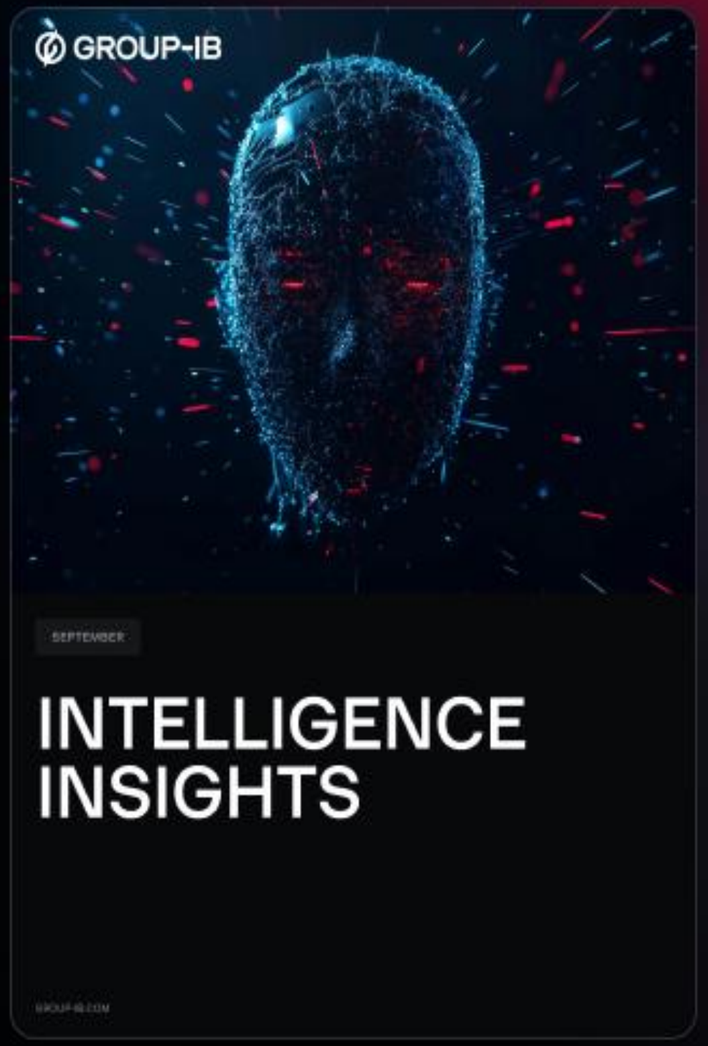
GROUP-IB



SEPTEMBER INTELLIGENCE INSIGHTS

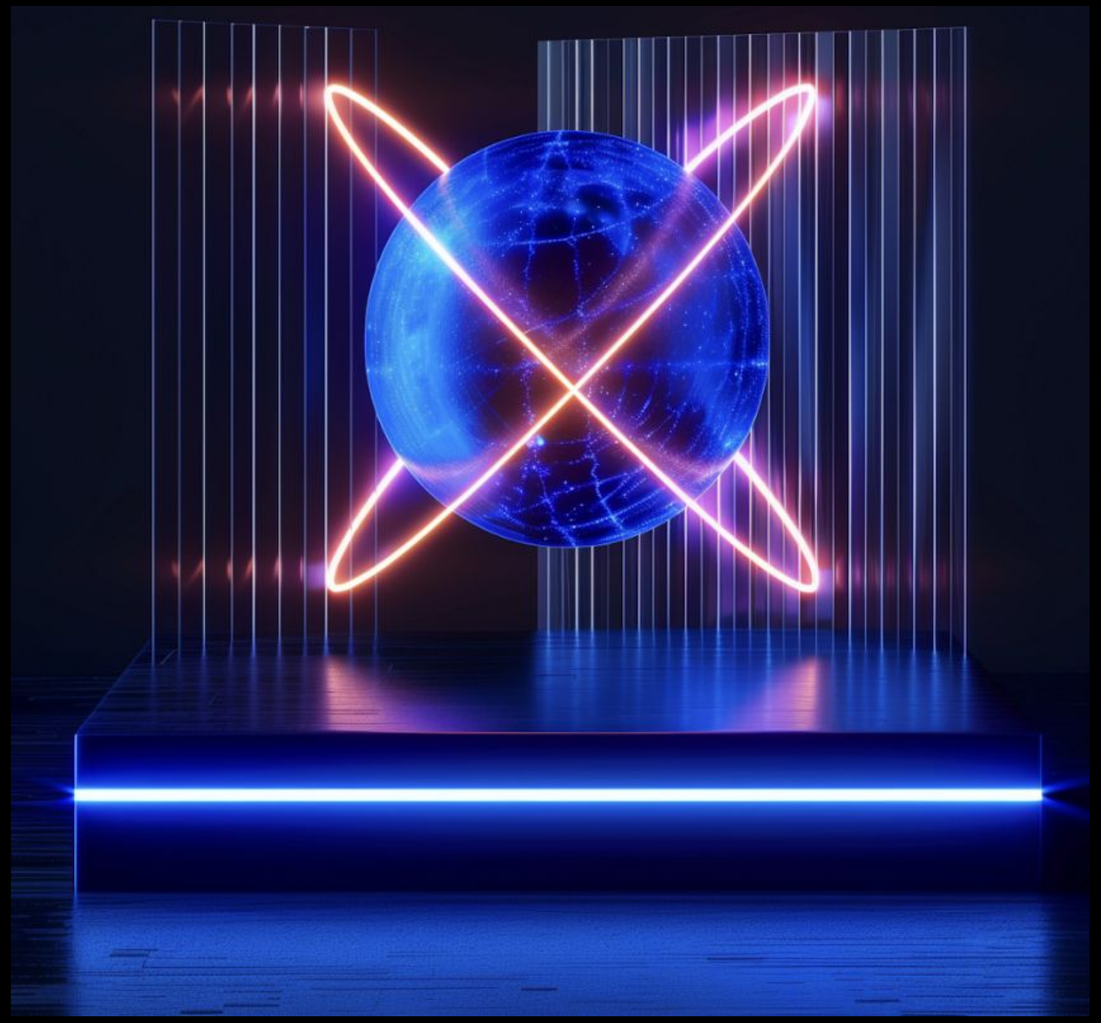
Executive Summary and Key Findings
Middle East, Türkiye and Africa

INTRODUCTION

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

2 most significant events of the month:

- **Group-IB report highlights an ongoing campaign by the North Korean Lazarus Group, known as the “Eager Crypto Beavers” campaign.**
- Group-IB CERT Team has uncovered a new fake investment scam campaign targeting Facebook & Instagram users in Türkiye



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

Global Trends with a brief description:

01	Group-IB report highlights an ongoing campaign by the North Korean Lazarus Group, known as the “Eager Crypto Beavers” campaign.	Lazarus Group has intensified its operations with a new campaign using fraudulent job interviews and malicious video conferencing apps to deploy their latest malware-BeaverTail and InvisibleFerret. More details.
02	Group-IB researchers recently published their in-depth research on the RansomHub group's activity	In February 2024 RansomHub has launched an aggressive affiliate program and is targeting key industries worldwide. Group-IB blog dives deep into their tactics, from recruiting former Scattered Spider members to executing double-extortion attacks. More details.
03	Group-IB have supported INTERPOL and the EUROPOL in a Joint Task Force as a Gateway Partner during the Paris Olympics 2024	Our collaboration with INTERPOL and EUROPOL enabled the French authorities to enhance cybersecurity measures before and during the event. Group-IB contributed by monitoring violations in social media, countering phishing threats, tracking the activity of threat groups, hackers, scammers, and illicit traders, as well as detecting DDoS attempts, data leaks, and compromised accounts.

