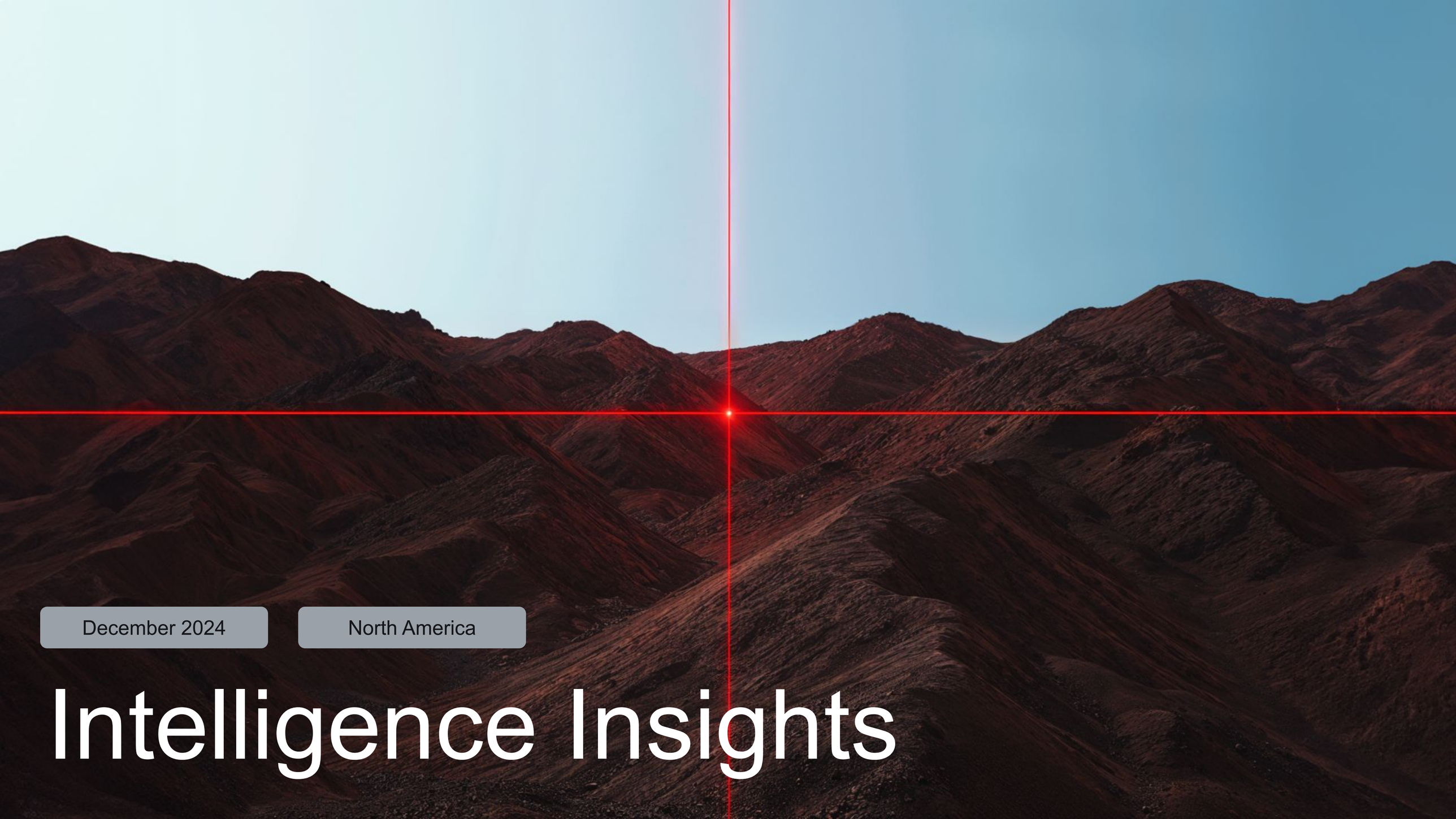


December 2024

North America

Intelligence Insights

INTRODUCTION

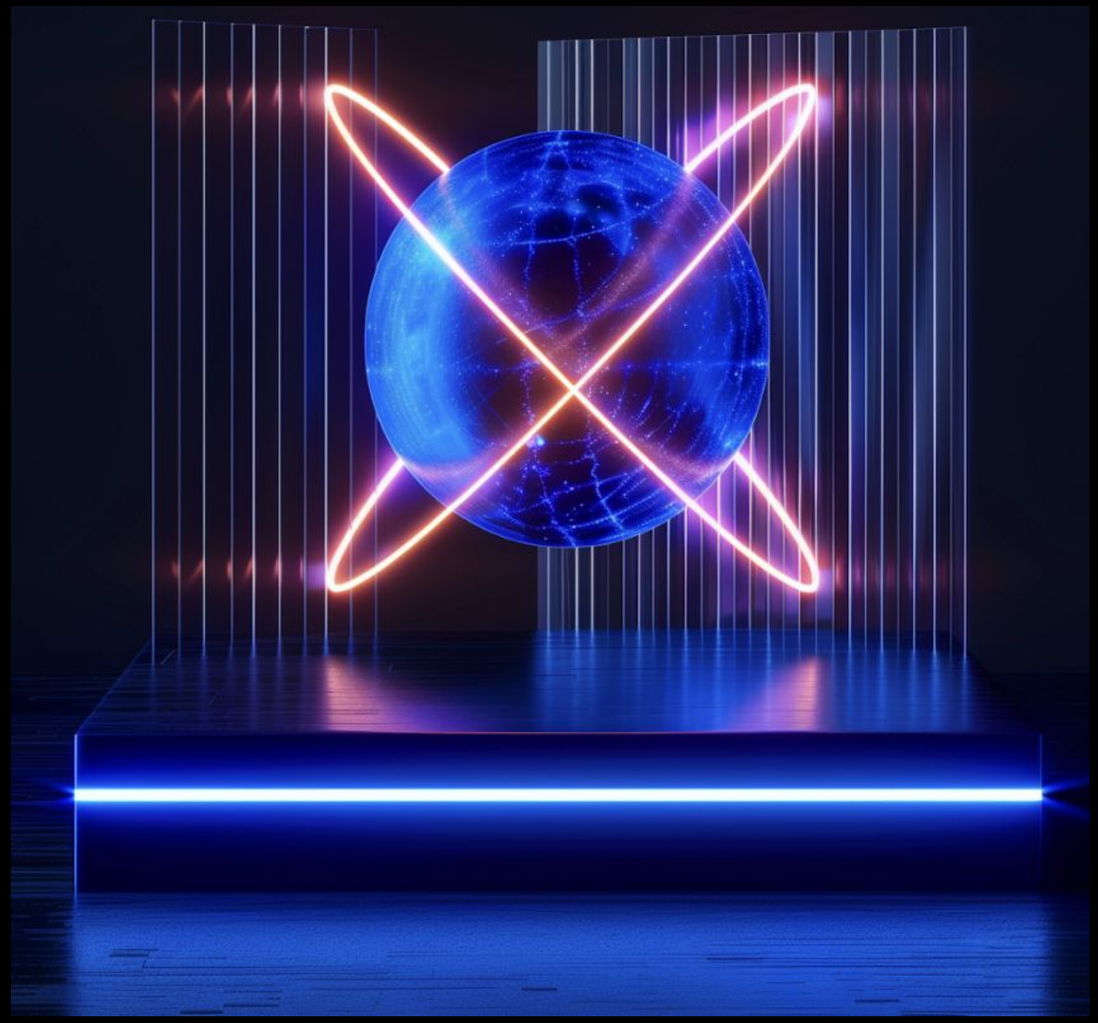
This report contains information on the most significant cybersecurity events that occurred worldwide and in North America over the last month

2 most striking events of the month:

- **Group-IB CERT has identified a growing trend in the use of Blob URIs in phishing attacks across the Americas**

- **Group-IB detected at least 9 incidents against clinics and hospitals in the US and Canada authored by different ransomware groups including RansomHub, Rhysida and Lynx.**

Group-IB CERT has observed a rising use of IPFS (InterPlanetary File System) in phishing campaigns



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.

