

December, 2025

INTELLIGENCE INSIGHTS. META & PAKISTAN

This report offers an overview of the latest threat landscape in META, covering key developments such as ransomware attacks, leaked credentials, data breaches, phishing scams, and more. It includes a month-over-month trend analysis to track evolving patterns. Additionally, the report spotlights a newly identified threat actor, campaign, or emerging technique, providing actionable insights for proactive defense.

2 Notable Events of the Month

- [Group-IB's 2026 cyber predictions](#) warn that AI-driven autonomous attacks, agentic extortion, and increasingly automated exploitation of modern technologies like APIs, crypto, and identity systems will reshape the threat landscape, requiring collaborative, real-time defenses to keep pace with rapidly evolving cybercrime.
- [CVE-2025-55182](#) (React2Shell) was discovered, this is a CVSS 10.0 flaw in React Server Components (react-server-dom-*) where a crafted RSC/Server Function ("Flight") request can trigger unauthenticated, pre-auth remote code execution, making it critical because a single malicious HTTP request can rapidly lead to full server compromise at scale for internet-exposed apps.

Global Trends:

- GoldFactory mobile fraud: Group-IB profiled GoldFactory, a threat actor trojanizing legitimate banking apps across APAC and distributing them via smishing/vishing/phishing while impersonating government services, using app-hooking frameworks and loaders like Gigabud to steal banking data, with mitigation guidance for banks and users.
- “Ghost Tapped” NFC fraud: Group-IB reports a China-linked, Telegram-driven Android malware ecosystem enabling remote contactless payment fraud by capturing card data via fake apps, supported by an organized underground supply chain and showing rapid growth through late 2025.
- DeadLock ransomware: Group-IB highlights DeadLock ransomware’s use of Polygon smart contracts to hide and rotate C2 infrastructure, complicating

Regional Trends:

MENA “online job” scams: Group-IB reports a MENA-focused scam using paid social ads to impersonate trusted brands, moving victims to WhatsApp/Telegram to steal IDs, banking data, and money, with 1,500+ localized ads seen in 2025 and guidance to curb scalable social-engineering fraud.

