GROUP-IB

AUGUST INTELLIGENCE INSIGHTS

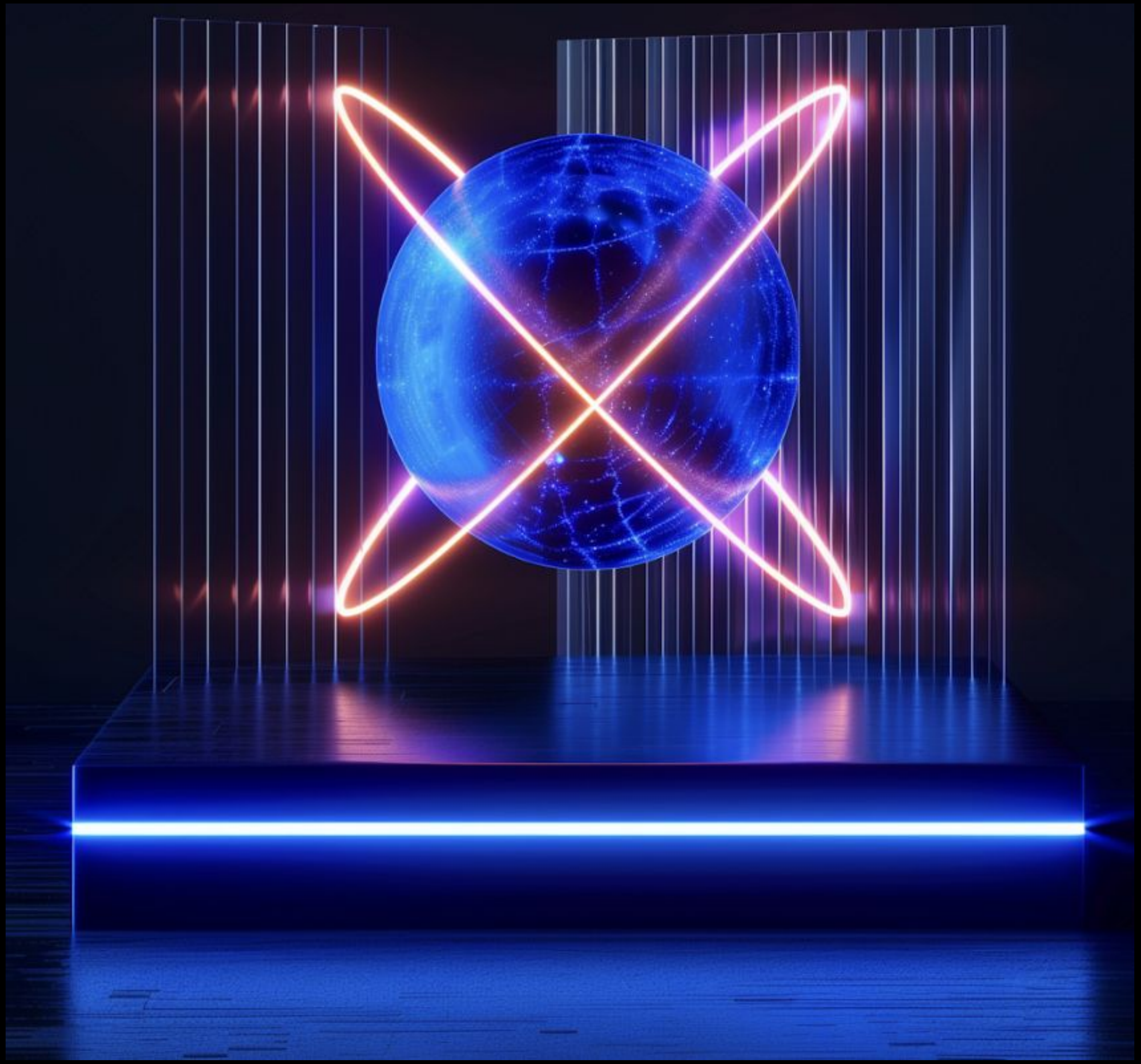
Executive Summary and Key Findings

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 specialists uncovered GXC criminal group,** that operates a sophisticated AI-powered phishing-as-a-service platform.
- A Threat Actor ”shafo” advertised the sale of a database containing the clients of ServiceNow on Breached forum.



