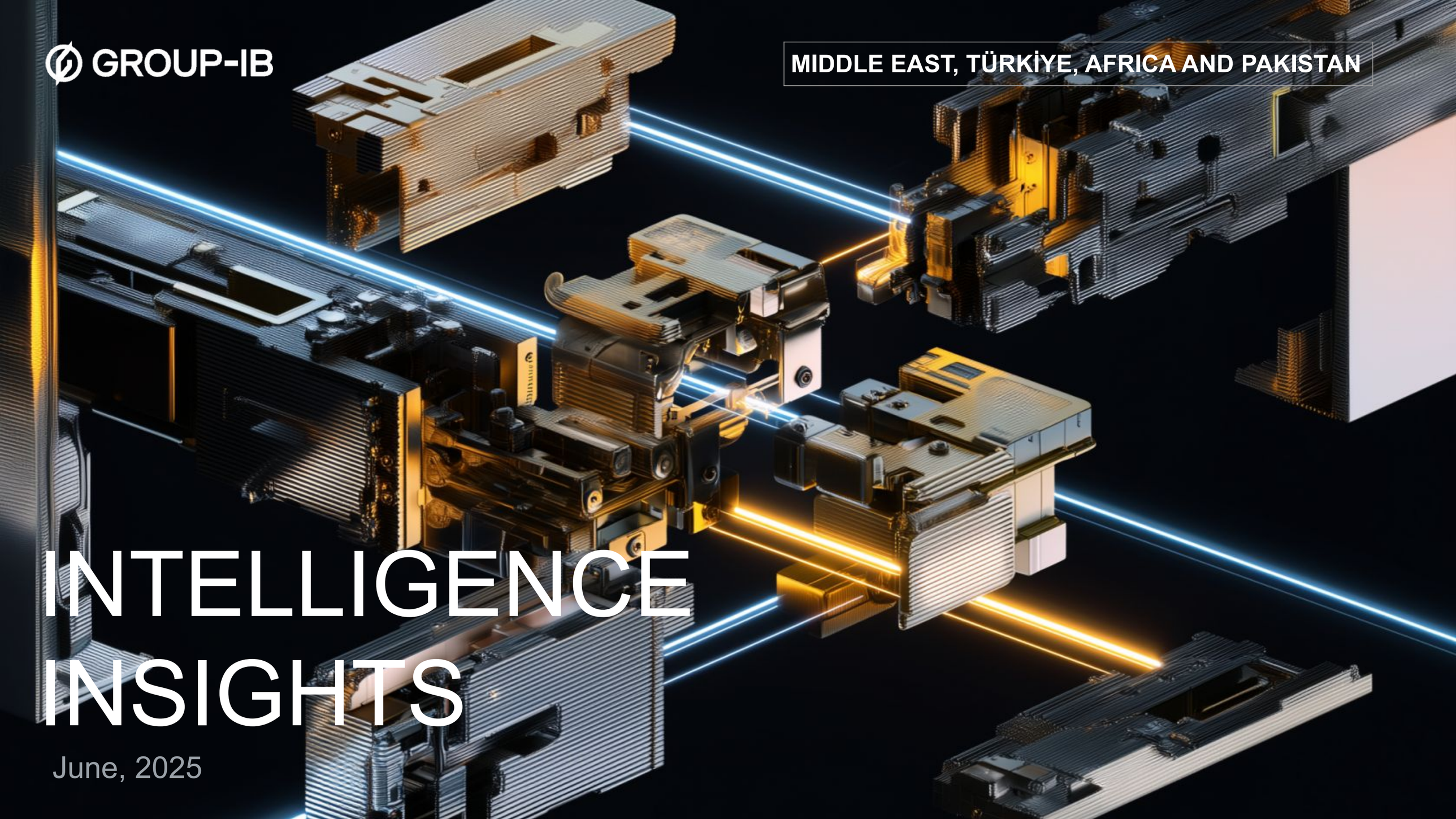
GROUP-IB

MIDDLE EAST, TÜRKİYE, AFRICA AND PAKISTAN



INTELLIGENCE INSIGHTS

June, 2025

INTRODUCTION

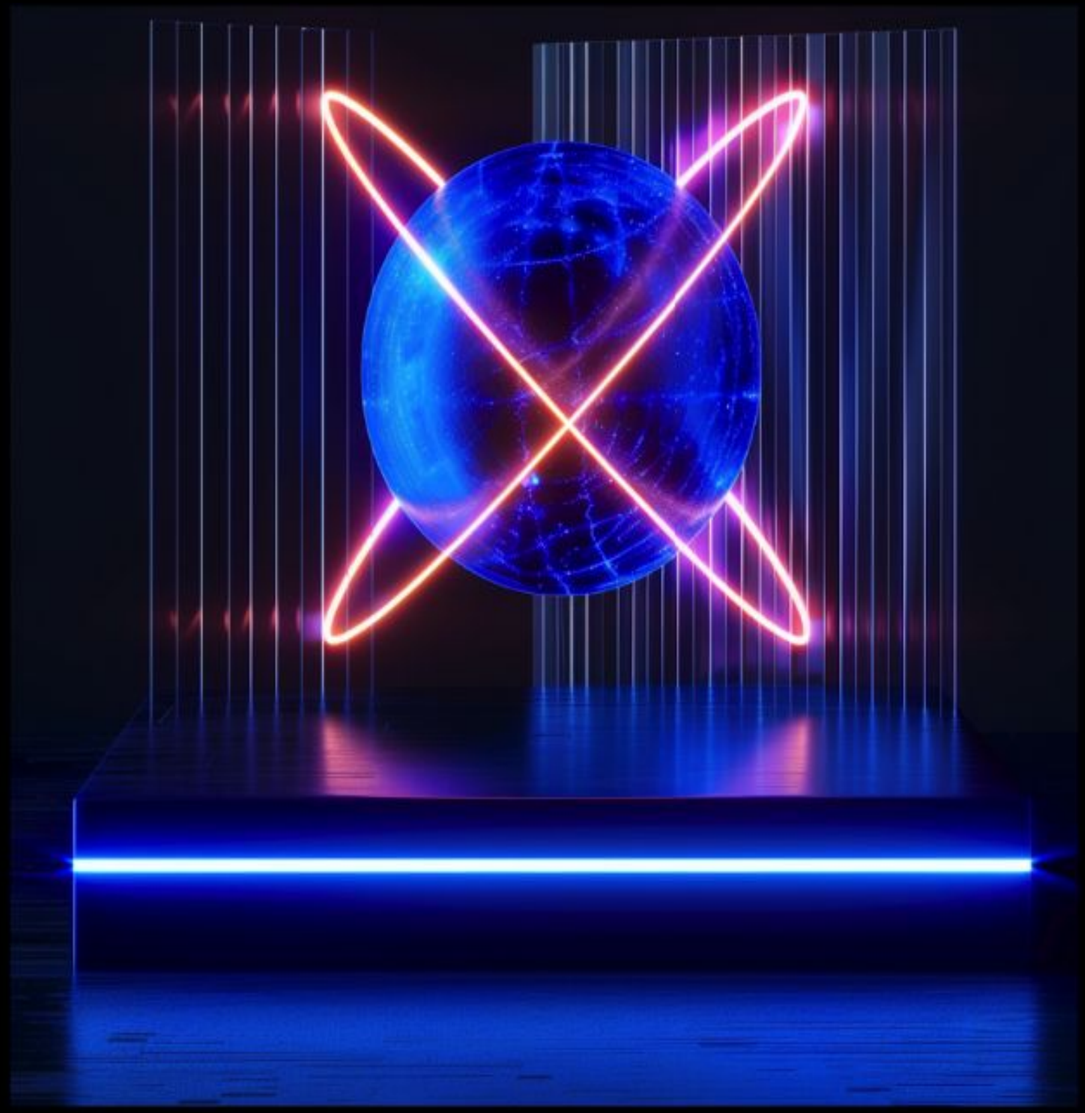
This report contains information on the most significant cybersecurity events that occurred worldwide and in the META region over the last month.

