INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for November 2024

Report is based on data from 01.11.2024 till 01.12.2024

INTRODUCTION

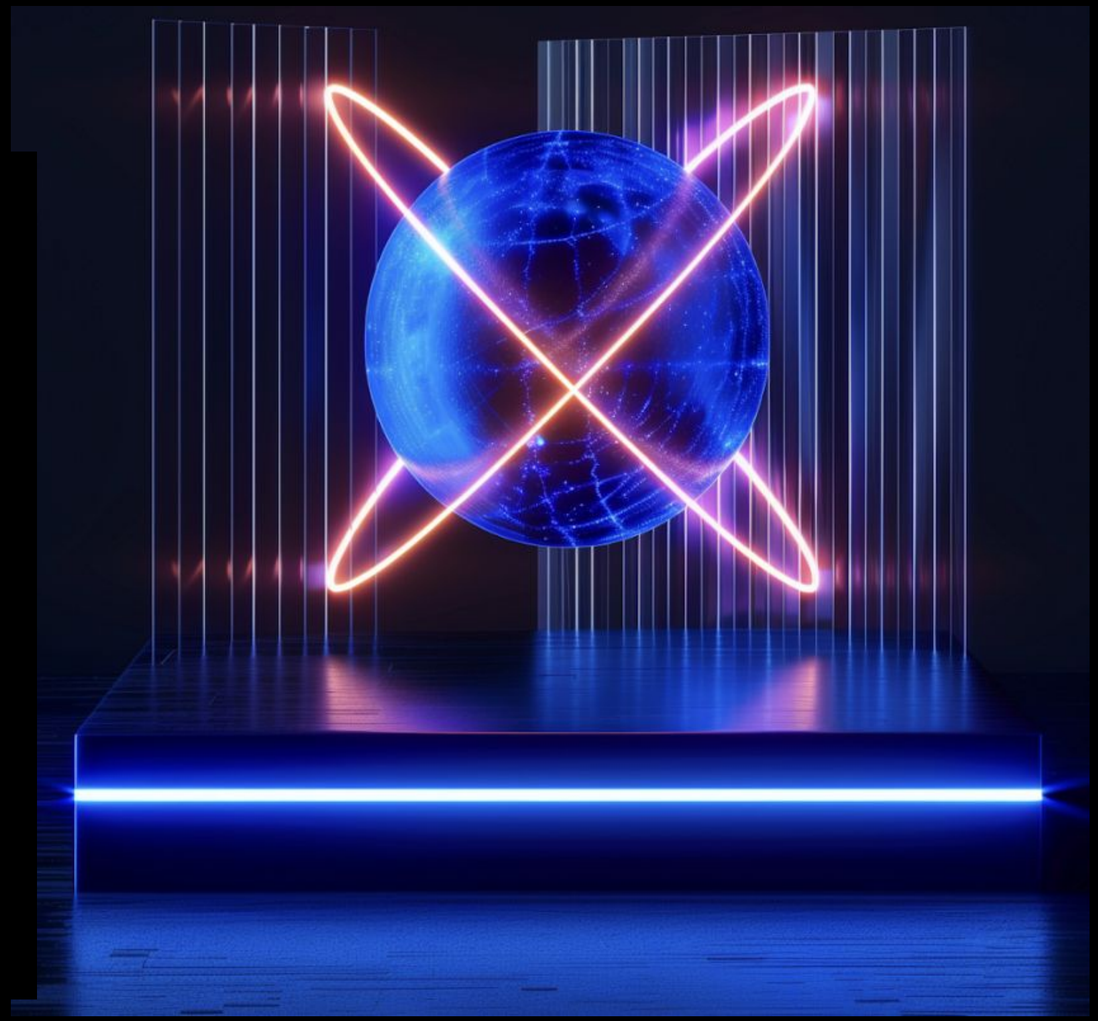
This report contains information on the most significant cybersecurity events that occurred worldwide and in the APAC region over the last month.

3 Most striking events of the month:

- Group-IB examines a fresh take on APT Lazarus techniques regarding concealing codes in Extended Attributes in order to evade detection in macOS systems. This is a new technique that has yet to be included in the MITRE ATT&CK framework.

