GROUP-IB

MIDDLE EAST, TÜRKİYE, AFRICA AND PAKISTAN

INTELLIGENCE INSIGHTS

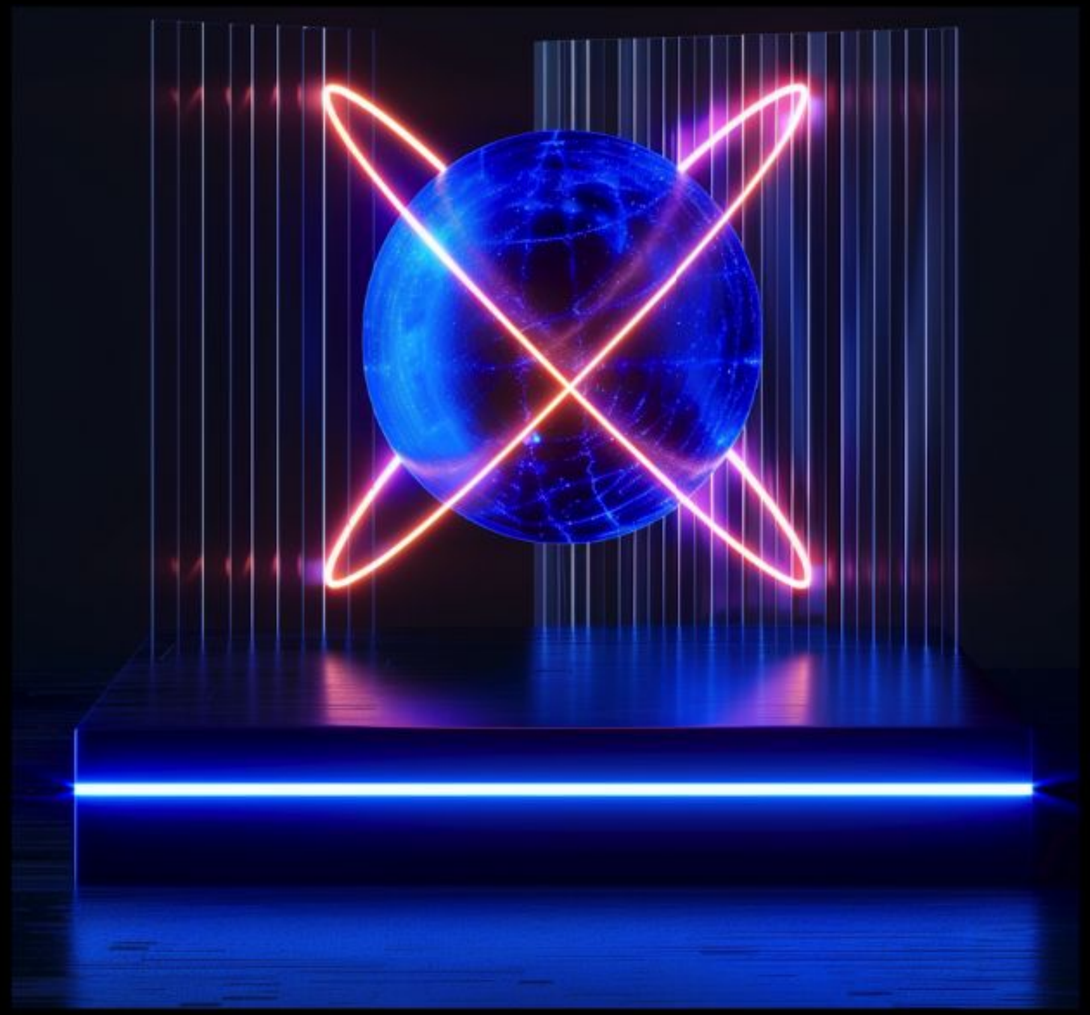
July Edition

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:

- **In mid-July two critical vulnerabilities (CVE-2025-53770 and its variant CVE-2025-53771) were discovered in on-premises SharePoint Server. Active exploitation began in mid-July 2025 both by state-sponsored and financially motivated threat actors.**
- **Group-IB published blogpost where explain how attackers can still obtain valid Microsoft signatures for malicious Windows kernel drivers, allowing these drivers to run as if they were legitimate and giving threat actors kernel-level control to disable security tools and evade detection.**



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. Exploiting Trust: How Signed Drivers Fuel Modern Kernel-Level Attacks on Windows	In the new blogpost Exploiting Trust: How Signed Drivers Fuel Modern Kernel Level Attacks on Windows the Group-IB team explains how despite Microsoft's significant efforts to secure driver signing, the threat actors still manage to sign and run malicious kernel drivers in a seemingly legitimate way. This ongoing loophole poses a serious threat, enabling attackers to bypass security measures and operate at the kernel level.
2. Predictive AI: The Understated Force in Cyber Defense	The Group-IB team published the post which argues that while generative AI captures most headlines, predictive AI — driven by threat intelligence, human analysts, and campaign telemetry — serves as a subtle yet significant force in foreseeing cyberattacks before they unfold. It emphasizes how intelligence-led predictive approaches offer a strategic edge in anticipating adversaries' moves and improving security posture.

