

For Data From March 2026

ANZ Threat Landscape

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 Threat Landscape 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 01st March - 31st 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](#). On 25th March 2026, we passed a count of over 500 reported cyber attacks related to the conflict.

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 01 March- 31 March 2026 are: [DieNet](#), [Keymous](#), [313 Team](#), [APT Iran](#), [Mr Hamza](#), [RealLulzSec](#), [THE GARUDA EYE](#), [SYLHET GANG-SG](#), [Cyber Resistance Axis](#), [Handala Hack](#), [Cyber Fattah Team](#), [Winter Vivern](#), [Moroccan Black Cyber Army](#), [Coup Team](#), [FaD Team](#), [Rocket Kitten](#) (Department 50/ Department 40), [Transparent Tribe](#), [WIRTE](#), [Z-Pentest](#), [Mustang Panda](#), [Cyber Isnaad Front \(C.I.F.\)](#), [Mobir](#), [Cyber Resistance Axis](#), [Team Insane PK](#), [Predatory Sparrow](#), [Evil Markhors](#), [UniT 313](#), [CyberToufan](#), [Fatimion Cyber Team](#), [Hider Nex](#), [DarkStorm Team](#), [STUCX TEAM](#), & [Fatimion Cyber Team](#).

This is a significant increase in Threat Actor activity and participation when compared to the initial reporting cycle of this conflict of 27th Feb -4th March.

These [attacks](#) predominantly include DDoS, with large numbers of claimed data breaches and access to systems. Hacktivism defacement attacks have become common. Attacks on any government ministry of a government not aligned with Iran have become common.

Victim nations include: Israel, Bahrain, Italy, Egypt, Qatar, Morocco, Saudi Arabia, USA, Cyprus, Kuwait, France, UAE, Pakistan, Romania & Syria.



Middle East Regional Conflict

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

04

Notable Cyber Incidents that Group-IB reported

The threat landscape demonstrates a clear transition into a sustained hybrid conflict phase including:

- Iran remaining largely offline for over 30 days, with intermittent abnormal routing activity suggesting controlled and selective connectivity.
- Confirmed efforts by Iranian authorities to detect and confiscate satellite internet devices (Starlink), indicating active enforcement of digital isolation using advanced monitoring capabilities.
- A destructive cyber incident affecting a Stryker, involving remote wiping of tens of thousands of devices via legitimate enterprise tools. The attacker, Handala, leveraged Microsoft Intune and wiped over 80,000 devices.
- Law enforcement action linking hacktivist infrastructure to Iranian intelligence (MOIS), confirming the role of cyber operations in psychological and influence campaigns. The U.S. Department of Justice announced the seizure of four domains used in cyber operations.
- Continued expansion of fraud campaigns exploiting geopolitical narratives, including investment scams and logistics-related phishing. Group-IB Digital Risk Protection observed a new fraud campaign distributing sponsored advertisements on social media, leveraging geopolitical tensions to promote investment scams linked to the energy sector.
- Evidence of device-level risk clustering, including spoofing, remote access tooling, and anonymization tools. Group-IB's Fraud Protection flagged several geohashes where devices were found to simultaneously contain multiple categories of risk-indicative tools.
- Real-world operational exposure through fitness tracking applications leaking sensitive military movement data. A publicly accessible Strava profile belonging to a French naval officer enabled near real-time tracking of the aircraft carrier Charles de Gaulle (FS CdG) and its escort group.

04

Notable Cyber Incidents

- Handala Group continues multi-stage malware campaign using Telegram as C2 infrastructure to assist in Iranian government-linked espionage activities, focusing on user-interaction-based infection chains and integrating espionage capabilities into broader hybrid operations.
- DieNet claims DDoS, defacement and data leak attacks on Interpol, Europol. Universities from Haifa, Jerusalem, Ono, Saudi Arabia, Tel Aviv, Capital were targeted. Of increasing concern is the targeted attacks against critical infrastructure, such as the attacks on Bahrain Electricity and Water Authority, Egyptian National Railways, Egyptian Ministry of Water Sources and Irrigation, as well as Cranfield Airport and Lockheed Martin.
- 313 team claims DDoS attacks on Interpol, Europol, United Nations, Internet Archive, Saudi Ministries, Saudi Press, Google, Tenor, Kuwait Government, Donald Trump's brand, 4chan, Blackbaud, Moodle, Appfolio, Microsoft, British Army, Qatari Government, Commerce Bank, UAE Government, Romanian Government, Bahraini Government.
- Unit 313 claims DDoS attacks on Qatari Government, Saudi universities, Qatari critical infrastructure (water and electricity), US Government, Saudi Government, Afghani Government, Dubai Mall, UAE Taxi and Transportation websites, Syrian Government, Afghan Film, Saudi Aramco, LibanPost, Tayyar, Lebanese Universities, Azerbaijani Government and social media, NATO Watch, Der Spiegel (Newspaper), Technical University of Berlin, University of Munich, French Government and US Government.