- Group-IB contributes to INTERPOL and AFRIPOL-led “Operation Serengeti” resulting in the arrest of 1,006 suspects involved in cyber criminal activities in Africa.

- Group-IB contributes “Operation Synergia II”, an INTERPOL-led global operation aimed at combating the surge of phishing, ransomware and information stealer attacks.



GLOBAL TRENDS

GROUP-IB

Global trends with a brief description:

01	Group-IB examines a fresh take on APT Lazarus techniques regarding concealing codes in Extended Attributes in order to evade detection in macOS systems. This is a new technique that has yet to be included in the MITRE ATT&CK framework.	Group-IB researchers have identified a new technique that has yet to be included in MITRE ATT&CK framework – Code smuggling using extended attributes.Moreover, Group-IB researchers discovered a new macOS trojan dubbed RustyAttr. Trojans were developed using the Tauri framework, originally signed with a leaked certificate that was later revoked. Files are fully undetected on VirusTotal. Activity is attributed to APT Lazarus with moderate confidence. **More details**
02	Group-IB contributes to INTERPOL and AFRIPOL-led “Operation Serengeti” resulting in the arrest of 1,006 suspects involved in cybercriminal activities in Africa	Operation Serengeti,” a two-month INTERPOL and AFRIPOL-led initiative aimed at combating cybercrime across Africa took place between 2 September to 31 October 2024, culminating in the arrest of 1,006 suspects, the dismantling of 134,089 malicious infrastructure and networks that facilitated ransomware attacks, business email compromise, digital extortion, and online scams. The operation identified more than 35,000 victims, with financial losses of nearly US$193-million worldwide. These threats were highlighted in INTERPOL’s 2024 Africa Cyber Threat Assessment Report, of which Group-IB was a contributor. **More details**
03	Rise of gambling scams and fraud in MEA, EU and APAC regions.	Scammers are using fake betting game advertisements on social media to target users, with over 500 deceptive advertisements and 1,377 malicious websites identified by Group-IB CERT. Scammers use social media ads that look legitimate, luring users with promises of quick financial gain through betting games. While the majority of the ads detected are focused on Egypt, they have also been spotted targeting various regions, including the Cooperation Council for the Arab States of the Gulf (GCC), Europe, and Asia, using the same methods but different languages. **More details.**

REGIONAL TRENDS

GROUP-IB

Regional trends with a brief description:

01	Tracing the Path of VietCredCare and DuckTail: Vietnamese dark market of infostealers' data Group-IB experts have compared the tactics of operators behind VietCredCare and DuckTail stealers.	Key Discoveries: - Comparison of malware mechanisms: We compared the decompiled code of VietCredCare and DuckTail, highlighting their distinct operational models. While both target Facebook business accounts, they differ significantly in their code structures. - Ongoing presence of malware variants in Vietnam's Facebook accounts **harvesting**: The market for malware targeting Facebook accounts in Vietnam remains active and widespread. - Monetisation of infostealer business: The presence of Vietnamese actors behind Facebook infostealers is primarily observed in Facebook and Telegram groups. The monetisation of the stolen data is facilitated by selling compromised accounts, selling Facebook ad campaigns for different businesses including dropshipping, as well as creating their own campaigns to fake online shops. **More details.**
02	Group-IB contributes "Operation Synergia II", an INTERPOL-led global operation aimed at combating the surge of phishing, ransomware and information stealer attacks.	Operation Synergia II", an INTERPOL-led global operation with 95 countries participated in the operation that took down 22,000 malicious servers. In total, 41 individuals were arrested by a multinational coalition of law enforcement agencies, with 65 other suspects still under investigation. As part of the operation, Group-IB's analysts identified over 2,500 IP addresses linked to 5,000 phishing websites, and more than 1,300 IP addresses tied to various malware activities spanning 84 countries. **More details.**
03	Threat Actors continue targeting and attacking Indonesia, publishing different databases with leaked information	On November 3, 2024, an attacker with the nickname "lXXXl" on the breachforums forum published the National Archives of Indonesia database. On November 3, 2024, data belonging to an Indonesian Software company was published in the GoldPack telegram channel (belongs to TA Chucky \ Leabkase).
04	Threat Actors continue targeting and attacking Thailand, publishing different databases with leaked information	On November 7, 2024, the SQL database of jJobM E-doclite was published in the private GoldPack telegram channel (the channel belongs to the attacker Chucky\Leakbase). On November 19, 2024, 0mid16B put on sale the database of members a Thai loyalty program from Central Group. He exploited a compromised API endpoint within the Central Retail network to access and exfiltrate the data. On November 21, 2024, r57 (and partners) on the Breachforums forum put up for sale the data of the Thai insurance company Allianz Ayudhya.