GLOBAL TRENDS

GROUP-IB

Global trends and their context:

3. SharePoint Critical Vulnerabilities Under Active Exploitation (CVE-2025-53770 & CVE-2025-53771)	In mid-July two critical vulnerabilities (CVE-2025-53770 and its variant CVE-2025-53771) were discovered in on-premises SharePoint Server. The vulnerability allows unauthenticated attackers to upload a rogue ASPX page, steal machine-key secrets, and craft forged __VIEWSTATE payloads, resulting in full remote-code execution without any login. Active exploitation began in mid-July 2025, with actors such as Storm-2603 pivoting to ransomware attacks; Microsoft and CISA have issued urgent guidance and patches for Subscription Edition and 2019 (a 2016 fix is pending), while SharePoint Online remains unaffected. Two more groups were also detecting in exploitation of this vulnerability: Linen Typhoon and Violet Typhoon.
4. The Dark Web's Obsession with "Combolists" and ULP Files	Cybercriminals circulate enormous "combolist" and ULP text files on the dark web that simply pair stolen usernames (or emails) with passwords, making credential-stuffing and similar attacks easy. Group-IB's research shows that although these dumps are still traded as if they were brand-new, most of the data is recycled and outdated, so they are poor indicators of fresh compromises and are better suited to historical exposure tracking than real-time threat detection.

REGIONAL TRENDS

GROUP-IB

Key regional trends with a brief description:

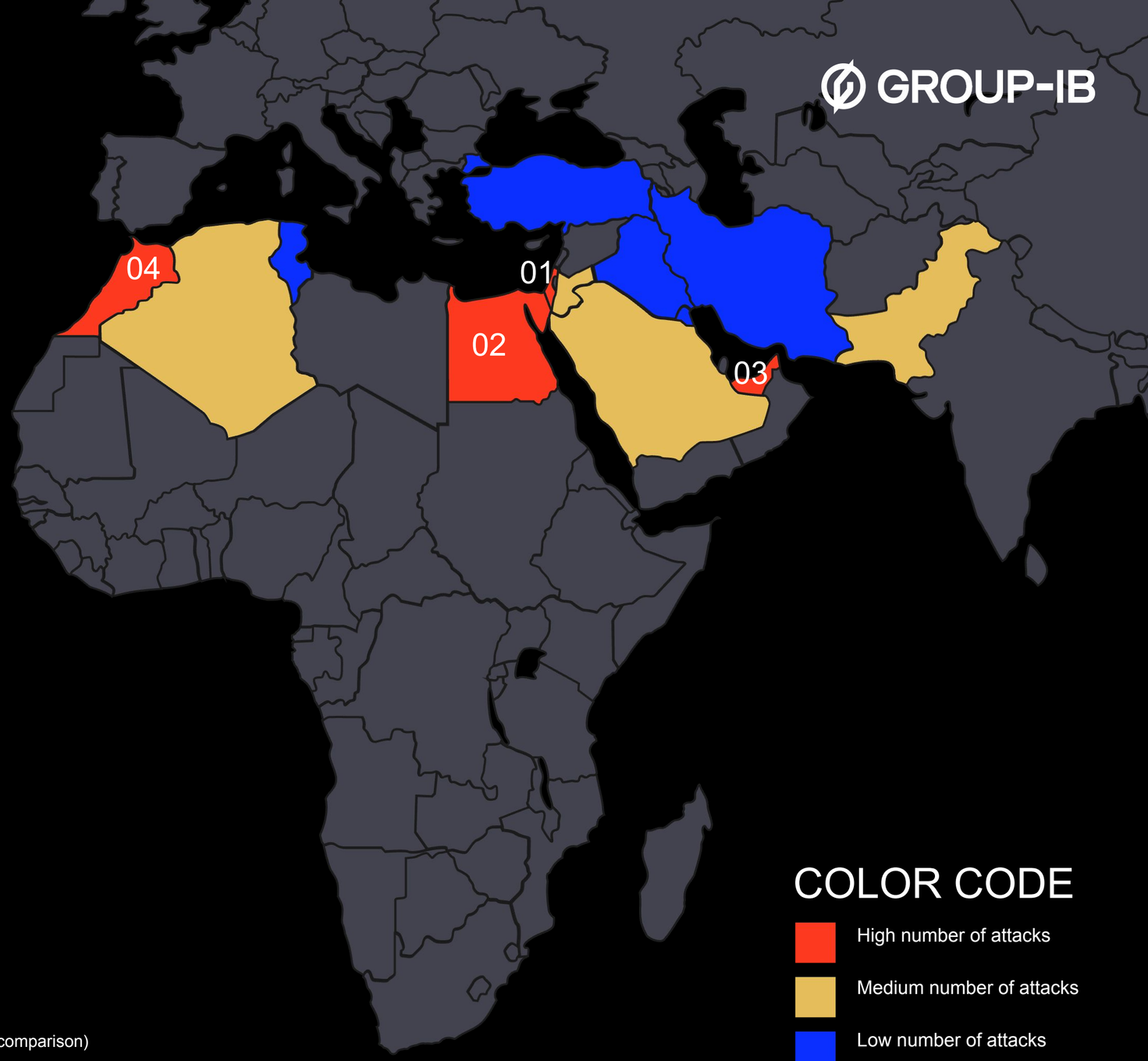
1. Fake Greek Real Estate Lure Targets MEA Region	In July 2025, Group-IB discovered campaign which involved a fake Greek real estate document, likely aiming to compromise users in the MEA region. The group used a DocuSign-themed lure that delivered a remote access tool after a fake CAPTCHA step. This operation follows their established tactics of abusing legitimate tools and services to evade detection and hinder attribution. This campaign has similarities to previous MuddyWater campaigns, as well as a Brazil-based threat cluster that utilize RMMs.
2. Group-IB Identifies New DarkBlinder Malware Sample in GCC: Multi-Stage Infection Chain Underway	The Group-IB team has observed a new wave of Classiscam phishing and scam campaigns targeting the GCC region. The team will keep clients informed about the threat.
3. Rise in QR Code-Based Phishing Attacks	In July 2025, Group-IB observed a surge in QR code phishing attacks aimed at credential theft, often impersonating employees or executives and spoofing organizational IT infrastructure.

