December 2024

Latin America

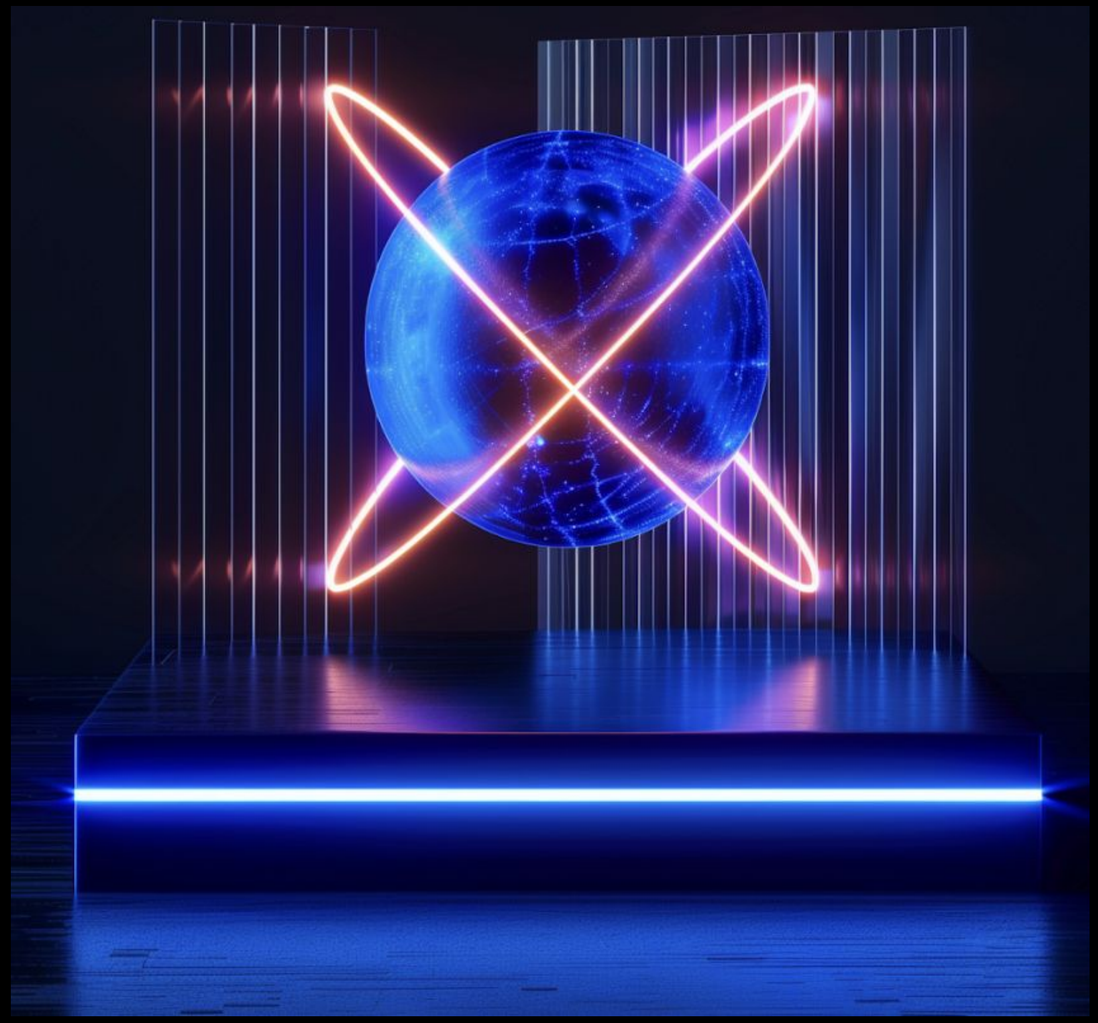
Intelligence Insights

INTRODUCTION

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

2 most striking events of the month:

- **Group-IB CERT discovered a sophisticated scam scheme targeting insurance companies and payment systems in Colombia.**
- **Group-IB discovered a malspam campaign disseminating Grandoreiro banking trojan targeting Spanish speaking countries including Spain and Argentina.**



