GROUP-IB


# NOVEMBER INTELLIGENCE INSIGHTS

Executive Summary and Key Findings

Download the full report

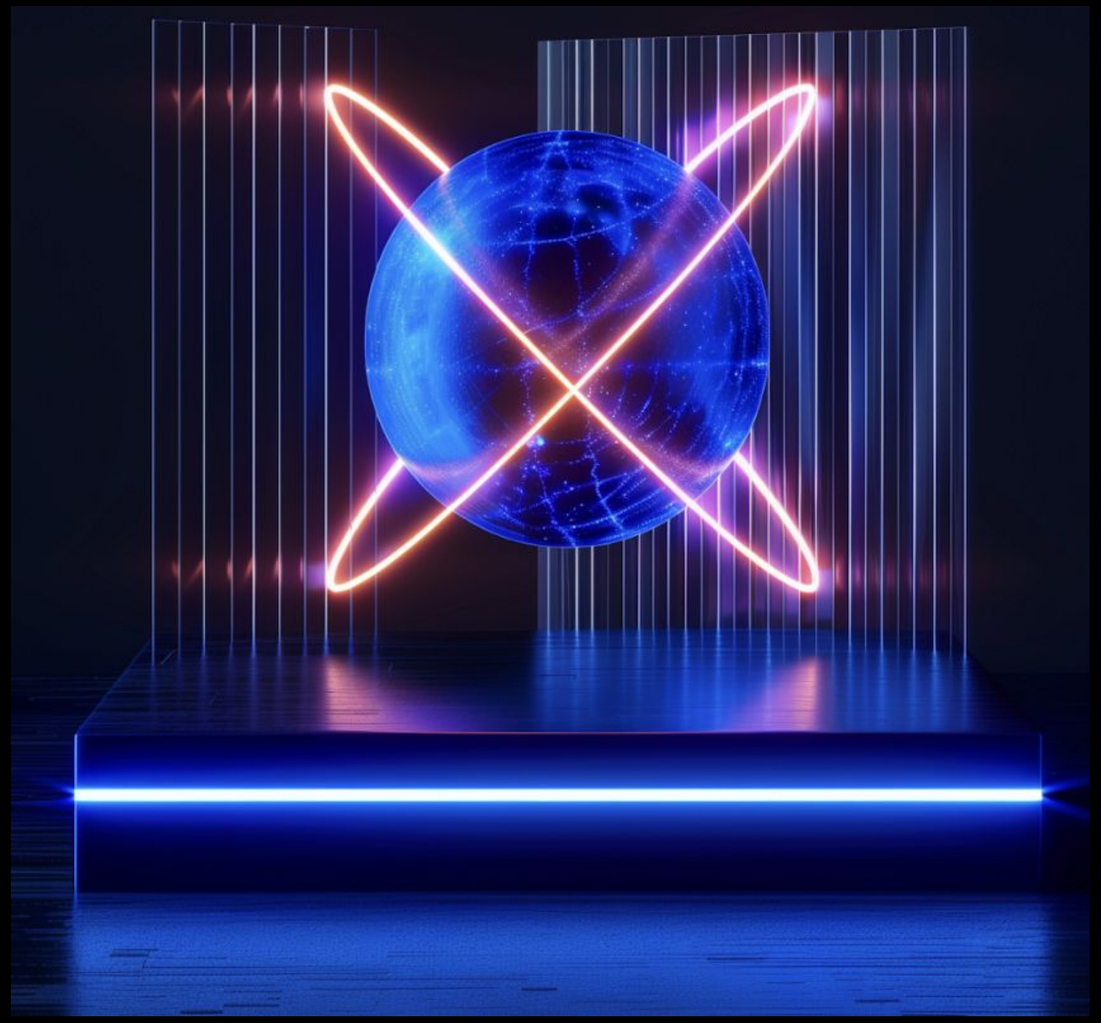
# INTRODUCTION

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 discovered utilization of the fake reCAPTCHA technique by MuddyWater APT group**

- **Group-IB discovered increase in sales of access and databases of organizations in the region for the past 6 months**



