February 2025

Latin America

INTELLIGENCE INSIGHTS

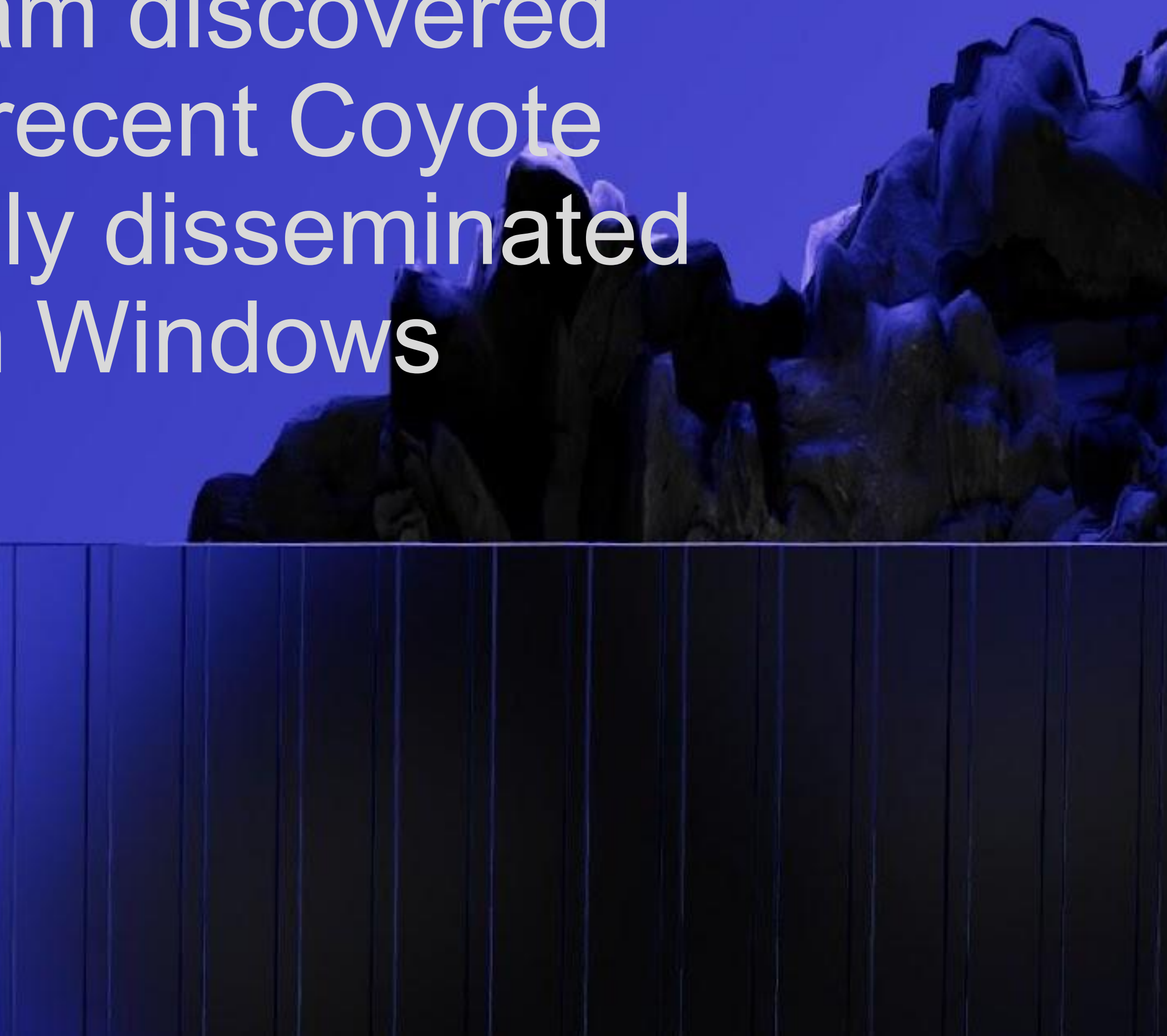
HIGHLIGHT OF THE MONTH

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

2 most striking events

Group-IB CERT has identified a new phishing scam in Chile targeting users via SMS messages to steal personal and financial data