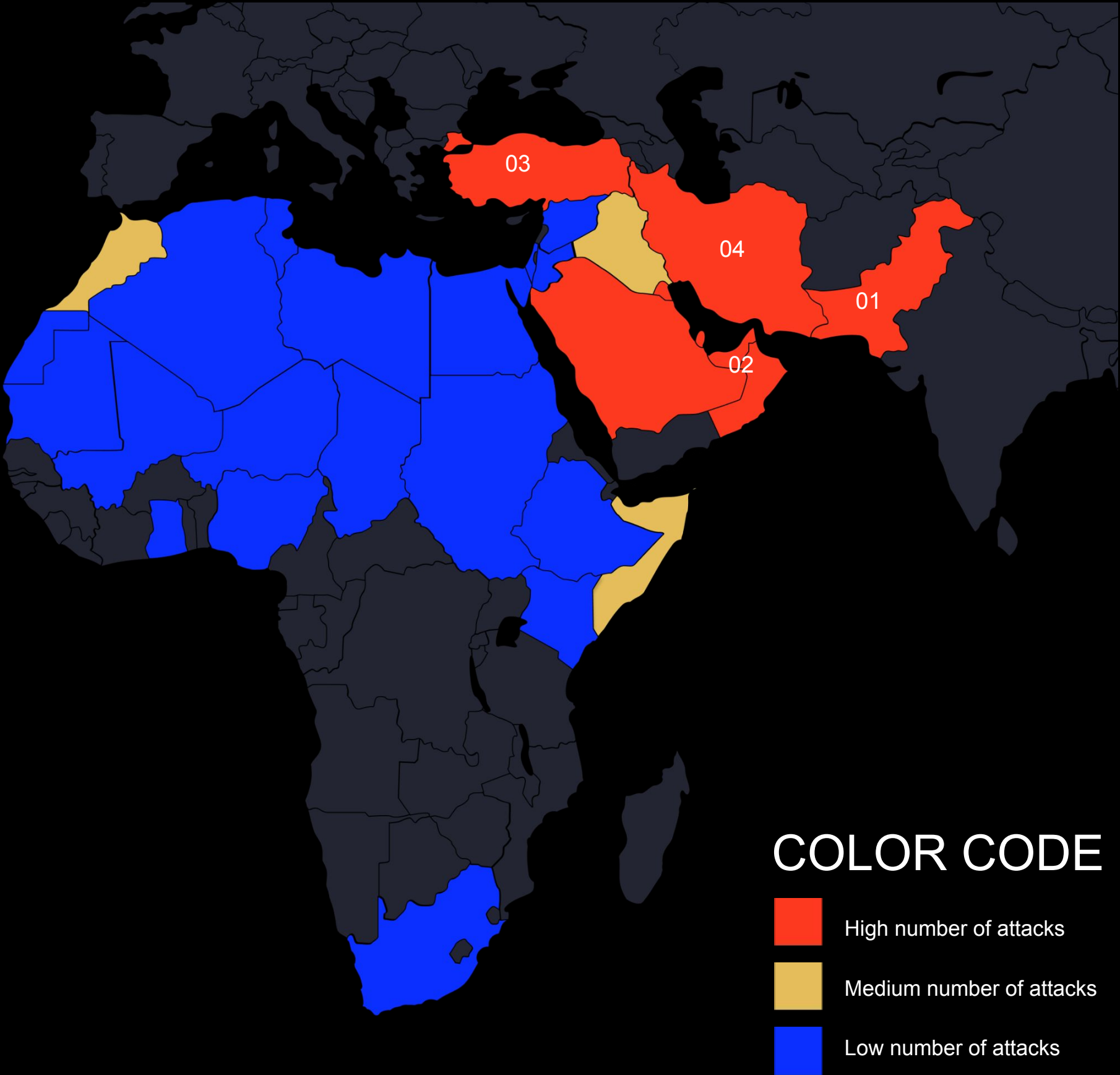
DDOS & HACKTIVISM STATISTICS

The scope is limited to DDOS & hacktivism-related activity.

Hacktivism is the use of hacking techniques to support political or social agendas. Usually hacktivist groups are low-skilled hackers who perform DDoS, Defacement, and Data Breaches (mostly leveraging compromised accounts) attacks. Unfortunately, during the last month these groups attracted a lot of attention.

STATISTICS (ON HACKTIVISM) BY COUNTRY (TOP 4)

01	02	03	04
Pakistan	GCC	Turkey	Iran
