

January 2026

ANZ INTELLIGENCE INSIGHTS

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

Key Findings & Global Cybersecurity Trends – January 2026

01. Infrastructure Destruction Squad Claims Massive FBI Data Breach

The Infrastructure Destruction Squad hacking group has reportedly claimed a significant data leak involving the Federal Bureau of Investigation (FBI), according to recent analysis by the Group-IB Threat Intelligence team. This 121 GB breach allegedly exposes a vast repository of sensitive information, including confidential client documents, internal FBI budgets, payroll records, and financial data. Of particular concern to cybersecurity experts is the inclusion of highly sensitive personal identifiers such as Social Security numbers, tax records, and private identities, alongside internal system images classified as confidential by the Bureau.

[Click for more information](#)

02. Unattributed State-Linked Actor Targets Kazakhstan and Afghanistan

A suspected state-affiliated threat actor is currently targeting government and commercial entities in Kazakhstan and Afghanistan through a persistent cyber espionage campaign. According to recent threat intelligence, the command-and-control (C2) infrastructure supporting this activity has been operational since at least August 2022 and remained active as of January 20, 2026. Central to this campaign is a sophisticated Windows-based remote access trojan (RAT) dubbed "KazakRAT," which is typically delivered as a DLL file. This malware allows the unidentified attackers to enumerate host information, execute secondary payloads, and exfiltrate specific files from compromised systems. To increase infection rates, the threat actor utilizes a streamlined installation process and deploys decoy content specifically tailored to the geopolitical interests of victims in the Kazakhstan and Afghanistan regions.

[Click for more information](#)

03. Pro-Russian Hacktivists NoName057(16) Target UK Infrastructure in New DDoS Wave

The pro-Russian hacktivist collective NoName057(16) has claimed responsibility for a series of distributed denial-of-service (DDoS) attacks targeting several high-profile UK organizations, according to reports from the Group-IB Threat Intelligence team. The coordinated campaign aimed to disrupt the digital services of critical infrastructure and local government entities, including National Rail, the Port of Felixstowe, Wessex Water, and the Stirling and Buckfastleigh councils. Technical analysis using check-host[.]net confirmed temporary connectivity issues for these sites, consistent with the group's "DDoSia" project tactics. This latest activity follows a pattern of ideologically motivated strikes by NoName057(16) against NATO member states and allies supporting Ukraine, underscoring the persistent threat hacktivist groups pose to UK operational resilience and public service accessibility.

[Click for more information](#)

Key Findings & Global Cybersecurity Trends – January 2026

04. Hider_Nex Hacktivist Group Launches DDoS Strike on Saudi Media Giant Thmanyah

The pro-Palestinian hacktivist collective known as Hider_Nex, also identified as the "Tunisian Maskers Cyber Force," has claimed responsibility for a distributed denial-of-service (DDoS) attack against Thmanyah, a prominent media and entertainment organization in Saudi Arabia. The incident was detected and verified by the Group-IB Threat Intelligence team, with external network monitoring via Check-Host confirming significant service disruptions. This strike is part of a broader campaign by Hider_Nex—often operating in coordination with groups like Anonymous Russia—to target high-profile entities in the MENA region. By leveraging DDoS tactics to silence influential media voices, the group aims to amplify its geopolitical narrative, underscoring the increasing vulnerability of digital broadcasting and publishing platforms to ideologically motivated cyber operations.

[Click for more information](#)

05. Microsoft Uncovers Multistage AiTM Phishing Campaign Leveraging SharePoint to Target Energy Sector

On January 21 2026, Microsoft security researchers detailed a sophisticated, multi-stage adversary-in-the-middle (AiTM) phishing and business email compromise (BEC) campaign specifically targeting organizations within the global energy sector. The attackers exploited trusted SharePoint file-sharing services to deliver malicious phishing payloads, effectively bypassing traditional email filters by leveraging legitimate infrastructure. Once initial access was gained, the threat actors utilized automated inbox rule creation to maintain long-term persistence and hide their activity from legitimate account holders. This transition from credential theft to high-impact BEC activity allowed the attackers to move laterally across multiple organizations, highlighting a significant evolution in how AiTM techniques are being used to facilitate large-scale financial fraud and corporate espionage.

[Click for more information](#)

Key Findings & Global Cybersecurity Trends – January 2026

06. Infrastructure Destruction Squad Claims Breach of Italian Water Control Systems

The Group-IB Threat Intelligence team has reported a critical unauthorized access event involving Italian water infrastructure, purportedly carried out by the "Infrastructure Destruction Squad" hacking group. The targeted operational technology (OT) manages vital systems responsible for monitoring and regulating water levels and flow between major rivers and regional waterways. Because these automated systems control sluice gates based on real-time sensor data, they are essential for both large-scale flood prevention and agricultural irrigation management across Italy. This breach highlights a severe risk to national safety and resource distribution, as any manipulation of these automated environmental controls could lead to significant physical disruption or ecological damage within the affected regions.

[Click for more information](#)

07. Scattered Lapsus Hunters Resurface with New Data Leak Site and Fresh Victims

On January 22, 2026, the cybercriminal alliance known as "Scattered Lapsus\$ Hunters"—a high-profile merger of the **Scattered Spider**, **ShinyHunters**, and **Lapsus\$** collectives—unveiled a new Tor-based data leak site (DLS) to facilitate their ongoing extortion campaigns. This launch, announced via their "shseller13" Telegram channel, marks a strategic resurgence for the group following a temporary dormancy late last year. The new platform features three newly claimed victims, adding to a growing repository of exfiltrated data that reportedly includes major hauls from recent supply chain attacks and identity-based intrusions. By consolidating their technical expertise in social engineering and bulk data harvesting, the alliance is actively promoting an "extortion-as-a-service" model, signaling a shift toward more structured, persistent operations targeting large-scale enterprises and cloud service providers throughout 2026.

