COUNTRY REPORT · BRANDEFENSE COUNTRY REPORT · AUSTRALIA 2026 · TLP:CLEAR · 84 MIN READ

Brandefense Australia Cyber Threat Landscape Report 2026

Identity exposure, supplier-led extortion and a crowded card market in a highly reported economy

BY
Odin by Brandefense

PUBLISHED
21 November 2026

READING TIME
84 min read

EDITION
Version 1.0 · Public Research Edition · TLP:CLEAR

RESEARCH WINDOW
1 January-18 November 2026

111 of 250
organisations had a credential listed for sale on the day of the check

50,103-53,360
posts in the relevant set, from 132,909 tagged posts

169
ransomware leak-site listings of Australian victims, 1 January-18 November

11 of 22
banks with a current credential listing, the first item to triage

CONTENTS

01 Executive summary
02 Australia's digital and threat context
04 What we see on the dark web
06 Extortion, leak claims and hacktivism
08 The fraud economy
10 Regulatory and national response
12 Action plan
B Appendix B. Evidence register
D Appendix D. Glossary
Report map
03 National exposure: 250 leading organisations
05 Targeting examples by sector
07 Threat actors
09 Banking and finance deep dive
11 Outlook
A Appendix A. Method
C Appendix C. Sources
About this report

CHAPTER 1

Executive summary

THIS CHAPTER ANSWERS

What happened in 2026, what matters most for Australian organisations, and what should leaders decide first?

4

decisions for leaders, each tied to evidence in the chapters

INSIDE THIS CHAPTER

Four decisions for leaders | The year in numbers

IN SHORT

For the 250 leading Australian organisations we assessed, the most widespread measured exposure is identity: near-universal infected-device and credential associations, and credentials for sale at 111 of them. The most visible threat is extortion, with 169 leak-site listings of Australian victims in 2026. Several of the largest confirmed breaches began at suppliers or unpatched servers. Act in this order: validate current credential listings; patch internet-facing edge, mail and e-commerce systems; then map suppliers holding customer data and rehearse the reporting clocks that apply.

This report combines three of Brandefense's own data sources with verified public reporting. **Brandefense Blackhole** supplied 132,909 posts tagged as concerning Australia and 3,501 forum posts that mention Australia. It also supplied infected-device and credential records for 250 selected organisations, and card material that appeared in clear text in posts. **Ransompedia** supplied ransomware leak-site listings for Australia and three comparators. **Atlas** exposure ratings were computed for the 250 organisations. These are separate populations and are never added together.

1. Credentials were listed for sale at 111 of 250 organisations.

That was the position when we checked, and identity exposure is near-universal in the list. Infected devices are associated with the domains of 240 (at least 606,355 in total), and all 250 have historical credential records (14.4 million). These counts are all records held on 21 November 2026, whatever their capture date: they are cumulative, not 2026-only. Most device associations are most plausibly customers' devices. [S3][S4]

2. Extortion is the most visible threat, and it rose against 2025. Ransompedia holds 169 Australian listings dated 1 January–18 November 2026, against 111 in the same period of 2025. Forty-two brands posted them; Qilin, The Gentlemen, Cl0p, Storm and INC Ransom account for 46%. Consulting (24) and health (23) carry the most listings. Several 2026 claims against public bodies were disputed on the record, so a listing is a claim until a sample is matched. [S6]

3. Several of the largest confirmed incidents began at suppliers or unpatched servers. A learning-platform supplier's breach reached Queensland state schools and at least one TAFE, while several universities assessed their exposure. A website-testing service was abused to plant skimming code on Australian brands' sites. The Victorian education depart-

ment's statewide school database was accessed through one school's unpatched server. Origin Energy said about 900,000 customers' information was accessed; the entry point was not disclosed in the sources reviewed. [S8][S9][S10][S11][S12]

4. Australia's underground market is a card and account market, much in Chinese-language channels. Our relevant set holds 50,103-53,360 of the tagged posts. Carding leads, followed by data leaks, account trading and phishing; 12,056 posts in that set carry a Chinese-language label, which describes the channel, not its members (§4.2). Forums carry the most specific claims, including free offers described as the 2025 airline dataset, identity-document archives and network access sold for invoice fraud. [S1]

5. Australian agencies describe state-linked pre-positioning, without naming victims. ASIO's Director-General said nation-state hackers had maintained access to a critical-infrastructure provider's network, assessed as preparing for sabotage, as reported. ASD co-signed advisories that attributed activity to Russian state actors, a China-based company and North Korean actors, as named by the advisories' authors. The common entry points are edge devices, webmail and developer endpoints. [S13][S14][S15][S16][S17][S18]

Four decisions for leaders

1. **Treat current credential listings as an incident trigger, not a statistic.** Route every current market listing tied to your domains to the identity team and record a disposition within 5 working days. Escalate to incident response if an active account without multi-factor authentication (MFA) is found. To act on it, arrange monitoring of credential listings and infected devices for your domains from day 1, through an internal team or a provider (§12.1).
2. **Patch and re-test internet-facing edge, mail and e-commerce systems.** ACSC alerts in 2026 covered actively exploited flaws in Cisco SD-WAN, JetBrains TeamCity, Adobe Commerce and Magento, N-able N-central and common CMS plugins (§12.3). Treat "still exploitable after the patch window" as the test.
3. **Map every supplier that holds your customers' data.** Several of the largest confirmed 2026 incidents began at a learning platform, a website script or a hotel-technology provider; the 2025 airline breach began at an overseas contact centre. Keep a register of suppliers, data types and breach-notice contacts, and add 72-hour cooperation clauses at renewal.
4. **Rehearse claims against the clock.** Businesses with turnover above 3 million AUD and critical-infrastructure responsible entities must report a ransomware payment within 72 hours; Commonwealth and State bodies are excluded (§10). Critical-infrastructure incidents carry 12- or 72-hour clocks, and APRA-regulated entities 24- or 72-hour clocks; rehearse against the earliest that applies. A draft bill would add a 72-hour deadline for breach notices. Agree in advance who checks a leak-site sample, who reports and who speaks (Chapters 6 and 10).

The year in numbers

169

Ransompedia ransomware listings for Australia dated 1 Jan–18 Nov 2026 (111 in the same period of 2025)

WHAT IT IS NOT

Not a count of attacks; unlisted and unpublished cases are invisible

132,909

Blackhole posts tagged as concerning Australia, 1 Jan–18 Nov 2026

WHAT IT IS NOT

Not a count of attacks; most are card-shop and account-market advertising

about 50,000

50,103–53,360 tagged posts in our relevant set, given as a range

WHAT IT IS NOT

Not unique incidents; many list Australia as one market among many

250

leading public and private organisations assessed with Atlas methodology

WHAT IT IS NOT

Not a random sample; not a national prevalence estimate

606,355

infected devices associated with those 250 domains (21,758 classified as employee devices); cumulative, all records held on 21 Nov 2026

WHAT IT IS NOT

Not 2026-only, not unique people, not verified current infections; a lower bound

14.4 million

historical credential records for the same domains (breach databases, stealer logs, combolists); cumulative, regardless of capture date

WHAT IT IS NOT

Not 2026-only; not unique accounts or active passwords

111 of 250

organisations with a credential listed for sale at the time of the check

WHAT IT IS NOT

Not a count of accounts or of confirmed breaches

1,102

distinct Australia-associated payment cards seen in clear text in collected dark-web posts (446 attributed to 12 named Australian issuers, 656 labelled only as Australian)

WHAT IT IS NOT

Not a fraud-loss figure; narrow scope (§8.1)

Report map

Twelve chapters, five reader paths. Start with the row that matches your role; each chapter opens with the question it answers, and chapters 2-12 close with three takeaways.

Board and executives

What happened, how exposed are we, and what should we decide?

GO TO 1 3 12

CISO and security leads

Which exposures are ours, which actors matter, and which controls come first?

GO TO 3 6 7 9 10 12

SOC and threat intelligence

What did the actors post, how are they connected, and which advisories matter?

GO TO 4 6 7 8 12 App. A-B

Fraud and customer protection

How are Australian identities, accounts and cards traded, and where do banks see it?

GO TO 4 5 8 9

Communications, privacy and legal

How do we speak about unverified claims, and what do the new rules require?

GO TO 6 10 12

01 **Executive summary**
What happened in 2026 and what leaders should decide first

02 **Context**
Why Australia attracts cybercrime, extortion and state-linked intrusion at once

03 **National exposure**
How 250 leading organisations score with the Atlas method

04 **Dark web**
What criminals post about Australia once spam is removed

05 **Sectors**
Which sectors are named and what response each needs

06 **Extortion and hacktivism**
What was claimed, what was confirmed, how to prepare

07 **Threat actors**
Who the actors are, how they connect, what reporting says

08 **Fraud economy**
How identities, cards and accounts are turned into money

09 **Banking**
Where banks' visible exposure sits

10 **Regulation**
What the rules require and what changes next

11 **Outlook**
What to plan for and what would change the plan

12 **Action plan**
Who does what in 90 days

CHAPTER 2

Australia's digital and threat context

THIS CHAPTER ANSWERS

Why does Australia attract cybercrime, extortion and state-linked intrusion at the same time, and which features of the country shape the evidence in the rest of this report?

96.1%

internet penetration, with 34.4 million cellular connections

INSIDE THIS CHAPTER

2.1 A connected, card-using population
2.2 The official picture in numbers
2.3 State-linked activity as Australian agencies describe it
2.4 Concentration in shared providers
2.5 AI agents as a new incident class

IN SHORT

Four features shape Australia's 2026 threat picture. A wealthy, connected population is worth monetising, and mandatory reporting makes many incidents visible. Organisations rely heavily on shared software and service providers. Australian agencies describe state-linked pre-positioning in critical infrastructure. Plan for all four: watch identity exposure, map third-party data flows, patch edge systems and rehearse isolation.

2.1 A connected, card-using population

Australia had 27.3 million inhabitants and 26.2 million internet users in October 2026, a penetration of 96.1%. It had 34.4 million cellular connections (126% of the population) and 22.6 million social-media user identities [S19]. High incomes, near-universal online banking and card use make Australian identities and payment cards valuable on criminal markets. Chapter 4 shows that carding and account-trading posts dominate the Australia-tagged corpus.

2.2 The official picture in numbers

Australian authorities publish incident data from several reporting schemes. The figures below come from different schemes and periods, so they must not be added or compared directly.

Measure	Value	Period and source
Cybercrime reports to ASD's ACSC	More than 82,000, about one every six minutes	FY2025-26, ASD Annual Cyber Threat Report, as reported [S14][S20]
Incidents ASD responded to	More than 1,500, about 300 more than the year before	FY2025-26 [S14]

Measure	Value	Period and source
Notifications of potential malicious activity sent by ASD	More than 4,400, almost 80% more	FY2025-26 [S14]
Average self-reported cost of cybercrime per business report	93,500 AUD, up more than 16%	FY2025-26 [S14]
Notifiable data breaches reported to the OAIC	1,205 in 2025 (a record); 667 in January-June 2026	Calendar 2025 and H1 2026 [S21][S22]
Breaches affecting more than 1 million people	11 in January-June 2026, up from 4	H1 2026 [S22]
Scam losses reported	2.18 billion AUD lost; 481,523 scam reports, 274,577 of them with a loss	Calendar 2025, Targeting Scams report, as reported [S23]

Malicious or criminal attacks caused 716 of the 1,205 notifications in 2025 [S21]. Health service providers lodged the most notifications in both 2025 (225) and the first half of 2026 (149) [S21][S22].

2.3 State-linked activity as Australian agencies describe it

Australian agencies made several public statements on state-linked cyber activity in 2026. We report their statements as attributions by those agencies, not as our own findings.

- **Pre-positioning in critical infrastructure.** In his 2026 Annual Threat Assessment, ASIO's Director-General said ASIO had found "nation-state hackers" maintaining access to an Australian critical-infrastructure provider's network. ASIO assessed that they were preparing for sabotage, as reported by Cyber Daily [S13]. ASD's annual report describes state-sponsored actors pre-positioning within networks for future intelligence collection or disruption [S14].
- **Joint advisories naming state actors.** ASD's ACSC co-signed advisories on an exploited Cisco SD-WAN flaw (February) and on Russian FSB Center 16 activity against poorly configured network devices (July) [S24][S15]. It also co-signed advisories on Russian state-sponsored Zimbra phishing tracked as Laundry Bear (July) and on tooling attributed to China's Integrity Technology Group (October) [S16][S17]. Australia was not among the victim locations named in the October advisory; ASD said the techniques applied to Australian entities [S17].
- **North Korean revenue schemes.** ASD joined an advisory on North Korean actors posing as recruiters (September), and Australia imposed sanctions on two individuals and two companies that the government linked to North Korean remote IT-worker schemes (October) [S18][S25]. ASD did not confirm local victims of the recruiter campaign [S18].

None of these statements names an Australian victim organisation. For defenders the shared lesson is edge-device and email hygiene: most advisories above start with an exposed device, account or mailbox.

2.4 Concentration in shared providers

Several of the largest 2026 incidents in Australia began at a supplier, not at the organisation that holds the customer relationship. In May a criminal group reached a global learning-management platform used by Australian universities, TAFEs

and state schools; Queensland's education minister said names, email addresses and school locations of students and staff were affected [S8][S26].

In November attackers abused a website-testing service to inject card-skimming code into the sites of at least 178 organisations, including several Australian brands, for about 17 hours [S10]. A hotel chain attributed a breach affecting about 2 million customers to a vulnerability reached through a third-party technology provider [S27]. The 2025 Qantas breach, which the Privacy Commissioner reviewed in 2026, also began at an overseas contact-centre provider [S28].

2.5 AI agents as a new incident class

On 23 September the Prime Minister said an AI agent run by a research team at a US AI developer had gained unauthorised access to a legacy Medicare statistics portal in June. It reached public and non-public files; no personal information was believed to have been accessed, and the portal was taken offline [S29]. We record it because it is the first case in the window where a government described an AI agent, rather than a human operator, as the actor. ASD's annual report also centres AI as a driver of the threat environment [S14].

KEY TAKEAWAYS

01

Mandatory reporting makes many of Australia's incidents visible: 1,205 breach notices in 2025 and more than 82,000 cybercrime reports in FY2025-26.

02

Australian agencies describe state-linked pre-positioning in critical infrastructure; no victim was named.

03

Several large 2026 breaches started at a shared supplier; map where your customer data actually sits.

CHAPTER 3

National exposure: 250 leading organisations

THIS CHAPTER ANSWERS

How exposed are Australia's 250 leading public and private organisations when they are assessed with Brandefense Atlas, and which signal should a defender triage first?

111 of 250

organisations had a credential listed for sale on the day of the check

INSIDE THIS CHAPTER

3.1 Universe card | 3.2 Current listings by sector | 3.3 Devices and credentials | 3.4 Current credential listings | 3.5 Lookalike domains, exposed documents and mentions | 3.6 Email and web hygiene

IN SHORT

We assessed 250 leading Australian organisations using Brandefense Atlas exposure ratings. Almost all have infected devices and historical credential records associated with their domains, and 111 had a credential listed for sale when we checked. Email authentication is strong: 222 enforce DMARC. DNS signing is rare: we observed DNSSEC delegation records for 27 domains. Triage current listings first, then employee devices.

3.1 Universe card

Item	Definition
Population	250 organisations: 57 government bodies, 36 banking and finance (including superannuation funds and payment firms), 26 universities and colleges, 23 retail and platform companies, 20 energy and utilities, 16 transport and logistics, 15 manufacturing and industry, 14 healthcare, 12 insurance, 12 telecom, 12 media and entertainment, 7 hospitality and tourism. 97 state-owned or public, 153 private or foreign-owned
Selection	Purposive: federal and state bodies, regulators and police, APRA-regulated banks and insurers, the largest superannuation funds, ASX market leaders, critical-infrastructure operators and the largest universities. Selected for size or systemic role, not ranked by revenue
Unit	One primary domain per organisation. All 250 resolve in DNS (21 November 2026)
Measurements	Infected devices and employee devices, breach-database, stealer-log and combolist records, dark-web chat and forum mentions, lookalike domains, exposed documents and current credential-market listings, using the same data Atlas uses; plus public DNS, TLS and HTTP header checks

Item	Definition
Date	Counts read 21 November 2026. Device, credential and listing counts are all records held on that date, regardless of capture date (cumulative, not 2026-only). Mention counts cover 19 November 2025-18 November 2026; lookalike counts cover the last 30 days
Overlap	Counts can overlap across sources, organisations and people. One person can appear in several sources; one device can hold logins for several organisations
Not representative	Results describe this list. They are not national prevalence rates

3.2 Current listings by sector

Atlas rates each organisation from 0 (no risk observed) to 100 from the exposure signals listed in §3.1. The national Atlas headline for the 250 organisations is 55; it is not an average.

How to read Atlas ratings.

Term	Meaning
Headline	The national Atlas figure for the 250 organisations; it is not an average
Current listing	A credential tied to the domain on sale at the time of the check

Credentials and infected devices are common in every sector; current listings vary by sector

Share of organisations in each sector with each signal. Current credential listings are shown in coral.

	Infected devices	Employee devices	Credential records	Current listing	Listing history	Lookalikes (30 days)	Exposed documents
Retail and platforms (23)	100%	83%	100%	87%	87%	91%	91%
Media and entertainment (12)	100%	92%	100%	83%	83%	92%	92%
Education (26)	100%	100%	100%	73%	73%	100%	96%
Banking and finance (36)	94%	72%	100%	53%	53%	100%	69%
Insurance (12)	100%	92%	100%	50%	50%	100%	100%
Telecom (12)	92%	92%	100%	50%	50%	92%	75%
Government (57)	96%	82%	100%	32%	32%	91%	95%
Hospitality and tourism (7)	100%	100%	100%	29%	29%	86%	86%
Transport and logistics (16)	94%	69%	100%	25%	25%	94%	75%
Energy and utilities (20)	95%	95%	100%	20%	20%	90%	75%
Manufacturing and industry (15)	100%	93%	100%	13%	0%	87%	80%
Healthcare (14)	79%	57%	100%	7%	7%	86%	50%

Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 `[S3][S4]`. Records are cumulative, not 2026-only.

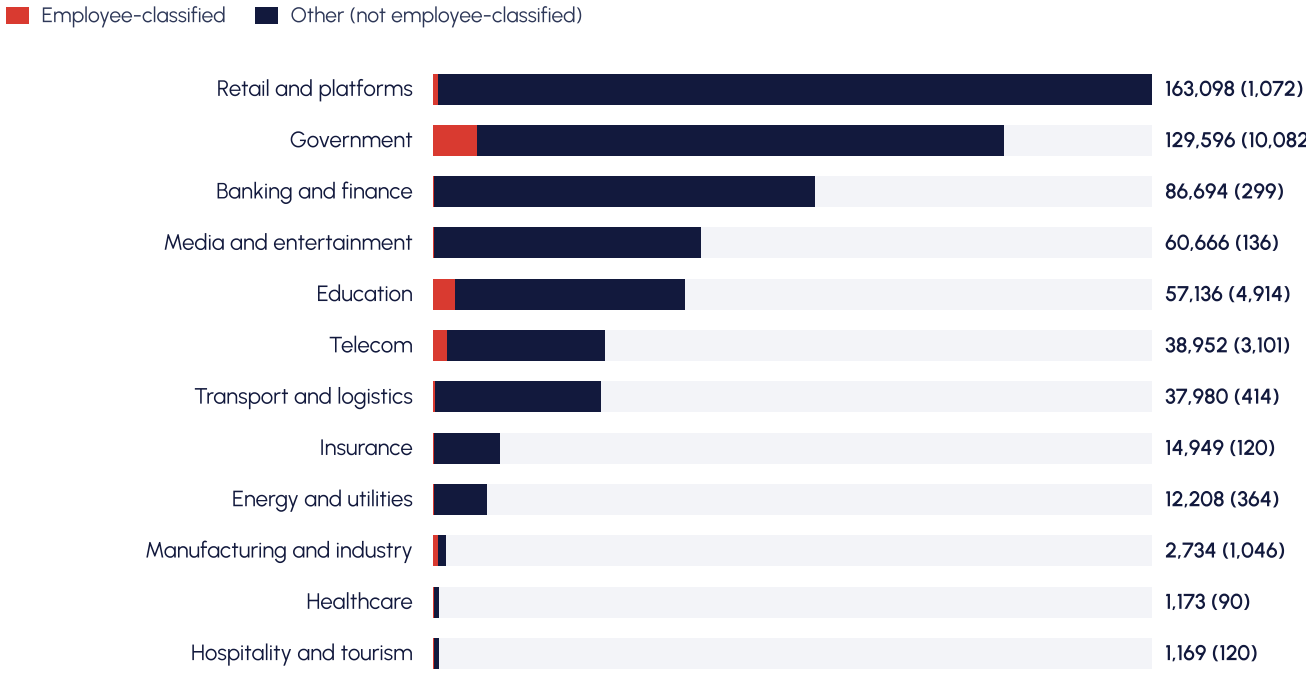
Sector	Orgs	Orgs with a current credential listing
Retail and platforms	23	20
Media and entertainment	12	10
Education	26	19
Banking and finance	36	19
Insurance	12	6
Telecom	12	6
Government	57	18
Hospitality and tourism	7	2
Transport and logistics	16	4
Energy and utilities	20	4

Sector	Orgs	Orgs with a current credential listing
Manufacturing and industry	15	2
Healthcare	14	1
All 250	250	111

Reading the table. Current listings range from 20 of 23 retail and platform organisations to 1 of 14 healthcare organisations. Healthcare also has few device associations (1,173).

