
GROUP-IB
June 2024
INTELLIGENCE
INSIGHTS

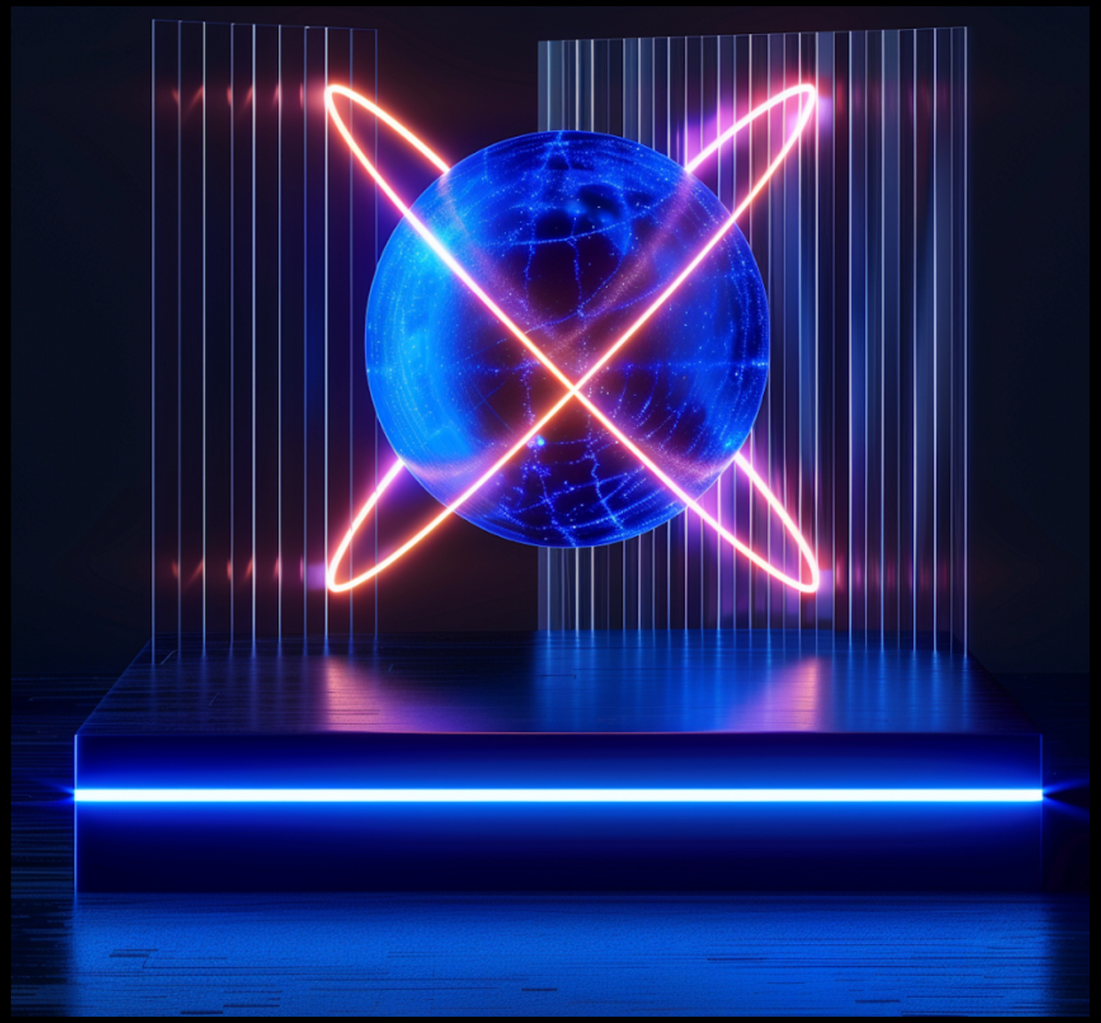
INTRODUCTION

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

2 most significant events of the month:

- **TeamViewer's announcement** of a cyber incident, which had been contained at the time of writing the report, and according to the company, user data was not affected.
- As for the META region, the discovered threat actor which creates **bank accounts for mules based on stolen know-your-customers documents** attracted the most attention, especially in the GCC region.

