GROUP-IB

LATIN AMERICA

INTELLIGENCE INSIGHTS

APRIL 2025

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 Brazil where cybercriminals use rogue mobile base stations to send SMS messages to steal personal and financial data

Group-IB's specialists discovered several web open directories with Python scripts allegedly used to brute force email accounts in order to get unauthorized access to SMTP servers of Brazilian companies

GLOBAL TRENDS

Global trends with a brief description:

01 A threat actor known as rose87168 offered for sale data allegedly stolen from Oracle.	In March 2025, a threat actor known as **rose87168** offered for sale data allegedly stolen from Oracle, the American multinational computer technology corporation—specifically targeting its Oracle Cloud services. The attacker claimed the breach occurred in January 2025 and initially attempted to negotiate a private sale with Oracle, which was reportedly unsuccessful
02 The Group-IB published the comprehensive blog on ClickFix	The Group-IB published the comprehensive blog describes a social engineering technique called ClickFix, usually used by attackers to trick users into executing malicious PowerShell scripts. Victims are lured into clicking fake "Fix It" buttons or CAPTCHA prompts, which copy malware code to their clipboard and instruct them to run it manually. This method has been used to deliver infostealers like Lumma and has gained popularity among both cybercriminals (even APT groups). Group-IB warns of its growing use and advises increased user awareness to prevent compromise

GLOBAL TRENDS

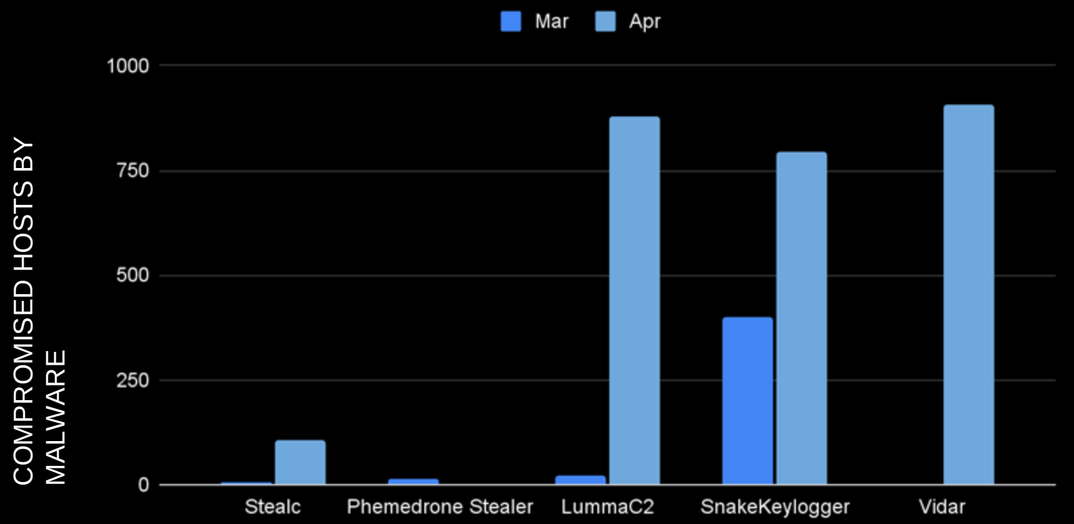
Global trends with a brief description:

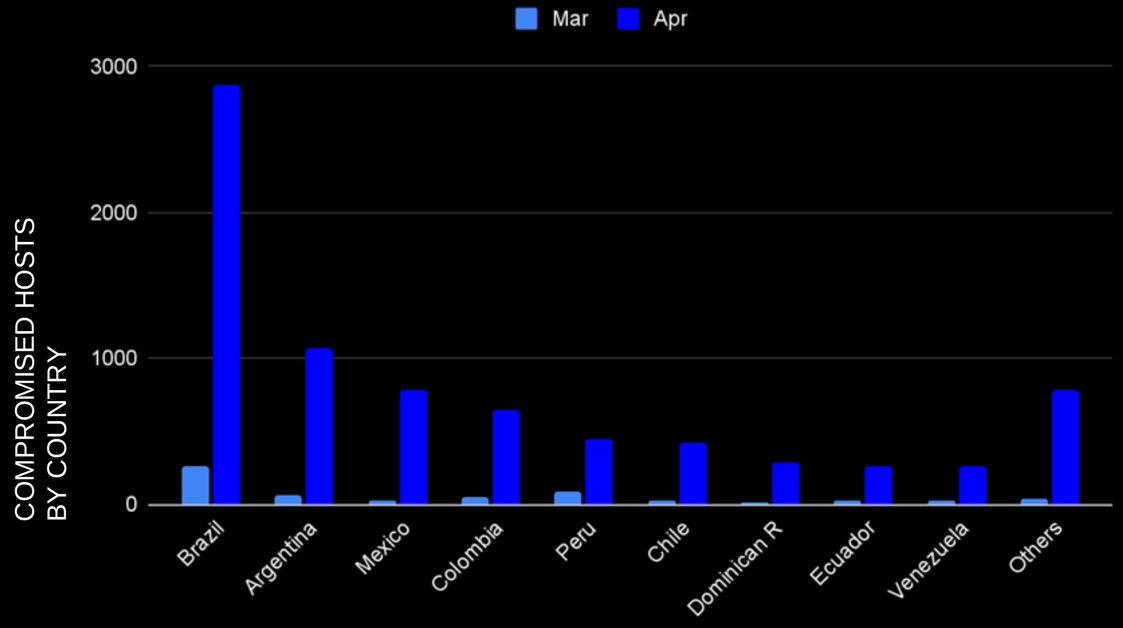
01 Cybercriminal responsible for over 90 data breaches worldwide apprehended in joint operation

