GROUP-IB

MIDDLE EAST, TÜRKIYE & AFRICA

INTELLIGENCE INSIGHTS

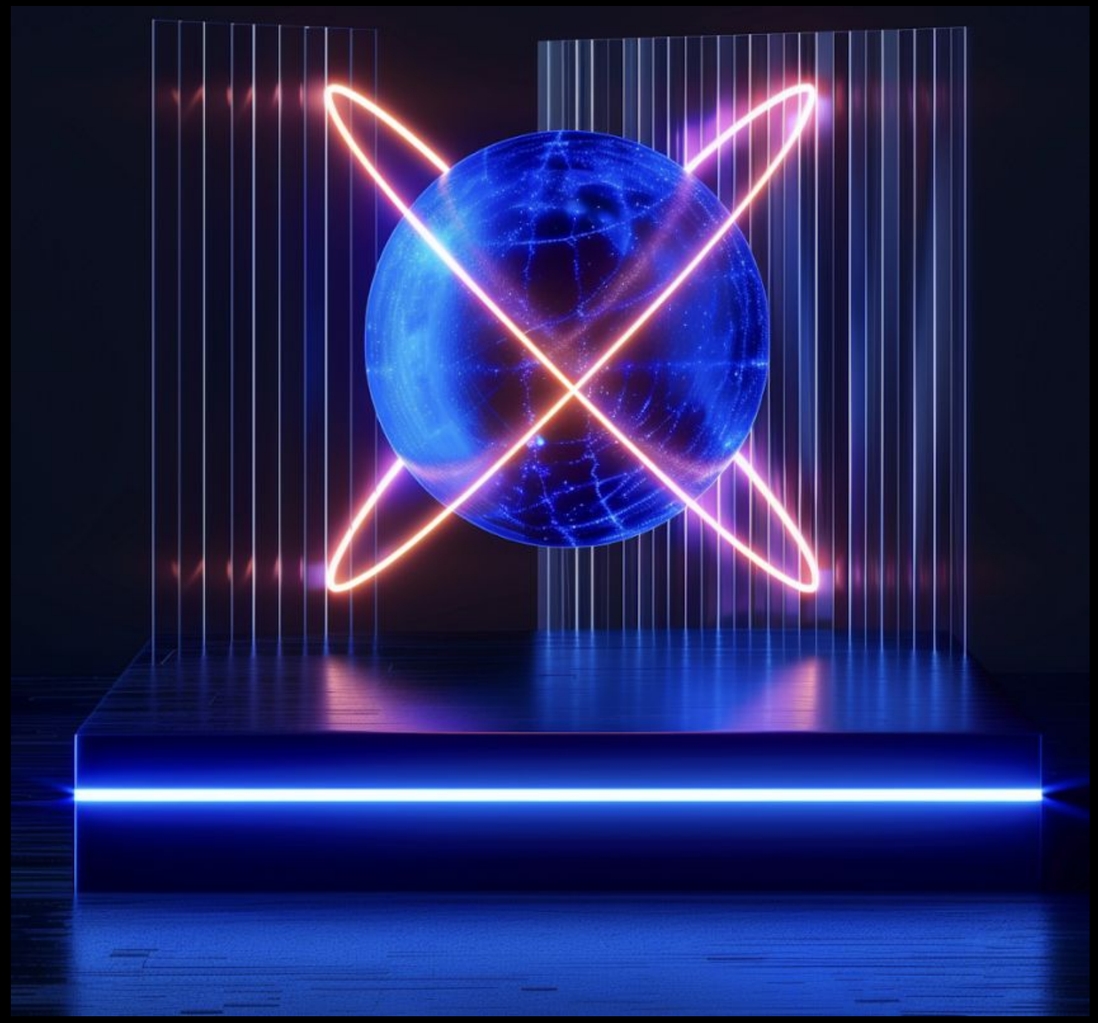
May, 2025

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:

- **Google/ Mandiant distils five essentials help-desk verification, phishing-proof MFA, healthy-device enforcement, tight network segmentation, and focused detections—to blunt UNC 3944 (“Scattered Spider”) SIM-swap and ransomware attacks.**
- **RansomHub, a Knight/Cyclops offshoot, enticed LockBit and ALPHV vets with a 90 / 10 payout and cross-platform locker, then disappeared on 1 Apr 2025, with signs its crew moved to Qilin.**



