GROUP-IB

February 2025

North America

INTELLIGENCE INSIGHTS

HIGHLIGHT OF THE MONTH

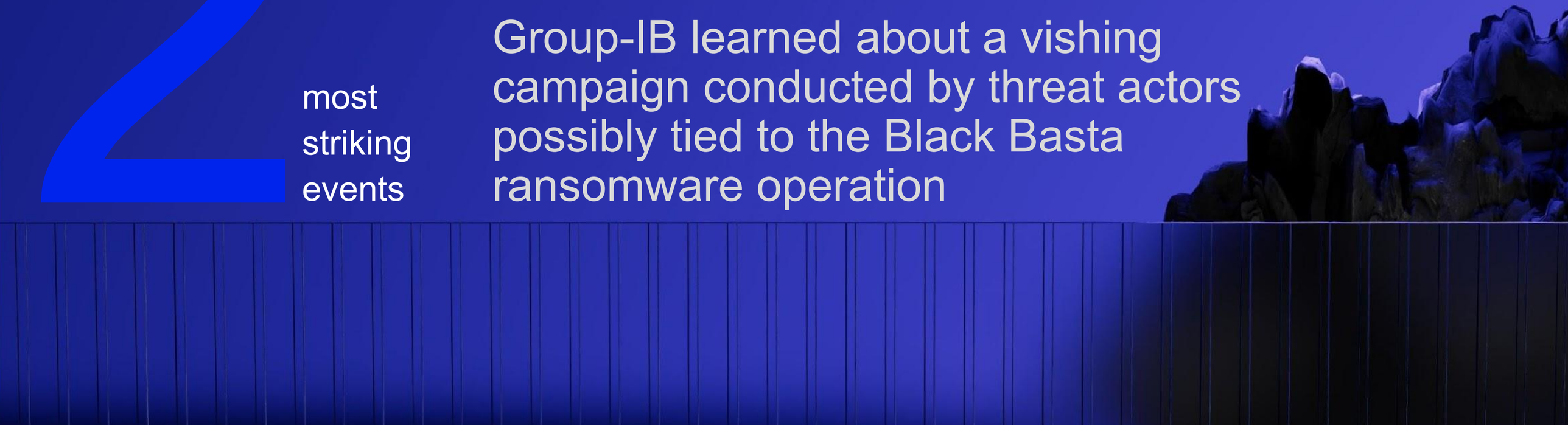
This report contains information on the most significant cybersecurity events that occurred worldwide and in North America over the last month

2

most striking events

Group-IB CERT observes new trend in QR code-based phishing for account takeovers

Group-IB learned about a vishing campaign conducted by threat actors possibly tied to the Black Basta ransomware operation



GLOBAL TRENDS

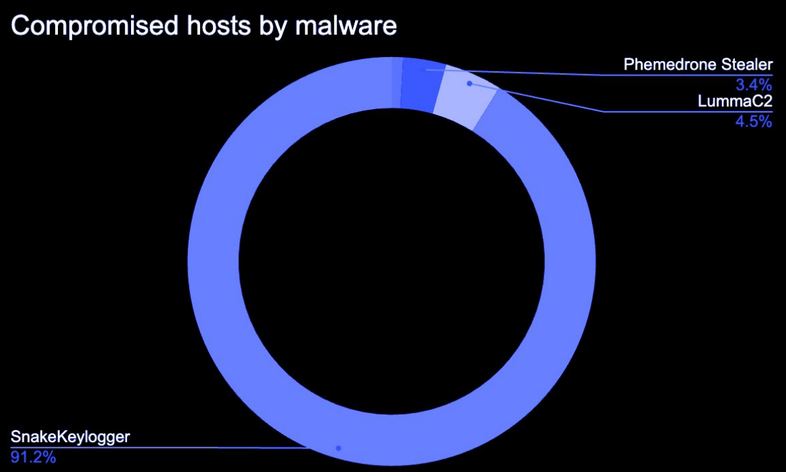
Global trends with a brief description:

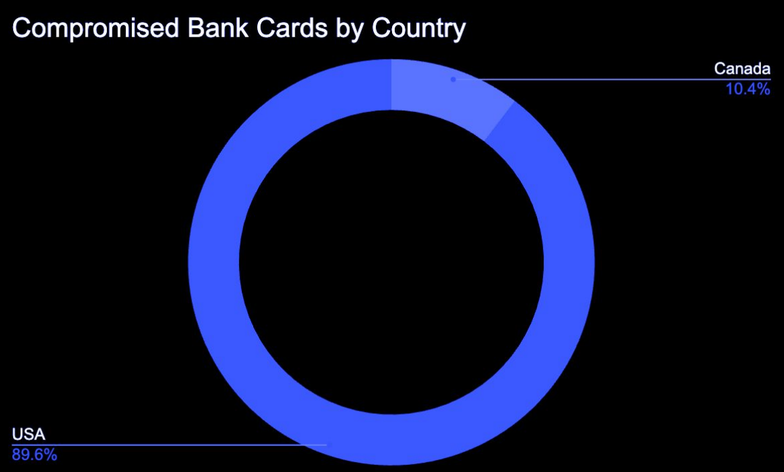
01	"The Dark Side of Automation and Rise of AI Agents: Emerging Risks of Card Testing Attacks" by Group-IB	Group-IB delves into how cybercriminals are exploiting advanced automation and AI technologies to conduct card testing attacks. These attacks involve fraudsters using stolen credit card information to make small, often unnoticed purchases to verify the card's validity before committing larger fraudulent transactions. By leveraging bots, proxies, and automation tools, attackers can efficiently test numerous cards while evading detection. The article emphasizes the challenges this poses for real-time fraud prevention and underscores the need for advanced detection systems that can identify and mitigate such automated threats. **Read more**
02	Group-IB published blogpost about RansomHub Ransomware group	A blogpost by Group-IB examines the emergence of RansomHub, a Ransomware-as-a-Service (RaaS) group that surfaced in early 2024. Capitalizing on law enforcement actions against groups like LockBit and ALPHV, RansomHub recruited affiliates and acquired ransomware source code from the defunct Knight group. Their ransomware is versatile, targeting various operating systems, including Windows, ESXi, Linux, and FreeBSD. Notably, RansomHub has compromised over 600 organizations globally, with a significant focus on the healthcare sector. The article underscores the group's adaptability and the evolving nature of ransomware threats. **Read more**

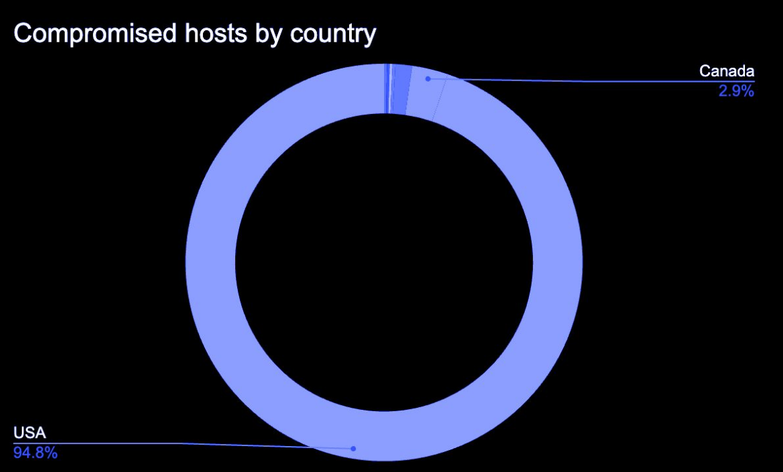
STATISTICS. **COMPROMISED DATA**

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 QR code-based phishing for account takeovers	Group-IB has identified an increase in the use of QR code manipulation for targeted phishing attacks. The latest Star Blizzard campaign demonstrates how attackers exploit broken or misleading QR codes to deceive victims into linking their accounts to attacker-controlled devices. By impersonating trusted entities, such as U.S. government officials, threat actors increase the credibility of their attacks. This highlights the rising adoption of QR code-based social engineering techniques for credential theft and unauthorized account access.
02	Group-IB CERT warns of rising Google Ads phishing attack	Cybercriminals are using fake Google Ads to steal login credentials from advertisers. They create deceptive ads that appear in Google Search, leading victims to phishing sites that look like real Google Ads login pages. These fake pages, hosted on Google Sites, make the scam more convincing and harder to detect. This growing trend shows how attackers are misusing trusted platforms to take over valuable accounts while avoiding traditional security measures.

