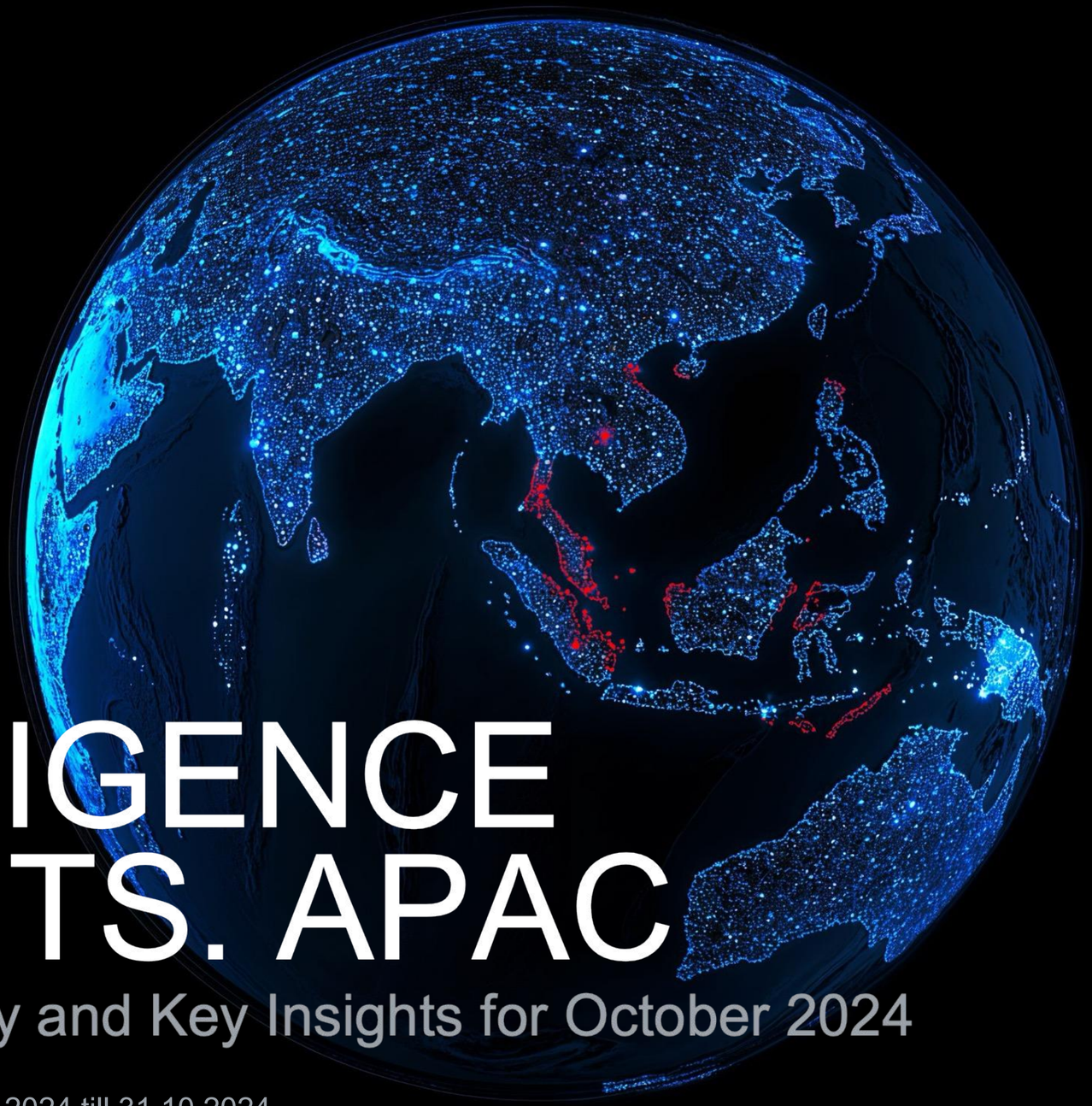
GROUP-IB



INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for October 2024

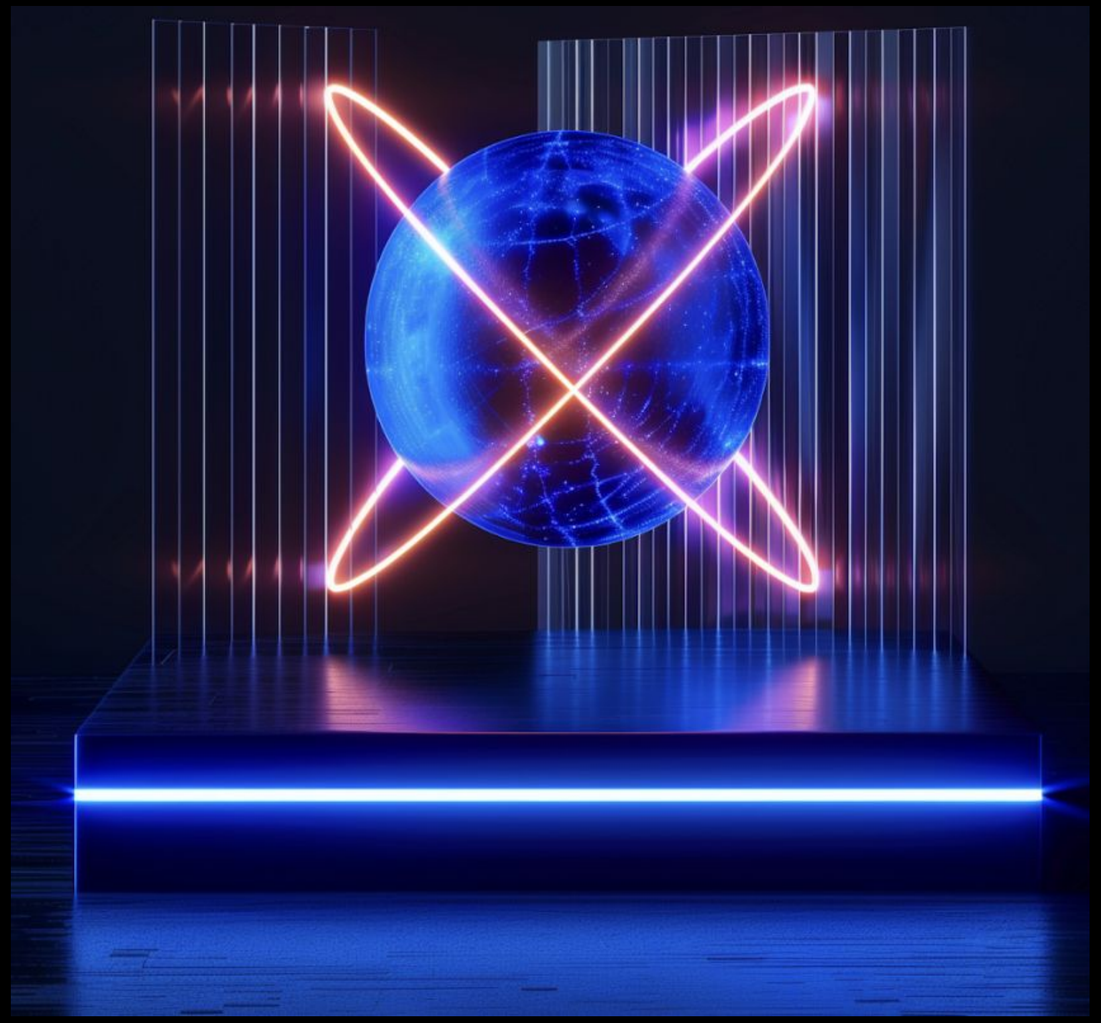
Report is based on data from 01.10.2024 till 31.10.2024

INTRODUCTION

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

2 most striking events of the month:

- **Group-IB specialists uncovered a large-scale fraud campaign involving fake trading apps targeting Apple iOS and Android users**
- **Group-IB contributed to INTERPOL's "Operation Contender 2.0" which led to the arrest of two individuals by the Nigerian Police Force**



