ANOMALI

AUSTRALIA'S RANSOMWARE THREAT LANDSCAPE

INDUSTRY TARGETING AND 2026 FORECAST

REPORT DATE: January 2026

SCOPE AND METHODOLOGY

This report summarizes observed ransomware targeting across Australian industries based on threat intelligence collected during the previous calendar year, using ransomware targeting-to-industry mappings to assess where ransomware activity appears most consistently concentrated.

The dataset represents observed targeting presence, not confirmed compromise. Indicators show whether ransomware has been assessed as targeting an industry during the reporting period; they do not measure frequency, victim count, operational impact, or the severity of individual incidents. As a result, the analysis should be interpreted as a sector exposure and pressure model, rather than a definitive ranking of "most attacked" industries.

The dataset comprises 73 distinct entries including both organized threat groups and malware families. The term "ransomware entities" is used throughout as a neutral umbrella term that encompasses both types. This terminology is necessary because the dataset includes both organized actors (e.g., Play) and malware families (e.g., Clop)—referring to all 73 as "groups" or "malware families" would be analytically inaccurate. Both are tracked identically for industry targeting patterns.

EXECUTIVE SUMMARY

Ransomware targeting in Australia shows clear concentration around a small set of high-leverage industries. The data suggests that ransomware groups continue to prioritize sectors that offer strong extortion leverage through a combination of operational disruption risk, data sensitivity, and downstream supply-chain impact.

KEY OBSERVATIONS:

Targeting concentration is highest in five industries: Technology, Financial Services, Manufacturing, Healthcare, and Energy.

Technology stands out as the most consistently targeted sector, reflecting both direct monetization potential and its role as an access pathway into other organizations and environments.

Multiple ransomware entities demonstrate broad cross-industry scope, indicating many ransomware operations are not constrained by sector specialization and may pursue targets opportunistically based on access and leverage.

Sector pressure and actor breadth should be treated as indicators of systemic exposure, not predictions of attack likelihood.

RANSOMWARE ENTITIES

73

Targeting Australia

HIGH PRESSURE SECTORS

9

50%+ Group Targeting

INDUSTRIES ANALYZED

18

Across the Economy

BROADEST ENTITY

12

Industries (Play)

INDUSTRIES RANKED BY RANSOMWARE TARGETING

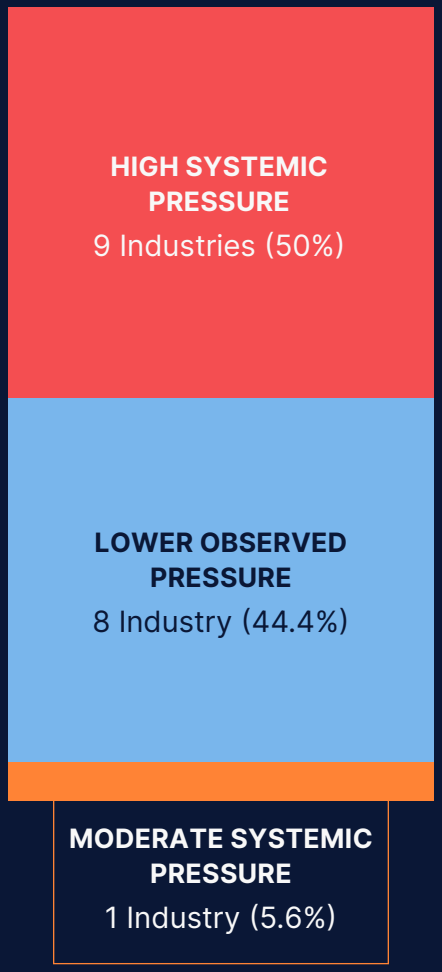
The following analysis examines which Australian industries appear most frequently within ransomware targeting scope during 2025. This data reveals clear patterns of concentration, with certain sectors consistently appearing across a majority of observed ransomware groups.

The data shows extreme concentration at the top of the distribution. Technology (67 groups, 92%), Financial Services (66 groups, 90%), and Manufacturing (63 groups, 86%) dominate the targeting landscape, while the majority of industries face substantially lower observed pressure.