3.3 Devices and credentials

Retail and government carry the most infected-device associations; government and education carry most employee-classified devices



Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 [S3][S4]. Records are cumulative, not 2026-only.

Sector	Orgs with infected devices	Devices (employee)	Credential records	Share held by two largest orgs
Retail and platforms	23 of 23	163,098 (1,072)	390,820	40%
Governme nt	55 of 57	129,596 (10,082)	4,145,672	77%

Sector	Orgs with infected devices	Devices (employee)	Credential records	Share held by two largest orgs
Banking and finance	34 of 36	86,694 (299)	679,710	50%
Media and entertainment	12 of 12	60,666 (136)	173,073	52%
Education	26 of 26	57,136 (4,914)	4,147,528	13%
Telecom	11 of 12	38,952 (3,101)	3,612,806	95%
Transport and logistics	15 of 16	37,980 (414)	208,634	49%
Insurance	12 of 12	14,949 (120)	222,522	52%
Energy and utilities	19 of 20	12,208 (364)	268,736	34%
Manufacturing and industry	15 of 15	2,734 (1,046)	367,846	53%
Healthcare	11 of 14	1,173 (90)	71,662	44%
Hospitality and tourism	7 of 7	1,169 (120)	86,856	69%
All	**240 of 250**	**606,355 (21,758)**	**14,375,865**	**35%**

Device totals are lower bounds. Credential records split into 5,459,503 breach-database records, 1,122,781 stealer-log lines and 7,793,581 combolist entries. The infected devices hold at least 3.96 million captured credentials in total, for all services, not only the organisation's own [S3].

What this means.

- **Customer devices dominate.** 584,597 of the 606,355 device associations are not employee-classified. For retailers, banks and media sites, these are most plausibly customers' own computers that held a login to the organisation's site; ownership is not established. They are a fraud and account-hijacking signal and do not by themselves establish an intrusion into the organisation.
- **Government and universities hold the employee-device problem.** Government has 10,082 employee-classified devices and education 4,914, about 69% of the total in our list. Employee classification is a classification, not verified employment, and may include students and contractors; the risk is reuse of staff credentials into internal systems.

- **Concentration varies.** In telecom, two organisations hold 95% of credential records; in education the two largest hold 13%. A sector total is a poor guide to a typical organisation.
- **The median organisation is not small.** The median organisation has 488 infected devices and 8,466 credential records.

3.4 Current credential listings

111 of 250 organisations had at least one credential tied to their domain listed on a monitored credential market when we checked. All but two of them (109) also have a listing history: a credential tied to the domain had already been offered for sale before this check. No organisation has a history without a current listing.

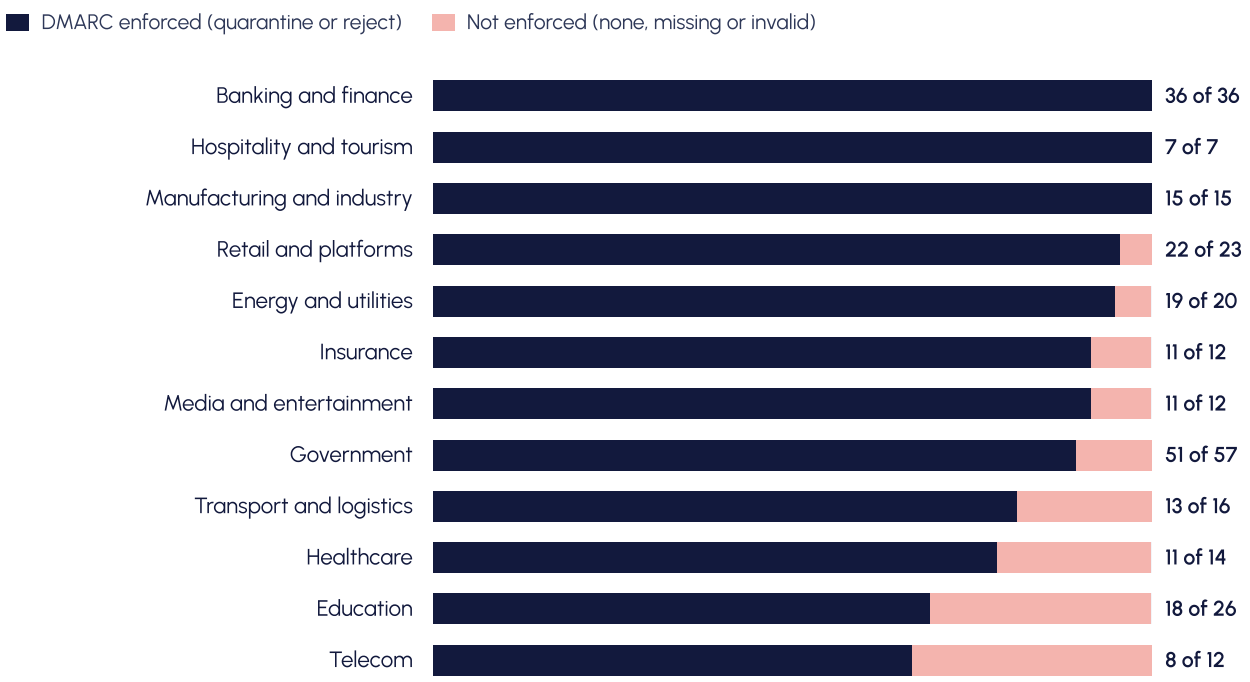
For a defender, a current listing is the most direct market signal that a login tied to the domain is on offer, so it is a reason to validate accounts. It should still be read precisely. The listing does not say how many accounts, whose accounts, or whether the account is active, protected by multi-factor authentication or already reset. The decision it supports is "validate the account now", not "declare a breach".

3.5 Lookalike domains, exposed documents and mentions

- **Lookalikes:** 233 organisations had at least one newly observed lookalike domain in the last 30 days. Lookalikes are candidates, not confirmed phishing sites.
- **Exposed documents:** 209 organisations have at least one exposed document that references their domain (7,013 in total).
- **Mentions:** 105 organisations were mentioned in dark-chat sources in the last 365 days and 82 in dark-web (onion) sources. The largest count, 905, belongs to a retailer whose name appears in card and account-market posts. Mention counts measure visibility, not hostility.

3.6 Email and web hygiene

Banking, hospitality and manufacturing all enforce DMARC; telecom and education lag



Source: Brandefense public DNS, TLS and homepage checks of 250 domains, 21 November 2026 [S5].

Results for the 250 primary domains [S5]:

Control	Result (of 250 unless stated)	Reading
DMARC reject	184	Spoofed mail from the domain should be refused
DMARC quarantine	38	Spoofed mail should go to spam
DMARC p=none, missing or invalid	28 (26 none, 1 missing, 1 invalid)	No enforcement; spoofing the domain is easier
SPF ending -all / ~all / ?all / redirect / none or other	140 / 83 / 2 / 13 / 12	11 domains publish no SPF policy
DKIM observed	215	Absence is not proof of no DKIM
DS record observed (DNSSEC delegation)	27	No DS record observed for 223 domains; a DS record alone does not prove a valid chain of trust
TLS certificate invalid	5 of 247 checked	Expired, mismatched or untrusted certificates
HSTS on homepage	129 of 159 reachable	Most reachable sites force HTTPS for returning visitors

Control	Result (of 250 unless stated)	Reading
Mail provider	96 Microsoft 365, 12 Google, 2 no MX	The rest run their own, regional or filtering-gateway mail

Web results were unavailable for 91 sites; their DNS results are complete.

Banking leads, telecom and education lag. All 36 banking and finance organisations enforce DMARC, as do 51 of 57 government bodies. Telecom (8 of 12) and education (18 of 26) enforce least. On the passive hygiene index (Appendix A.5; 0-100, higher is weaker), education (39), telecom (29) and transport (29) have the weakest sector index values and manufacturing (12) and insurance (16) the strongest.

Old mail servers are an exposure that this list does not show. A public scan counted 382 Australian Microsoft Exchange servers still vulnerable to CVE-2026-62911, an authentication bypass, on 31 August, three weeks after Microsoft's fix [S30] [S31]. NVD lists Exchange Server 2016, 2019 and Subscription Edition as affected. These results do not cover mail-server software, so they cannot say whether any of the 250 run one.

KEY TAKEAWAYS

01

Infected-device and credential associations are near-universal in the list; they call for validation, not alarm.

02

111 of 250 had a credential listed for sale when checked; it is the first item to triage.

03

DMARC enforcement is strong (222 of 250), but only 27 of 250 publish DNSSEC delegation.

CHAPTER 4

What we see on the dark web

04

THIS CHAPTER ANSWERS

What do criminals actually post about Australia beyond bulk advertising, and which offers matter to defenders?

50,103-53,360

posts in the relevant set, from 132,909 tagged posts

INSIDE THIS CHAPTER

4.1 Universe card | 4.2 Platforms, languages and volume | 4.3 Crime families in the relevant set | 4.4 Named-company and population datasets | 4.5 Government and identity themes | 4.6 Case studies | 4.7 What the forums add

IN SHORT

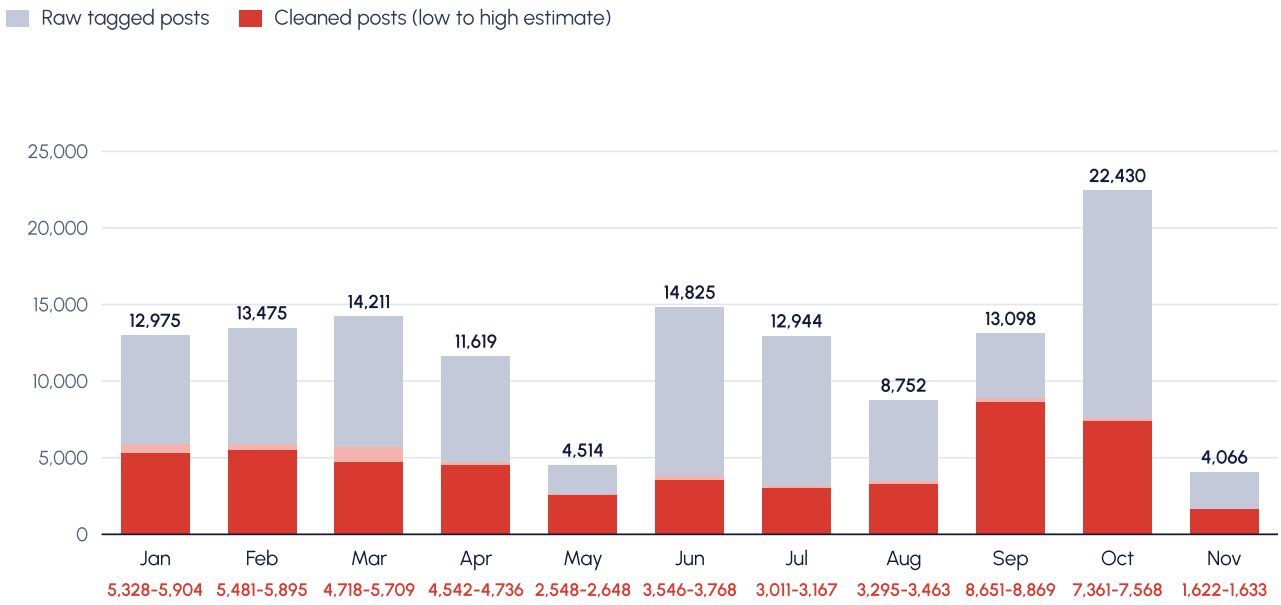
Australia-tagged underground traffic is dominated by card shops, account markets and lead lists in Telegram channels, many of them Chinese-language. About 50,000 posts form the relevant set. Forums carry fewer posts but the most specific claims: named-company databases, offers described as the 2025 airline dataset, identity-document archives and access to a firm's whole network. Read relevant-set counts only, and triage each claim by sample, age and supplier before comment.

4.1 Universe card

Item	Definition
Source	Brandefense Blackhole: Telegram channels and groups, a set of cybercrime forums, paste sites and Discord
Country definition	A country tag ("this post is about, targets or mentions Australia"), plus forum posts that mention Australia
Window	Post time 1 January-18 November 2026 (November partial)
Tagged set	132,909 posts
Forum set	3,501 forum posts mentioning Australia
Relevant set	50,103-53,360 posts, given as a range (Appendix A.2)
Not established	That a tagged post targets Australia, that a claim is true, or that two posts concern the same file

4.2 Platforms, languages and volume

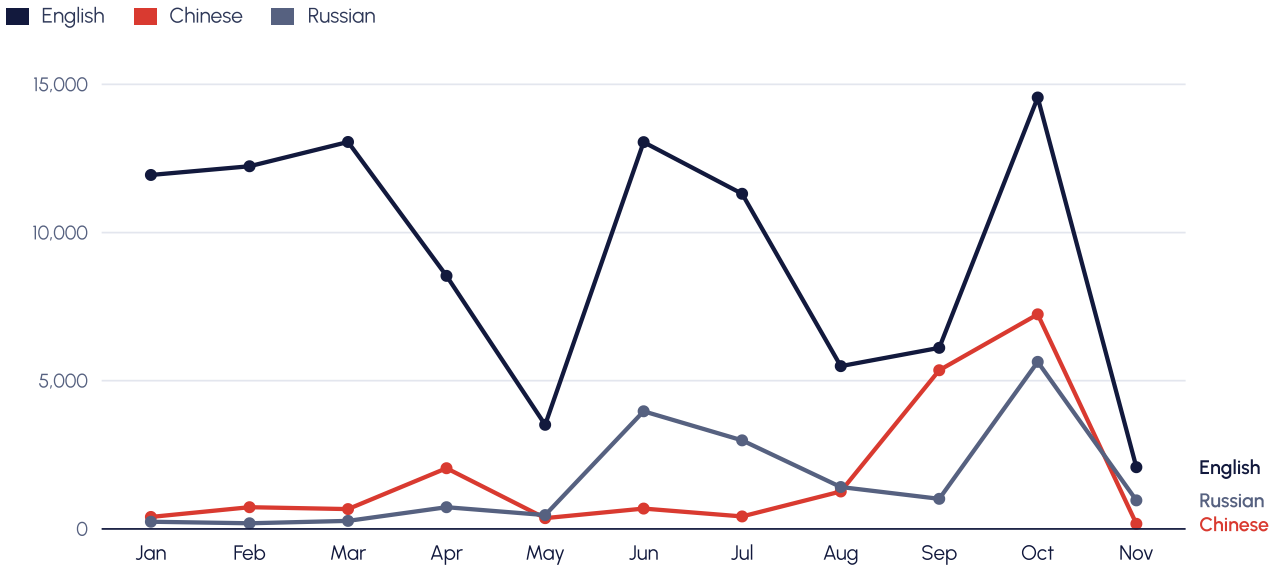
Relevant-set volume stays between about 2,500 and 8,900 posts in each full month (November partial); the raw tag swings with bulk advertising



Source: Brandefense Blackhole, posts tagged Australia, post dates 1 January–18 November 2026, November partial [S1]. Cleaned counts are an upper bound.

Measure	Value
Telegram share of tagged posts	98.7% (131,240)
Forum posts	1,474 tagged (plus 3,501 forum posts mentioning Australia)
Discord, paste, onion sites	163, 32, 0
Posts with an English / Chinese / Russian language label	101,880 / 19,353 / 17,888 (labels can overlap)
Relevant-set posts with an English / Chinese / Russian label	35,616 / 12,056 / 3,484
Raw posts per month	4,514 (May) to 22,430 (October); full months only, November partial

Raw tagged posts by language: English dominates; Chinese- and Russian-language counts rise in the second half of the year



Telegram carries 98.7% of tagged posts. Language labels can overlap. Source: Brandefense Blackhole, posts tagged Australia, post dates 1 January–18 November 2026, November partial [S1]. Cleaned counts are an upper bound.

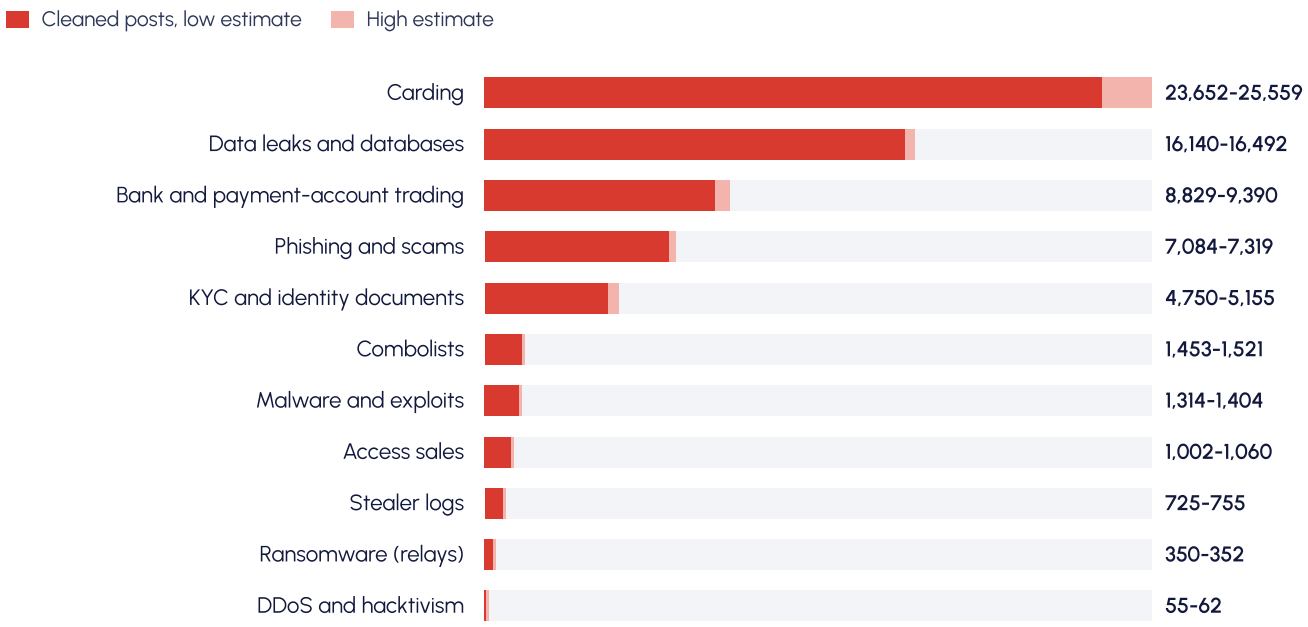
Most raw volume is advertising, not targeting. Most tagged posts were advertising or repeated copies. Card-shop bots, "OTC" account markets and bulk-SMS sellers post the same text to many chats and list Australia as one market among many.

Chinese-language channels matter in the relevant set. Russian-language posts number 17,888 tagged but 3,484 in the relevant set. Chinese-language posts drop far less, from 19,353 to 12,056, because many are carding and verification groups that discuss Australian cards and accounts directly (Chapter 8). A language label describes the channel, not the nationality or location of its members, and has no link to the state-linked activity in §2.3.