2 notable
events of the month:

- **Group-IB's June findings reveal that hacktivist chatter around the Middle East conflict, increased by 46 % on the 13 June, but collapsed by roughly 70 % within a week. 84 % of the posts were driven by eight main Telegram channels.**

- **Group-IB's 19 June 2025 blog "Declaration trap" revealed a phishing campaign, where adversaries masqueraded as European tax authorities—primarily the Dutch Belastingdienst—luring users to fake sites that steal wallet seed phrases or exploit WalletConnect for malicious smart-contract requests via the Inferno Drainer kit secured with anti-analysis scripts.**

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

Global trends and their context:

1. Crypto Tax Scam Alert: Group-IB Uncovers Sophisticated Phishing Campaign Targeting Dutch Residents	Group-IB's 19 June 2025 blog post "Declaration trap" documents a phishing wave impersonating European tax agencies—chiefly the Dutch Belastingdienst—telling residents they must urgently file a special crypto-asset declaration. Victims who follow the email link land on near-perfect clones of official portals where attackers either (1) steal wallet seed phrases, or (2) use WalletConnect to push malicious smart-contract requests and drain funds, an approach tied to the Inferno Drainer-as-a-Service kit and protected by anti-analysis scripts. The campaign, now spreading beyond the Netherlands, shows how threat actors exploit tax-related anxiety. Group-IB urges users to never share seed phrases, scrutinise sender domains/URLs, and remember that legitimate crypto taxes are handled in the standard annual return, not via ad-hoc "declaration" forms.
3. Group-IB Uncovers Global SEO Spam Campaign Hijacking 250+ WordPress Sites for Gambling Traffic	Group-IB discovered a long-standing 2021 SEO spam campaign which has compromised over 250 legitimate WordPress websites, including small blogs, e-commerce sites, and yacht charter services. The attackers inject hidden frames that load personalized gambling content, targeting users in numerous countries worldwide. This tactic leverages the websites' SEO authority to evade detection, likely gaining access through weak admin credentials or unsecure plugins, and aims to generate affiliate commissions by driving traffic to gambling sites. Details are available in Group-IB Threat Intelligence portal.

GLOBAL TRENDS

Global trends with a brief description:

1. BuzzToll Phishing Campaign Exposed: Group-IB Links Toll Scam to Threat Actor PendingLocust	Group-IB published research about the BuzzToll Phishing campaign in Threat Intelligence portal, attributed to the threat actor PendingLocust. It began in April 2024 and remains active as of June 2025. The campaign mainly leverages unpaid tolls and delivery issues to create a sense of urgency to prompt victims to act quickly. PendingLocust's main objective is to harvest login credentials and credit card information to perform Adversary-in-the-Middle (AiTM) attacks to facilitate unauthorised transactions. The phishing sites designed to imitate the original sites, were propagated via emails and SMS messages to trick victims.

REGIONAL TRENDS

Key regional trends with a brief description:

01 Group-IB Brief Reveals Hacktivist Surge and Tactical Cyberstrikes Amid Israel–Iran Escalation

Group-IB's brief finds that hacktivist chatter around the Israel–Iran flare-up increased by 46 % on 13 June, but collapsed by roughly 70 % within a week, with 84 % of posts driven by eight core Telegram channels. Amid the noise, a handful of operations delivered real impact: Predatory Sparrow "burned" about $90 million in its breach of Iranian crypto-exchange Nobitex, Iranian actors hijacked Israeli emergency-alert SMS, GPS spoofing disrupted regional ship and aircraft navigation, and thousands of exposed Israeli cameras were tapped for live battle-damage assessment.

02 Group-IB Identifies New DarkBlinder Malware Sample in GCC: Multi-Stage Infection Chain Underway

Group-IB's continuous monitoring of the DarkBlinder malware has uncovered a new sample, HTTPServiceHandler.dll, uploaded to VirusTotal from the GCC region on May 29, 2025. This DLL is identified as the first stage of a multi-stage infection chain. While the first-stage component has been sourced, the second-stage component, HTTPApiV2.dll (previously identified as a backdoor), has not yet been uploaded or sourced. Further details regarding the threat actor's activities and this specific event are available on the Threat Intelligence portal.

