FalconFeeds

Democratising Cybersecurity
www.falconfeeds.io

Cyber Threat Intelligence Report: Australia H1 2025

Unpacking the Numbers, Patterns, and Implications for National Cyber Resilience

The Deepest Watch on the Darkest Web

FalconFeeds.io delivers the largest real-time monitoring of deep and dark web activity—from ransomware gangs to Telegram dumps and access marketplaces.

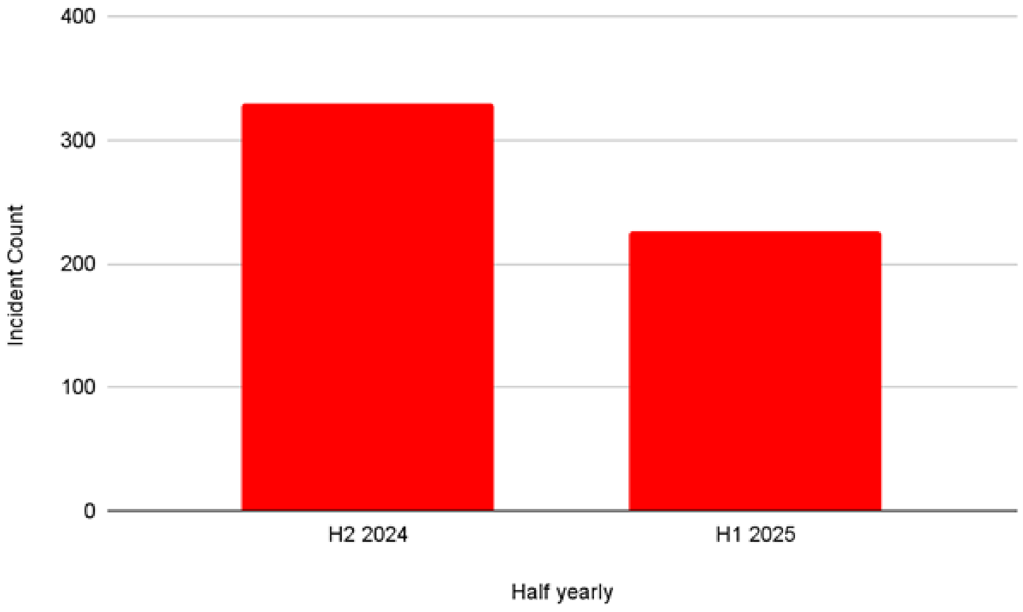
Executive Summary

Calm Before a Storm?

Attackers didn't retreat. They just upgraded their toolkit.

Australia saw a sharp **31% drop in reported cyber incidents** in H1 2025 compared to H2 2024—**226 vs. 329 attacks.** On the surface, this might appear as a win. But a closer look reveals a more complex reality: **while frequency dipped, sophistication rose.**

Ransomware remained dominant, initial access listings spiked in Q2, and underground chatter showed growing attention on Australian networks. For critical industries—especially **Tech, Finance, and Healthcare**—the threat is no less real. Australia may be momentarily off the radar in terms of volume, but cybercriminals are simply shifting gears.