Asia-Pacific Region

More Information in Group-IB Threat Intelligence Portal

STATISTICS. **ATTACKS**

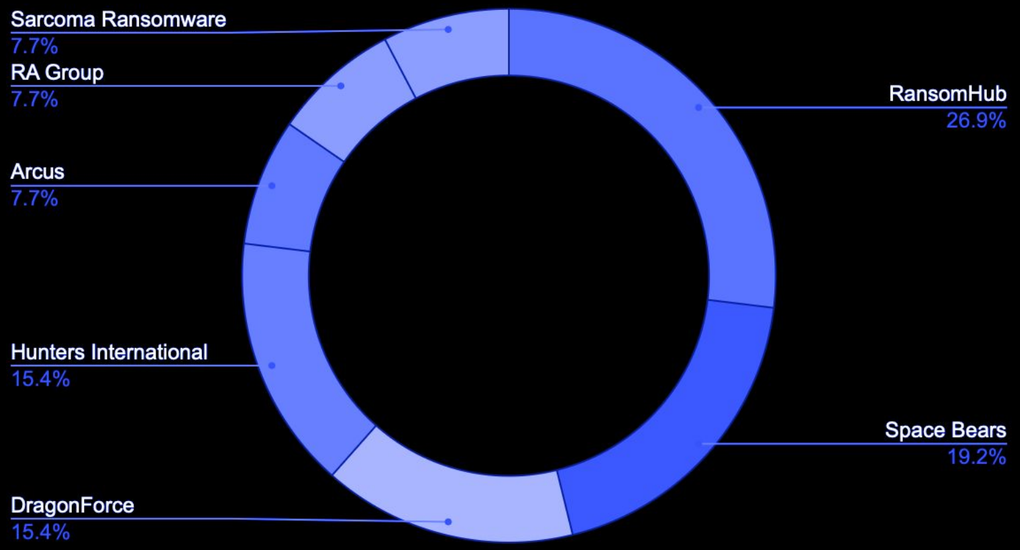
GROUP-IB

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:

- RansomHub is leading group in APAC region
- Space Bears became more active and took the 2nd place
- DragonForce and Hunters international continuing their attacks in APAC region