[Click for more information](#)

Key Findings & Global Cybersecurity Trends – January 2026

08. DieNet Hacktivists Target Indian Infrastructure with Widespread DDoS Attacks Ahead of Republic Day 2026

The most prominent threat actor currently targeting India is **DieNet**, an ideologically motivated hacktivist group that launched an extensive campaign of distributed denial-of-service (DDoS) attacks throughout January 2026. These coordinated strikes specifically aimed to disrupt Indian digital infrastructure in the lead-up to the nation's Republic Day celebrations, demonstrating a clear pattern of targeting essential government portals and telecommunications services. Leveraging "DieNet v2" infrastructure known for utilizing massive botnets and multi-vector techniques like DNS amplification, the group sought to destabilize public-facing services during a period of high national sensitivity. This surge in activity underscores the growing trend of "hybrid warfare," where digital disruptions are timed to amplify geopolitical tensions and challenge the operational resilience of critical national infrastructure.

[Click for more information](#)

09. Infrastructure Destruction Squad Claims Breach of South Korean Manufacturer HYBUSUNG TECH

The Group-IB Threat Intelligence team has reported a critical unauthorized access event involving the industrial control systems (ICS) at **HYBUSUNG TECH**, a specialized manufacturer in South Korea. The breach reportedly targets the operational technology (OT) responsible for managing high-precision throttle shaft production within an automated, multi-node environment. These compromised systems synchronize complex axis and drive movements across independent manufacturing stations, ensuring the precise sequence of technological operations required for automotive component assembly. By gaining a foothold in this automated production line, the "Infrastructure Destruction Squad" poses a significant threat to industrial safety and supply chain integrity, highlighting the increasing vulnerability of South Korea's smart manufacturing sector to targeted cyber-physical attacks.

[Click for more information](#)

Key Findings & Global Cybersecurity Trends – January 2026

10. Mirage Broker Targets Singapore with Massive Facebook Malvertising Campaign

A comprehensive investigation by Group-IB has uncovered an extensive malicious Facebook advertising campaign orchestrated by the threat actor known as **Mirage Broker**. While the operation has reached residents in Poland, Belgium, Hong Kong, Italy, and the Czech Republic, the campaign predominantly targets citizens in **Singapore**, leveraging social media reach to deploy fraudulent financial schemes and phishing lures. To date, Group-IB has identified 822 active domains linked to this infrastructure over the past six months, with analysts currently monitoring an additional 166 suspicious domains poised for imminent activation. This multi-regional malvertising threat underscores a sophisticated approach to audience segmentation, using Facebook's ad platform to bypass traditional web filters and exploit the trust of users across high-value global markets.

[Click for more information](#)

11. Infrastructure Destruction Squad Claims Compromise of South Korean Industrial Hub Jeonnam Technopark

The Group-IB Threat Intelligence team has reported a critical security breach at **Jeonnam Technopark** in South Korea, with the "Infrastructure Destruction Squad" claiming unauthorized access to its industrial control systems. The attackers reportedly gained deep visibility into the facility's operational technology (OT), enabling them to monitor real-time machine performance, access downtime logs, and analyze sensitive production analytics. Beyond mere observation, the threat actors demonstrated the ability to remotely manage production processes, alter network configurations, and manipulate basic machine operations. To signal their full administrative control, the group defaced system interfaces by displaying their logo on operational screens. This intrusion into a key South Korean technological hub underscores the severe physical and economic risks posed by threat actors targeting the management and monitoring systems of high-tech industrial parks.

[Click for more information](#)

LOCAL INSIGHTS (Australia)

Local Insights from Group-IB with a brief description:

01

Whole IT Data published on “CI0P” Ransomware DLS

On the 27th January 2026, the ransomware group **CI0P** published evidence of **Whole IT's** breach and threatened to release sensitive data if their demands were not met. The Threat Actor uses **Data Encrypted for Impact** as part of the MITRE ATT&CK. In addition, on 17th January 2026, the Threat Actor **Big-Bro** posted a thread on dark forums claiming to be selling Domain access as a Domain User to an **unspecified grocery retail company**.

02

Ransomware activities during the month

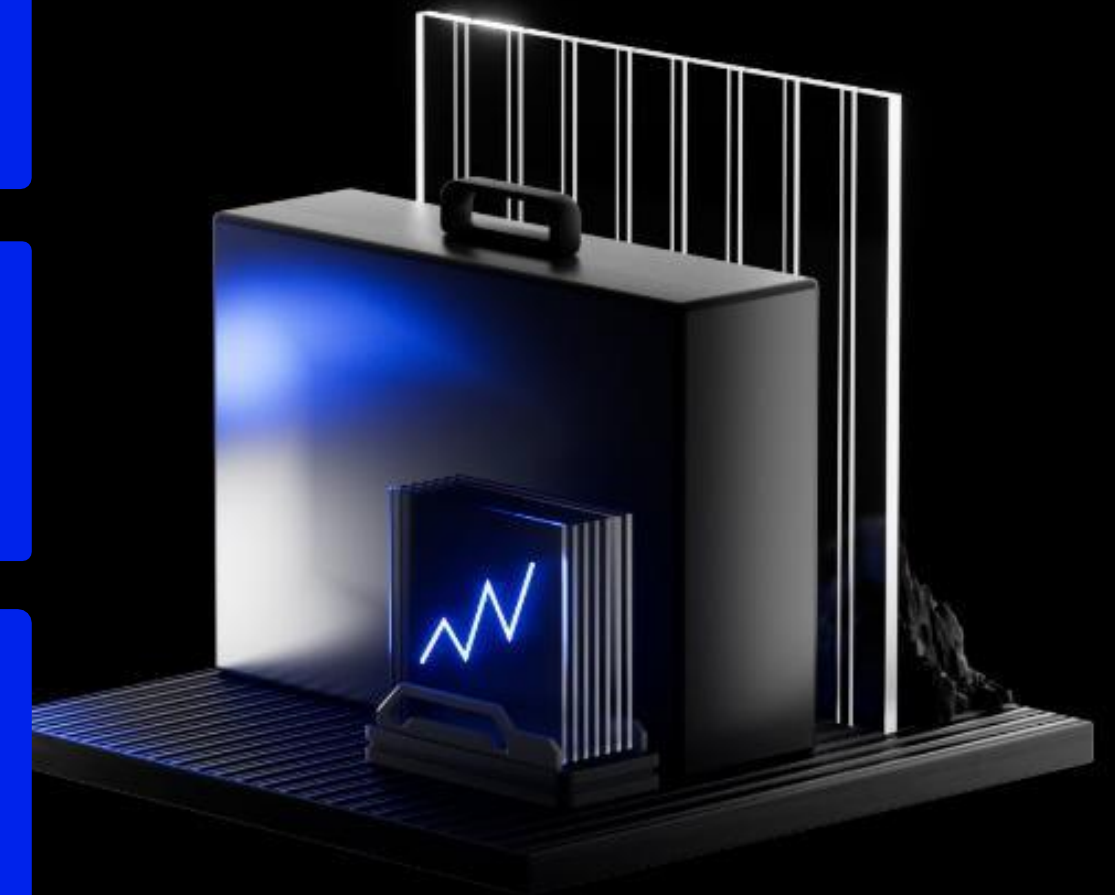
In addition to CI0P's activities, other actor groups continue to be active in attacks against Australia and New Zealand. 'New' names such as **Lynx**, and notable names such as **IncBlog**, **Qilin** and **DireWolf** announced multiple ransomware attacks to organisations of various industries, including **Esperance Communications**, **Brinks NZ**, **St. Josephs College**, **Echuca** and **Regis Resources**.

