AC3

CYBER THREAT INTELLIGENCE REPORT

JANUARY 2026

STAY INFORMED. STAY RESILIENT.

CONTENTS

Executive Summary	3
Industry Sector: Insurance	4
Industry Sector: Government	10
Industry Sector: Private	16
Vulnerability Landscape	23
Document References	28

EXECUTIVE SUMMARY

The cyber threat landscape across Australia and the wider Asia–Pacific continued to intensify through 2025, with adversaries converging on the same common weaknesses across sectors. Financially motivated groups increasingly prioritised data theft as the primary lever for extortion, using encryption, disruption and harassment as optional pressure tools rather than the core outcome. In parallel, exploit-first intrusions against internet-facing services accelerated and often outpaced patch cycles, while identity-led compromise became more repeatable through credential abuse, vishing and service-desk workflow manipulation. State-aligned actors maintained steady long-dwell access and reconnaissance against strategic targets, reinforcing that espionage and criminal tradecraft are now overlapping in both targets and techniques.

This Quarterly Threat Intelligence Report examines these dynamics across three sector lenses: insurance, government and the broader private sector. The insurance ecosystem remains highly exposed due to dense connectivity between carriers, brokers, portals, SaaS platforms and outsourced service partners, where a compromise in one trust pathway can quickly enable access to policyholder data and sensitive customer channels. Government environments continue to face a blended mix of espionage, disruption and theft-first extortion amplified by shared services, uneven security maturity and high-trust operational workflows that can be abused without sophisticated malware. Across the private sector more broadly, the dominant risk themes were exploit-driven entry via edge and enterprise platforms, service-channel compromise for privileged access and third-party concentration risk that expands blast radius.

For business leaders, cyber risk is now inseparable from operational continuity, regulatory exposure and reputation. Resilience depends on reducing external attack surface, hardening identity and service-desk processes and tightening governance over third-party access and data handling. This report provides an executive view of the most relevant threats, sector-specific context and the recurring attack paths driving incidents, alongside clear defensive priorities. This report has been produced by the AC3 Security Operations Centre to support informed leadership decisions and uplift defensive readiness across the sectors covered.

INDUSTRY SECTOR:
INSURANCE

INSURANCE - THREAT INTEL REPORT

KEY JUDGEMENTS

The Australian insurance sector remained a priority target as insurers and brokers centralise highly valuable and sensitive customer data across interconnected and partner-facing systems, making the sector a consistent focus for financially motivated threat actors. Financially motivated ransomware and data extortion activity remained elevated. Insurers were targeted both directly and via brokers, superannuation linked environments and data rich service partners. Data theft remained the primary source of leverage, driving extortion pressure even when encryption was not used and extending business impact beyond system recovery. Identity driven intrusion remained the dominant pathway, including compromised credentials, phishing, MFA fatigue and vishing targeting help desks and contact centres.

THREAT LANDSCAPE UPDATE

Sector exposure is driven by long-lived data holdings and dense connectivity, with environments spanning core policy and claims systems, customer portals, mobile apps, contact centre platforms, SaaS services such as CRM and document management and APIs linking partners and digital channels. During the quarter, financially motivated ransomware and extortion campaigns targeted insurers' extended ecosystems and treated insurers, brokers and tightly integrated partners as one target environment.

TOP SECTOR THREATS

Ransomware with double extortion and extortion-only operations remained the most disruptive threats. In both models, data theft occurs early and is used to coerce payment through disclosure pressure, with encryption used selectively. Quadruple extortion increased pressure further by adding DDoS and targeted harassment to raise business impact and public visibility. Across these activity sets, credential-based intrusion and social engineering continued to remain the most common enabler for initial access.

INSURANCE

COMMON ATTACK PATHS AND EXPOSURE POINTS

Identity compromise remained the most common entry point, driven by stolen credentials, phishing, MFA fatigue and account misuse reaching cloud apps, customer portals and admin tooling. Large-scale credential stuffing campaigns aimed at Australian super funds, prove how recycled credentials can be used at scale, forcing widespread password resets and a heightened degree of monitoring.

Edge-facing services remained high-risk, especially internet-exposed VPNs, remote access gateways and partner portals were made more attractive by the initial-access-broker and cybercrime-as-a-service ecosystems.

SaaS and third-party connections increased exposure, as high-trust partner workflows (broker/claims) are often found directly integrated with core systems and policyholder data. Recurring gaps in API security, access controls, authentication discipline, data retention and third-party oversight magnify impact.