8	6	3	3



COLOR CODE

- High number of attacks
- Medium number of attacks
- Low number of attacks

RANSOMWARE ACTIVITIES

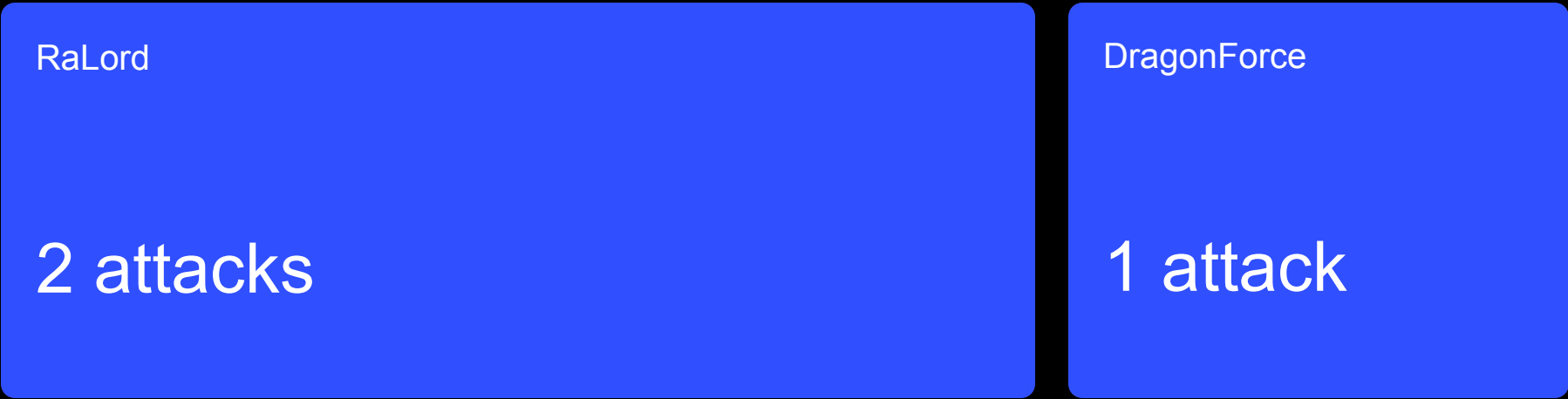
Ransomware is a type of malicious software that encrypts the victim's data, rendering it inaccessible. The attacker then demands a ransom payment from the victim to restore access to the data, typically threatening to delete or publicly expose the data if the ransom is not paid. Ransomware statistics for the last month in META region were as follows:

↓ 40%
(Nov to Dec)

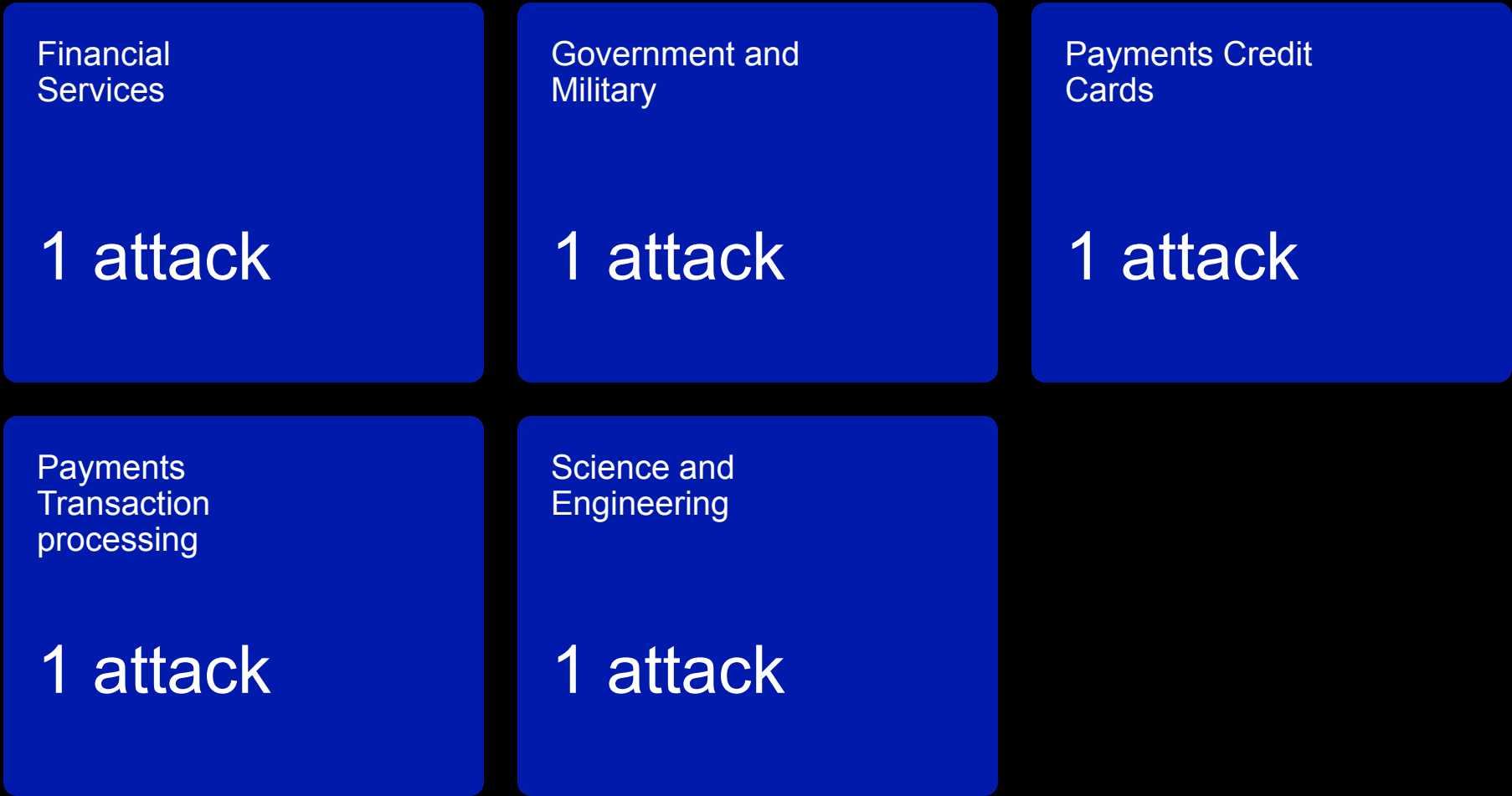
3 Ransom incidents



BREAKDOWN BY RANSOMWARE GROUPS



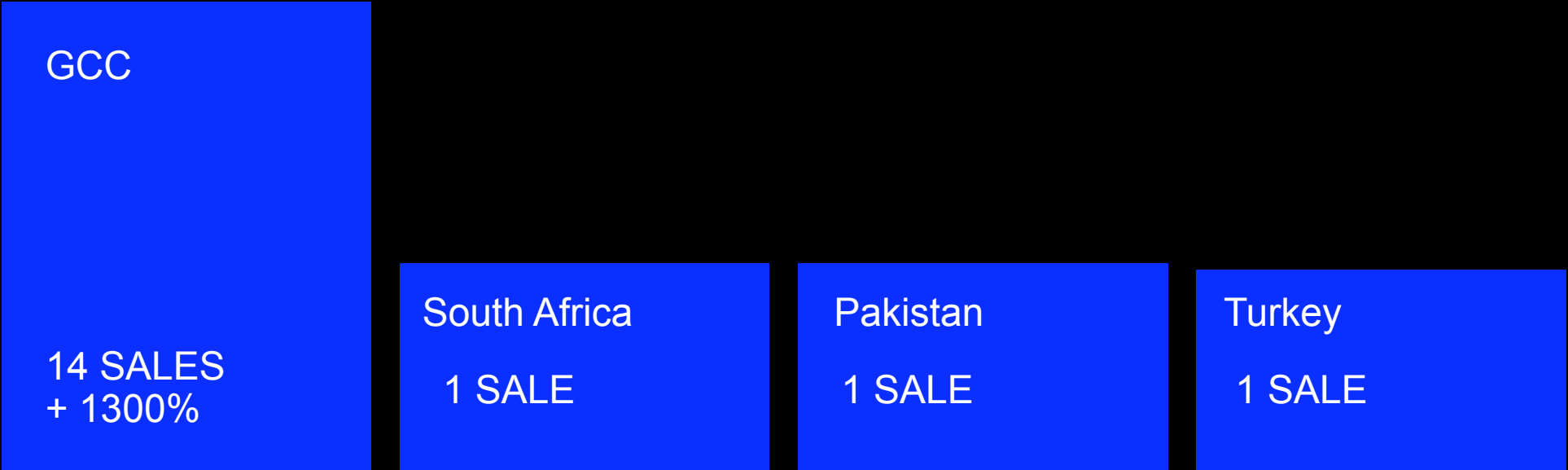
BREAKDOWN BY INDUSTRIES



INITIAL ACCESS BROKER SALE ON DARK WEB

Initial access to a company’s systems can lead to data theft, corporate espionage, and the deployment of malware for various malicious purposes. This page shows the volume and geographic distribution of corporate infrastructure access currently for sale on the dark web.

Top countries with the most initial access broker sale



Breakdown by industries



.....

