

For Data from February 2026

ANZ Newsletter

Actionable threat intelligence and sharp insights into the threats, attack trends and adversaries shaping the Australia New Zealand cybersecurity landscape.



WHY THIS REPORT MATTERS

The Asia-Pacific (APAC) region continues to experience **rapid digital growth**, making it a prime target for cybercriminals, organised threat groups and nation-state-aligned actors.

This newsletter helps you:

- Understand **how cyber threats are evolving across ANZ and the globe**
- Identify **which industries and geographies are most targeted**
- Anticipate **new attack techniques and criminal business models**
- Translate intelligence into **practical defensive actions**
- Whether you are responsible for **security strategy, risk management, fraud prevention, or regulatory compliance**, this report provides clarity in a fast-changing threat landscape.

Middle East Regional Conflict

Insights from Group-IB covering the period 28 Feb – 04 March 2026

01

Group-IB Reports

Group-IB continues to attribute Middle East Tension tags to reports that are relevant to the conflict. A complete timeline list of all cyber-threats in order of date published is available [here](#).

02

Group-IB Conflict Watch Updates

Published by the Analyst team overnight where possible [here](#).

03

Attributed Threat Actors

The attributed TAs that are attributed to this conflict and are active in the time period 27 Feb-05 March 2026 are: [Evil Markhors](#), [Keymous](#), [Fatimion Cyber Team](#), [313 Team](#), [DarkStorm Team](#), [Cyber Resistance Axis](#), [FaD Team](#), [THE GARUDA EYE](#), [RealLulzSec](#), [Moroccan Black Cyber Army](#), [DieNet](#) & [SYLHET GANG](#).

These attacks predominantly include DDoS, with limited numbers of claimed data breaches and access to systems.

04

Notable Cyber Incidents

Reported by Group-IB 5th March 2026 AEST time

- Iran remaining largely offline for over 100 hours, with connectivity dropping to approximately 1% of normal levels, severely limiting visibility into domestic cyber activity.
- Ongoing credibility issues surrounding hacktivist claims, particularly those attributed to the pro-Iranian group Handala.
- Emergence of new phishing campaigns impersonating UAE government authorities.
- Evidence suggesting targeted reconnaissance against internet-connected surveillance cameras potentially linked to Iranian operational doctrine.
- Attempts to recruit foreign collaborators for Iranian intelligence activities through online platforms.
- Exposure of sensitive infrastructure belonging to the Iranian-linked MuddyWater APT group, potentially impacting their operations.



Middle East Regional Conflict

Insights from Group-IB covering the period 28 Feb – 05 March 2026

04

Notable Cyber Incidents

Reported by Group-IB 4th March 2026 (AEST Time)

- UAE Banking Disruptions Potentially Linked to Regional Cloud Issues
- Evacuation-from-UAE Scam Narrative Detected- ~70% of detected activity originated from Facebook Ad Library entries, suggesting active use of paid promotion to increase reach and perceived legitimacy
- Use of Telegram bots/channels
- Forms collecting passport data
- Hacktivist Expansion and Increased Attention to OT/SCADA
- Shift toward OT, SCADA, and manufacturing targets

Reported by Group-IB 2nd March 2026 (AEST Time)

- [APT IRAN](#) claiming unauthorized access to internal systems of Jordan Silos Company
- [Cyber Islamic Resistance](#) claiming compromise of 130+ remote control systems across multiple countries and naming Shlomi Control Applications Ltd (DDC) as an Israeli infrastructure-related target
- Fraud Telemetry: Spike from Syria + High-Risk App Signals
- 100–150 suspicious devices (depending on severity thresholds), associated with hosting usage and fraudulent apps distribution/behavior
- 20+ unique VPN apps from high-risk geohash areas correlated with hosting + fraudulent app activity
- Dark web chatter remains quiet and consists of generic discussions
- Fake Red Alert Android applications were observed likely targeting individuals in Israel to exfiltrate data
- TDRA cautioning users of sharing personal data and UAE PASS-codes with external parties.

- Misinformation and disinformation is prominent, with a message perpetrated to originate from US CYBERCOM/CENTCOM, advising US service members to disable location services from devices
- Amazon Web Services experienced disruptions and outages in the United Arab Emirates and Bahrain.
- GPS jamming and spoofing activity continues to be present across the region, affecting aviation and maritime operations.

Reported by Group-IB 1st March (AEST time)

- Iran remains mostly offline
- Fraud and Social Engineering Activity Emerging
- Global Hacktivist Activity Surge
- Handala Hack Team claimed compromise of a Jordanian Oil & Gas company system
- Evil Markhors, a self-proclaimed Pakistani hacktivist group reported attacks targeting banking organizations including Riyadh Bank and Israel Discount Bank.
- DieNet Telegram Channel, a channel associated with pro-Russian and pro-Iran cyber narratives claimed responsibility for an incident affecting Bahrain Airport online services and additional government-related targets in Bahrain and Qatar.