RANK	INDUSTRY	CODE	GROUP TARGETING	% OF ALL GROUPS
1	Technology	TCH	67	92%
2	Financial Services	FIN	66	90%
3	Manufacturing	MFG	63	86%
4	Healthcare	HLT	58	79%
5	Energy	NRG	54	74%
6	Education	EDU	45	62%
7	Government	GOV	43	59%
8	Government-Public-Services	GPS	41	56%
9	Construction	CON	37	51%
10	Retail	RTL	8	11%
11	Agriculture	AGR	6	8%
12	Commercial	COM	3	4%
13	Chemical	CHM	3	4%
14	Transportation	TRN	3	4%
15	Utilities	UTL	2	3%
16	Aerospace	AER	1	1%
17	Automotive	AUT	1	1%
18	Entertainment	ENT	1	1%

SECTOR PRESSURE BANDS

To support risk prioritization, industries can be grouped into pressure bands based on how broadly they appear within ransomware targeting scope. This framework helps distinguish between sectors facing systemic exposure versus those with more limited observed targeting.



HIGH SYSTEMIC PRESSURE

9

- Technology
- Financial Services
- Manufacturing
- Healthcare
- Energy
- Education
- Government
- Gov-Public-Services
- Construction

Targeted by 50%+ of ransomware entities (≥37 groups)

The top five sectors reflect maximum extortion leverage; these sectors combine high operational disruption risk with data sensitivity and time-critical business impact that increases payment pressure to ransomware demands.

MODERATE SYSTEMIC PRESSURE

1

- Retail

Targeted by 10-49% of ransomware entities (7-36 groups)

Retail can be profitable for threat actors, but it typically delivers less consistent urgency and leverage than highly regulated or operationally critical sectors.

LOWER OBSERVED PRESSURE

8

- Agriculture
- Commercial
- Chemical
- Transportation
- Utilities
- Aerospace
- Automotive
- Entertainment

Targeted by <10% of ransomware entities (<7 groups)

Lower observed pressure may reflect Australia's economic structure. Several sectors have limited domestic operations (automotive manufacturing ceased in 2017) or overlap with broader industry categories. These sectors typically offer less operational leverage or payment capacity than high-pressure industries, though individual organizations may still present attractive targets based on their specific profile.

RANSOMWARE-BY-INDUSTRY TARGETING MATRIX

While the previous sections show aggregate patterns, the following heatmap provides granular visibility into which specific ransomware entities have targeted which industries. This enables identification of overlapping threats and assessment of exposure at the individual entity level.

Each cell indicates observed targeting presence during 2025. The matrix reveals both narrow specialists and broad opportunistic ransomware entities, highlighting the diversity of threat profiles Australian organizations face.

RANSOMWARE HEAT MAP - AUSTRALIAN INDUSTRY TARGETING

Industry targeting coverage by ransomware entities operating against Australian organizations (2025)

Actively Targeting Not Observed

THREAT ACTOR	TCH	FIN	MFG	HLT	NRG	EDU	GOV	GPS	CON	RTL	AGR	COM	CHM	TRN	UTL	AER	AUT	ENT	TOTAL
8BASE	●	●	●	●	●	●	●												7
ABYSS	●	●	●	●	●		●		●	●									8
AKIRA	●	●	●	●	●	●	●	●	●	●	●								11
ALPHV	●	●	●	●	●														5
ANUBIS		●	●	●	●				●										5
APT73	●	●	●	●	●		●	●											7
ARCUSMEDIA	●	●	●	●		●	●	●	●										8
AVADDON	●				●														2
BABUK2	●	●	●	●	●	●		●											7
BEAST	●	●	●	●	●	●		●	●										8
BIANLIAN	●	●	●	●	●		●	●	●										8
BLACKBASTA	●	●	●	●	●		●												6
BLACKBYTE	●	●	●				●												4
BLACKLOCK	●	●	●	●	●	●		●	●										8
BLACKSHRANTAC	●	●	●	●	●			●	●										7