Business Email Compromise remained a reliable vector through trusted-process abuse through invoice redirection, vendor payment fraud, mailbox rule manipulation and change-of-details scams tied to claims/partners.

OPERATIONAL AND BUSINESS IMPACT

Activity observed throughout the quarter continued to demonstrate deliberately timed attacks occurring on weekends and public holidays, added additional complexity when staffing and decision makers are less available. Recovery across financial and insurance services was often measured in weeks, delaying restoration of core systems and customer facing operations.

For insurers, this translated into delayed claims processing, disrupted policy servicing, strained broker relationships, rising cyber cover costs and measurable erosion of trust. DDoS enabled extortion increased the impact of outages affecting claims workflows and customer and broker self-service channels, where small periods of downtime often escalated into reputational damage and regulatory attention.

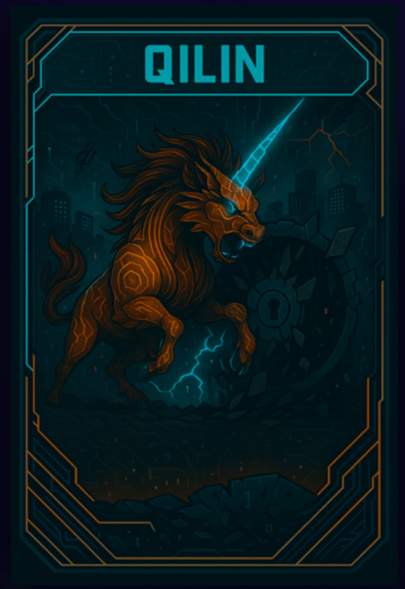
KEY EVIDENCE HIGHLIGHTS

ASD reporting identified financial and insurance services as the most frequently reported non-government sector for cyber incidents, accounting for the largest share of critical infrastructure cases and a significant proportion of DDoS activity. Quarterly reporting highlighted exploitation of Fortinet edge appliances associated with theft-first ransomware, exploitation of Oracle E-Business Suite at Allianz, leak site pressure against a regional insurance brokerage with more than sixty gigabytes of claimed theft and a continued shift toward extortion-only activity that prioritises confidentiality loss over encryption-led disruption.

NOTEABLE ACTOR TRADECRAFT & TECHNIQUES

INSURANCE

Qilin



Threat Type: Russian-speaking RaaS crew, financially motivated and prolific, running double extortion with data theft and encryption.

Tech Profile: Qilin utilises Rust and C-based ransomware across Windows, Linux and ESXi. Intrusions leverage exposed RDP or vulnerabilities in Fortinet, Citrix and VMware. Tactics include credential theft, data exfiltration and rapid encryption to maximize downtime, supported by leak sites and negotiation portals to enforce ransom demands.

DragonForce

Threat Type: RaaS cartel with affiliates, using leak site pressure and choreographed negotiations to coerce a quick payment.

Tech Profile: DragonForce favors intrusion chains at edge infrastructure or management tooling, then pivots across Windows and ESXi. Operators use credential theft, discovery and lateral movement with Mimikatz, PsExec and Cobalt Strike and abuse RMM like SimpleHelp. They stage exfiltration, disable backups, then encrypt for disruption, whilst leaking posts and continuing negotiations in order to sustain pressure.

Scattered Spider

Threat Type: Financially motivated collective tracked as UNC3944 and Octo Tempest, specialising in support desk MFA bypass.

Tech Profile: Scattered Spider uses vishing, SIM swaps and MFA fatigue to trick support staff into resetting credentials, enrolling devices or granting SSO access to Okta, Entra ID and Salesforce. After access, they pivot through mail and data stores to steal data and apply extortion pressure. Ransomware is deployed through partners to maximise downtime.

ClOp

Threat Type: Russian-speaking financially motivated extortion brand linked to TA505 or FIN11 infrastructure, focused on theft.

Tech Profile: ClOp leverages 0 day exploits in MOVEit and Oracle E-Suite, using web shells for automated exfiltration. Prioritizing theft over encryption, they rely on leak site extortion. Campaigns scale rapidly via supply chain attacks, where a single vendor compromise exposes numerous downstream partners.