LOCAL INSIGHTS (Australia & New Zealand)

Local Insights from Group-IB with a brief description:

01

youX Leaked Database

Group-IB analysts have had further engagement with the threat actor to uncover additional details about the youX data breach incident, including any further activity, decisions, and details to share. The threat actor, Fulcrumsec, claims to have tens of terabytes of data that they are 'sifting' through and deciding what to leak on their DLS. Their most recent claim is to have breached the [Lexis Nexis](#) Legal and Professional database.

02

Booktopia Leaked Database

The Group-IB Threat Intelligence team identified a database sale from [Booktopia](#) Pty Ltd. by data broker actor [Telephone Hooliganism](#). Telephone Hooliganism operates as a dedicated data broker on BreachForums, exclusively focused on selling leaked databases and personal information datasets.

03

Forex Australia Leaked Database

The Group-IB Threat Intelligence team identified an alleged database leak from [Forex Australia](#) by threat actor [Kirby](#). Kirby was first seen in February 2026 and specializes in selling large-scale personal information databases, primarily targeting FOREX trading platforms and B2B companies across Australia, Spain, and the United States. All activity occurred within a 4-day window, with the user creating 4 database sale topics containing between 30,000 to 500,000 records each.



RANSOMWARE ACTIVITIES (Australia & New Zealand)

↓57.14%
From January 2026



10 ransomware incidents

Statistics regarding ransomware activities in February 2026:

- **Australia** remains out of the top 5 countries globally from February sitting in 13th place globally, down from 6th place in February 2026.
- New Zealand is well out of the top 10 targeted countries, sitting in 43rd place for February 2026. Lack of activity can be attributed to multiple reasons, and it is important for businesses with New Zealand connections to not become complacent.
- New Zealand’s most notable victim was the attack on [Sika Technology Limited](#) by [Play](#). Files were disclosed on their DLS.
- For Australia, the most notable incidents included ransomware attacks on [Distinctive Systems Ltd](#) by Qilin (a usual suspect), as well as the attack with [Lockbit](#) deploying ransomware on the [Aeromedical Society of Australasia](#).
- Although case-specific TTPs and IOCs may be restricted, IOCs of these actors are collected from previous incidents can be found on the Threat Intelligence Portal. We have linked them in this report.
- The MITRE ATT&CK used is **Data Encrypted for Impact**.

Most active threat actors (compared to the previous month)

CIOP 0 activities in February 11 activities in January	Play 2 activities	Space Bears 2 activities
Qilin 2 activity +100%	INCBlog 1 activity	Kairos 1 activities

Most targeted industries

Industrial Manufacturing

2 activities

Retail

1 activity

Healthcare

2 activities

Transportation

1 activity

DDoS AND HACKTIVISM (Australia & New Zealand)

Hacktivism is the use of hacking to promote political or social agendas. Usually hacktivist groups are low-skill hackers who perform DDoS, Defacement, and Data Breaches (mostly leverages compromised accounts) attacks.

In **Australia**, 6 Hacktivism incidents were recorded in January 2026.

The Group-IB Threat Intelligence team reported that the **TAZ-Pentest Alliance** claimed a successful attack on Aquacorp’s control systems in January. They have followed this up with further aqua infrastructure attacks with claimed access to an Australian wastewater [treatment plant](#) and an Australian [irrigation management system](#). The attacker claims access to pumps and sensors and claims to be able to manipulate readings and alarms without detection.

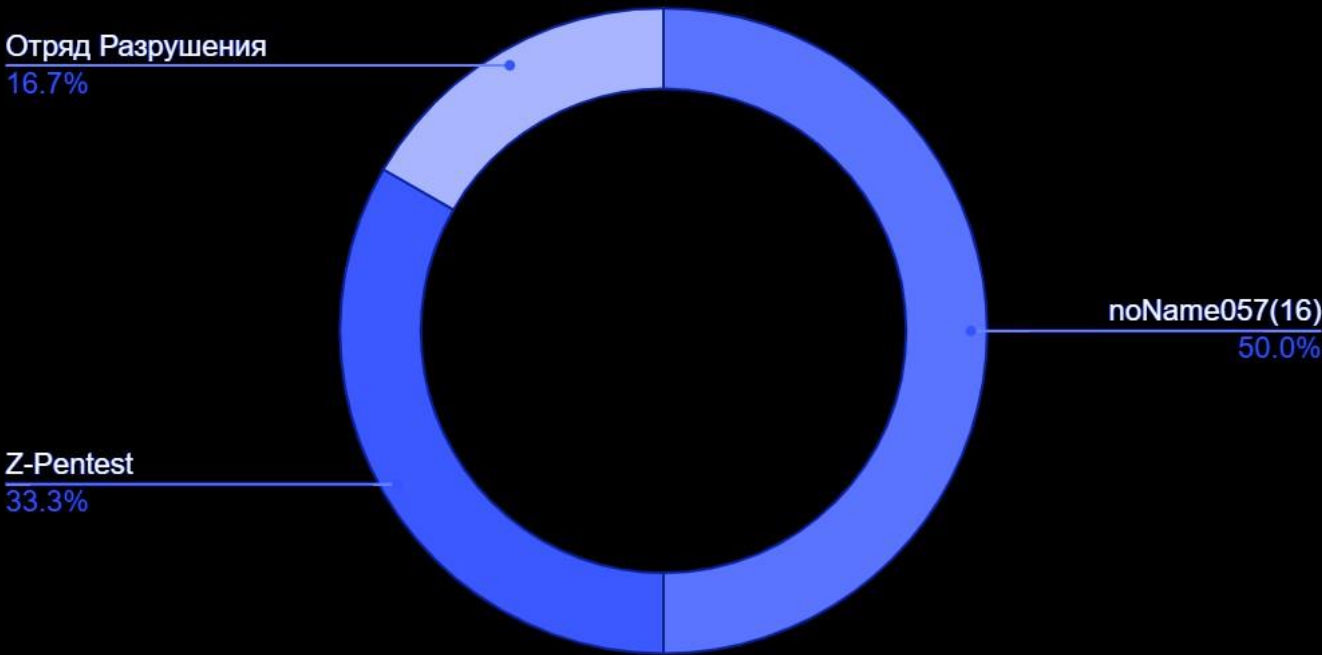
In December’s DRP report, Group-IB reported that this same group had gained unauthorized access to the pump control and tank monitoring system at the **Burnt Hut** facility in Australia.