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 uncovered a previously unknown Spanish-speaking criminal group

Group-IB specialists uncovered GXC criminal group, that operates a sophisticated AI-powered phishing-as-a-service platform. Targeting users of Spanish banks. Read more

02 Global IT outage: banks, flights and media outlets caused by CrowdStrike software

On July 18 and 19, 2024, a global IT outage happened affected big number of companies due to an update of CS software. The outage also affected all Microsoft products. More details.

03 Group-IB experts discovered messages advertising phishing sites that distribute PWAs apps

The phishing pages designed to install a progressive web app (PWA). After downloading the app, opening it, a page will open requesting the victim for authentication for Gmail or Microsoft.

04 Android Remote Access malware strikes in Malaysia

Group-IB's Fraud Protection team has detected over 210 samples and developed cutting-edge detection rules to combat this evolving threat. Read more

REGIONAL TRENDS

Key Regional Trends with a brief description:

01 Selling database of vulnerable ServiceNow instances

On July 28, the actor “shafo” advertised the sale of a database containing the clients of ServiceNow on Breached forum. According to the TA, the data was collected through scanning for ServiceNow instances that were still vulnerable to CVEs.

02 Scammers are promoting fake mobile applications aimed at banks in MEA region

Group-IB CERT team discovered raise in distributing fake applications aimed at banks and payment systems in MEA region. The mentioned apps are not hosted on general app stores but on fake websites created to distribute this malicious application.

03 Aggressive phishing attack aimed at banks in the Levant region

Group-IB CERT Team monitors an aggressive 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.