Monthly Attack Patterns

A Game of Timing

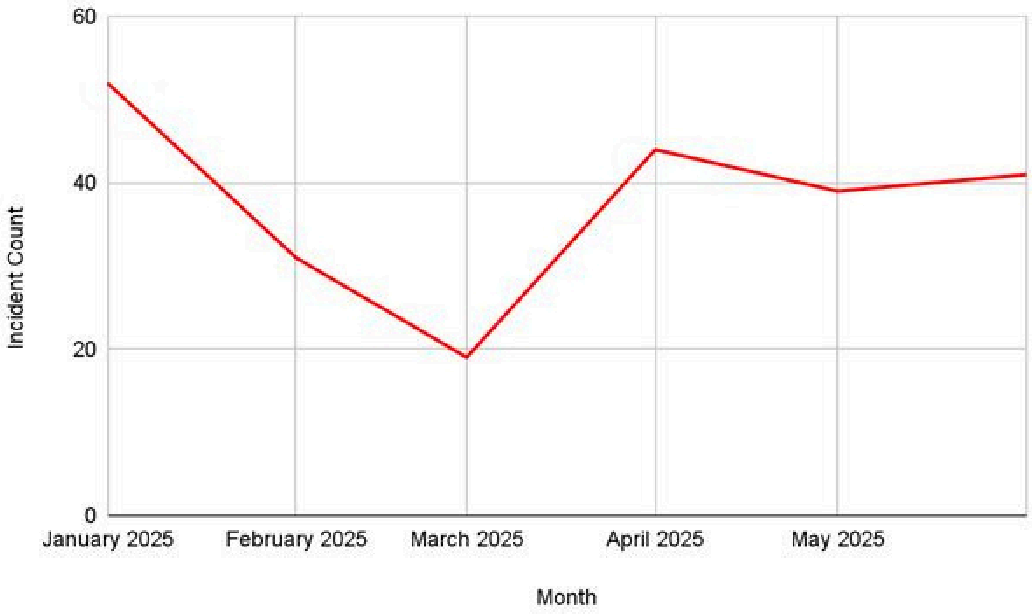
Attack distribution across H1 2025:

- **January:** 52 incidents (peak)
- **February:** 31
- **March:** 19 (lowest)
- **April:** 44
- **May:** 39
- **June:** 41

The story?

A Q1 cooldown followed by a Q2 ramp-up.

Analysts interpret this as the winding down of one actor campaign and the beginning of another—suggesting coordinated, cyclic operations, not random noise.

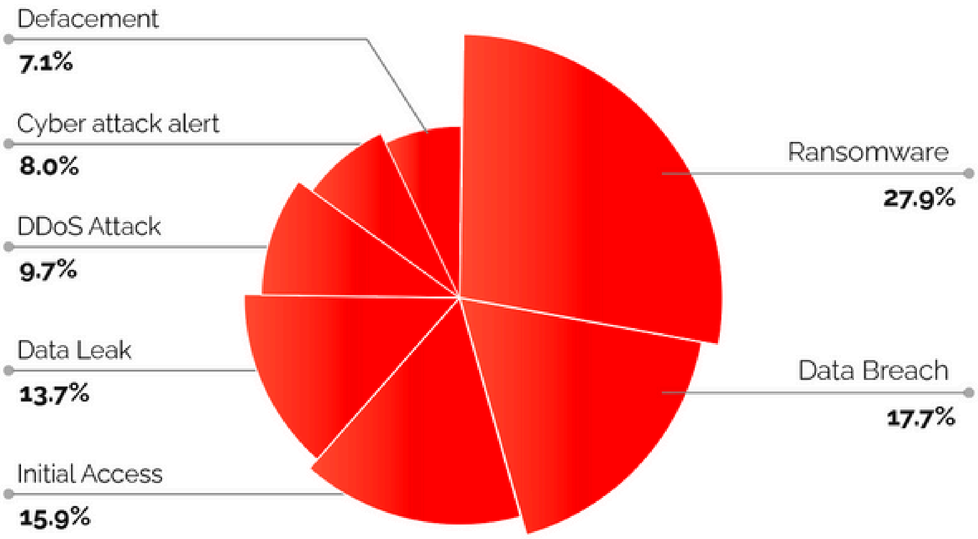


What's Hitting Us and How Often?

Top Threat Categories in H1 2025:

The spike in Initial Access Listings signals Australia's growing value as an entry point in global cybercrime. Notably, these listings often precede ransomware attacks.

- **Ransomware:** 63 incidents (28% of total)
- **Data Breaches:** 40
- **Initial Access Listings:** 36
- **Data Leaks:** 31
- **DDoS Attacks:** 22
- **Cyber Attack Alerts:** 18
- **Website Defacements:** 16