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:

| | | |
|---|---|---|
| 01 | Group-IB published detailed research of the Cicada3301 Ransomware-as-a-Service Group | Group-IB recently and successfully gained access to the Cicada3301 ransomware affiliate panel. We share the inner workings of the group in our recently published blog, based on our thorough analysis of the available ransomware versions offered within the affiliate panel, and all accessible sections. |
| 02 | Lazarus APT's Stealth Tactics with Extended Attributes Uncovered by Group-IB specialists | Group-IB specialists have uncovered a novel Lazarus APT technique that hides malicious code in extended attributes, evading detection on macOS. This method, absent from the MITRE ATT&CK framework, includes a new trojan, "RustyAttr," developed with the Tauri framework and undetected by VirusTotal. While macOS Gatekeeper blocks unsigned apps, social engineering poses a significant risk, highlighting the need for robust security measures against evolving threats. Read more |
| 03 | Group-IB discovered utilization of the fake reCAPTCHA technique by MuddyWater APT group. | A campaign utilizing the ClickFix technique to deliver RMM tool was executed, allegedly targeting law enforcement employees in one of the countries bordering Iran. Group-IB asses with moderate confidence that the threat actor behind this campaign is MuddyWater. |
| 04 | Group-IB CERT Team discovered Fake Firewood Scams Target French Consumers Online | Fraudsters known as "Les brouteurs" exploit social media to sell non-existent firewood to French residents during winter. Using AI-generated fake documents and impersonating legitimate businesses, they trick victims into transferring money. Group-IB's investigation highlights the evolving sophistication of these scams. Consumers and businesses must stay vigilant, verify credentials, and adopt fraud prevention measures to mitigate financial losses. Read more. |

# REGIONAL TRENDS

## Key regional trends with a brief description:

| | | |
|---|---|---|
| 01 | Group-IB discovered utilization of the fake reCAPTCHA technique by MuddyWater APT group. | A campaign utilizing the ClickFix technique to deliver RMM tool was executed allegedly targeting law enforcement employees in one of the countries bordering Iran, we asses with moderate confidence that the threat actor behind this campaign is MuddyWater. |
| 02 | Group-IB discovered increase in sales of access and databases of organizations in the region for the past several months | Over the past six months, the number of events in the dark web related to the sale of access and leaked databases from organizations in the META region has increased by 78%. |

## Middle East, Türkiye and Africa

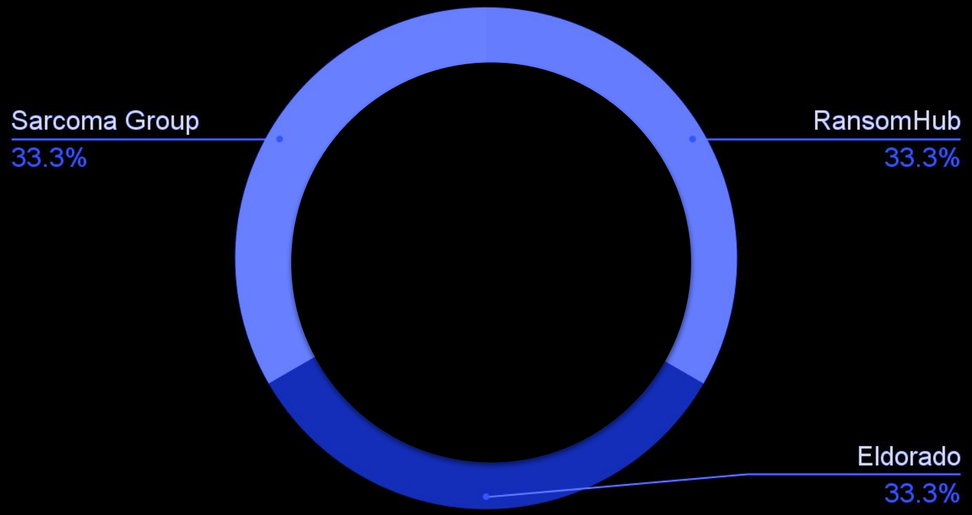
# STATISTICS: **ATTACKS**

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:

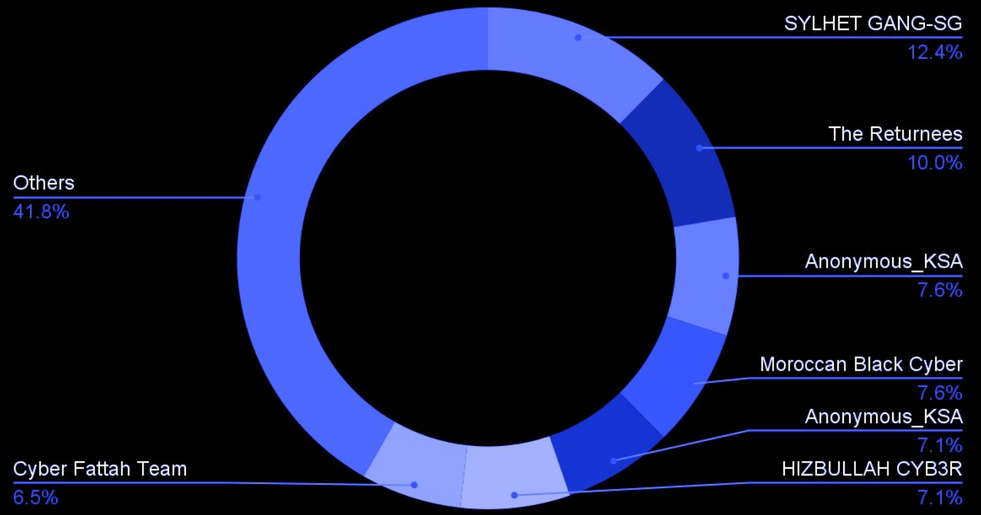
RANSOMWARE Attacks per Group




## 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 is a  brief overview of groups that were active in the region during the previous month.

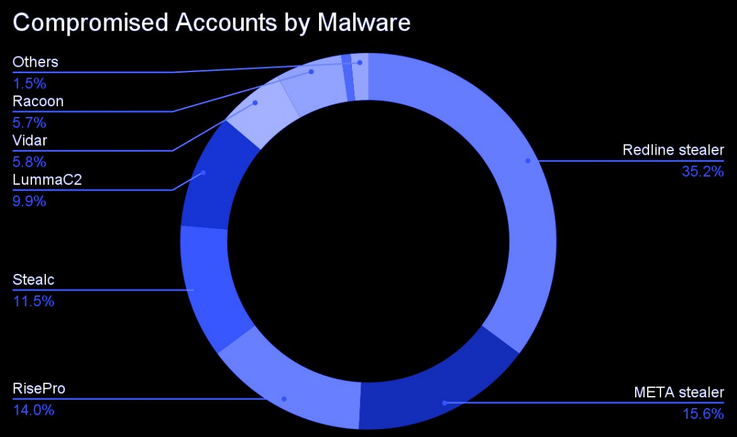
HACKTIVISM Attacks per Group

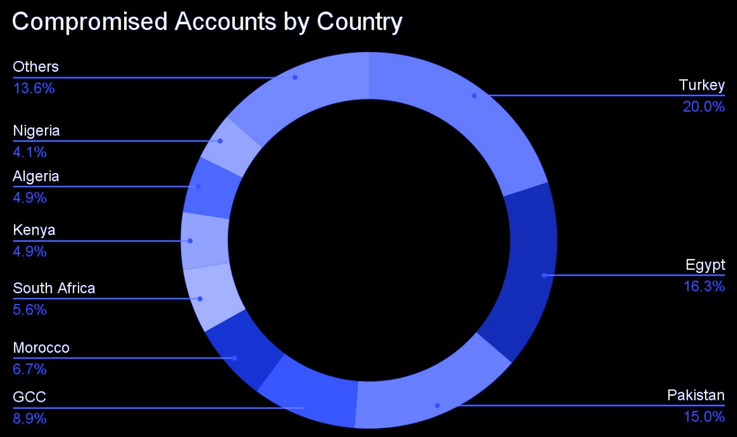


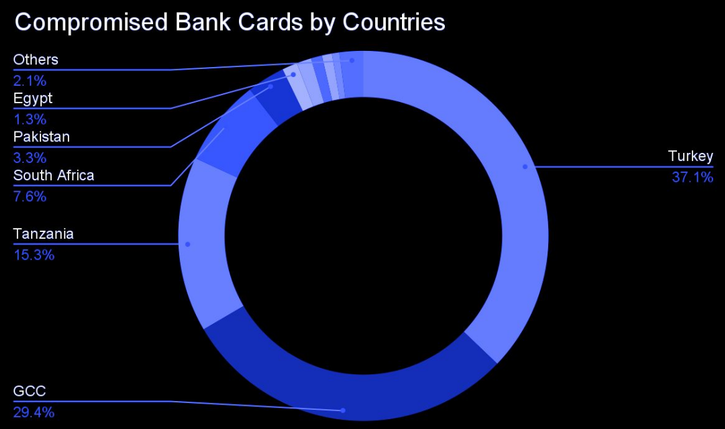
# STATISTICS: **COMPROMISED DATA**

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 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