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

GROUP-IB

Global trends with a brief description:

01	Group-IB observed how the Cicada3301 Ransomware-as-a-Service group operates, detailing the workflow of their affiliates, panel examining, different variants of the ransomware.	Cicada3301 has rapidly targeted 30 organizations across critical sectors within three months, with a significant focus on the USA and the UK.The ransomware is written in Rust, supporting Windows, Linux, ESXi, and NAS platforms, even extending to uncommon architectures like PowerPC.Utilizes ChaCha20 and RSA encryption with configurable modes (Full, Fast, Auto), capable of both full and partial file encryption to optimize the speed and impact of the attacks. **More details**
02	Group-IB uncovers DragonForce ransomware tactics and affiliate program: Double extortion attacks target key industries with advanced tools	DragonForce runs a Ransomware-as-a-Service program using LockBit3.0 and ContiV3 variants, employing double extortion to encrypt data and demand ransom. Affiliates receive 80% of profits and tools for customizing attacks. Group-IB has revealed the attackers use of advanced defense evasion techniques and targeting of 82 victims across industries like manufacturing and real estate. **More details**
03	Group-IB specialists uncovered a large-scale fraud campaign involving fake trading apps targeting Apple iOS and Android users	Cybercriminals use fake trading apps to lure victims and steal funds, often starting contact through dating apps. These fraudulent apps, built using the UniApp Framework and dubbed UniShadowTrade by Group-IB, support multiple languages. They have been found in the Apple App Store and Google Play, with victims detected globally. **More details**
04	Group-IB contributed to INTERPOL's "Operation Contender 2.0." which led to the arrest of two individuals by the Nigerian Police Force	These two individuals had a role in a romance scam that resulted in significant financial losses for a victim in Finland. As an INTERPOL Gateway Partner, Group-IB provided critical intelligence that helped the law enforcement pinpoint and apprehend these cybercriminals. **More details**

REGIONAL TRENDS

GROUP-IB

Regional trends with a brief description:

01	TopKit Phishing Kit designed to steal email account credentials by mimicking a variety of email platforms is continuously used to attack APAC countries and companies by threat actors.	TopKit Phishing Kit is a phishing kit primarily targeting email accounts. It presents victims with a themed or generic email account login page where victims are expected to enter their email address and password to login. These credentials are then sent to a hard-coded exfiltration address from where they are sent to the threat actor.
02	Threat Actors continue targeting and attacking Thailand government organisations, publishing different databases with leaked information.	On October 11, 2024, the telegram channel "Kingdom of Databases (Free)" published the database of Vehicle Inspection System Division (VISD), Thailand's Department of Land Transport (DLT), Unrelated intersections with other confirmed leaks confirm the authenticity of the published user data. On October 30, 2024, an attacker with the nickname "infamous" put up for sale the database with 181 thousand registered users of the company/site that organizes vehicle plate number sales in Thailand.
03	AI-Powered attacks are rising in Asia	Cybercriminal groups have been leveraging generative AI to produce phishing messages in various languages, deploy chatbots to manipulate victims, spread disinformation on social media at scale, and forge documents to bypass KYC verification processes. The number of scam casesa and attacks are on the rise. The United Nations Office on Drugs and Crime also highlighted a range of AI-driven threats in its latest report on cybercrime in Southeast Asia.
04	Group-IB specialists have identified a malicious campaign, ongoing since at least May 2024, injecting on compromised Magento websites a Bablosoft JS script aimed to collect fingerprints of visiting users.	The threat actor behind the detected campaign is likely exploiting known vulnerabilities affecting vulnerable Magento versions, since many of the compromised websites are using Magento 2.3 which is in EOL status and not supported since September 2022, to gain control over the website and inject a JS script on the homepage with the aim to collect the fingerprint of the website visitors attacking different organisations in Asia Pacific. A deeper analysis of the injected clientsafe.js script revealed that it is part of the Bablosoft BrowserAutomationStudio (BAS) suite; its purpose is to collect users' fingerprints for later use on the Bablosoft FingerprintSwitcher module.