REGIONAL TRENDS

Key Regional Trends with a brief description:

01 Group-IB CERT Team has uncovered a new fake investment scam campaign targeting Facebook & Instagram users in Türkiye

Group-IB CERT has discovered that In this scheme scammers utilize deep fake videos featuring public figures, including politicians, to deceive victims. Social media ads, are used to lure users into clicking on links that lead to fraudulent surveys designed to mimic legitimate brands.

02 Group-IB CERT Team keeps tracking the classiscam scheme and identifies 24 brands involved from MEA region

Classiscam is operating in an automated scam-as-a-service model. This scam scheme was first identified in Russia in the summer of 2019. Since then, it is still operating worldwide. Classiscam campaigns began on classified sites, where scammers posted fake ads and used social engineering to steal payments. These campaigns have since evolved into highly automated operations targeting online marketplaces and carpooling sites.

Middle East, Türkiye and Africa

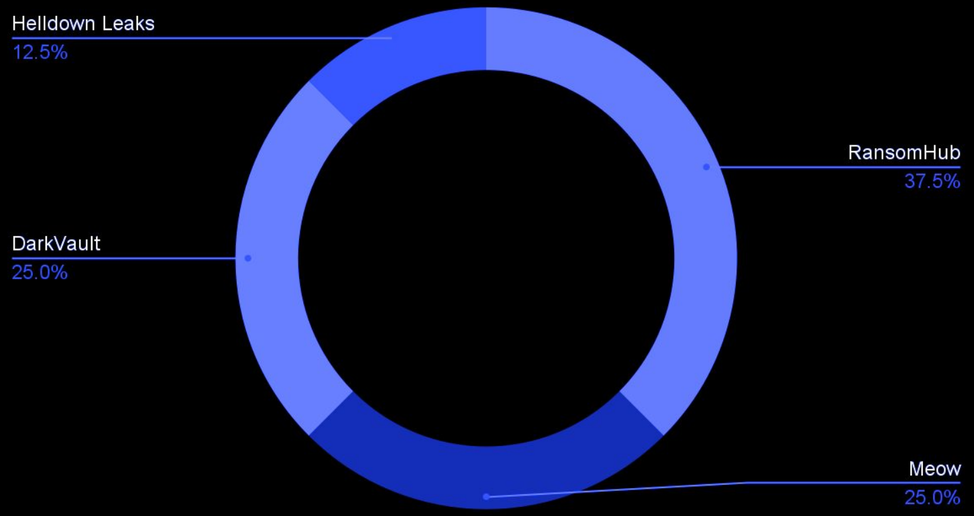
STATISTICS. **ATTACKS**

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:

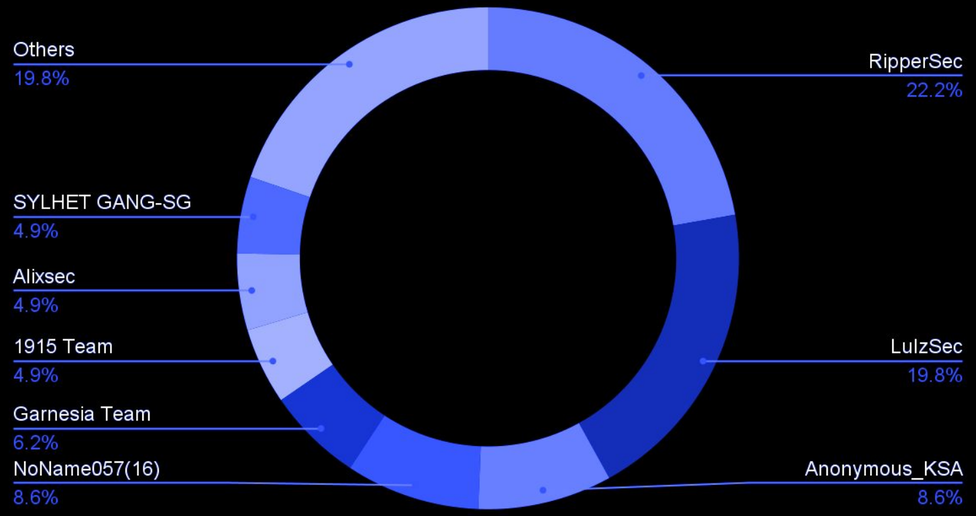
RANSOMWARE Attacks per Group



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.