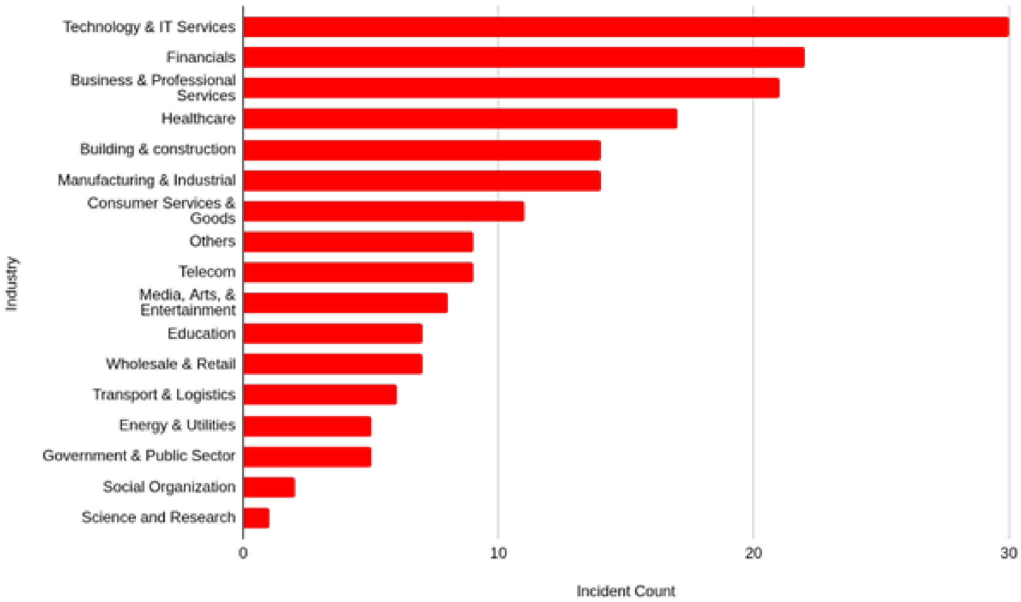


Who’s Being Targeted and Why It Matters

Sectoral Breakdown:

Tech and Business Services are targeted not just for what they hold—but **who they’re connected to.** These industries are **supply chain amplifiers,** making them high-leverage targets.

Sector	Incidents
Technology & IT Services	30
Financial Services	22
Business & Professional Services	21
Healthcare	17
Manufacturing & Construction	14 each



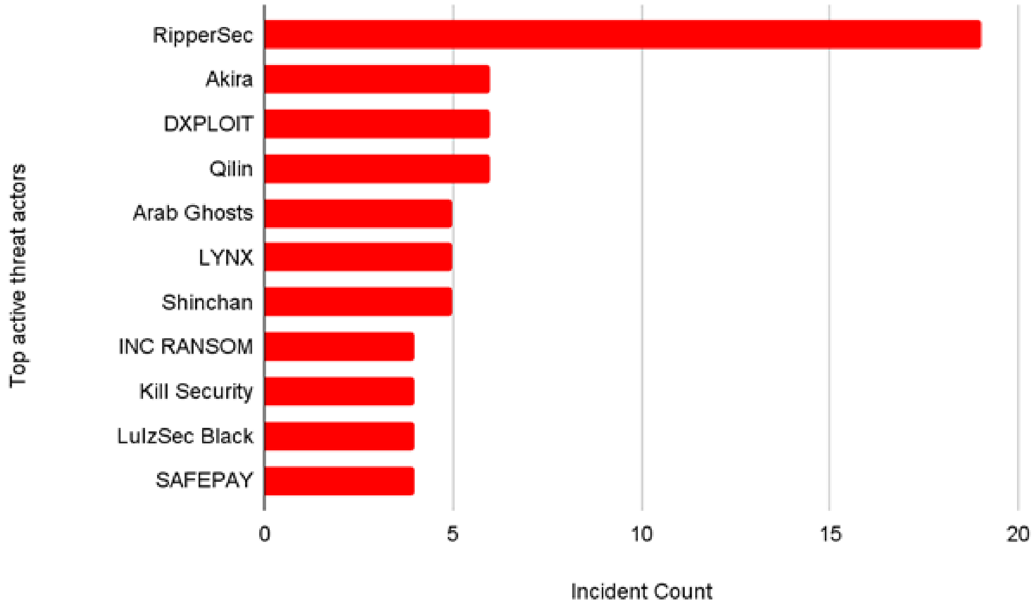
Which Actors Are Active in Australia?

Australia was targeted by **over 100 unique threat actors.** These weren't just ransomware crews—they included defacers, DDoS operators, and access brokers.

The fragmented threat landscape means more noise, more unpredictability, and a faster threat cycle.