NoName057(16) and “ 🚨 Отряд Разрушения ИнфраструктурыRU ~ 🚨 ”/ (Infrastructure Destruction Squad^{RU}) claimed attacks on the Australian Olympic Committee, the German Olympic Team, and an Australian wastewater treatment plant.

All three of these actors are using OT Access attacks involving unauthorized entry into operational technology (OT) environments, including industrial control systems (ICS), SCADA, and HMI interfaces.

No DDos or Hacktivism events were reported for New Zealand for February 2026.

DDOS and Hacktivism Activities - Australia & New Zealand, per group, February 2026



COMPROMISED ACCOUNTS (Australia & New Zealand)

↓ 60.23%

From January 2026

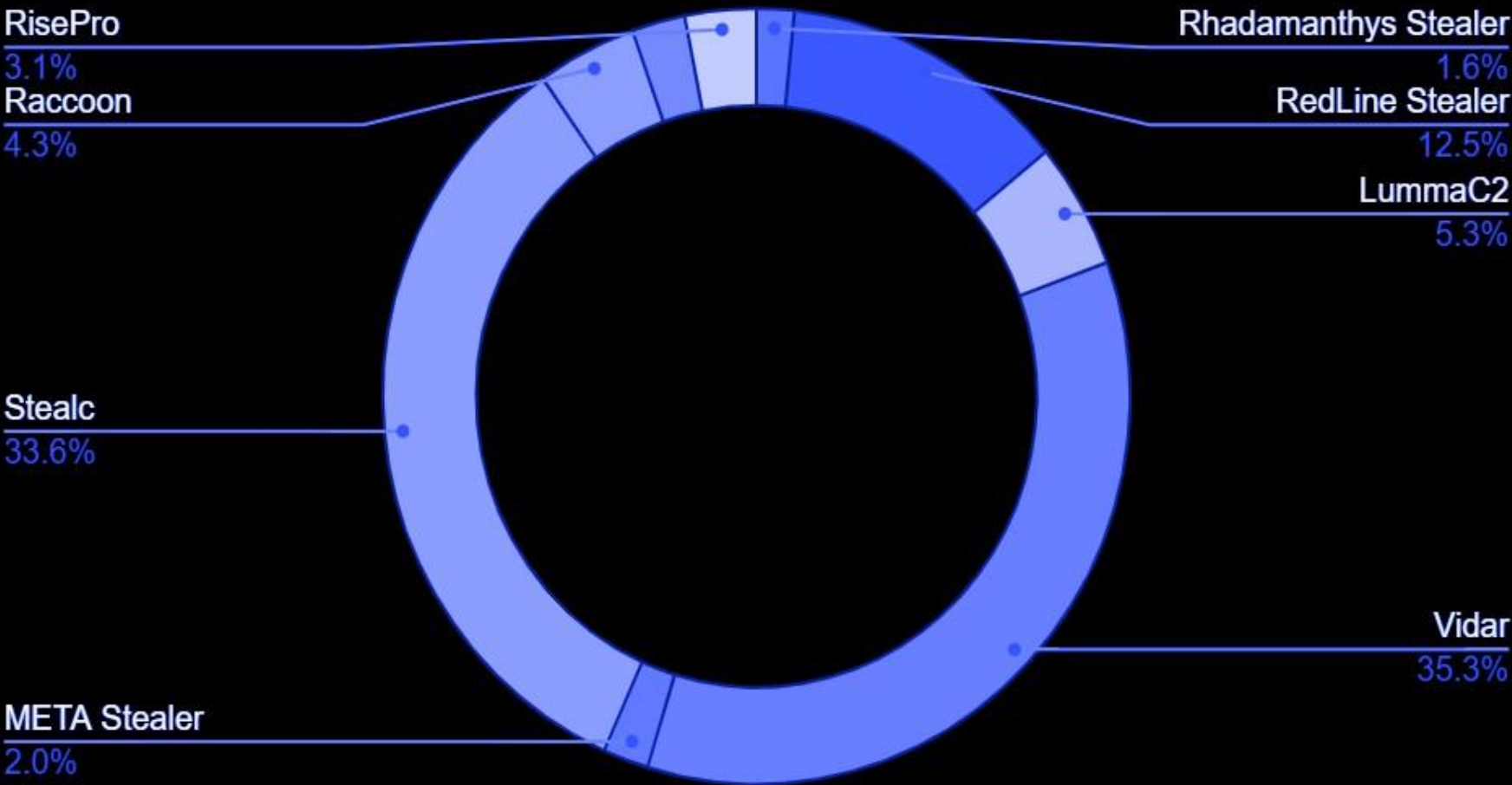


121,350 account compromises

Statistics regarding compromised accounts in February 2026:

- The overwhelming majority of leaked data was from Vidar this month, which is primarily distributed through ClickFix attack via social media, phishing emails with malicious attachments and malicious phishing websites.
- Please see Vidar's information, including signatures and IOCs at the following [link](#).
- Most affected accounts this month are associated with domains belonging to **Roblox, Google, Facebook login[.]live[.]com**.
- Unknown and Gmail login domains are the most impacted.

Top Malware for Compromised Accounts Australia & New Zealand February 2026



COMPROMISED ACCOUNTS (Australia & New Zealand)