Actively Targeting Not Observed

THREAT ACTOR	TCH	FIN	MFG	HLT	NRG	EDU	GOV	GPS	CON	RTL	AGR	COM	CHM	TRN	UTL	AER	AUT	ENT	TOTAL
BLACKSUIT	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	9
BROTHERHOOD	○	●	●	○	●	○	○	●	●	○	○	○	○	○	○	○	○	○	5
CACTUS	●	●	●	●	●	●	●	○	●	○	○	○	○	○	○	○	○	○	8
CHAOS	●	●	●	●	○	○	○	●	●	○	○	○	○	○	○	○	○	○	6
CLOAK	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	8
CLOP	●	●	●	●	●	●	●	●	●	○	○	●	●	○	○	○	○	○	11
COINBASECARTEL	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	6
D4RK4RMY	●	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	3
DIREWOLF	●	●	●	●	●	●	○	●	●	○	○	○	○	○	○	○	○	○	8
DRAGONFORCE	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	9
ELDORADO	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	7
EMBARGO	●	●	●	●	○	○	●	○	○	○	○	○	○	○	○	○	○	○	5
EVEREST	●	●	●	●	●	○	○	●	●	○	○	○	○	○	○	○	○	○	7
FLOCKER	●	●	○	○	○	●	●	●	○	○	○	○	○	○	○	○	○	○	5
FOG	●	●	●	●	●	●	●	●	○	●	○	○	○	○	○	○	○	○	9
FUNKSEC	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	8
GLOBAL	●	●	●	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○	5
HIVE	●	●	●	○	●	○	●	○	●	○	○	●	○	●	●	○	●	○	10
HUNTERS	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	9
INCRANSOM	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	9

Actively Targeting | Not Observed

THREAT ACTOR	TCH	FIN	MFG	HLT	NRG	EDU	GOV	GPS	CON	RTL	AGR	COM	CHM	TRN	UTL	AER	AUT	ENT	TOTAL
INTERLOCK	●	●	●	●	○	●	●	●	●	○	○	○	○	○	○	○	○	○	8
J	○	●	●	○	●	●	○	●	●	○	○	○	○	○	○	○	○	○	6
KAIROS	●	●	●	●	●	●	○	●	○	●	○	○	○	○	○	○	○	○	8
KILLSEC	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	9
KNIGHT	●	●	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	4
KRYPTOS	○	○	○	○	○	●	○	●	○	○	○	○	○	○	○	○	○	○	2
LOCKBIT3	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	7
LYNX	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	10
MAZE	●	○	○	○	●	○	○	○	○	○	○	●	●	○	○	○	○	○	4
MEDUSA	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	9
MEOW	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	7
MOGILEVICH	○	●	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	2
MONEYMESSAGE	●	○	○	●	○	●	●	●	○	○	○	○	○	○	○	○	○	○	5
MONTI	●	●	●	●	●	○	●	○	○	○	○	○	○	○	○	○	○	○	6
MORPHEUS	○	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	4
NETWALKER	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	1
PEAR	●	●	●	●	○	●	○	●	●	○	○	○	○	○	○	○	○	○	7
PLAY	●	●	●	●	●	●	●	●	●	○	●	●	○	●	○	○	○	○	12
QILIN	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	11
QUANTUM	●	●	●	○	●	●	●	○	●	○	○	●	○	●	●	●	○	○	11

Actively Targeting | Not Observed

THREAT ACTOR	TCH	FIN	MFG	HLT	NRG	EDU	GOV	GPS	CON	RTL	AGR	COM	CHM	TRN	UTL	AER	AUT	ENT	TOTAL
RADAR	●	●	●	●	○	○	○	○	●	○	○	○	○	○	○	○	○	○	5
RANSOMEXX	●	●	●	●	○	○	●	○	○	○	○	○	○	○	○	○	○	○	5
RANSOMHOUSE	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	9
RANSOMHUB	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	9
RAWORLD	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	7
REVIL	●	○	○	○	●	○	○	○	○	○	○	●	●	○	○	○	○	○	4
RHYSIDA	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	8
SAFEPAY	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	10
SARCOMA	●	●	●	●	●	○	○	○	●	●	○	○	○	○	○	○	○	○	7
SHINYHUNTERS	●	●	●	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	5
SINOBI	●	●	●	●	●	●	○	●	●	○	○	○	○	○	○	○	○	○	8
SPACEBEARS	●	●	●	●	○	○	●	●	●	○	○	○	○	○	○	○	○	○	7
TERMITE	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	7
THREEAM	●	●	●	●	○	●	●	○	○	○	○	○	○	○	○	○	○	●	7
TRIGONA	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	4
VANHELSING	●	●	○	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○	4
WARLOCK	●	●	●	●	●	●	○	○	●	○	○	○	○	○	○	○	○	○	7
WORLDLEAKS	●	●	●	●	●	●	○	●	●	○	○	○	○	○	○	○	○	○	8
TOTAL	67	66	63	58	54	45	43	41	37	8	6	3	3	3	2	1	1	1	