Middle East,Türkiye, Africa & Pakistan

DDOS AND HACKTIVISM ATTACKS BY COUNTRY

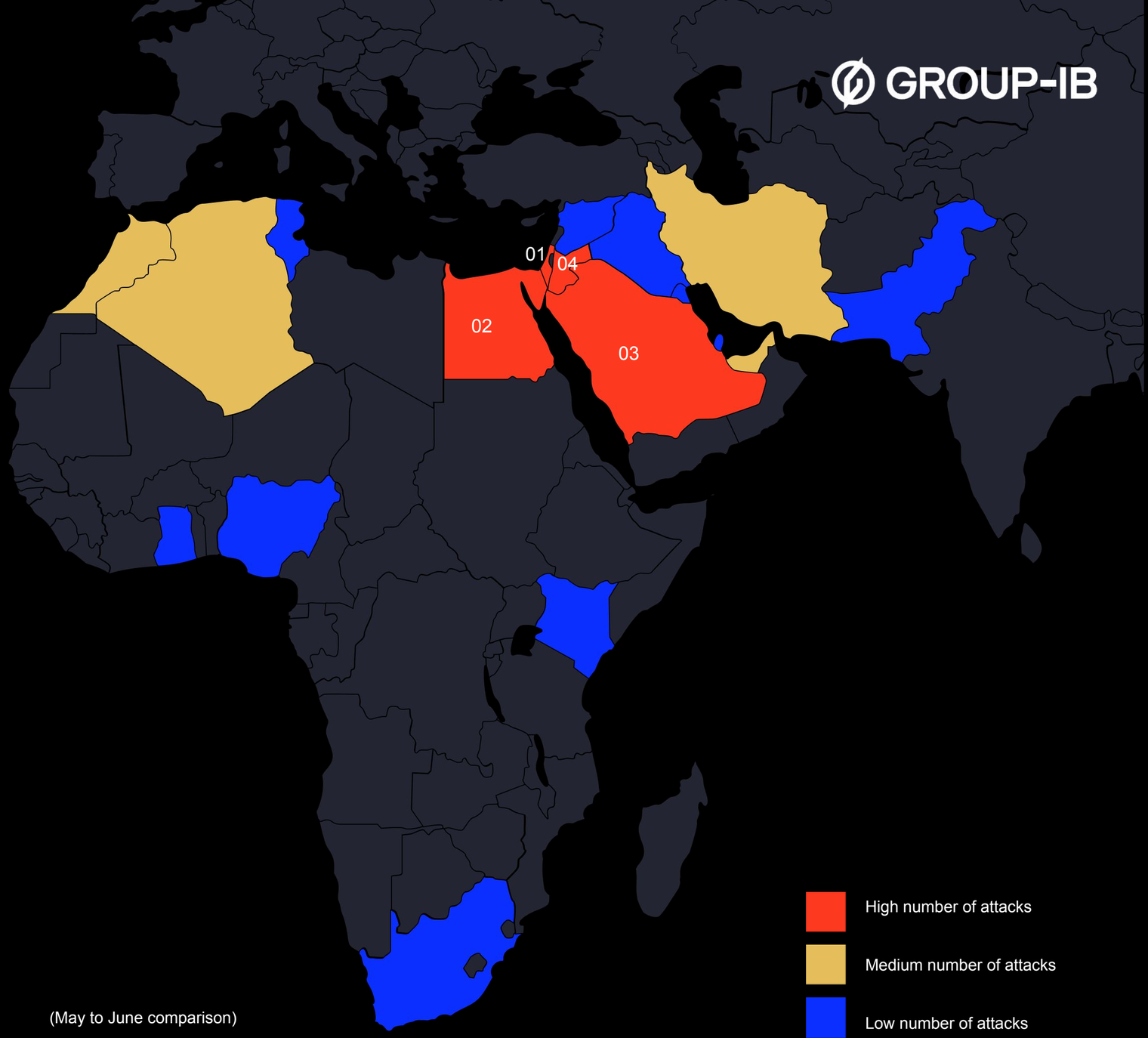
Key Events:

Hacktivist Surge Amid Conflict
Hacktivist activity surged during the ongoing Middle East conflict, driven by decentralized participation and rapid content amplification across key social media channels.