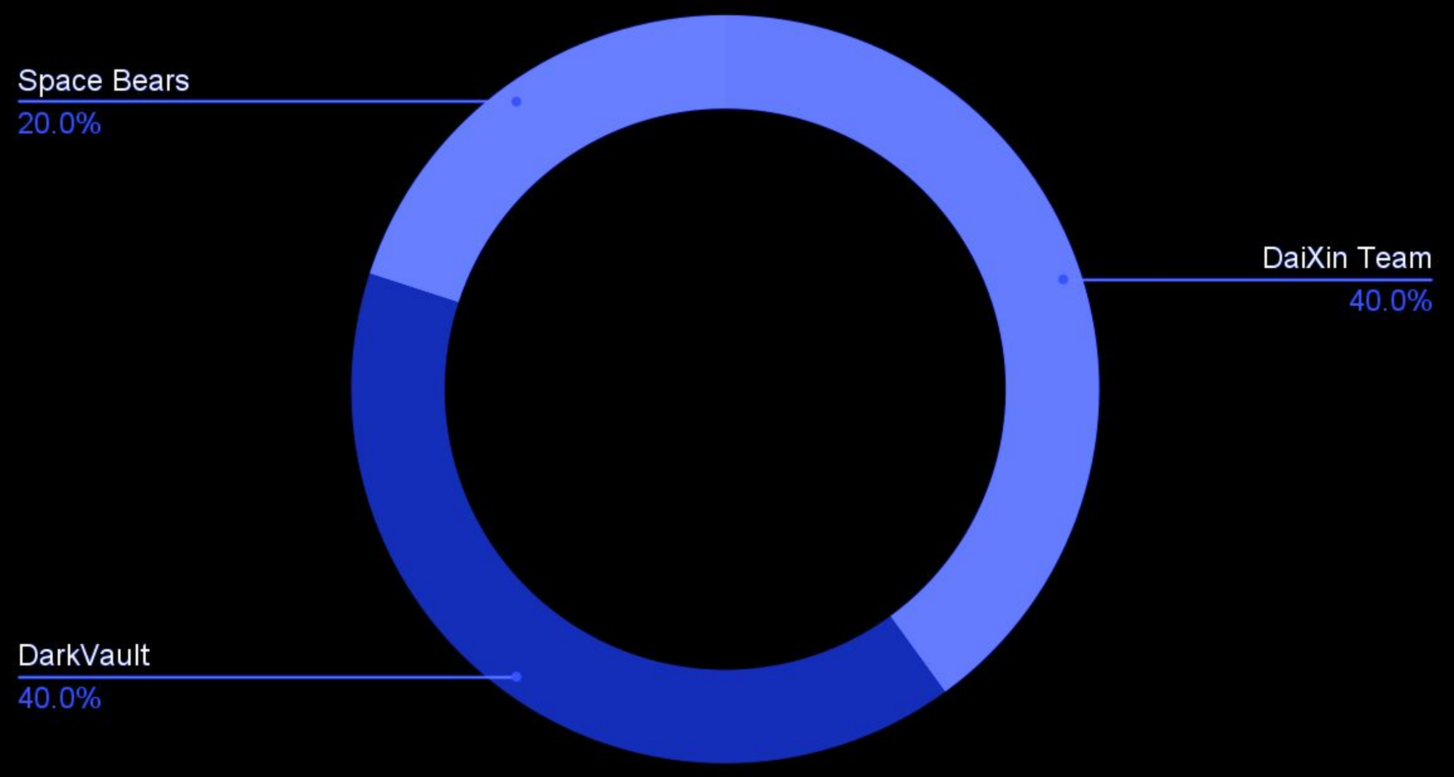
Middle East, Türkiye and Africa

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:

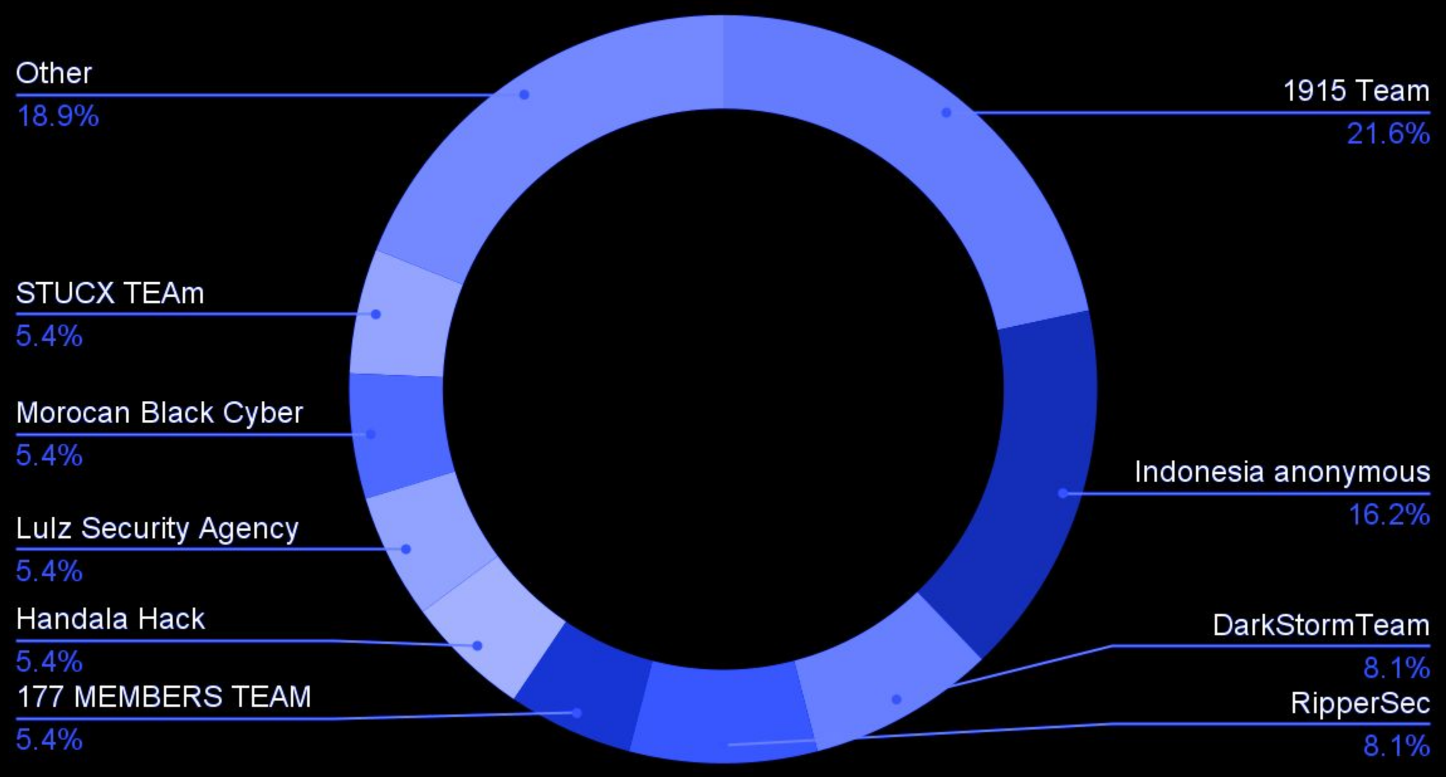
RANSOMWARE Attacks per Group



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.