COLUMN KEY: TCH=Technology | FIN=Financial Services | MFG=Manufacturing | HLT=Healthcare | NRG=Energy | EDU=Education | GOV=Government | GPS=Government-Public-Services | CON=Construction | RTL=Retail | AGR=Agriculture | COM=Commercial | CHM=Chemical | TRN=Transportation | UTL=Utilities | AER=Aerospace | AUT=Automotive | ENT=Entertainment

STRATEGIC CONTEXT: WHY THESE SECTORS ARE TARGETED

Understanding which industries are targeted most frequently is only part of the picture. The following analysis examines the strategic factors that make specific sectors attractive to ransomware operators, including leverage dynamics, disruption impact, and downstream multiplier effects.

TECHNOLOGY

Technology shows the highest overlap across ransomware entities, reflecting its role as both a direct extortion target and an access pathway into other environments. Compromise in this sector can enable downstream impact across multiple industries, particularly where managed service providers, cloud platforms, or software supply chains are involved. This positioning makes Technology not only high-value, but multiplicative in impact.

FINANCIAL SERVICES

Financial Services remains a core ransomware target due to data sensitivity, regulatory pressure, and time-critical operations. Its presence across a wide range of ransomware entities suggests it is viewed as a consistently reliable source of leverage regardless of campaign maturity or operating model. Even limited disruption can carry outsized financial, legal, and reputational consequences, increasing attacker confidence in payment pressure.

MANUFACTURING

Manufacturing appears prominently due to its operational fragility and low tolerance for downtime. Ransomware groups targeting this sector often prioritize disruption leverage over data value, reflecting a focus on rapid extortion outcomes rather than prolonged negotiation. Legacy systems, OT dependencies, and constrained maintenance windows further increase exposure during recovery efforts.

HEALTHCARE

Healthcare's consistent presence indicates it remains a high-pressure environment, where service disruption and patient safety considerations can significantly influence response decisions. Its targeting by both narrow and broad scope actors reinforces its perceived leverage value.

ENERGY

Energy stands out as both an operational and strategic target. Its frequent appearance alongside commercial sectors suggests ransomware groups increasingly view it as part of the core economic attack surface rather than a specialised critical-infrastructure niche. This pattern indicates convergence between financially motivated targeting and infrastructure-adjacent risk, especially where IT and OT environments intersect.

RANSOMWARE TARGETING BREADTH AND SCOPE

Having examined industry-level patterns, this section shifts focus to the ransomware entities themselves. The 73 entities assessed show significant variation in targeting breadth, from single-industry specialists to broad opportunistic operators pursuing targets across two-thirds of the economy.

The distribution reveals that Australia's exposure is driven less by a handful of exceptionally broad operators and more by a large "generalist tier." While five entities target 11 to 12 industries, the largest concentration (40%) operates across seven to eight sectors. This suggests cross-industry flexibility is the norm among ransomware entities targeting Australia, with most maintaining capability to pursue targets across multiple industries rather than focusing on narrow sector expertise.

Breadth of targeting reflects operational flexibility, access dependencies, and strategic intent. It does not directly indicate attack volume or impact, but signals which entities maintain the infrastructure and tradecraft to operate across diverse environments.

RANSOMWARE ENTITIES RANKED BY BREADTH OF TARGETING

Higher breadth can be interpreted as a marker of cross-sector flexibility or access-driven targeting.

Table shows top 30 groups. Full ranking includes 73 actors ranging from 1 to 12 industries.

RANK	ENTITY	INDUSTRIES TARGETED
1	play	12
2	akira	11
2	clop	11
2	qilin	11
2	quantum	11
6	hive	10
6	lynx	10
6	safepay	10
9	blacksuit	9
9	dragonforce	9
9	fog	9
9	hunters	9
9	incransom	9
9	killsec	9
9	medusa	9
9	ransomhouse	9
9	ransomhub	9
18	abyss	8
18	arcusmedia	8
18	beast	8
18	bianlian	8
18	blacklock	8
18	cactus	8
18	cloak	8
18	direwolf	8
18	funksec	8
18	interlock	8
18	kairos	8
18	rhysida	8
18	sinobi	8
18	worldleaks	8

TARGETING EXTREMES: NARROW SPECIALISTS VS BROAD OPPORTUNISTS

The spectrum of targeting breadth ranges from single-industry specialists to entities pursuing targets across two-thirds of the economy. These extremes illustrate fundamentally different operational models and risk profiles.