GLOBAL TRENDS

GROUP-IB

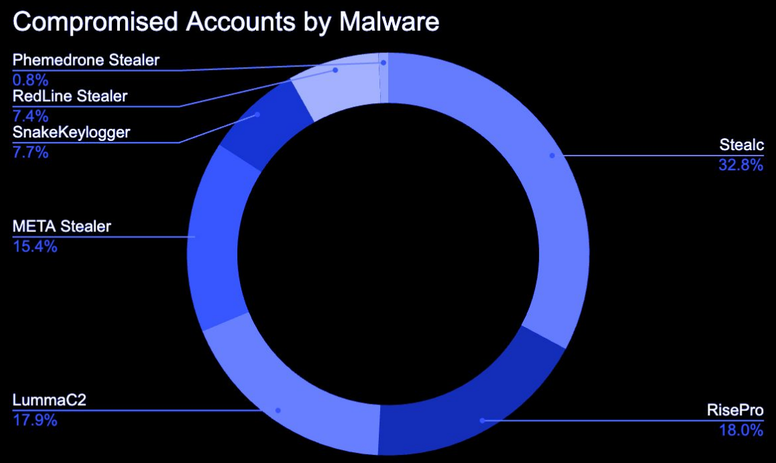
Global trends with a brief description:

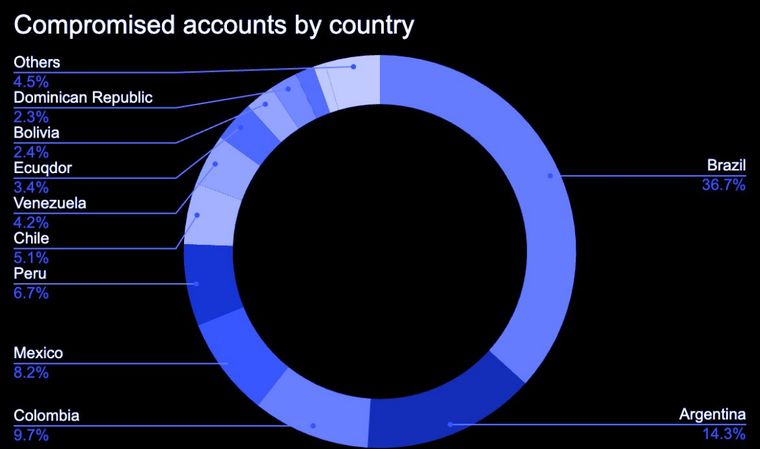
01	Group-IB published detailed research of the Cicada3301 Ransomware-as-a-Service Group	Group-IB has recently and successfully gained access to the Cicada3301 ransomware affiliate panel. In this blog, we share its inner workings based on our thorough analysis of the available ransomware versions offered within the affiliate panel, and all accessible sections to provide a definitive assessment of this threat
02	Lazarus APT's Stealth Tactics with Extended Attributes Uncovered by Group-IB specialists	Group-IB specialists have uncovered a novel Lazarus APT technique that hides malicious code in extended attributes, evading detection on macOS. This method, absent from the MITRE ATT&CK framework, includes a new trojan, "RustyAttr," developed with the Tauri framework and undetected by VirusTotal. While macOS Gatekeeper blocks unsigned apps, social engineering poses a significant risk, highlighting the need for robust security measures against evolving threats. Read more
03	Group-IB discovered utilization of the fake reCAPTCHA technique by MuddyWater APT group	A campaign utilizing the ClickFix technique to deliver RMM tool was executed allegedly targeting law enforcement employees in one of the countries bordering Iran, we asses with moderate confidence that the threat actor behind this campaign is MuddyWater
04	Group-IB CERT Team discovered a Fake Firewood Scams Target French Consumers Online	Fraudsters known as "Les brouteurs" exploit social media to sell non-existent firewood to French residents during winter. Using AI-generated fake documents and impersonating legitimate businesses, they trick victims into transferring money. Group-IB's investigation highlights the evolving sophistication of these scams. Consumers and businesses must stay vigilant, verify credentials, and adopt fraud prevention measures to mitigate financial losses. Read more.