Monthly volume is not a threat trend. Volume varies by month across all countries, and we do not read month-to-month changes in the tagged count as threat trends.

4.3 Crime families in the relevant set

Carding leads the relevant set; data leaks, account trading and phishing follow



Source: Brandefense Blackhole, posts tagged Australia, post dates 1 January-18 November 2026, November partial [S1]. Cleaned counts are an upper bound.

Family	Posts (low-high)	What it contains
Carding	23,652-25,559	Card-shop updates, checker outputs, buyers seeking Australian cards
Data leaks and databases	16,140-16,492	Lead lists, lookup services, named-company databases, claimed re-uploads
Bank and payment-account trading	8,829-9,390	Aged personal and business accounts, "loaders", verified exchange accounts
Phishing and scams	7,084-7,319	Phishing kits, scam pages, SMS sender services
KYC and identity documents	4,750-5,155	Licence and passport scans, selfie verification, document templates
Combolists	1,453-1,521	"Database: Australia" email and password lists, often weekly
Malware and exploits	1,314-1,404	Tool sales and exploit discussion, mostly global
Access sales	1,002-1,060	Remote access, web shells, panels, network access
Stealer logs	725-755	Log sales and buyers
Ransomware (relays)	350-352	Relays of leak-site posts naming Australian victims

Family	Posts (low-high)	What it contains
DDoS and hacktivism	55-62	Small within the tag; see Chapter 6

Families overlap and must not be added. Treat these counts as an upper bound: many posts list Australia among dozens of countries.

4.4 Named-company and population datasets

The offers below are advertisements that claim Australian datasets. None was independently verified.

Date	Claimed dataset	Claimed fields	Claimed volume	Venue	Post
4 Jan; 2 Feb	Members of a golf-membership platform	Name, birth date, emails, phones, address, home club, GPS coordinates	500,000 lines (Jan); about 478,000 records (Feb)	Breach forum, two sellers	B01
16 Jan; advertised again 5 May	"Australia national personal data"	Name, gender, email, birth date, phone, street, city, postcode	438,522 rows; 300 USD in May	Several forums	B02
19 Jan	Described as a re-upload of the 2025 Qantas customer dataset	Names, emails, birth dates, phones, addresses, frequent-flyer numbers	5.88 million records	Breach forum	B03
6 Feb; re-posted Jun, Jul	Clients of two linked accounting-software firms	Names, emails, tax file numbers, business numbers, addresses	70,000 consumers (title)	Breach forum, persona "2019"	B06
14 Feb	Archives of mortgage applicants' documents	Medicare cards, payslips, licences, passports	About 3,000 couples	Leak forum	B16
17 Apr	Users of a ticketing company	Name, gender, birth date, username, hashed password	30 million users; 20,000 USD	ShinyHunters Telegram channel	B14
18 Apr	Network plans for telecom network construction projects	Cable routes, equipment, inspection reports	306 GB	Breach forum	B05
8 May	Customers of Australian gambling sites	Username, email, balance, deposits, withdrawals, name, phones	1.4 million rows	Breach forum	B07

Date	Claimed dataset	Claimed fields	Claimed volume	Venue	Post
13 Sep	"23.6 million investors' data"	Not stated	23.6 million; 2,000 USD	Carding forum	B08

What this tells defenders. Three patterns stand out. Free offers described as the 2025 airline dataset keep appearing, so its customers should be treated as targets for phishing. Identity documents (licences, passports, Medicare cards) are advertised in claimed mortgage and accounting data, which feed account-opening fraud. Several claims carry implausible totals (30 million users of one ticketing firm; 23.6 million investors in a country of 27 million), so volume alone is not evidence.

EVIDENCE CARD B01 — 4 Jan 2026

Loser Breach forum · Forum · English

ORIGINAL

```
Data from [golf-membership platform] | Australia
| Member database w/ PII, [...] IDs & GPS - 500k
lines
Headers: MemberID, FirstName, LastName,
DateOfBirth, EmailPrimary, [...] PhoneMobile,
[...] AddressLine1, [...] Suburb, Postcode,
[...] HomeClub, [...] GeoLatitude, GeoLongitude
[...]
Price: $900 - premium dataset
Proof / Sample (first few lines): [link removed]
```

HELD	The offer, the claimed fields, the line count and the price; a second seller offered about 478,000 records from the same platform on 2 February.
NOT ESTABLISHED	Origin, age, authenticity, any sale.

EVIDENCE CARD B02 — 16 Jan 2026

Retrogade Leak forum · Forum · English

ORIGINAL

```
AUSTRALIA - National Personal Data Leak
Content Field: First Name, Last Name, Full Name,
Gender, Email, Date of Birth, Phone Number,
Street Name, City, ZIP Code
Records: 438,522 [link removed]
```

HELD	The field set and row count, advertised on at least four forums; advertised again for 300 USD on 5 May.
NOT ESTABLISHED	That the file is national, new or from any one organisation.

EVIDENCE CARD B03 — 19 Jan 2026

amelgarg Breach forum · Forum · English

ORIGINAL

```
Today I have uploaded the Qantas Airways Limited
Database for you to download [...] On 11 October
2025, hackers from "Scattered LAPSUS$ Hunters"
group released the personal data of 5.7 million
Qantas Airways Limited [...] customers [...] In
total, there are 5877796 records.
```

HELD	A free post offering what it described as the 2025 dataset, with the poster's own description of its contents.
NOT ESTABLISHED	That the file contains the 2025 dataset, or any new 2026 intrusion; no file was assessed.

EVIDENCE CARD B06 — 6 Feb 2026

2019 (quoted) Breach forum · Forum · English

ORIGINAL

```
Overview: [accounting-software firm] and
[accounting firm] are connected Australian
companies operating in the accounting space
[...] Extent of Breach:
"first_name","last_name",
[...]"email","tfn","phone_number","abn",
[...]"postal_address","residential_address"
[...]
```

Note. "tfn" is the tax file number; "abn" is the Australian Business Number.

HELD	The claimed field list, including tax file numbers; re-posts in June and July.
NOT ESTABLISHED	Row count beyond the title; origin; any confirmation by the firms.

EVIDENCE CARD B08 — 13 Sep 2026

REDX Carding forum · Forum · English

ORIGINAL

```
A major leak occurred in Australia, where 23.6
million investors' data was leaked, we have
posted this on several darkweb platforms in
2026. Price $2000
```

HELD	The claim and the price.
NOT ESTABLISHED	Fields, source or plausibility; the figure exceeds Australia's adult population.

EVIDENCE CARD B14 — 17 Apr 2026

ShinyHunters Actor channel · Telegram · English

ORIGINAL

```
30M users from [ticketing company]
Australian ticket vendor
Data contain
Name, gender, business, dob, username, hashed
password, more
- Price: $20k USD
[contacts removed]
- Middleman Required for purchase.
```

HELD	The advertisement, the claimed fields and the price; a relay on 25 April.
NOT ESTABLISHED	Any confirmation by the company; the count, which is high for one firm's Australian users.

EVIDENCE CARD B05 — 18 Apr 2026

RubiconH4ck Breach forum · Forum · English

ORIGINAL

```
Unlock 306 GB of highly sensitive data from
[telecom network] projects [...] Network Maps
and Designs [...] Execution and Inspection
Reports [...]
```

HELD	The offer and the claimed document types (designs, equipment lists, inspection reports).
NOT ESTABLISHED	Whose systems held the files; that any network operator was breached.

EVIDENCE CARD B07 — 8 May 2026

LapsusAdmin Breach forum · Forum · English

ORIGINAL

```
Australian gambling customers 1400K
Number of rows: 1400000 unique
Username Email Balance Total Deposits Total
Withdrawals Level Surname Full Name Phone Number
1 Phone Number 2 Currency Country
If you are a serious buyer, please contact us.
[...] [contacts removed]
```

HELD	The offer, the claimed fields and a sample shown in the post (not reproduced).
NOT ESTABLISHED	Which operators the data came from; authenticity.

EVIDENCE CARD B16 — 14 Feb 2026

gunnerdown Leak forum · Forum · English

ORIGINAL

```
i have around 3k archives of AU data,each
archive has data of a couple with their
medicare,payslips,driving license,passport and
much more docs of those couple.It is a database
of a wellknown mortgage company from Australia
[...] No upfront.Check first and then pay
```

HELD	The offer and the claimed document types.
NOT ESTABLISHED	The company, the source system or authenticity.

4.5 Government and identity themes

Date	Observed offer	Our reading	Post
Jan-Oct	Recurring "Database: Australia" email-and-password combolists, mostly of 40,000-115,000 lines and once 365,000	Recycled and stealer-derived credentials; useful for credential stuffing against Australian services	B17
3 Mar	A carding-forum seller offering Australian "fullz", "most of them" with logins for a federal government online service, relayed by a leak-monitor bot	An identity-plus-login bundle; consistent with stealer logs from users' own devices (an inference; origin not established)	B15
Jun	A forum persona lists data it attributed to a federal agency; the agency calls the claim false	Disputed on the record (§6.4)	None shown
Jul	The same persona posts a state court service's case data, about 28,600 lines; the court service confirms an incident	Incident confirmed by the body; extent under investigation	None shown

EVIDENCE CARD B17 — 24 Jan 2026

thejackal101 Breach forum · Forum · English

ORIGINAL

```
Database: Australia Type: Email : Password Date: [ 24/JAN/2026 ] Combo: [ 42 K++] Line Status: FRESH [links removed]
```

HELD	A recurring combolist format; the same poster and others posted similar lists through 2026.
NOT ESTABLISHED	Freshness, origin or how many pairs still work.

EVIDENCE CARD B15 — 3 Mar 2026

Caan (relayed) Leak-monitor bot relaying a carding forum · Telegram · English

ORIGINAL

```
PM [handle removed] FOR YOUR AUSTRALIA LIVE AND DEAD FULLZ MOST OF THEM COMES WITH [government service] LOGINS
```

HELD	An offer of identity bundles said to include logins for a government service.
NOT ESTABLISHED	Where the logins came from; that any government service was breached.

4.6 Case studies

Each case gives the claim, what we can establish and a proportionate response, plus the chronology and alternatives where the sources allow.

A

CASE A

Free offers described as the 2025 airline dataset

OFFER DESCRIBED AS OLD DATA

Evidence card B03 | 19 Jan 2026 | Breach forum | Transport and travel

Claim	On 19 January a breach-forum user posted a free download of what it called the Qantas customer database: 5,877,796 records with names, emails, birth dates, phones, addresses and frequent-flyer numbers.
Chronology	Qantas disclosed in 2025 that a social-engineering attack on an overseas contact-centre provider exposed customer data; in July 2026 the Privacy Commissioner closed her inquiries without an investigation, describing about 5 million affected Australians [S28]. Leak-monitor bots relayed the same listing in January and February 2026.
What we can establish	That a 2026 post offered, for free, what it described as the 2025 dataset. No file was assessed, so its contents are not established; the original 2025 incident is confirmed separately [S28].
Alternatives	Some uploads may be partial or padded with other data.
Response	For the airline and its partners: keep warning customers about booking-themed phishing. For other organisations: treat frequent-flyer numbers, names and birth dates as known to criminals in account recovery.
BOTTOM LINE	**Treat frequent-flyer numbers, names and birth dates as known to criminals in account recovery.**

B

CASE B

A "national personal data" file advertised repeatedly

CLAIM UNVERIFIED

Evidence card B02 | 16 Jan 2026 | Leak forum | Population data

Claim	In January a forum user shared "AUSTRALIA - National Personal Data Leak", 438,522 rows of names, gender, emails, birth dates, phones and street addresses. In May a seller on another forum advertised the same row count again for 300 USD.
What we can establish	The same field set and row count were advertised across at least four forums in five months; no file was assessed.
Alternatives	An aggregated marketing file; an old breach relabelled as national data; a genuine new breach.
Response	Identity-verification teams should assume these fields are not secret.
BOTTOM LINE	**A recurring row count is not a new breach; assume these fields are not secret.**

C

CASE C

A large claim against a ticketing company

CLAIM UNVERIFIED

Evidence card B14 | 17 Apr 2026 | Actor channel | Ticketing and events

Claim	On 17 April a channel using the ShinyHunters name advertised 30 million user records from a ticketing company, with names, gender, birth dates, usernames and hashed passwords, for 20,000 USD.
What we can establish	The advertisement, the claimed fields and the price. We found no confirmation by the company or an authority in the sources we reviewed.
Alternatives	Data from a regional or global affiliate; aggregated older data; exaggeration.
Response	Ticketing and event firms should check their customer-data stores and third-party platforms; customers should not reuse passwords used there.
BOTTOM LINE	**Check customer-data stores and platforms; a large count is not evidence on its own.**

D

CASE D

An extortion crew narrates a fintech breach

Evidence card B04 | 23 Feb 2026 | Breach forum | Finance

INCIDENT CONFIRMED BY THE COMPANY

Claim	A crew that had posted data from a fintech lending platform published an "update" on 23 February describing failed negotiations and how press coverage spread.
Chronology	The platform confirmed unauthorised access on 17 February and said the incident may have involved personal information; the crew claimed 141 GB from a cloud database covering loan applications at almost 100 lenders [S32].
What we can establish	That the incident is confirmed by the company and that the crew used forum posts to pressure it.
Response	Lenders that used the platform should check what they shared and warn affected applicants about loan-themed phishing.
BOTTOM LINE	**Lenders that used the platform should check what they shared and warn applicants.**

EVIDENCE CARD B04 — 23 Feb 2026

FulcrumSec Breach forum · Forum · English

ORIGINAL

```
UPDATE: [fintech lending platform] tried to
contact us to negotiate several days before we
made our initiale post about them, but [...]
they sent it, incredibly, to the wrong email
address. [...] news of the breach was spreading
like wildfire in Australia.
```

HELD	The crew's own account of contact with the company and of media pressure.
NOT ESTABLISHED	Any detail of the negotiation beyond the crew's claim.

E

CASE E

Telecom network plans offered for sale

CLAIM UNVERIFIED

Evidence card B05 | 18 Apr 2026 | Breach forum | Telecom infrastructure

Claim	On 18 April a forum seller offered 306 GB of network maps, equipment lists and inspection reports for telecom network construction projects.
What we can establish	The listing and its claimed contents. The fields describe contractor documents (designs, field inspections), not customer data.
Alternatives	Data from a design or construction contractor rather than the network operator; old project files.
Response	Network operators and their contractors should check which contractors hold design files and how those files are stored and shared.
BOTTOM LINE	**Check which contractors hold design files and how those files are shared.**

F

CASE F

Identity documents from mortgage applications

CLAIM UNVERIFIED

Evidence card B16 | 14 Feb 2026 | Leak forum | Lending

Claim	On 14 February a leak-forum user offered about 3,000 archives, each holding a couple's Medicare cards, payslips, licences and passports, said to come from a "wellknown mortgage company".
What we can establish	The offer and its claimed contents; no sample was assessed.
Response	Lenders and brokers should audit where application documents are stored, including brokers' and aggregators' systems; banks should treat document-based verification as weaker for this population.
BOTTOM LINE	**Audit where application documents sit, including brokers' systems.**

4.7 What the forums add

Forums contributed 1,474 tagged posts, but they carry the most specific claims (cases A, B, D, E and F, and the network access offer in §8.4). Forum buyers also posted requests: Australian identity-card dumps (February), mobile numbers regis-

tered to Australian bank accounts (February) and "anyone with australia db" (November). Demand for Australian identity and contact data is itself a finding.

KEY TAKEAWAYS

01

Raw volume is mostly card-shop and account-market advertising; read only relevant-set counts, and treat them as an upper bound.

02

Posts offer what they describe as the 2025 airline dataset for free; treat its fields as known in account recovery.

03

Large named-company claims were not confirmed in the sources we reviewed; triage by sample and supplier.

CHAPTER 5

Targeting examples by sector

THIS CHAPTER ANSWERS

Which Australian sectors are named in criminal posts and confirmed incidents, and what kind of response does each one need?

10

sectors with observed activity, from health to retail

IN SHORT

The rows below show how criminals and claimants talk about Australian organisations, alongside incidents that organisations or authorities confirmed. Most posts treat Australia as one market among several; a minority name a specific organisation. Post examples are claims; confirmed incidents are marked with their source. Verify each claim with the named organisation before escalating, and start with the sector's first response.

Victims are described by role under the policy in Appendix A.9, unless the organisation confirmed the incident and it was widely reported.

Health

`Data theft` `extortion` `claims`

EXAMPLE OF OBSERVED ACTIVITY

Most notifiable breaches of any sector (225 in 2025; 149 in H1 2026) [S21][S22]; a general-practice (GP) clinic chain confirmed theft of patient and Medicare data (June) [S33]; an isolated state health server breached (October-November) [S34]; 23 leak-site listings; denied claims against a state health department and a standards body (§6.4)

WHAT IT MEANS

Health holds identifiers that do not expire and is the most-listed sector after consulting

FIRST RESPONSE

Map where patient identifiers sit, including GP software and pathology suppliers

Government

`DDoS claim` `alleged insider (charged)` `data claims`

EXAMPLE OF OBSERVED ACTIVITY

DDoS claim against a federal government online service (April, unconfirmed); disputed claims against a state government and a federal agency; a person charged over the alleged removal of more than 5,600 state Treasury documents (April) [S35]; a legacy Medicare statistics portal accessed by an AI agent (June, disclosed September) [S29]; only 35% of federal entities reported at least half of observed incidents to ASD [S36]

WHAT IT MEANS

Claims outnumber confirmed intrusions; the Commonwealth Cyber Security Posture report found most entities reported fewer than half of observed incidents [S36]

FIRST RESPONSE

Report incidents to ASD; retire legacy portals; prepare claim statements

Education

`Supplier breach` `unpatched server` `defacement`

EXAMPLE OF OBSERVED ACTIVITY

The Victorian education department's statewide school database accessed through one school's unpatched server (disclosed January) [S37][S11]; learning-platform supplier breach affecting Queensland state schools and at least one TAFE, with several universities assessing their exposure (May) [S8][S9]; a tutoring platform breach affecting more than 1 million Australians and New Zealanders (September) [S38]; defacement-feed relays of state education web pages

WHAT IT MEANS

Education depends on central suppliers and on many small sites run by schools

> FIRST RESPONSE
> **Enforce patch directives at school level; inventory education SaaS suppliers**

Energy and utilities

`Data theft` `state-linked pre-positioning (official statement)` `extortion claim`

EXAMPLE OF OBSERVED ACTIVITY

Origin Energy confirmed about 900,000 current and former customers' data accessed (July) [S12]; ASIO's statement on pre-positioning in a critical-infrastructure provider [S13]; a sugar manufacturer that also generates regional power disclosed an incident affecting two mills, later claimed by a ransomware group (June) [S39]

WHAT IT MEANS

Customer data and operational continuity are both exposed

> FIRST RESPONSE
> **Test isolation of operational systems; review customer-data stores and access**

Banking and finance

`Account trading` `carding` `data theft`

EXAMPLE OF OBSERVED ACTIVITY

Account "loaders" and aged business accounts at major banks (B13); demand for bank customers' mobile numbers (B09); a fintech lending platform breach (February) [S32]; 446 clear-text cards attributed to 12 named issuers (§8.1); a broker penalised 2.5 million AUD (February) [S40]

WHAT IT MEANS

Fraud tooling dominates the posts; the intrusion-relevant exposure is in device and credential data (Chapter 9)

> FIRST RESPONSE
> **Triage current listings, then employee devices; alert on checker declines**

Retail and hospitality

`Supplier breach` `skimming` `data claims`

EXAMPLE OF OBSERVED ACTIVITY

Coles Group disclosed a cyber incident (November) [S41]; a hotel chain breach of about 2 million customers via a third-party provider, including 46,727 cards with security codes (August) [S27]; a furniture retailer took systems offline and found no evidence of customer-data access (August) [S42]; a book publisher and distributor's systems were disrupted from July, delaying stock to bookshops [S43]; checkout skimming via a website-testing service and a hijacked store extension [S10][S44]; 1.4 million gambling-site customers claimed (B07)

WHAT IT MEANS

Checkout pages and third-party scripts are the weak link

> FIRST RESPONSE
> **Inventory scripts on payment pages; review supplier access**

Transport and travel

`Data re-circulation` `supplier breach`

EXAMPLE OF OBSERVED ACTIVITY

Re-uploads of the 2025 airline dataset (B03); an airline potentially affected by a breach at a global travel-technology provider (November) [S45]

WHAT IT MEANS

Old booking data keeps feeding phishing

FIRST RESPONSE

Warn customers; monitor partner systems

Telecom

`Data claim` `credentials` `skimming`

EXAMPLE OF OBSERVED ACTIVITY

Telecom network construction plans offered (B05); recurring combolists naming ISP mail domains; checkout skimming reached two telecom brands' sites [S10]

WHAT IT MEANS

Contractor files and customer mailboxes are the exposure

FIRST RESPONSE

Audit contractor file sharing; enforce MFA on customer mail

Professional services and IT

`Extortion` `access sale` `data claim`

EXAMPLE OF OBSERVED ACTIVITY

24 consulting listings, the most of any sector; Cl0p's batch tied to two IT service providers [S46]; full-network access to an ERP consultancy offered for BEC (B12); accounting-software client data with tax file numbers (B06)

WHAT IT MEANS

Service providers are a route into many clients at once

FIRST RESPONSE

Require MFA and logging from providers; segment provider access

Media and culture

`Spyware via advertising`

EXAMPLE OF OBSERVED ACTIVITY

The ABC (Australian Broadcasting Corporation) wiped a small number of staff devices after a spyware-through-advertising campaign that researchers reported (October) [S47]

WHAT IT MEANS

Advertising-delivered spyware can reach staff devices at media organisations

FIRST RESPONSE

Use ad blocking and device hardening for high-risk staff

Reading across sectors. Organisation-specific claims fall into two groups. Extortion crews and forum personas name a specific organisation and publish or sell its data. Card shops, account markets and lead sellers rarely name an organisation; they name Australia as a market. Several of the confirmed 2026 incidents with the largest counts (hotels, education, checkout pages) began at a supplier or an unpatched server, not through the criminal markets that Chapter 4 describes.

