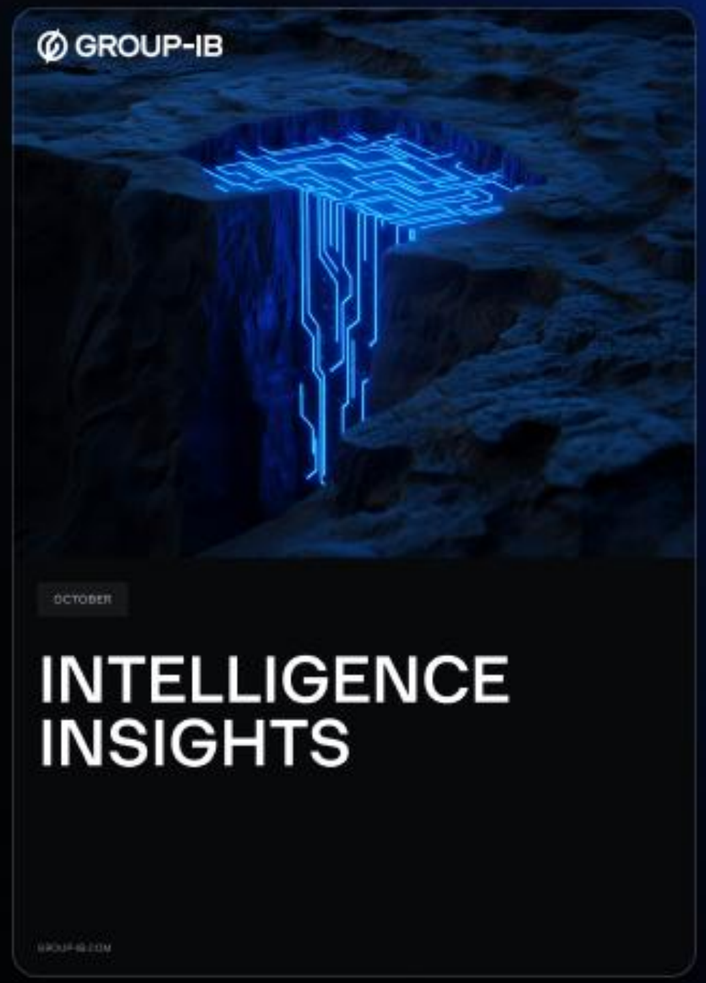
GROUP-IB



OCTOBER INTELLIGENCE INSIGHTS

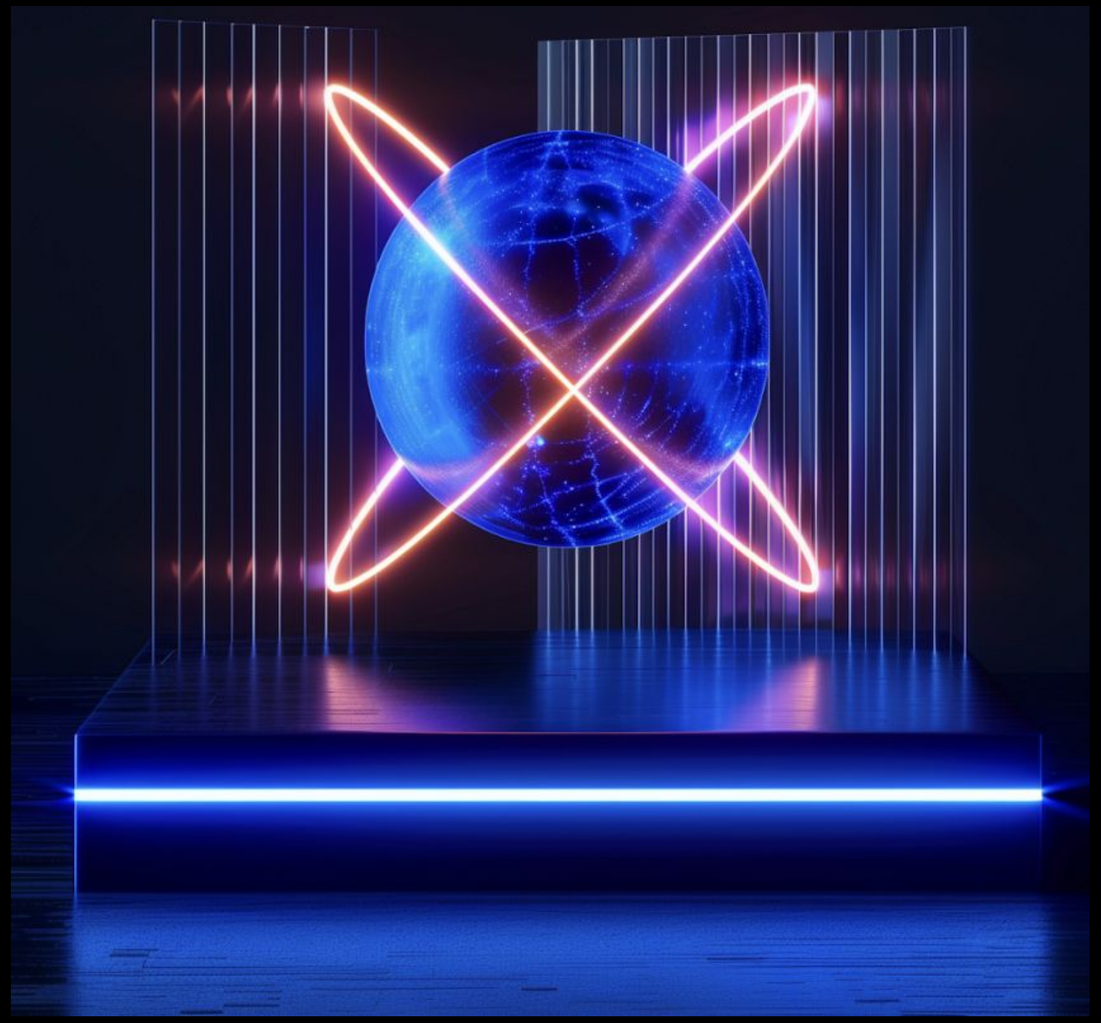
Executive Summary and Key Findings
Middle East, Türkiye and Africa

INTRODUCTION

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

2 most striking events of the month:

- **Group-IB specialists uncovered a large-scale fraud campaign involving fake trading apps targeting Apple iOS and Android users**
- **Group-IB contributed to INTERPOL's "Operation Contender 2.0" which led to the arrest of two individuals by the Nigerian Police Force**



Group-IB specialists discovered several notable phishing and scam campaigns. 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:

01	Group-IB exposes TeamTNT's ongoing cloud infrastructure attacks: Stealthy Malware Targets VPS Environments with Advanced Rootkits	TeamTNT targets VPS on CentOS using SSH brute force and malicious scripts to disable security, kill mining processes, and modify DNS. Group-IB revealed their use of the Diamorphine rootkit for stealth and root access, along with backdoor creation and log erasure to hide activities. More details