Top groups:

- **RipperSec:** 19 attacks
- **Akira, Qilin, DXPLOIT:** 6 each
- **Arab Ghosts Hackers, LYNX, Shinchan:** 5 each
- **SAFEPAY, Kill Security, INC RANSOM:** 4 each



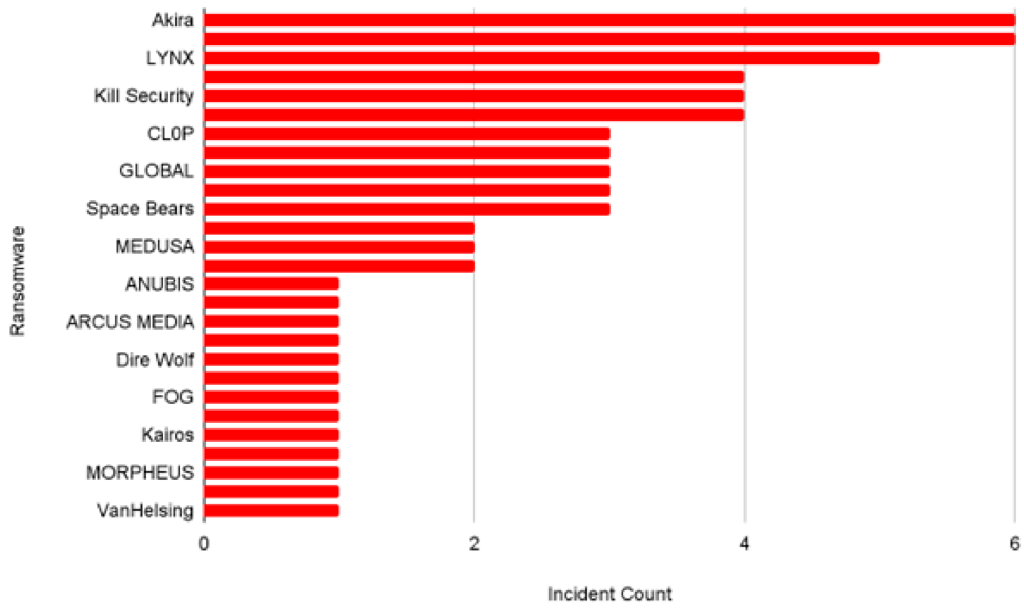
Ransomware's Grip on Australian Targets

Ransomware accounted for **63 of the 226 total incidents** in H1. These were led by **27 different groups**—showcasing how commoditized and accessible ransomware has become.

Affected sectors spanned Healthcare, Manufacturing, Construction, and Finance, reflecting **no safe zones left.**

Top Ransomware Actors in Australia (H1 2025):

- Akira & Qilin: 6 each
- LYNX: 5
- SAFEPAY, INC RANSOM, Kill Security: 4
- CL0P, DragonForce, Space Bears: 3