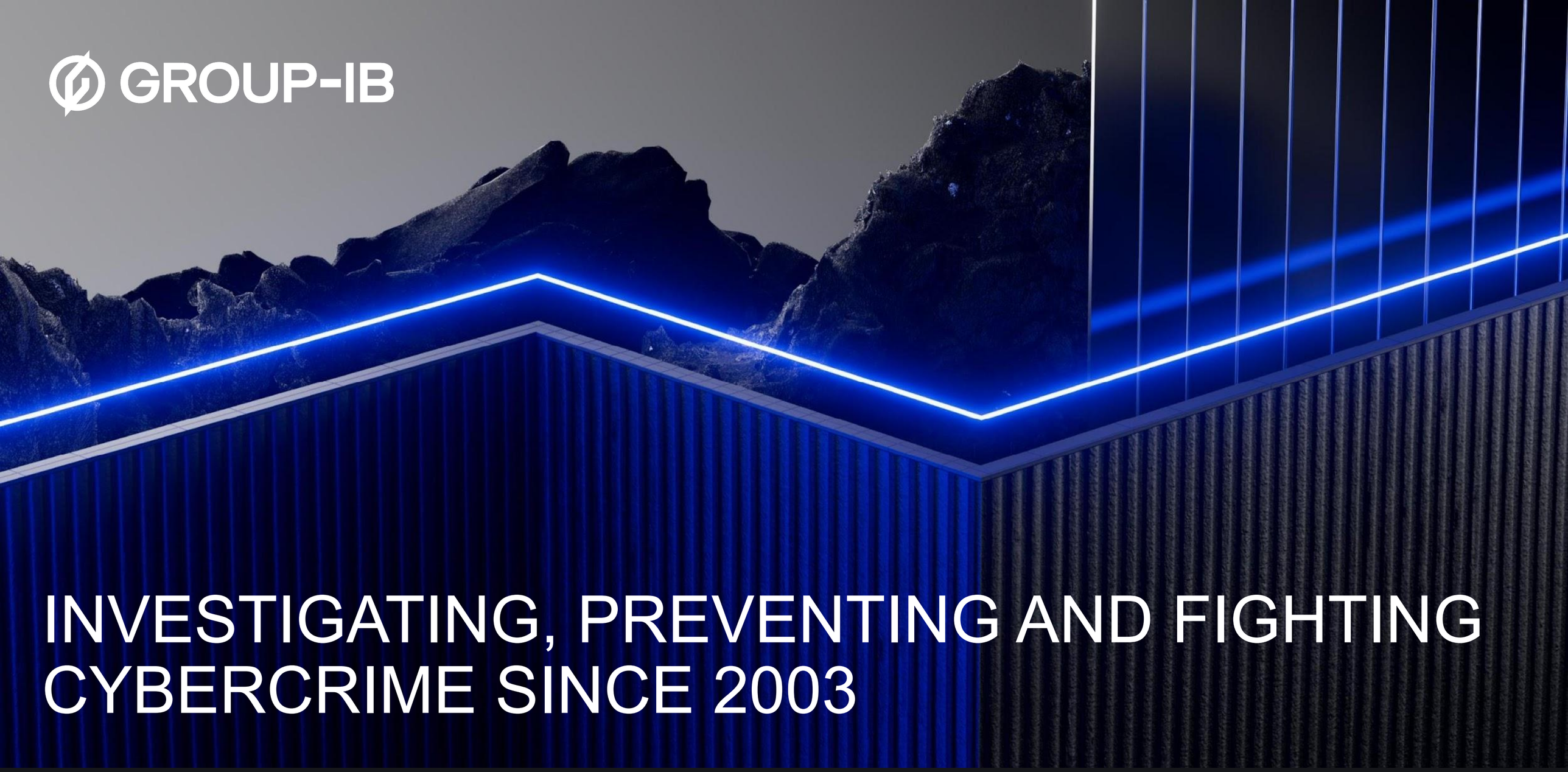
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

### 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