GROUP-IB

MIDDLE EAST, TÜRKIYE & AFRICA

INTELLIGENCE INSIGHTS

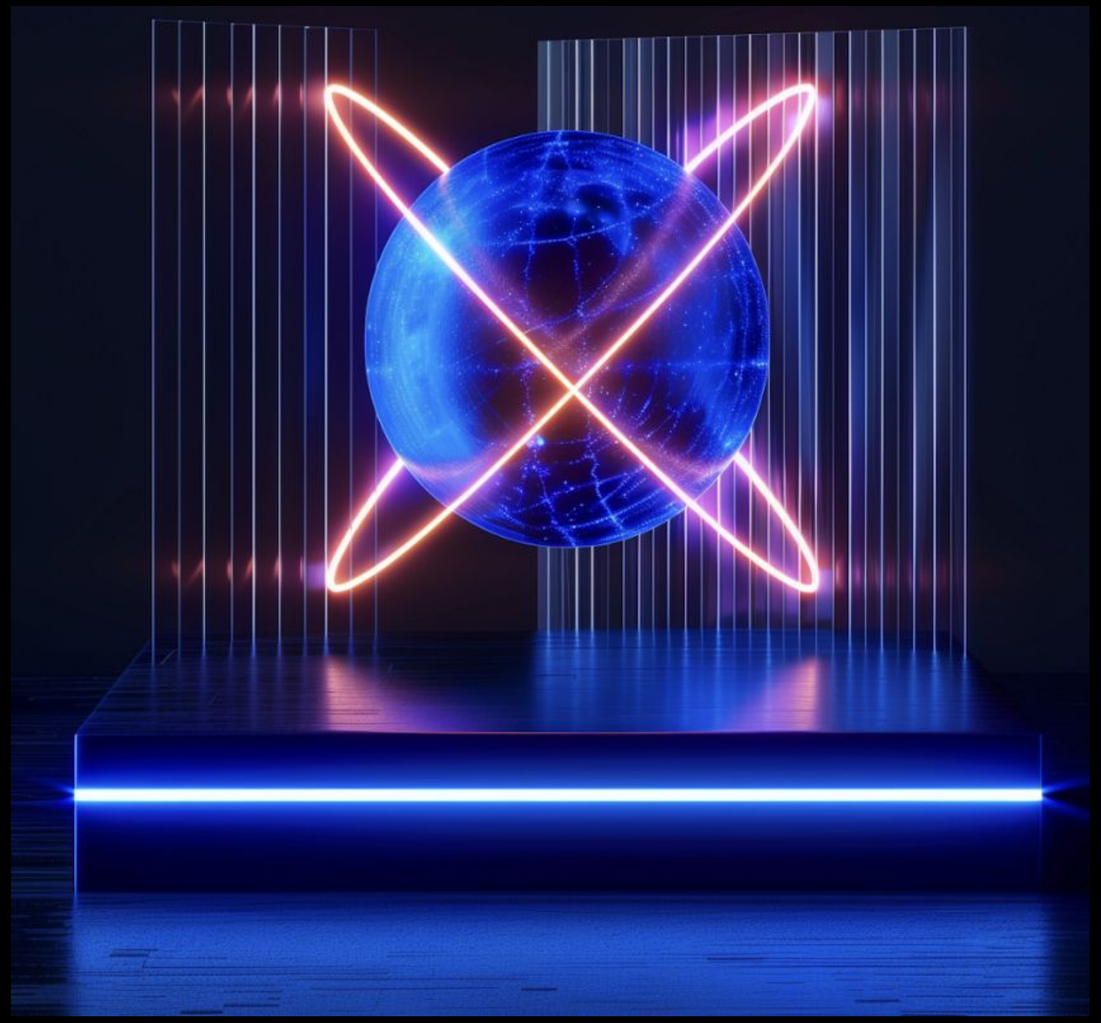
February, 2025

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 published the blog where it explained how cybercriminals exploit AI and automation for card testing attacks, using bots and proxies to evade detection, highlighting the need for advanced fraud prevention systems.**
- **Group-IB published the first chapter of research of RansomHub - the group that might become the top ransomware threat in 2025.**



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

Global trends with a brief description:

01	Group-IB published the blog about card testing scheme	The blog post titled "The Dark Side of Automation and Rise of AI Agents: Emerging Risks of Card Testing Attacks" by Group-IB delves into how cybercriminals are exploiting advanced automation and AI technologies to conduct card testing attacks. These attacks involve fraudsters using stolen credit card information to make small, often unnoticed purchases to verify the card's validity before committing larger fraudulent transactions.By leveraging bots, proxies, and automation tools, attackers can efficiently test numerous cards while evading detection.The article emphasizes the challenges this poses for real-time fraud prevention and underscores the need for advanced detection systems that can identify and mitigate such automated threats.
02	Group-IB published blogpost about RansomHub Ransomware group	This blogpost by Group-IB examines the emergence of RansomHub, a Ransomware-as-a-Service (RaaS) group that surfaced in early 2024. Capitalizing on law enforcement actions against groups like LockBit and ALPHV, RansomHub recruited affiliates and acquired ransomware source code from the defunct Knight group.Their ransomware is versatile, targeting various operating systems, including Windows, ESXi, Linux, and FreeBSD.Notably, RansomHub has compromised over 600 organizations globally, with a significant focus on the healthcare sector. The article underscores the group's adaptability and the evolving nature of ransomware threats.

REGIONAL TRENDS

Key regional trends with a brief description:

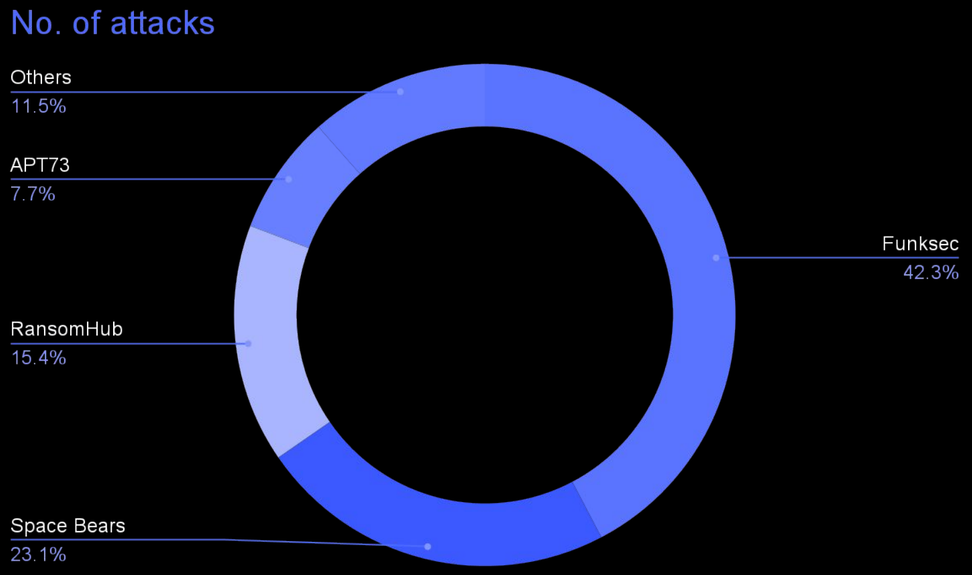
01	Returning of the MuddyWater APT group	After one month break MuddyWater group continued spreading of RMM tools. In January 2025, MuddyWater launched targeted campaigns in the MEA region, leveraging RMM tools to maintain remote access and control over compromised systems. These operations follow their established tactics of abusing legitimate tools and services to avoid detection and complicate attribution.