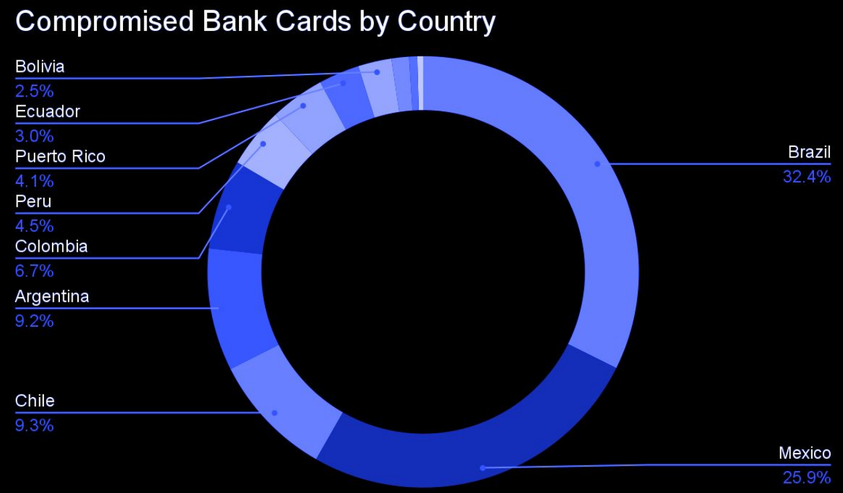
STATISTICS. **COMPROMISED DATA**

Stealer plays an import role in the cybercrime supply chain as the data stolen from the computer infected by this type of malware can lead to incident of higher impact such as ransomware, extortion and espionage. Valid accounts, that is, credentials exfiltrated by stealers are commonly used by threat actors get initial access to companies as well as to escalate privileges and perform defense evasion.

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: Latin America

Key Regional Trends with a brief description:

01	The Group-IB CERT team has identified a scam targeting Argentine banks, exploiting fake ads to impersonate official contact channels	These ads, often designed to attract elderly individuals with offers of benefits and discounts, include WhatsApp links where scammers use social engineering to extract sensitive personal and banking information. The scheme leverages trust in well-known brands and is part of a broader trend targeting financial institutions in Argentina
02	Group-IB CERT has identified a sophisticated scam scheme targeting insurance companies and payment systems in Colombia	The scam involves a multi-stage process utilizing fraudulent websites impersonating legitimate brands. The first stage exploits public car license databases to convince users of the site's authenticity by displaying accurate vehicle insurance details. Victims with expired insurance are redirected to a second site, where they are prompted to provide sensitive banking information under the guise of purchasing insurance. Finally, the scheme culminates in a third site mimicking payment systems to execute fraudulent transactions. This method leverages trust in well-known brands and public data to deceive users and facilitate financial theft

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:

VERIFY OFFICIAL CHANNELS

Always verify the authenticity of contact channels by visiting the official website of your bank or contacting their official customer service

BE CAUTIOUS WITH PERSONAL INFORMATION

Never share sensitive personal or banking information, such as account details, card numbers, PIN codes, or One-Time Password, through phone calls, emails, or messaging apps like WhatsApp

EDUCATE VULNERABLE GROUPS

Spread awareness among elderly family members and friends about scams targeting retirees, teaching them how to recognize and avoid such threats

STRENGTHEN AWARENESS CAMPAIGNS

Launch public awareness initiatives to educate customers about phishing and impersonation scams, emphasizing the importance of verifying communication channels.

ENHANCE AUTHENTICATION PROCESSES

Implement robust multi-factor authentication for sensitive transactions, reducing the likelihood of fraud even if some information is compromised.

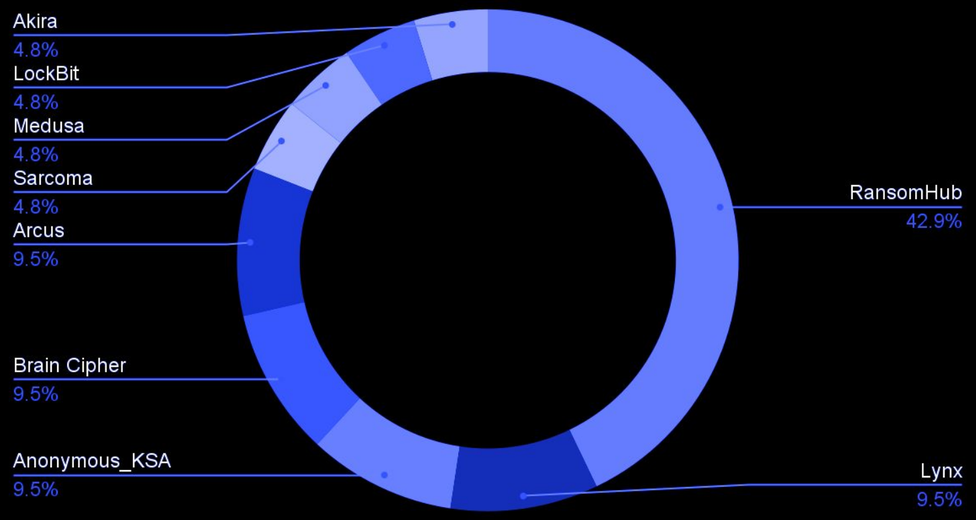
LEVERAGE THREAT INTELLIGENCE

Regularly analyze scam trends and indicators of compromise (IOCs) to update fraud detection systems and adapt defenses to emerging threats.

