January 2025

Latin 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 has uncovered a wave of loan scams in Brazil, where fraudsters use ads with public figures to impersonate banks and financial institutions

Group-IB's threat intelligence team recently attributed a Telegram shop to a threat actor who was previously active as an access broker in the underground forums XSS and RAMP

GLOBAL TRENDS

GROUP-IB

Global trends with a brief description:

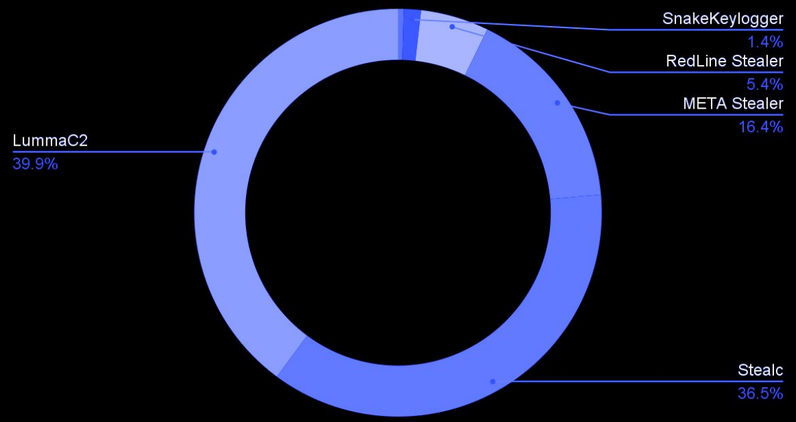
01	Halcyon published the blog about encryption of the data in Amazon S3 buckets	The blog post "Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C" by Halcyon details a novel ransomware campaign where the threat actor, dubbed Codefinger, uses compromised AWS credentials to encrypt data in Amazon S3 buckets via Server-Side Encryption with Customer Provided Keys (SSE-C). This method renders the data irrecoverable without the attacker's encryption key, as AWS does not store these keys, and CloudTrail logs only an HMAC insufficient for decryption.
02	Unveiling OtterCookie: A North Korea-Linked Attack Campaign Targeting Japan	The NTT Security Technical Blog post "Contagious Interview and the Newly Identified Malware OtterCookie" discusses a North Korea-linked attack campaign, "Contagious Interview," which employs a newly identified malware named "OtterCookie." This malware uses Socket.IO to receive remote commands, enabling actions such as executing shell commands, stealing device information, and extracting cryptocurrency wallet keys, with reported cases in Japan emphasizing the need for vigilance.

STATISTICS. **COMPROMISED DATA**

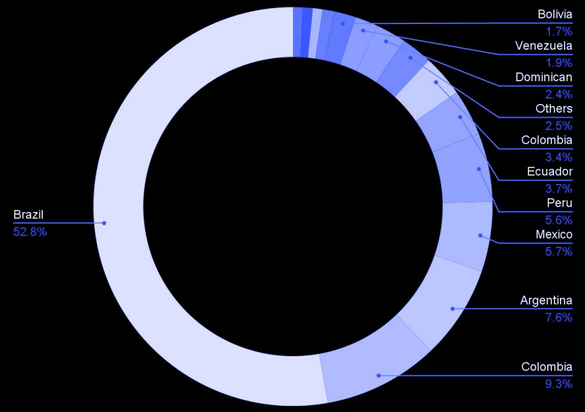
Stealer plays an import role in the cybercrime supply chain as the data stolen from the computer infected by this type of malware can lead to incident of higher impact such as ransomware, extortion and espionage. Valid accounts, that is, credentials exfiltrated by stealers are commonly used by threat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