↑18% (Nov vs Dec)

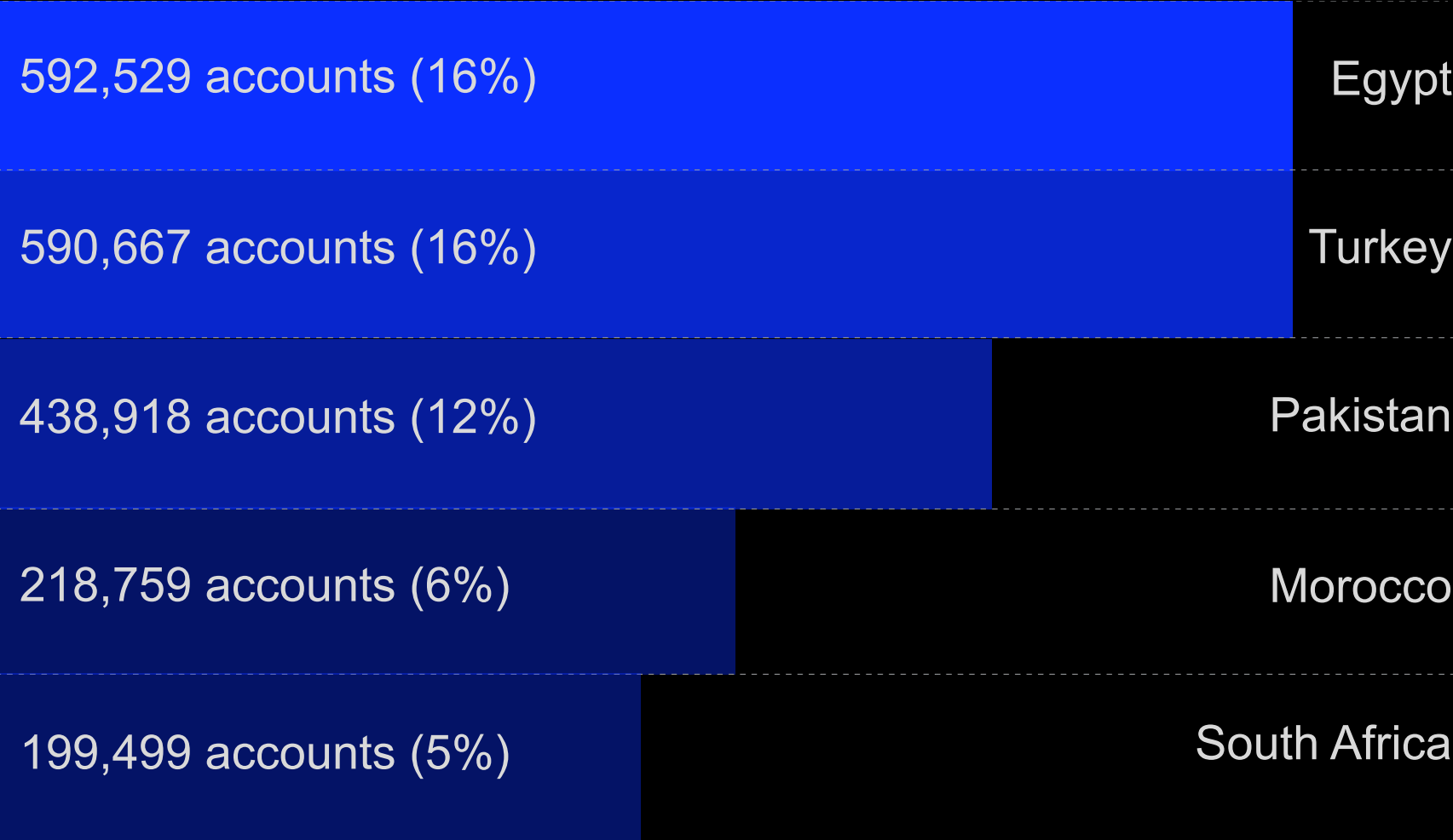
13 Sales

LEAKED CORPORATE CREDENTIALS

Key events

- Nigerian Banking Infrastructure Mass Compromise: This indicates a coordinated attack on Nigeria’s banking infrastructure, with multiple Access Bank employee accounts compromised. Attackers accessed the internal service desk system, potentially exposing customer data and operations, possibly exploiting reduced security during the December holiday period.
- Moroccan Tourism & E-commerce Platform Breach: This reflects a widespread breach of Morocco’s tourism tech infrastructure, impacting customer-facing platforms and backend systems, with risks of data theft or supply chain attacks during peak tourism season.