Key Findings & Global Cybersecurity Trends – March 2026

01. Cybersecurity Strategy Planning: The Essential Reset for Security Teams and Leaders in 2026

Cybersecurity is widely discussed at the boardroom table, but integrating it into the broader business context is where the gap lies: it shows up in uninformed security investments and decisions, misaligned business expectations, increased threat exposure without threat prioritization, and a lack of shared understanding of the current vs. desired security posture.

[Click for more information](#)

02. The Rise of Fake Shipment Tracking Scams in MEA

According to the 2024 Universal Postal Union's State of the Postal Sector report , postal services now serve a population of 7.3 billion people, and without them, a country's GDP could drop by a median of 7%.

And according to Statista, about 161 billion parcels were shipped worldwide in 2022 alone. Some of the top countries driving this volume include:

- China, which handled roughly 110 billion parcels in 2022, by far the largest share of global parcel traffic.
- United States, which shipped about 21 billion parcels in the same year.
- Japan, with around 9 billion parcels in 2022.

[Click for more information](#)

03. Six Supply Chain Attack Groups to Watch Out for in 2026

SaaS platforms, open-source ecosystems, MSPs, and cloud integrations now act as force multipliers, where a single compromise can create a ripple effect and affect hundreds of downstream organizations.

The methods used by the six threat actors described below show how supply chain abuse ties together phishing, data breaches, ransomware, and espionage into one interconnected attack ecosystem.

[Click for more information](#)

04. Conflict Watch Update: Week 5 — State-Linked Malware Campaigns, Infrastructure Targeting, and Escalating Hybrid Pressure

During Week 5, the threat landscape demonstrates a further escalation into coordinated hybrid operations, combining state-linked cyber campaigns, opportunistic destructive activity, infrastructure targeting narratives, and large-scale fraud exploitation.

This report continues Group-IB monitoring of the cyber dimension of the ongoing Iran–Israel–U.S. escalation and related regional developments.

Previous updates covering earlier phases of the conflict are available here: [Conflict Watch Reporting](#)

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – March 2026

01. Hasta la vista, Hastalamuerte: An Overview of The Gentlemen's TTPs

The report provides an overview on tactics, techniques, and procedures (TTPs) of The Gentlemen observed by Group-IB in intrusions conducted by its affiliates, as well as relevant information about the group's capabilities collected from underground private sources.

[Click for more information](#)

02. DieNet claimed DDoS attack on Kuwait Finance House

The Group-IB Threat Intelligence team identified a DDoS attack claimed by the threat actor DieNet targeting the website of Kuwait Finance House. The message indicates multiple connection attempts with varying response times, suggesting a disruption in service.

[Click for more information](#)

03. HIME666 claimed data leak from multiple countries

The Group-IB Threat Intelligence team identified a message from the threat actor HIME666, who claimed to possess a 30TB+ database collection containing over 100,000 private databases. The databases reportedly include information from various countries such as the Netherlands, France, Belgium, Italy, Germany, Switzerland, Poland, Vietnam, Iran, Sweden, the USA, Spain, Greece, Colombia, Ukraine, India, and others. The databases are said to contain sensitive information like phone numbers, emails, citizen data, passports, and more.

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – March 2026

04. Evil Markhors claimed defacement of multiple websites

The Group-IB Threat Intelligence team identified a defacement attack by Evil Markhors targeting multiple websites, including those in Israel, Belgium, and China. The attack involved altering web pages to display unauthorized content.

[Click for more information](#)

05. Hider_Nex claimed DDoS attacks on South Korean government websites

The Group-IB Threat Intelligence team identified a series of DDoS attacks claimed by the threat actor Hider_Nex targeting various South Korean government websites. The attacks were confirmed through check-host reports.