03

DDoS and Hacktivism activities during the month

There were two Hacktivism events in January- **Z-Pentest's** reported OT access to **AQUACORP**, as well as the attack on Victoria Police referenced in this report.

Australia and New Zealand recorded a single DDoS event during January- the HellR00ters Team claimed an attack on Victoria Police. Looking further abroad into Oceania, Team BD Cyber Ninja claimed defacement attacks on multiple domains. The attackers shared mirror links on Haxor ID as evidence of their actions. [More information on Group-IB Threat Intelligence Portal](#).



LOCAL INSIGHTS (Australia)

Local Insights from Group-IB with a brief description:

04

Sale of scraped data claimed to belong to Linktree profiles

On January 15 2026, a newly registered **breachforums** user with the nickname **tree_lover** created a thread announcing the sale of **SCRAPED** data they claimed to have obtained through enumeration on an exposed endpoint of **Linktree**. Linktree is an Australian link-in-bio platform allowing to build a landing page where one can put multiple social media / shop and other promo links. This data would assist in OSINT investigations as it has the ability to link people's social medias together. A detailed report is available in the **Group-IB [portal](#)**.

05

False Alarm: Database Australia Data Leak is a rebrand of the 2021 Oxfam Leak

During January, **Group-IB** has observed many reports from across the Darkweb of a **Database Australia- National Personal Data Leak**. Following a thorough investigation, **Group-IB** has determined that the data is a re-branding of data obtained during the **Oxfam** leak in 2021. Detailed information of these events is available in the Darkweb section of the **Group-IB [portal](#)**.

06

AUKUS & USA Department of Defense Data Breach

On Jan 12, 2026, Threat Acto **Kraxs** posted a thread on **breachforums** advertising allegedly compromised data from the **USA DoD** and **AUKUS** for sale. No sample data has currently been published. The thread also claims to be selling information pertaining to national government planning and assessments of regional tensions including the Ukraine conflict, Taiwan, South-East Asia as well as **US Space Force** and **AUKUS** weaponry.

Detailed information of this event, including recommendations, is available in the Last Threats section of the **Group-IB [portal](#)**.



RANSOMWARE ACTIVITIES



Key Events – January 2026

- The global ransomware landscape experienced a sharp **46% decrease** in activity during January 2026, with total recorded attacks dropping to **54**, down from the **100** incidents documented in December 2025.
- **Qilin** maintained its position as the most prolific ransomware group with **16 successful attacks**. Conversely, **The Gentlemen** bucked the downward trend by increasing their activity by **33.3%**, even as competitors like **Dire Wolf** significantly scaled back operations.
- The **Manufacturing sector** remained the primary focus for cybercriminals, accounting for approximately **28% of all monthly incidents**. Other highly targeted industries included **Professional Services** and **Consumer Electronics**, reflecting a continued interest in high-value supply chain targets.
- A notable shift in regional targeting saw **Malaysia** emerge as the top-targeted country globally. This represents a pivot away from previously high-volume regions like **India** and **Thailand**, which saw a marked reduction in ransomware pressure during this period.