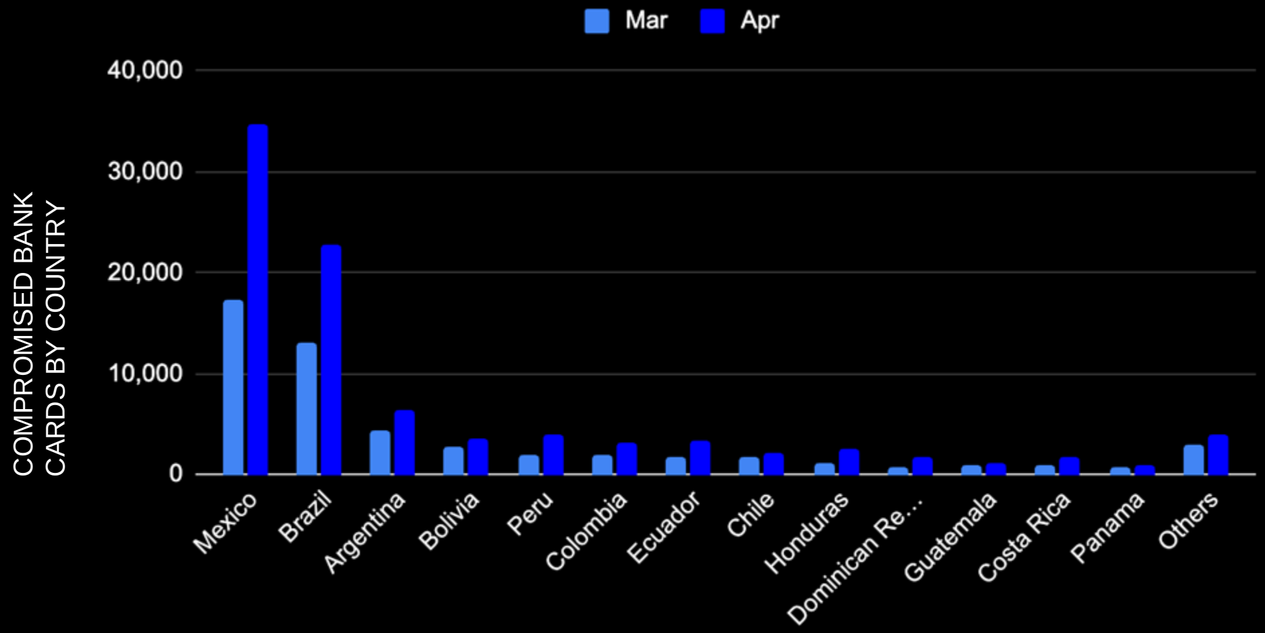
Group-IB, in collaboration with the Royal Thai Police and the Singapore Police Force, successfully apprehended a cybercriminal responsible for over 90 data breaches worldwide. The individual, operating under aliases such as ALTDOS, DESORDEN, GHOSTR, and 0mid16B, targeted large private companies across various sectors, including finance, retail, and manufacturing. Group-IB's Threat Intelligence and High-Tech Crime Investigation teams tracked the cybercriminal across multiple aliases, contributing significantly to the investigation. The arrest took place on February 26, 2025, in Thailand, marking a significant milestone in combating global cybercrime

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

Group-IB CERT has identified a new phishing scam in Brazil where cybercriminals use rogue mobile base stations to send SMS messages to steal personal and financial data

Group-IB CERT has discovered a phishing campaign in Brazil, where attackers use portable mobile base stations, like IMSI-catchers or femtocells, to send SMS messages. These rogue devices bypass telecom filters, targeting users even without an active cellular connection. The SMS informs recipients of nearly 100,000 expiring loyalty points, offering rewards like cashback, electronics, or miles. A malicious link leads to a phishing site designed to steal personal and financial data, including credit card details

