GROUP-IB

INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for December 2024

Report is based on data from 01.12.2024 till 01.01.2025

INTRODUCTION

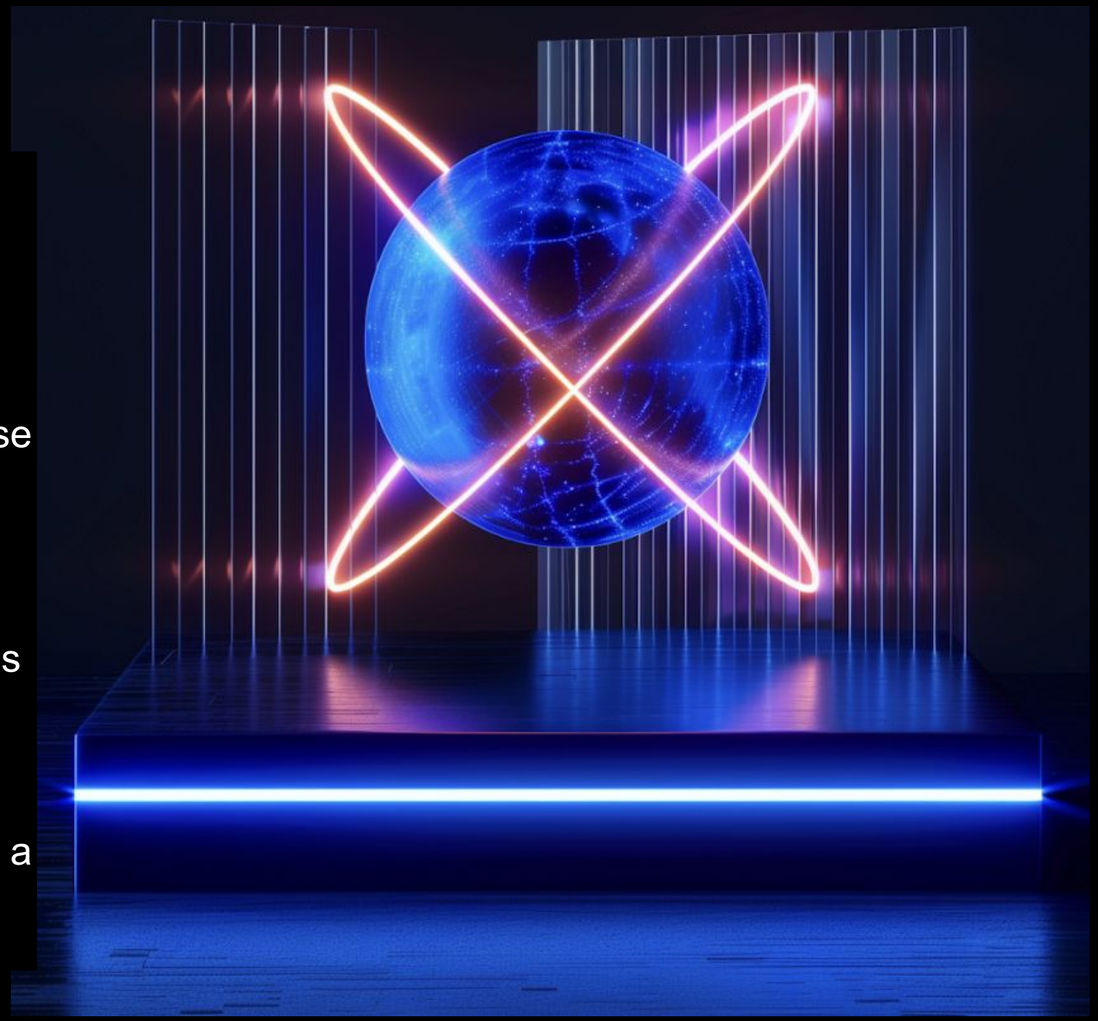
This report contains information on the most significant cybersecurity events that occurred worldwide and in the APAC region over the last month.