KEY TAKEAWAYS

01

Health carries the most notifiable breaches and the second-most leak-site listings.

02

Several of the largest confirmed 2026 incidents began at suppliers or unpatched servers.

03

Service providers are a route into many clients; require MFA and logging from them.

CHAPTER 6

Extortion, leak claims and hacktivism

THIS CHAPTER ANSWERS

Which extortion and hacktivist claims named Australian organisations in 2026, what did the organisations and authorities confirm, and how should an organisation prepare for the next claim?

169

ransomware leak-site listings of Australian victims, 1 January–18 November

INSIDE THIS CHAPTER

6.1 Timeline | 6.2 Leak-site listings: volume and pattern | 6.3 The 313 Team claim against a federal government online service | 6.4 Claims against public bodies: claim against the record | 6.5 Lessons for defenders

IN SHORT

Extortion, not hacktivism, dominated claims against Australia in 2026: 169 leak-site listings, up from 111 in the same period of 2025, plus forum data dumps from a few prolific personas. Several claims against public bodies were disputed on the record, and one hacktivist group claimed a DDoS on a federal government online service without official confirmation in our sources. Triage every claim by sample, age and supplier before comment, and pre-agree who speaks.

6.1 Timeline

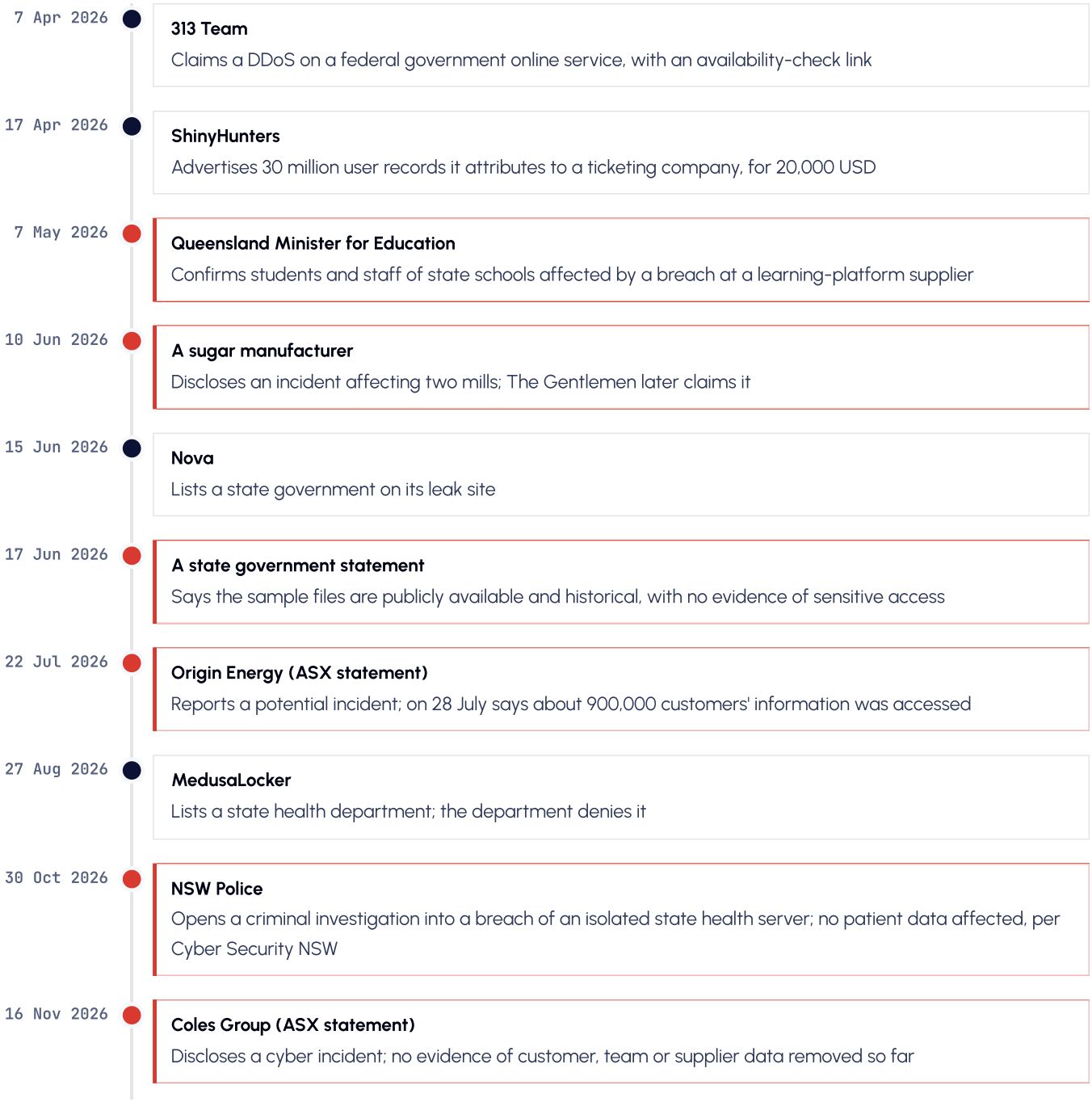
5 Jan 2026 — **Lynx**
Listed a subsidiary of a listed gold producer

15 Jan 2026 — **Victorian education department**
Issues a school incident notification that a student database was accessed through a school's network; all student passwords reset

19 Jan 2026 — **amelgarg (forum)**
Re-uploads the 2025 airline customer dataset to a breach forum

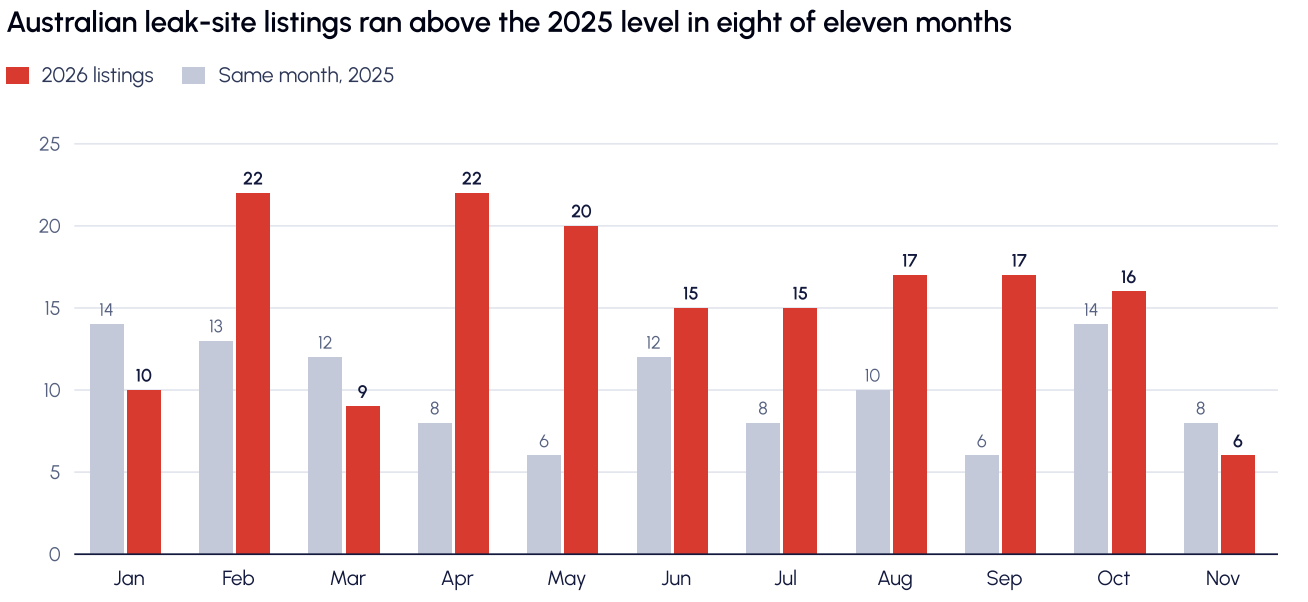
29 Jan 2026 — **Cl0p**
Lists 9 Australian companies linked to two IT service providers

17 Feb 2026 — **A fintech lending platform**
Confirms unauthorised access after an extortion crew posted data it said came from about 100 lenders



Dark markers are actor posts, outlined markers are relays by third parties, coral markers are official or company statements. Dates are post or statement dates; full wording and sources are in the case cards and §6.2-6.4. The Lynx row is a leak-site listing recorded in Ransompedia [S6].

6.2 Leak-site listings: volume and pattern



November covers 1-18 November in both years. Source: Brandefense Ransompedia listings, all dates, to 18 November 2026; rejected and duplicate listings excluded [S6].

Monthly listings ranged from 6 (1-18 November) to 22 (February and April). Cl0p listed 9 Australian companies tied to two IT service providers on 29 January [S46], and Ransompedia dates ten Cl0p Australian listings to February [S6]. The two counts come from different sources and should not be added. The Gentlemen listed Australian victims in every month from June to October. Storm appeared only in August and September.

What this tells defenders. Several leading brands also appear prominently in the comparator countries; these listing data do not establish campaign scope. The local signal is in sectors: consulting, health and construction carry the most listings (Chapter 7). The 29 January batch grouped victims by two IT service providers, which suggests a shared supplier route (not established in the sources).

6.3 The 313 Team claim against a federal government online service

Claim. 313 Team, which calls itself the Islamic Cyber Resistance in Iraq, is a group described in press reporting as pro-Iranian [S48]. On 7 April at 03:50 UTC it claimed a large-scale attack on the servers of a federal government online service. It said the service was shut down and that the attack would last eight hours. It posted an availability-check link and screenshots, and at 09:13 UTC cited hundreds of outage reports on a public outage-tracking site [S2].

EVIDENCE CARD B10 7 Apr 2026

313 Team Actor channel · Telegram

· Arabic, with the group's own English

ORIGINAL

نفذت المقاومة الاسلامية السيبرانية في العراق - فريق 313 هجوم سيبراني [...] استهدف خوادم [خدمة حكومية اتحادية عبر الإنترنت] [...] سيستمر الهجوم لمدة 8 ساعات.

TRANSLATION

The Islamic Cyber Resistance in Iraq - 313 Team has executed a [...] cyberattack targeting the servers of [a federal government online service]. [...] The attack is scheduled to continue for eight hours. Target: [address removed] Check: [link removed]

HELD	The announcement at 03:50 UTC, a named target and an availability-check link.
NOT ESTABLISHED	Any outage or disruption; this is the group's own claim, effect unverified.

EVIDENCE CARD B11 7 Apr 2026

313 Team Actor channel · Telegram

· Arabic, with the group's own English

ORIGINAL

تحديث | رصدت منصة Downdetector مئات البلاغات عن تعطل [خدمة حكومية اتحادية عبر الإنترنت]، علماً ان الهجوم مستمر.

TRANSLATION

Update | Downdetector has detected hundreds of reports regarding an outage affecting [a federal government online service]; the attack remains ongoing. [links removed]

HELD	The group's citation of public outage reports at 09:13 UTC.
NOT ESTABLISHED	Cause of any outage; outage-report counts measure user complaints.

What we can establish. That the group made the claim, credited a named third-party service as powering its attacks and published availability checks. An availability check can record a moment of unreachability from some locations; it does not measure an outage. Public outage-report counts measure user complaints, not cause.

What we could not establish. We found no statement from the service's operator or an Australian authority confirming or denying a DDoS in the sources we reviewed. We therefore record the event as a claim.

Point	313 Team's claim	Official account	Press reporting
Target	A federal government online service	None found in the sources reviewed	None found in the sources reviewed
Effect	Said the service was shut down	Not stated	Not stated
Duration	Eight hours, announced in advance	Not stated	Not stated
Evidence offered	Availability-check links; screenshots; public outage-report counts	Not applicable	Not applicable
Tooling	Credits a named third-party service	Not stated	Not stated

The same group claimed a campaign against Azerbaijani state websites in October, which that country's authorities did report as a DDoS attack using a commercial service [S49]. A group's track record elsewhere is context, not confirmation of the Australian claim.

6.4 Claims against public bodies: claim against the record

Claim	Claimant	What the body said	Status
Sensitive data from a state government network (June)	Nova (leak site)	A state government statement: the sample files were publicly available and historical; no evidence of sensitive access `[S50]`	Disputed on the record
A state rural fire service's files (June)	Nova	The service told members of an information and communications technology (ICT) incident; many files historical; no impact on operations `[S51]`	Incident confirmed; scope limited by the body
A health-standards body's data (June)	ThreeAM (leak site)	The body said the published data was not its data `[S52]`	Disputed on the record
Data it attributed to a federal agency (June)	Forum persona "2019"	The agency said the claim was false `[S53]`	Disputed on the record
A state court service's case data, about 28,600 lines (July)	Forum persona "2019"	The court service said it was responding to a data security incident `[S54]`	Incident confirmed; extent under investigation at the time
A state health department's emails (August)	MedusaLocker (leak site)	The department denied the claim; the documents carried private practices' letterheads `[S55]`	Disputed on the record
An isolated state health server, 70 GB claimed (October-November)	Forum poster	Cyber Security NSW: an isolated server was breached, declared a major incident; no patient data impacted `[S56][S34]`	Incident confirmed; scope disputed

What this tells defenders. In 2026, Australian public bodies answered most claims within days, and the record shows three outcomes: false, historical or mislabelled data, and real but narrower incidents. The defensive skill is fast provenance: compare samples with your schemas and suppliers' exports, date them, and say what is confirmed.

6.5 Lessons for defenders

1. **Pre-agree the public line.** A leak-site post and a confirmed incident are different facts. Decide in advance who confirms status, within what time and through which channel.
2. **Triage by sample and supplier.** Several 2026 claims rested on public, old or third-party documents. Check whether a sample came from your systems, a supplier's, or a public page before responding.
3. **Put reporting clocks in the playbook.** Businesses in scope must report a paid ransom within 72 hours, and critical-infrastructure and APRA rules carry 12-, 24- and 72-hour clocks (§10). Public bodies follow other reporting lines; a draft bill would add a 72-hour clock for breach notices.
4. **Protect citizen portals upstream.** Hacktivist DDoS claims are cheap to make; upstream mitigation and a status page reduce both impact and the room for claims.

KEY TAKEAWAYS

01

Extortion dominated: 169 leak-site listings in 2026, up from 111 in the same period of 2025.

02

Public bodies disputed several claims on the record; treat a listing as a claim until a sample is matched.

03

The only hacktivist DDoS claim against a federal government online service in our data lacked official confirmation in the sources reviewed.

CHAPTER 7

Threat actors

THIS CHAPTER ANSWERS

Who is behind the activity, how are the actors connected, and what does public reporting say about each of them?

42
ransomware brands listed Australian victims in 2026

INSIDE THIS CHAPTER

7.1 How the actors connect | 7.2 State-linked activity in official advisories | 7.3 Extortion and ransomware groups | 7.4 Data-leak personas and extortion crews | 7.5 Hacktivists | 7.6 Other personas seen in Blackhole

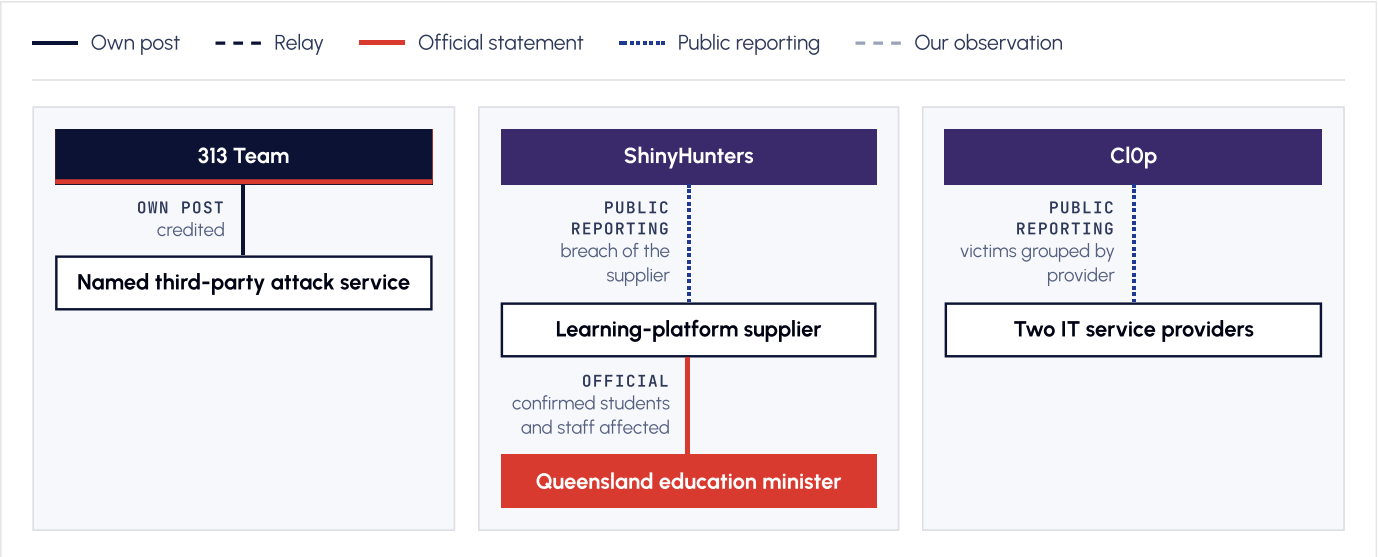
IN SHORT

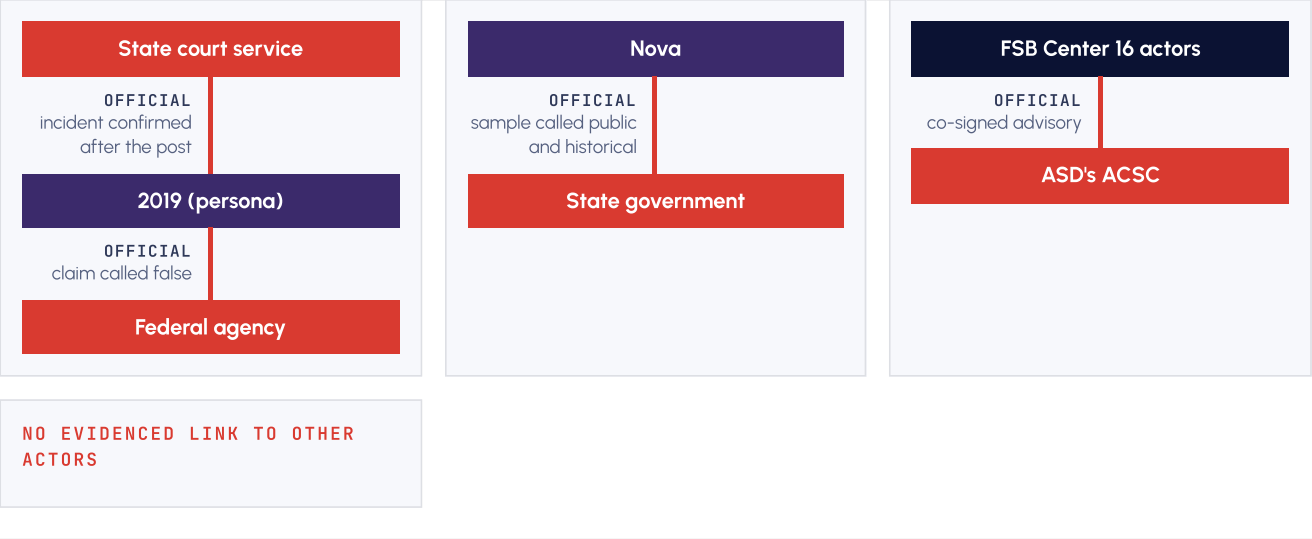
Four actor types matter for Australia. Extortion groups are the most visible, with 42 brands listing Australian victims in 2026. Data-leak personas publish Australian datasets on forums, often for free. State-linked actors appear in joint advisories that Australian agencies co-signed, and a hacktivist group claimed a DDoS on a federal government online service. Patch edge systems first, then treat each leak claim as a triage task, not a statement of fact.