[Click for more information](#)

06. Everest Ransomware attack on Hyundai Elevator

On 2026-03-06, the ransomware group Everest claimed responsibility for an attack targeting Hyundai Elevator. The incident was disclosed through a post on the group's leak site (DLS), where the threat actors allegedly published evidence of the breach and threatened to release sensitive data if their demands were not met.

[Click for more information](#)

07. Qilin Ransomware attack on Omesti Berhad

On 2026-03-03, the ransomware group Qilin claimed responsibility for an attack targeting Omesti Berhad (omesti[.]com). The incident was disclosed through a post on the group's leak site (DLS), where the threat actors allegedly published evidence of the breach and threatened to release sensitive data if their demands were not met.

[Click for more information](#)

LOCAL INSIGHTS (Australia & New Zealand)

Local Insights from Group-IB with a brief description:

01 **Supply-chain compromise affecting Aqua Security's Trivy scanner**

On 20th March 2026, Aqua Security disclosed an incident compromising their Trivy open-source security scanner. The compromise affected various Trivy versions across multiple distribution channels, as well as their Github Actions CI/CD implementation, which is a pre-built workflow hosted on GitHub Actions. Because it is common to rely on version tags (instead of hashes) the attackers were able to affect ongoing pipelines without any indication that the code has been tampered with. The compromise involved the inclusion of malicious code which facilitated credential stealing and exfiltration. This attack has been attributed to TeamPCP.

02 **Infinity Australia Leaked Database**

The Group-IB Threat Intelligence team identified a database sale from financial service provider Infinity Australia, by data broker actor einein786. Posted to the underground exploit[.]in forum on 31st March, the leak contained several company documents from 2024, including PII such as passport details, drivers licenses, tax file numbers, and bank statements. einein786 is a newly registered user on the exploit[.]in forum with a primary motivation of financial gain through database sales.

03 **Phonebot Leaked Database**

The Group-IB Threat Intelligence team identified an alleged database leak from the Australian retailer Phonebot by threat actor 2019. The leak contains customer details as well as account specific point balances and rewards, increasing the risk of targeted attacks towards affected customers. 2019 was first seen in February 2026 and specializes in selling large-scale personal information databases from healthcare companies, ecommerce platforms and business service providers.



RANSOMWARE ACTIVITIES (Australia & New Zealand)

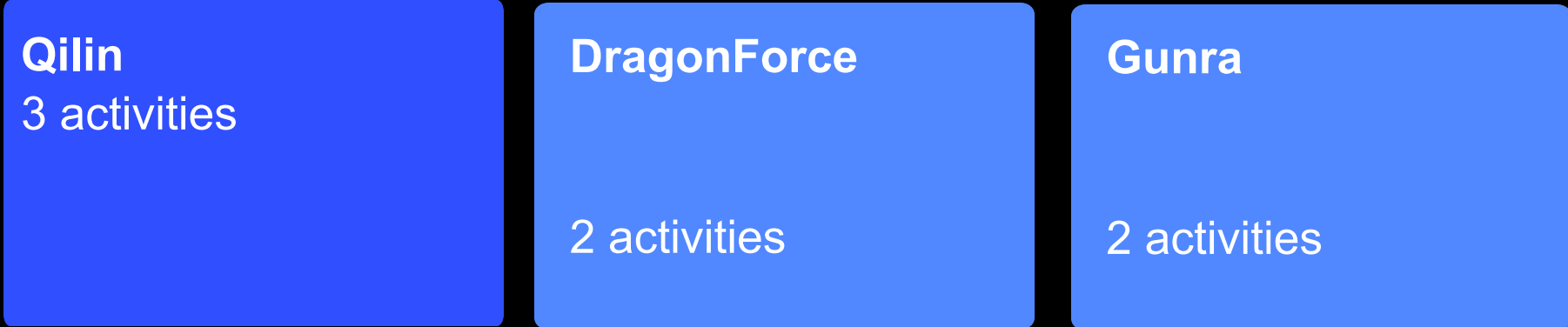
↑10.0%
From February 2026
11 ransomware incidents



