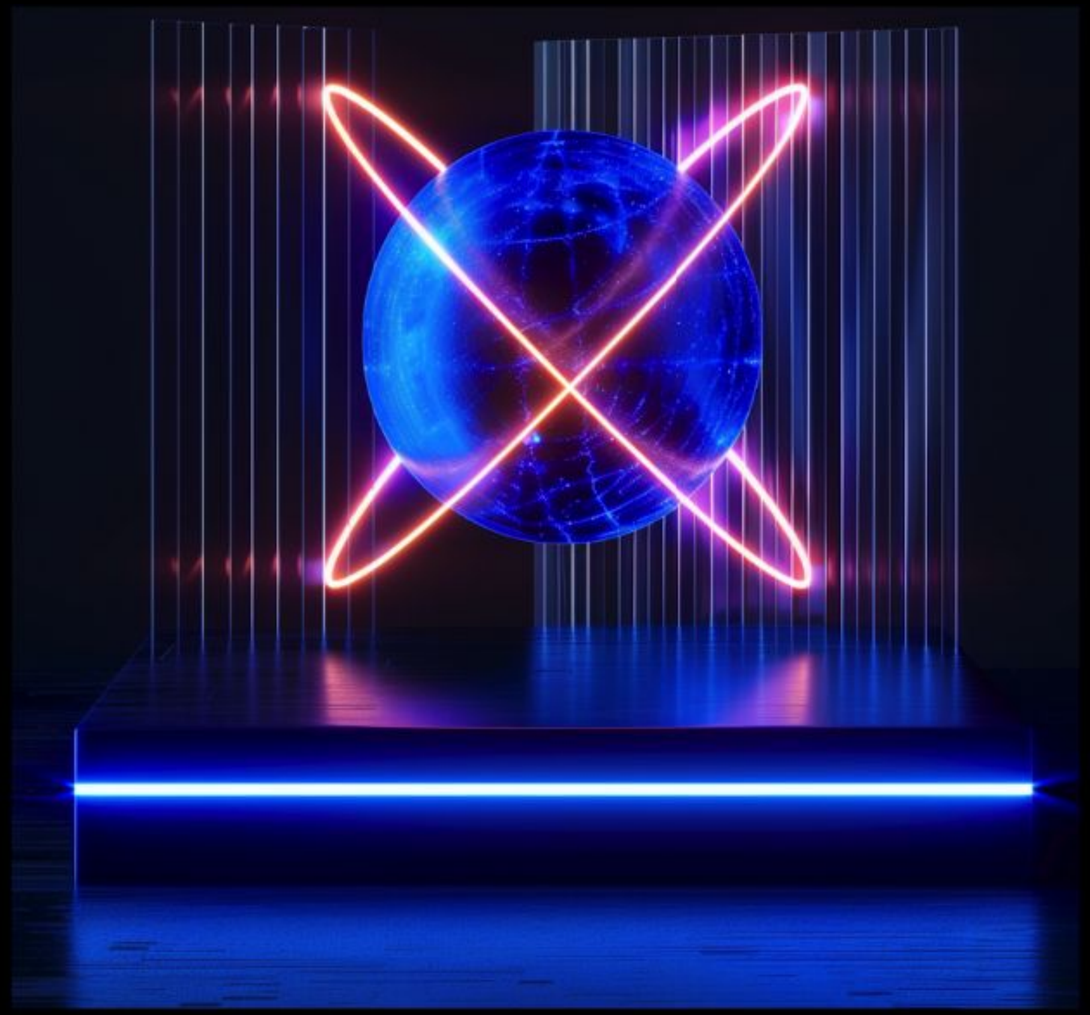

GROUP-IB
MIDDLE EAST, TÜRKİYE, AFRICA AND PAKISTAN
INTELLIGENCE
INSIGHTS
August Edition

INTRODUCTION

This report contains information on the most significant cybersecurity events that occurred worldwide and in the META region over the last month.

