January 2025

North America

Intelligence Insights

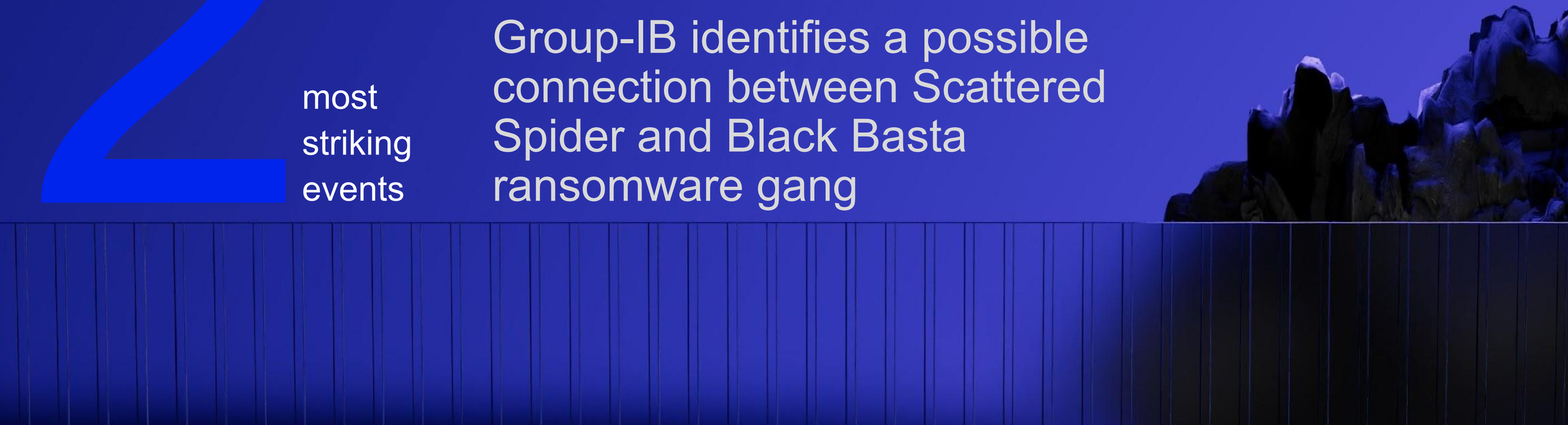
HIGHLIGHT OF THE MONTH

This report contains information on the most significant cybersecurity events that occurred worldwide and in North America over the last month

2 most striking events

Group-IB CERT identifies impersonation of U.S. marketplace brands

Group-IB identifies a possible connection between Scattered Spider and Black Basta ransomware gang



GLOBAL TRENDS

GROUP-IB

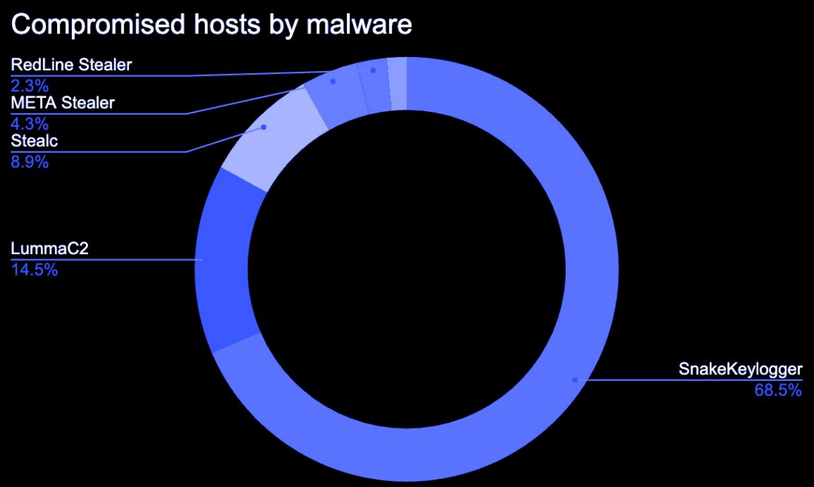
Global trends with a brief description:

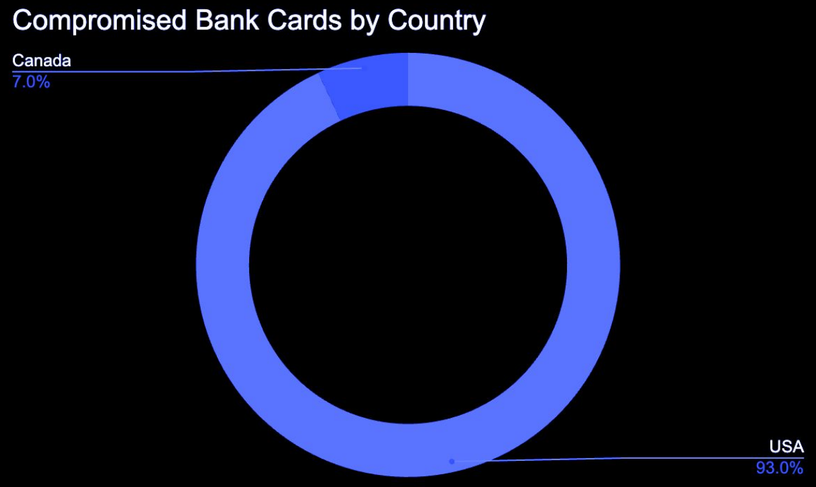
01	Halcyon published the blog about encryption of the data in Amazon S3 buckets	The blog post "Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C" by Halcyon details a novel ransomware campaign where the threat actor, dubbed Codefinger, uses compromised AWS credentials to encrypt data in Amazon S3 buckets via Server-Side Encryption with Customer Provided Keys (SSE-C). This method renders the data irrecoverable without the attacker's encryption key, as AWS does not store these keys, and CloudTrail logs only an HMAC insufficient for decryption.
02	Unveiling OtterCookie: A North Korea-Linked Attack Campaign Targeting Japan	The NTT Security Technical Blog post "Contagious Interview and the Newly Identified Malware OtterCookie" discusses a North Korea-linked attack campaign, "Contagious Interview," which employs a newly identified malware named "OtterCookie." This malware uses Socket.IO to receive remote commands, enabling actions such as executing shell commands, stealing device information, and extracting cryptocurrency wallet keys, with reported cases in Japan emphasizing the need for vigilance.

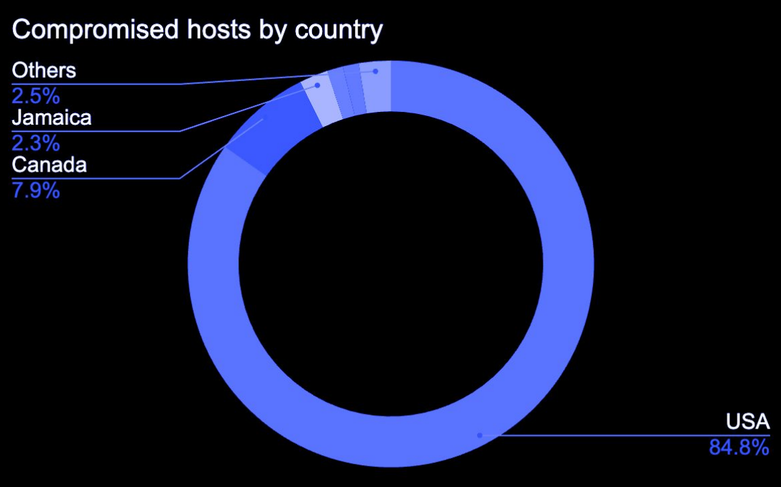
STATISTICS. **COMPROMISED DATA**

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 infected hosts and compromised cards — it will help to understand which malware families are the most active in the region.







