GROUP-IB

MIDDLE EAST, TÜRKIYE & AFRICA

INTELLIGENCE INSIGHTS

April, 2025

INTRODUCTION

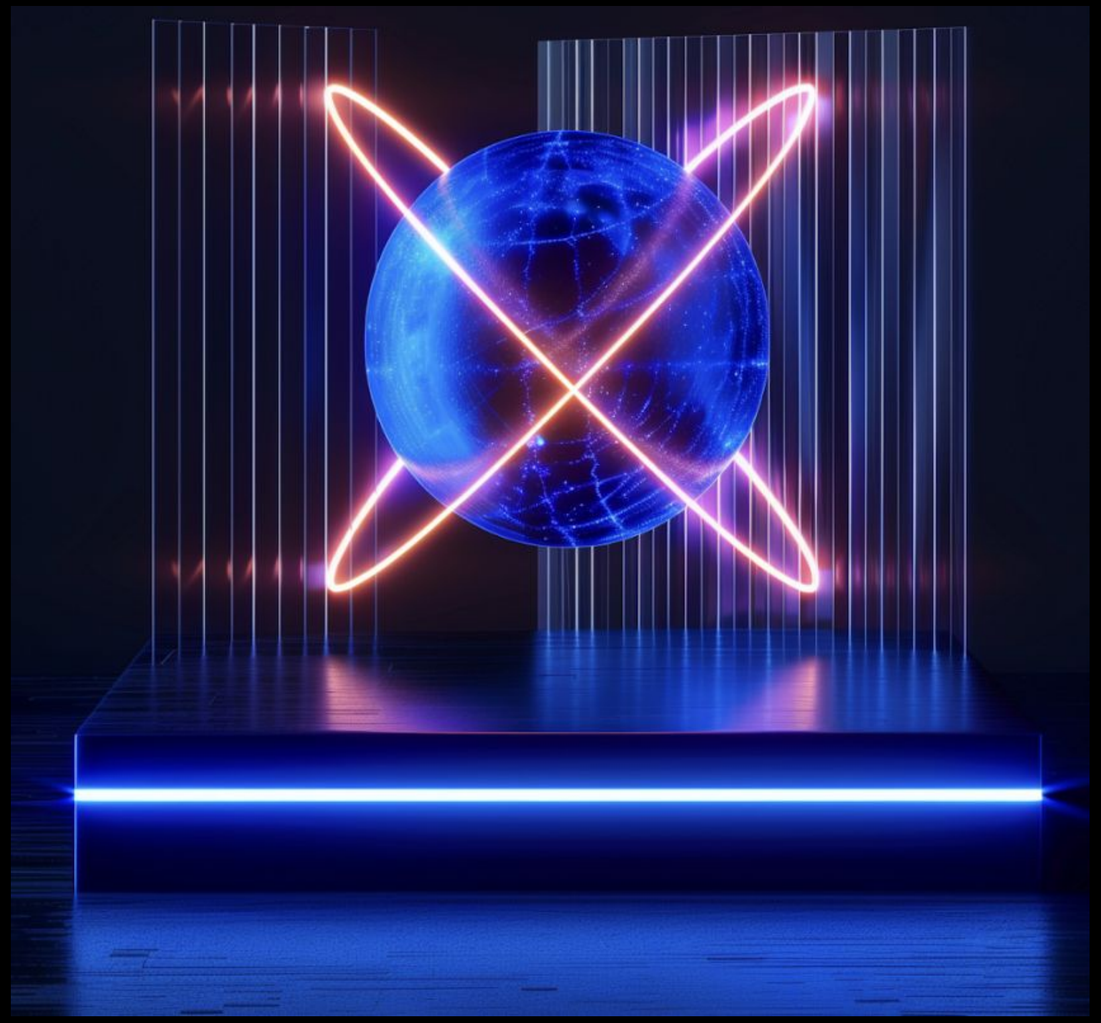
This report contains information on the most significant cybersecurity events that occurred worldwide and in the META region over the last two months.

2 notable
events of the month:

- **A threat actor known as rose87168 offered for sale data allegedly stolen from Oracle.**

- **A joint operation by Group-IB, the Royal Thai Police, and the Singapore Police Force led to the arrest of a cybercriminal known by aliases such as ALTDOS and DESORDEN, responsible for over 90 global data breaches and the theft of more than 13 terabytes of personal data.**

Group-IB specialists discovered multiple phishing and scam campaigns and took active steps to negate their disruptive impact. We want to highlight that **Group-IB customers are well-protected** and aware about such types of threats.