↓ 60.23%

From January 2026

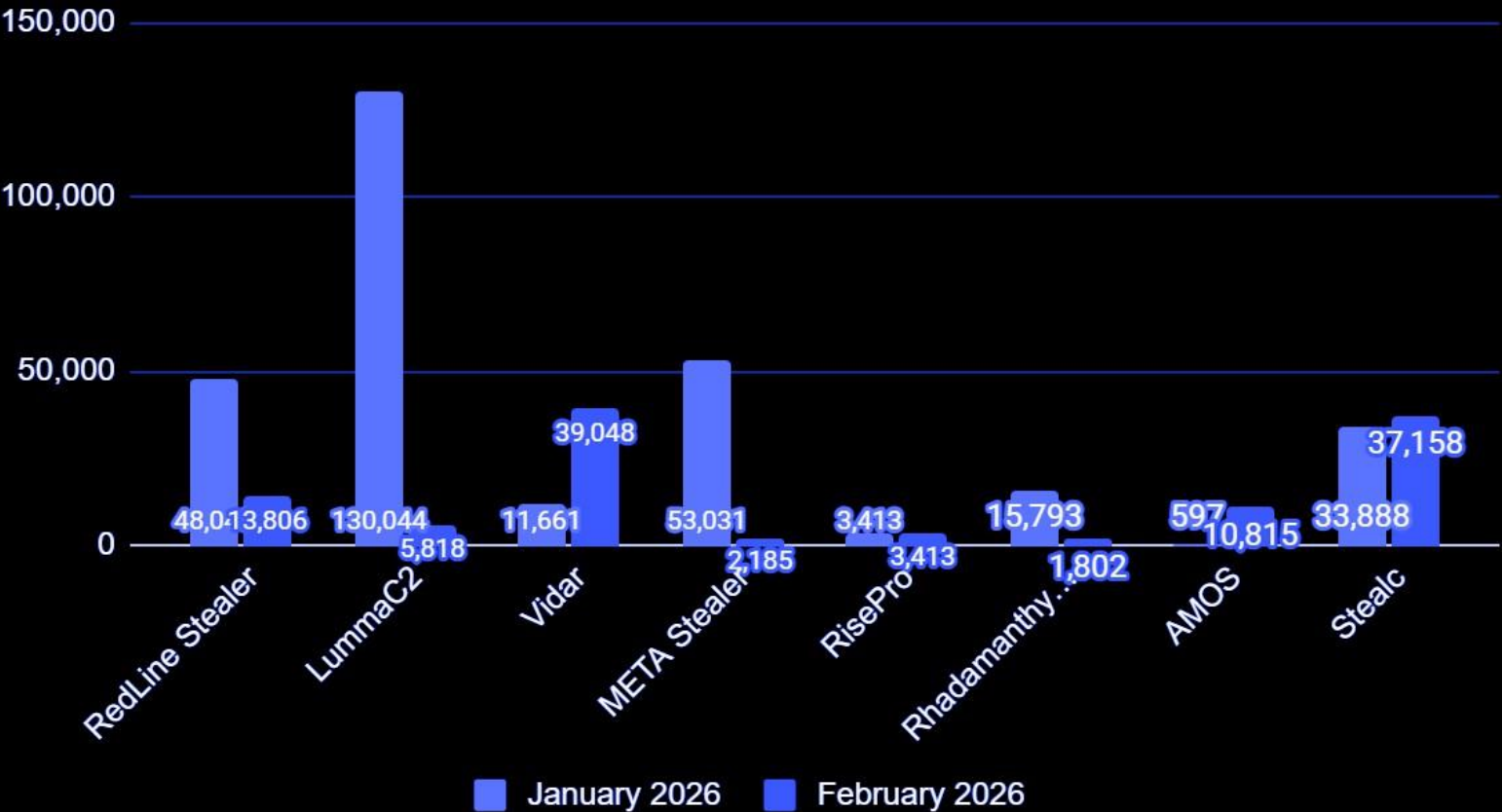


121,350 account compromises

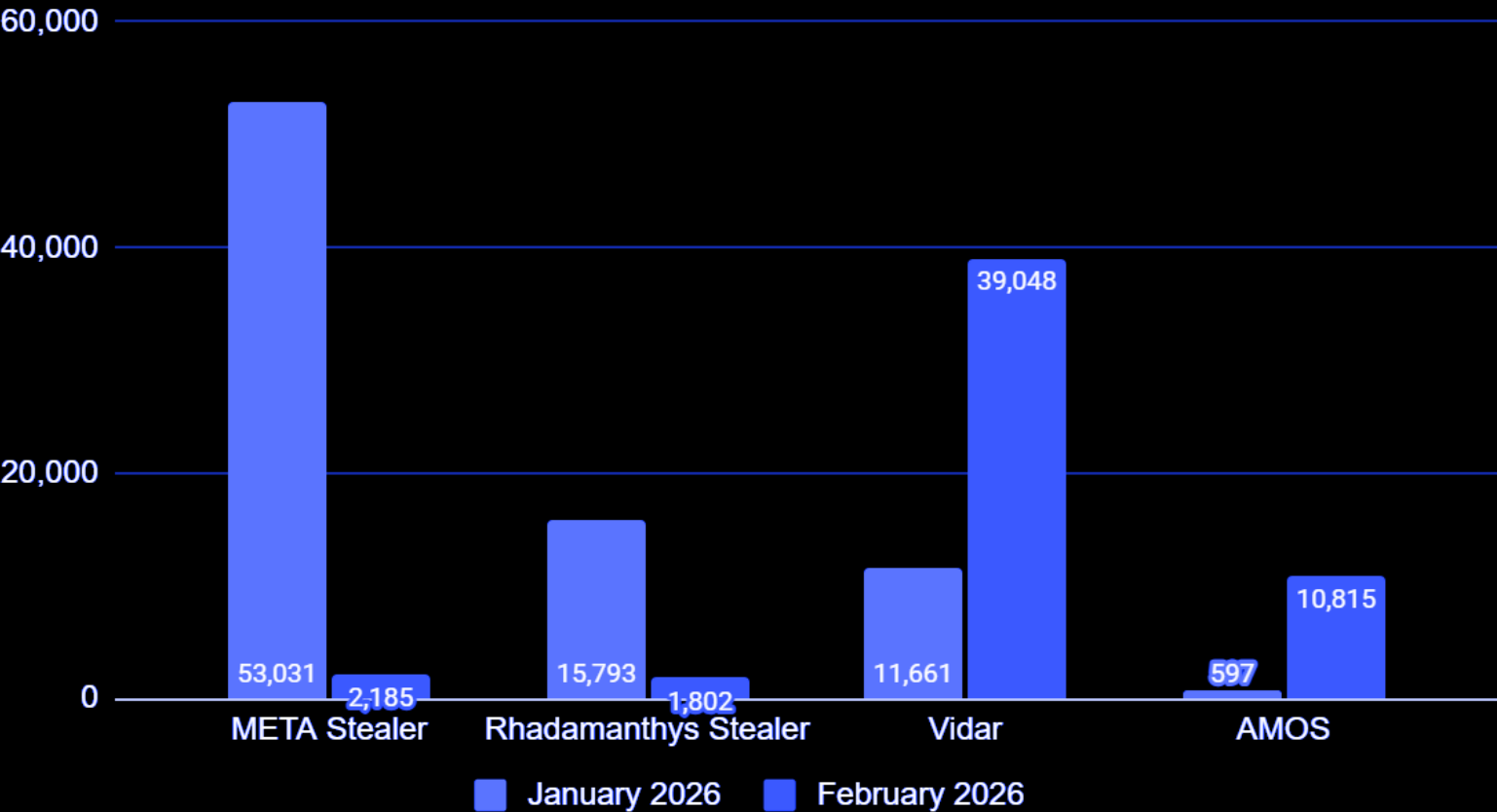
Statistics regarding compromised accounts in February 2026:

- Serious reductions of **LummaC2**, **META Stealer**, **Redline Stealer** and **Rhadamanthys Stealer** activities are responsible for the large drop in Malware activity in February.
- **Vidar**, **Stealc** and **RedlineStealer** and are the top malware families responsible for 74.17% of the compromised accounts in Australia/ New Zealand during the month.