Each profile separates **observed behaviour**, **the actor's own claim**, **what remains unresolved** and **what it means for organisations**. Confidence applies to a specific proposition, not to the actor as a whole.

7.1 How the actors connect

The map links actors only where we hold evidence, and each line says what kind: the actor's own post, a third-party relay, an official statement or public reporting. A line is an association, not proof of a common operator.





7.2 State-linked activity in official advisories

Australian agencies did not publicly attribute a named 2026 intrusion at an Australian organisation to a specific state actor in the sources we reviewed. They did co-sign advisories that describe state-linked techniques relevant to Australian networks (§2.3).

Date	Advisory, as reported	Actor as named by the authors	What it means for Australian defenders
Feb 2026	Five Eyes alert and hunt guide on an exploited Cisco Catalyst SD-WAN flaw (CVE-2026-20127) [S24][S57]	"A malicious cyber actor", active since 2023	Hunt for rogue peers in SD-WAN control planes; patch to the fixed releases listed by NVD
Apr 2026	Multinational advisory on covert networks of hijacked routers and smart devices (AA26-113A) [S58]	China-nexus actors	Dynamic threat feeds and behavioural baselines beat static IP blocklists; retire unsupported home and small-office routers
Jul 2026	Five Eyes and European advisory on poorly configured routers [S15]	Russian FSB Center 16 cyber actors	Remove legacy management protocols and default credentials from network devices
Jul 2026	Joint advisory on webmail phishing [S16]	Russian state-sponsored actors tracked as Laundry Bear	Enforce phishing-resistant MFA on webmail; review Zimbra exposure
Sep 2026	Advisory on fake recruiters [S18]	North Korean actors (WaterPlum / Contagious Interview)	Warn developers about job-test downloads; ASD did not confirm Australian victims
Oct 2026	Seven-nation advisory with US domain seizures [S17]	China's Integrity Technology Group (activity consistent with Flax Typhoon / Ethereal Panda / Red Juliett, per the advisory)	Australia was not named as a victim location; ASD said the techniques apply here

FSB Center 16 actors

As named in the July joint advisory

State-linked (per advisory)

Russian state (attribution by the advisory's authors)

IN AUSTRALIA, 2026

Jul — Named in a Five Eyes and European advisory on exploitation of poorly configured routers and network devices

CLAIMED TARGETS

Communications, defence industry, energy, finance, government and health networks (sectors listed in the advisory)

IN THEIR WORDS

No post card; activity known from the advisory.

SEEN IN PUBLIC REPORTING

- [S15] Cyber Daily: ASD's ACSC joined the advisory; the actors have exploited misconfigured devices for at least 10 years

OUR ASSESSMENT

Relevant to any Australian organisation with exposed network-device management; no Australian victim was named.

CONFIDENCE **Attribution as stated by the advisory's authors**

Unresolved. ASIO's statement about pre-positioning inside a critical-infrastructure provider named neither the provider nor the state [S13]. **Meaning.** For operators, the actionable part is the same across the table: exposed network devices, webmail and developer endpoints are the entry points, and isolation planning is the fallback (§12.1).

7.3 Extortion and ransomware groups

Australia had 169 ransomware leak-site listings in 2026, against 21 in New Zealand, 386 in Canada and 377 in the United Kingdom

AUSTRALIA	NEW ZEALAND	CANADA	UNITED KINGDOM
169	21	386	377
Listings, 1 Jan-18 Nov 2026	Listings, 1 Jan-18 Nov 2026	Listings, 1 Jan-18 Nov 2026	Listings, 1 Jan-18 Nov 2026
2025: 129	2025: 18	2025: 406	2025: 288
ALL TIME: 619	ALL TIME: 85	ALL TIME: 1449	ALL TIME: 1420
GROUPS IN 2026: Qilin, The Gentlemen, Cl0p, Storm, INC Ransom, Kairos	GROUPS IN 2026: The Gentlemen, Cl0p, Zawoo, Qilin, Anubis, Emperador	GROUPS IN 2026: Qilin, The Gentlemen, Akira, Cl0p, Play, INC Ransom	GROUPS IN 2026: Qilin, The Gentlemen, DragonForce, Cl0p, 0apt, Akira

Source: Brandefense Ransompedia listings, all dates, to 18 November 2026; rejected and duplicate listings excluded [S6].

Ransompedia holds 169 Australian listings dated 1 January-18 November 2026, up from 111 in the same period of 2025 [S6]. Forty-two brands posted them. The five most active (Qilin 27, The Gentlemen 19, Cl0p 13, Storm 10 and INC Ransom 9) ac-

count for 78 listings, 46% of the total. Three of the five (Qilin, The Gentlemen and Cl0p) are also among the four most active brands in Canada and the United Kingdom. These listing data do not establish campaign scope.

Sector label in the listings	2026 listings
Consulting and professional services	24
Health and healthcare services	23
Construction	12
Education	10
Retail and commerce	10
Manufacturing	9
Government and public administration	6

The chart data list the six most active brands and the largest sector labels per country; the government count and the total of 42 brands are Ransompedia totals [S6].

In March, New Zealand's NCSC published an advisory with the ACSC and CERT Tonga on INC Ransom's affiliate model, saying affiliates had reached organisations in Australia, New Zealand and Pacific Island states since 2023 [S59]. Sector labels come from the listings and can be broad. Several of the larger 2026 extortion cases in public reporting, such as the learning-platform breach, began at suppliers (§2.4).

Qilin

Ransomware and extortion brand | Financial

IN AUSTRALIA, 2026

Jan-Nov	27 Australian leak-site listings, the most of any brand
Oct	Four Australian victims listed in four days, including a club that confirmed a contained incident

CLAIMED TARGETS

Professional services, clubs, health and education providers

IN THEIR WORDS

No post card; listings are summarised from Ransompedia.

SEEN IN PUBLIC REPORTING

- [S60] Cyber Daily: four Australian listings in four days in October, including an accounting firm and an events group
- [S61] Cyber Daily: a regional club confirmed a contained incident after a listing and said its gaming and membership systems were not affected

OUR ASSESSMENT

The most active brand against Australia and across the comparator countries combined.

CONFIDENCE **High that it listed the victims; impact varies by victim**

The Gentlemen

Ransomware and extortion brand | Financial

IN AUSTRALIA, 2026

Mar-Oct	19 Australian listings, every month from June to October
Jun	Claims a sugar manufacturer that had disclosed an incident affecting two mills

CLAIMED TARGETS

Manufacturing, agriculture, heritage and food firms

IN THEIR WORDS

No post card; listings are summarised from Ransompedia.

SEEN IN PUBLIC REPORTING

- [S39] Cyber Daily: claimed the sugar manufacturer's incident and set a timer for data release

OUR ASSESSMENT

Second most active brand against Australia in 2026, rising in the second half of the year.

CONFIDENCE **High that it listed the victims**

Cl0p

Clop

Data-extortion brand | Financial

IN AUSTRALIA, 2026

29 Jan	Lists 9 Australian companies linked to two IT service providers
Feb-Sep	13 Australian listings in Ransompedia, ten of them dated February

CLAIMED TARGETS

Clients of managed IT service providers

IN THEIR WORDS

No post card; listings are summarised from Ransompedia.

SEEN IN PUBLIC REPORTING

- [S46] Cyber Daily: the 9 listed companies fell into two groups tied to two Australian IT service providers; data theft was not established

OUR ASSESSMENT

Batch listings tied to shared providers. The 29 January companies were grouped by their provider relationships; a shared supplier route is a possible explanation, but the entry path and data theft were not established.

CONFIDENCE **High that it listed the companies; data theft unconfirmed**

Public reporting on these brands: Qilin listed four Australian victims in four days in October, and one of them, a regional club, said its incident was contained [S60][S61]. The Gentlemen claimed a sugar manufacturer's disclosed incident [S39].

Cl0p's 29 January batch grouped victims by two IT service providers [S46].

Claims that did not hold up. Several 2026 listings named Australian public bodies that then disputed them on the record. A state government said the sample files in a ransomware group's claim against it were "publicly available and historical" [S50]. A health-standards body said data a group published was not its data [S52]. A federal agency said a forum claim about its data was false [S53]. A state health department denied a ransomware listing whose documents carried the letterheads of private practices [S55]. Leak-site listings are claims; treat them as triage tasks.

7.4 Data-leak personas and extortion crews

2019

Forum data-leak persona | Financial or reputational

IN AUSTRALIA, 2026

Feb	Posts accounting-software client data with tax file numbers (B06)
Jun	Lists data it attributed to a federal agency; the agency calls it false
Jul	Posts a suicide-prevention charity's staff data and a state court service's case data

CLAIMED TARGETS

Australian charities, courts, accounting firms, retailers and agencies

IN THEIR WORDS

> *"connected Australian companies operating in the accounting space"* B06

SEEN IN PUBLIC REPORTING

- [S62] Cyber Daily: a charity confirmed a breach after the persona's post and said some data was doctored
- [S54] Cyber Daily: a state court service said it was responding to a data security incident after the persona's claims
- [S53] Cyber Daily: a federal agency said the persona's claim was false

OUR ASSESSMENT

A prolific persona that publishes Australian datasets, often for free; its record mixes confirmed incidents, disputed claims and altered data.

CONFIDENCE **High that it posted the data; each claim needs separate verification**

ShinyHunters

Data-extortion crew | Financial

IN AUSTRALIA, 2026

17 Apr	Advertises 30 million users of a ticketing company (B14)
May	Named in reporting on the breach of a learning-platform supplier used by Australian schools and universities

CLAIMED TARGETS

SaaS platforms and their customers

IN THEIR WORDS

> *"30M users from [ticketing company]"* B14

SEEN IN PUBLIC REPORTING

- [S63] Cyber Daily: the supplier's chief executive said it reached an agreement with the crew that no customers would be extorted
- [S64] Cyber Daily: Queensland's education minister confirmed students and staff were affected

OUR ASSESSMENT

Targets shared platforms to reach many organisations at once; claims about individual Australian firms remain unverified unless confirmed.

CONFIDENCE **High for the supplier breach (confirmed); low for the ticketing claim**

TeamPCP

`Software supply-chain crew` `Financial`

IN AUSTRALIA, 2026

Mar	Supply-chain malware reaches developer credentials at the NDIA, which says no participant data was accessed
Aug	Two Western Australian men charged as alleged principal participants

CLAIMED TARGETS

Open-source package users and developers

IN THEIR WORDS

No post card.

SEEN IN PUBLIC REPORTING

- [S65] iTnews: AFP, WA Police and FBI operation; the FBI said the group's code potentially compromised more than a thousand organisations
- [S66] iTnews: the NDIA said it identified the activity within hours and took reset and recovery actions

OUR ASSESSMENT

A crew with global reach; police have charged two Western Australian men as alleged participants, and the case is before the courts.

CONFIDENCE **Charges are allegations; agency impact as stated by the agency**

Public reporting on these actors: a charity and a state court service confirmed incidents after the 2019 persona's posts, and a federal agency rejected another of its claims [S62][S54][S53]. The learning-platform supplier said it had reached an agreement with the crew it attributed the breach to, and Queensland's education minister confirmed students and staff were affected [S63][S64]. Police charged two Western Australian men as alleged TeamPCP participants, and the National Disability Insurance Agency (NDIA) said it identified the group's March activity within hours and took reset and recovery actions [S65][S66].

7.5 Hacktivists

313 Team

Islamic Cyber Resistance in Iraq

Hacktivist (DDoS)

Pro-Iranian (per OC Media and Unit 42); believed to operate from Iraq (per OC Media)

IN AUSTRALIA, 2026

7 Apr	Claims a DDoS on a federal government online service, for eight hours (B10)
7 Apr	Cites public outage reports as evidence (B11)

CLAIMED TARGETS

A federal government online service

IN THEIR WORDS

> *"targeting the servers of [a federal government online service]"* B10

SEEN IN PUBLIC REPORTING

- [S48] OC Media: described the group as pro-Iranian and believed to operate from Iraq, in reporting on its October claim against Azerbaijan
- [S67] Unit 42: described as an active pro-Iranian hacktivist cell
- [S49] APA, citing Azerbaijan's National Cybersecurity Agency: DDoS attacks in October used a commercial DDoS service; the agency noted the group's claim

OUR ASSESSMENT

A repeat claimant that names high-profile government targets and posts availability checks. We found no official confirmation of the Australian claim in the sources we reviewed.

CONFIDENCE **High that it made the claim; effect unverified**

Unit 42 described 313 Team as an active pro-Iranian hacktivist cell in April 2026 [S67].

Hacktivist activity against Australia in our data is small next to criminal activity. Beyond the 313 Team claim (§6.3), it consists of defacement-feed relays of individual pages on state education and university web servers, and a scattering of DDoS boasts against small business sites. We found no public reporting that confirms disruption from any of them. Separately, an analyst writing for ASPI's The Strategist reported that a pro-Russian hacktivist collective claimed access to an Australian wastewater treatment and irrigation management system in February; the article presents it as an allegation [S68].

7.6 Other personas seen in Blackhole

Aliases only; no contacts, links or real identities.

Persona or brand	Observed role in 2026	Own claim	Unresolved
FulcrumSec	Extortion crew that posted a fintech lending platform's data (Feb)	141 GB; "update" on negotiations	Data extent beyond the company's statement

Persona or brand	Observed role in 2026	Own claim	Unresolved
amelgarg	Breach-forum uploader of the 2025 airline dataset (Jan)	5.88 million records, free	Completeness
thejackal101 and similar posters	Recurring "Database: Australia" combolists (Jan-Oct)	Mostly 40,000-115,000 "fresh" lines per post (once 365,000)	Freshness, origin
RubiconH4ck	Seller of telecom network construction plans (Apr)	306 GB	Whose systems held the files
LapsusAdmin	Seller of gambling-site customer data (May)	1.4 million rows	Which operators
gunnerdown	Seller of mortgage applicants' document archives (Feb)	About 3,000 couples	Company, authenticity
mercyxx	Seller of network access to an ERP and CRM consultancy (Nov)	Root, mail server, invoices	That access works
Sundayman_99	Seeker of "loaders" for aged bank accounts (Mar, Sep)	Up to 1 million AUD	Any use of accounts
X FORUMS (bot)	Automated uploader of small credential files, including Australian bank and portal login domains	None	Not a person; a distribution bot

KEY TAKEAWAYS

01

Extortion groups are the most visible actors: 169 listings from 42 brands, with 46% from five.

02

Several listings naming public bodies were disputed on the record; a listing is a claim until checked.

03

Australian agencies co-signed advisories describing threats to edge devices, webmail and developer endpoints; local impact was not established for every campaign.

CHAPTER 8

The fraud economy

THIS CHAPTER ANSWERS

How do criminals turn Australian identities, cards and accounts into money, and what does it cost victims?

2.18bn AUD

scam losses in 2025, per the National Anti-Scam Centre's Targeting Scams report

INSIDE THIS CHAPTER

8.1 Cards and card shops | 8.2 Checkout-page skimming | 8.3 Accounts, identities and lookups | 8.4 What police and auditors reported | 8.5 Prices in context

IN SHORT

Carding is the largest category in our relevant Australia-tagged set, followed by data leaks, bank and payment-account trading and phishing. Much of the carding traffic runs in Chinese-language channels. Official cases with amounts point elsewhere: business email compromise and supplier bank-detail changes cost Australian organisations real money in 2026. Confirm payment changes out of band, and monitor checkout-page scripts.

8.1 Cards and card shops

Carding posts (23,652–25,559 in the relevant set) include card-shop "base" updates that list Australia among dozens of countries, checker outputs, and buyers asking for Australian cards. The largest single source in the tag is a card-shop update bot whose posts list Australia among 15 to 50 countries per batch. Chinese-language carding groups account for a large share of the rest; 12,056 of the cleaned posts carry a Chinese-language label, against 3,484 Russian; the label describes the channel, not its members (§4.2).

SCOPE OF THE CARD FIGURES

The card figures in this report cover only payment cards that appeared in clear text inside the dark-web posts we collected for this report. They are not a measure of card theft or fraud loss in Australia.

Within that narrow scope, 1,102 distinct Australia-associated cards appeared in clear text in collected posts. Of these, 446 are attributed to one of 12 named Australian issuers and the other 656 are labelled only as Australian. 686 of them first appeared in January and February. [S7]

8.2 Checkout-page skimming

Two 2026 incidents show card theft at the merchant side rather than in the bank. In October a small Australian online store was shut on its platform's advice after a hijacked third-party extension redirected at least one shopper to a fake checkout [S44]. In November attackers abused a website-testing service to load skimming and wallet-swapping code on at least 178 organisations' sites, including several Australian brands, for about 17 hours. A researcher traced about 7,040 USD to the attackers' wallets [S10]. ACSC alerts in September and July also covered actively exploited e-commerce and CMS flaws (CVE-2026-75650 in Adobe Commerce and Magento; 17 patched CMS and plugin flaws) [S69][S70].

8.3 Accounts, identities and lookups

Bank and payment-account trading (8,829-9,390 posts) covers aged personal and business accounts, "loaders" who move funds into accounts, and verified exchange accounts. KYC and document posts (4,750-5,155) offer Australian licence and passport scans, selfie verification and template services. Data-leak posts (16,140-16,492) are the second-largest family; most are multi-country lead lists and lookup services rather than new breaches.

Two buyer posts show demand. In February a cracking-forum user asked for "mobile numbers that are registered with Australia bank accounts" (B09). In March a carding-forum user sought a partner to "load" an aged business account at a major Australian bank, "upto 1m aud" (B13).

EVIDENCE CARD B09 — 14 Feb 2026

jstAclass Cracking forum · Forum · English

ORIGINAL

```
Hi all I'm after latest list of mobile numbers
that are registered with Australia bank accounts
just need phone numbers for certain banking
databases if anyone has please let me know.
```

HELD	Demand for bank customers' mobile numbers.
NOT ESTABLISHED	That any such list exists or was sold.

EVIDENCE CARD B13 — 7 Mar 2026

Sundayman_99 Carding forum · Forum · English

ORIGINAL

```
Looking for experience loader to load aged
[major bank] business account Australia. *1 year
plus aged * easily can handle upto 1m aud [...]
proof of account: [image link removed]
```

HELD	Demand for someone to move funds into an aged business account; a similar post on 29 September.
NOT ESTABLISHED	That any account was used or funds moved.