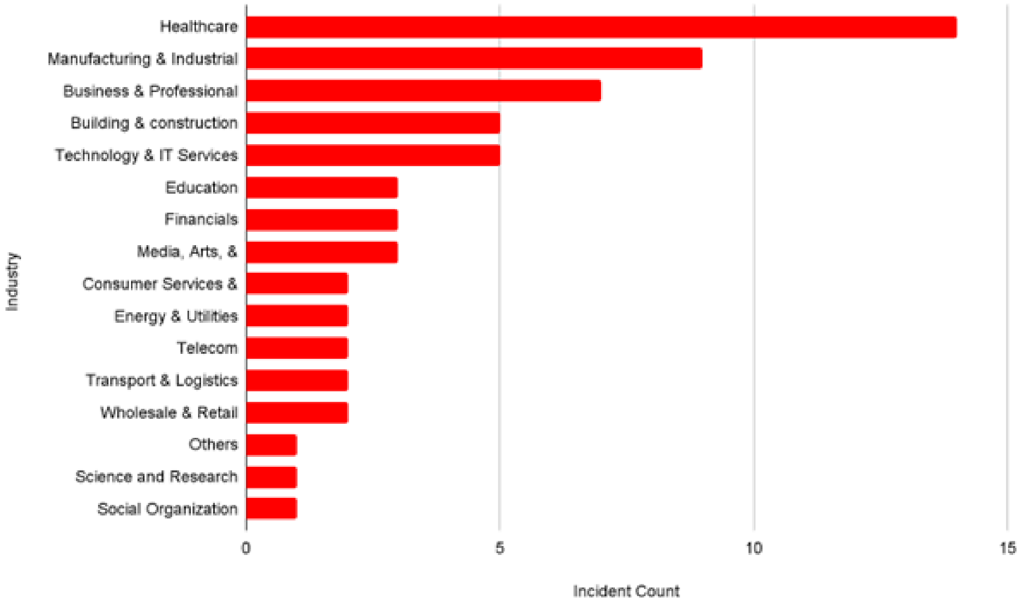


Sector Snapshot of Ransomware

Takeaway:

Attackers aren't chasing volume—they're chasing vulnerability

Healthcare (14): Still the most targeted—sensitive data and critical services make it a prime ransomware victim.
Manufacturing (9): Legacy tech and operational urgency leave it vulnerable.
Business Services (7): Data-rich and reputation-sensitive—an easy mark.
Tech & Construction (5 each): Digitally connected, but often under-secured.
Others: Education, finance, and telecom saw scattered hits.



Where the Threats Are Brewing

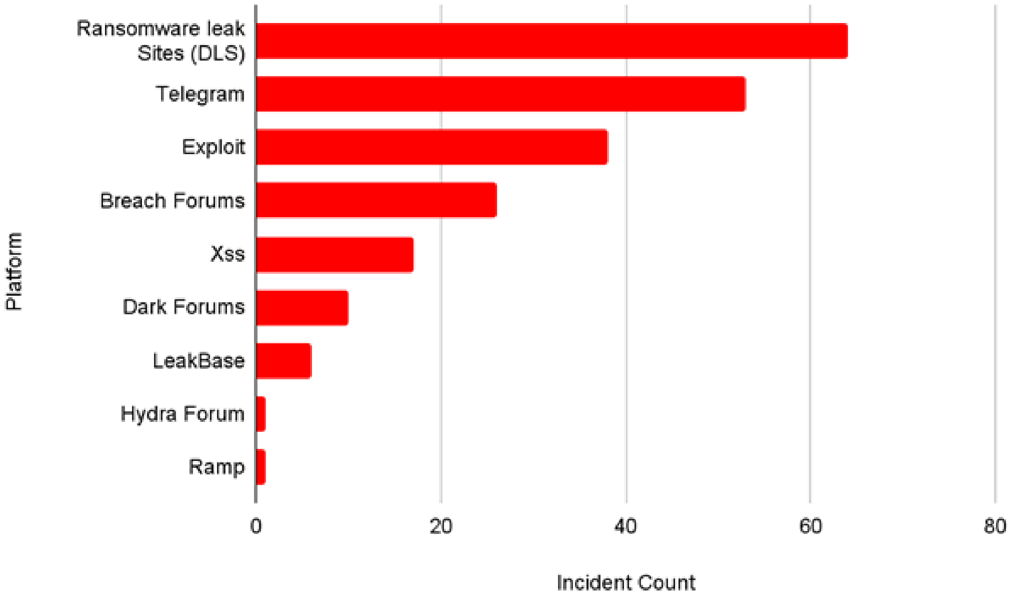
Platform Analysis

The modern cyber battlefield is highly distributed, and Australia is deeply exposed to it.

Top Platforms Used in Australia-Related Threat Activity:

- **Ransomware DLS (Leak Sites):** 64
- **Telegram:** 53
- **Exploit Forums:** 38
- **Breach Forums:** 26
- **XSS, Dark Forums, LeakBase:** various uses

Telegram remains the **real-time engine of hacktivist ops,** while leak sites serve as extortion stages and reputation management tools for threat actors.