02

Group-IB CERT has identified a widespread investment scam targeting multiple Latin American countries, where cybercriminals use WordPress-based websites to promote fake money-making schemes involving trading, AI, and e-commerce

Group-IB CERT has discovered a phishing campaign in Latin America, where attackers use WordPress-based websites to promote fake investment schemes. These sites promise to teach users how to earn money through trading company shares or selling products online. Scammers collect personal information, such as name, email, and phone number, claiming they will contact users within 24 hours. However, after submitting their details, victims receive no follow-up emails and no phone call. The scam is spread through Facebook and Instagram ads, targeting users in Chile, Colombia, Brazil, Peru, Costa Rica, Mexico, Salvador, and Ecuador. The campaign uses social engineering to encourage personal data submission

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 SMS SOURCES

Ensure that any unsolicited SMS messages come from legitimate sources. Be cautious of unknown numbers or suspicious shortcodes, especially when the message urges immediate action

USE OFFICIAL CHANNELS FOR REDEMPTIONS

Contact the company directly through official customer service channels to confirm any offers, promotions, or loyalty points before redeeming them. Avoid using links or phone numbers provided in the SMS

ENABLE TWO-FACTOR AUTHENTICATION (2FA)

Always enable two-factor authentication on accounts that support it, especially for financial and personal services. This adds an extra layer of security in case your credentials are compromised

MONITOR YOUR ACCOUNTS REGULARLY

Keep a close watch on bank statements, credit card transactions, and loyalty program accounts. Report any suspicious activity immediately to prevent further damage

BE CAUTIOUS WITH ADS ON SOCIAL MEDIA

Avoid clicking on suspicious ads on platforms like Facebook and Instagram, especially those promoting quick money-making schemes or investment opportunities

NEVER SHARE PERSONAL INFORMATION WITH UNSOLICITED SOURCES

Refrain from sharing personal details, such as your name, email, and phone number, with websites or platforms that you cannot verify as legitimate

RANSOMWARE & EXTORTION ACTIVITIES

February had a significant decrease of disclosures with only 23 companies published on DLS, 11 of them from Brazil and 3 from Chile. Although there was only 1 disclosure, Akira is still present in the LATAM ransomware landscape as in the last 3 months.
Although Arcus, KillSec and APT73 (aka Bashe) have also disclosed companies in the region, we point out that these are groups usually conduct extortion-only attacks even though they provide ransomware to their affiliates. Additionally, in comparison to Akira, they pose are low risk to the organizations

DISCLOSURES BY GROUP

BABUK_v2 new 9 attacks	CLOP 6 attacks + 500%	AFEPAY 5 attacks - 28%	AKIRA 4 attacks - 60%
ARCUS new 4 attacks	FUNKSEC 4 attacks - 33%	RANSOMHUB 3 attacks	FOG new APOS_SECURITY ELDORADO 2 attacks

Ransom incidents

DATA LEAK SITE DISCLOSURE BY COUNTRY

Brazil 21 incidents - 4%	Mexico 30 incidents + 33%
Colombia 5 incidents -54%	Peru 4 incidents + 300%
Argentina 4 incidents -20%	Dominican Republic 2 incidents

LATAM INCIDENTS AND THREATS HIGHLIGHTS

Key Regional Highlights with a brief description:

01	Group-IB's identified a Malspam campaign disseminating Grandoreiro	Group-IB's threat intelligence team learned about a Malspam campaign aimed at stealing sensitive data from Spanish and Colombian Windows users by infecting them with a Grandoreiro banking trojan. The emails impersonated companies such as Endesa, Mercadona, Naturgy, Binance and Mapfre. The infection process started once a victim downloaded a malicious ZIP file available on cld[.]pt and executed the malware whose filename followed the pattern F{NUM}.{COMPANY}.xxx-A4-IDfecha{NUM}.zip
02	Group-IB's detected brute force campaign aimed to get unauthorized access to SMTP servers	Group-IB's specialists discovered several web open directories with Python scripts allegedly used to brute force email accounts to get unauthorized access to SMTP servers concerning Brazilian companies. One of the scripts named "*crack.py*" had an email address owned by the criminal which was used to test the the brute forced credentials as well as the SMTP servers. Based on logs, the criminal allegedly compromised 154 credentials

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:

LNK Files

Banking trojans targeting EU and LATAM region have a multi-staged infection chain which often begins with the download of malicious files available on a legitimate cloud services such cld[.]pt and MediaFire

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

Social Engineering

Never download files such as EXE, MSI, ISO, LNK and ZIP even if the email was sent by a known source. Also, always check the filename. Malicious files may have double extensions such as “.exe.pdf”