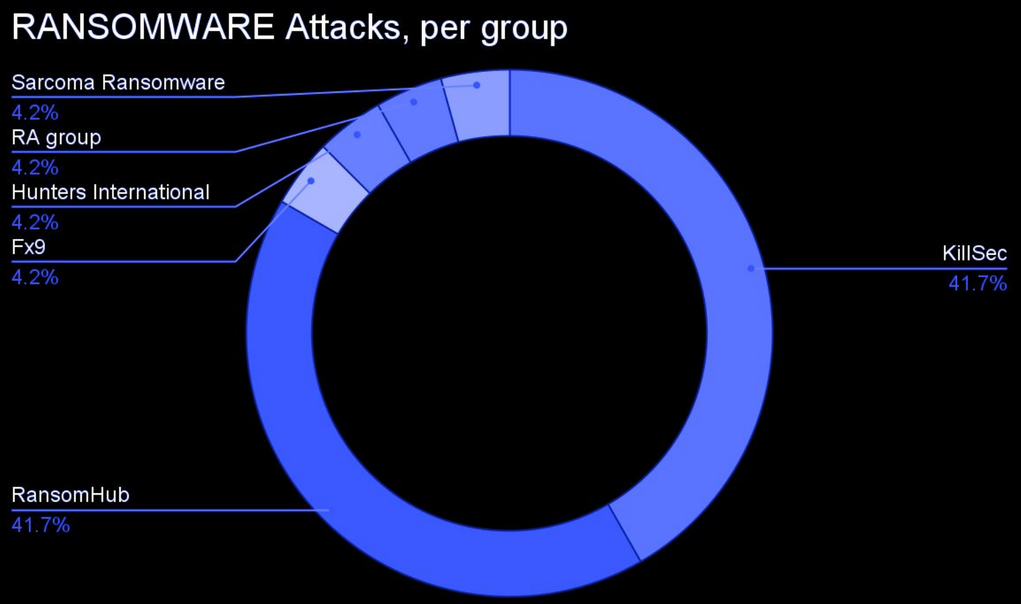
Asia-Pacific Region

STATISTICS. **ATTACKS**

GROUP-IB

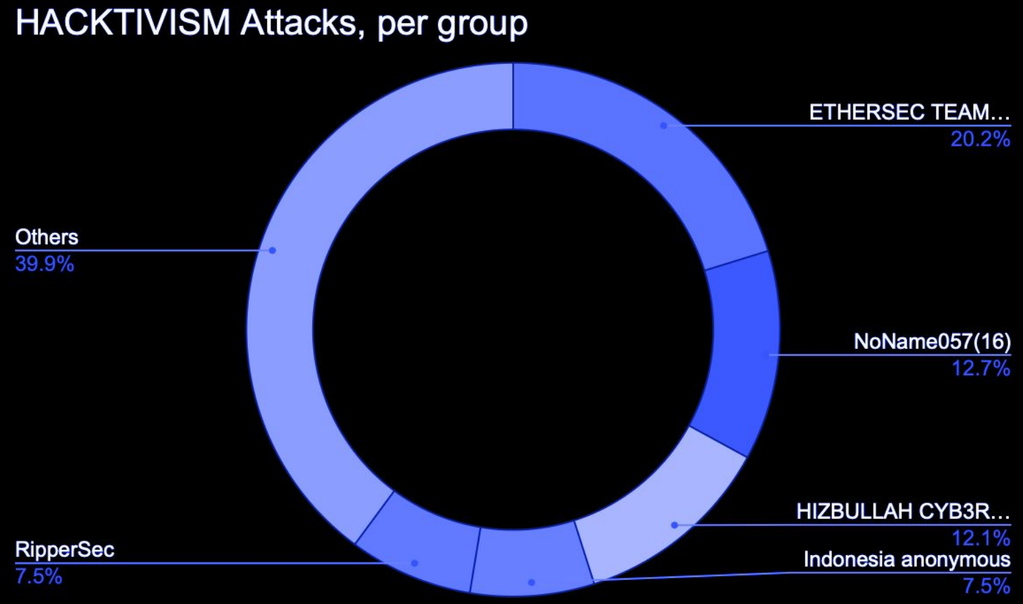
RANSOMWARE ACTIVITIES

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 APAC region:



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.