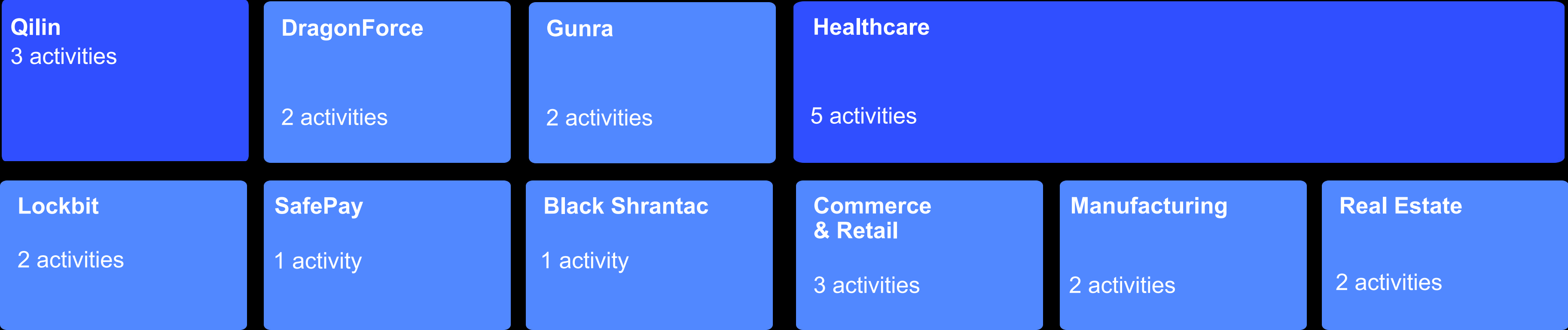
Statistics regarding ransomware activities in February 2026:

- **Australia** remains out of the top 5 countries globally from March sitting in 19th place globally, down from 13th place in February 2026.
- New Zealand is well out of the top 10 targeted countries, sitting in 78th place for March 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 Intra Ltd by The Gentlemen. Files were disclosed on their DLS.
- For Australia, the most notable incidents included ransomware attacks on Fortress Systems by Qilin, as well as multiple attacks to the Australian healthcare industry from groups such as Rhysida, DragonForce and SafePay Ransomware.
- 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)



Most targeted industries



Data: number of not unique events and activities (with updates).

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**, **3** Hacktivism incidents were recorded in March 2026.

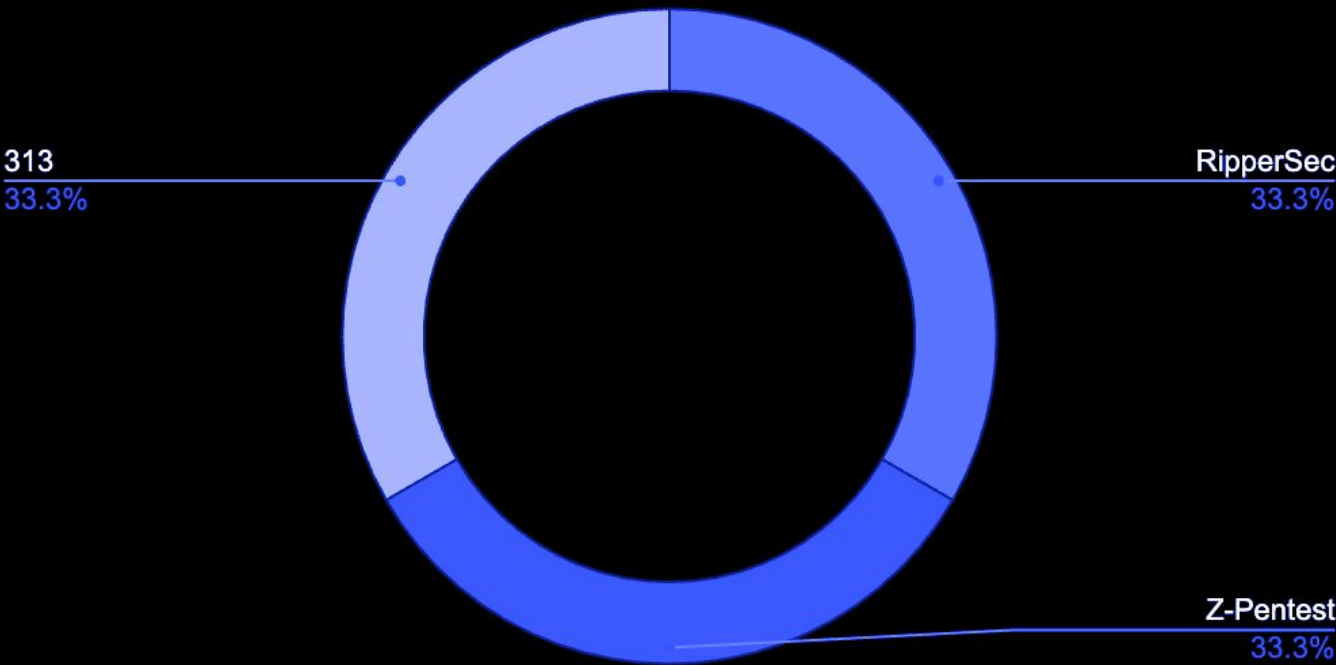
The Group-IB Threat Intelligence team reported that the TA **RipperSec** claimed a DDoS attack on ZFA Australia, posting their updates on targets and scheduled attacks across instant messaging platforms. These attacks conducted by RipperSec are mainly motivated by Australia’s support of actions during a time of tension in the Middle East.