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:

USER AWARENESS TRAINING

Educate employees and users on the risks of scanning unsolicited QR codes and the importance of verifying their authenticity before interaction

QR CODE VERIFICATION TOOLS

Implement solutions that analyze QR codes for suspicious redirects or unauthorized access attempts before they are scanned

ENABLE TWO-FACTOR AUTHENTICATION

Require MFA for all accounts associated with Google to add an extra layer of protection against unauthorized access

INCIDENT MONITORING & RESPONSE

Continuously monitor for emerging phishing techniques and respond quickly to detected threats to minimize potential damage

VERIFY LOGIN URLs

Always double-check the URL of resources login pages to ensure they are legitimate and not fake phishing sites

USE SECURE LOGIN PRACTICE

Enforce strong password policies and recommend the use of password managers to prevent password reuse and enhance account security

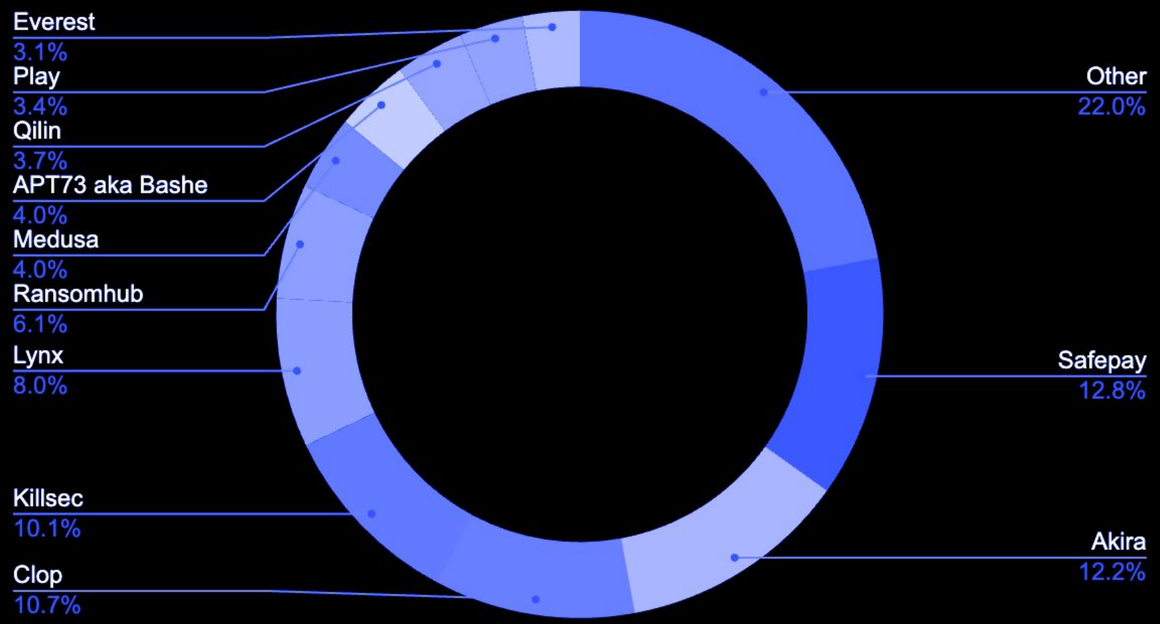
STATISTICS. **ATTACKS**

RANSOMWARE & EXTORTION ACTIVITIES

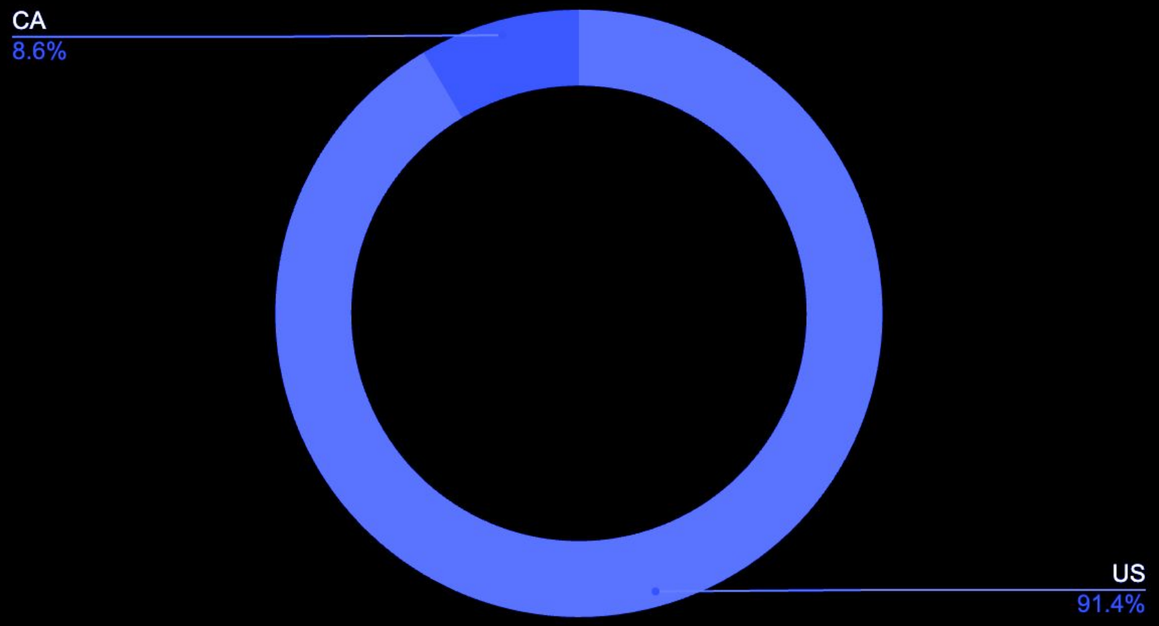
Although we observed a significant number of disclosures in the DLS of Safepay, Killsec. Bashe aka APT73, Group-IB's specialists assess that these groups pose a lower risk compared to Akira, Cl0p and PLAY, whose affiliates have already exploited complex vulnerabilities including zero days.

Despite the fact that groups like Killsec and Bashe provide ransomware to their affiliates, the criminals conducting the intrusions generally exfiltrate data and extort companies without encrypting the victims' data. This suggests that the criminals who collaborate with these groups may not be skilled enough to perform lateral movement or privilege escalation in the network.

Disclosures by group - US & CA



Data Leak Sites disclosure by country



NORTH AMERICA INCIDENTS AND THREATS HIGHLIGHTS

GROUP-IB

Key Regional Trends with a brief description:

01 Criminals abuse of Microsoft Teams to conduct *vishing* campaigns.

In the last month, Group-IB's threat intelligence team learned about a malicious *vishing* campaign conducted by financially motivated threat actors possibly tied to the Black Basta ransomware operation.

After flooding mailboxes, the criminals call companies' employees by using Microsoft Teams and pretend to be IT support of the targeted organizations, in order to deceive the users and gain initial access to the networks.

According to security company Sophos, Black Basta ransomware has been deployed in one of the intrusions conducted by the criminals. Vishing campaigns have been observed as the *modus operandi* of different adversaries including members of The Comm who are allegedly affiliated to other ransomware groups.