Group-IB specialists discovered multiple phishing and scam campaigns and took active steps to negate 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 with a brief description:

1. Disguised Cyber Risks On The Colombian Shore: The Insurance Trap	Group-IB revealed a Colombian “Insurance Trap” in which more than 100 cloned car-insurance sites, promoted via Facebook ads and WhatsApp, query the public SOAT database with a victim’s licence-plate to appear legitimate and, if coverage is expired, funnel motorists to counterfeit PSE payment pages or QR codes that steal their banking credentials—an elegant example of open data and polished UX being weaponized for fraud.
2. Ransomware debris: an analysis of the RansomHub operation	Group-IB’s post charts how RansomHub, born from the bought-out Knight/Cyclops codebase, wooed ex-LockBit and ALPHV affiliates with an unprecedented 90/10 profit split and a cross-platform locker plus scripted extortion (even urging threats to regulators), only to disappear on 1 April 2025—with telemetry suggesting many of its operators are now swelling Qilin’s ranks.
3. Defending Against UNC3944: Cybercrime Hardening Guidance from the Frontlines	Google Cloud’s security team says the best way to block the SIM-swap and ransomware group UNC 3944 (“Scattered Spider”) is to lock down five basics: (1) make help-desk staff positively verify users’ identities, (2) drop SMS/e-mail codes in favour of phishing-proof MFA like FIDO2 keys, (3) allow access only from devices that pass health checks and run your EDR, (4) keep admin portals and critical services on segmented, egress-restricted networks, and (5) hunt for the group’s tell-tale social-engineering and MFA-bypass tricks in your logs.

REGIONAL TRENDS

Key regional trends with a brief description:

01 Group-IB Uncovers “DarkBlinders”: New Nation-State APT Linked to SHELBY Malware Emerges from Iraq

During ongoing threat hunting operations, the GROUP-IB Threat Intelligence team identified multiple malicious files that were uploaded to VirusTotal from Iraq on 30/04/2025. Further analysis revealed that these files belong to the SHELBY malware family, a recently discovered strain attributed to a newly identified threat actor designated as DarkBlinders by GROUP-IB (named in reference to the group's thematic use of 'Peaky Blinders' iconography). Concurrently, Elastic has published independent research on the same actor, assigning the identifier REF8685. Although the actual motives of the Threat Actor remain unknown at this time (due to lack of data), based on their victims, toolset and sophisticated TTPs, the GROUP-IB Threat Intelligence team assesses with moderate confidence that this is a National-State APT.

Middle East, Türkiye and Africa

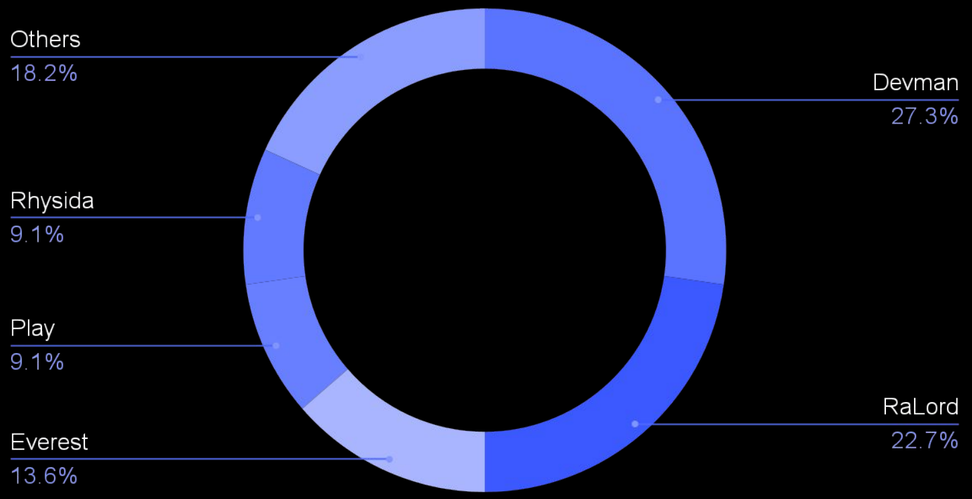
STATISTICS: **CYBER ATTACKS**

GROUP-IB

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:

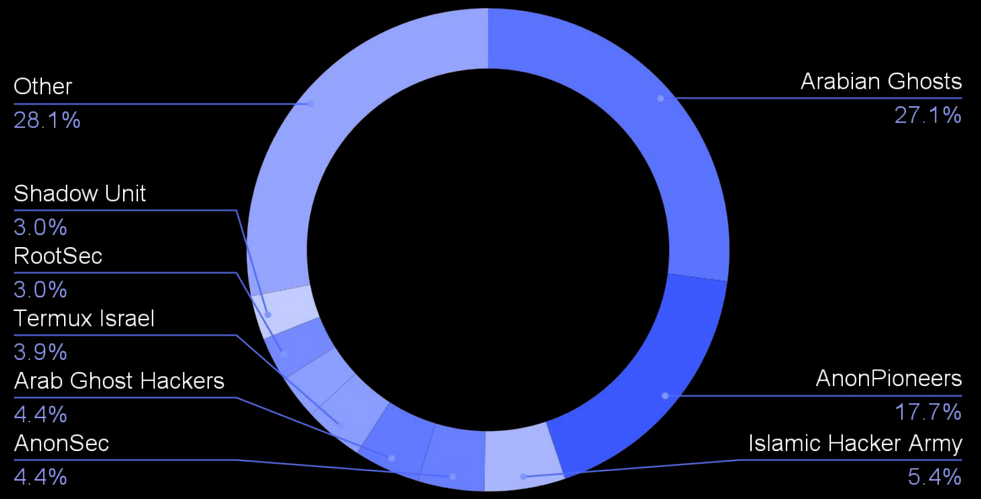
RANSOMWARE attacks per group



HACKTIVISM ACTIVITIES

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 year these groups attracted a lot of attention. Below is a brief overview of groups that were active in the META region during May 2025:

HACKTIVISM Attacks per group

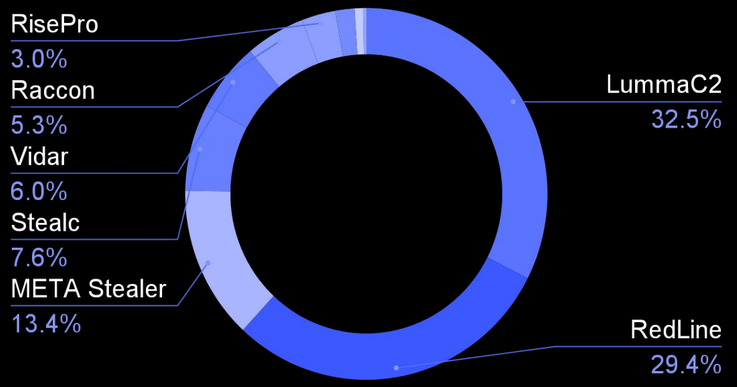


STATISTICS: **COMPROMISED DATA**

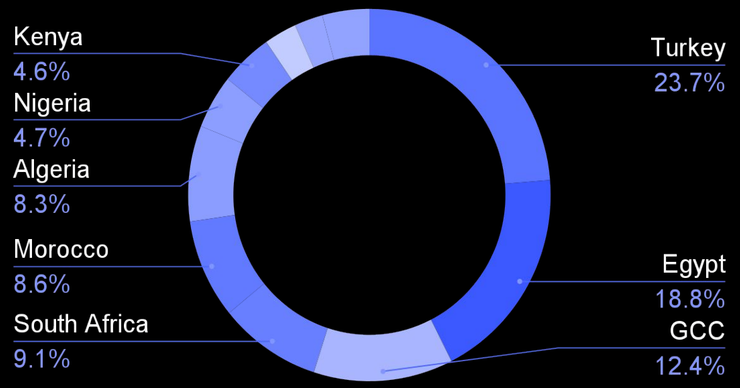
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational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