THREAT ACTOR DEEP DIVE

INSURANCE

SUPPORT DESK TAKEOVER, MASS EXPORT, PUBLIC SHAMING: THE SLH THREAT PROFILE

Overview

Scattered LAPSUS$ Hunters (SLH) is a merged extortion collective comprising Scattered Spider, LAPSUS$ and ShinyHunters, operating within "The Com" ecosystem. Despite active moderation, the group maintains a persistent, high-profile presence on Telegram to coordinate large-scale attacks and share infrastructure.

Threat Type

SLH is a high-severity Extortion-as-a-Service actor that combines Scattered Spider's social engineering, LAPSUS$'s pressure tactics and ShinyHunters' cloud automation. Affiliates leverage this merged brand and infrastructure to target and extort organizations reliant on major SaaS platforms like Salesforce and Workday.

Threat Profile

Attacks typically begin with aggressive social engineering (vishing, MFA fatigue) against help desks to reset credentials or authorize malicious OAuth applications. Operators utilize typo squatted domains and fake login portals to gain access, followed by the bulk export of core data tables and immediate, noisy public extortion.

Defensive Implications

Defenders must shift focus from the perimeter to identity verification and SaaS configuration. Mitigation requires strict identity-proofing procedures for help desks, hardening of OAuth and connected apps and ensuring CRM and ticketing platforms send granular telemetry to the SOC for early detection.

RECOMMENDATIONS

AC3 provides comprehensive services to strengthen critical security areas through red and blue team operations, advanced threat hunting and mature vulnerability management programmes.

USER AWARENESS AND TRAINING PROGRAMMES

The widespread use of spear phishing techniques across threat actors emphasises the critical importance of user education as a primary defence. AC3's security awareness training specifically addresses social engineering methodologies used by groups.

Industry-specific threat scenarios for the financial sector targeting, Interactive modules on cryptocurrency-focused social engineering, Executive briefings on nation-state threat actor methodologies and Continuous awareness programmes reflecting evolving threats.

CORE SECURITY SERVICES

Red Teaming

Realistic defensive posture assessments through controlled adversarial emulation, Threat actor TTP replication, White box and black box testing

Blue Teaming

IRAP-certified SOC addressing systematic security circumvention techniques, Expert guidance on defensive system configuration

Threat Hunting

Proactive and retrospective hunting services, Ongoing exercises to stay ahead of threat actors

Vulnerability Management

Structured programmes aligned with Essential Eight Maturity Levels 1-3, Service level agreements ensuring timely remediation, Specialised assessment of APAC-specific financial software platforms

INDUSTRY SECTOR:
GOVERNMENT

GOVERNMENT - THREAT INTEL REPORT

KEY JUDGEMENTS

Australia's government sector is facing a blended threat environment where state-aligned espionage, financially motivated extortion and disruptive activities appear to occur in parallel. Rapid digital transformation especially increased cloud adoption and reliance on outsourced service providers have expanded the attack surface and created extensive trust relationships that adversaries can exploit for initial compromise and lateral movement. State-aligned activity, particularly PRC-linked operations, remains a persistent risk with concerns focused on long-dwell reconnaissance and pre-positioning in telecommunications and other critical infrastructure. Financially motivated groups continue to pressure victims through ransomware and extortion campaigns that often prioritize data theft and exfiltration, using the threat of public disclosure to force expedited payment. Across incidents, identity and trust failures are a recurring root cause, with attackers using stolen credentials, impersonation and abuse of trusted access to evade controls and maintain persistence.

THREAT LANDSCAPE UPDATE

The government sector spans federal, state and territory and local entities that deliver essential public services and hold highly valuable government and personally identifiable information.

Exposure is amplified by a dense operating ecosystem of departments, statutory bodies, regulators, commissions and councils, interconnected through shared services, common suppliers and cross agency information sharing.

Security maturity remained uneven across the sector. Larger agencies typically run stronger central security programs, while smaller councils often operate with lean IT teams and greater reliance on managed service providers and shared platforms. This imbalance creates simplified practical entry points, where compromise of a smaller entity can still provide access to trusted communication channels, sensitive data, or connected government environments.

Digital transformation increased connectivity across portals, mobile apps, contact centres, SaaS services and third-party platforms linked through APIs. This raised the likelihood that a compromise in one area could cascade via shared identity services, supplier access and cross-agency workflows.

TOP SECTOR THREATS

State-sponsored espionage and pre-positioning remained the most strategically significant threat. China-linked actors continued to compromise networks at scale to collect intelligence and establish access that could be leveraged later for disruption. This risk is highest in environments connected to telecommunications and other critical infrastructure services.