Group-IB's threat intelligence team discovered hundreds of LNK files used in a recent Coyote banking trojan campaign allegedly disseminated via WhatsApp targeting Brazilian Windows users



GLOBAL TRENDS

GROUP-IB

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

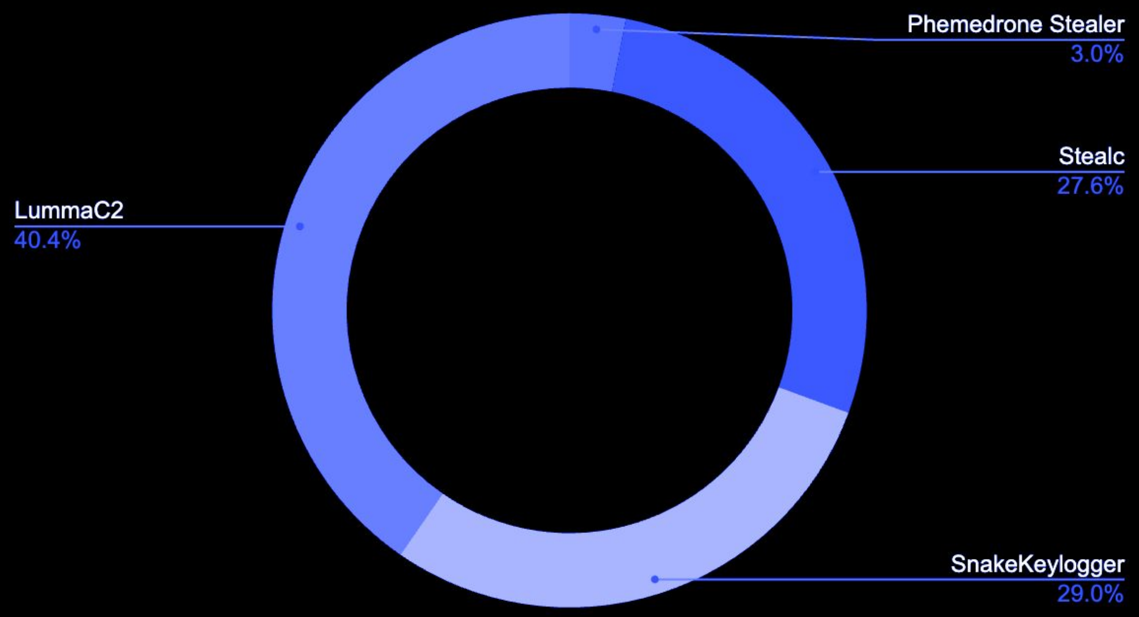
A blogpost by Group-IB examines the emergence of RansomHub, a Ransomware-as-a-Service (RaaS) group that surfaced in early 2024. Capitalizing on law enforcement actions against groups like LockBit and ALPHV, RansomHub recruited affiliates and acquired ransomware source code from the defunct Knight group. 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.