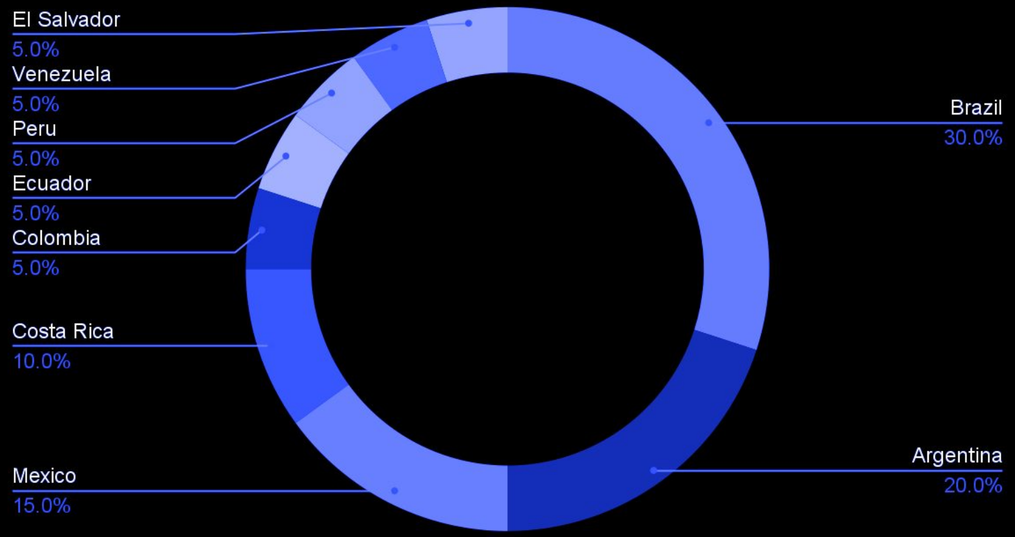
STATISTICS. **ATTACKS**
RANSOMWARE ACTIVITIES

RansomHub is not only the group with the most victims disclosed on its DSL, but also the RaaS operation which has victimized the most companies in Latin America (LATAM). Therefore, organizations in the LATAM region should prioritize TTPs related to intrusions conducted by affiliates of this group. This month we highlight the attacks against the Brazilian companies **Lojas Marisa** and **Aeris Energy** authored by Medusa and Hunters International, respectively.

Ransomware Attacks per group



Dedicated Leak Sites by country



LATAM INCIDENTS AND THREATS HIGHLIGHTS

GROUP-IB

Key Regional Highlights with a brief description:

01	GhostSpy Android Remote Access Trojan (RAT) partnership campaign	Group-IB identified a partnership campaign which allegedly give criminals access to the GhostSpy's source code and a reseller opportunity. GhostSpy (aka Brazilian Spy) is an Android RAT and possibly a rebrand of GoatRAT also known as FantasyMW and CriminalMW. Although criminals collaborating with this group have been arrested, the malware has resurfaced in early 2024 as GhostSpy
02	Malicious campaign targeting Spanish speaking countries disseminating Grandoreiro	Group-IB has discovered a *malspam* campaign disseminating Grandoreiro banking trojan targeting Spanish speaking countries including Spain and Argentina. The malicious campaign impersonates the Spanish company Endesa and utilizes the domain “cld.pt” associated with MEO Cloud cloud storage to download a zip file which is the first stage of the infection chain

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:

OFFICIAL APK STORE

Android RATs including GhostSpy are usually available on third-party APK repositories such as APKMirror, APKPure and Uptodown. Make sure to install apps only from Google Play

APK PERMISSIONS

Most Android RATs require *root* privileges and the activation of accessibility features. So do not grant permission nor active any feature on Android unless you are sure it is a legitimate application

MALICIOUS WEBSITES

Threat actors may disseminate malicious APK through Phishing pages. Therefore, do not download and install apps from unknown and doubtful sources