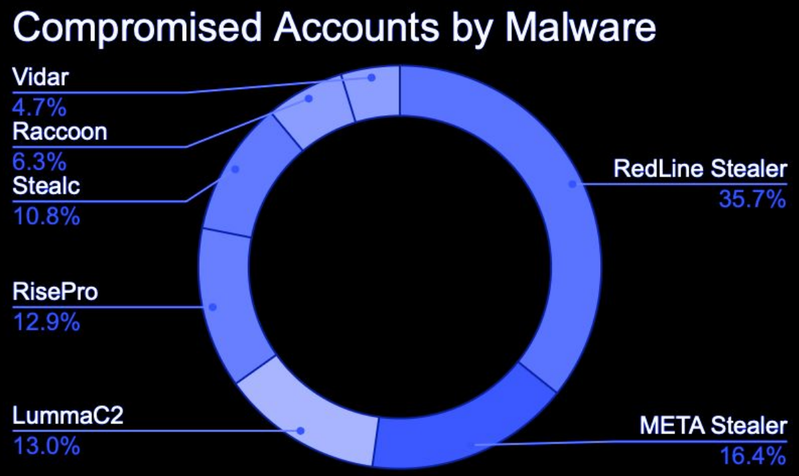


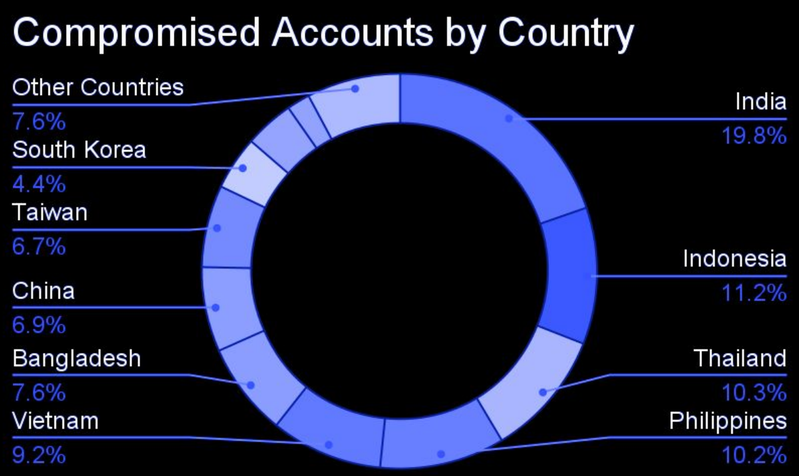
STATISTICS. **COMPROMISED DATA**

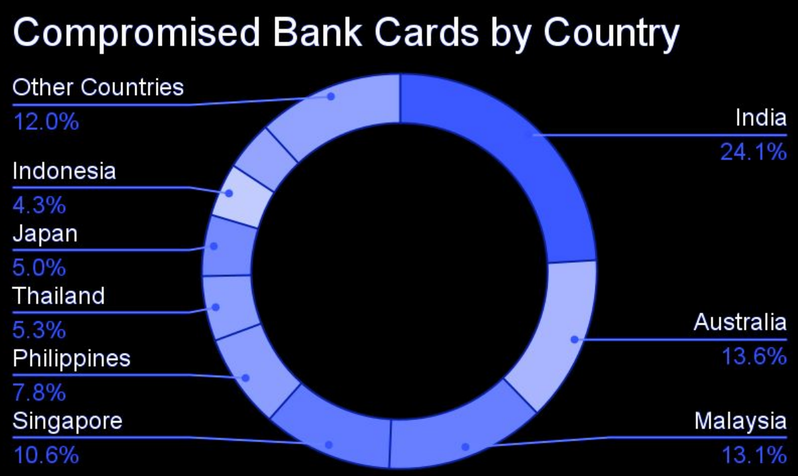
GROUP-IB

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