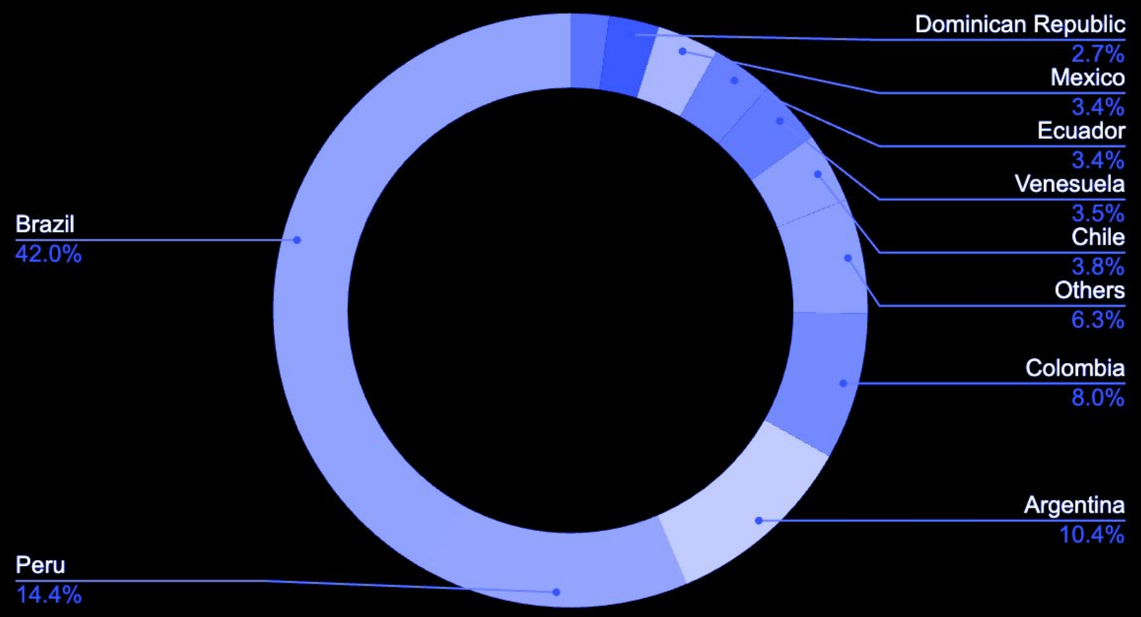
Read more

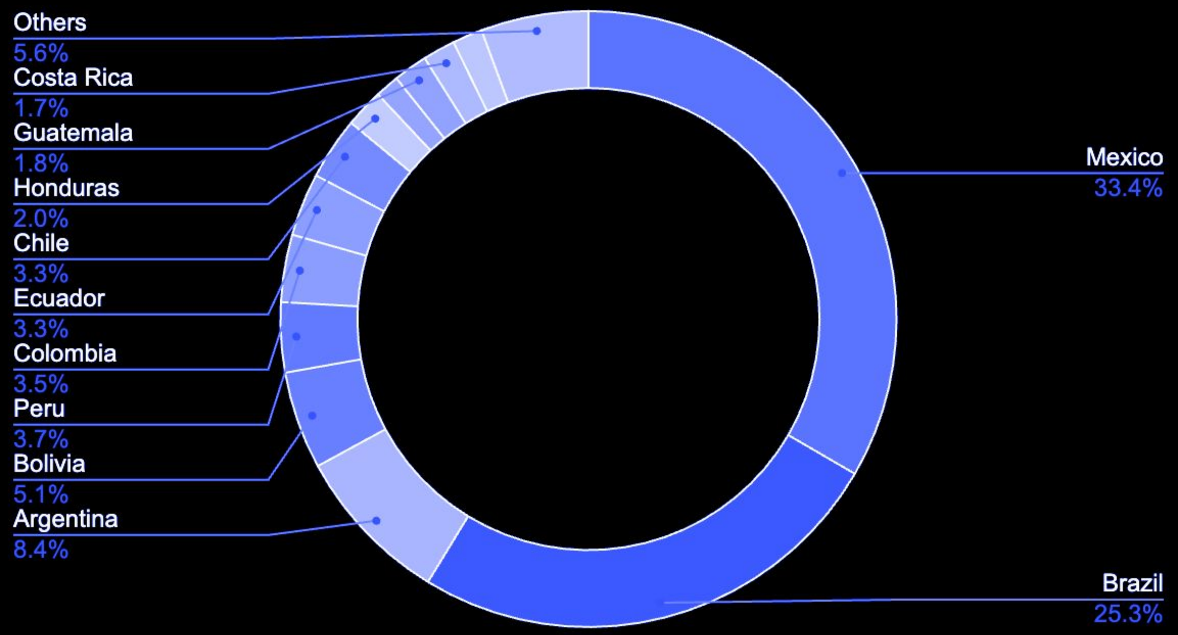
STATISTICS. **COMPROMISED DATA**

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.