The hacktivist group **Z-Pentest** continues to show focus in gaining access into Australian infrastructure after events earlier in 2026, claiming access into surveillance infrastructure of food services in Queensland, Australia. Additionally, the group **313** have also been reported to have successfully conducted a DDoS attack on the education platform Moodle, a widely used tool among the largest universities in Australia, affecting access for university staff and students.

While reported activity may seem low for this critical time of escalated tension, it is vital to continue monitoring scheduled attacks and chatter within the Threat Intelligence platform to gain more insight into what attacks may be expected over the next month.

No DDoS or Hacktivism events were reported for New Zealand for March 2026.

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



COMPROMISED ACCOUNTS (Australia & New Zealand)

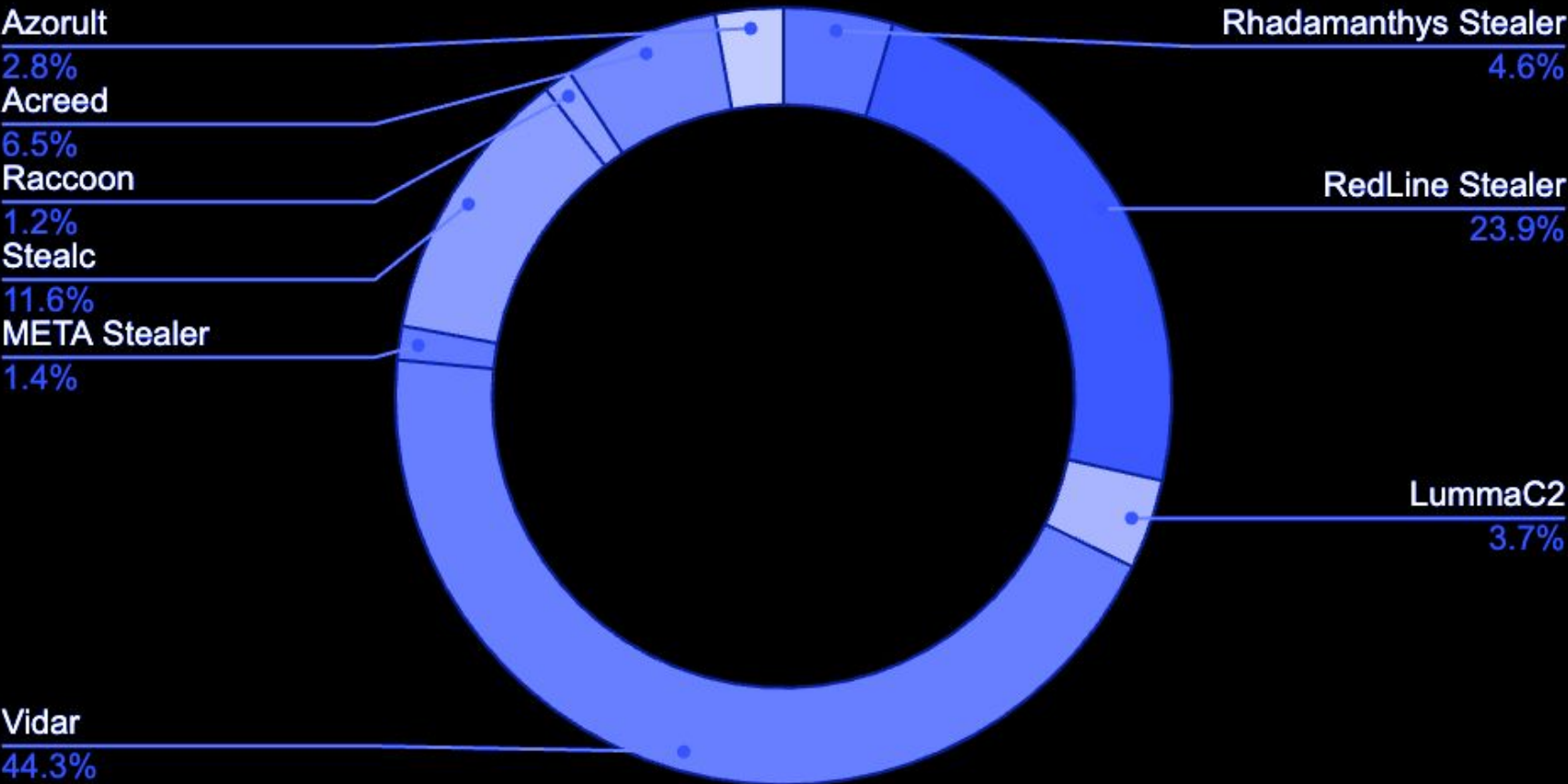
↓ 28.9%
From February 2026
78,592 account compromises