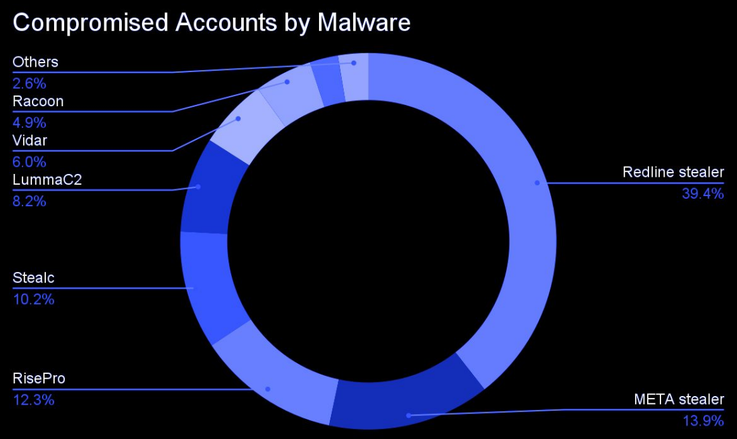
HACKTIVISM Attacks per Group

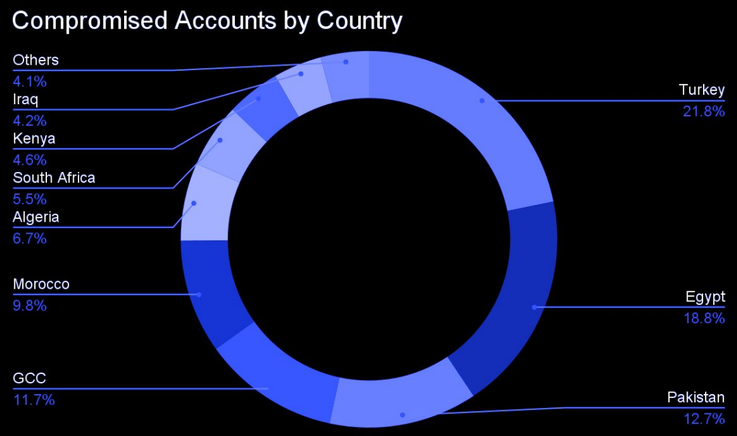


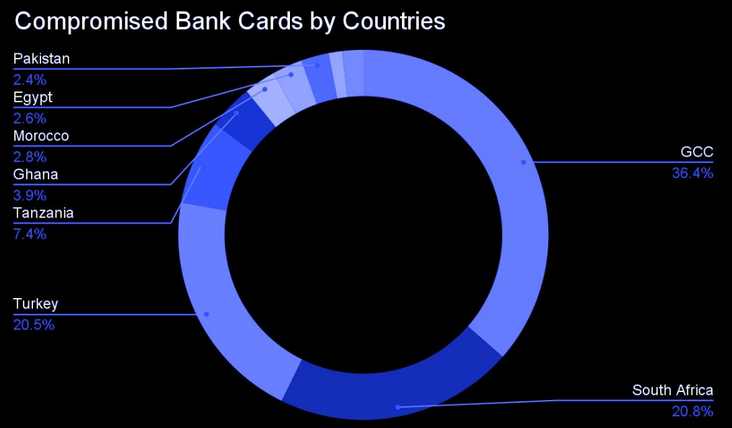
STATISTICS. **COMPROMISED DATA**

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