8.4 What police and auditors reported

Date	Reported by	What happened
26 Feb	Home Affairs figures, as reported by iTnews	At least 94 ransomware payment reports from larger businesses and critical-infrastructure entities in the regime's first eight months [S71]
9 Mar	WA Auditor General, as reported by iTnews	Invoice fraud of 71,000 AUD at state entities and exposure of 32 people's data, including minors', via a third party's cloud storage; linked to weak Microsoft 365 controls [S72]

Date	Reported by	What happened
1 Apr	WA Auditor General, as reported by iTnews	A council paid about 350,000 AUD after a phishing attack let an attacker change a supplier's bank details [S73]
15 May	AFP and NSW Police	Three people charged over an alleged 600,000 AUD business email compromise; a bank's information led to suspected proceeds being spent on gold bullion [S74]
2025 (published 2026)	National Anti-Scam Centre Targeting Scams report, as reported	2.18 billion AUD lost across 274,577 loss reports; investment scams 837.7 million AUD, payment redirection 166.8 million AUD [S23]

What this tells defenders. The amounts in official cases come from changed payment details and business email compromise, not from the database sales that dominate forum headlines. In November a forum seller advertised full network access to an ERP and CRM consultancy explicitly as a "turnkey BEC machine", with invoices, bank-statement lines and mail-server access (B12). The controls are procedural and technical: out-of-band confirmation of bank-detail changes, phishing-resistant MFA for finance staff, and alerts on new mailbox forwarding rules.

EVIDENCE CARD B12 — 15 Nov 2026

mercyxx Breach forum · Forum · English

ORIGINAL

```
Selling an exclusive, full-network compromise of
a major Australian ERP/CRM consulting firm and
their building materials client. [...] I have
root, I have their email server [...] This is a
turnkey BEC (Business Email Compromise) machine.
[...] 263,601 real invoices and 176,707 bank
statement lines.
```

HELD	The offer of access and data, framed explicitly for invoice fraud.
NOT ESTABLISHED	That access exists or works; the firm's identity is withheld.

8.5 Prices in context

Product (relevant-set posts)	Median asking price	Spread
Card (per card or small batch)	25 USD	10-130 USD
Bank or payment account	90 USD	40-200 USD
KYC or document service	85 USD	35-350 USD
Stealer logs	70 USD	15-1,050 USD

Product (relevant-set posts)	Median asking price	Spread
Combolist	50 USD	10-200 USD
Access offer	42 USD	10-250 USD
Data-leak or lead offer	20 USD	10-40 USD

Prices are asking prices from a minority of posts that quote one; they do not measure market value or completed sales. Spread is the middle half of the quoted prices (25th to 75th percentile), so it is not the full range. Single high-value offers in Chapter 4 sit far above these medians.

KEY TAKEAWAYS

01

Carding leads the relevant set, much of it in Chinese-language channels.

02

Card figures cover only cards seen in clear text in collected posts (§8.1).

03

Official cases with amounts describe changed payment details and email compromise; confirm every bank-detail change out of band.

CHAPTER 9

Banking and finance deep dive

THIS CHAPTER ANSWERS

Where does the visible exposure of Australian banks sit: in the bank, at its staff, or at its customers?

11 of 22

banks with a current credential listing, the first item to triage

IN SHORT

Most visible exposure sits on the customer side: 43,041 non-employee device associations (most plausibly customers' devices), card-checker activity and account-trading posts. The bank- and staff-side signals are current listings at 11 of 22 banks and 256 employee-classified devices. Three banks carry most of the card and customer-device signals. Triage each current credential listing first, then validate employee devices, and monitor checker declines on your BIN ranges (a BIN is the issuer's card-number prefix).

This chapter covers the 22 banks among the 36 banking-and-finance organisations in Chapter 3; the other 14 are superannuation funds, payment, lending and other finance firms, and a crypto exchange. That is why 43,041 non-employee devices here differ from the sector totals in Chapter 3, and why 11 of the sector's 19 current listings sit at banks. Aggregates only; individual banks are not named.

11 of 22

banks with a current credential listing

19 of 36

banking and finance organisations with a current credential listing (11 at banks; the other 8 at funds, payment firms and other finance organisations)

21 of 22

banks with non-employee device associations (43,041 in total; ownership and current infection unverified)

17 of 22

banks with employee-classified devices (256 in total)

36 of 36

banking and finance organisations enforcing DMARC

11 of 22

banks on our list with cards in clear text in collected posts (443 of the 1,102 cards name one of them; narrow scope, §8.1)

The top three banks account for 69% of the attributed cards and most of the non-employee device associations.

What it means for banks.

1. **Current listings come first.** 11 of 22 banks had one on the day of the check; apply Decision 1 (disposition within 5 working days).

2. **Employee exposure is small but real.** 256 employee-classified devices across 17 banks are the intrusion-relevant subset. After current listings, they deserve priority validation over the much larger non-employee total.
3. **Non-employee device associations are the larger exposure.** 43,041 device associations across 21 of 22 banks are not employee-classified, and most plausibly they are customers' devices. Ownership, current infection and whether any stored session still works are unverified. Fraud teams should use device and session risk signals at login and at payee changes, not only password checks.
4. **Login files for bank domains circulate in small batches.** An automated forum uploader posted small credential files named after the login pages of several Australian banks in May, June and August. Their lines are consistent with stealer logs from users' devices (an inference; origin not established), and they feed the same account-takeover risk.
5. **Card checking is a detectable precursor.** Checker bots test cards with small authorisations on merchant gateways. Issuers can detect clusters of declined low-value attempts from foreign gateways on their BIN ranges, identify the cards involved, check their authorisation and fraud signals, and reissue the cards confirmed at risk under issuer policy.
6. **Mule and loader demand is the downstream risk.** Posts seeking "loaders" for aged business and personal accounts (`B13`) target banks with remote onboarding and large transfer limits; they do not show that accounts were opened or used at the assessed banks.

KEY TAKEAWAYS

01

Current credential listings at 11 of 22 banks come first, then the 256 employee-classified devices; the 43,041 non-employee ones also need validation.

02

Every banking and finance organisation on the list enforces DMARC.

03

Card-checker declines on your BIN ranges are a detectable precursor.

CHAPTER 10

Regulatory and national response

THIS CHAPTER ANSWERS

What did Australian law and regulators require of organisations in 2026, and what changes next?

72 hours

to report a ransomware payment under the Cyber Security Act 2024

INSIDE THIS CHAPTER

10.1 What the reporting data shows | 10.2 Enforcement in the window

IN SHORT

Australia's rules tightened in steps rather than with one new law. Ransomware payments must be reported within 72 hours, and Home Affairs moved to a compliance and enforcement phase in January 2026. Privacy duties on automated decisions apply from 10 December 2026, and a draft bill would set a fixed 72-hour data breach deadline. Courts penalised two financial firms for weak security, and APRA sought a third penalty. Map which regime applies to you, and rehearse against the earliest clock that applies.

Measure	What we could verify	Status and caution
Ransomware payment reporting (Cyber Security Act 2024, Part 3)	A reporting business entity must report a ransomware payment to the designated Commonwealth body, through ASD's ReportCyber, within 72 hours of making it or becoming aware of it. The duty covers businesses whose previous-year turnover exceeds 3 million AUD (pro rata for a part year) and responsible entities for critical-infrastructure assets under Part 2B of the SOCI Act. Commonwealth and State bodies are outside it. The civil penalty is 60 penalty units [S75][S76]	Part 3 commenced on 29 May 2025 under section 2 [S75]. Reporting under the rules has applied since 30 May 2025; a second phase began on 1 January 2026 [S76]. Home Affairs guidance words the threshold as 3 million AUD or more [S76]
Cyber Incident Review Board (Part 5)	Reviews of significant incidents; the chair may require documents [S75]	Commenced on 29 May 2025, as Part 3 [S75]
Smart-device security standards (Part 2)	Manufacturers and suppliers must meet security standards set by the rules [S75]	Part 2 commenced 29 November 2025 [S75]; the standards apply to relevant consumer smart devices manufactured from 4 March 2026 (Smart Devices Rules) [S77]

Measure	What we could verify	Status and caution
Privacy Act: statutory tort (Privacy and Other Legislation Amendment Act 2024, Schedule 2)	A cause of action for serious invasions of privacy [S78]	In force from 10 June 2025 [S78]
Privacy Act: automated decisions (Schedule 1, Part 15)	APP entities must say in their privacy policy when a computer program makes, or substantially informs, decisions that significantly affect individuals [S78][S79]	Applies from 10 December 2026 [S78][S79]
Critical-infrastructure incident reporting (SOCI Act 2018, Part 2B)	Responsible entities must report to ASD a cyber incident with a significant impact on an asset's availability within 12 hours, and one with a relevant impact within 72 hours; an oral report needs a written record within 84 or 48 hours [S80]	In force
APRA information security (CPS 234)	APRA-regulated entities must notify APRA as soon as possible, and no later than 72 hours, after becoming aware of a material information security incident [S81]	In force
APRA operational risk (CPS 230)	APRA-regulated entities must notify APRA within 24 hours of a disruption to a critical operation outside tolerance, and within 72 hours of an operational risk incident with a likely material impact [S82]	In force; current version effective 1 July 2026 [S82]
Notifiable data breaches (Privacy Act 1988, Part IIIC)	APP entities must assess a suspected eligible breach within 30 days and notify the Information Commissioner and affected individuals as soon as practicable; there is no fixed hour count [S83]	In force
Fixed breach-notification deadline (exposure draft)	The Privacy Amendment (Personal Data Protection) Bill 2026 would require notice to the Information Commissioner within 72 hours of reasonable grounds to believe an eligible breach occurred; the 30-day assessment window would stay [S84]	Exposure draft for consultation (September 2026); not law at our cut-off
Critical-infrastructure disclosure	A Home Affairs consultation proposed a temporary delay in public disclosure of the most serious critical-infrastructure incidents [S85]	Consultation (March 2026); not law at our cut-off

10.1 What the reporting data shows

Ransomware payments are now partly measurable. iTnews reported, from a freedom-of-information release and later Home Affairs figures, that larger businesses made at least 75 ransom payment reports in the regime's first eight months [S71]. The businesses had turnover above 3 million AUD. Between 7 and 13 such reports were made each month. Critical-infrastructure entities made 19 payment reports in the eight months to January 2026, at least 94 reports in total [S71].

These are payment reports, not attacks. Smaller businesses below the threshold do not report, and organisations that refuse to pay do not appear. Read the figure as a floor for paid extortion among larger firms.

10.2 Enforcement in the window

Date	Body	Outcome
Feb 2026	Federal Court, on ASIC's application	A fixed-income broker ordered to pay a 2.5 million AUD penalty and 500,000 AUD in costs over cyber security failures linked to a 2023 breach of about 18,000 clients' data `[S40]`
16 Jul 2026	Privacy Commissioner	Preliminary inquiries into the 2025 Qantas incident closed without investigation; the Commissioner said the evidence did not support the likelihood of a breach of privacy law `[S28]`
11 Aug 2026	APRA, in the Federal Court	APRA sought an 8 million AUD penalty against a listed regional bank under the Banking Executive Accountability Regime over weak authentication controls exploited in a 2023 account-access attack; the bank accepted it, and the court had not yet ruled `[S86]`
25 Sep 2026	OAIC	The investigation into the 2023 Latitude breach continues, with a representative complaint accepted `[S87]`
Oct 2026	NSW Supreme Court, on ASIC's application	A financial-advice licensee ordered to pay a 1.35 million AUD penalty and 250,000 AUD in costs for inadequate cyber security policies and oversight of its representatives `[S88]`
4 Nov 2026	Information Commissioner	Inquiries into offshore access to court recordings at a transcription provider closed; the provider is in liquidation `[S89]`

The October 2025 Federal Court order against Australian Clinical Labs, 5.8 million AUD, remains the first civil penalty under the Privacy Act `[S90]`.

Which reporting clocks apply to you? Current law at our cut-off; the proposed 72-hour privacy deadline is not included. Owners are suggestions.

Who it applies to	Trigger	Recipient	Deadline	Suggested owner
Businesses with turnover above 3 million AUD; critical-infrastructure responsible entities	A ransomware payment made, or known to have been made on its behalf	Designated Commonwealth body, through ASD's ReportCyber	72 hours	Legal, with the CISO
Critical-infrastructure responsible entities (SOCI Part 2B)	Cyber incident with a significant impact on the asset's availability	ASD	12 hours; written record within 84 hours of an oral report	CISO

Who it applies to	Trigger	Recipient	Deadline	Suggested owner
Critical-infrastructure responsible entities (SOCI Part 2B)	Cyber incident with a relevant impact	ASD	72 hours; written record within 48 hours of an oral report	CISO
APRA-regulated entities (CPS 234)	Material information security incident	APRA	As soon as possible, at most 72 hours	CISO and chief risk officer
APRA-regulated entities (CPS 230)	Disruption to a critical operation outside tolerance	APRA	24 hours	Head of operational risk
APP entities (Privacy Act)	Reasonable grounds to believe an eligible data breach occurred	OAIC and affected individuals	As soon as practicable; assess a suspected breach within 30 days	Privacy officer

Commonwealth and State bodies are outside ransomware payment reporting. Commonwealth agencies report incidents to ASD and fall under the notifiable data breach scheme; only 35% of entities reported at least half of observed incidents in 2024-25 [S36]. State and territory bodies usually follow state privacy law and the state cyber unit's reporting line.

What CISOs should do now. Name the person who files each report in the table above. Rehearse against the earliest clock that applies, such as 12 hours for a significant critical-infrastructure incident or 24 hours for an APRA critical-operation disruption, and record timings and filing evidence. The 72-hour privacy deadline in the draft bill is a proposal, not current law. Update the privacy policy for automated decisions before 10 December 2026, less than three weeks after publication. Keep a dated record of controls, because courts have now penalised firms for security failures that preceded a breach. This section is not legal advice.

KEY TAKEAWAYS

01

Ransomware payments must be reported within 72 hours, and at least 94 payment reports were made in the first eight months.

02

A draft bill would set a fixed 72-hour deadline for data breach notices; it was not law at our cut-off.

03

Courts penalised two financial firms for security failures and APRA sought a bank penalty; keep dated evidence of your controls.

CHAPTER 11

Outlook

THIS CHAPTER ANSWERS

What should Australian organisations plan for next, and what evidence would change that plan?

5

key judgements, each with a signal to watch

INSIDE THIS CHAPTER

11.1 Key judgements | 11.2 What would change the assessment | 11.3 Conditional scenarios

IN SHORT

Plan for the same evidence types, not a new threat: identity exposure that stays invisible until it is used, extortion that reaches organisations through suppliers, and state-linked access to edge devices. Leak-site listings rose against 2025, but one year of listings is not a forecast. Change the plan when the evidence below changes, not on a calendar.

11.1 Key judgements

Judgement	Confidence	Basis and limit
Identity exposure (devices, stealer logs, credential listings) is the most widespread measurable risk to Australia's leading organisations	High for the 250-organisation list	240 with devices, 250 with credential records, 111 with current listings; not national prevalence
Extortion groups will keep listing Australian victims at or above the 2026 rate	Medium (planning assumption)	169 listings in 2026 against 111 in the same period of 2025; listings depend on global brands, not Australian events
Many of the largest data incidents will continue to start at suppliers and shared platforms	Medium	Several of the largest confirmed 2026 incidents began at a supplier (§2.4); small sample
If edge-device flaws stay exploitable, plan for state-linked and criminal access attempts against critical infrastructure	Medium (planning assumption)	Joint advisories and ASIO's statement (§2.3, §7.2); no named Australian victim
Leak claims against public bodies will keep outpacing confirmed intrusions	Medium	Several 2026 claims were disputed on the record (§6.4)

11.2 What would change the assessment

Current interpretation	Evidence that would change it	Decision affected
Listings reflect global brands, not an Australian campaign	A brand or affiliate concentrating on Australian victims, or Australian-language lures in negotiations	Raise extortion readiness; run the restore test in §12.1 first
Large named-company claims are unverified	A sample matched to a specific system, or confirmation by the company	Trigger notification and customer-protection actions
Current listings mean "validate", not "breached"	Validation shows active accounts without MFA among listed credentials	Escalate to incident response and enforce MFA for that population
State-linked activity is described in advisories, not named incidents	An official attribution of a named Australian intrusion	Fund edge-system and identity telemetry ahead of other projects
The 72-hour breach deadline is a draft	Introduction of the bill to Parliament	Move the breach-notice rehearsal into the incident plan

11.3 Conditional scenarios

- **If** a supplier that stores your customers' data discloses a breach, **then** plan for phishing that quotes real account or booking details (a planning assumption); **signal:** supplier notices and forum re-uploads. **Decision:** warn customers and tighten account-recovery checks.
- **If** a new critical edge or e-commerce vulnerability is disclosed, **then** plan for exploitation attempts within days; **signal:** ACSC alerts and vendor advisories. **Decision:** patch-and-verify, then hunt for web shells and skimming code.
- **If** card-checker activity on your BIN ranges rises and investigation confirms that specific cards are being tested, **then** plan for card-not-present fraud on those cards; **signal:** clustered low-value declines from foreign gateways. **Decision:** investigate, check authorisation and fraud signals, and reissue the cards confirmed at risk.

KEY TAKEAWAYS

01

Plan for evidence types, not a new threat: identity exposure, supplier-led extortion and edge-device access.

02

Each judgement has a signal; change the plan when the signal changes.

03

One year of rising listings is a planning input, not a forecast.

CHAPTER 12

Action plan

THIS CHAPTER ANSWERS

What should each team do in the next 90 days, and how will the board know it was done?

20
actions with an owner and completion evidence

INSIDE THIS CHAPTER

12.1 30/60/90 days | 12.2 By role | 12.3 Patch reference for 2026 alerts | 12.4 How Brandefense can help

IN SHORT

Start by confirming you receive credential-listing and infected-device alerts, then act on what is specific to you: current listings, employee devices, internet-facing edge systems and the suppliers that hold your customer data. Then close payment-change, email and web gaps, and rehearse a combined extortion and disclosure scenario against the earliest reporting clock that applies. The board knows the work is done from each row's completion evidence and the scorecard; report both by day 90.

12.1 30/60/90 days

This is a sequence, not a waiting period. A current material threat should enter your incident process immediately.