REGIONAL TRENDS. CERT INSIGHTS

GROUP-IB

Key Regional Trends with a brief description:

01	Group-IB CERT observes new trend in abuse of Cloud Storage for phishing	Group-IB CERT has identified a growing issue where cybercriminals are exploiting Microsoft's cloud-based storage solution, Azure Blob Storage, to host phishing pages. These pages use techniques like HTML smuggling and include elements like the "doom" ID attribute. These pages gather OS and browser information through JScript. Attackers use the *.blob.core.windows[.]net subdomain, extract company logos through email parsing, and send stolen data to nocodeform[.]io.
02	Group-IB CERT identifies impersonation of U.S. marketplace brands	Group-IB CERT has detected a rising trend of cybercriminals impersonating major U.S. marketplace brands. These scam sites offer fake promotions, discounts, and gift cards, mimicking legitimate online store interfaces. Victims are often prompted to register, create fake stores, or enter sensitive personal data, including IDs and payment details, which are used for identity theft and fraud. The scammers target both consumers and legitimate marketplace sellers, making these scams a growing threat to U.S. retail brands.

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:

USE SECURE PAYMENT METHODS

Only use trusted and secure payment methods when making online transactions. Avoid entering sensitive information on unfamiliar or suspicious websites.

AVOID SHARING PERSONAL INFORMATION

Never provide sensitive personal information, like your ID number or banking details, on websites or chat pages that seem suspicious or unfamiliar.

ENABLE TWO-FACTOR AUTHENTICATION

Enable two-factor authentication (2FA) on your accounts, especially for banking or payment platforms, to add an extra layer of security.

STRENGTHEN BRAND MONITORING

Retailers and marketplace operators should enhance monitoring of unauthorized websites and domains impersonating their brands to quickly identify and take down fraudulent sites before they can affect consumers.

EDUCATE CONSUMERS

It is essential to raise awareness among consumers about the risks of fraudulent marketplace websites, providing them with tips on how to recognize fake platforms, checking for secure payment options, and avoiding unverified offers.

AVOID SHARING SENSITIVE PERSONAL INFORMATION

Do not provide personal or financial information, including email addresses, home addresses, or ID images, on any unverified or suspicious marketplace websites.