Enable 2FA

Always enable 2FA on email accounts and, if possible, avoid SMS and email as 2FA. Prefer to use authenticators or hardware authentication such as Yubikey

Password Policy

To not use easy and obvious passwords such as Mudar@123 or John2025; avoid repeating the last 3 passwords; set up a long and complex password by using mobile or desktop password managers

Brute Force

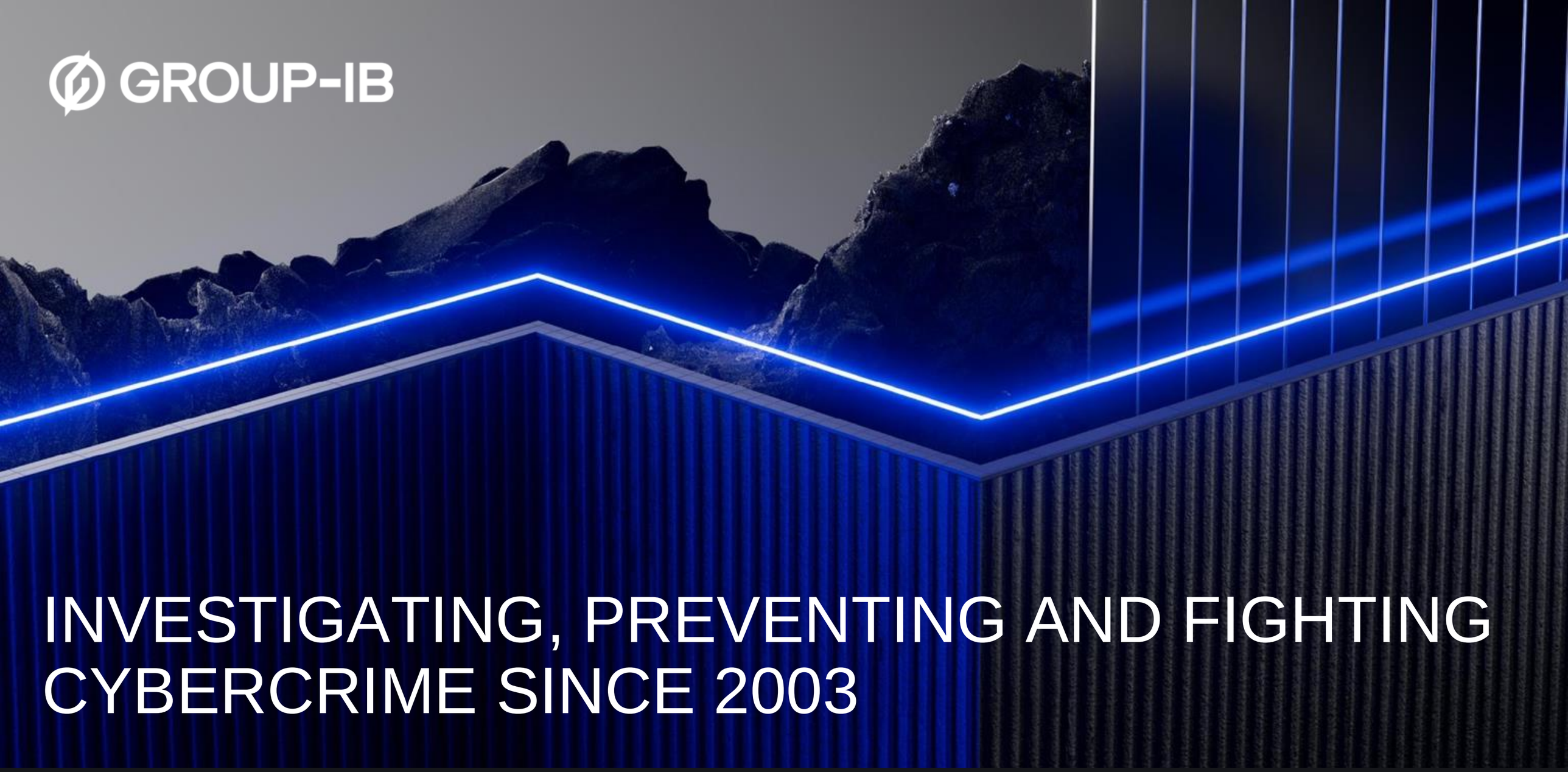
Set the maximum number of login attempts on the server. This way, you can mitigate brute force attacks. Also, make 2FA the default for all users

SCAM CASE OF THE MONTH:

Technologies · March 27, 2025

Navigating Cybercrime Currents in Latin America: Strengthening the Region's Defenses

LEARN MORE



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