2 notable
events of the month:

- **A threat actor (UNC6395) stole OAuth tokens for Salesloft's Drift integrations and, between Aug 8–18, 2025, used them to siphon Salesforce data from numerous customers—and in a few cases read mail via Drift Email tokens in Google Workspace—prompting widespread token revocations and the app's takedown.**
- **Group-IB identifies "ShadowSilk" as a cross-border espionage cluster (overlapping with YoroTrooper) that has targeted ~35 government entities across Central Asia and APAC since 2023, using spear-phishing and Telegram-bot C2 to exfiltrate data**



Group-IB specialists discovered multiple phishing and scam campaigns and took active steps to mitigate their disruptive impact. It is important to mention that **Group-IB customers are well-protected** and aware about such types of threats.

GLOBAL TRENDS

GROUP-IB

Global trends and their context:

1. UNC6395 OAuth Token Theft: Targeting Drift Integrations to Breach Salesforce and Google Workspace	In early–mid August 2025, threat actor UNC6395 stole OAuth tokens for the Salesloft Drift integration and used them to access customers' Salesforce tenants and exfiltrate case/contact data; Google later confirmed the actor also abused "Drift Email" tokens to read mail in a very small number of Google Workspace accounts tied to that integration. Cloudflare, Palo Alto Networks, Zscaler and others disclosed impact and revoked Drift access, with guidance to treat all Drift-linked tokens as compromised, rotate credentials, and audit OAuth/API logs and permissions.
2. ShadowSilk Returns: Cross-Border Espionage Targeting Central Asia and APAC Governments	Group-IB's August 27, 2025 post details of "ShadowSilk," a cross-border data-exfiltration cluster overlapping with YoroTrooper that has targeted government entities across Central Asia and APAC since at least 2023, with more than 35 victims and activity observed through July 2025. After earlier public exposure in January 2025, the operators rebuilt infrastructure and resumed operations in June; a joint effort with CERT-KG yielded a server image that revealed their TTPs and confirmed a singular motive: data theft.

GLOBAL TRENDS

GROUP-IB

Global trends and their context:

3. Critical WhatsApp and Apple Vulnerabilities Enable iOS/macOS/iPadOS Compromise Without User Interaction	From May through August 2025, were discovered two critical vulnerabilities — WhatsApp (CVE-2025-55177, an authorization flaw in linked-device sync allowing content to be processed from an arbitrary URL) and Apple platforms (CVE-2025-43300, an ImageIO out-of-bounds write on image handling) — enabling compromise of iOS/iPadOS/macOS without user interaction. Vendors released updates (at minimum: WhatsApp for iOS 2.25.21.73 / Mac 2.25.21.78; iOS 18.6.2 with corresponding macOS/iPadOS patches), Meta notified fewer than 200 carefully selected targets; immediate updating is advised, and if compromise is suspected, a full device reset is recommended.
4. AI-Powered Trading Scams: Deepfakes, Fake Reviews, and Industrial-Scale Fraud Networks	Group-IB's Aug 13, 2025 blog explains how modern "AI-trading" investment scams weaponize deepfake videos, fabricated reviews, and targeted ads to funnel victims into slick but fake trading platforms. Using its Graph Network Analysis, Group-IB links clusters of scam domains to just a handful of registrants—one of them tied to ~50 sites—illustrating industrial-scale operations behind the lures. The report cites deepfakes of public figures (e.g., Dutch politician Geert Wilders) to add credibility and drive clicks via social media and spoofed news pages.

REGIONAL TRENDS

GROUP-IB

Key regional trends with a brief description:

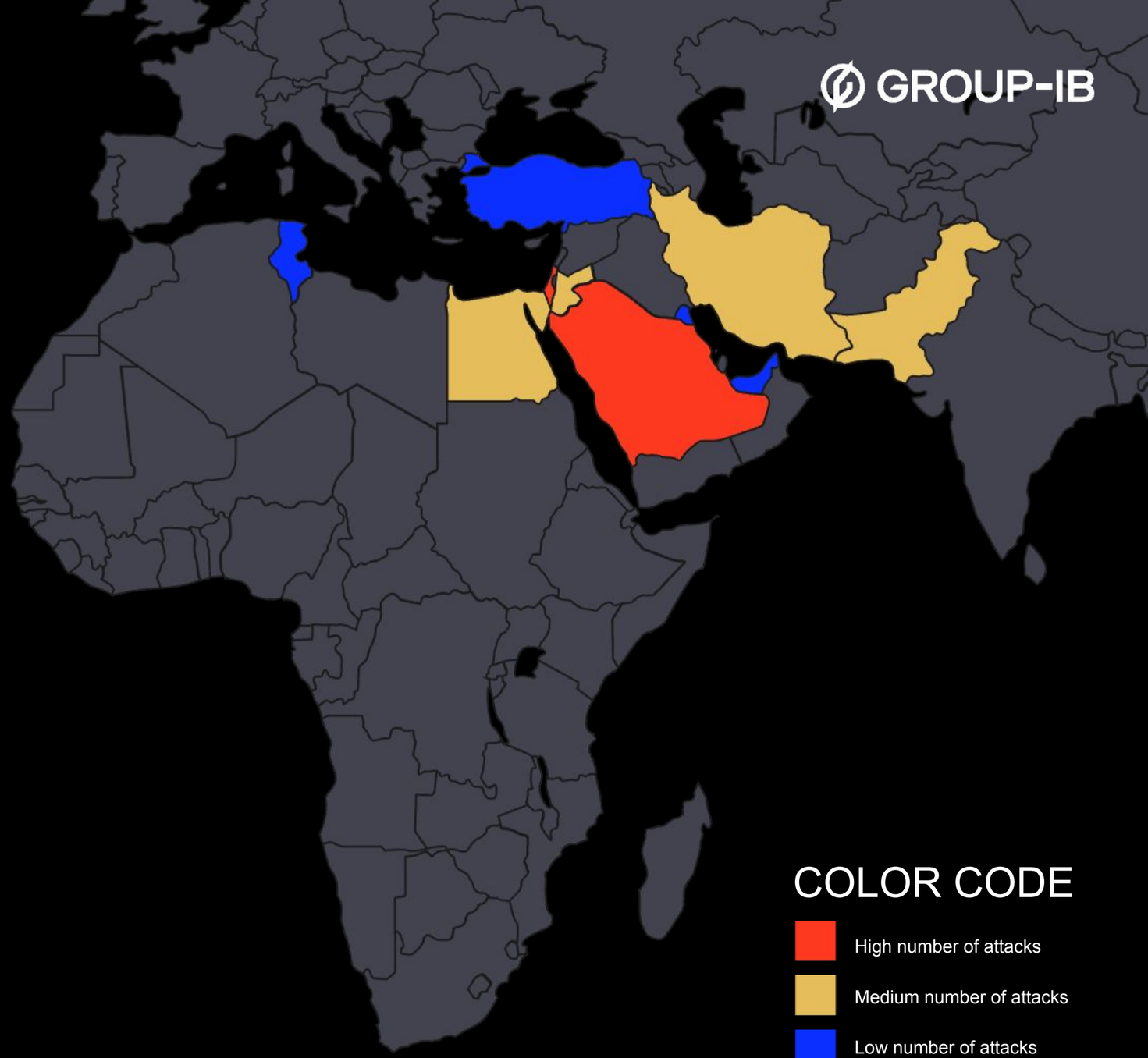
Middle East,Türkiye, Africa & Pakistan

1. The Evolving Threat of Banking Mules in META: From IP Masking to Device Muling	Group-IB's post highlights how META banking mule operators have upgraded their tradecraft—from basic IP masking to satellite connectivity, GPS spoofing, SIM abuse, and device muling. As banks deploy countermeasures, mule networks adapt, showing that single-signal defenses are easily bypassed. Layered controls combining network, device, and behavioral signals are essential to detect and disrupt these operations.
2. Spear-Phishing Targeting Finance Executives	A sophisticated spear-phishing campaign is targeting CFOs and finance executives worldwide, using legitimate remote-access tools like NetBird to maintain control of compromised systems. Posing as Rothschild & Co recruiters, attackers deploy Firebase-hosted phishing pages, custom CAPTCHAs, malicious VBS scripts, and multi-stage payloads. Investigations reveal new infrastructure, updated payloads, and links to APT MuddyWater, highlighting a highly targeted, evolving threat.