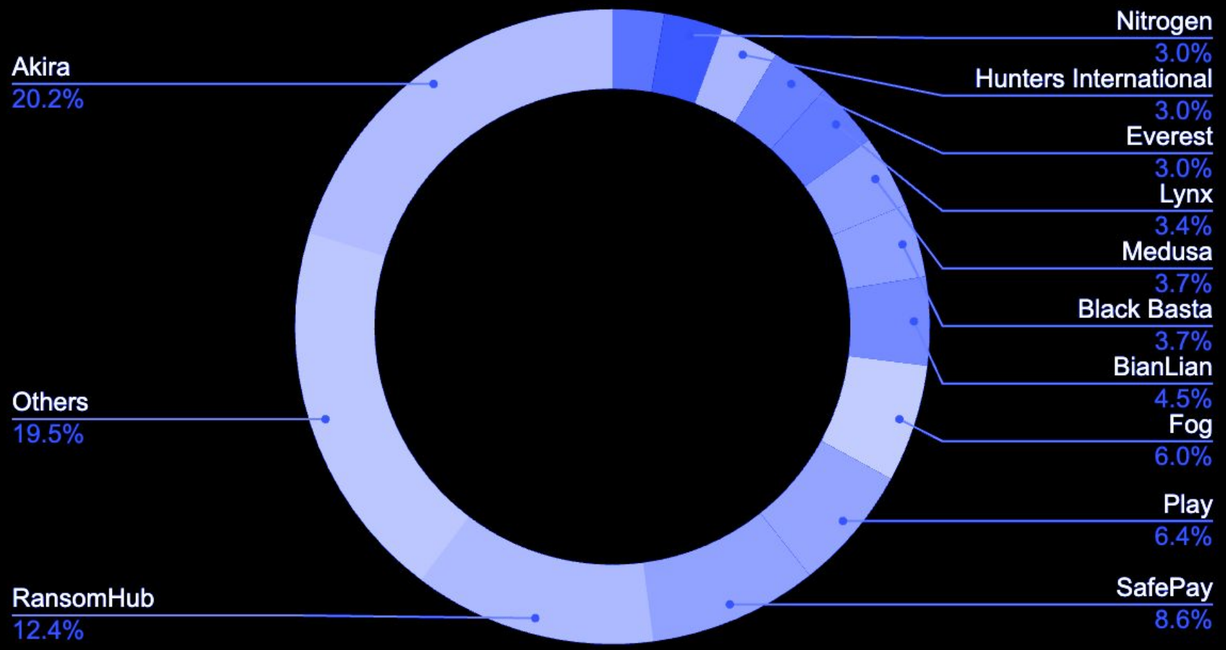
STATISTICS. **ATTACKS**

RANSOMWARE ACTIVITIES

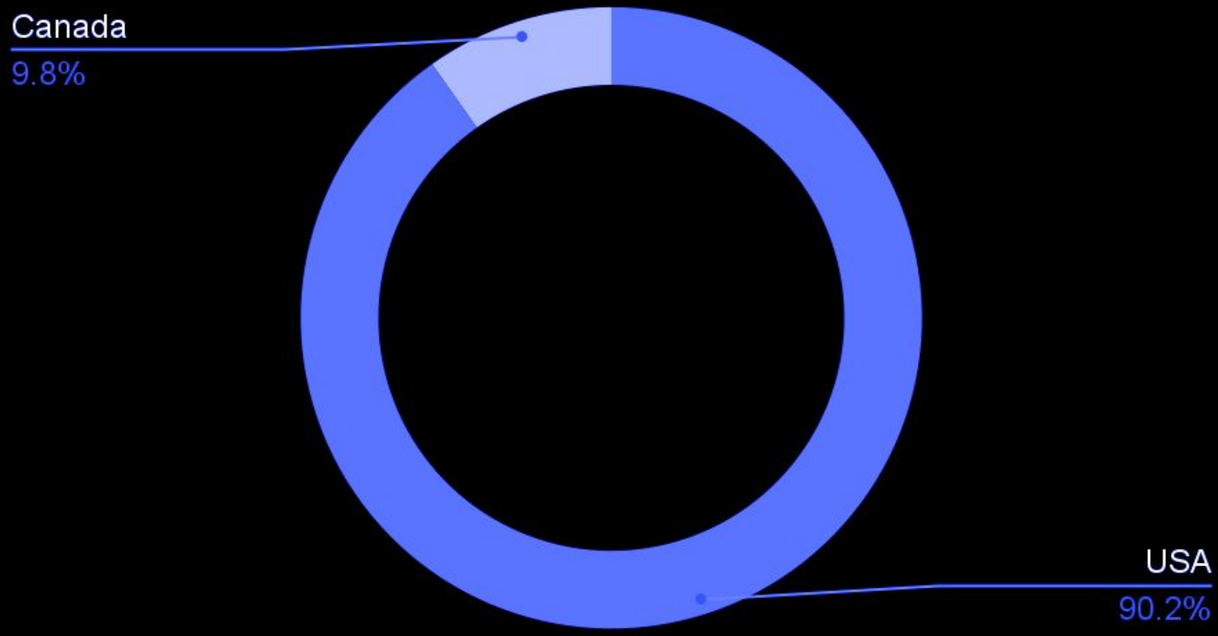
As in the LATAM region, RansomHub's affiliates authored most of the attacks against companies in the US and Canada, followed by the Conti-linked groups Akira, Black Suit, Black Basta.

According to a US congress' bill from 2024, those groups as well as Play, INC, Cl0p and some others constitute hostile foreign cyber actors due to the high risk these ransomware and extortion operations pose to US companies and critical infrastructure.

Ransomware attacks per groups:



Data Leak Sites Disclosure by Country



NORTH AMERICA INCIDENTS AND THREATS HIGHLIGHTS

GROUP-IB

Key Regional Trends with a brief description:

01 Group-IB identifies a possible connection between Scattered Spider and Black Basta ransomware gang

Group-IB's threat intelligence team identified an overlap in the network infrastructure used in a Black Basta's Cobalt Strike server and in a Phishing campaign mimicking SSO portals of US financial institutions disseminated by Scattered Spider.

Additionally, the same IP address associated to domains used by these threat actors had also been used in a previous Phishing campaign disseminated by Scattered Spider around May 2024. Therefore, this relation leads to the assumption that Scattered Spider could be affiliated with Black Basta ransomware gang.