Middle East,Türkiye, Africa & Pakistan

DDOS AND HACKTIVISM ATTACKS BY COUNTRY

The scope is comprised of attacks, DDOS and hacktivism.

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 DDOS / HACKTIVISM) BY COUNTRY (TOP 4-5)

01	02	03	04	
Israel	Egypt	GCC	Morocco	
152 attacks	44 attacks	16 attacks	13 attacks	
-66%	+7%	-75%	-63%	(June to July 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:

↑ 50% (June vs july)

9 Ransomware incidents

GROUP-IB

Most active threat actors

D4RK 4RMY

2 attacks

Qilin

2 attacks

WALocker

2 attacks

Devman

1 attack

fSociety

1 attack

Most targeted industries

Financial Services Banking

2

Messaging & Telecommunications

2 attack

E-commerce

1 attack

Real Estate & Construction

2 attack

Sports

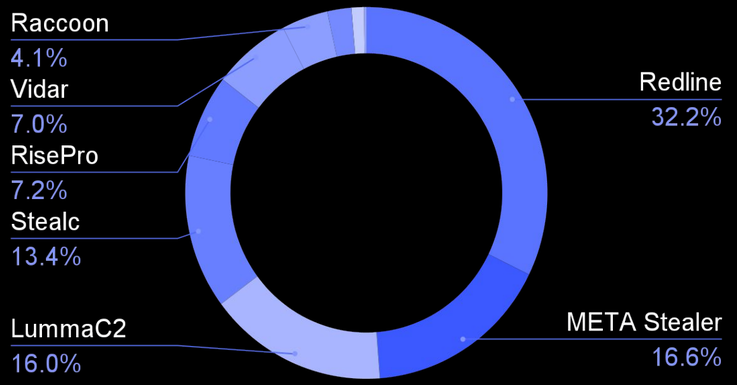
1 attack

STATISTICS: **COMPROMISED DATA**

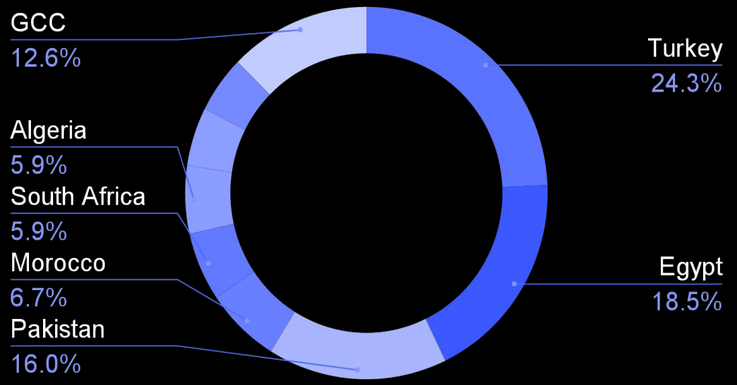
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational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

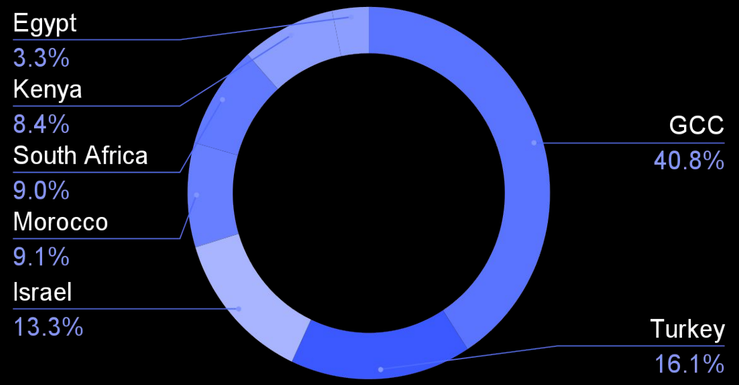
Compromise data by malware



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

GROUP-IB

[Talk to our team]

RECENT
RESOURCES

Read now

Watch now

Register now