GLOBAL TRENDS

GROUP-IB

Global trends with a brief description:

1. Oracle Cloud Breach: Threat Actor Attempts to Sell Stolen Data	In March 2025, a threat actor known as **rose87168** offered for sale data allegedly stolen from Oracle, the American multinational computer technology corporation—specifically targeting its Oracle Cloud services. The attacker claimed the breach occurred in January 2025 and initially attempted to negotiate a private sale with Oracle, which was reportedly unsuccessful.
2. Global Cybercriminal Behind 90+ Data Breaches Arrested in Thailand	Group-IB, in collaboration with the Royal Thai Police and the Singapore Police Force, successfully apprehended a cybercriminal responsible for over 90 data breaches worldwide. The individual, operating under aliases such as ALTDOS, DESORDEN, GHOSTR, and 0mid16B, targeted large private companies across various sectors, including finance, retail, and manufacturing. Group-IB's Threat Intelligence and High-Tech Crime Investigation teams tracked the cybercriminal across multiple aliases, contributing significantly to the investigation. The arrest took place on February 26, 2025, in Thailand, marking a significant milestone in combating global cybercrime.
3. ClickFix: New Social Engineering Tactic Targets Users with Clipboard Malware	The Group-IB published the comprehensive blog describes a social engineering technique called ClickFix, usually used by attackers to trick users into executing malicious PowerShell scripts. Victims are lured into clicking fake "Fix It" buttons or CAPTCHA prompts, which copy malware code to their clipboard and instruct them to run it manually. This method has been used to deliver infostealers like **Lumma** and has gained popularity among cybercriminals (even APT groups). Group-IB warns of its growing use and advices increase in user awareness to prevent compromises.

REGIONAL TRENDS

Key regional trends with a brief description:

01 Dark Blinders APT Group Uncovered: Targeted Attacks on Iraqi Telecoms Using Peaky Blinders-Themed Infrastructure

During continuous threat monitoring, the Group-IB Threat Intelligence team identified several targeted campaigns against the Iraqi Telecommunication companies attributed to a single APT group. The group's TTPs and toolset do not align with those of any previously known threat actors, indicating a distinct and unique operational profile. **Elastic** published a public blog post detailing the group's activity and gave it the name REF8685. The Group-IB team assigned the name “Dark Blinders” to the APT group, due to its active usage of a Peaky Blinders theme, incorporating names of the Shelby brothers in their usernames and domain infrastructure. In addition, a distinctive feature of the group is the use of well-crafted phishing emails, custom modular .NET applications, and the use of GitHub platform as C2 and, in another case, DNS tunneling.

Middle East, Türkiye and Africa

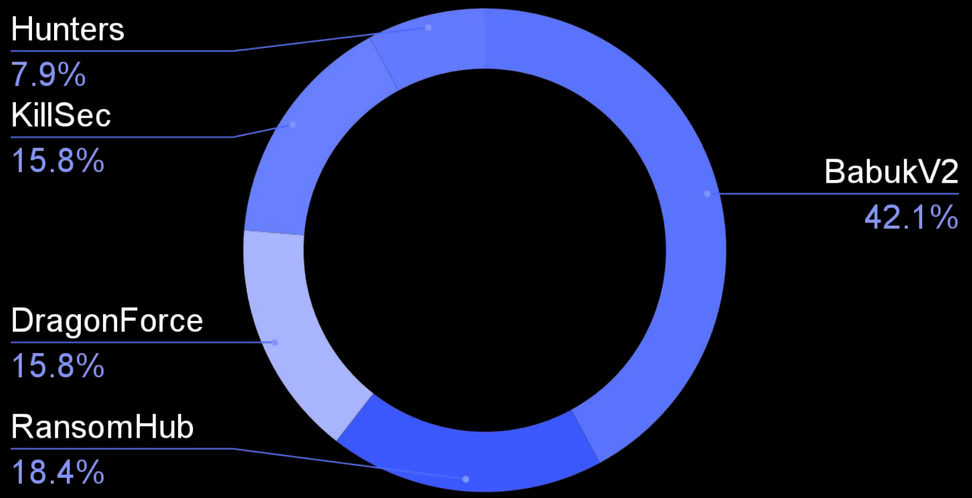
STATISTICS: **CYBER ATTACKS**

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:

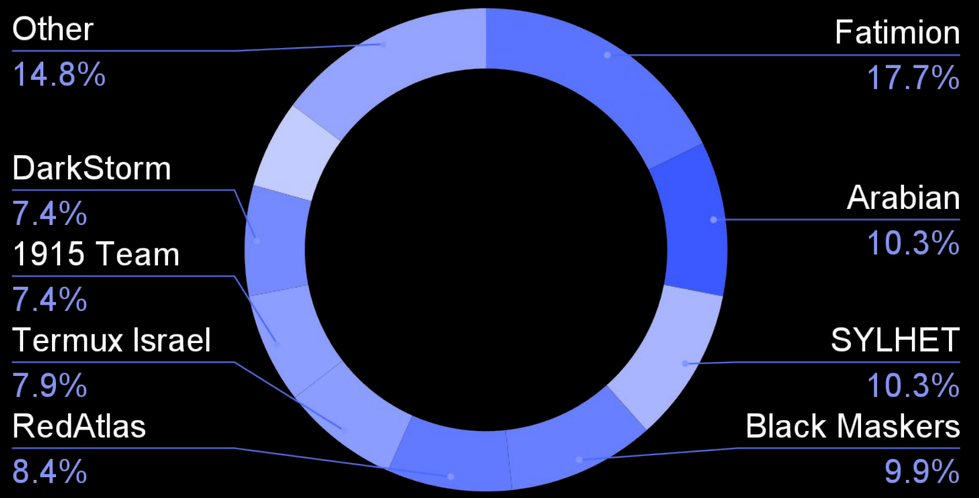
RANSOMWARE attacks per group



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 the March,2025:

HACKTIVISM Attacks per group

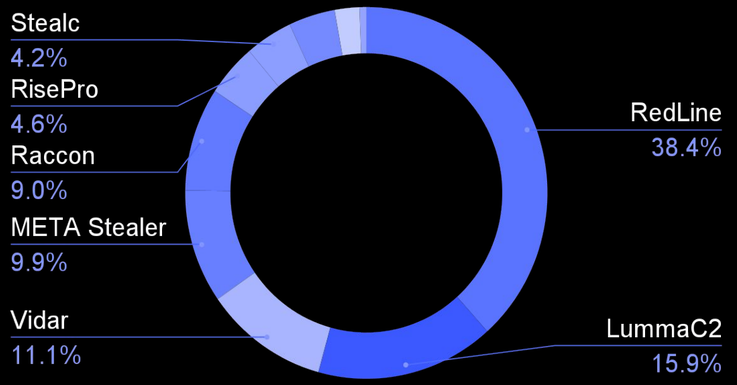


STATISTICS: **COMPROMISED DATA**

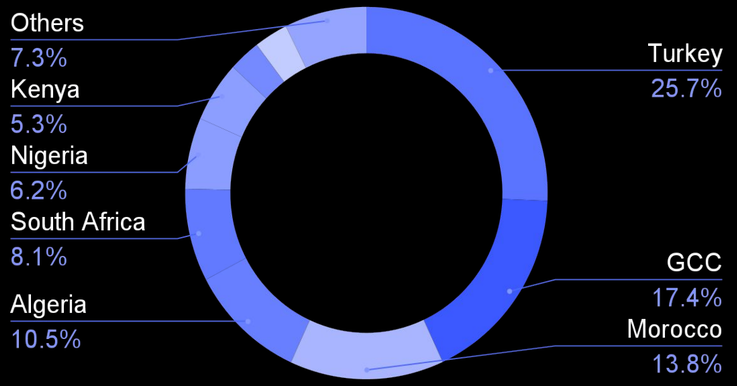
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational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