Countries with the most compromised accounts



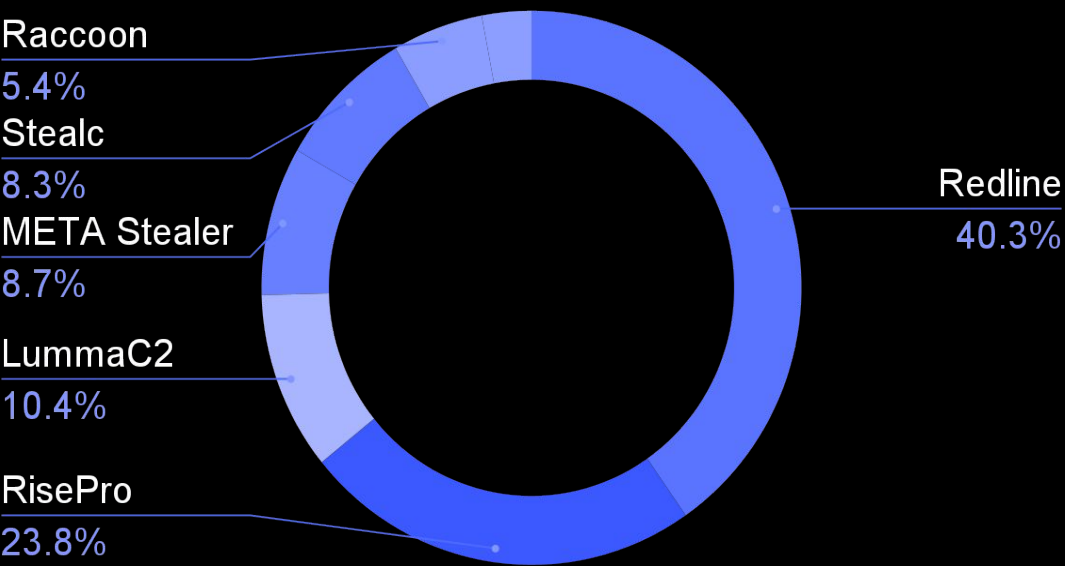
36,724,54
compromised accounts

STATISTICS: COMPROMISED DATA

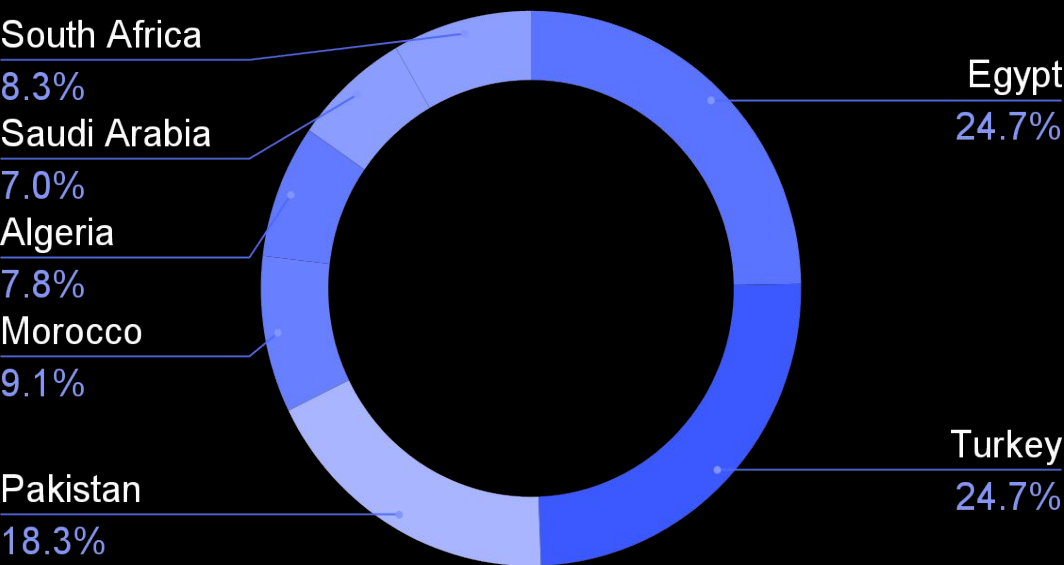
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational disruptions and exposing organizations to legal and regulatory consequences.

