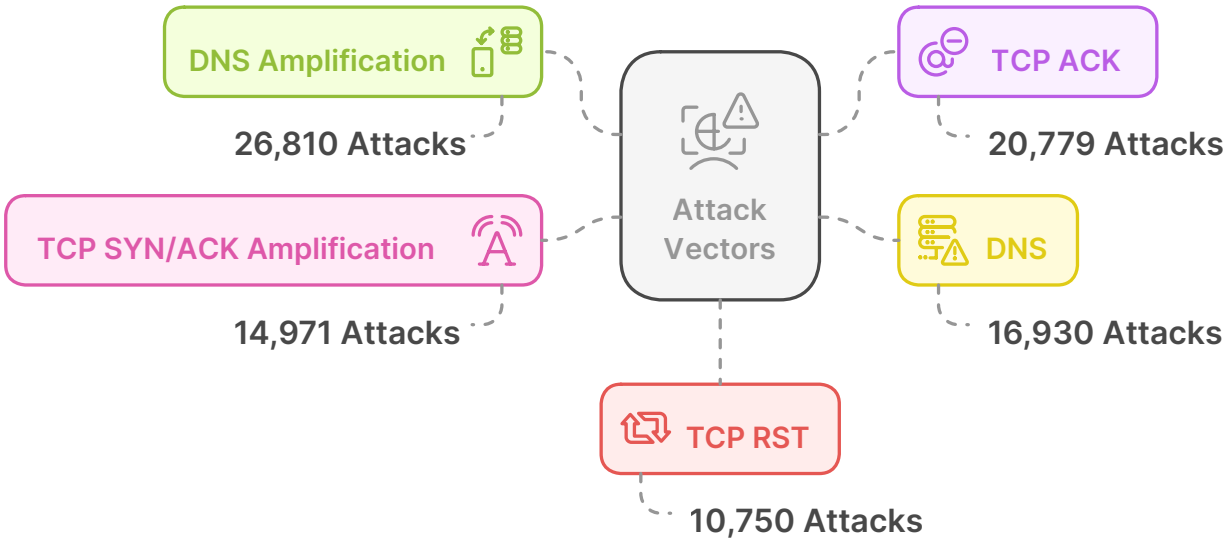
Despite the use of HTTPS, users should remain cautious, as attackers are increasingly leveraging SSL certificates to give phishing sites a more legitimate appearance. This trend emphasizes the importance of careful URL inspection and not solely relying on the presence of "HTTPS" as a security indicator.

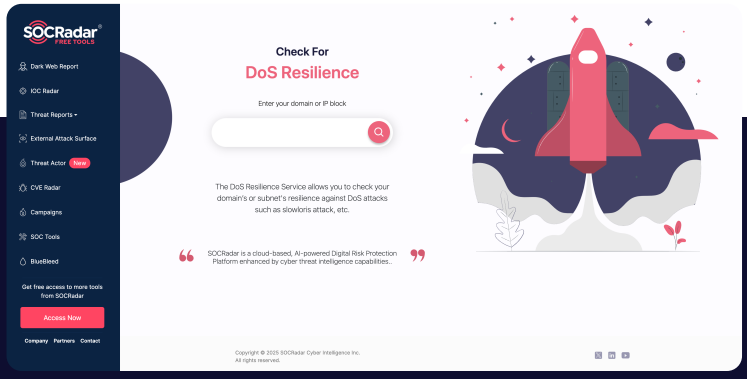


DDoS Attack Statistics

- The peak bandwidth witnessed during a DDoS attack reached 188.74 Gbps, highlighting a significant capacity from the cyber threats.
- The highest recorded throughput during these incidents was 17 Mpps.
- Most DDoS attacks lasted between 60.57 minutes on average.
- 57,319 DDoS attacks were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for Kenya.

Top DDoS Attack Vectors





SOCRadar's DoS Resilience Free Tool

Enhance your DDoS defense with *SOCRadar's DoS Resilience Free Tool*, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks.

Lessons Learned: Key Insights and Strategic Recommendations

- **Kenya as a Prime Cyber Target:** With 69.01% of threats targeting Kenya exclusively, it's clear that the country is a focal point for malicious actors. Organizations must prioritize cybersecurity as a critical business enabler.
- **Ransomware's Increasing Threat:** The Manufacturing sector is the hardest hit, accounting for 26.23% of ransomware incidents, followed by sectors such as Information and Retail Trade. This underscores the need for robust backup and recovery solutions and rapid incident response strategies.
- **Credential Theft via Stealer Logs:** High-traffic platforms like betika.com, ecitizen.go.ke, and jumia.co.ke are frequently targeted, indicating attackers' focus on financial transactions, government services, and e-commerce data. Strengthening user authentication measures and monitoring for compromised credentials are critical defensive actions.
- **Phishing Attacks Continue to Thrive:** National Security, Banking, and Information Services sectors face significant phishing risks, with 50% of attacks targeting national security. Employee training and phishing-resistant security measures, such as MFA, remain essential.
- **HTTPS Doesn't Guarantee Safety:** Despite the perception of security, 56.7% of phishing domains use HTTPS, highlighting the need for user education and advanced threat detection tools that go beyond SSL validation.
- **Ransomware Operators Lead the Charge:** The LockBit family dominates the ransomware landscape, with Cl0p and RansomEXX also playing significant roles. Proactive threat intelligence and defensive measures must be employed to counter evolving ransomware threats.
- **Strategic Targeting Patterns:** 44.93% of ransomware incidents indicate that Kenya was not the primary target but still suffered collateral damage, emphasizing the need for global threat awareness and collaborative defense strategies.
- **Data as a Lucrative Commodity:** 61.8% of threats focus on data theft, signaling the need for strong data encryption, access control policies, and regular audits to safeguard sensitive information.

Strategic Recommendations:

- **Invest in Comprehensive Threat Intelligence:** Staying informed about evolving threats and actors enables more proactive defenses.
- **Harden Authentication Mechanisms:** Deploy MFA and encourage password hygiene to protect against credential theft.
- **Enhance Incident Response Capabilities:** Develop and regularly test robust response and recovery plans, particularly for ransomware attacks.
- **Strengthen Employee Awareness:** Security awareness training is essential to combat phishing and social engineering attacks.
- **Collaborate for Greater Resilience:** Share intelligence with industry peers and cybersecurity alliances to stay ahead of emerging threats.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in **150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.