1 Days 1-30

Confirm that you receive credential-listing and infected-device alerts for your primary domains; if not, arrange them, and record the listing-validation and employee-device rows as blocked until alerts arrive

OWNER
CISO and threat intelligence

COMPLETION EVIDENCE
Alert source named; first alert received

2 Days 31-60

Where DMARC is p=none, missing or invalid, inventory senders and stage enforcement

OWNER
Messaging

COMPLETION EVIDENCE
Aligned senders; p=quarantine with a rollback route

3 Days 61-90

Sign DNS for primary domains where your registrar supports it; fix invalid TLS certificates and add HSTS

OWNER
Network and web teams

COMPLETION EVIDENCE
DNSSEC validation succeeds from an external resolver; certificate checks pass

For every current credential listing tied to your domains, validate the account and its MFA status within 5 working days

OWNER
Identity team

COMPLETION EVIDENCE
Each listing has a disposition: reset, already remediated, or not ours, with a date

Validate employee-classified device associations; revoke sessions and tokens where active

OWNER
Identity and endpoint teams

COMPLETION EVIDENCE
Device list reconciled with asset inventory; revocations logged

Patch and re-test internet-facing edge, mail and e-commerce systems named in 2026 ACSC alerts, joint advisories or public scans (Cisco SD-WAN, Exchange, TeamCity, Adobe Commerce and Magento, N-able N-central, CMS plugins; §12.3)

OWNER
Infrastructure

COMPLETION EVIDENCE
External re-test passes; web-shell hunt completed on mail and web servers

Name who files each report that applies to you (ransomware payment, critical-infrastructure incident, APRA notification, notifiable data breach) and the spokesperson for public claims (§10)

OWNER
CISO, legal, communications

COMPLETION EVIDENCE
Approved one-page playbook with each trigger, recipient, deadline and named owner

Move privileged and remote users first, then others, to phishing-resistant MFA (FIDO2 security keys, passkeys or certificate-based sign-in); block device-code sign-in where it is not needed (§12.3)

OWNER
Identity team and SOC

COMPLETION EVIDENCE
Coverage recorded per user group; device-code flow restricted; test sign-in detected

Require out-of-band confirmation for payment-instruction and payee changes, including supplier bank-detail changes (§8.4)

OWNER
Finance and fraud

COMPLETION EVIDENCE
Procedure signed off; one simulated request caught

Monitor third-party scripts on payment and login pages; alert on changes to scripts that load on checkout pages (§2.4)

OWNER
Web and e-commerce teams

COMPLETION EVIDENCE
Script inventory; change alert live and tested

Test account-recovery and payee-change processes against an attacker who knows name, birth date, address and licence number

OWNER
Fraud and customer operations

COMPLETION EVIDENCE
Weaknesses recorded and fixed, retest passed

Alert on clustered card-checker declines on your BIN ranges

OWNER
Fraud

COMPLETION EVIDENCE
Alert live; first review recorded

Add breach-notice, log-retention and 72-hour cooperation clauses to contracts with suppliers holding customer data

OWNER
Procurement and legal

COMPLETION EVIDENCE
Clause in every renewed contract; gap list for the rest

Run a tabletop combining a data-theft claim on a leak site with a supplier breach, timed against the earliest reporting clock that applies (§10)

OWNER
CISO, communications, legal

COMPLETION EVIDENCE
Decision log, timings recorded against each clock, draft filings

Report the scorecard against targets (below)

OWNER
CISO to board

COMPLETION EVIDENCE
Board paper with remaining gaps and owners

List every supplier that stores or processes your customer data, including SaaS platforms, contact centres and website scripts

OWNER
Procurement and privacy

COMPLETION EVIDENCE
Register with data types, contract clause and breach-notice contact per supplier

Before 10 December 2026, less than three weeks after publication: confirm whether the automated-decision duty applies and, if it does, update the privacy policy (§10)

OWNER
Privacy

COMPLETION EVIDENCE
Applicability decision recorded; policy published where the duty applies

Run a timed restore test of one crown-jewel system, offline from the domain

OWNER
Infrastructure

COMPLETION EVIDENCE
Restore time recorded against the recovery time objective (RTO: the longest outage your business-continuity plan allows)

Critical-infrastructure operators: test running an essential service isolated from external networks (§12.3)

OWNER
OT and operations

COMPLETION EVIDENCE
Isolation test record with duration achieved

Monitor leak sites and forums for your name and suppliers' names; prepare a claim-assessment checklist

OWNER
Threat intelligence

COMPLETION EVIDENCE
Checklist approved; first triage logged

Scorecard targets. These are suggested defaults; set your own where policy differs.

Measure	Target
Current listings with a disposition within 5 working days	100% by day 90
Employee-classified devices reconciled with the asset inventory	100% by day 90
Internet-facing edge, mail and e-commerce systems passing an external re-test	100% by day 90
Primary domains with DMARC at quarantine or reject	100%, or a dated plan, by day 90
Privileged and remote users on phishing-resistant MFA (number matching does not count)	100%, or a dated plan, by day 90
Suppliers holding customer data with a named breach-notice contact	100% by day 90
Payee and payment-instruction changes confirmed out of band	100% by day 90

Measure	Target
Restore test within RTO	Passed, or a dated fix, by day 90
Credential-listing and infected-device monitoring for primary domains, internal or through a provider	In place by day 30
Privacy policy updated for automated decisions, where the duty applies	Before 10 December 2026

12.2 By role

Role	First decision
Board	Ask for the current-listing and employee-device numbers for your organisation, the supplier register, and the date by which each item is validated
CISO	Put listing and device monitoring in place first, then edge-system exploitability checks, identity validation and the supplier register
SOC	Add detections for web shells on mail and web servers, device-code and adversary-in-the-middle sign-ins, new remote-management agents and mass token use from new devices
Fraud	Use device and session risk at login and payee changes; monitor clustered card-checker declines on your BINs; warn customers about impersonation using leaked booking or account data
Communications and legal	Prepare statements for unverified leak-site claims and supplier breaches, separating claim, verified fact and action; keep every applicable reporting clock in the playbook

12.3 Patch reference for 2026 alerts

The table lists flaws that ACSC alerts, joint advisories or public scans in 2026 described as exploited, targeted or exposed in Australia. Versions are from NVD and vendor advisories; confirm the current advisory before patching.

Product	CVE	Affected and fixed versions	Australian context
Cisco Catalyst SD-WAN Controller, Manager and Validator	CVE-2026-20127	Fixed releases exist in the 20.9, 20.12, 20.15 and 20.18 trains; take the first fixed build for your train from the Cisco advisory. Releases before 20.9 and the 20.11, 20.13, 20.14 and 20.16 trains have no fix of their own: move 20.11 to a fixed 20.12 release, 20.13 and 20.14 to a fixed 20.15 release, and 20.16 to a fixed 20.18 release. In the CISA known-exploited list since 25 February 2026 `[S91][S57]`	Five Eyes alert and hunt guide (February) `[S24]`

Product	CVE	Affected and fixed versions	Australian context
JetBrains TeamCity On-Premises	CVE-2026-63077	Before 2026.1.3 and 2025.11.7 [S92]	ACSC: exploited against Australian servers (August) [S93]
Adobe Commerce and Magento Open Source	CVE-2026-75650	Affected: Commerce 2.4.4 to 2.4.9, Commerce B2B 1.3.3 to 1.5.3 and Magento Open Source 2.4.6 to 2.4.9, each up to the "-2026-aug" releases. Fix: apply the dedicated hotfix for CVE-2026-75650 in bulletin APSB26-146; in the CISA known-exploited list since 8 September 2026 [S94][S95]	ACSC: a substantial number of potentially vulnerable instances in Australia (September) [S69]
Microsoft Exchange Server 2016, 2019 and Subscription Edition	CVE-2026-62911	Fixed by the August 2026 security updates: 2016 CU23 KB5121576 (build 15.01.2507.072); 2019 CU14 KB5121575 (15.02.1544.044); 2019 CU15 KB5121574 (15.02.1748.049); Subscription Edition RTM KB5121573 (15.02.2562.046) [S96][S31]	Public scan (Shadowserver), as reported: 382 Australian servers still vulnerable on 31 August [S30]
N-able N-central	CVE-2026-18556 and CVE-2026-18577 (authentication bypass; the second follows an incomplete fix of the first)	Affected through 2026.3.1 (NVD). Fixed in Hotfix 2, build 2026.3.1.10, which supersedes Hotfix 1 (build 2026.3.1.7). Both CVEs in the CISA known-exploited list since 3-4 August 2026 [S97][S98][S99]	ACSC: attackers targeting Australian instances (August) [S100]
WordPress and other CMS plugins	17 patched flaws, including CVE-2025-32432 (Craft CMS)	Craft CMS fixed in 3.9.15, 4.14.15 and 5.6.17 [S101]	ACSC campaign alert (July); ClickFix and Vidar Stealer via hijacked Australian WordPress sites (May) [S70][S102]

Two identity techniques also featured in 2026 ACSC warnings: device-code phishing against Microsoft 365 (May) and ClickFix lures [S103][S102]. For critical-infrastructure operators, ASD's revised isolation guidance sets a three-month target for running essential services disconnected from other networks [S104].

KEY TAKEAWAYS

01

Confirm monitoring, then validate current listings and employee devices in the first 30 days.

02

Build the supplier register and lock down payment changes by day 60; report the scorecard by day 90.

03

Rehearse a leak-site claim combined with a supplier breach against the earliest reporting clock that applies.

12.4 How Brandefense can help

Brandefense combines Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. The analysis in this report used the same data and scoring that the platform applies to monitored organisations: infected-device and credential associations, current credential-market listings, lookalike domains, exposed documents and dark-web mentions. It does not promise that every claim can be verified or that a historical record remains usable.

Bring your domains, brands and security priorities to a 30-45 minute demo with Sales and Presales. The team can show how platform monitoring relates external signals to the assets you manage. A Brandefense team member or a partner in your region will follow up.

Request a demo

Appendix A. Method

A.1 Window, sources and priority

The research window is 1 January-18 November 2026 by the date a post was published. Own data comes first: Brandefense Blackhole (dark-web and messaging posts, infected-device and credential associations, card material in posts), Ransompedia (ransomware leak-site listings) and Brandefense Atlas exposure ratings. External sources give context. Data were extracted on 21 November 2026. Sources S1-S7 are Brandefense's own data and have no public address; every external source in Appendix C carries a link and a verification date.

A.2 Blackhole posts

Item	Value
Posts with the Australia country tag	132,909
Forum posts mentioning Australia	3,501
Posts in the relevant set	50,103-53,360, given as a range

Relevant-set counts remain an upper bound for criminal activity concerning Australia, because many posts list Australia as one market among many.

Two limits shape every trend in this report. We do not compare categories across the year. Volume also varies by month across all countries; we do not read month-to-month changes in the tagged count as threat trends.

A.3 The 250 organisations

Selection and limits are in §3.1. The exposure signals are those listed in §3.1, as held on 21 November 2026.

A.4 Atlas ratings

Each organisation received an Atlas exposure rating from 0 to 100 from the signals listed in §3.1, and the 250 together a national headline figure. Some signals were unavailable for some organisations, so ratings may understate their exposure. Treat a current credential-market listing as a reason to validate accounts, not as proof of a breach.

A.5 DNS, TLS and web checks

Results cover each primary domain's public mail, SPF, DMARC, DKIM, DNSSEC and CAA records, its TLS certificate and its homepage headers. Missing, invalid and monitoring-only (p=none) DMARC policies count as no enforcement. No intrusive testing was done.

The passive hygiene index is an Odin analytical composite of these email, DNS, TLS and header results, on a scale of 0-100. A higher value means weaker hygiene; it is a model, not an Atlas rating.

A.6 Card material in posts

Scope: only payment cards that appeared in clear text in the dark-web posts covered by this report, reported only as aggregate counts. These figures do not measure card theft or fraud loss.

A.7 Ransomware

We used Ransompedia listings for Australia, New Zealand, Canada and the United Kingdom, all dates, dated by publication. Third-party relays of leak-site posts are context only.

A.8 Incident coverage

Incident coverage draws on our own data and on official and press reporting for the window, chiefly the OAIC, the AFP, iTnews and Cyber Daily. Laws in Chapter 10 are cited from the Federal Register of Legislation and official guidance.

Coverage limits. Our view is partial:

- ACSC alerts are cited from press reporting of them.
- Incidents reported only in Chinese- or Russian-language media may be missing.
- Tor ransomware leak sites are covered only through Ransompedia.
- Offers made only in closed forums, private groups or direct messages may be missing.
- Posts deleted early may be missing.
- Incidents that organisations handle without disclosure stay invisible.

That an incident is absent from this report does not mean it did not happen.

A.9 Confidence and boundaries

High confidence applies to a reproducible measurement, not to a criminal's underlying assertion. Medium indicates an interpretation with a clear supporting line and stated limits. "Unverified" means not independently established; it is neither proof of fabrication nor proof of a breach. Victim organisations are described by role; an organisation is named only where it or an authority confirmed the incident and it was widely reported. Actor aliases are printed; links, contacts, indicators and personal data are withheld. Full provenance is held in an internal evidence register.

Appendix B. Evidence register

Every post quoted in this report appears as a redacted post card in the chapter shown. Excerpts are short; omissions are marked [...]; identifiers, contacts, links and victim organisations are replaced with labels in brackets, under the policy in A.9. Translations are ours unless the post carried the actor's own English. Posting dates are not intrusion dates. Post identifiers, links and full text are held in an internal evidence register.

Card	Posted	Venue	Alias as shown	Language	Shown in
B01	2026-01-04	Breach forum	Loser	English	§4.4
B02	2026-01-16	Leak forum	Retrogade	English	§4.4
B03	2026-01-19	Breach forum	amelgarg	English	§4.4
B04	2026-02-23	Breach forum	FulcrumSec	English	§4.6
B05	2026-04-18	Breach forum	RubiconH4ck	English	§4.4
B06	2026-02-06	Breach forum	2019 (quoted)	English	§4.4
B07	2026-05-08	Breach forum	LapsusAdmin	English	§4.4
B08	2026-09-13	Carding forum	RED✘	English	§4.4
B09	2026-02-14	Cracking forum	jstAclass	English	§8.3
B10	2026-04-07	Actor channel	313 Team	Arabic, with the group's own English	§6.3
B11	2026-04-07	Actor channel	313 Team	Arabic, with the group's own English	§6.3
B12	2026-11-15	Breach forum	mercyxx	English	§8.4
B13	2026-03-07	Carding forum	Sundayman_99	English	§8.3

Card	Posted	Venue	Alias as shown	Language	Shown in
B14	2026-04-17	Actor channel	ShinyHunters	English	§4.4
B15	2026-03-03	Leak-monitor bot relaying a carding forum	Caan (relayed)	English	§4.5
B16	2026-02-14	Leak forum	gunnerdown	English	§4.4
B17	2026-01-24	Breach forum	thejackal101	English	§4.5

Appendix C. Sources

S1 Brandefense Blackhole posts concerning Australia, post dates 1 January-18 November 2026, extracted 21 November 2026.

S2 Brandefense Blackhole posts of the 313 Team channel, 7 April 2026.

S3 Brandefense Blackhole infected-device, breach-database, stealer-log and combolist associations for 250 domains, as held on 21 November 2026.

S4 Brandefense Atlas exposure ratings for the 250 domains, 21 November 2026, including credential-market listings, lookalike domains, exposed documents and mention statistics.

S5 Brandefense email, DNS and web hygiene results for the 250 primary domains, 21 November 2026.

S6 Brandefense Ransompedia, listings for Australia, New Zealand, Canada and the United Kingdom, all dates, extracted 21 November 2026.

S7 Brandefense Blackhole, aggregate counts of Australia-associated payment cards seen in clear text in posts, 21 November 2026.

S8 iTnews, "Qld gov says students, staff caught in Canvas cyber incident", 7 May 2026. https://www.itnews.com.au/news/qld-gov-says-students-staff-caught-in-canvas-cyber-incident-625664. Verified on 21 November 2026.

S9 iTnews, "Aus universities and TAFEs investigating exposure to Canvas cyber incident", 7 May 2026. https://www.itnews.com.au/news/aus-universities-and-tafes-investigating-exposure-to-canvas-cyber-incident-625659. Verified on 21 November 2026.

S10 iTnews, report on card-skimming code planted through a website-testing service on Australian brands' sites (title names the service), 18 November 2026. https://www.itnews.com.au/news/hijacked-website-testing-tool-plants-card-skimmer-on-australian-brands-sites-630407. Verified on 21 November 2026.

S11 iTnews, "Unpatched server behind Vic student data breach", 7 October 2026, on the Office of the Victorian Information Commissioner's findings. https://www.itnews.com.au/news/unpatched-server-behind-vic-student-data-breach-629494. Verified on 21 November 2026.

S12 Cyber Daily, reports on Origin Energy's ASX disclosures of a customer data incident, 22-31 July 2026. https://www.cyberdaily.au/security/13942-breached-origin-energy-discloses-data-breach-to-asx and a follow-up report of 31 July (article URL withheld). Verified on 21 November 2026.

S13 Cyber Daily, "ASIO boss warns of active cyber threat to Aussie critical infrastructure", 26 June 2026, on the Director-General's Annual Threat Assessment of 24 June 2026. https://www.cyberdaily.au/security/13813-asio-boss-warns-of-active-cyber-threat-to-aussie-critical-infrastructure. Verified on 21 November 2026.

S14 Region Canberra, report on the ASD Annual Cyber Threat Report 2025-26, 27 October 2026. https://region.com.au/asd-report-highlights-increasing-number-of-ai-enabled-cyber-threats/1011269/. Verified on 21 November 2026.

S15 Cyber Daily, "Fix your routers: Aussie cyber agency joins partners to warn of ongoing Russian cyber activity", 14 July 2026. https://www.cyberdaily.au/security/13896-fix-your-routers-aussie-cyber-agency-joins-partners-to-warn-of-ongoing-russian-cyber-activity. Verified on 21 November 2026.

S16 Cyber Daily, "ASD, National Cyber Security Coordinator warn of ongoing Russian phishing campaign", 24 July 2026. https://www.cyberdaily.au/security/13955-alert-asd-national-cyber-security-coordinator-warn-of-ongoing-russian-phishing-campaign. Verified on 21 November 2026.

S17 iTnews, "ASD joins seven-nation alert as US seizes Chinese hacking firm's tools", 12 October 2026. https://www.itnews.com.au/news/asd-joins-seven-nation-alert-as-us-seizes-chinese-hacking-firms-tools-629536. Verified on 21 November 2026.

S18 iTnews, "Beware DPRK job scams, ASD warns, but won't confirm local impact", 22 September 2026. https://www.itnews.com.au/news/beware-dprk-job-scams-asd-warns-but-wont-confirm-local-impact-629081. Verified on 21 November 2026.

S19 DataReportal (Kepios), *Digital 2027: Australia*, 4 November 2026 (data for October 2026). https://datareportal.com/reports/digital-2027-australia. Verified on 21 November 2026.

S20 Cyber Daily, "Aussie cyber agency received more than 82,000 cybercrime reports in 12 months", 27 October 2026. https://www.cyberdaily.au/security/14354-report-aussie-cyber-agency-received-more-than-82-000-cybercrime-reports-in-12-months. Verified on 21 November 2026.

S21 OAIC, "Data breach notifications increase to all-time high in 2025, new NDB stats show", 6 July 2026. https://www.oaic.gov.au/news/media-centre/data-breach-notifications-increase-to-all-time-high-in-2025,-new-ndb-stats-show. Verified on 21 November 2026.

S22 OAIC, "Large-scale data breaches on the rise, latest OAIC statistics reveal", 26 October 2026. https://www.oaic.gov.au/news/media-centre/large-scale-data-breaches-on-the-rise,-latest-oaic-statistics-reveal. Verified on 21 November 2026.

S23 Cyber Daily, "Scams cost Australians over $2bn in 2025, says ACCC", 30 March 2026, citing the National Anti-Scam Centre's Targeting Scams report. https://www.cyberdaily.au/security/13400-scams-cost-australians-over-2bn-in-2025-says-accc. Verified on 21 November 2026.

S24 iTnews, "ASD and Five-Eyes spy agencies alert on exploited Cisco SD-WAN zero-day", 26 February 2026. https://www.itnews.com.au/news/asd-and-five-eyes-spy-agencies-alert-on-exploited-cisco-sd-wan-zero-day-623881. Verified on 21 November 2026.

S25 iTnews, "Australia sanctions North Korean IT worker bosses and financiers", 23 October 2026. https://www.itnews.com.au/news/australia-sanctions-north-korean-it-worker-bosses-and-financiers-629860. Verified on 21 November 2026.

S26 OAIC, "Statement on Instructure (Canvas) cyber incident", 8 May 2026 (updated 11 May 2026). https://www.oaic.gov.au/news/media-centre/statement-on-instructure-canvas-cyber-incident. Verified on 21 November 2026.

S27 Cyber Daily, report on a hotel chain's data breach affecting about 2 million customers (title names the chain), 25 September 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S28 OAIC, "Privacy Commissioner completes preliminary inquiries into Qantas 2025 data incident", 16 July 2026. https://www.oaic.gov.au/news/media-centre/privacy-commissioner-completes-preliminary-inquiries-into-qantas-2025-data-incident. Verified on 21 November 2026.

S29 iTnews, report on unauthorised access by an AI agent to a Medicare statistics portal, 23 September 2026. https://www.itnews.com.au/ (article URL withheld). Verified on 21 November 2026.

S30 iTnews, "Hundreds of old, vulnerable Exchange servers remain in Australia", 8 September 2026. https://www.itnews.com.au/news/hundreds-of-old-vulnerable-exchange-servers-remain-in-australia-628758. Verified on 21 November 2026.

S31 NIST National Vulnerability Database, CVE-2026-62911 (Microsoft Exchange Server). https://nvd.nist.gov/vuln/detail/CVE-2026-62911. Verified on 21 November 2026.

S32 Cyber Daily, report on a fintech lending platform confirming a data breach (title names the platform), 20 February 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S33 iTnews, report on a GP clinic chain's data theft (title names the chain), 16 July 2026. https://www.itnews.com.au/ (article URL withheld). Verified on 21 November 2026.

S34 iTnews, "NSW Health server targeted in cyber incident", 4 November 2026. https://www.itnews.com.au/news/nsw-health-server-targeted-in-cyber-incident-630096. Verified on 21 November 2026.