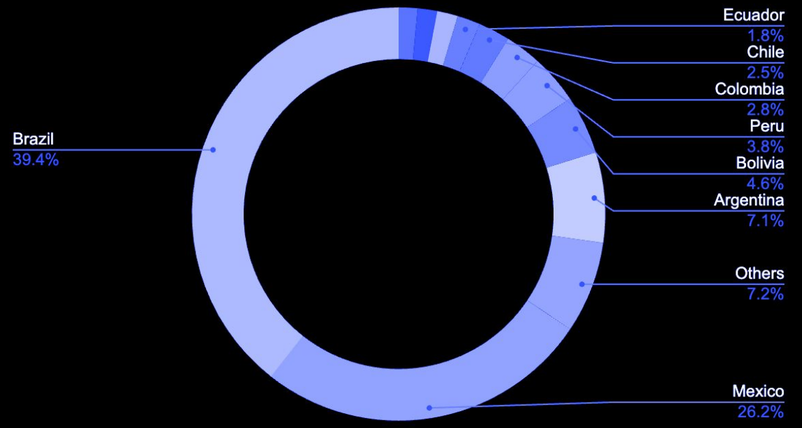
Compromised hosts by malware



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 wave of fake loan scams in Brazil, where fraudsters use deceptive ads featuring public figures to impersonate banks and financial institutions.	Group-IB discovered a new scam in Brazil where scammers use fake Facebook ads to trick people. These ads show pictures of famous people to make them look real and promise easy loans. When someone clicks the ad, they are taken to a fake chat page that looks professional. There, they are asked to share personal details, such as their CPF (Cadastro de Pessoa Física), under the pretense of applying for a loan, but the true intention is to unlawfully obtain their personal information.
02	Group-IB CERT has detected a phishing scheme using SMS campaigns targeting Colombian banks and telecommunications services.	Group-IB has detected a new fraudulent scheme that starts with an SMS targeting users in Colombia. The message offers a 50% discount on mobile services and contains a shortened link that leads to a fake payment page mimicking a well-known mobile operator. The page asks for the phone number and service type, accepting only specific numbers and displaying fake billing information. It then prompts users to make payments through various platforms, with the interface adapted to look like online banking services and popular local payment systems in order to steal login credentials and two-factor authentication details.

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:

BEWARE OF FAKE ADS

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

AVOID SHARING PERSONAL INFORMATION

Never provide sensitive personal information, like your ID number or banking details, on websites or chat pages that seem suspicious or unfamiliar

VERIFY THE LEGITIMACY OF LOAN OFFERS

Before applying for loans or any financial services, verify the legitimacy of the company by visiting their official website or contacting them through official channels

VERIFY SMS MESSAGES

Always double-check the authenticity of SMS messages offering deals or discounts. If in doubt, contact the company directly using known communication channels

USE SECURE PAYMENT METHODS

Only use trusted and secure payment methods when making online transactions. Avoid entering sensitive information on unfamiliar or suspicious websites

ENABLE TWO-FACTOR AUTHENTICATION

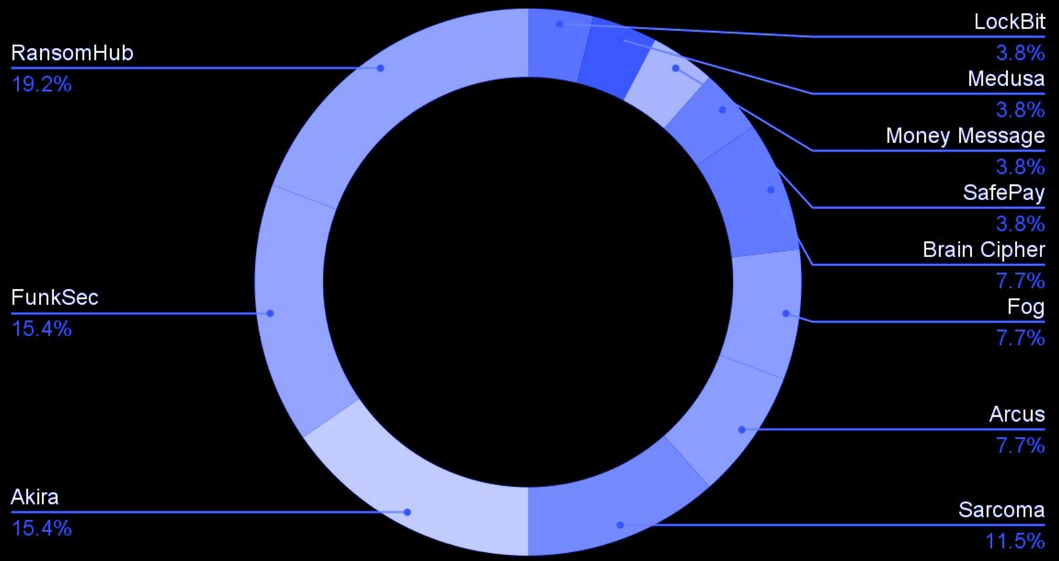
Enable two-factor authentication (2FA) on your accounts, especially for banking or payment platforms, to add an extra layer of security