Statistics regarding compromised accounts in March 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 March 2026



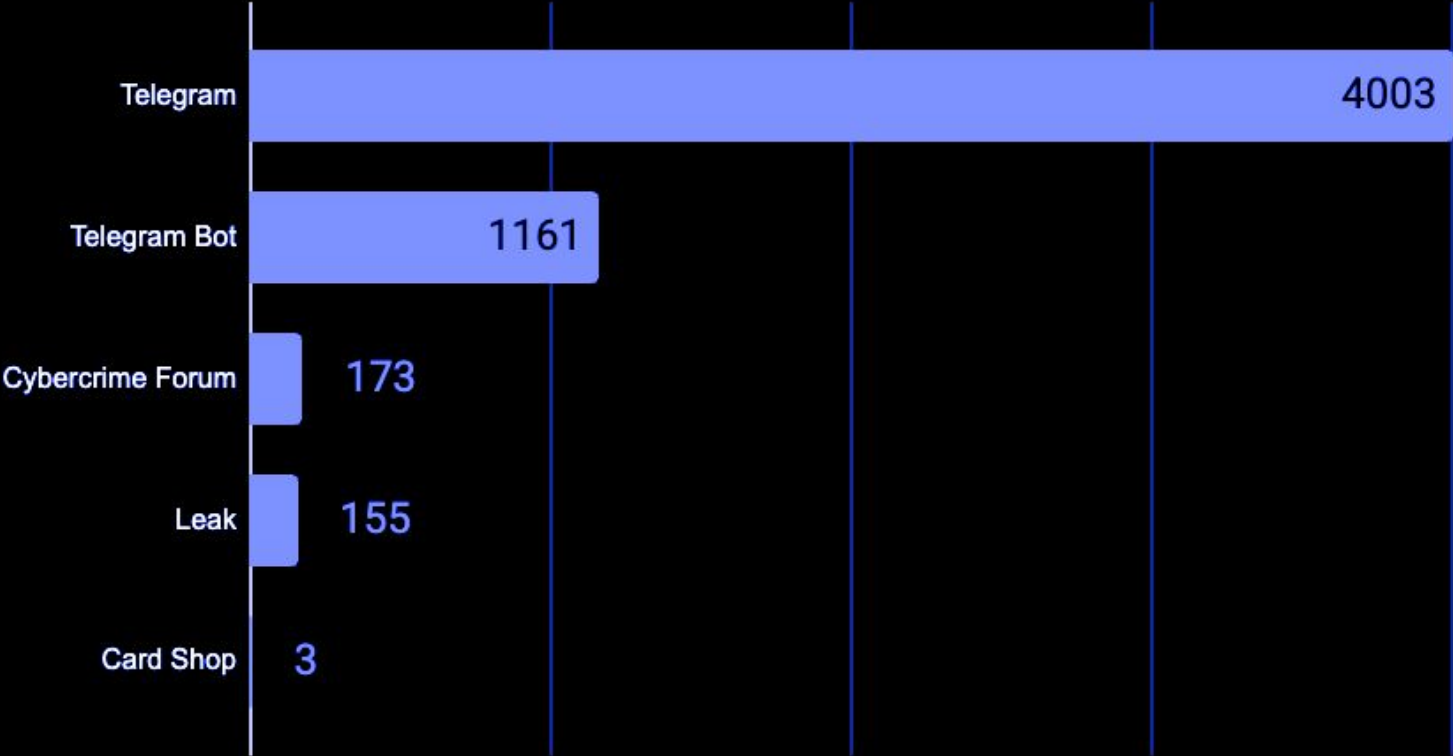
COMPROMISED BANK CARDS (Australia & New Zealand)