Compromised hosts by malware


Compromised hosts by country


Compromised Bank Cards by Country

REGIONAL TRENDS
CERT Insights: Latin America

Key Regional Trends with a brief description:

01 Group-IB CERT has identified a new phishing scam in Chile targeting users via SMS messages to steal personal and financial data

Group-IB CERT has identified a phishing scam in Chile where cybercriminals send SMS messages to users, pretending to be from legitimate companies. These messages claim that users have expiring points they can redeem for rewards. The SMS includes a link that leads to a fake form asking for personal and financial information, including credit card details. This scam primarily targets customers of telecom and service providers in Chile

02 Group-IB CERT has detected a phishing scheme in Peru impersonating financial institutions to steal banking credentials

Group-IB CERT has identified a phishing scam in Peru targeting individuals through fraudulent loan application processes. Victims are prompted to enter their DNI number and contact details before being asked to verify their identity via facial recognition or bank card information. The facial recognition option is intentionally non-functional, coercing users into providing their card details, online banking password, and PIN. The scheme is designed to collect only valid credentials, which are then exploited for fraudulent activities. Upon completion, victims are redirected to a legitimate banking website, leaving them unaware that their data has been compromised

CONCLUSIONS AND RECOMMENDATIONS

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 MESSAGES DIRECTLY

Contact the company through official channels to confirm any promotional offers before clicking on links

AVOID CLICKING ON LINKS IN SMS

Do not open links from unsolicited messages, especially those claiming urgency or rewards

CHECK THE URL CAREFULLY

Scam websites may look legitimate but often have small differences in the domain name

REPORT SUSPICIOUS MESSAGES

Forward phishing SMS to local cybersecurity authorities or your service provider to help prevent further attacks

BE CAUTIOUS WITH LOAN APPLICATION

Only apply for loans through official channels and avoid unsolicited offers that ask for personal information