REGIONAL TRENDS. CERT INSIGHTS

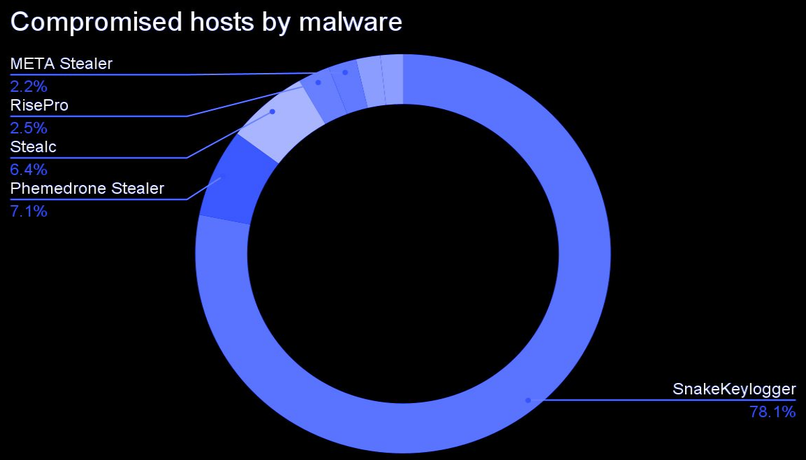
Key Regional Trends with a brief description:

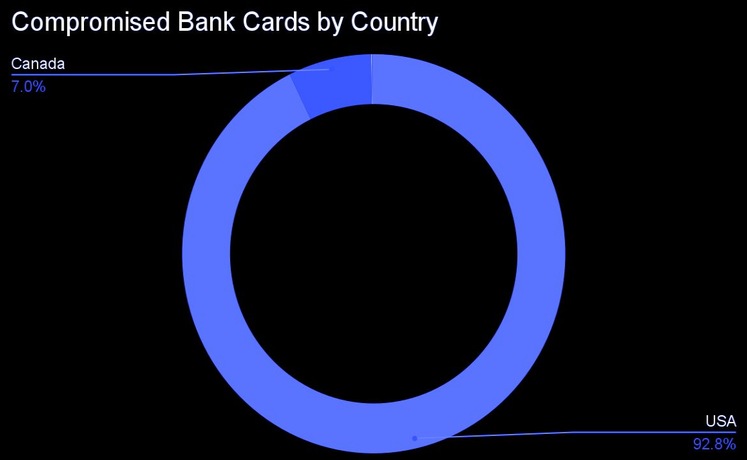
01	Group-IB CERT has identified a growing trend in the use of Blob URIs in phishing attacks across the Americas	This technique enables attackers to deliver malicious content directly within the browser, bypassing external server calls and evading traditional URL filtering and scanning tools. As a result, the process of detecting and blocking such phishing resources becomes significantly more complex, posing new challenges for cybersecurity efforts in the region
02	Group-IB CERT has observed a rising use of IPFS (InterPlanetary File System) in phishing campaigns	This decentralized peer-to-peer file-sharing protocol allows threat actors to host phishing pages on a distributed network, making them harder to detect and take down through traditional methods. The use of IPFS highlights a shift towards more resilient hosting techniques, requiring updated detection rules and enhanced monitoring to identify and counter such malicious activities

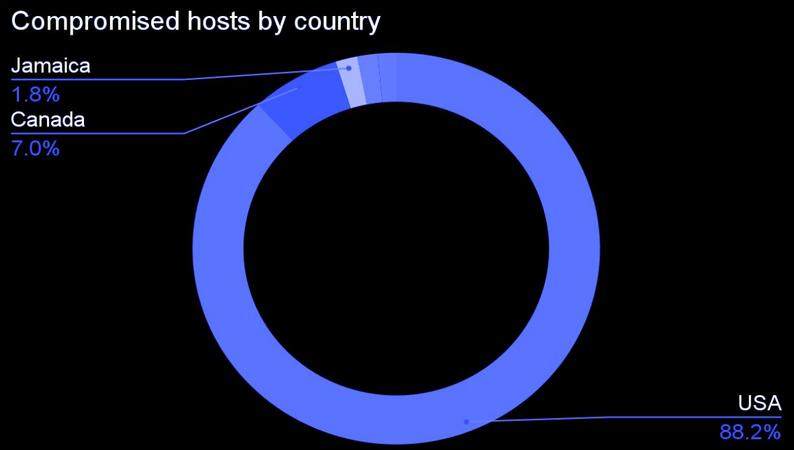
STATISTICS. **COMPROMISED DATA**

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.