VERIFY EMAIL INFORMATION

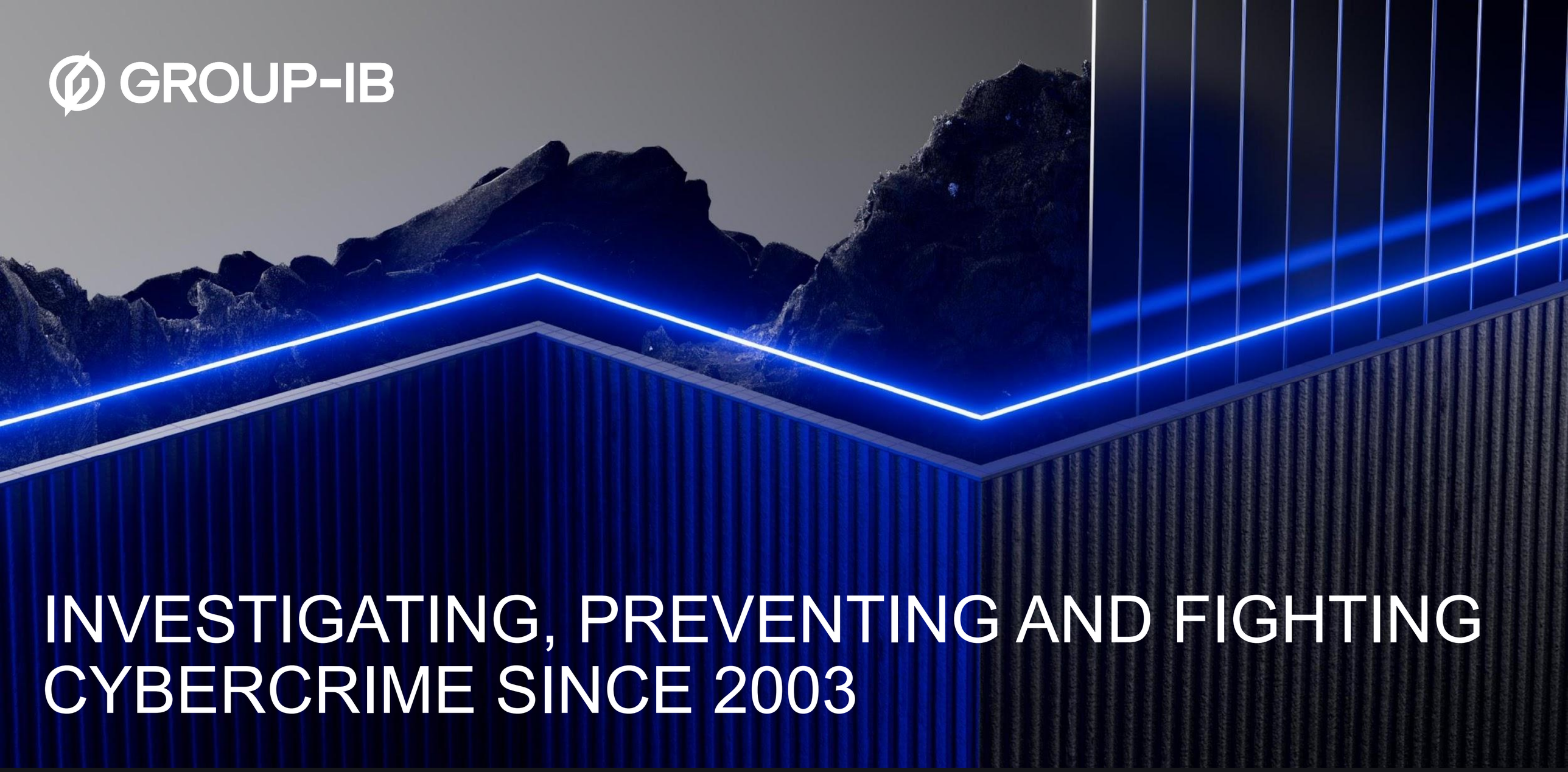
Threat actors may disseminate malspam campaigns from legitimate compromised accounts. Therefore in addition to checking the email sender, always verify information presented in the email and validate with your bank

DO NOT BE GUIDED

Social engineering campaigns require from users an action such as clicking, downloading and providing information. Therefore, instead of performing any action contact the company you are client of

ENABLE MFA

Avoid SMS and Email as MFA. Prefer to use hardware security keys, authenticator apps in addition to the the resources provided by the bank systems



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