In conclusion, 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

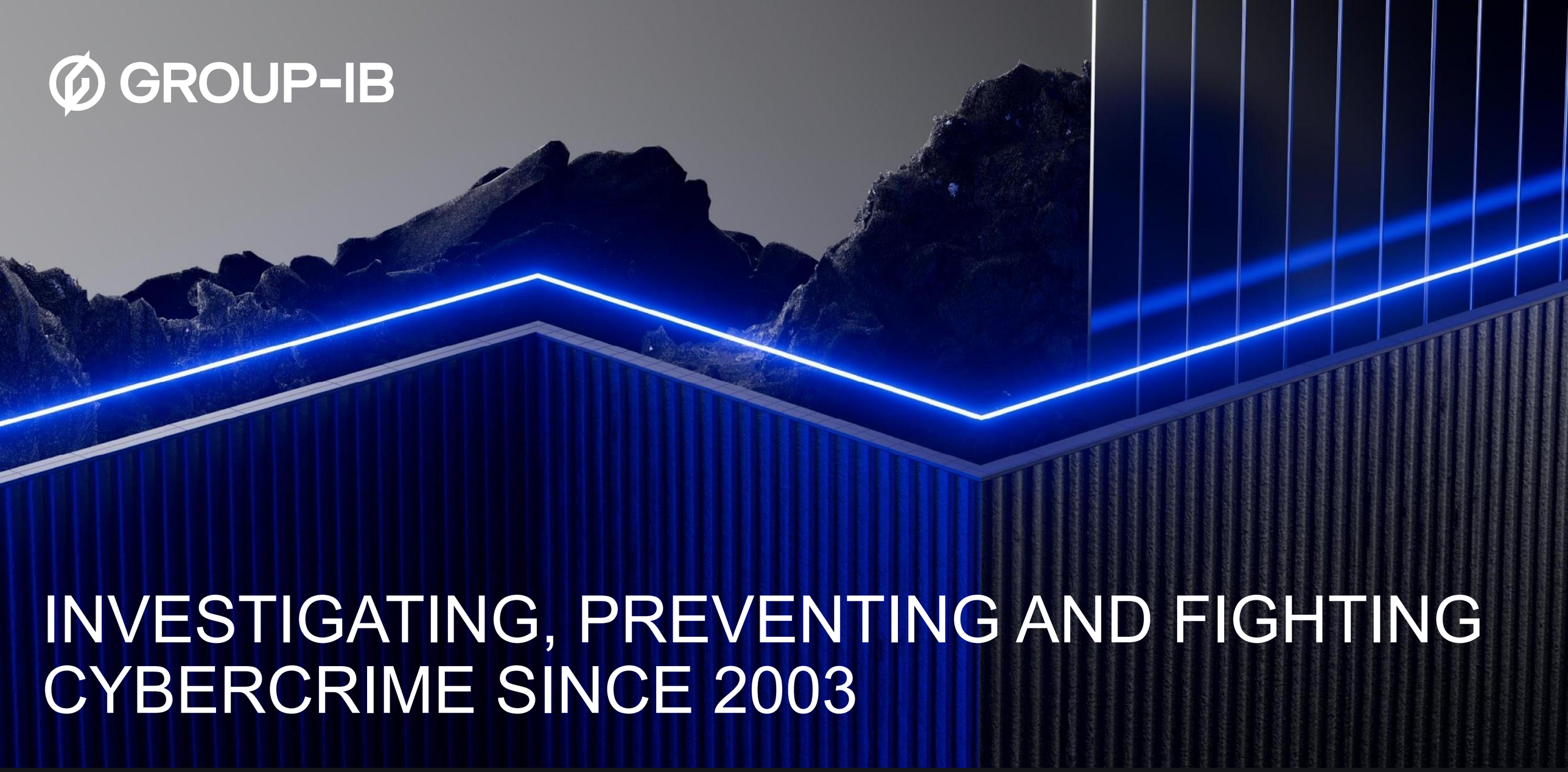
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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