3 Most notable events of the month:

- Group-IB published a blogpost where discussed how smartphone manufacturers conceal security flaws, the risks these vulnerabilities pose to users and businesses, and actionable steps to protect devices from data breaches, identity theft, and exploitative attacks.

- AI Deep Fake Fraud cases are on the rise. Group-IB analysed How AI is Bypassing Biometric Security in Financial Institutions in this blogpost.

- Group-IB has analyzed the correlations between North Korea's cryptocurrency thefts and missile launches. Our experts have compiled a comprehensive list of cryptocurrency exchanges targeted by the group and the amounts stolen between 2017 and 2024.



GLOBAL TRENDS

GROUP-IB

Global trends with a brief description:

01	Group-IB published blogpost with brief overview of exploitation vulnerabilities in mobile OSes.	Recent findings suggest that smartphone manufacturers frequently downplay or conceal security vulnerabilities. This leaves both individuals and businesses exposed to risks such as data breaches, identity theft, and corporate espionage. Find how concealed vulnerabilities affect all users of modern smartphones, review key risks exposed by the Cellebrite leak, and discuss actionable recommendations for manufacturers and users alike in the article. **More details.**
02	Deepfake Fraud: How AI is Bypassing Biometric Security in Financial Institutions	Our research highlights several key aspects of deepfake fraud. It explores the main deepfake techniques used by fraudsters to bypass Know Your Customer (KYC) and biometric verification systems. It also outlines observed behavior patterns of deepfake fraud, based on insights from the Group-IB Fraud Protection Team. **More details.**
03	Phishing campaigns are on the rise.	Explore the advanced tactics employed in recent email phishing campaigns targeting employees from over 30 companies across 12 industries and 15 jurisdictions. The blog unveils sophisticated techniques used to outsmart Secure Email Gateways (SEGs) and exploit trusted platforms, creating highly convincing schemes to deceive victims and steal their credentials. **More details.**
04	Correlation Between North Korean Cryptocurrency Thefts and Missile Launches	North Korea’s use of stolen cryptocurrency to fund missile development and testing has been widely reported. These cyber attacks enable the regime to acquire funds while circumventing international sanctions. To explore this claim, we conducted a detailed analysis, examining the timing of cryptocurrency thefts in relation to missile launches to uncover any significant correlation. Our findings shed light on potential operational links and patterns in North Korea’s strategies. **More details.**

REGIONAL TRENDS

Regional trends with a brief description:

01	Group-IB identifies phishing campaign targeting Singapore residents disguised as SupportGoWhere government website	The campaign, which began in mid-December 2024, involves victims clicking on a link found in a SMS, which would redirect them to a phishing website impersonating the government portal SupportGoWhere. From there, victims would be instructed to provide their personal information and credit card details, ostensibly for verifying their identity. Along with the submission of their credit card information, the victims would also be required to provide the issuing bank's two-factor authentication (2FA) code, in order to claim the "subsidies". **More details.**
02	During the investigation, Group-IB's specialists have discovered a new family of malware that has been dubbed SkyHook. At the moment SkyHook was discovered in three regions: Vietnam, Thailand, Indonesia.	SkyHook is malware based on the original mobile banking application, the functionality can be different from one target to other, but mainly it reduces the security measures of the original banking application. SkyHook launches before the original application and executes different hooks. It is based on publicly available projects. Based on the latest investigation SkyHook is delivered by another Trojan called Gigabud. The malicious part is added as an additional DEX file that will be loaded automatically. **More details.**
03	Threat Actors continue targeting and attacking Malaysia, publishing different databases with leaked information	On December 3, 2024, an attacker with the nickname Ciph3r from Breachforums announced that he intended to sell Malaysian Nuclear Agency data. The data being sold contains 180 CSV files, which contain 1,650,000 lines. On December 6, 2024, an attacker with the nickname "Br34cHM45t3r" on the Breachforums forum stated that he was selling access that gives access to 1500+ servers of a Malaysian telecommunications company that he had not publicly named. On December 15, 2024, an attacker with the nickname Corp put access to 12 virtual machines belonging to a "Malaysian energy giant" up for sale. The attacker claims that these machines are integral to the company's operations.