Middle East, Türkiye and Africa

STATISTICS: **ATTACKS**

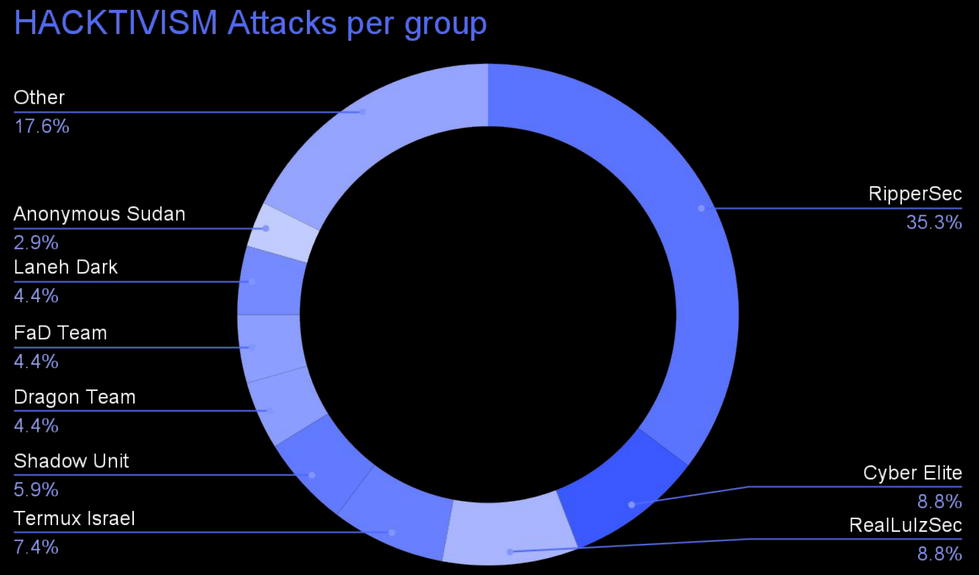
RANSOMWARE ACTIVITIES

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:



HACKTIVISM ACTIVITIES

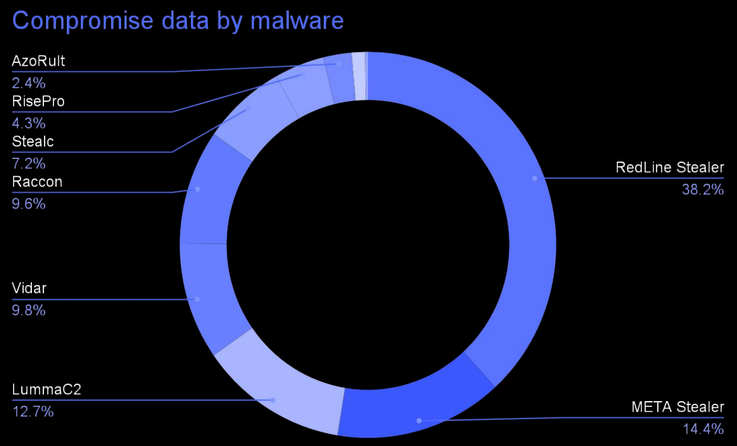
Hacktivism is the use of hacking to promote political or social agendas. Usually hacktivist groups are low-skill hackers who perform DDoS, Defacement, and Data Breaches (mostly leverages compromised accounts) attacks. Unfortunately, during the last year these groups attracted a lot of attention. Below is a brief overview of groups that were active in the region during the previous month.

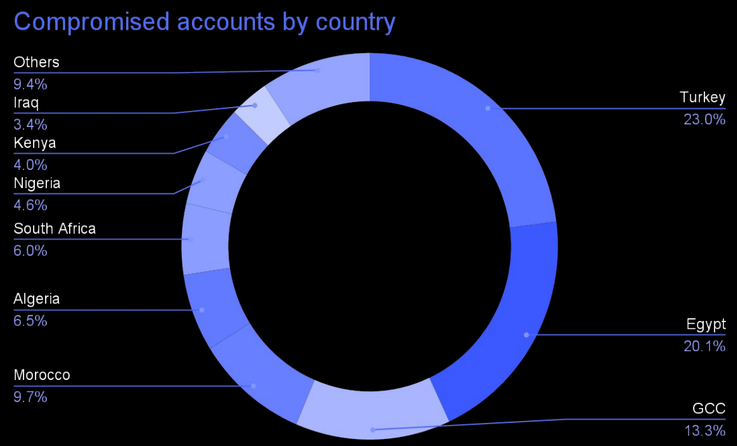


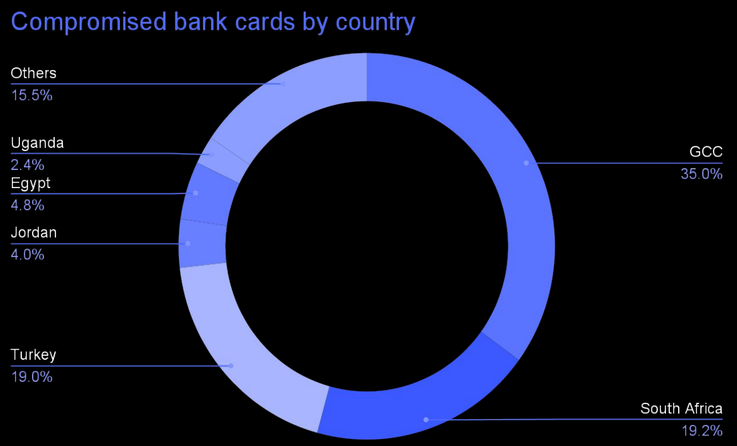
STATISTICS: **COMPROMISED DATA**

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.







