GROUP-IB

NORTH AMERICA

INTELLIGENCE INSIGHTS

APRIL 2025

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

Information collected by Group-IB suggests that VanHelsing is managed by former affiliates previously involved with at least 3 ransomware groups

Group-IB CERT has observed a surge in tax-season phishing attacks across the United States, with threat actors leveraging AI-generated voice and video deepfakes

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

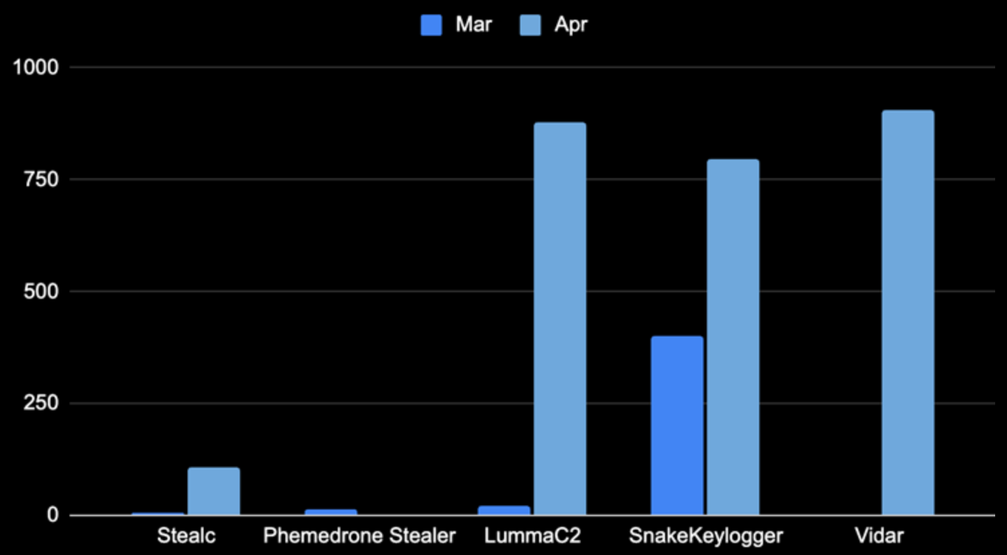
Group-IB, in collaboration with the Royal Thai Police and the Singapore Police Force, successfully apprehended a cybercriminal responsible for over 90 data breaches worldwide. The individual, operating under aliases such as ALTDOS, DESORDEN, GHOSTR, and 0mid16B, targeted large private companies across 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

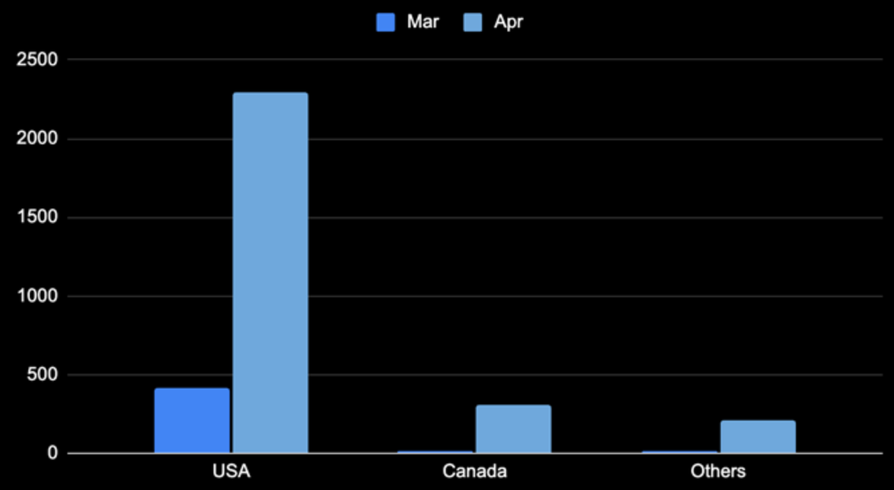
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational 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.

↑ growth in compromised activities

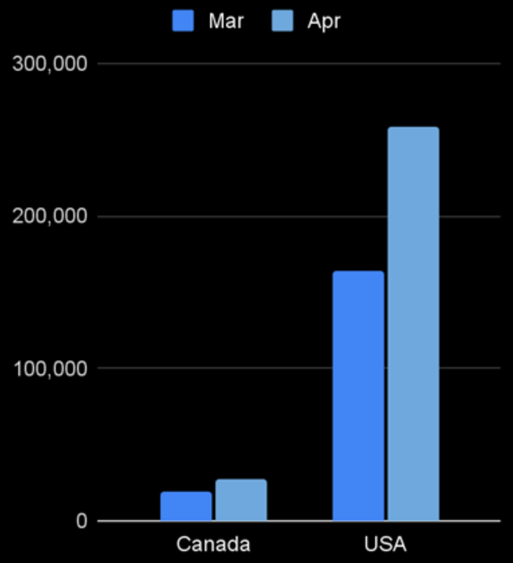
COMPROMISED HOSTS BY MALWARE



COMPROMISED HOSTS BY COUNTRY



COMPROMISED BANK CARDS BY COUNTRY



REGIONAL TRENDS. CERT INSIGHTS

Key Regional Trends with a brief description:

01 Group-IB CERT has uncovered a phishing campaign exploiting compromised corporate mailing systems to deliver fake crypto wallet recovery phrases. The goal is to steal victims' digital assets by tricking them into using attacker-controlled wallet credentials.

Threat actors gain access to corporate email marketing platforms and use them to send phishing messages that appear trustworthy. These emails urge recipients to migrate or update their crypto wallets using a provided recovery phrase - which actually grants access to wallets controlled by the attackers. Once used, victims unknowingly transfer their assets directly to the criminals. The campaign targets users across sectors, abusing legitimate infrastructure to maximize reach and bypass security filters.

02 Group-IB CERT has observed a surge in tax-season phishing attacks across the United States, with threat actors leveraging AI-generated voice and video deepfakes to impersonate tax professionals, the IRS, and even family members.

In the U.S., cybercriminals are increasingly exploiting generative AI to create convincing voice phishing (vishing) attacks during tax season. Using previously stolen personal data, attackers imitate accountants and IRS representatives to extract sensitive financial information from victims. In addition to voice scams, the campaigns include highly realistic phishing emails, fake websites using SEO poisoning (e.g., "Trump tax refund"), and mobile-first SMS attacks that redirect to credential-stealing pages or malicious apps.

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:

WALLET RECOVERY PHRASE AWARENESS

Never enter a wallet recovery phrase from an email, text, or website prompt. Always access crypto wallets and services directly through official apps or websites

DOUBLE-CHECKING URGENT REQUESTS

If an email or call demands urgent action - like creating an IRS account or updating wallet credentials - verify through official channels before responding

CYBER HYGIENE AND AWARENESS TRAINING

Conduct regular training sessions to teach how to recognize fake websites, impersonation attempts, malicious apps, and AI-generated content

INCIDENT RESPONSE READINESS

Establish a clear response plan for phishing attacks and data breaches. Include customer notification procedures, internal coordination, and digital forensics

CHECK EMAIL ADDRESSES

Always verify the sender’s email address before interacting with any email requests. Be cautious of emails with misspelled domain names or addresses that don’t match the expected organization’s domain

ENFORCE MULTIFACTOR AUTHENTICATION

Require MFA for all accounts that handle sensitive information, including email, banking, and cloud-based services. This additional step makes it significantly harder for attackers to gain unauthorized access

RANSOMWARE & EXTORTION ACTIVITIES

GROUP-IB

This month we have noticed a significant decrease in disclosures on Cactus group's DLS from 33 in February to only 7 in March.

Qilin remains very active compared to the amount of disclosures made by the group from July 2024 to January 2025.

↑%

Ransom incidents

DISCLOSURES BY GROUP

CLOP 173 attacks + 394%	INC_BLOCK new 121 attacks	RANSOMHUB 59 attacks + 195%	AKIRA 33 attacks - 17%
QILIN 29 attacks + 141%	PLAY 27 attacks + 145%	BABUK_v2 29 attacks + 141%	CACTUS new 7 attacks

DATA LEAK SITE DISCLOSURE BY COUNTRY

UNITED STATES OF AMERICA 462 + 54%
CANADA 60 + 114%

NORTH AMERICA INCIDENTS AND THREATS HIGHLIGHTS

Key Regional Trends with a brief description:

01	Group-IB's insights on Cactus and Rhysida	Since information from Black Basta's Matrix server has been leaked around February 20, Group-IB's threat intelligence team has observed an increase in the activity regarding Cactus ransomware group. Although it is not clear yet, information collected by Group-IB so far suggests that threat actors who previously worked with Black Basta are now divided into at least 2 ransomware operations: Cactus and Rhysida
02	VanHelsing new RaaS operation	On March 7, a new RaaS partnership program named VanHelsing was advertised on RAMP forum. The group's affiliates have already disclosed 8 companies from different countries on its DLS, including an organization from the US. Group-IB assesses with high confidence based on information collected so far that VanHelsing is managed by former affiliates who previously worked to at least 3 ransomware groups

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:

EXTORTION METHODS

Criminals may eventually contact executives of organizations, as well as IT teams, by different means in order to extort and negotiate ransom. Don't respond to criminals before analyzing the situation.