Asia-Pacific Region

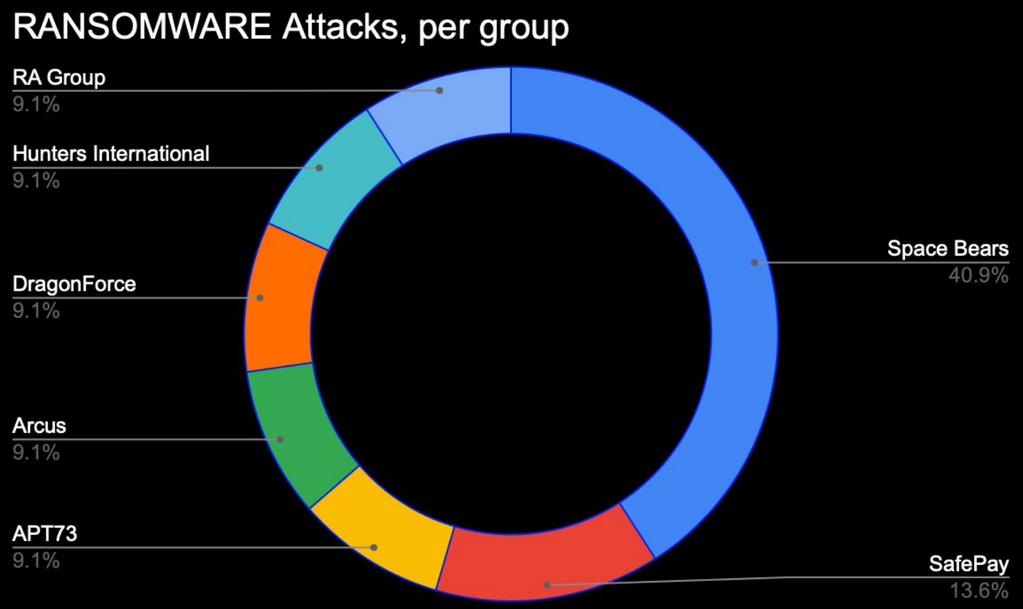
STATISTICS. **ATTACKS**

RANSOMWARE ACTIVITIES

Ransomware is a type of malicious software that encrypts the victim's data, rendering it inaccessible.
Ransomware statistics for the last month in APAC region:

- Space Bears continue active attacks and took the 1st place
- New attacks from SafePay, APT73 (two of it we think is a fake one), Arcus TAs compared to November

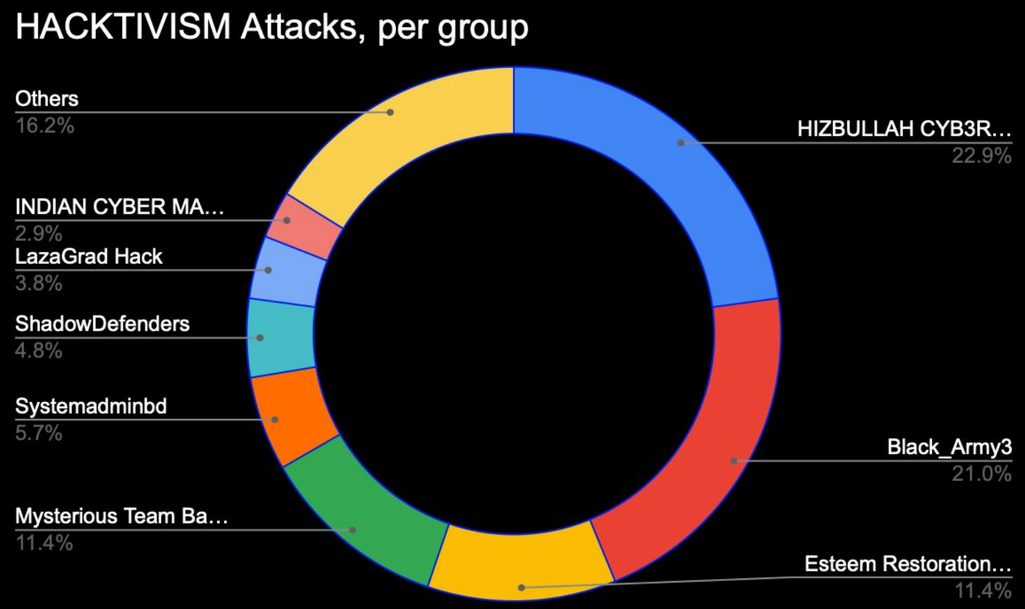
Below is a brief overview of groups that were active in the APAC region during the previous month:



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 APAC region during the previous month:



STATISTICS. **COMPROMISED DATA**

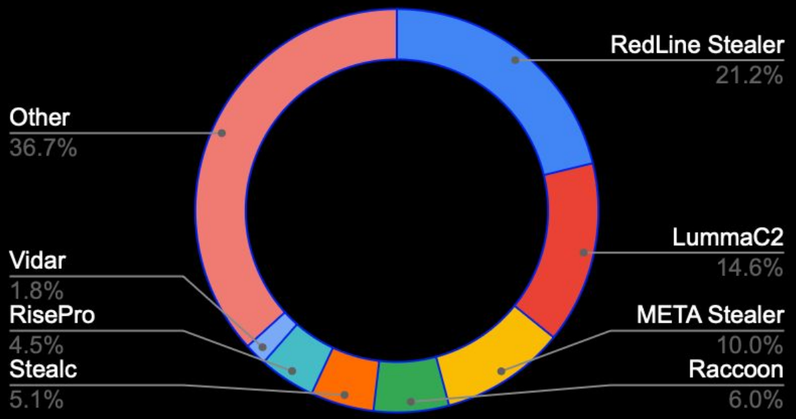
GROUP-IB

Statistics regarding compromised accounts and compromised bank cards.

Key Trends in November:

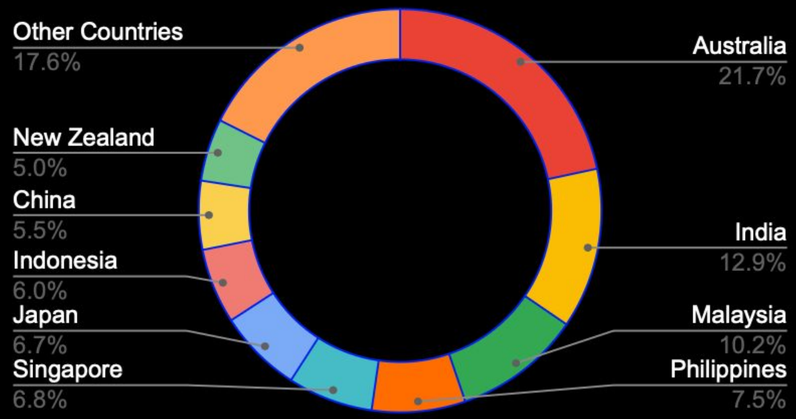
- We see a small decline in the number of compromised accounts in APAC, with a small increase in Thailand
- The Number of compromised accounts in India, Indonesia and Thailand is consistently high.
- Malware-stealers are doing what they were created for: RedLine stealer, LummaC2 and META stealer is surging in APAC.
- We see increased number of compromised Bank Cards in APAC, with a big increase in Australia in December 2024