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

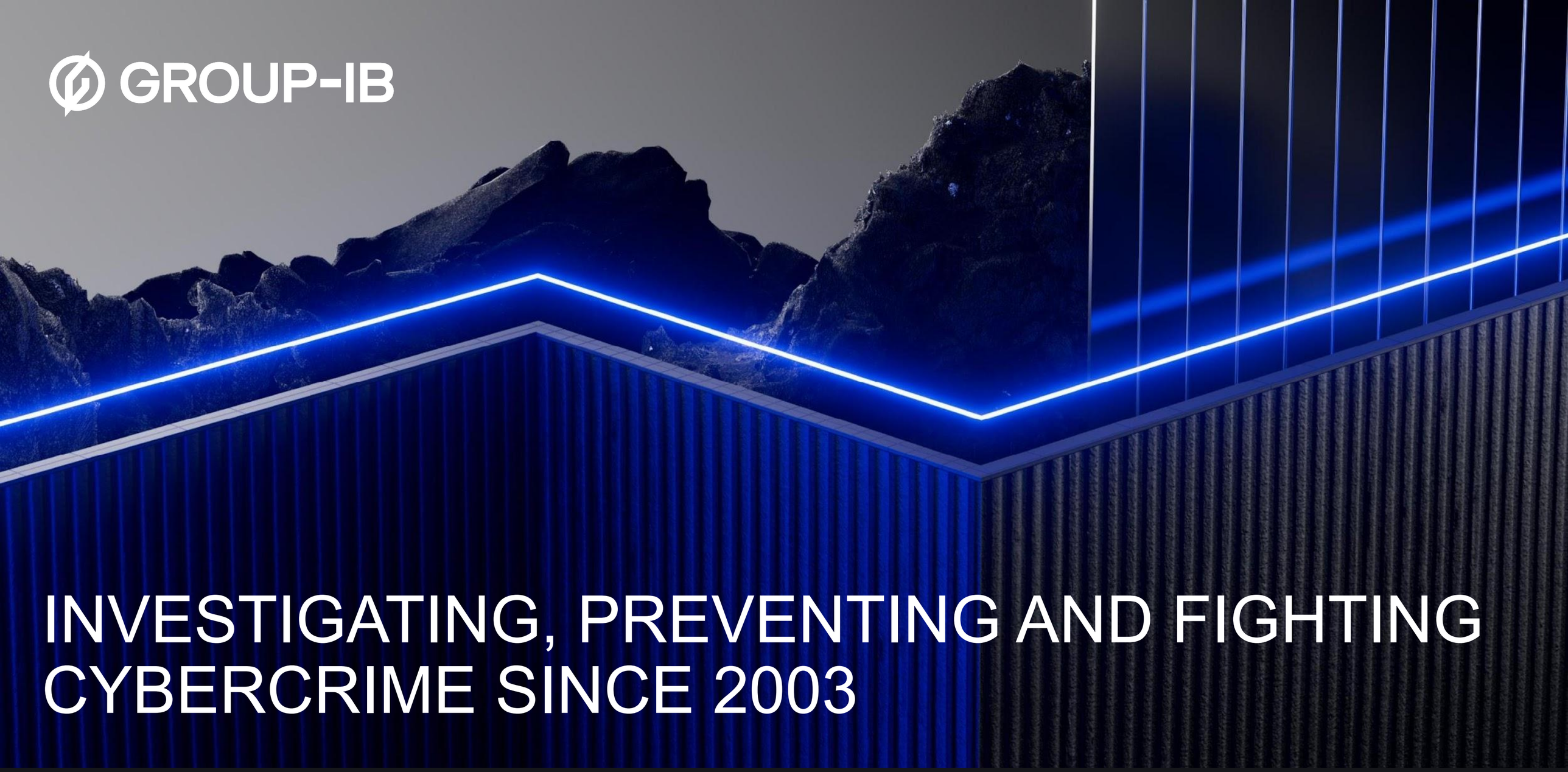
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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