NARROW TARGETING: SECTOR-FOCUSED OPERATIONS

Five entities exhibit highly constrained targeting, limited to one to three industries. This pattern may reflect specialized access vectors, sector-specific expertise, or deliberately focused operations.

ENTITY	INDUSTRIES TARGETED	FOCUS AREAS
netwalker	1	Energy
avaddon	2	Energy, Financial Services
kryptos	2	Education, Government-Public-Services
mogilevich	2	Government, Technology
d4rk4rmy	3	Education, Financial Services, Technology

BROAD TARGETING: CROSS-SECTOR OPERATORS

Four ransomware entities demonstrate exceptionally broad scope, targeting 11-12 industries. This breadth suggests flexible opportunistic approaches, diverse access pathways, or mature affiliate networks capable of pursuing targets across the entire economic landscape.

PLAY — 12 INDUSTRIES

- Agriculture
- Commercial
- Construction
- Education
- Energy
- Financial Services
- Government
- Government-Public-Services
- Healthcare
- Manufacturing
- Technology
- Transportation

AKIRA — 11 INDUSTRIES

- Commercial
- Construction
- Education
- Energy
- Financial Services
- Government
- Government-Public-Services
- Healthcare
- Manufacturing
- Retail
- Technology

CLOP — 11

- Agriculture
- Chemical
- Construction
- Education
- Energy
- Financial Services
- Government
- Government-Public-Services
- Healthcare
- Manufacturing
- Technology
- Industries

QILIN — 11 INDUSTRIES

- Commercial
- Construction
- Education
- Energy
- Financial Services
- Government
- Government-Public-Services
- Healthcare
- Manufacturing
- Retail
- Technology

PATTERN ANALYSIS

The broadest ransomware entities: play, quantum, clop, and akira, consistently span both high-value commercial sectors and critical infrastructure. This suggests mature operating models capable of adapting to diverse environments rather than relying on sector-specific tradecraft.

Notably, play remains the only actor observed across 12 of 18 industries, while quantum has uniquely targeted Aerospace alongside other critical sectors.

FEATURED PROFILES

The following profiles detail the four broadest-targeting ransomware entities observed during 2025, providing operational context, tradecraft patterns, and typical attack pathways for each.

PLAY

Category: Ransomware group

Primary Malware: Playcrypt

Active Since: ≥ 2022

Operating Model: Closed/semi-closed; double extortion

OVERVIEW:

Play is a ransomware group that conducts hands-on intrusions followed by data exfiltration and encryption. Activity observed across multiple regions and sectors suggests a mature operational model rather than opportunistic mass deployment.

OBSERVED INDUSTRY SCOPE (AUSTRALIA):

12 of 18 industries, spanning commercial, government, healthcare, manufacturing, energy, and transportation sectors.

COMMON TRADECRAFT THEMES:

- Initial access via exposed services or remote access mechanisms
- Credential abuse and lateral movement using standard administrative tooling
- Data staging and exfiltration prior to encryption
- Active defense evasion, including security tool interference and log removal

REPRESENTATIVE ATT&CK TECHNIQUES:

- Exploit Public-Facing Application
- External Remote Services
- Valid Account
- Archive Collected Data
- Exfiltration Over Alternative Protocol
- Impair Defenses
- Indicator Removal

AKIRA

Category: Ransomware group

Platform: Windows, ESXi

Active Since: ≥ 2023

Operating Model: Double extortion; affiliate-style deployment

OVERVIEW:

Akira operations commonly begin with compromised credentials against external access services, followed by lateral movement, data theft, and encryption. Tradecraft frequently blends legitimate administrative tools with commodity malware techniques.

OBSERVED INDUSTRY SCOPE (AUSTRALIA):

11 of 18 industries, including technology, financial services, manufacturing, healthcare, and retail.