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	TeamViewer's corporate network was compromised in APT attack	On June 27, TeamViewer announced a security breach affecting its internal IT systems, reassuring users it didn't impact products or data. Learn through here
02	USD 257 million seized in global police crackdown against online scams	The project team includes eDiscovery, forensic analysts, economic security, financial audit, corporate law specialists, and financial crime experts. Read more
03	Group-IB analyzed Singapore scam campaign, threat infrastructure, and apps	The Singapore scam campaign used a fake app by Craxs Rat, likely run by Chinese-speaking actors, starting April 2023. Read more
04	Group-IB discovered Boolka's operations involving malware and delivery platforms	In January 2024, Group-IB discovered a landing page distributing BMANAGER trojan by Boolka, who used SQL injections since 2022. Read more
05	Eldorado Ransomware: Analysis of RaaS Model and Sophistication	The Singapore scam used a fake app by Craxs Rat, controlled by Chinese-speaking actors since April 2023, sold via Telegram. Read more

REGIONAL TRENDS

Key Regional Trends with a brief description:

01	Group-IB Threat Intelligence team has detected a threat actor who is selling bank accounts from various banks in the META region	Since April 18, the actor has been offering to sell bank accounts from various banks in several META countries. What caught the attention of Group-IB analysts is that these accounts are either stolen through compromised credentials or created manually by the criminals via leaked Personally identifiable information.
02	Phishing attack aimed at banks in the Levant region	Group-IB CERT Team detected a rise in phishing attacks targeting banks in the Levant region. The phishing attacks starts by a post on social networks promoting winning prizes from well-known banks Clicking on the attached link, the victim will be redirected to a phishing web page, where the login credentials or bank card details will be required to get the prize.
03	Phishing attack aimed at telecom providers in the Middle East and Africa	Group-IB CERT team discovered a phishing attack aimed at telecom providers in the MEA regions. The main goal of this attack is to steal users' payment details. The scheme consists of fake websites impersonating the telecom providers' official websites. These fake websites are suggesting victims pay their bills.