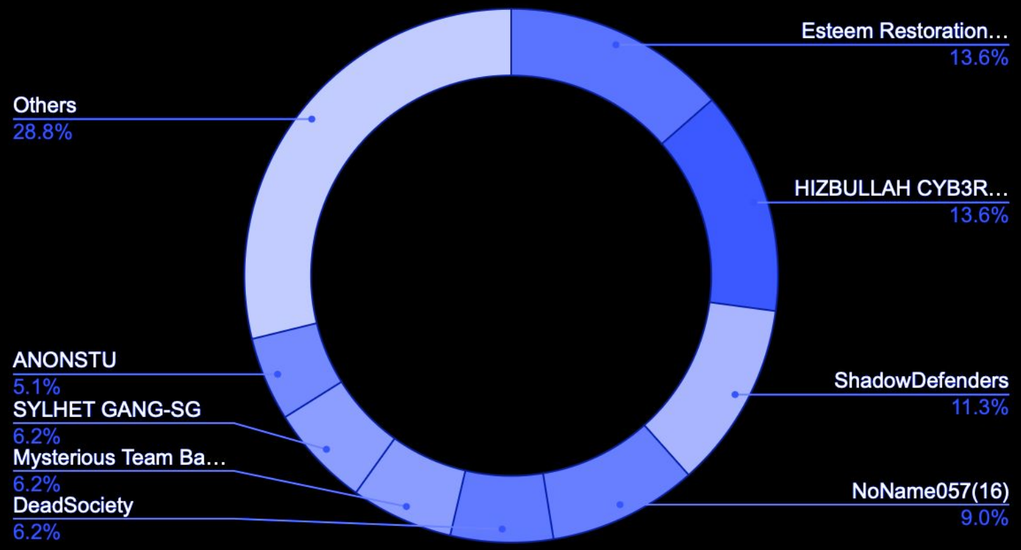
RANSOMWARE Attacks, per group



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:

HACKTIVISM Attacks, per group



STATISTICS. **COMPROMISED DATA**

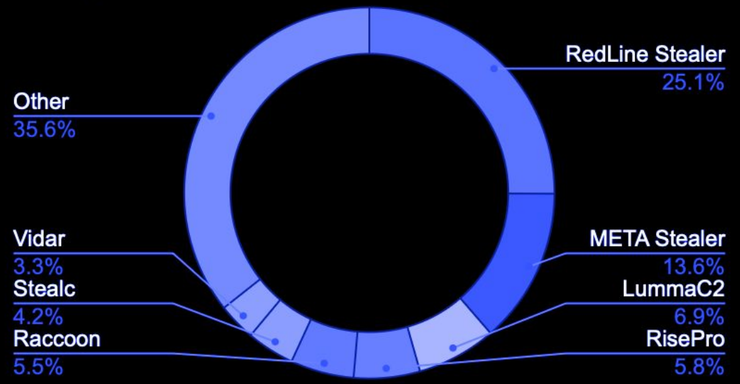
GROUP-IB

In this part of the report we will provide statistics regarding compromised accounts and compromised cards.

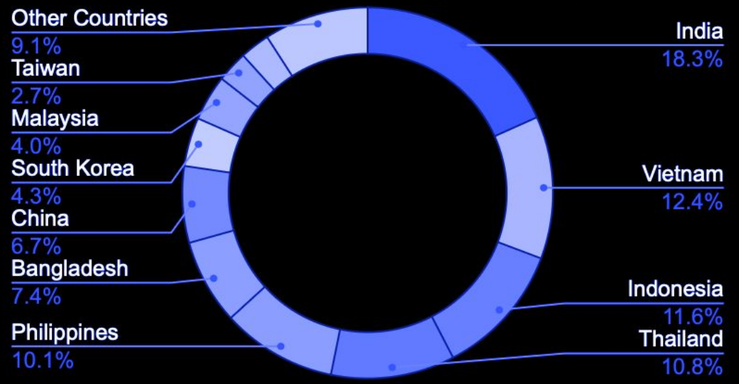
Key Trends in November:

- We see a big spike in the number of compromised accounts in APAC, especially in Vietnam, Australia and South Korea.
- The Number of compromised accounts in India, Indonesia and Thailand is consistently high.
- Malware-stealers are on the rise: RedLine stealer and META stealer is surging in APAC.
- We see increased number of compromised Bank Cards in Malaysia and Australia in November