ENABLE TWO-FACTOR AUTHENTICATION

Secure your accounts with 2FA to reduce the risk of unauthorized access

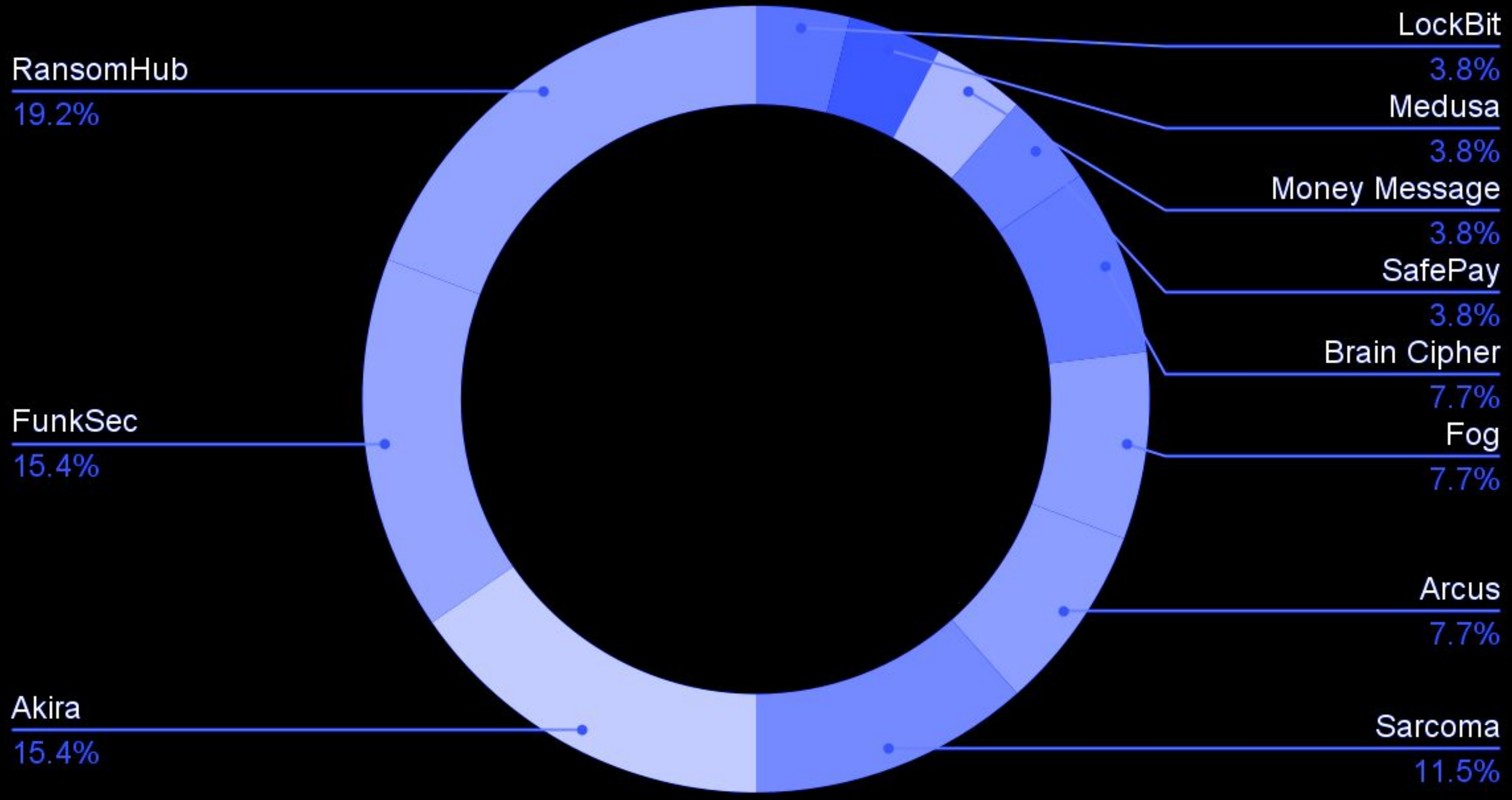
STATISTICS. **ATTACKS**

RANSOMWARE & EXTORTION ACTIVITIES

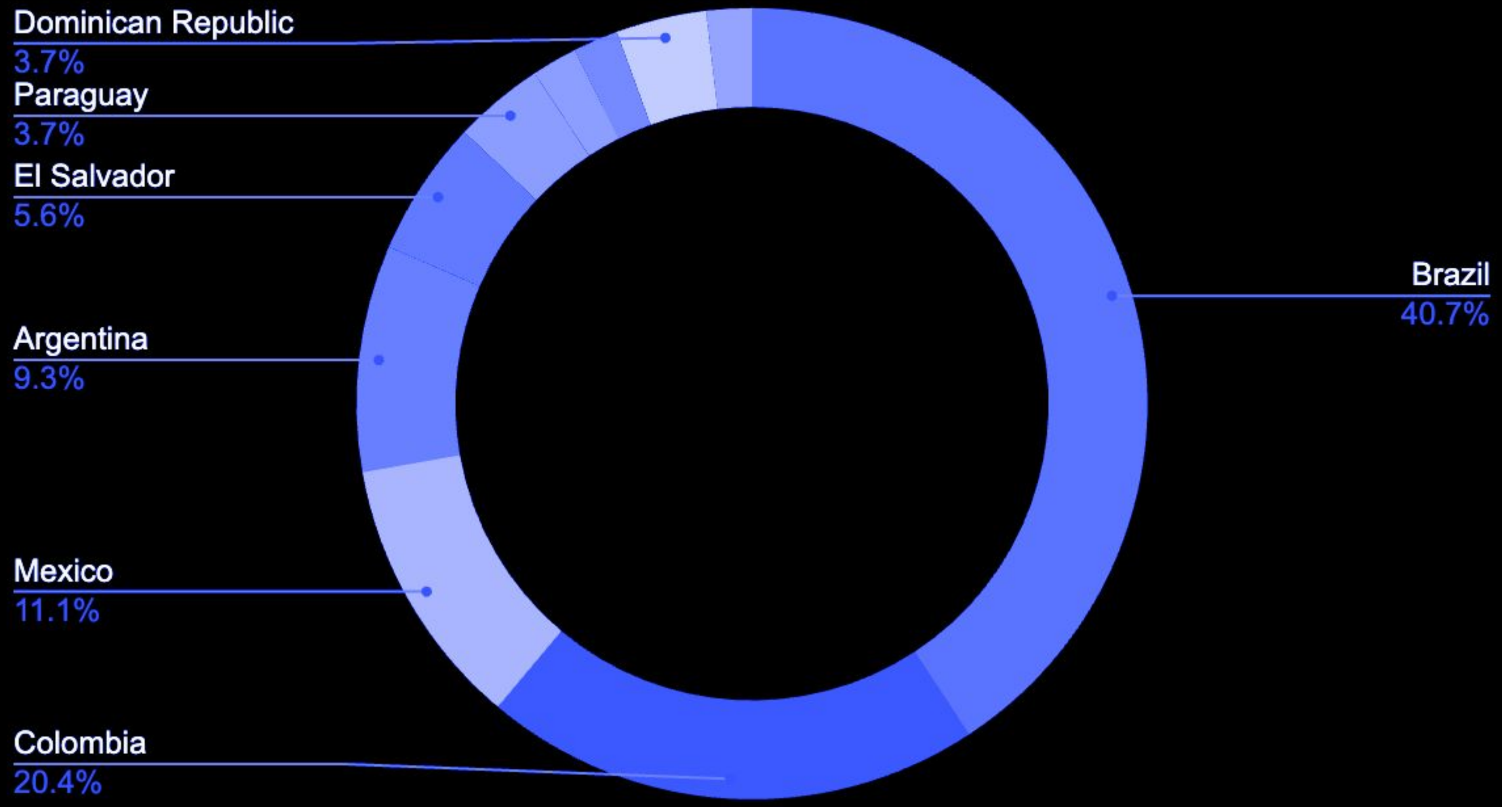
In this month we observed an increase **from 26 to 54** in the number of companies disclosed on DLS of extortion and ransomware operations.