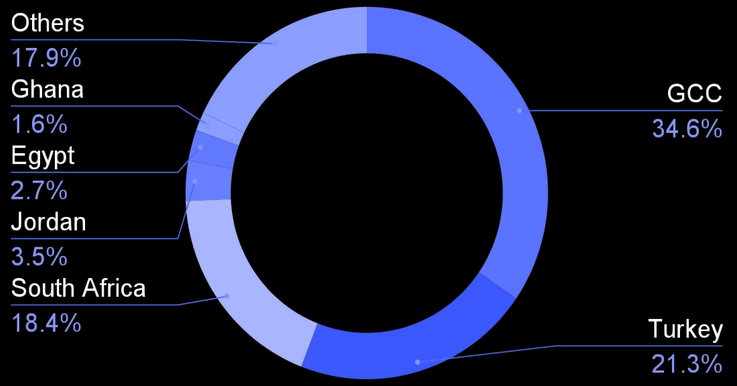
Compromise data by malware



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

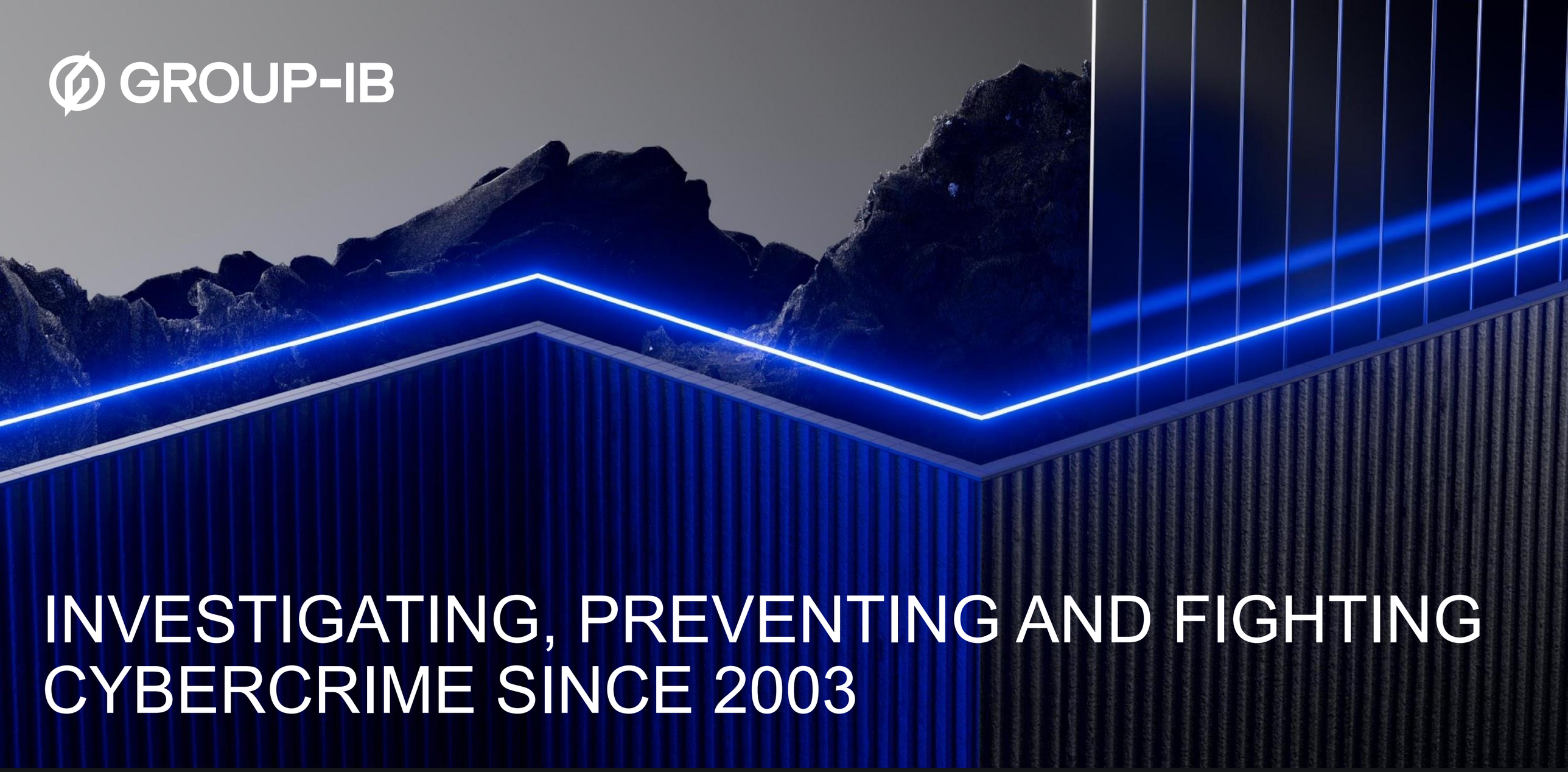
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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