COMMON TRADECRAFT THEMES:

- Initial access via compromised VPN or remote access credentials
- Extensive network and directory discovery
- Cloud-based data exfiltration
- Pre-encryption security control disruption

REPRESENTATIVE ATT&CK TECHNIQUES:

- External Remote Services
- Valid Accounts
- Remote Desktop Protocol
- Remote System Discovery
- Exfiltration to Cloud Storage
- Data Encrypted for Impact
- Impair Defenses

FEATURED PROFILES, CONTINUED

CLOP

Category: Ransomware group

Platform: Windows

Active Since: ≥ 2019

Operating Model: Targeted campaigns shaped by upstream access

OVERVIEW:

Clop is a long-standing ransomware family associated with enterprise-scale intrusions. Victim selection often appears driven by access availability rather than narrow sector focus, leading to episodic spikes in activity.

OBSERVED INDUSTRY SCOPE (AUSTRALIA):

11 of 18 industries, including manufacturing, healthcare, financial services, energy, and chemical sectors.

COMMON TRADECRAFT THEMES:

- Native command execution and process enumeration
- Network share discovery and broad file targeting
- Backup and recovery inhibition
- Security tooling discovery and disruption

REPRESENTATIVE ATT&CK TECHNIQUES:

- Windows Command Shell
- Data Encrypted for Impact
- Inhibit System Recovery
- Network Share Discovery
- Security Software Discovery
- Service Stop
- Impair Defenses

QILIN

Category: Ransomware-as-a-Service (RaaS)

Platform: Windows, ESXi

Active Since: ≥ 2022

Operating Model: Affiliate-driven deployment

OVERVIEW:

Qilin is a RaaS ecosystem supporting full-domain impact when affiliates achieve sufficient access. Reported activity reflects flexible deployment paths rather than a fixed intrusion methodology..

OBSERVED INDUSTRY SCOPE (AUSTRALIA):

11 of 18 industries, spanning commercial, government, healthcare, manufacturing, energy, and retail sectors.

COMMON TRADECRAFT THEMES:

- Initial access via exposed services or compromised credentials
- Domain-wide discovery and lateral movement
- Systematic recovery inhibition
- Log clearing and post-execution cleanup

REPRESENTATIVE ATT&CK TECHNIQUES:

- Exploit Public-Facing Application
- Data Encrypted for Impact
- Inhibit System Recovery
- Clear Windows Event Logs
- SMB/Admin Share Movement
- Scheduled Task Execution
- Impair Defenses

RANSOMWARE THREAT PROJECTIONS: AUSTRALIA 2026

Based on observed targeting patterns and attacker tradecraft evolution, the following predictions identify the most likely shifts in ransomware operations against Australian organizations during 2026.

1. FASTER "SMASH-AND-GRAB" OPERATIONS

Ransomware incidents will move from initial access to business impact faster, with less time spent lurking inside networks before encryption or extortion demands are made

Attackers understand defenders are getting faster at detection, so their advantage now lies in speed. The tradecraft that dominated 2025 (credential abuse, lateral movement via standard administrative tooling, and deliberate recovery inhibition) is being executed on compressed timelines. Threat landscape observations show dwell times collapsing across ransomware incidents, with some intrusions moving from breach to encryption in days rather than weeks.

For Australian defenders, the window for detection and containment continues to shrink. The shift isn't about attackers becoming more sophisticated; it's about them optimizing the operational tempo of campaigns that already work.

Why this matters: Response speed becomes as critical as detection capability when attackers compress their operational timelines.

2. ATTACKS BEGIN "UPSTREAM" AND LAND "DOWNSTREAM"

Supplier-driven incident spikes will increase, where a single upstream breach creates access to multiple downstream victims simultaneously

Technology is not merely a target but an access pathway with multiplicative downstream impact via managed service providers, cloud platforms, and supply chain dependencies. Some ransomware campaigns are shaped by upstream access availability and can produce episodic spikes rather than steady targeting. Threat landscape observations from 2025 showed multiple cases where a single MSP compromise delivered access to dozens of clients in a coordinated wave.

For Australia, this pattern is particularly relevant given the concentration of organizations in high-pressure sectors. Technology (92% of entities), Financial Services (90%), and Manufacturing (86%) all rely heavily on common platforms, shared service providers, and interconnected infrastructure. A breach at an upstream provider used by Australian banks, retailers, or manufacturers doesn't just affect one victim. It creates a clustered campaign affecting an entire segment of the economy.

Why this matters: Trusted partner relationships become potential intrusion vectors, with single points of compromise creating cascading impact across multiple organizations.