Compromised Accounts by Malware



Compromised Accounts by Country

Compromised Bank Cards by Country



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

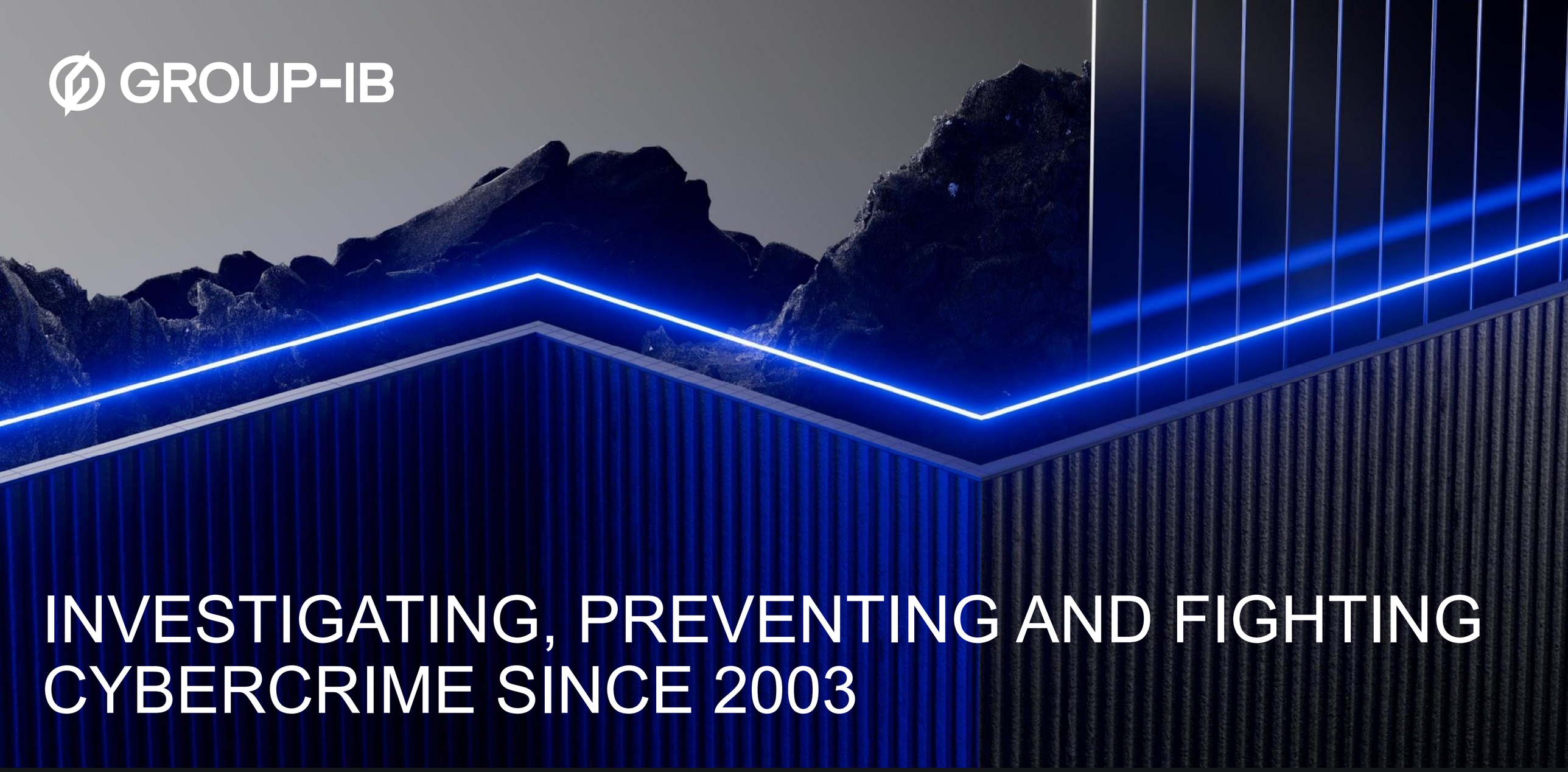
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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