HACTIVISM Attacks per Group

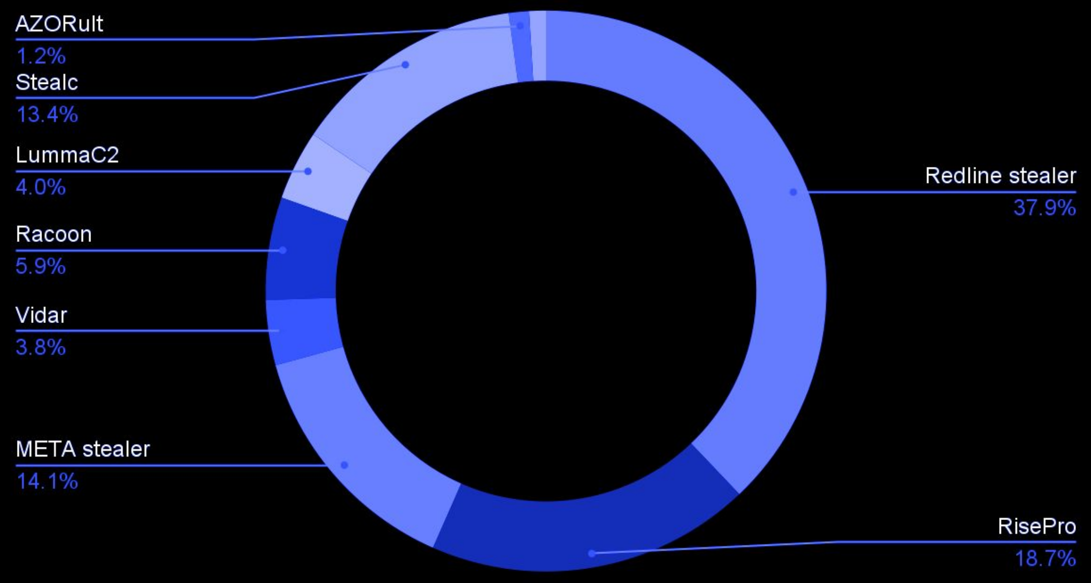


STATISTICS. **COMPROMISED DATA**

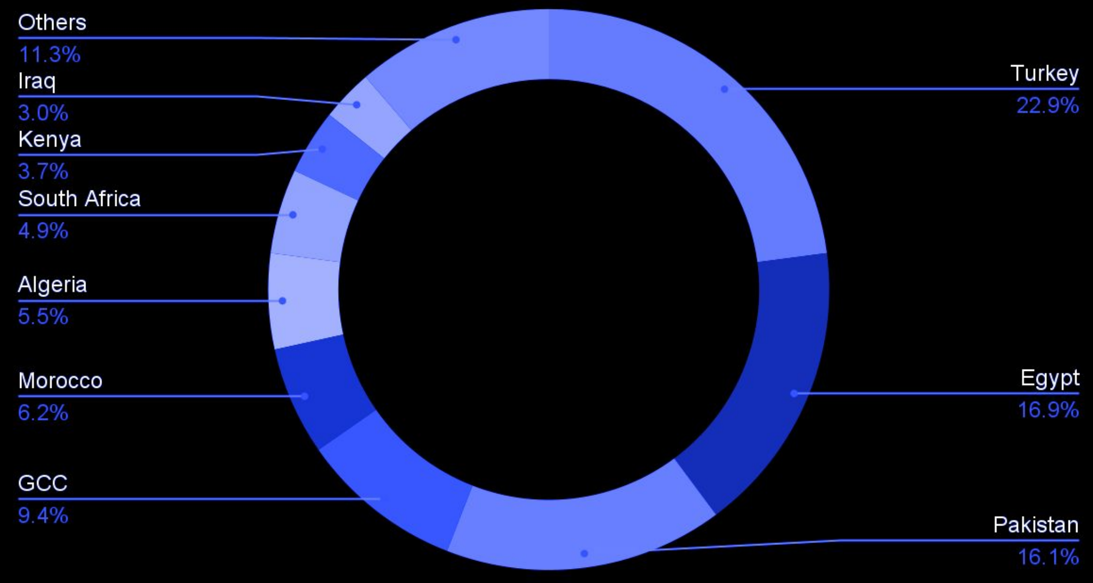
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational 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.