H1 Trends

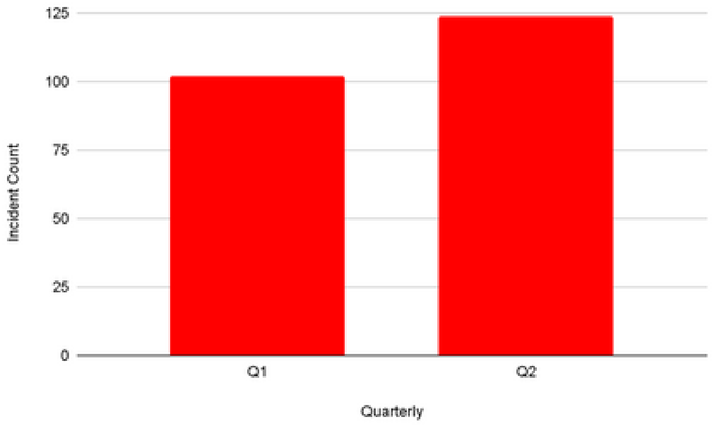
What Shifted in Q2?

Q2 brought smarter attacks. Uncover the surge in stealthy access sales and data leaks.

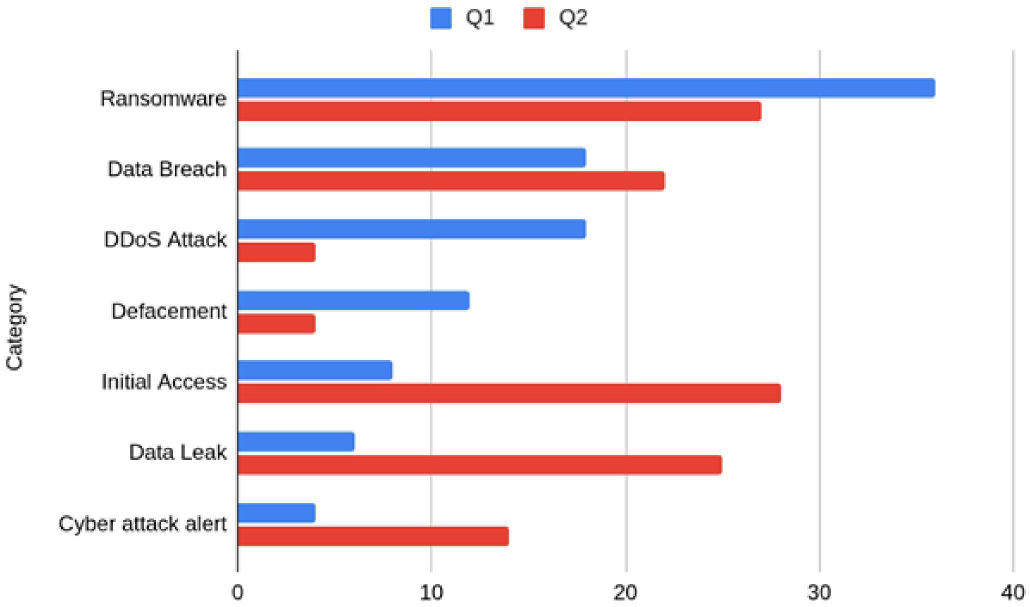
While overall incident numbers dropped from H2 2024, Q2 2025 alone saw more action than Q1.

- **Q1:** 102 incidents
- **Q2:** 124 incidents

Q1 was defined by noise (DDoS, ransomware). Q2 got quieter—but smarter, with surging access sales and stealthier data leaks.



Category Shift Insight:

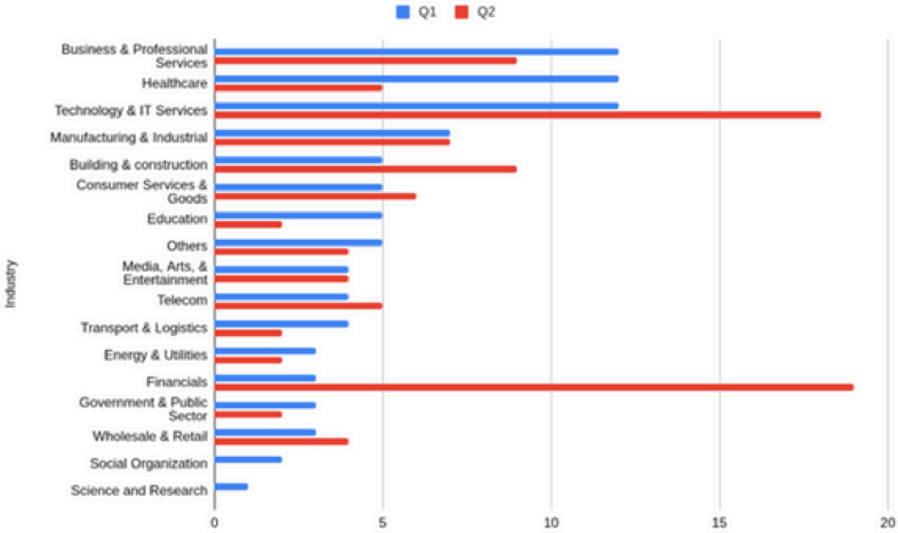


Industry Focus Shifts

(Q1 vs. Q2 2025)

Tech remained a constant — targeted both as a direct victim and a supply chain gateway.

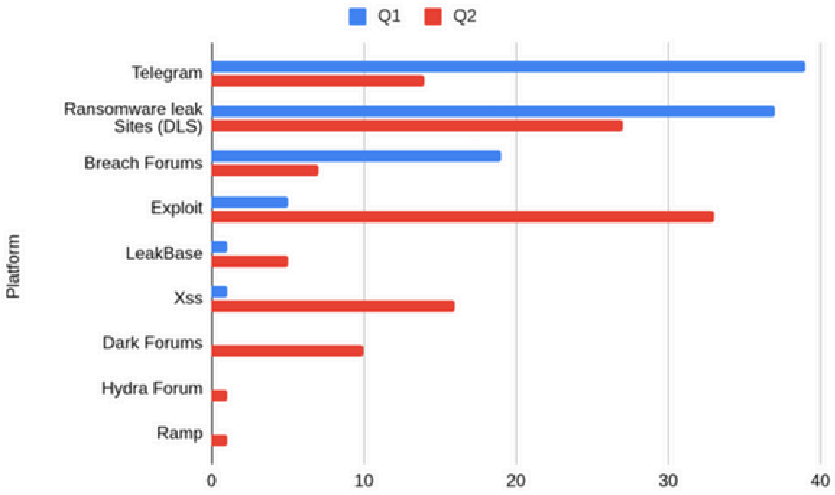
- **Q1:** Attacks cantered on Healthcare, Tech, and Business Services.
- **Q2:** Shift toward Financials, Tech, and Construction.



Platform Usage Trends

Threat actors are getting more strategic — planning breaches before broadcasting them.

- **Q1:** Telegram and Ransomware Leak Sites led threat coordination.
- **Q2:** Exploit forums gained traction, reflecting deeper focus on access sales and tool trading.



What Australia Should Do Now

Australia: Fewer attacks, more private sales. Act now to counter hidden threats.

Key Takeaways:

- Australia may be seeing fewer attacks, but **it's being sold more in private.**
- Initial access listings **point to future ransomware attacks.**
- **Healthcare and Tech firms are under silent siege**—especially those with third-party linkages.

Recommendations:

- Enforce **MFA and network segmentation.**
- Monitor **dark web markets for access listings.**
- Patch known vulnerabilities quickly.
- Conduct **ransomware response simulations.**
- Train employees to spot **social engineering and phishing attempts.**

How FalconFeeds.io Helps Australia Stay Ahead

From noisy DDoS chatter to stealthy initial access listings—FalconFeeds helps translate threat signals into action.

FalconFeeds.io provides:

- **Live monitoring** of DLS, forums, Telegram, breach sites.
- **Early alerts** on actor claims, access listings, and mentions of Australian companies.
- **Custom threat feeds** by industry and region.
- **Actor attribution** to correlate attacks with group TTPs
- **Support for investigations and remediation** through threat actor tagging and historical context.

Conclusion

Australia’s Cyber Silence Isn’t Safety

As threats grow stealthier, see them before damage. Stay prepared with FalconFeeds.

A decline in reported attacks is not a decline in risk. As cybercrime becomes quieter, stealthier, and more persistent, Australia remains squarely in scope—as both a direct target and an attack vector in global campaigns.

It’s not about if attackers are coming.
It’s about whether you see them before they do damage.

Stay safe and prepared with Falconfeeds. Get your 14-day free trial today!