STATISTICS. **ATTACKS**

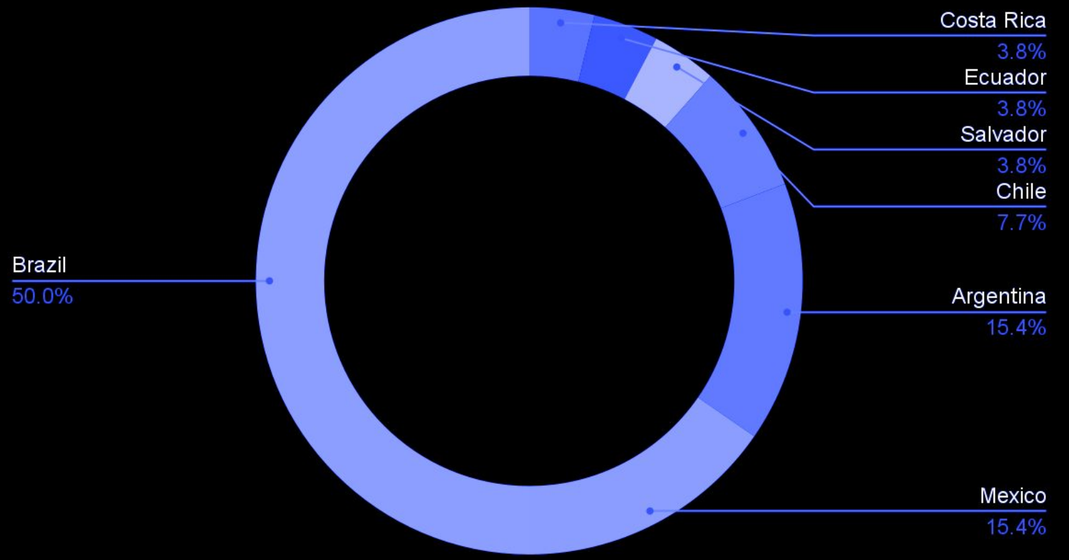
RANSOMWARE ACTIVITIES

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 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 identifies the new Android Remote Access Trojan BT-MOB promoted by GhostSpy on Telegram.	A new Android Remote Access Trojan named **BT-MOB** has been advertised on December 14th, 2024 in GhostSpy's Telegram group. According to the advertisement written in Portuguese, BT-MOB works on Android 7 to 13 and is able to bypass Play Protect. As most Android RATs, in order to have full remote control of the infected mobile device, BT-MOB requires accessibility to be enabled. So far, Group-IB did not detect any malicious campaign disseminating this malware.
02	Credit card theft through web application exploitation.	Group-IB's threat intelligence team recently attributed a Telegram shop to a threat actor who was previously active as an access broker in the underground forums XSS and RAMP. After its accounts were banned in these forums, it started advertising on Facebook and Telegram credit cards allegedly stolen by using the same approach it used to gain initial access to companies: web application exploitation.