Malware Activity Comparison, Jan- Feb 2026



Malware Big Movers, excluding LummaC2, Jan-Feb 2026



COMPROMISED BANK CARDS (Australia & New Zealand)

↓ 61.29%

From January 2026

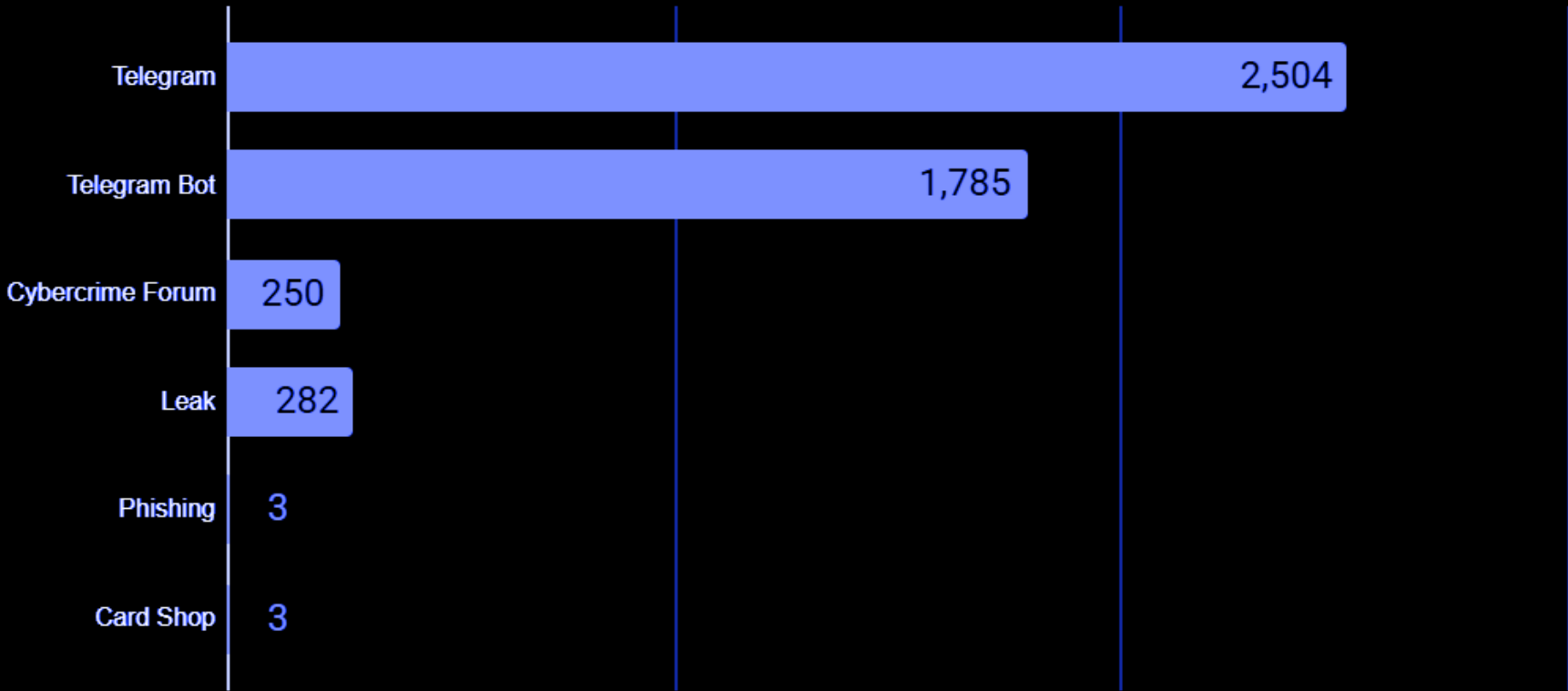


4,216 Compromised Bank Cards

Statistics regarding compromised accounts in February 2026:

- **Australia** has moved down to 18th place of the countries with compromised cards during the month, after placing 7th place in January 2026 with 9,995.
- New Zealand ranks at 71st place of the countries with compromised data, moving down from 43rd place in January 2026.
- The majority of leaked card data came from Telegram, Cybercrime Forums and Leaks.
- 53% of the compromised cards came from Visa this month, followed by Mastercard (42%), with a small amount from American Express. Maestro had over 150 compromises.

Compromised Bank Cards by Sources, Australia & New Zealand



Top 6 source types, February 2026

Interview With An Analyst

In the Customer Success team, we work very closely with your Group-IB Analyst Team. Your Analyst Team work on many aspects of your solution. They don't just spend their time analysing malware and last threats. They're also key members as part of the Digital Risk Protection response process, they correspond with threat actors, they respond to your urgent RFIs and help get the message out when it comes to urgent updates. Our analysts are a wealth of information.