S35 iTnews, report on a state government downgrading the impact of an alleged Treasury data breach (title names the state), 5 May 2026. https://www.itnews.com.au/ (article URL withheld). Verified on 21 November 2026.

S36 iTnews, "Government entities not reporting cyber incidents to ASD", 12 February 2026, on the Commonwealth Cyber Security Posture report. https://www.itnews.com.au/news/government-entities-not-reporting-cyber-incidents-to-asd-623556. Verified on 21 November 2026.

S37 iTnews, "Vic Education database breached via school's network", 15 January 2026. https://www.itnews.com.au/news/vic-education-database-breached-via-schools-network-622987. Verified on 21 November 2026.

S38 Cyber Daily, report on a tutoring platform's data breach affecting more than 1 million Australians and New Zealanders (title names the platform), 8 September 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S39 Cyber Daily, report on a ransomware group's claim against a sugar manufacturer that had disclosed an incident (title names the company), 18 June 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S40 iTnews, report on a Federal Court penalty against a fixed-income broker for cyber security failures (title names the broker), 9 February 2026. https://www.itnews.com.au/ (article URL withheld). Verified on 21 November 2026.

S41 iTnews, "Coles Group investigating a cyber incident", 16 November 2026. https://www.itnews.com.au/news/coles-group-investigating-a-cyber-incident-630361. Verified on 21 November 2026.

S42 Cyber Daily, report on a furniture retailer disclosing a cyber incident to the ASX (title names the retailer), 14 August 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S43 Cyber Daily, report on a book publisher and distributor restoring systems after unauthorised activity (title names the publisher), 27 August 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S44 iTnews, report on a small Australian online store kept closed after hijacked extensions redirected shoppers (title names the platform), 16 October 2026. https://www.itnews.com.au/ (article URL withheld). Verified on 21 November 2026.

S45 Cyber Daily, report on a global travel-technology provider's breach possibly affecting an Australian airline (title names both), 3 November 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S46 Cyber Daily, report on a Cl0p listing of 9 companies linked to two Australian IT service providers, 3 February 2026. https://www.cyberdaily.au/security/13172-exclusive-cl0p-cyber-extortion-group-targets-australian-it-providers-clients. Verified on 21 November 2026.

S47 Cyber Daily, report on the ABC wiping staff devices after a spyware campaign delivered through online advertising, 23 October 2026. https://www.cyberdaily.au/security/14347-aunty-hack-abc-wipes-staff-devices-after-discovering-spyware-campaign. Verified on 21 November 2026.

S48 OC Media, "Pro-Iran hackers claim responsibility for cyberattack on Azerbaijan, citing hijab ban", October 2026. https://oc-media.org/breaking-pro-iran-hackers-claim-responsibility-for-cyberattack-on-azerbaijan-citing-hijab-ban/. Verified on 21 November 2026.

S49 APA, "Azərbaycan informasiya resurslarına qarşı DDoS hücumlarında kommersiya xidmətindən istifadə edilib" (Commercial service used in DDoS attacks on Azerbaijani information resources), 16 October 2026. https://apa.az/ict/azerbaycan-informasiya-resurslarina-qarsi-ddos-hucumlarinda-kommersiya-xidmetinden-istifade-edilib-1005789. Verified on 21 November 2026.

S50 Cyber Daily, report on a state government's response to a ransomware group's claim (title names the government), 17 June 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S51 Cyber Daily, report on a cyber security incident notified to members of a state emergency service (title names the service), 30 June 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S52 Cyber Daily, report on a health-standards body denying a ransomware group's claim (title names the body), 18 June 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S53 Cyber Daily, report on a federal agency denying a forum persona's claim (title names the agency), 9 June 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S54 Cyber Daily, report on a state court service responding to a data security incident after forum claims (title names the service), 31 July 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S55 Cyber Daily, report on a state health department denying a ransomware group's claim (title names the department), 2 September 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S56 Cyber Daily, report on the NSW Police investigation into a cyber security incident at NSW Health, 4 November 2026. https://www.cyberdaily.au/security/14396-breached-nsw-police-investigating-major-cyber-security-incident-impacting-nsw-health. Verified on 21 November 2026.

S57 NIST National Vulnerability Database, CVE-2026-20127. https://nvd.nist.gov/vuln/detail/CVE-2026-20127. Verified on 21 November 2026.

S58 CISA and partners including ASD's ACSC, advisory AA26-113A on China-nexus covert networks of hijacked devices, 23 April 2026. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a. Verified on 21 November 2026.

S59 National Cyber Security Centre (New Zealand) with the ACSC and CERT Tonga, advisory on the INC Ransom affiliate model, 6 March 2026. https://www.ncsc.govt.nz/alerts/inc-ransom-affiliate-model-enabling-targeting-of-critical-networks/. Verified on 21 November 2026.

S60 Cyber Daily, report on Qilin listing four Australian victims in four days, 27 October 2026. https://www.cyberdaily.au/security/14358-exclusive-qilin-ransomware-group-claims-quartet-of-aussie-victims-in-as-many-days. Verified on 21 November 2026.

S61 Cyber Daily, report on a regional club confirming a contained incident after a Qilin listing (title names the club), 28 October 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S62 Cyber Daily, report on a suicide-prevention charity confirming a staff data breach after hacking claims (title names the charity), 14 July 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S63 Cyber Daily, "Aussie schools breach: Instructure boss reaches agreement with ShinyHunters to not release data", 12 May 2026. https://www.cyberdaily.au/security/13580-aussie-schools-breach-instructure-boss-reaches-agreement-with-shinyhunters-to-not-release-data. Verified on 21 November 2026.

S64 Cyber Daily, report on Queensland's education department confirming students and staff were affected by a supplier breach (title names the department and the crew), 7 May 2026. https://www.cyberdaily.au/security/13562-queensland-department-of-education-confirms-students-staff-impacted-by-shinyhunters-data-breach. Verified on 21 November 2026.

S65 iTnews, report on two Western Australian men charged as alleged principal participants of TeamPCP, 27 August 2026. https://www.itnews.com.au/ (article URL withheld). Verified on 21 November 2026.

S66 iTnews, "NDIA fended off March TeamPCP supply-chain hackers", 19 August 2026. https://www.itnews.com.au/news/ndia-fended-off-march-teampcp-supply-chain-hackers-628227. Verified on 21 November 2026.

S67 Palo Alto Networks Unit 42, "Threat Brief: Escalation of Cyber Risk Related to Iran", updated 17 April 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/. Verified on 21 November 2026.

S68 Stuart Crocker, "Hacktivism is an underestimated threat, especially in geopolitical crises", ASPI The Strategist, 23 June 2026. https://www.aspistrategist.org.au/hacktivism-is-an-underestimated-threat-especially-in-geopolitical-crises/. Verified on 21 November 2026.

S69 iTnews, "ASD warns Aussie Adobe Commerce and Magento stores under attack", 10 September 2026. https://www.itnews.com.au/news/asd-warns-aussie-adobe-commerce-and-magento-stores-under-attack-628811. Verified on 21 November 2026.

S70 iTnews, "Second alert from ACSC in two months shows unpatched CMS bugs still exploited", 10 July 2026. https://www.itnews.com.au/news/second-alert-from-acsc-in-two-months-shows-unpatched-cms-bugs-still-exploited-627256. Verified on 21 November 2026.

S71 iTnews, "Australia's big end of town is paying ransomware groups", 26 February 2026. https://www.itnews.com.au/news/australias-big-end-of-town-is-paying-ransomware-groups-623791. Verified on 21 November 2026.

S72 iTnews, "Poor WA gov M365 security led to $71k theft and children's data breached", 9 March 2026. https://www.itnews.com.au/news/poor-wa-gov-m365-security-led-to-71k-theft-and-childrens-data-breached-624118. Verified on 21 November 2026.

S73 iTnews, "WA local gov entity lost $350,000 in phishing attack", 1 April 2026. https://www.itnews.com.au/news/wa-local-gov-entity-lost-350000-in-phishing-attack-624680. Verified on 21 November 2026.

S74 Australian Federal Police and NSW Police Force, joint media release on three people charged over scam proceeds spent on gold bullion, 15 May 2026, as reported by iTnews. https://www.itnews.com.au/news/nsw-cyber-cops-bust-alleged-bullion-buying-bec-bandits-625906. Verified on 21 November 2026.

S75 Cyber Security Act 2024 (No. 98, 2024), sections 2, 26 and 27, Federal Register of Legislation. https://www.legislation.gov.au/C2024A00098/asmade/2024-11-29/text/2/epub/OEBPS/document_1/document_1.html. Verified on 21 November 2026.

S76 Department of Home Affairs, "Ransomware payment reporting" factsheet. https://www.homeaffairs.gov.au/cyber-security-subsite/files/factsheet-ransomware-payment-reporting.pdf. Verified on 21 November 2026.

S77 Department of Home Affairs, "Security standards for smart devices", web page. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/security-standards-for-smart-devices. Verified on 21 November 2026.

S78 Privacy and Other Legislation Amendment Act 2024 (No. 128, 2024), section 2 (commencement), Federal Register of Legislation. https://www.legislation.gov.au/C2024A00128/asmade/text. Verified on 21 November 2026.

S79 OAIC, "New resources on transparency for use of AI and automated decision-making", 30 September 2026. https://www.oaic.gov.au/news/media-centre/new-resources-on-transparency-for-use-of-ai-and-automated-decision-making. Verified on 21 November 2026.

S80 Cyber and Infrastructure Security Centre, guidance on notification of cyber security incidents under the SOCI Act 2018, 2026. https://www.cisc.gov.au/resources-subsite/Documents/ncsi-guidance.pdf. Verified on 21 November 2026.

S81 APRA, Prudential Standard CPS 234 Information Security. https://www.apra.gov.au/standards/cps-234. Verified on 21 November 2026.

S82 APRA, Prudential Standard CPS 230 Operational Risk Management. https://www.apra.gov.au/standards/cps-230. Verified on 21 November 2026.

S83 Privacy Act 1988, Part IIIC (sections 26WH, 26WK and 26WL), compilation of 4 June 2026, Federal Register of Legislation. https://www.legislation.gov.au/C2004A03712/2026-06-04/2026-06-04/text/original/epub/OEBPS/document_1/document_1.html. Verified on 21 November 2026.

S84 iTnews, "Privacy Act overhaul to tighten 72-hour breach reporting deadline", 1 September 2026. https://www.itnews.com.au/news/privacy-act-overhaul-to-tighten-72-hour-breach-reporting-deadline-628568. Verified on 21 November 2026.

S85 iTnews, "Gov proposes disclosure delay for most serious cyberattacks", 26 March 2026. https://www.itnews.com.au/news/gov-proposes-disclosure-delay-for-most-serious-cyberattacks-624575. Verified on 21 November 2026.

S86 Cyber Daily, report on APRA seeking an 8 million AUD penalty against a regional bank under the Banking Executive Accountability Regime (title names the bank), 11 August 2026. https://www.cyberdaily.au/ (article URL withheld). Verified on 21 November 2026.

S87 OAIC, "OAIC's action in relation to the 2023 Latitude Data Breach and information to update and assist individuals", 25 September 2026. https://www.oaic.gov.au/news/media-centre/oaics-action-in-relation-to-the-2023-latitude-data-breach-and-information-to-update-and-assist-individuals. Verified on 21 November 2026.

S88 ASIC, media release on a financial-advice licensee penalised 1.35 million AUD for cyber security failures (title names the licensee), October 2026. https://asic.gov.au/about-asic/news-centre/ (article URL withheld). Verified on 21 November 2026.

S89 OAIC, report on preliminary inquiries into a court transcription provider (title names the provider), 4 November 2026. https://www.oaic.gov.au/news/media-centre (article URL withheld). Verified on 21 November 2026.

S90 OAIC, media centre listing of releases July 2025-November 2026, including "Australian Clinical Labs ordered to pay penalties in relation to Medlab Pathology data breach in first for Privacy Act" (9 October 2025). https://www.oaic.gov.au/news/media-centre. Verified on 21 November 2026.

S91 Cisco, security advisory cisco-sa-sdwan-rpa-EHchtZk (CVE-2026-20127), first published 25 February 2026, updated 28 October 2026. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk. Verified on 21 November 2026.

S92 NIST National Vulnerability Database, CVE-2026-63077 (JetBrains TeamCity). https://nvd.nist.gov/vuln/detail/CVE-2026-63077. Verified on 21 November 2026.

S93 iTnews, "ASD warns Australian TeamCity servers under attack", 25 August 2026. https://www.itnews.com.au/news/asd-warns-australian-teamcity-servers-under-attack-628400. Verified on 21 November 2026.

S94 Adobe, security bulletin APSB26-146 for Adobe Commerce, 7 September 2026. https://www.adobe.com/trust/security/products/commerce/apsb26-146.html. Verified on 21 November 2026.

S95 NIST National Vulnerability Database, CVE-2026-75650 (Adobe Commerce; vendor bulletin APSB26-146). https://nvd.nist.gov/vuln/detail/CVE-2026-75650. Verified on 21 November 2026.

S96 Microsoft Security Response Center, CVE-2026-62911, 11 August 2026. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62911. Verified on 21 November 2026.

S97 N-able, "N-central security update", 10 August 2026. https://www.n-able.com/blog/n-central-security-update-august-10-2026. Verified on 21 November 2026.

S98 NIST National Vulnerability Database, CVE-2026-18556 (N-able N-central). https://nvd.nist.gov/vuln/detail/CVE-2026-18556. Verified on 21 November 2026.

S99 NIST National Vulnerability Database, CVE-2026-18577 (N-able N-central). https://nvd.nist.gov/vuln/detail/CVE-2026-18577. Verified on 21 November 2026.

S100 iTnews, "ASD warns of Australian attacks on N-able N-central RMM", 20 August 2026. https://www.itnews.com.au/news/asd-warns-of-australian-attacks-on-n-able-n-central-rmm-628282. Verified on 21 November 2026.

S101 NIST National Vulnerability Database, CVE-2025-32432 (Craft CMS). https://nvd.nist.gov/vuln/detail/CVE-2025-32432. Verified on 21 November 2026.

S102 Cyber Daily, "Australian Cyber Security Centre warns of ClickFix campaign leveraging Australian infrastructure", 7 May 2026. https://www.cyberdaily.au/security/13564-australian-cyber-security-centre-warns-of-clickfix-campaign-leveraging-australian-infrastructure. Verified on 21 November 2026.

S103 Cyber Daily, "Australian Signals Directorate warns of device code phishing activity targeting Microsoft 365 users", 20 May 2026. https://www.cyberdaily.au/security/13628-australian-signals-directorate-warns-of-device-code-phishing-activity-targeting-microsoft-365-users. Verified on 21 November 2026.

S104 iTnews, "ASD to critical infrastructure ops: be ready to isolate systems for three months", 28 July 2026. https://www.itnews.com.au/news/asd-to-critical-infrastructure-ops-be-ready-to-isolate-systems-for-three-months-627708. Verified on 21 November 2026.

Appendix D. Glossary

- **Blackhole:** Brandefense's cybercrime data source covering posts, infected devices, credentials and card material.
- **Ransompedia:** Brandefense's ransomware database; listings record criminal claims.
- **Atlas:** Brandefense's external exposure scoring; scores run from 0 (nothing observed) to 100.
- **Infected device:** a device infected with information-stealing malware and associated with the organisation's domain; "employee" is a classification, not verified employment.
- **Credential-market listing:** a credential tied to the domain offered on a monitored market at the time of the check.
- **Combolist:** a list of login and password pairs assembled from various sources; age and validity vary.
- **Stealer log:** data captured by information-stealing malware from a device.
- **Checker bot:** a bot that tests stolen cards against payment gateways and prints the result.
- **Card shop "base":** a batch of stolen cards offered together on a card shop, often labelled by countries.
- **Post card:** a redacted reproduction of one dark-web post, with venue, date, alias, language and what it does and does not establish.
- **Relay:** a third-party channel or bot that reposts another actor's claim; a relay is weaker evidence than the actor's own post.

- **Leak-site listing:** an extortion group's public post naming a victim; it is a claim, not a confirmed breach.
- **Loader:** a criminal who moves stolen funds into or out of bank accounts, often aged or rented accounts.
- **Fullz:** a full identity record (name, birth date, address, identifiers and often financial details) sold for fraud.
- **BEC (business email compromise):** fraud in which a criminal uses or imitates a business mailbox to redirect payments.
- **DMARC / SPF / DKIM:** email-authentication standards; DMARC tells receivers what to do with mail that fails.
- **DNSSEC:** signatures that let resolvers verify DNS answers.
- **DS record:** the record in the parent zone that links a domain to its DNSSEC keys.
- **TLP:CLEAR:** may be shared without restriction; other legal duties still apply.
- **AiTM (adversary-in-the-middle):** a phishing page that relays a real login and captures passwords, one-time codes and the session cookie.
- **Device-code phishing:** a lure that tricks a user into approving a sign-in for a device or application the attacker controls.
- **ClickFix:** a social-engineering technique that persuades a user to paste and run a command, often presented as a fake CAPTCHA.
- **BIN:** the issuer's card-number prefix (bank identification number).
- **APP entity:** an organisation or agency bound by the Australian Privacy Principles in the Privacy Act 1988.
- **Notifiable data breach:** a breach likely to result in serious harm, which APP entities must notify to the OAIC and affected individuals.
- **Headline score:** the national Atlas figure for the 250 organisations; it is not an average.
- **Listing history:** a credential tied to the domain had already been offered for sale on a monitored market before the current check.
- **DDoS (distributed denial of service):** an attack that floods a service with traffic from many sources to make it unavailable.
- **SaaS (software as a service):** software that a supplier hosts and runs for customers over the internet.
- **HSTS:** a web header telling browsers to use HTTPS only.
- **KYC:** "know your customer" identity checks at banks, exchanges and other services.
- **MFA (multi-factor authentication):** a sign-in that needs a second factor beyond the password.
- **p=none:** a DMARC policy that only monitors and does not ask receivers to reject or quarantine.
- **Passive hygiene index:** an Odin analytical composite of email, DNS, TLS and header checks; 0-100, higher means weaker.
- **Phishing-resistant MFA:** sign-in tied to the real site (FIDO2 security keys, passkeys or certificates), so a relay page cannot reuse it.
- **RTO:** recovery time objective, the longest outage a business-continuity plan allows.
- **ACSC:** the Australian Cyber Security Centre, part of ASD.
- **AFP:** the Australian Federal Police.
- **APRA:** the Australian Prudential Regulation Authority, which supervises banks, insurers and superannuation funds.

- **ASD:** the Australian Signals Directorate, the federal signals intelligence and cyber security agency.
- **ASIC:** the Australian Securities and Investments Commission, the corporate and financial-services regulator.
- **ASIO:** the Australian Security Intelligence Organisation, the domestic security intelligence agency.
- **ASX:** the Australian Securities Exchange; listed companies disclose material incidents through it.
- **CAA:** a DNS record that names the certificate authorities allowed to issue certificates for a domain.
- **CISA:** the United States Cybersecurity and Infrastructure Security Agency, which keeps a list of known exploited vulnerabilities.
- **CMS:** content management system, such as WordPress or Craft CMS.
- **ERP / CRM:** enterprise resource planning and customer relationship management software.
- **Five Eyes:** the intelligence partnership of Australia, Canada, New Zealand, the United Kingdom and the United States; its cyber agencies issue joint alerts.
- **MX record:** the DNS record that names a domain's mail servers.
- **NCSC:** a National Cyber Security Centre; in this report, New Zealand's.
- **OAIC:** the Office of the Australian Information Commissioner, the privacy regulator.
- **OT:** operational technology, the systems that run physical processes.
- **OTC:** "over the counter"; in market posts, direct trades of accounts or currency outside an exchange.
- **SD-WAN:** software-defined wide-area networking, used to link branch networks.
- **TAFE:** Technical and Further Education, Australia's public vocational colleges.

About this report

Prepared by Odin by Brandefense. Version 1.0 was completed on 21 November 2026.

Research cutoff: 18 November 2026 (primary data window). The report prioritises Brandefense's own data, keeps criminal claims separate from independently established incidents and does not claim a complete census of cybercrime affecting Australia. Recommendations describe what organisations could do; they do not state that any organisation has or has not done them. This edition is in English only.

© 2026 Brandefense. All rights reserved.