In this part of the report, we provide statistics regarding compromised accounts and compromised cards — all to understand which malware families are the most active in the region.

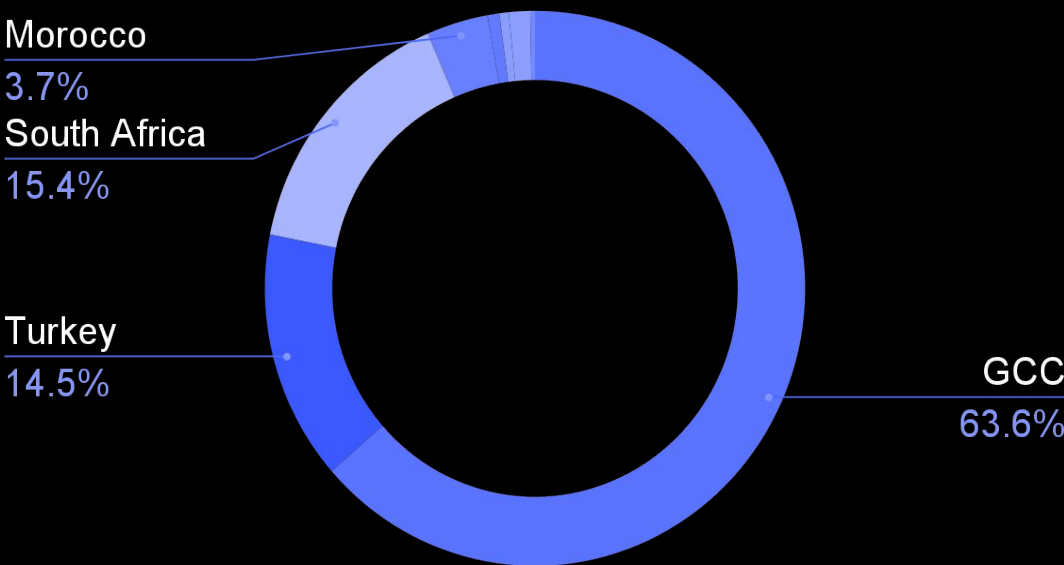
Compromise data by malware



Compromised accounts by country



Compromised bank cards by country



CONCLUSIONS AND RECOMMENDATIONS

The evolving threat landscape poses significant risks to organizations across various sectors. The incidents discussed in this report underscore the need for upgraded security measures and proactive threat management. To safeguard your organization, consider implementing the following recommendations:

ENHANCE SECURITY AWARENESS TRAINING Regularly educate employees on recognizing phishing attempts, social engineering tactics, and safe online practices.	STRENGTHEN IT INFRASTRUCTURE Ensure all systems are updated with the latest security patches and employ multi-factor authentication (MFA) to enhance access controls.	CONDUCT REGULAR SECURITY AUDITS Perform periodic assessments of your IT environment to identify and mitigate potential vulnerabilities.
DEPLOY ADVANCED THREAT DETECTION TOOLS Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and Endpoint Detection and Response (EDR), to detect and respond to threats in real-time.	ESTABLISH INCIDENT RESPONSE PROTOCOLS Develop and regularly update an incident response plan to quickly address and mitigate the impact of security breaches.	COLLABORATE WITH THREAT INTELLIGENCE SERVICES Leverage threat intelligence services to stay informed about emerging threats and adjust your risk and security management strategies accordingly.

STAY SMART. STAY CONNECTED. STAY SECURED



[Talk to our team](#)

RECENT RESOURCES

White Paper

Weaponized AI

Inside the criminal ecosystem fueling the fifth wave of cybercrime

[Read now](#)

Episode 02

Evolving defense tactics against rising authorized fraud

Fraud Intel Podcast Series

Podcast series

[Watch now](#)

From Deepfakes to Dark LLMs: 5 use-cases of how AI is Powering Cybercrime

[Read now](#)