02	Group-IB specialists uncovered a large-scale fraud campaign involving fake trading apps targeting Apple iOS and Android users	Cybercriminals use fake trading apps to lure victims and steal funds, often starting contact through dating apps. These fraudulent apps, built using the UniApp Framework and dubbed UniShadowTrade by Group-IB, support multiple languages. They have been found in the Apple App Store and Google Play, with victims detected globally. More details
03	Group-IB uncovers DragonForce ransomware tactics and affiliate program: Double extortion attacks target key industries with advanced tools	DragonForce runs a Ransomware-as-a-Service program using LockBit3.0 and ContiV3 variants, employing double extortion to encrypt data and demand ransom. Affiliates receive 80% of profits and tools for customizing attacks. Group-IB has revealed the attackers use of advanced defense evasion techniques and targeting of 82 victims across industries like manufacturing and real estate. More details
04	Group-IB contributed to INTERPOL's "Operation Contender 2.0." which led to the arrest of two individuals by the Nigerian Police Force	These two individuals had a role in a romance scam that resulted in significant financial losses for a victim in Finland. As an INTERPOL Gateway Partner, Group-IB provided critical intelligence that helped the law enforcement pinpoint and apprehend these cybercriminals. More details

REGIONAL TRENDS

GROUP-IB

Key regional trends with a brief description:

01 MuddyWater’s Cyber Campaign in the MEA Region: Leveraging Legitimate RMM Tools, File-Sharing Services, and Social Engineering	In September 2024, the MuddyWater threat group launched targeted cyber campaigns across the Middle East and Africa, using remote monitoring and management (RMM) tools to maintain access to compromised systems. This tactic aligns with their strategy of abusing legitimate software to evade detection. Their attacks often use RMM software delivered via trusted file-sharing services to bypass security filters. They also employ advanced social engineering, frequently using spear-phishing emails that mimic legitimate institutions. While the exact infection methods in this campaign are unclear, phishing is likely based on past attacks.
02 APT34 has intensified cyberattacks on government sectors in the UAE and Gulf region, exploiting critical infrastructure vulnerabilities.	They use a new backdoor which facilitates the exfiltration of sensitive credentials, including accounts and passwords, through on-premises Microsoft Exchange servers. APT34 has been observed using technique of abusing the dropped password filter policy - this technique enables attackers to extract clean-text passwords, further compromising the integrity of targeted systems. The group also utilizes ngrok for persistent access and exploits CVE-2024-30088 for privilege escalation, showcasing their ability to adapt. These activities highlight the ongoing threat posed by state-sponsored actors on backdrop of the tension in the Middle East region.
03 Threat Actor Jackoshh Advertises 'X-Panel' Phishing Service Targeting MEA Banks on Exploit[.]in Forum	The threat actor Jackoshh has advertised a new phishing service called "X-Panel" on the Exploit[.]in forum, targeting banks in the Middle East and Africa (MEA) region. Group-IB specialists contacted him via Telegram to gather more information about the service. Jackoshh shared proof videos showcasing phishing pages he developed for several banks, demonstrating the broad potential for malicious use.

Middle East, Türkiye and Africa

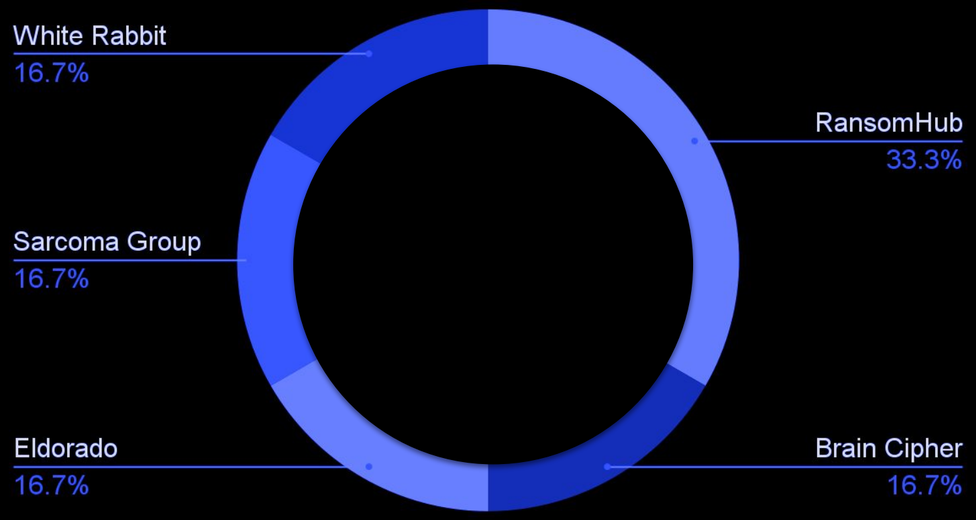
STATISTICS. **ATTACKS**

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:

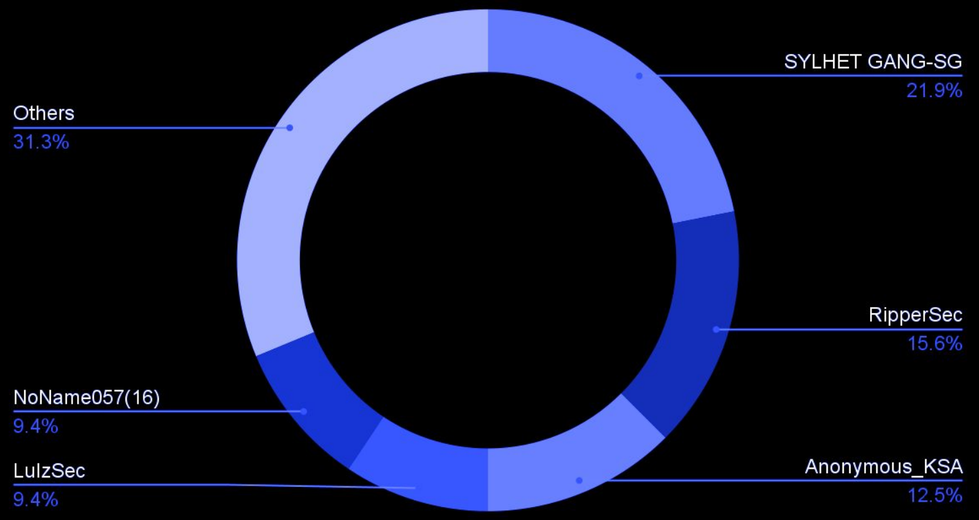
RANSOMWARE Attacks per Group



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 will be provided a brief overview of groups that were active in the region during the previous month.

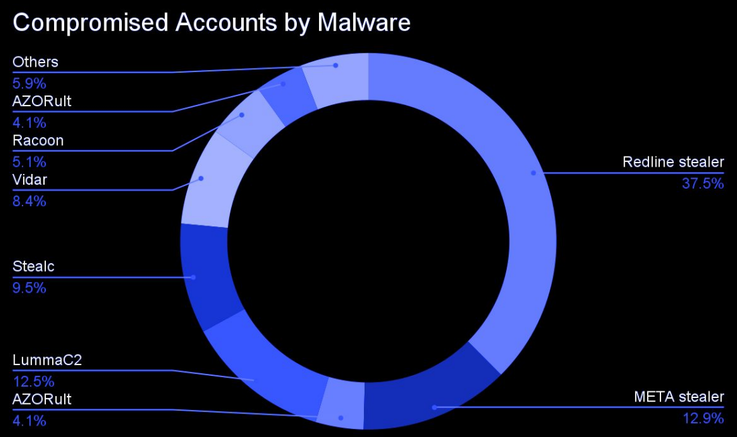
HACKTIVISM Attacks per Group

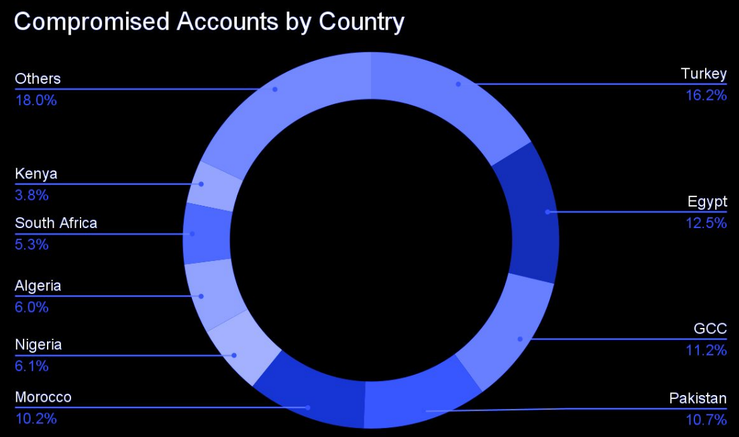


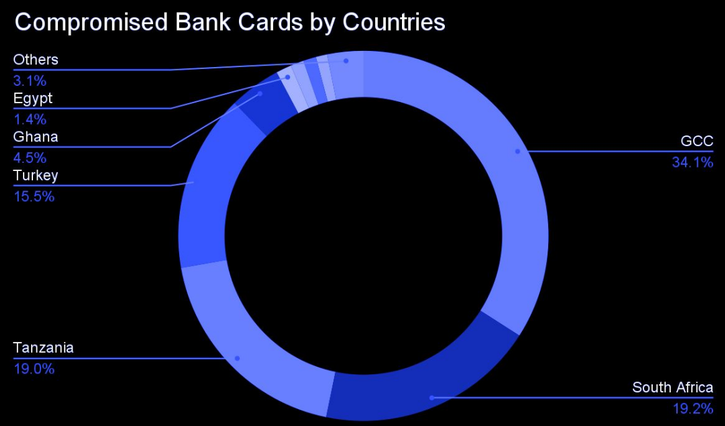
STATISTICS. **COMPROMISED DATA**

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 will provide statistics regarding compromised accounts and compromised cards — it will help 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 robust 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