Ransomware and extortion activity continued to drive impact, particularly across smaller government entities where service disruption and sensitive data increased attacker leverage. Incidents typically followed a consistent pattern: unauthorised access, rapid containment and investigation, then staged notifications and service restoration. Disruption-driven activity remains with credible pressure against public-facing services through distributed denial of service, website defacement and harassment-style campaigns. These operations prioritised visibility and narrative impact over stealth and were often linked to international events.

Fraud and impersonation became a major threat alongside traditional "system intrusion" activity. Rather than breaking in with malware, attackers often impersonated staff, executives, suppliers, or IT support to trick people into doing the work for them, such as approving urgent payments, changing bank details, resetting passwords, or adding MFA devices. This resulted in direct financial loss and operational disruption when core systems weren't technically compromised.

COMMON ATTACK PATHS AND EXPOSURE POINTS

Service-channel compromise remained a reliable leverage point for attackers. Attackers targeted service desks, shared inboxes and operational workflows, where they relied on urgency and process manipulation to trigger password resets, MFA re-enrolment, approval overrides and payment detail changes without needing complex tooling.

Public digital services expanded the available foothold surface. Citizen-facing portals, online forms, APIs and exposed admin interfaces increased exposure when patching, secure configuration, or authentication controls lagged. Once a foothold was established, attackers could pivot into internal environments through trusted connections, weak segregation, or misconfigurations.

Shared services and federation increased the potential blast radius. Whole-of-government platforms, identity federation and cross-agency integrations can concentrate risk in a small number of control points. When boundaries, delegation and access governance are weak, attackers can move laterally faster and inherit downstream access across connected agencies.

Third-party operated systems created inherited access pathways. Reliance on managed service providers and vendor-managed platforms allowed intrusion through upstream tooling, remote management channels, or supplier-held credentials. This reduced the need for direct entry and increased the risk that a compromise in one partner environment could cascade into government networks. Email and collaboration tooling remained a control plane, with impersonation, mailbox rule abuse, document-sharing lures and invoice redirection supported trusted change requests and operational manipulation being a main contributor.

Data theft and disruption drove the highest impact. Attackers stole sensitive datasets to enable extortion and increase public pressure. Disruption also remained common, with availability attacks and ransomware-style interruption degrading services and consuming response capacity.

OPERATIONAL AND BUSINESS IMPACT

Activity observed throughout the quarter continued to show incidents timed for weekends and public holidays, increasing response complexity when staffing and decision makers are less available. Recovery across financial and insurance services was often measured in weeks, delaying restoration of core systems and customer-facing operations.

For insurers, this translated into delayed claims processing, disrupted policy servicing, strained broker relationships, rising cyber cover costs and measurable erosion of trust. DDoS-enabled extortion increased the impact of outages affecting claims workflows and customer and broker self-service channels, where even short downtime can escalate into reputational damage and regulatory attention.

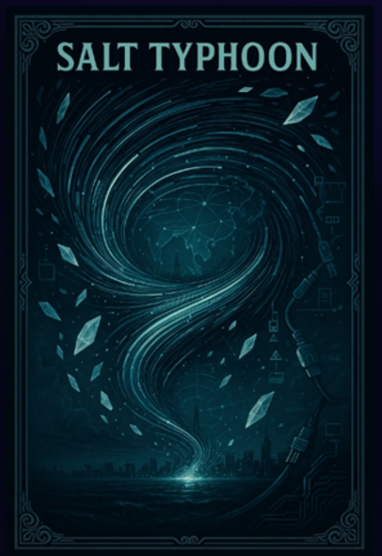
KEY EVIDENCE HIGHLIGHTS

ASD reporting identified financial and insurance services as the most frequently reported non-government sector for cyber incidents, accounting for the largest share of critical infrastructure cases and a significant proportion of DDoS activity. Quarter reporting highlighted exploitation of Fortinet edge appliances associated with theft-first ransomware, exploitation of Oracle E-Business Suite at Allianz, leak-site pressure against a regional insurance brokerage with more than sixty gigabytes of claimed theft and a continued shift toward extortion-only activity that prioritises confidentiality loss over encryption-led disruption.

NOTEABLE ACTOR TRADECRAFT & TECHNIQUES

GOVERNMENT

Salt Typhoon



Threat Type: PRC linked state sponsored espionage focused on access and long term collection through telecommunications pathways.