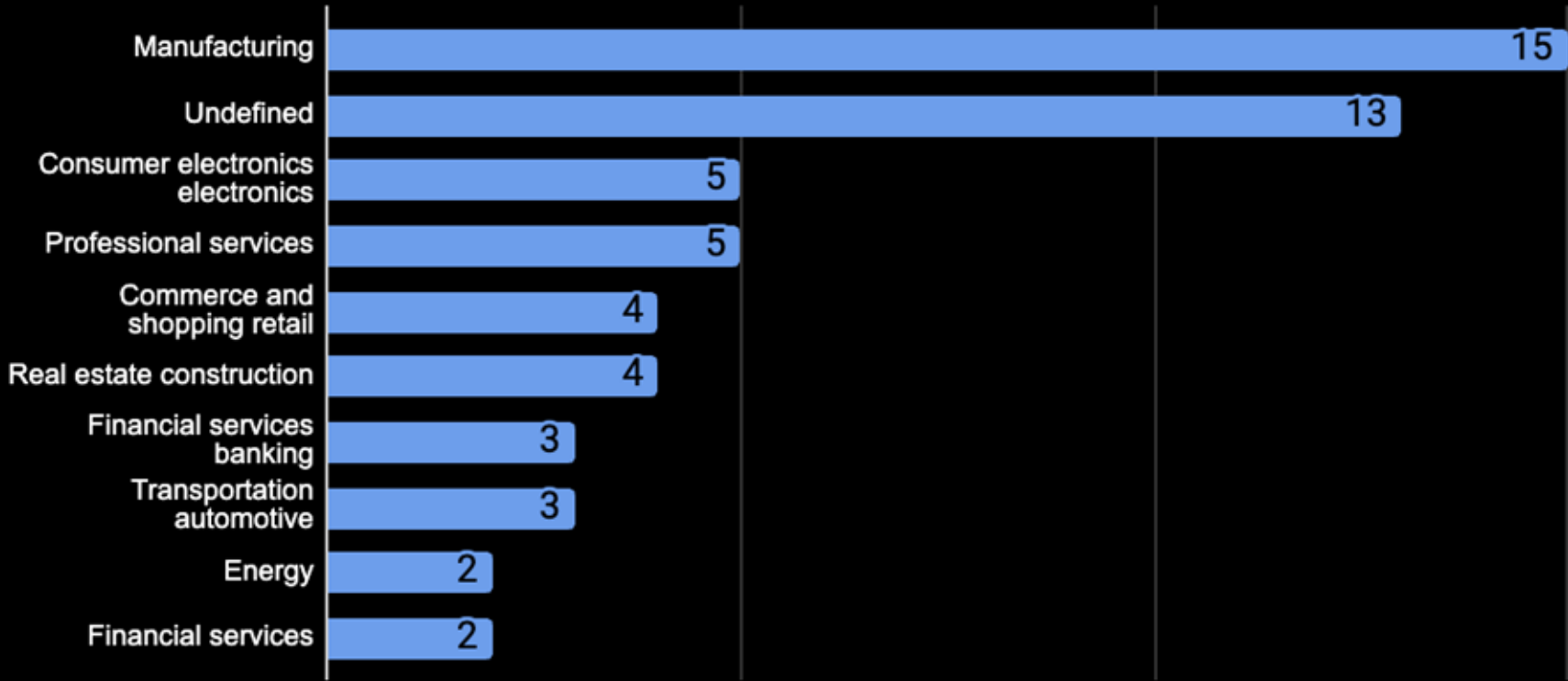
RANSOMWARE ACTIVITIES

Key Events – January 2026

54 Incidents ↓16%

Data: Number of Non-Unique Events and Activities (with Updates)

Ransomware attacks, per industry



Most Active Threat Actor Groups

Qilin		The Gentlemen	
16 activities		8 activities	
↓ 5%		↑ 33%	
Dire Wolf	DragonForce	NightSpire	Obscura
5 activities	3 activities	3 activities	3 activities
↓ 54%			

Most Targeted Countries

Malaysia		Thailand	
11 activities		9 activities	
↓ 15%		↓ 10%	
Taiwan	China	India	Japan
8 activities	5 activities	5 activities	4 activities
		↓ 61%	↓ 66%

RANSOMWARE ACTIVITIES (Australia and New Zealand)

↑ 42.86%

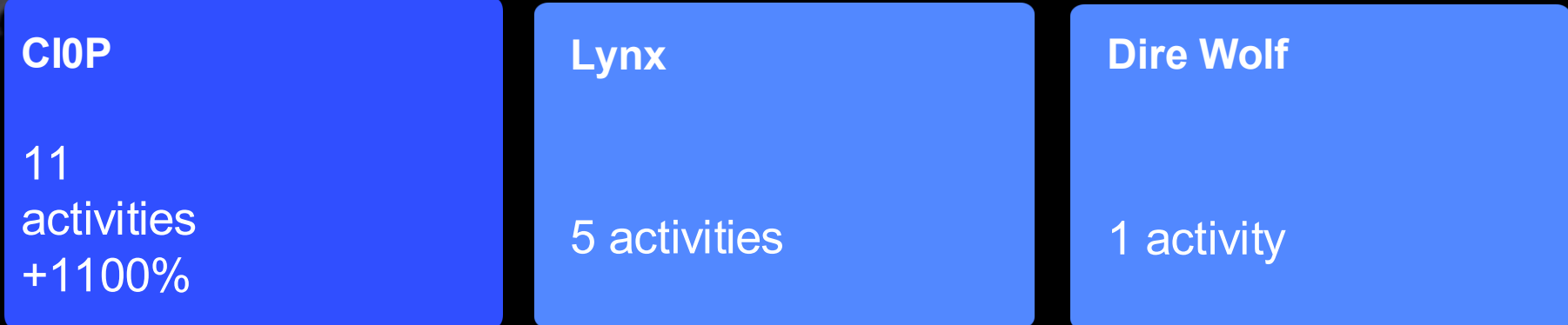
GROUP-IB

20 ransomware incidents

Statistics regarding ransomware activities in January 2026:

- **Australia** remains out of the top 5 countries globally from January sitting in 6th place globally, with a number of ransomware attacks, including 11 claimed by **CIOP**, up from zero in December 2025.
- The most notable incidents were **CIOP's** Ransomware of several companies, including **Etto Australia, Podiatry WA & NextPhaze**. **CIOP** continues to operate across APAC, where they announce their intention to disclose files through a post on the group's leak site (DLS). The Threat Actors allegedly published evidence of the breaches and threatened to release sensitive data if their demands are not met.
- Although case-specific TTPs and IOCs are restricted, IOCs of this actor collected from previous incidents can be found on the Threat Intelligence Portal.
- 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)

Hactivism is the use of hacking to promote political or social agendas. Usually hactivist groups are low-skill hackers who perform DDoS, Defacement, and Data Breaches (mostly leverages compromised accounts) attacks. Unfortunately, during the last year these groups attracted a lot of attention.

In **Australia**, 2 Hactivism incidents were recorded in January 2026.

The Group-IB Threat Intelligence team reported that the TA **Z-Pentest Alliance** claimed a successful attack on Aquacorp's control systems. The attacker has access to sanitization schedule settings, time and level settings, and alarm and warning history.

In December 2025's Digital Risk Protection (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. The attacker gained full control over the pumps and liquid delivery parameters, exploiting weak control interface protection. The system's vulnerabilities included remote access to pump controls and unprotected setpoint changes, allowing for covert tampering without triggering alarms. **Z-PENTEST ALLIANCE** or **Z-Pentest** is a pro-Russian hactivist group responsible for mostly DDoS and Deface attacks. Group also performs hybrid attacks targeting ICS systems in targeted regions, when they try to disrupt the operation of industrial systems by abusing management and control interfaces of these systems that are available either without proper authentication or after attackers allegedly gained initial access using brute force attacks. Their MITRE ATT&CK Methods include: **Exfiltration Over Alternative Protocol**, **Exfiltration over C2 Channel**, **Exfiltration Over Web Service**, **Defacement** and **Network Denial of Service**.

A single DDoS/ Hactivism incident was reported for Australia in January 2026. The TA **HellR00ters** claimed a DDoS attack on **Victoria Police** on January 1st, 2026. The MITRE ATT&CK used was **Network Denial of Service**.

No DDos or Hactivism events were reported for New Zealand for January 2026.