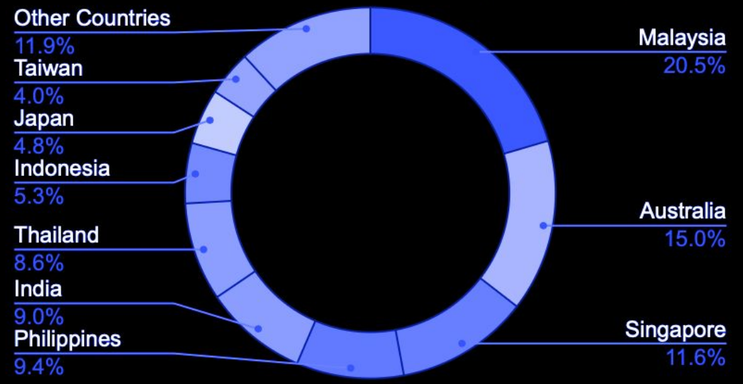
Compromised Accounts by Malware



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

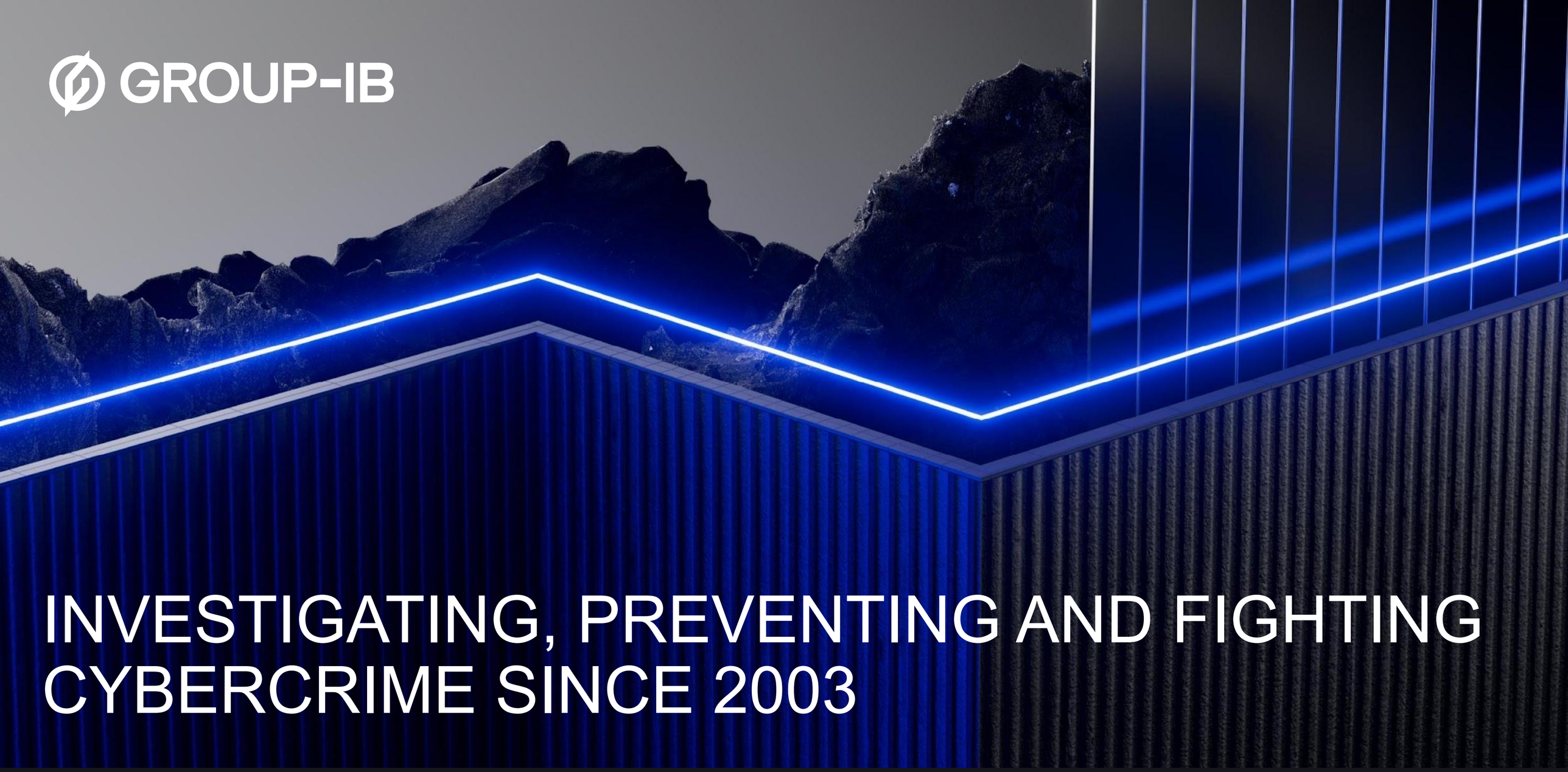
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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