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:

STRENGTHEN AWARENESS CAMPAIGNS

The human asset is the most vulnerable in an organization. Therefore, it's important to periodically conduct awareness initiatives to educate about threats and risks

ESTABLISH PROCESSES

It is really important to establish a process in the organization in order to reduces the chances of employees being deceived by social engineering campaigns such as *vishing*

NEVER SHARE INFORMATION

Never share information with anyone, especially those related to systems' authentication such as OTP and 2FA codes, RMM password etc. Also, never share information about yourself and the organization (Opsec)

ENHANCE AUTHENTICATION PROCESSES

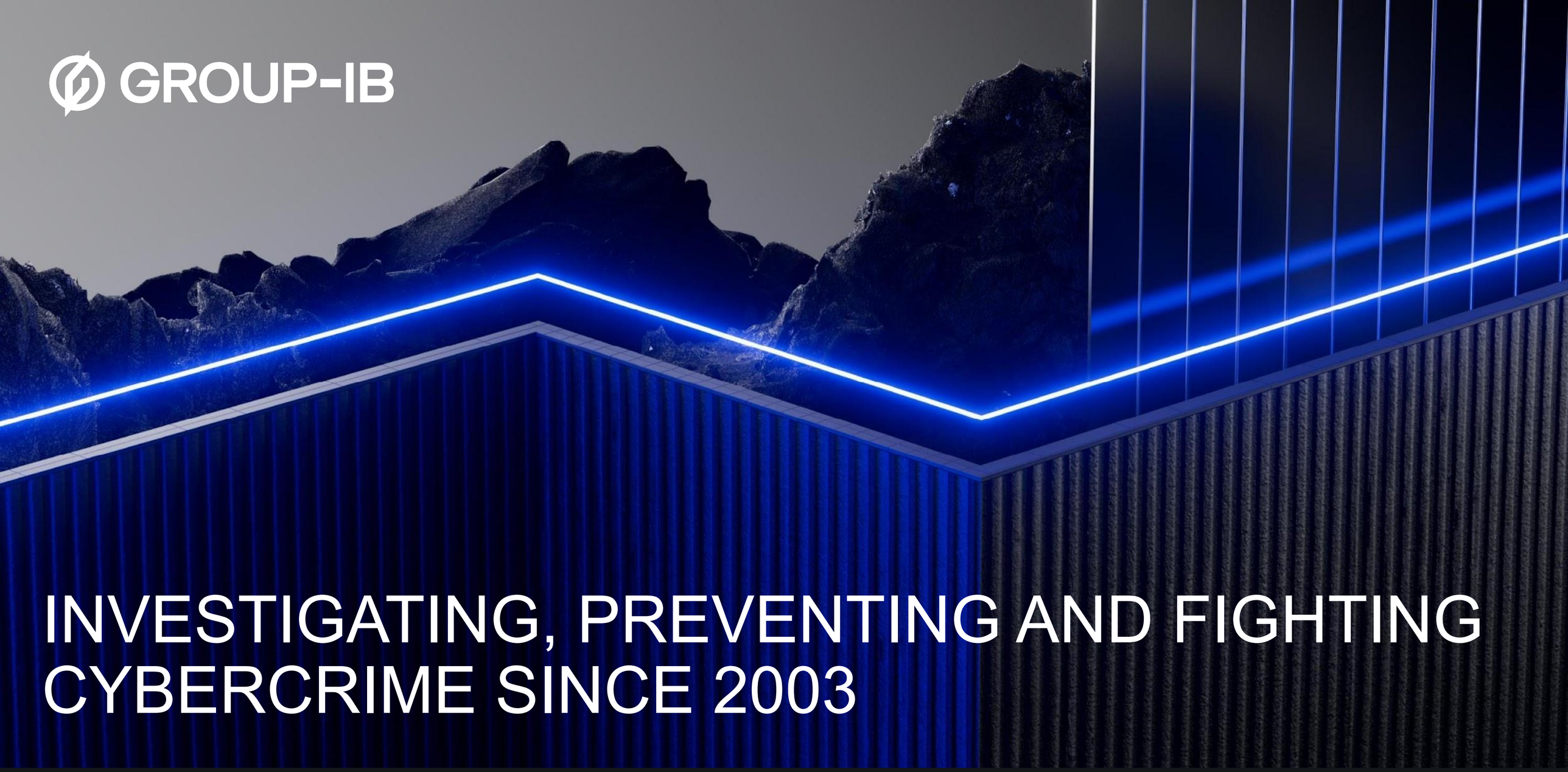
Implement MFA based on hardware or app authenticators, as they are harder to bypass in comparison to SMS and emails

DEPLOY ADVANCED THREAT DETECTION TOOLS

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

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