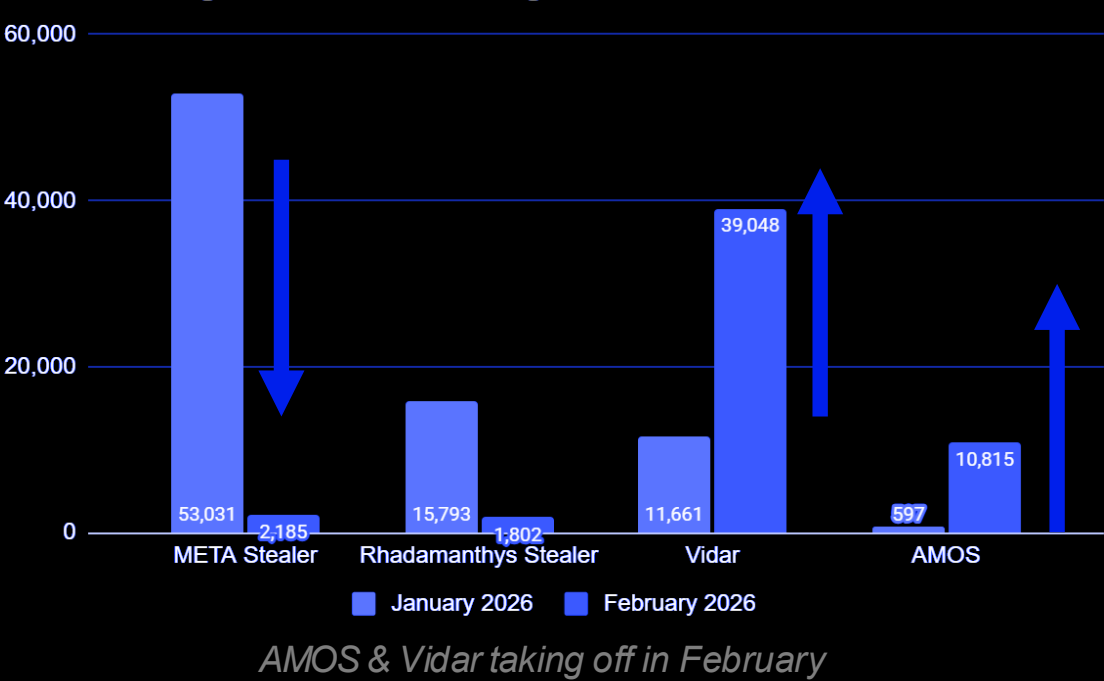
I sat down with Claudia Nave this week, your analyst for Australia & New Zealand, and asked her some questions about her work.

A: Thanks Brett, it's great to be able to contribute to the publication. Over the last month I've been researching some recent breaches involving Australian victims from actors such as FulcrumSec, who have been around since October 2025. They have been observed to target their victims through opportunity, conducting open-asset scanning and vulnerability identification like "React2Shell".

Q: Regarding malware, each month we see a big uptick in some families of malware, and then the next month it's down, but it's often a rotation of a top six. As an example, AMOS delivered nearly 11,000 victims in region in February, compared to about 600 in January. How does that happen?

A: Infostealers are delivered to victims using different methods, usually as MaaS (malware-as-a-service). Affiliates using this tooling could jump to another based on a number of reasons, like increased detection rates on defender tools, or disruptions to the supporting infrastructure. Developers of stealers will frequently release major updates that trigger new waves of use, adopting new features before the detection adapts again.

Malware Big Movers, excluding LummaC2, Jan-Feb 2026



Q: Let's shift to the regional conflict that we've reported on in this publication. Group-IB have reported on what is happening now, but how can our clients stay up to date about the conflict without relying on update emails?

A: If clients would like to continuously track developments related to Middle East escalation, they can:

- Set up a hunting rule in Group-IB's Threat Intelligence using the expertise: **mea_tension**, or
- Access the following link on the Group-IB Threat Intelligence Portal: https://tap.group-ib.com/ta/last-threats?q=expertise%3A+%22mea_tension%22

Group-IB's Global Investigation Team and CERT-GIB continue to monitor threat actor infrastructure 24/7 and remain committed to providing real-time updates as new threats are identified or neutralized. This will allow clients to see reports and updates, that is, 'finished intelligence', as soon as they get published.

Interview With An Analyst

Q: Staying with the regional conflict, are there any APTs or TAs that have popped up that we've detected over the past week?

A: You've quite rightly raised NONAME057(16) & Infrastructure Destruction Squad RU elsewhere in the document. We're concerned about DDoS Hactivism attacks presently. Other than named TAs, keep an eye out in the Group-IB Threat Actors section for unnamed APTs- where Group-IB has general information that hasn't been attributed to a Threat Actor group.

Globally, we're also seeing claimed DDoS attacks from [HellR00ters](#), [404 Cyber Crew Team](#) (global hacktivist- allied with [Dark Storm Team](#) & [BD Anonymous](#), [Moroccan Black Cyber Army](#) (Morocco), [Reallulzsec](#) (Lebanon). Looking at just Australia and New Zealand, we've recently seen activity from [HellR00ters](#), [404 Cyber Crew Team](#), [Team Azrael--Angel Of Death](#) (Pakistan) & [Leakbase](#) (country not attributed).