In addition to ALPHV, according to Microsoft, criminals linked to Scattered Spider were observed deploying Qilin and RansomHub ransomware.

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

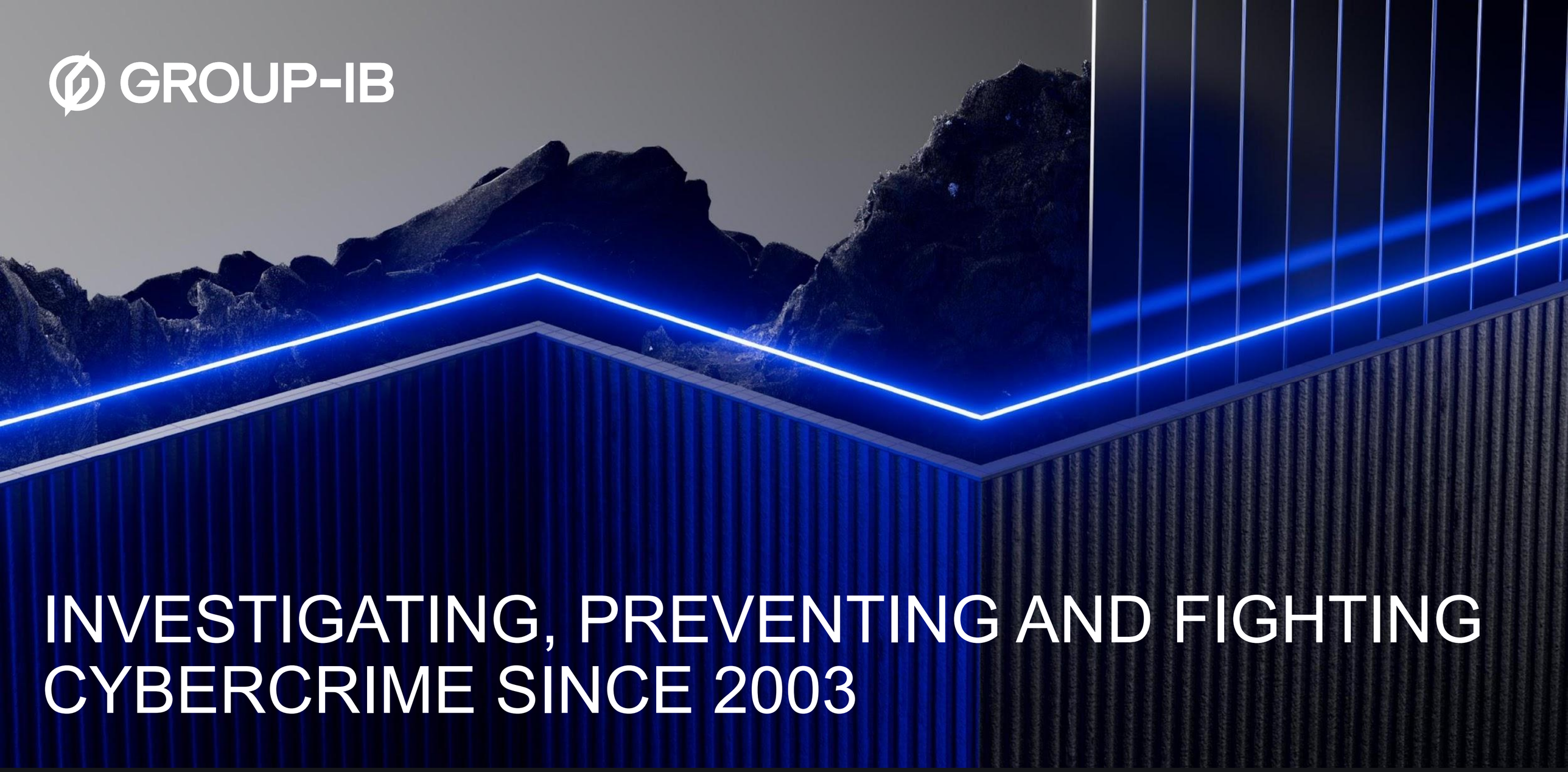
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time

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
+65 3159 3798

LINKEDIN FACEBOOK TWITTER INSTAGRAM