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:

ENHANCE SECURITY AWARENESS

Provide regular training for employees and stakeholders to recognize and respond to phishing attempts, social engineering tactics, and other evolving threats

UTILIZE ADVANCED SECURITY TOOLS

Adopt cutting-edge security solutions, such as AI-driven threat detection and decentralized monitoring systems, to combat sophisticated attack methods

REGULARLY AUDIT AND UPDATES SYSTEMS

Conduct frequent security audits to identify vulnerabilities and implement updates or patches promptly to mitigate risks

IMPROVE MFA DEPLOYMENT

Encourage the use of multi-factor authentication across all accounts, especially for systems susceptible to phishing. This adds an additional layer of protection that can mitigate the impact of stolen credentials

UPDATE DIGITAL RISK PROTECTION MEASURES

Ensure that security teams regularly update brand monitoring and protection systems to cover new phishing tactics and methods

IMPLEMENT URL AND FILE-TYPE FILTERING

Strengthen your security infrastructure by using URL filtering solutions capable of detecting and blocking suspicious domains, especially those leveraging new attack vectors like Blob URIs or IPFS gateways

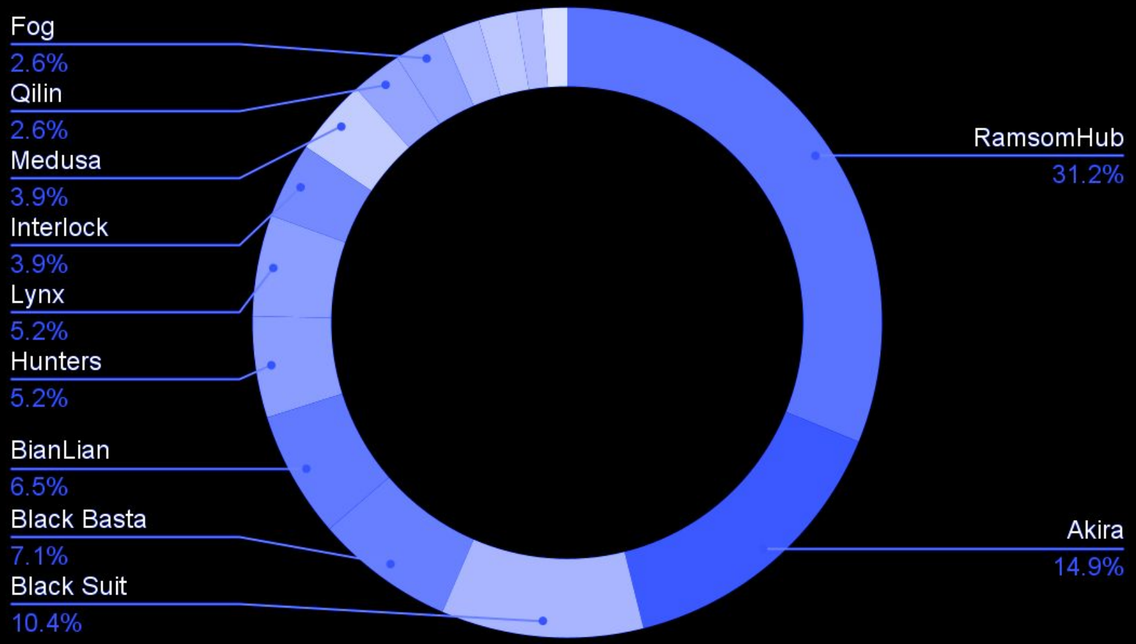
STATISTICS. **ATTACKS**
RANSOMWARE ACTIVITIES

GROUP-IB

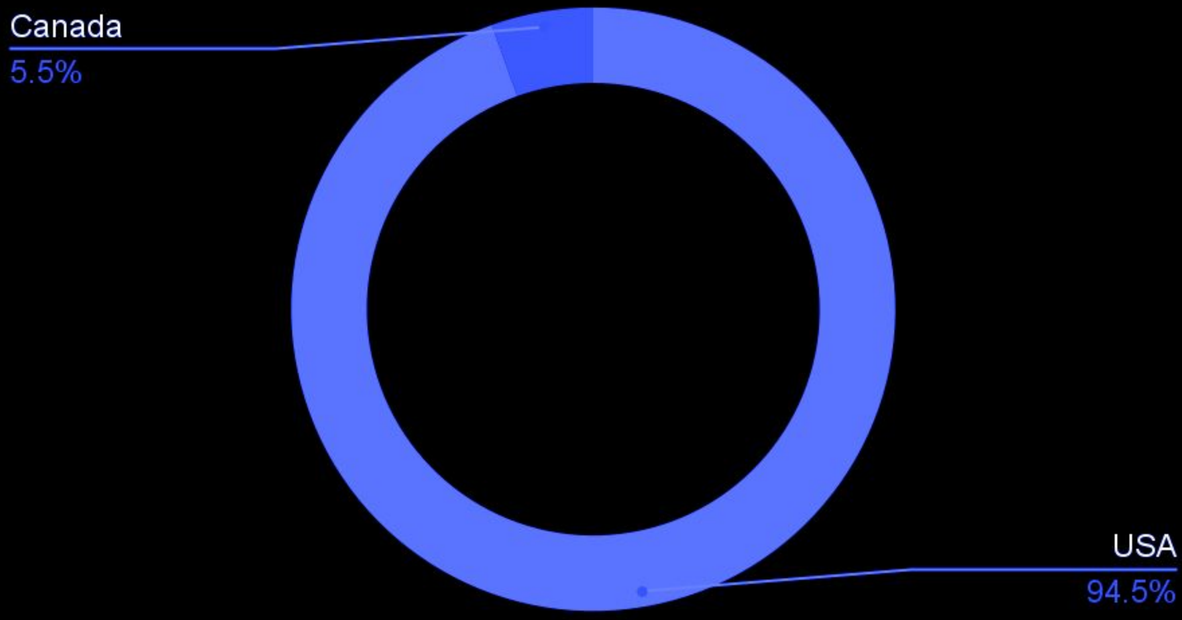
As in the LATAM region, RansomHub's affiliates authored most of the attacks against companies in the US and Canada, followed by the Conti-linked groups Akira, Black Suit, Black Basta.

According to a US congress' bill from 2024, those groups as well as Play, INC, Cl0p and some others constitute hostile foreign cyber actors due to the high risk these ransomware and extortion operations pose to US companies and critical infrastructure.

Companies disclosed on ransomware groups' DLS



DLS disclosure by country



NORTH AMERICA INCIDENTS AND THREATS HIGHLIGHTS

GROUP-IB

Key Regional Trends with a brief description:

01 Ransomware attacks against healthcare companies in the US and Canada.

Attacks against healthcare companies have been increasing every year since 2022. As the recent Law Enforcement operations such as Operation Cronos and EndGame as well as the actions taken by the US congress have affected the ransomware ecosystem, ransomware operators and affiliates have been targeting critical infrastructure including the healthcare industry as they are more likely to pay ransom, according to criminals.

Group-IB detected at least 9 incidents against clinics and hospitals in the US and Canada authored by different ransomware groups including RansomHub, Rhysida and Lynx.

Additionally, this year, Qilin has publicly stated on the group's DLS which has been targeting healthcare companies in the US.