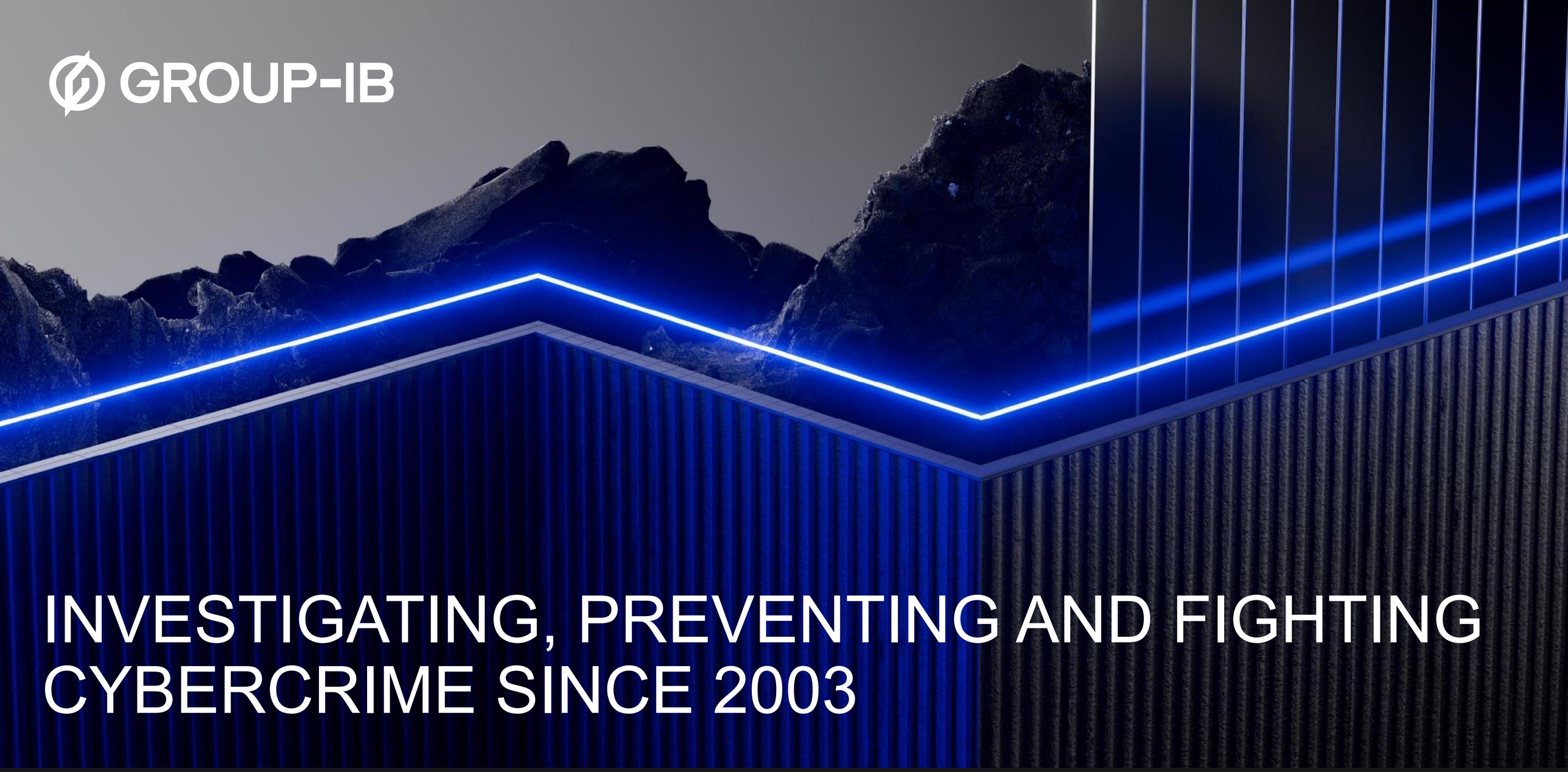
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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