3. IDENTITY ATTACKS INCREASINGLY TARGET "SESSIONS AND TOKENS"

As phishing-resistant MFA adoption grows, more ransomware incidents will involve post-authentication attacks (stolen sessions, hijacked tokens, and privilege escalation) alongside traditional credential theft

Most ransomware incidents succeed because attackers authenticate using stolen access rather than exploiting novel vulnerabilities. Traditional password-based attacks remain effective and widespread, but as Australian organizations roll out phishing-resistant MFA and improve password hygiene, attackers are adding post-authentication techniques to their playbooks. These methods let them operate as if they're legitimate users even when passwords are protected.

Session hijacking, OAuth token theft, and credential abuse of service accounts or legacy authentication paths don't trigger the same alerts as brute-force login attempts. These techniques allow attackers to move laterally, escalate privileges, and access sensitive systems while appearing to security tools as authorized administrative activity. The result is a broader attack surface where defenders must monitor for anomalous authentication patterns rather than just failed login attempts.

Why this matters: Identity attacks are evolving beyond stolen passwords to include any authentication method that grants access, requiring detection strategies that look at behavior rather than just credentials.

RANSOMWARE THREAT PROJECTIONS: AUSTRALIA 2026, CONTINUED

4. BACKUP AND VIRTUALIZATION PLATFORMS BECOME "DAY-ONE" TARGETS

Ransomware operators will prioritize taking away recovery options early in an intrusion, targeting backup repositories, virtualization management planes, and snapshot systems before encryption

Recovery inhibition is a common ransomware theme, with backup platforms and virtualization management planes routinely abused during intrusions. Threat landscape observations show sophisticated ransomware operators have adopted a deliberate sequencing. First, they compromise identity. Next, they access backup systems and delete repositories or snapshots. Then they access hypervisors. Finally, they encrypt virtual machines. The goal is to remove the victim's ability to recover before triggering detection.

Virtualization environments are particularly high-value targets because a single hypervisor compromise can encrypt hundreds of VMs simultaneously. For Australian organizations (many of which operate heavily virtualized infrastructure and rely on backup-based recovery for resilience), this represents a critical exposure. Attackers know that if they can take out both backups and virtualization infrastructure, they've maximized both impact and payment pressure.

Why this matters: The systems designed to enable recovery are now primary targets, fundamentally changing the threat model for backup and virtualization infrastructure.

5. "DATA-THEFT PRESSURE" RISES AS ENCRYPTION PRESSURE WEAKENS

Extortion will increasingly center on the consequences of stolen data (regulatory exposure, customer notification obligations, and public disclosure threats) rather than relying primarily on encryption

Modern ransomware operations commonly combine encryption with data theft. As organizations improve their backup and containment capabilities, they reduce the leverage attackers get from encryption alone. This creates an economic pressure; as more victims demonstrate they can restore operations from backup without paying, attackers must rely more heavily on the secondary extortion vector. Threatening to leak stolen data unless demands are met becomes the primary pressure point.

Threat landscape observations show this shift already underway, with some ransomware groups now conducting data-only extortion without encryption. The Australian context amplifies this pressure. Mandatory breach notification under the Privacy Act, ransomware payment reporting obligations for critical infrastructure, and sector-specific regulatory expectations all create compliance and reputational exposure that attackers can weaponize. Attackers are diversifying pressure tactics beyond traditional data leak sites. This includes direct contact with customers and partners, threats of regulatory disclosure, and harassment campaigns targeting executives.

Why this matters: Technical recovery capability no longer eliminates extortion risk when stolen data creates independent regulatory, reputational, and legal consequences.

STRATEGIC RECOMMENDATIONS

Based on observed targeting patterns and attacker tradecraft, the following recommendations address the core control failures most commonly exploited in ransomware operations against Australian organizations.

1. RANSOMWARE-RESILIENT BACKUPS AND RECOVERY

Make encryption survivable and extortion less effective

Implement offline, immutable-capable backups for critical systems with strict separation between production and backup administration. Backup infrastructure should assume compromise of domain credentials and remain recoverable even while an attacker retains active access to the environment.

Backups must be regularly tested through full restore exercises rather than validated solely through job completion or success logs. Recovery objectives such as RTO and RPO should be formally defined, measured, and aligned to business impact rather than operational convenience. Prior to restoration, backups should be verified as clean and recovered into a controlled environment to reduce the risk of reinfection.