COMPROMISED ACCOUNTS

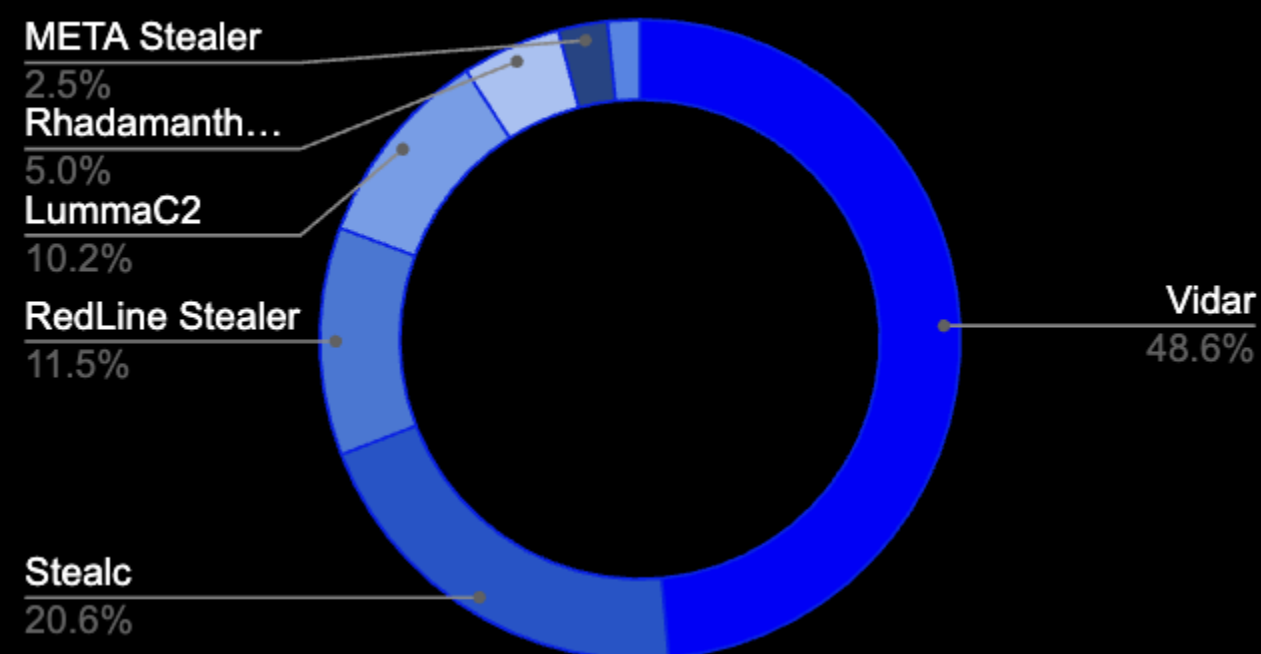
Key Events – January 2026

- In January 2026, the number of compromised accounts reached 6,050,369, representing an 8.96% increase from the 5,553,033 accounts recorded in December. Vidar remained the dominant malware threat, responsible for nearly half of all compromises with 3,738,151 accounts, followed by Stealc (1.58 million) and RedLine Stealer (887,807).
- Geographically, India was the most impacted nation with 1,974,036 compromised accounts, accounting for 32.6% of the global total. Other significant hotspots included Indonesia (965,682 accounts), Vietnam (725,174 accounts), and the Philippines (626,938 accounts), highlighting a heavy concentration of infostealer activity across South and Southeast Asia.

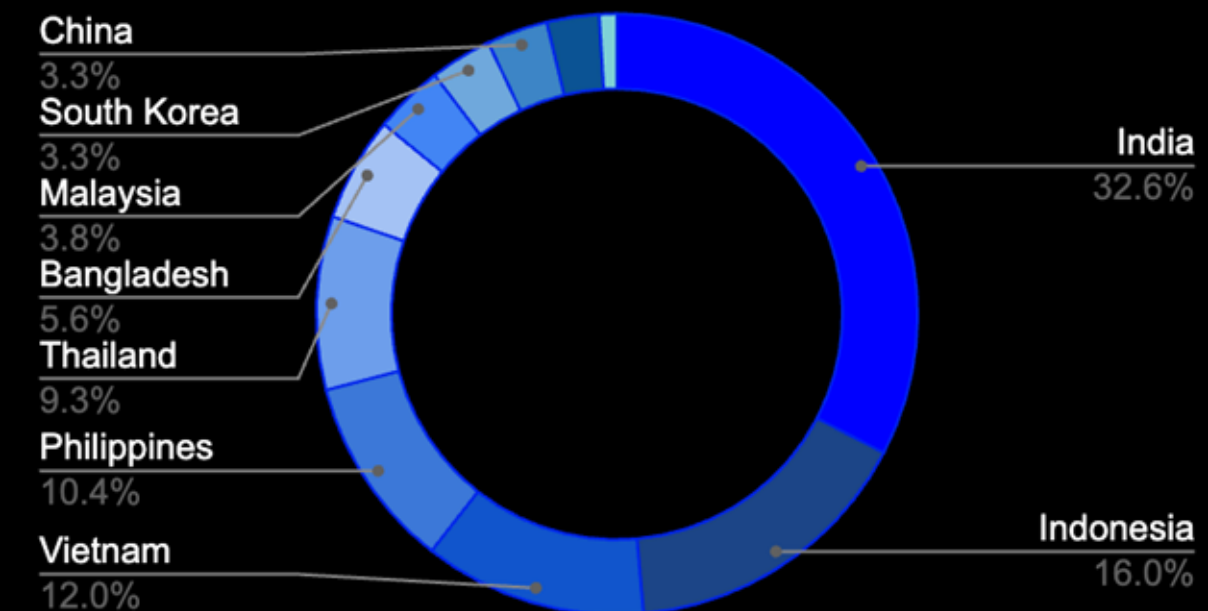
6,050,369 data leaks ↑ 8.96%

Data: Number of Events. Each malware can be part of the same event.