ESTABLISH PROCESSES

It is really important to establish a process in the organization in order to reduces the chances of employees being deceived by social engineering campaigns such as *vishing* and postal mail scam.

NEVER SHARE INFORMATION

Never share information with anyone, especially those related to systems' authentication such as OTP and 2FA codes, RMM password etc. Also, never share information about yourself and the organization (Opsec).

PUBLIC-FACING HOSTS

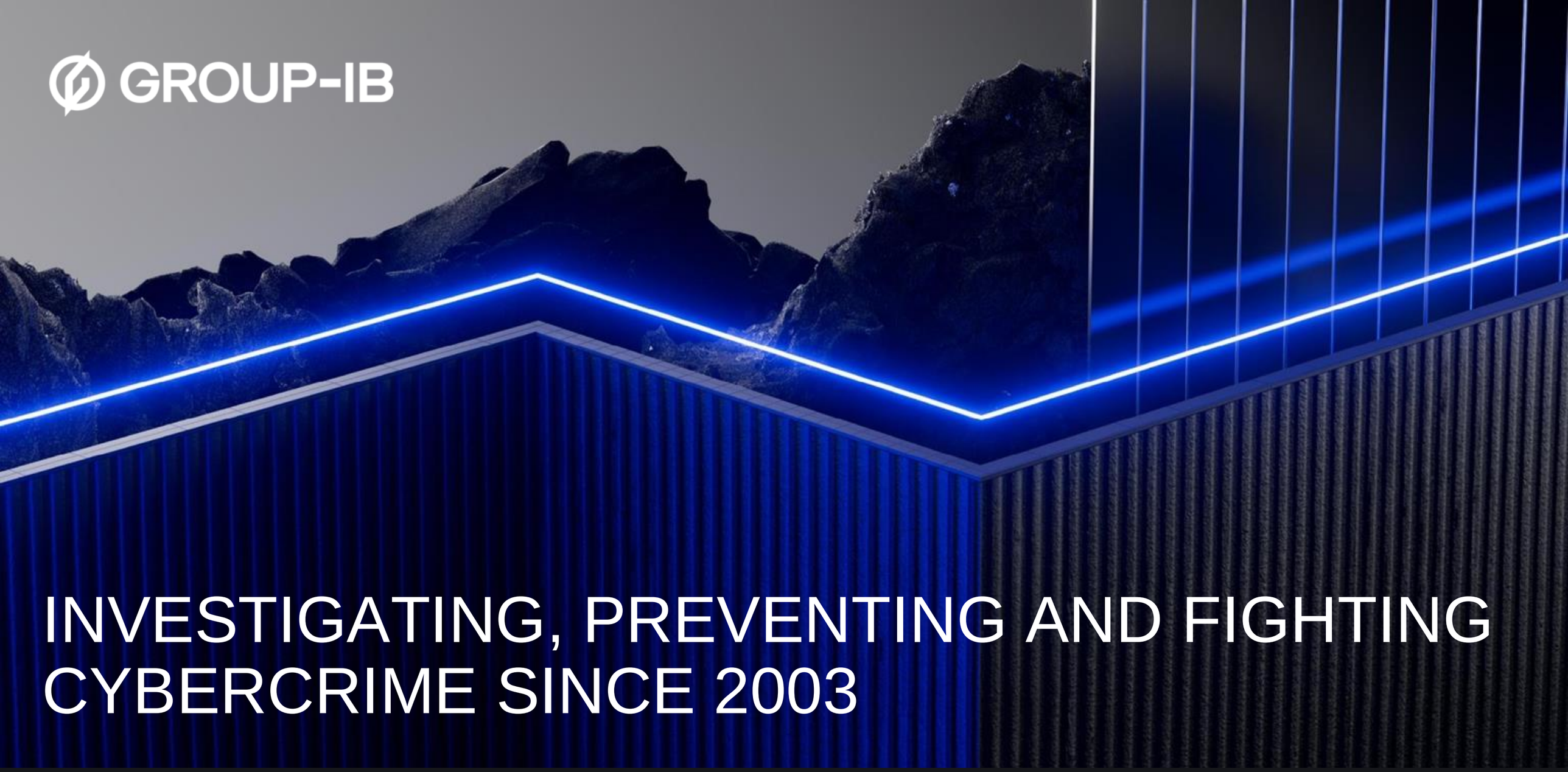
It is important to have visibility of which of the organization's assets are publicly accessible from the Internet, as well as the security flaws to which hosts may be vulnerable.

DEPLOY ADVANCED THREAT DETECTION TOOLS

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

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