Because modern ransomware operations commonly combine encryption with data theft, backup and recovery planning should be paired with predefined decision-making around data exposure, legal and regulatory obligations, communications strategy, and continuity planning.

Why this matters: Backups remain the last-resort control for restoring availability when preventive measures fail.

2. IDENTITY HARDENING WITH PHISHING-RESISTANT MFA

Remove the attacker's easiest path to full environment control

Enforce phishing-resistant multi-factor authentication for users, remote access pathways, and cloud identities as a priority. Where phishing-resistant MFA cannot be enforced, access should be tightly restricted, closely monitored, and limited in duration.

Standing administrative privileges should be eliminated through least-privilege access models and just-in-time elevation for critical systems. Service accounts, legacy authentication mechanisms, and non-interactive access paths should be fully inventoried, tightly controlled, and regularly reviewed.

Identity telemetry should be treated as high-signal security data, with active monitoring for abnormal authentication events, token or session abuse, privilege escalation, and lateral movement.

Why this matters: Most ransomware incidents succeed because attackers authenticate using stolen access rather than exploiting novel vulnerabilities.

3. EXPOSURE REDUCTION FOR INTERNET-FACING SYSTEMS

Close the doors ransomware crews routinely walk through

Prioritize patching and hardening of internet-facing and identity-adjacent systems including VPN infrastructure, email platforms, identity services, remote management interfaces, backup platforms, and virtualization management planes. Remediation efforts should focus on known exploited vulnerabilities rather than theoretical or low-likelihood risks.

Attack surface should be reduced by removing unused services, restricting inbound access, and isolating management interfaces from user networks. External exposure should be continuously inventoried and reviewed to identify forgotten, misconfigured, or newly exposed assets.

Baseline controls should align with established guidance such as the ACSC Essential Eight, which provides a widely adopted framework that materially reduces ransomware likelihood and impact for Australian organizations.

Why this matters: Opportunistic ransomware activity thrives on exposed, neglected, and poorly maintained systems.

STRATEGIC RECOMMENDATIONS, CONTINUED

4. SEGMENTATION AND RAPID CONTAINMENT

Limit blast radius when compromise occurs

Implement network and access segmentation around crown-jewel assets including identity infrastructure, backup systems, virtualization platforms, finance systems, and operational technology. Segmentation should assume credential compromise and restrict lateral movement by default, including along administrative and management pathways.

Organizations should maintain the ability to rapidly isolate endpoints, disable compromised accounts, and block network paths during an incident. These actions must be rehearsed and executable under operational pressure rather than improvised during a live attack.

Containment capability should be treated as a first-class security control and integrated into standard operations rather than deferred to incident response procedures alone.

Why this matters: Ransomware response is time-critical and effective containment directly limits enterprise-wide impact.

5. SESSION AND TOKEN SECURITY CONTROLS

Detect and prevent post-authentication attacks when credentials alone aren't enough

Implement session and token management controls that assume authentication credentials may be compromised or bypassed. Session lifetimes should be limited with automatic expiration for inactive sessions and forced re-authentication for high-risk actions. Where platform capabilities support it, token-based authentication should include device-bound tokens or cryptographic binding mechanisms that tie tokens to specific devices or network contexts, making stolen tokens harder to reuse from attacker infrastructure.

Monitor authentication telemetry for behavioral anomalies that indicate session hijacking or token abuse, including impossible travel scenarios, device fingerprint changes mid-session, unusual access patterns from authenticated accounts, and privilege escalation outside normal workflows. Service accounts and non-interactive authentication paths require particular attention, as these often operate with elevated privileges and may lack the behavioral patterns that make user account compromise detectable.

Legacy authentication protocols and applications that cannot support modern token security should be inventoried, risk-assessed, and either upgraded or tightly restricted. Where legacy systems must remain operational, compensating controls should include enhanced monitoring, network segmentation, and time-limited access windows.

Why this matters: As phishing-resistant MFA becomes standard, attackers are shifting to post-authentication techniques that bypass credential-based defenses entirely, requiring detection strategies focused on behavior rather than authentication success or failure.

This report is based on threat intelligence from Anomali Unified Security Data Lake, current as of January 2026. Threat landscapes evolve rapidly; continuous monitoring is recommended.