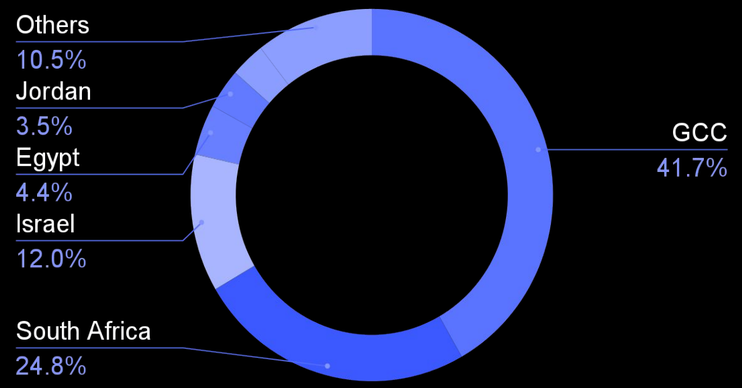
Compromise data by malware



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

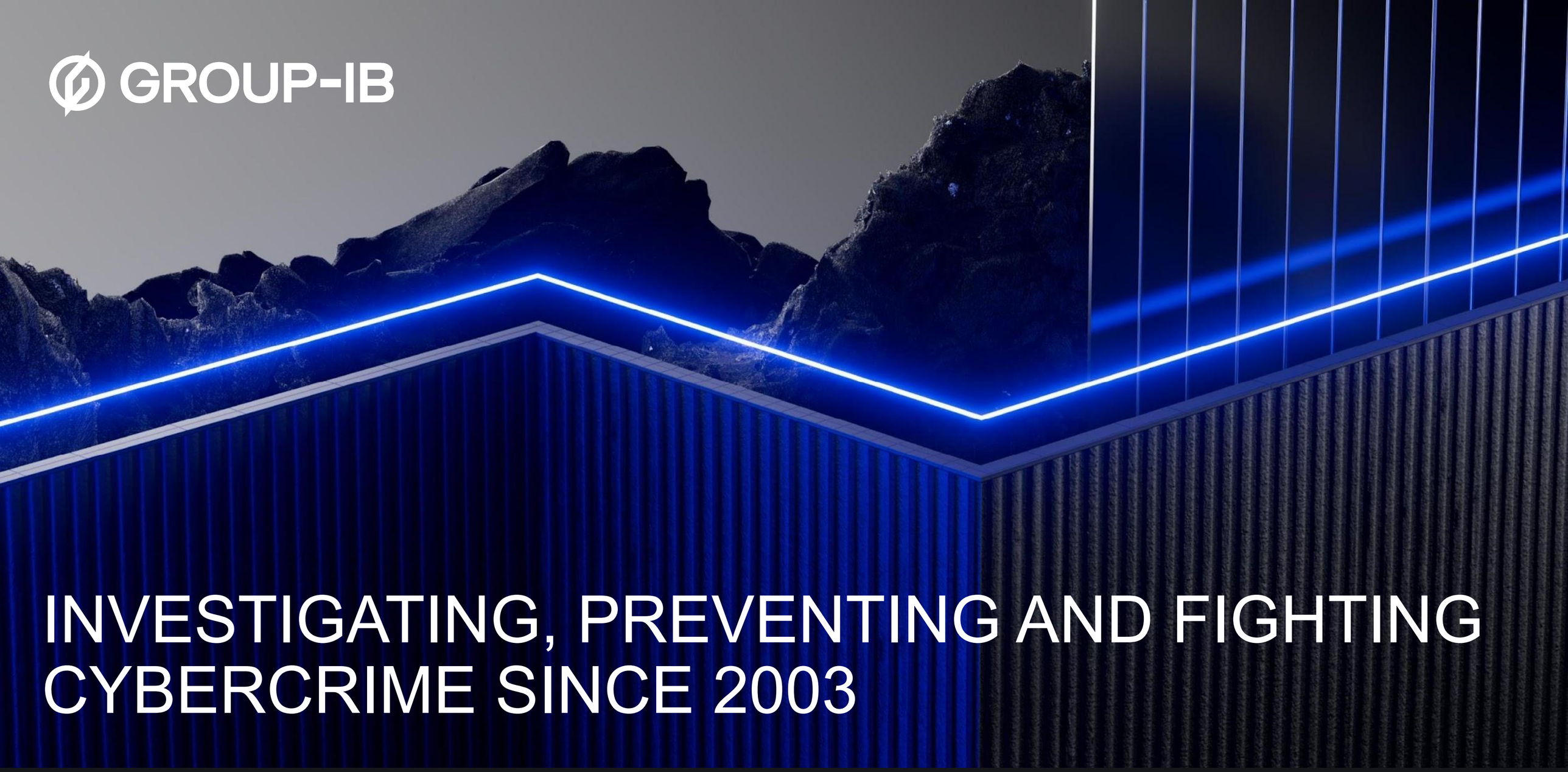
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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.



INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM
GROUP-IB.COM/BLOG
+971 45681785

LINKEDIN FACEBOOK TWITTER INSTAGRAM