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:

ENHANCE SECURITY AWARENESS TRAINING

Regularly educate employees on recognizing phishing attempts, social engineering tactics, and safe online practices

STRENGTHEN IT INFRASTRUCTURE

Ensure all systems are updated with the latest security patches and employ multi-factor authentication (MFA) to enhance access controls

CONDUCT REGULAR SECURITY AUDITS

Perform periodic assessments of your IT environment to identify and mitigate potential vulnerabilities

DEPLOY ADVANCED THREAT DETECTION TOOLS

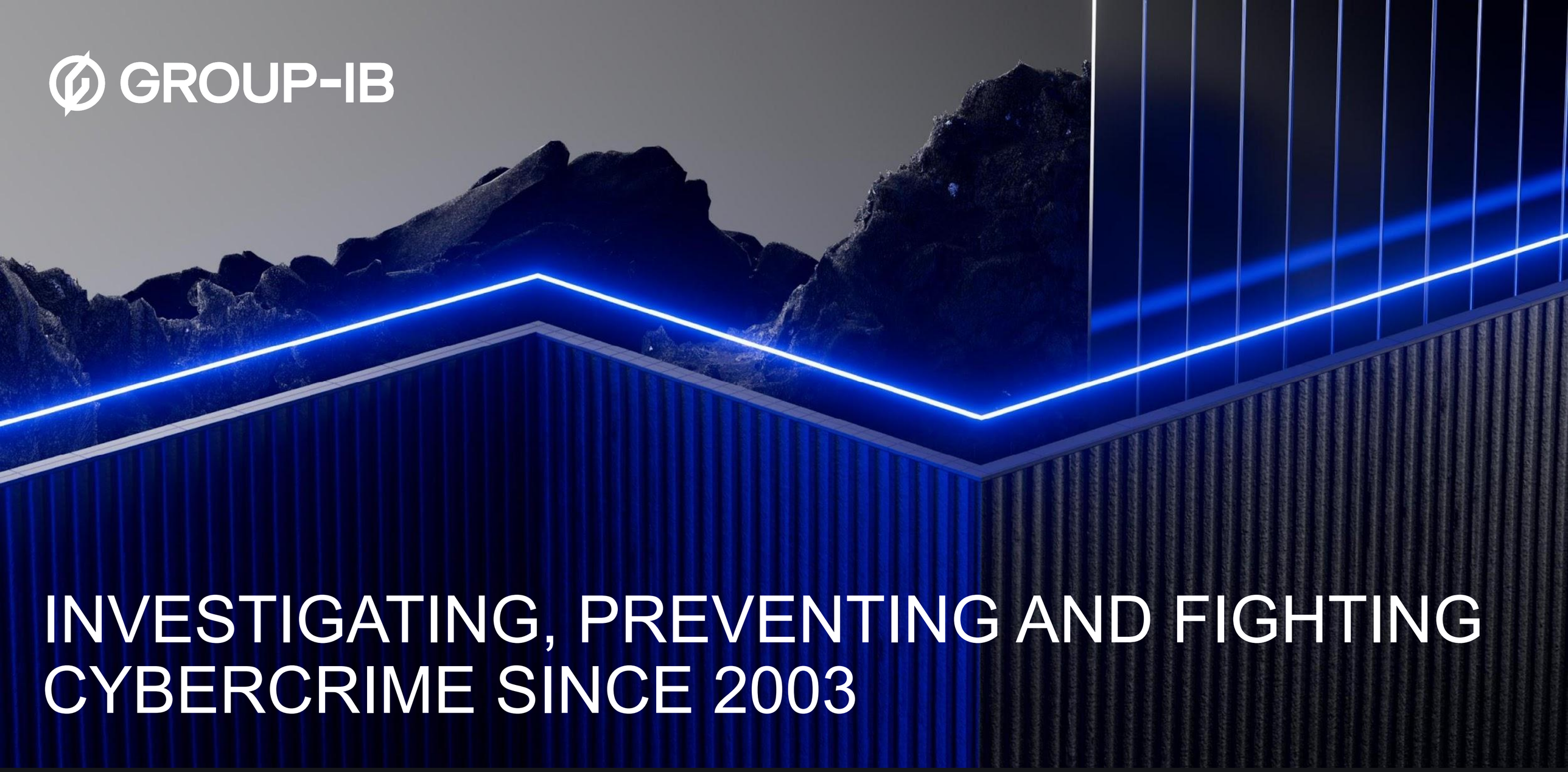
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time

ESTABLISH INCIDENT RESPONSE PROTOCOLS

Develop and regularly update an incident response plan to quickly address and mitigate the impact of security breaches

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