Akira, an alleged Conti-based ransomware operation, was the group with the most disclosures in the LATAM region, with 6 companies from Brazil, 2 from Argentina and 2 from Colombia.

Ransomware Atacks per groups:



Data Leak Sites disclosure by country



LATAM INCIDENTS AND THREATS HIGHLIGHTS

GROUP-IB

Key Regional Highlights with a brief description:

01 Group-IB's detected malicious campaign disseminating Coyote banking trojan.

Group-IB's threat intelligence team learned about a recent malicious campaign aimed at stealing sensitive data from Brazilian Windows users by infecting them with a new version of the Coyote malware allegedly delivered via WhatsApp.

The infection process begins once the victim executes an LNK file faking a *Comprovante* (payment confirmation) which runs a PowerShell to download the next stage of the threat.

02 Suspicious activity regarding the bypass of Appdome mobile security solution.

Group-IB's specialists observed what seems to be Brazilian criminals looking for a service or individual able to bypass security mechanisms of mobile apps protected with Appdome anti-fraud solutions.

The threat actors have asked for help on different sources such as Exploit forum, Facebook and a Chinese-speaking Telegram fraud group. In one of the posts, a forum user shared logs related to “Caixa Tem”, which suggests this might be one of the targeted apps.

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:

LNK Files

Most of the banking trojans prevalent in the LATAM region, such as Astaroth, Mispadu and Mekotio have a multi-staged infection chain which often begins (but is not limited to), with the execution of a malicious LNK file

Malpam campaigns

Banking trojans targeting the LATAM region share similar TTPs, including the dissemination of the malware via Malpam campaigns. To do this, criminals eventually use legitimate but compromised e-mail accounts

WhatsApp Social Engineering

Brazilian financial institutions found in the target list of Coyote do not contact account holders via WhatsApp in order to provide any document. Do not open any file allegedly from your bank sent to you via WhatsApp