HACTIVISM STATISTICS

The scope is limited to 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. There was an increase of 19.5% in hacktivism attacks from July to August.



STATISTICS (ON HACKTIVISM) BY COUNTRY (TOP 4-5)

01	02	03	04
Saudi Arabia	Israel	Pakistan	Jordan
113	90	21	18

RANSOMWARE ACTIVITIES

GROUP-IB

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:

↑ 155% (July vs August)

23 Ransomware incidents

Most active threat actors

Lockbit

4 attacks

Meow

4 attacks

RansomHub

4 attacks

Darkvault

3 attack

Most targeted industries

Financial Services Banking

5 attacks

Government & Military

2 attacks

Food & Beverage

3 attacks

Energy

1 attack

Consumer goods

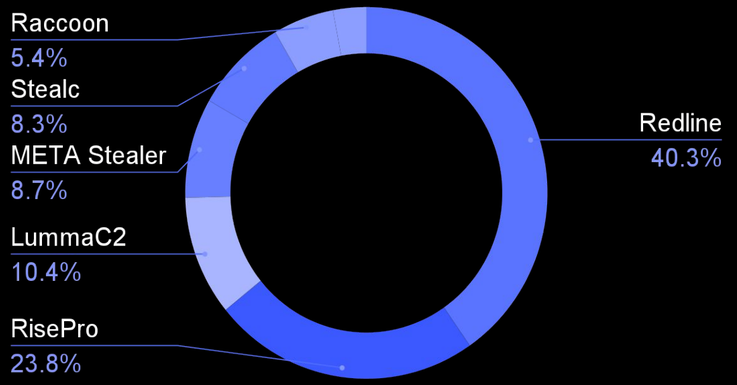
1 attack

STATISTICS: **COMPROMISED DATA**

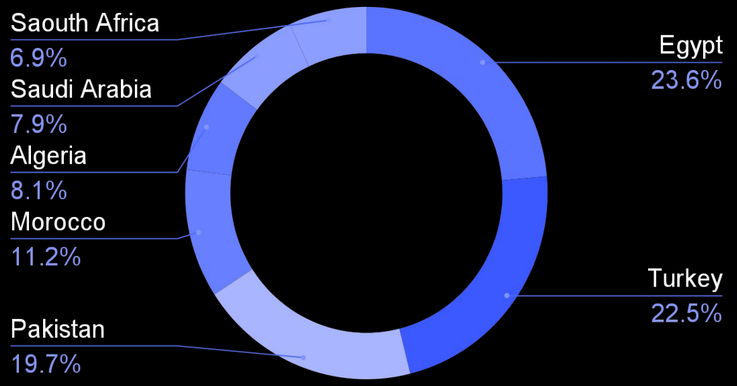
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational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

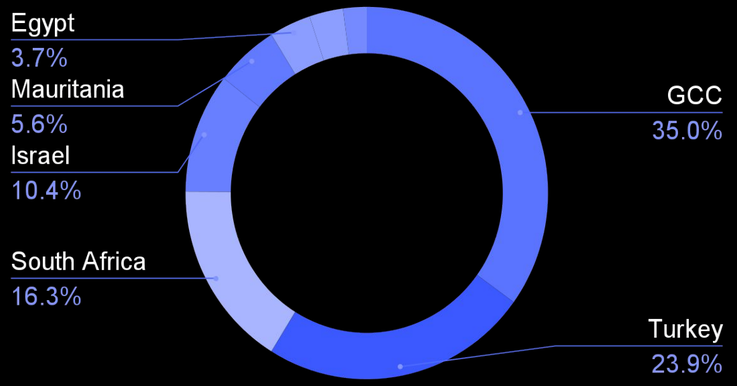
Compromise data by malware



Compromised accounts by country



Compromised bank cards by country



CONCLUSIONS AND RECOMMENDATIONS

GROUP-IB

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

GROUP-IB

[Talk to our team]

RECENT
RESOURCES

Read now

Watch now

Register now