Compromised Accounts by Malware



Compromised Accounts by Country



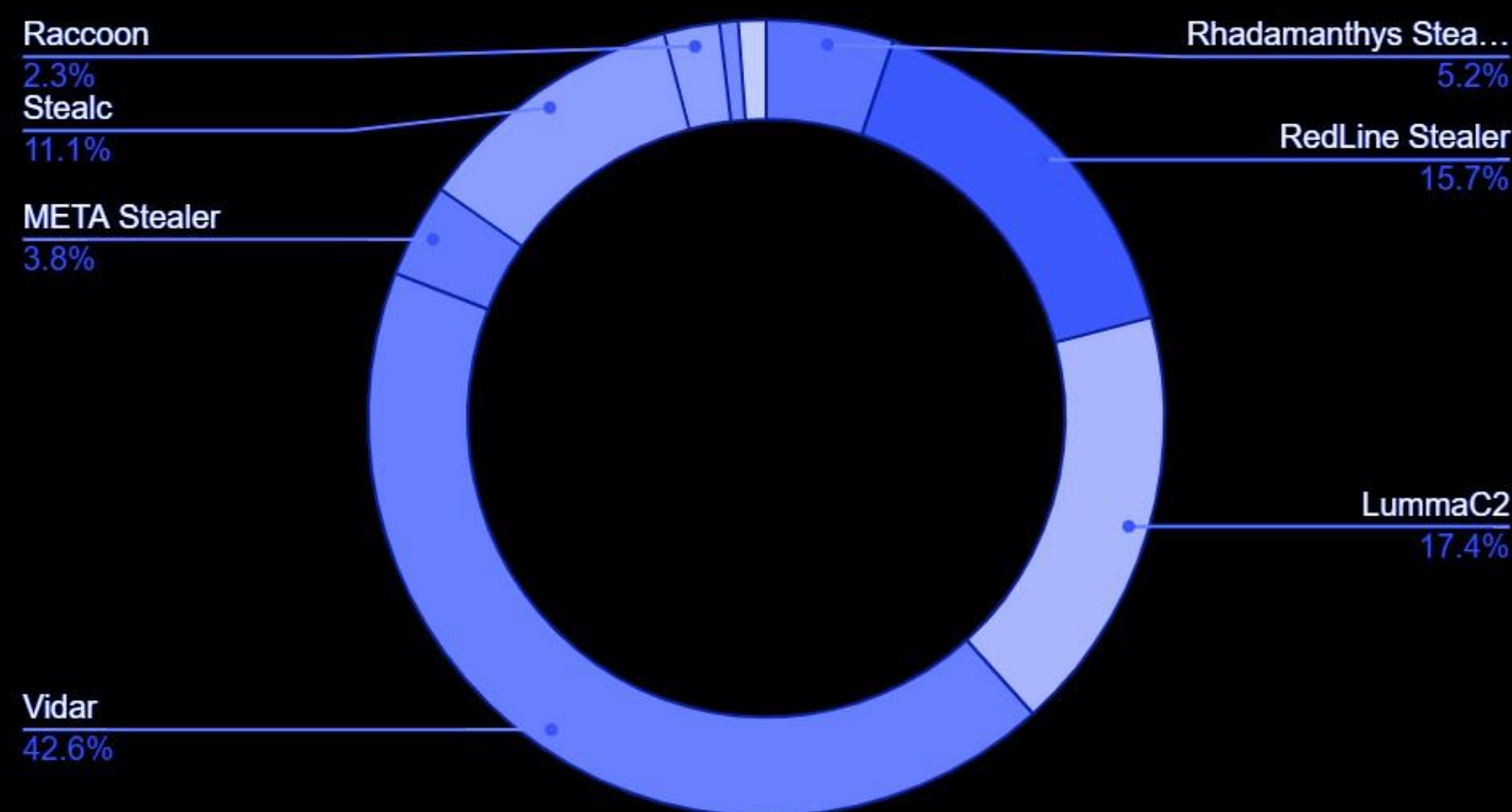
COMPROMISED DATA (Australia & New Zealand)

↓ 13.86%
215,584 account compromises

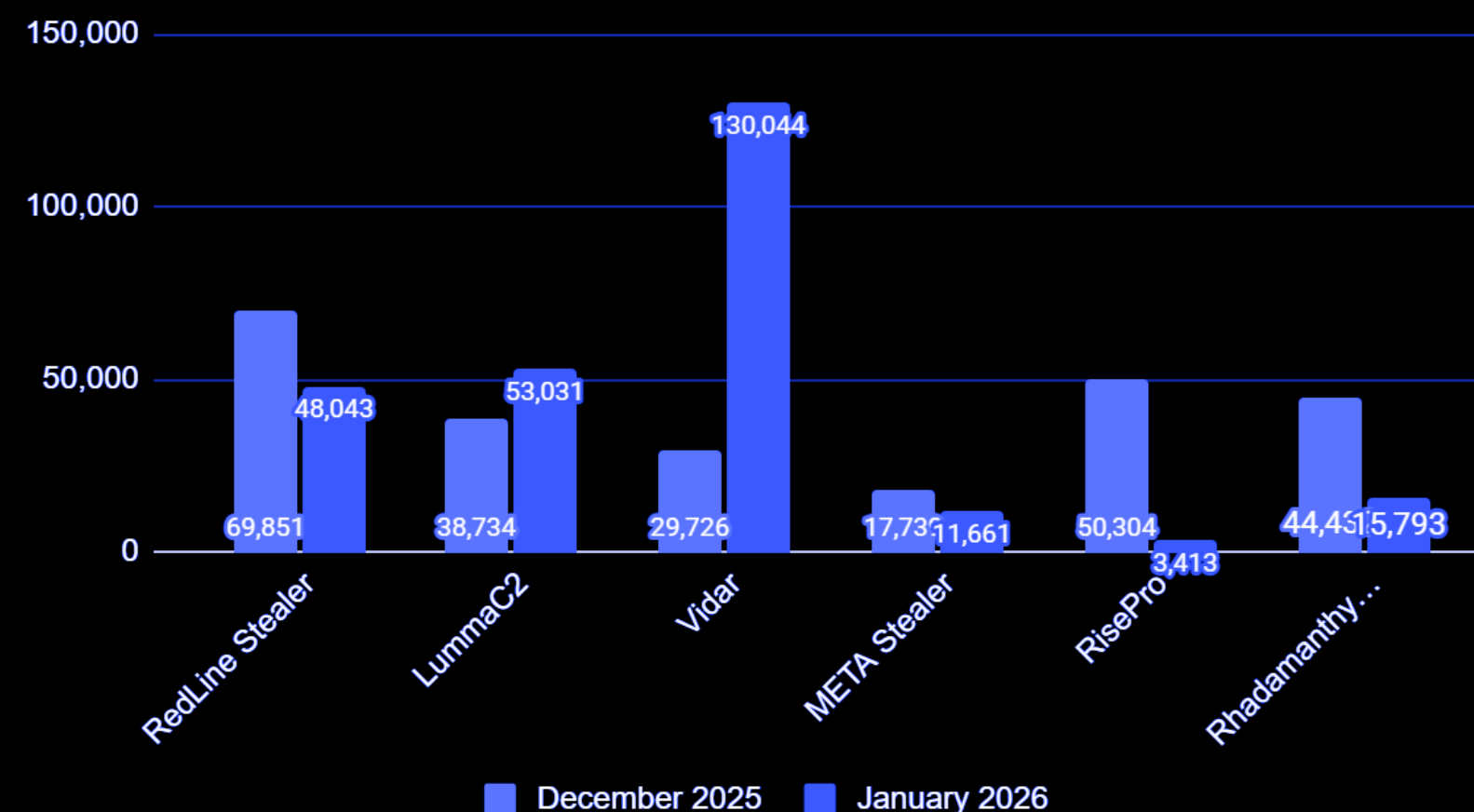
Statistics regarding compromised accounts in January 2026:

- Serious reductions of **Risepro**, **META Stealer** and **Rhadamanthys Stealer** activities are responsible for the large drop in Malware activity in January.
- **Vidar**, **RedLine Stealer**, **LummaC2** and are the top malware families responsible for 75.75% of the compromised accounts in Australia/ New Zealand during the month.
- The overwhelming majority of leaked data was from Vidar this month, which is primarily distributed through **private channels**, and **Boxedrobot** followed by **WlfrSpecialCloud** and **private supergroups**. Most affected accounts this month are associated with domains belonging to **Roblox**, **Google**, **Discord** and **Facebook** and **Discord**.

Top Malware for Compromised accounts



Malware Activity Comparison, Dec 2025 - Jan 2026



COMPROMISED BANK CARDS

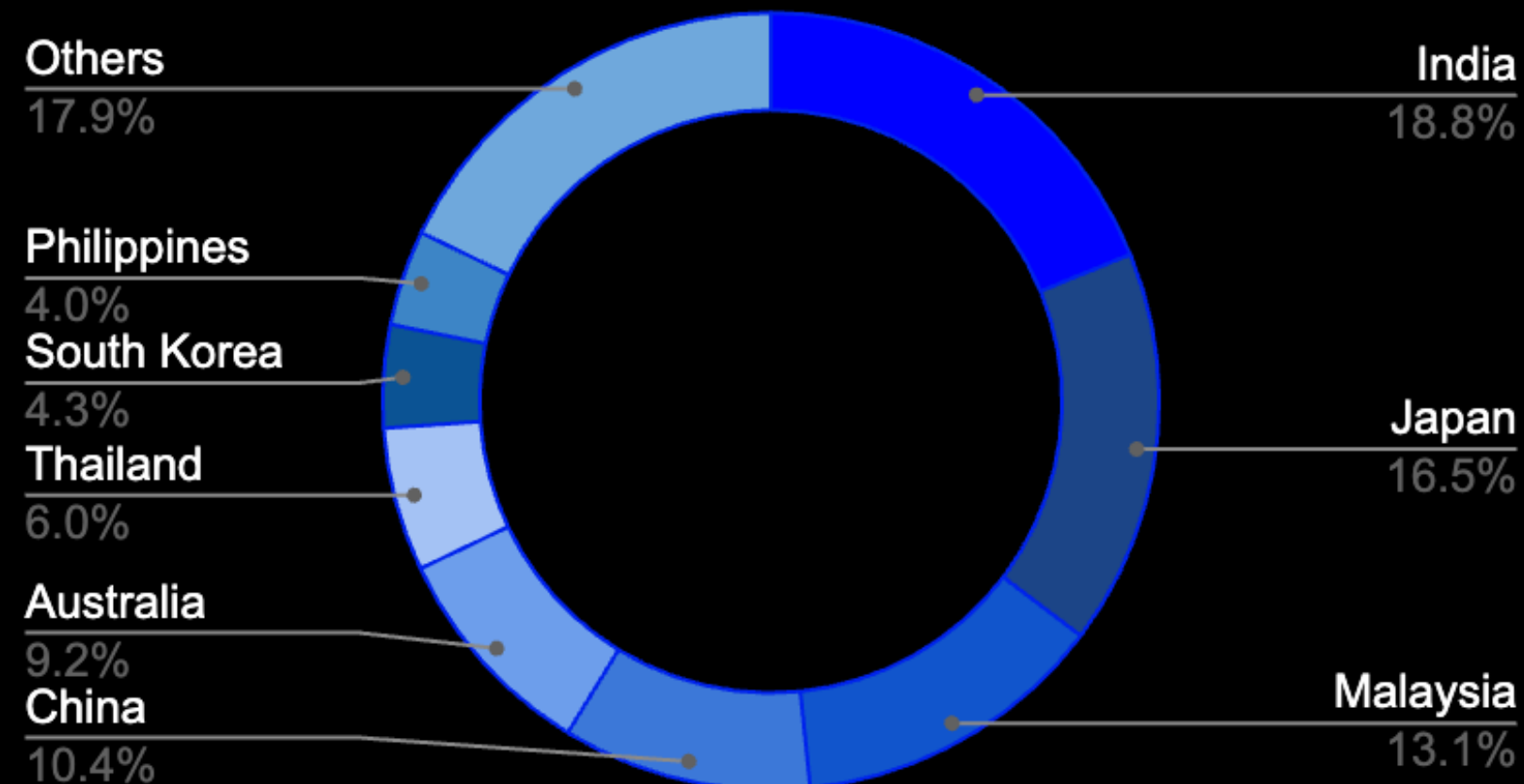
Key Events – January 2026

- In January 2026, the volume of compromised bank cards saw a significant 17% decline, dropping to a total of 47,245 incidents. This activity was heavily concentrated in the Asia-Pacific region, with Malaysia, India, and Singapore emerging as the primary targets. The distribution of this stolen data is increasingly centralized on Telegram, which serves as the leading source for nearly 40% of all compromises, followed by cybercrime forums and direct data leaks.