Enable 2FA & Registrato

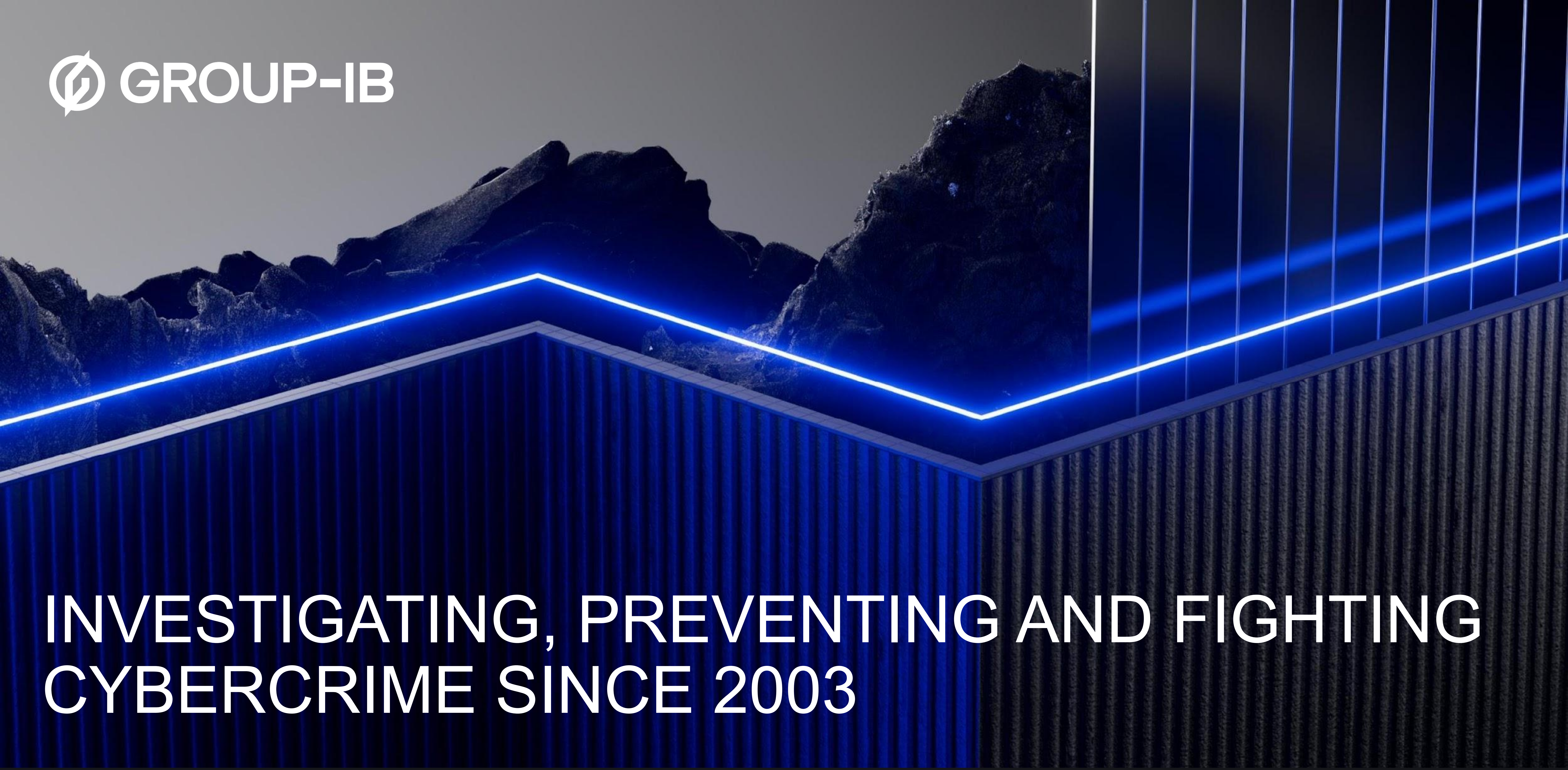
Always enable 2FA on every internet banking and apps account you have and periodically check for bank accounts associated to you on BACEN's system Registrato

VIRTUAL CREDIT CARD

Only use virtual credit card to make online purchases as it uses randomly generated numbers and masks your real card information. Also, create different cards so that you can better identify it in case of a data breach

ENABLE 3D SECURE

Card holders as well as e-commerces should enable 3D Secure such as MasterCard SecureCode, Verified by Visa and American Express SafeKey in order to have an extra verification to reduce fraudulent activity



GROUP-IB

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