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 BT-MOB 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

WEB APP EXPLOITATION

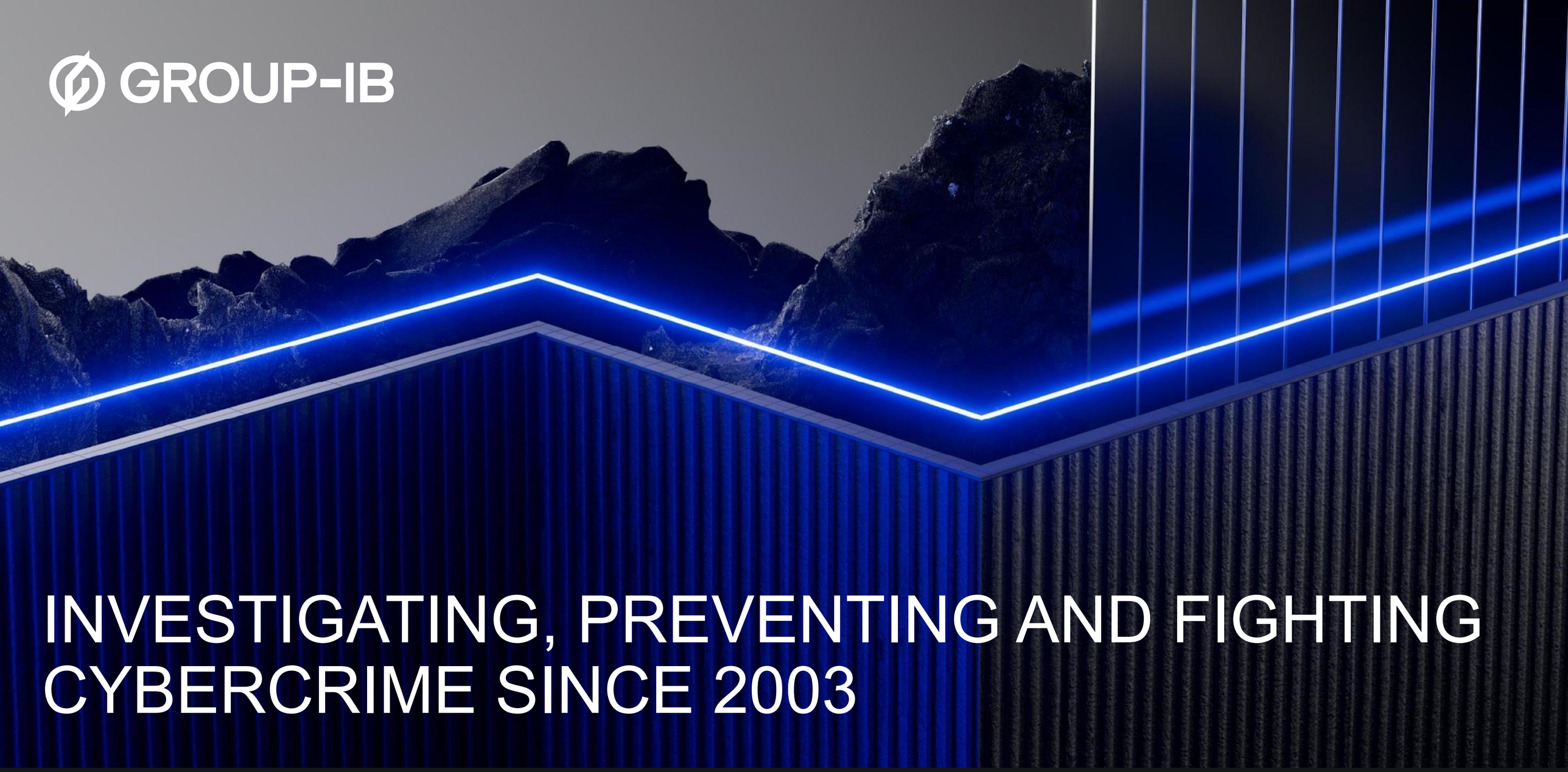
Criminals engaged into fraud may eventually exploit vulnerabilities on e-commerces and online shops. To mitigate this type of threat, it's important to be aware of OWASP Top Ten and OWASP API Security Top 10.

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.



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