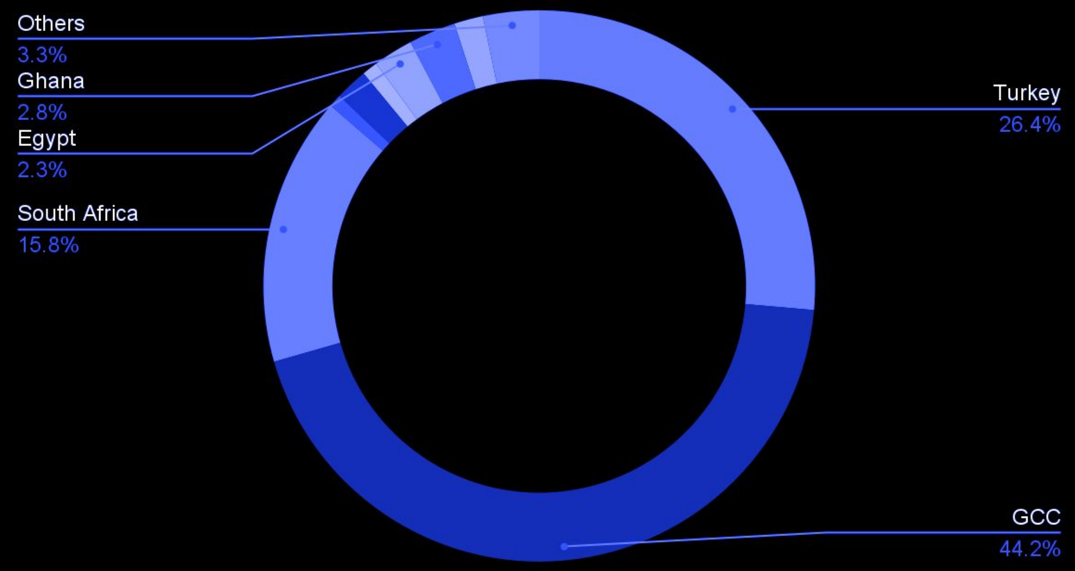
Compromised Accounts by Malware



Compromised Accounts by Country



Compromised Bank Cards by Countries



CONCLUSIONS AND RECOMMENDATIONS

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

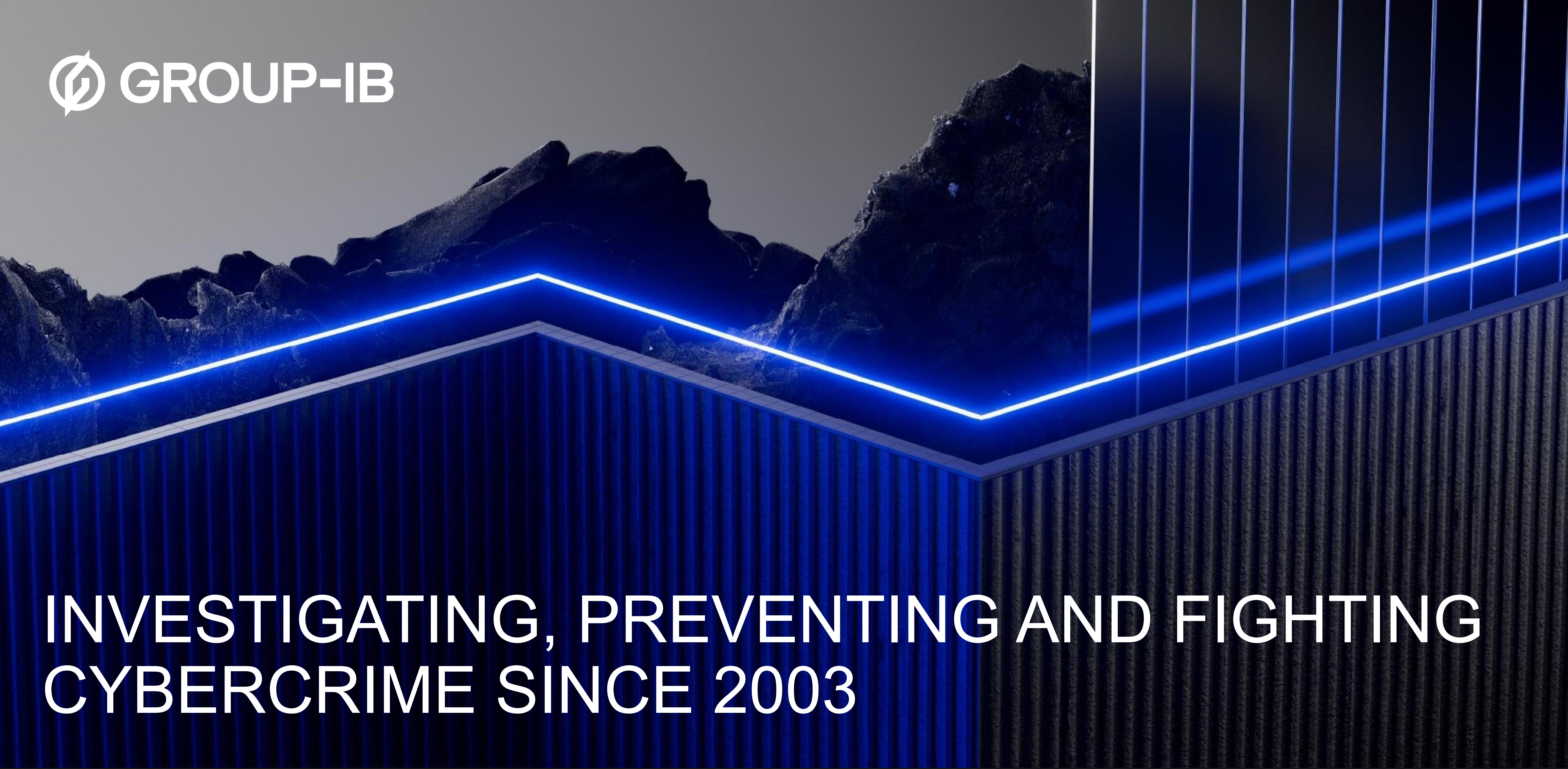
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM

GROUP-IB.COM/BLOG
+971 45681785

LINKEDIN FACEBOOK TWITTER INSTAGRAM