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

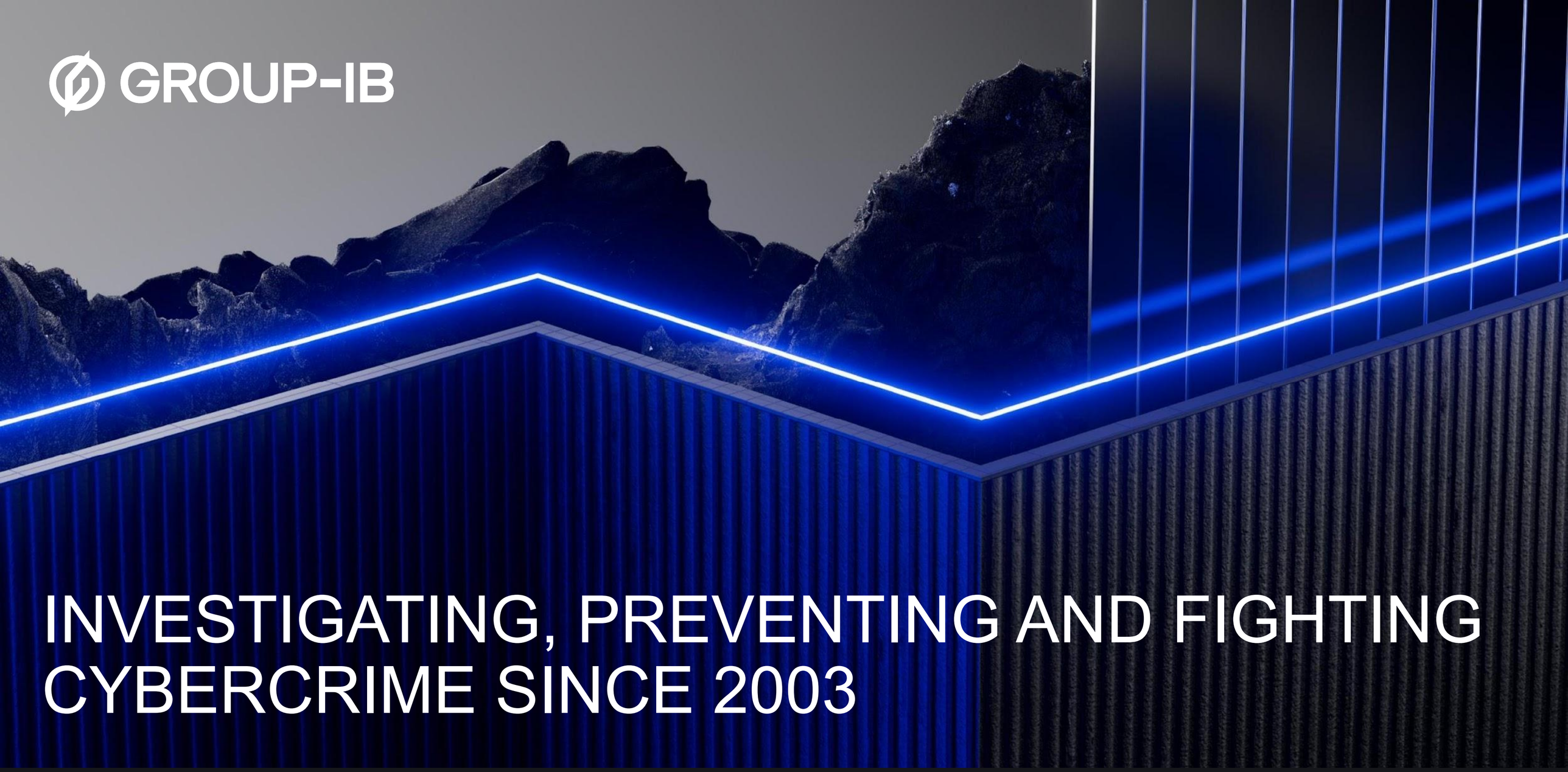
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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
+65 3159 3798

LINKEDIN FACEBOOK TWITTER INSTAGRAM