I'd urge TI teams to make sure to not just to focus on victim countries or a TA attributed country. Whilst hacktivism has been the main uptick, in February we also saw financially motivated cyberattacks from FulcrumSec targeting the financial services industry. Fulcrumsec claim to have tens of terabytes of organisational data that they are sifting through. Group-IB will provide information as it comes to hand. As we can see, threats and victims are global in nature.

Q: And finally, I've heard that you're from a background that eats a lot of pasta. What are your thoughts about putting carrots in lasagne?

A: It's a crime. Don't mess with lasagne. It's perfect as it is.

Maybe hard-boiled egg and ham in a pinch, but you can't go wrong sticking to the classics.

If you would like to have a question answered by our Analyst or Solutions Engineering teams in an upcoming publication, please email your question to the editor, b.stevenson@group-ib.com

Time sensitive requests should be in a service desk ticket.



ADVERSARIES OF THE MONTH

(Australia and New Zealand)



Threat actor groups

- Отряд Разрушения Инфраструктуры RU (Infrastructure Destruction Squad RU) &
- NONAME057(16)

Targeted industries:

Financial services	Electrical Distribution
Agriculture	Cyber Security
Critical Infrastructure	Law Enforcement
Biotechnology	Military
Food and Beverage	Insurance
Artificial Intelligence	Education
Media	Telecommunications
Professional Services	Aviation
Software	+58 Other Industries
Natural Resources	

Period of Activity:	2022 - Present
Targeted countries:	Australia, New Zealand, United States, Canada, Germany, United Kingdom, India, France +46 others
Attribution:	DDoS, Botnet, Crowdsourced attacks
Intent:	Political motives

Attack Summary

NONAME057(16), also known as DDOSIA is a pro-Russian hacktivist group mostly known for DDOS attacks. It appeared in July 2022.

The hacktivist group “ 🚨 Отряд Разрушения Инфраструктуры RU ~ 🚨 ” (Infrastructure Destruction Squad RU) is active on a private Telegram channel created on June 14, 2025.

Both of these Threat Actors spent the month of February targeting critical infrastructure, particularly the water and irrigation industries, across the globe, including four claimed DDoS attacks in Australia New Zealand.

Water and irrigation industries are considered critical infrastructure, with operational technology being used in energy generation, irrigation and manufacturing.

Key Observations

The attackers deliver OT Access attacks involving unauthorized entry into operational technology (OT) environments, including industrial control systems (ICS), SCADA, and HMI interfaces. Such access may allow attackers to disrupt production processes, manipulate equipment, or gain visibility into critical infrastructure operations.

Impact profile: 1057 Network Denial of Service impacts between the two groups. 102 Exfiltration Over Alternative Protocol & Exfiltration Over C2 Channel events.

Further information, including Indicators, can be found at the following links here [\(NONAME057\(16\)\)](#) and [\(Отряд Разрушения Инфраструктуры RU\)](#).

CONCLUSIONS AND RECOMMENDATIONS

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.

STAY SMART. STAY CONNECTED. STAY SECURED

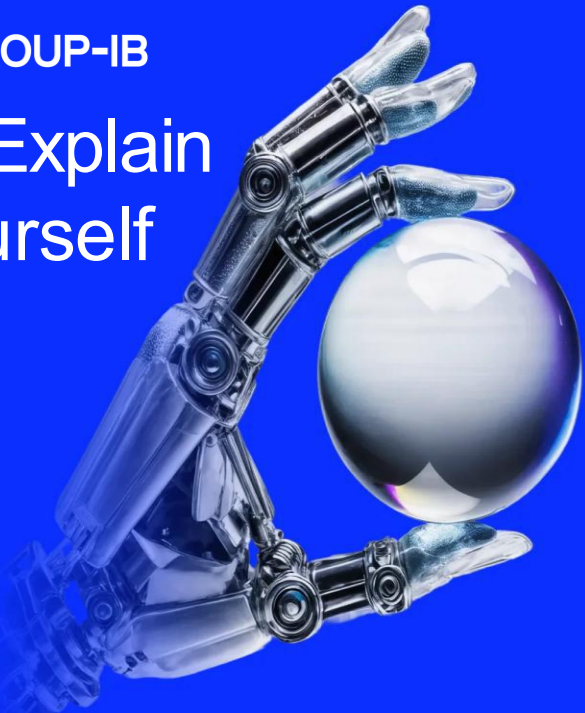


[Subscribe to our mailing list](#)

RECENT RESOURCES



AI, Explain Yourself



Why Is Explainable AI (XAI) Becoming Critical for Cybersecurity?

[Read now](#)



Operation Olampo:



Inside MuddyWater's Latest Campaign

[Discover more](#)



GT Fire Phishing Scheme



Avoiding Detection Using Google Services

[Read now](#)

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003