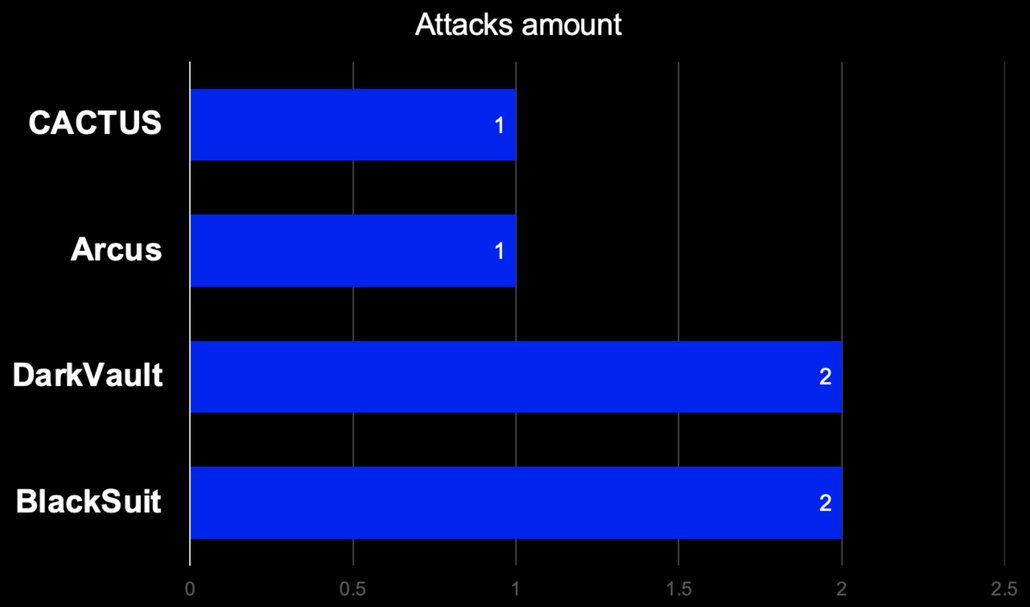
Middle East, Türkiye and Africa

STATISTICS. ATTACKS

GROUP-IB

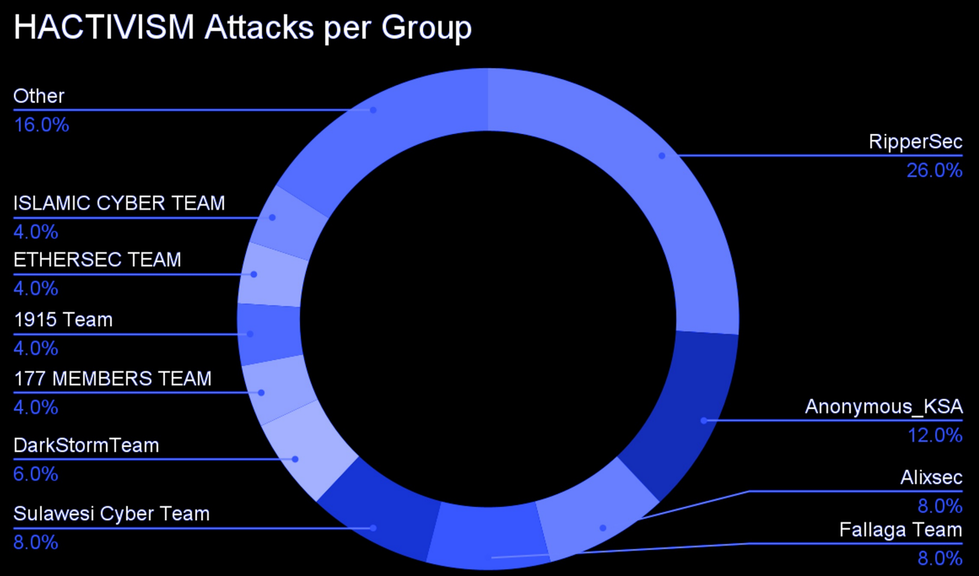
RANSOMWARE ACTIVITIES

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:



HACTIVISM ACTIVITIES

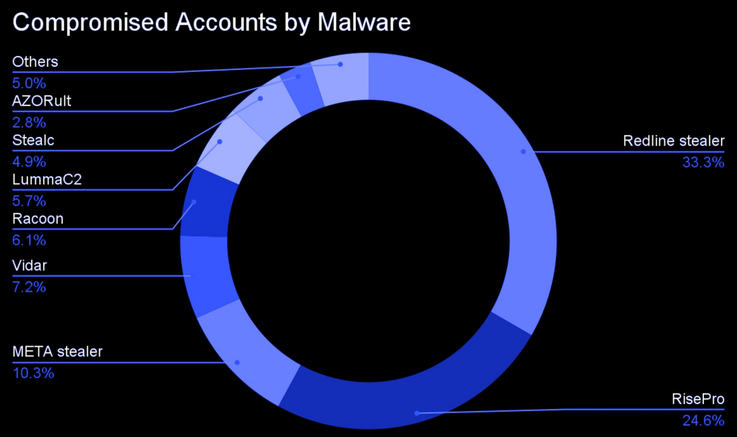
Hacktivism is the use of hacking to promote political or social agendas. Usually hacktivist groups are low-skill hackers who perform DDoS, Defacement, and Data Breaches (mostly leverages compromised accounts) attacks. Unfortunately, during the last year these groups attracted a lot of attention. Below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

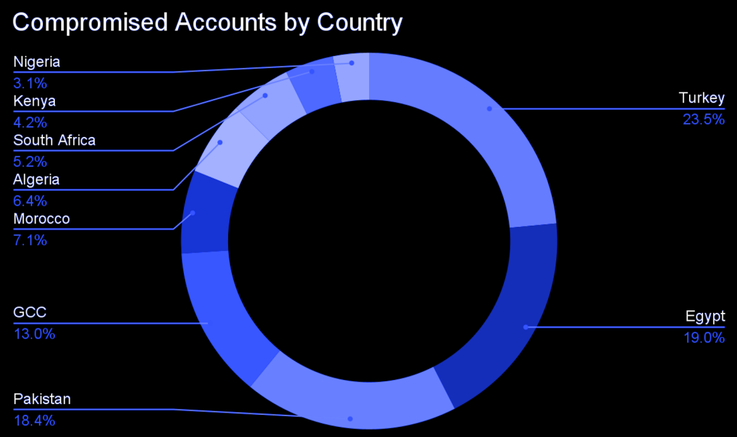


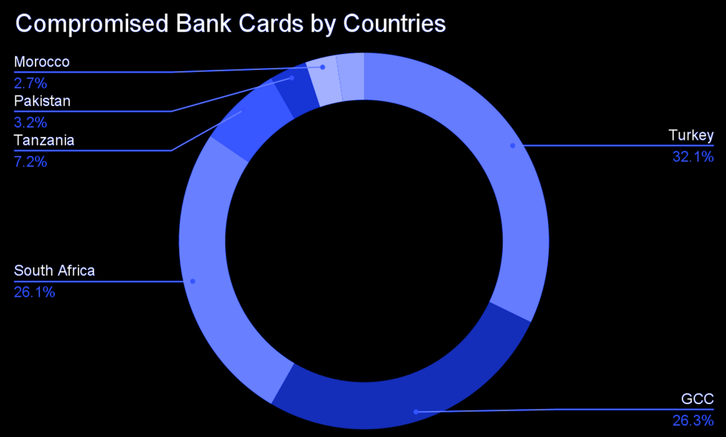
STATISTICS. COMPROMISED DATA

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.