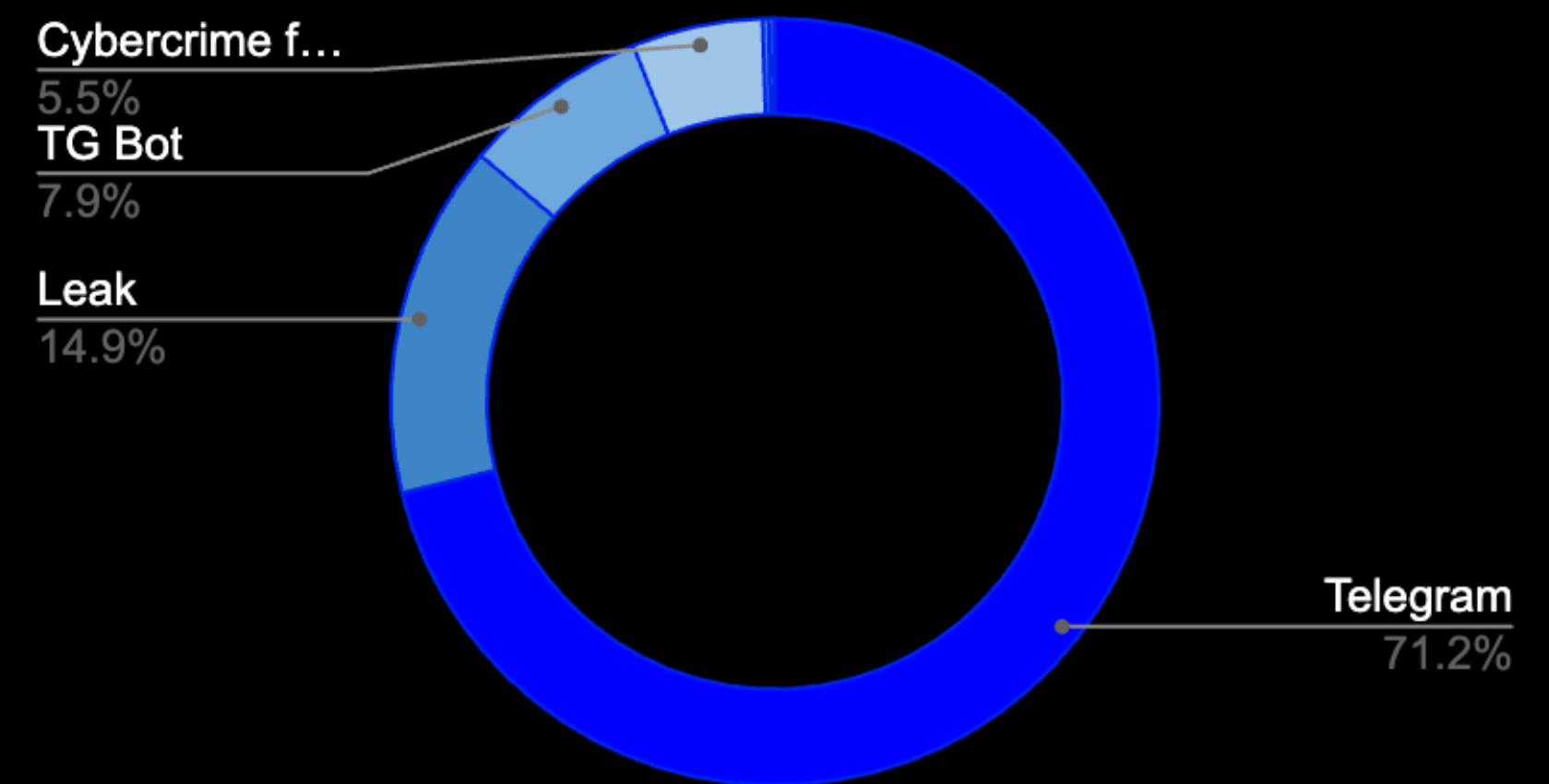
47,245 bank cards leaked ↓ 16.96%

Data: Percentage of Events

Compromised Bank Cards by Country



Compromised Bank Cards by Source Type



COMPROMISED BANK CARDS (Australia and New Zealand)

↑ 96.48%

Statistics regarding compromised accounts in January 2026:

- **Australia** has moved up to 7th place of the countries with compromised cards during the month, after placing 10th in December 2025.
- The majority of leaked card data came from Telegram, Cybercrime Forums and Leaks
- 54% of the compromised cards came from Mastercard this month, followed by Visa (43%), with a small amount from both American Express. Diners Club international and Maestro each had under 10 compromises.



Data: number of events. Each malware can be part of the same event.

ADVERSARY OF THE MONTH

(Australia and New Zealand)



Threat actor group

CI0P

Targeted industries:

- | | |
|------------------------|------------------------------|
| Financial services | Oil & Gas |
| Manufacturing | Consumer Electronics |
| Software | Printing |
| Commerce and shopping | Textiles |
| Professional Services | Non-profits |
| Information Technology | Transportation |
| Healthcare | Accounting |
| Food & Beverage | Freight Services |
| Chemical | Hospitals |
| Banking | +391 Other Industries |

Period of Activity: 2019 - Present

Targeted countries: Australia, United States, Canada, Germany, United Kingdom, India, France **+54 others**

Attribution: Ransom and data extortion with Dedicated Leak Sites (DLS)

Intent: Financial Gain

Attack Summary

CI0P is a cybercrime group discovered in February 2019. CI0P is one of the largest ransomware groups in history.

They conducted 11 successful attacks in Australia in January 2025.

Clop ransomware encrypts user's sensitive files and then demands a ransom in BTC to return the files.

Key Observations

The attacker uses Clop ransomware for attacks. Most recently, Get2 downloader has been used for downloading SDBbot backdoor which is used for reconnaissance and lateral movement in the victim's network.

Impact profile: Large ransom demands, including 973 Data Encrypted for Impact events.

Further information, including Indicators, can be found at the following [link](#).

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.

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003