Predatory Sparrow's Key Attacks
Notable incidents include Predatory Sparrow's breach of Nobitex, leaking internal data and code, and a cyberattack targeting Bank Sepah.

STATISTICS (ON DDOS / HACKTIVISM) BY COUNTRY (TOP)

01	02	03	04
Israel	Egypt	Saudi Arabia	Jordan
462 attacks	41 attacks	40 attacks	37 attacks
+160%	+583%	+700%	+3600%



(May to June comparison)

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:

↓ 70% (May vs June)

9 Ransomware incidents

GROUP-IB

Most active threat actors

Everest
2 attacks

Gunra
2 attacks

Nemesis
2 attacks

fSociety
2 attacks

INC Blog
1 attack

Most targeted industries

Government and Military
3

Health Care Hospital
3 attacks

Financial Services
1 attack

Financial Services Banking
1 attack

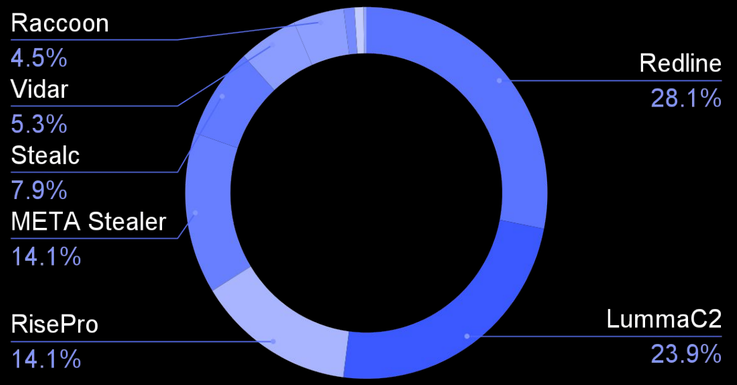
Other B2B
1 attack

STATISTICS: **COMPROMISED DATA**

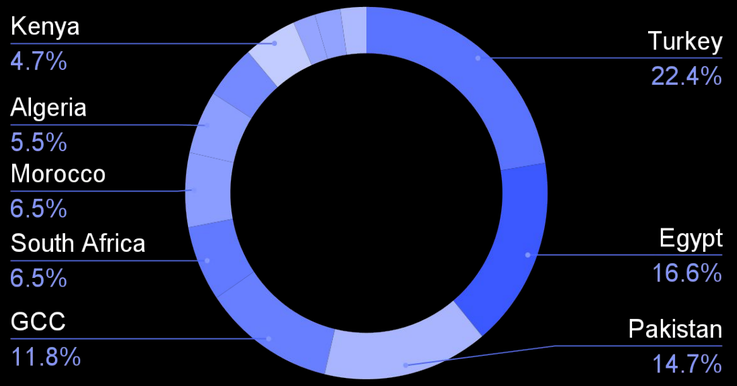
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational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

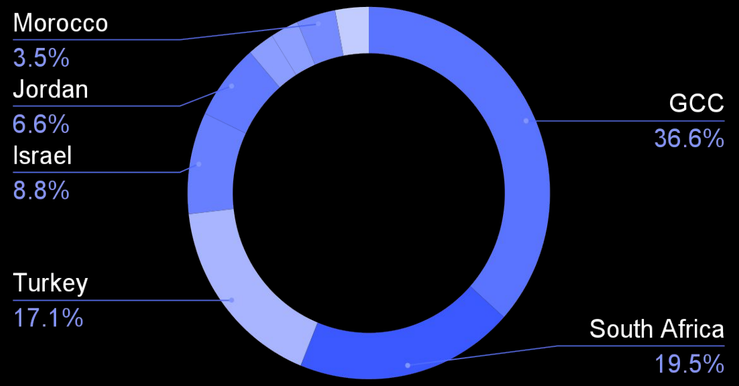
Compromise data by malware



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 security strategies accordingly.

STAY SMART. STAY CONNECTED. STAY SECURED

[Talk to our team]

RECENT
RESOURCES

Read now

Watch now

Read now