CONCLUSION 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

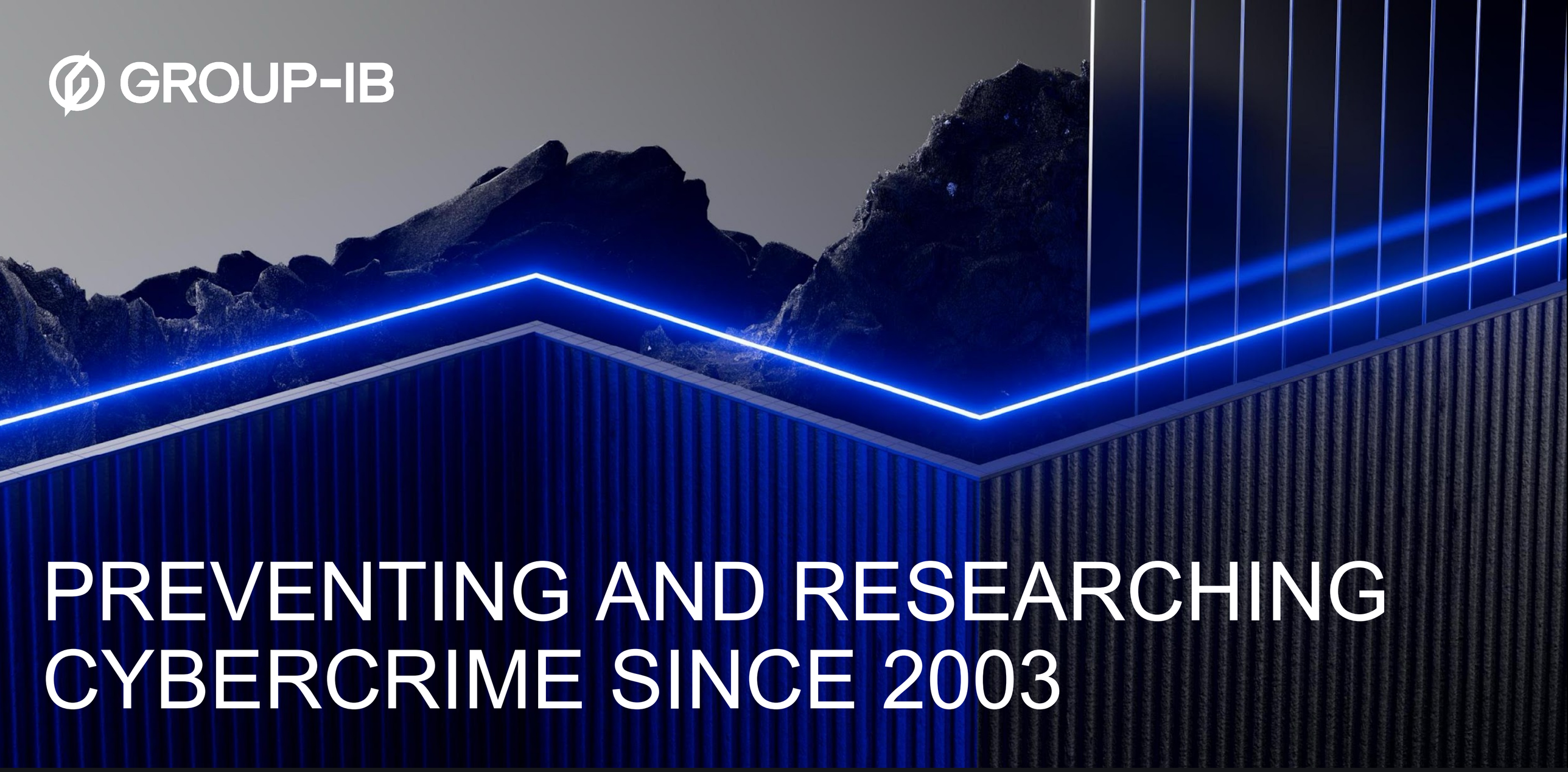
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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.



GROUP-IB

PREVENTING AND RESEARCHING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM
GROUP-IB.COM/BLOG
+971 4 568 1785

LINKEDIN FACEBOOK TWITTER INSTAGRAM