↑ 17.39%
From February 2026
4,949 Compromised Bank Cards

Statistics regarding compromised accounts in March 2026:

- **Australia** has moved down to 17th place of the countries with compromised cards during the month, after placing 18th place in February 2026 with 4,216.
- New Zealand ranks at 57th place of the countries with compromised data, moving up from 71st place in February 2026.
- The majority of leaked card data came from Telegram, Telegram Bots and Cybercrime Forums.
- 58% of the compromised cards came from Visa this month, followed by Mastercard (37%), with a small amount from American Express. Maestro had 127 compromises.

Compromised Bank Cards by Sources, Australia



Top 5 source types, March 2026

ADVERSARIES OF THE MONTH

(Australia and New Zealand)



Threat actor group

- **DieNet**

Targeted industries:

Government and Military	Transportation
Undefined Industries	Internet Services
Financial Services	Education
Telecommunications	Media & Entertainment
Software	Energy
Information Technology	Commerce and Shipping

Period of Activity: 2025 - Present

Targeted Countries: Israel, USA, India, Qatar, Jordan, UAE, Kuwait, Australia, UK, Netherlands, Sweden, France, Germany + 21 others

Attribution: DDoS, Hacktivism and Defacement

Intent: Political motives

Attack Summary

DieNet has been extremely active during the current Middle East Tension, elevating their attack patterns from once every four to five days to now delivering around 30 attacks daily.

Between March 2025- February 2026 DieNet had delivered 251 attacks. In March 2026 they claim to have delivered over 192 attacks, compressing a previous year's worth of work into a single month, with a primary MITRE ATT&CK of Network DDoS. Where possible, Defacement is also used; there were 19 reported Defacement incidents in March.

This month, DieNet's victims have mostly been targeted in Israel and GCC countries, but they have also targeted US Government agencies and businesses in Europe, including an attack on Lamborghini. Allied with the Threat Actors 'Arabian Ghosts' & 'Syrian Ghosts'

In Australia, DieNet have previously targeted the Australian Government, NSW Government, Canva, University of Western Australia, McGrath Real Estate and Amazon Australia.

Key Observations

DieNet DDoS attacks aim to overwhelm an organization's network resources or services, rendering them inaccessible to legitimate users. Attackers utilize numerous compromised devices to generate high volumes of traffic.

Impact profile: 401 Network Denial of Service attacks over the past 12 months. 12 Exfiltration Over C2 events. To combat against these types of attacks in the future, Group-IB recommend preparing with diversification of providers, scaling of resources to handle traffic spikes, using DDoS vendor products, upstream geographic and ip address filtering. During an attack, it's important to pay close attention to other possible attacks on your network as the DDoS attack may be a diversion.

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



An Overview of The Gentlemen's TTPs

Hasta la vista, Hastalamuerte

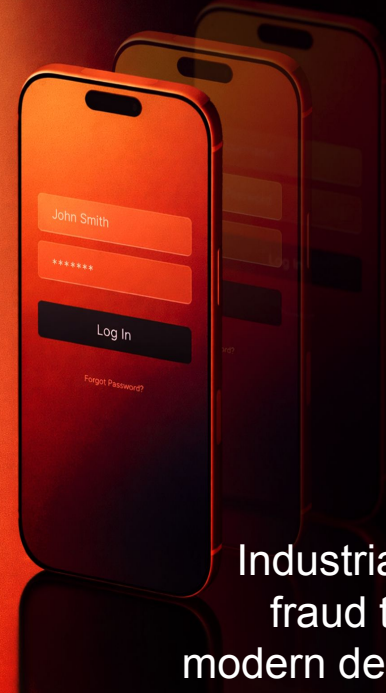
[Read now](#)



Who's attacking your vendors?

Six Supply Chain Attack Groups to Watch Out for in 2026

[Discover more](#)



Cloud Phones: The Invisible Threat

Industrial-scale financial fraud that's invisible to modern detection systems.

[Read now](#)

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003