Tech Profile: Tradecraft targets Cisco IOS and IOS XE by exploiting exposed services, then persisting through configuration changes. Operators dump configurations to harvest credentials, add SSH keys, create local users and modify access control lists. They establish GRE or IPsec tunnels and exfiltrate configuration data via FTP or TFTP, via Guest Shell.

Volt Typhoon

Threat Type: Stealth operator using “living off the land” techniques to blend into legitimate network activity and pre-position in critical infrastructure for future disruption.

Tech Profile: Stealth-driven activity focused on pre-positioning and durable access. Tradecraft prioritises living off the land techniques, valid credentials and low-noise lateral movement through trusted infrastructure to blend into normal operational workflows to avoid detection.

Safe Pay

Threat Type: Financially motivated double extortion operation stealing data before encryption and threatening leak site publication afterwards.

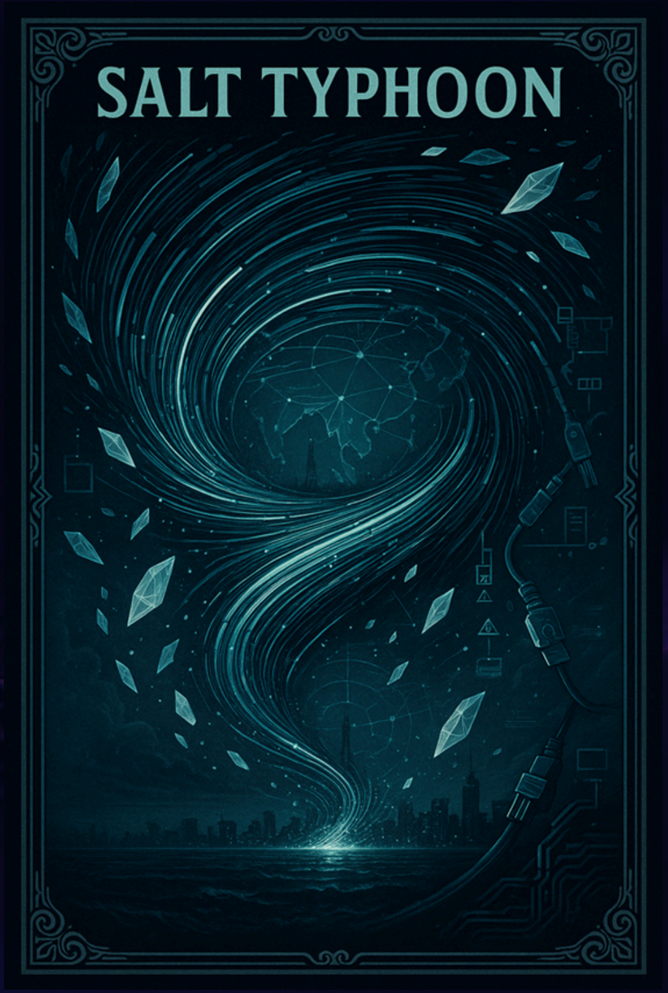
Tech Profile: Initial access is reported via VPN access using credentials, likely sourced from stealware infections or dark web markets. Reporting also notes suspected exploitation of VPN weaknesses without confirmed CVEs. Some incidents show rapid access to encryption and reportedly avoids affiliate RaaS models entirely.

Direwolf Ransomware

Threat Type: Financially motivated ransomware and data extortion operation applying coercive pressure through disruption and exposure risk.

Tech Profile: Advisories describe a multi stage attack chain with anti forensics to evade detection, confirm encryption and stop recovery. In the WA Legal Practice Board incident, systems were taken offline for containment and later unauthorised data access was confirmed, with notifications referencing health, identity and financial information and recovery delays which impacted many downstream insurers and partners.

THREAT ACTOR DEEP DIVE



Overview

Salt Typhoon is assessed as the most severe threat to Australian government because its telecom and network-edge access can support covert intelligence collection, large-scale credential exposure and persistent pre-positioning against critical dependencies. Australian security leaders have publicly linked Salt Typhoon to probing of telecommunications networks, indicating government communications and carrier trust relationships are being actively tested by a capable state-linked actor.

Initial Access Methodologies

T1190: Exploit internet-facing edge/network devices to gain an initial foothold and broaden access.

T1078: Use valid credentials for remote access/admin actions, including credentials taken from device configs or nearby management systems.

T1199: Pivot via trusted carrier/MSP relationships upstream of government services to move across connected agencies.

Persistence & Evasion Techniques

T1098.004 Add or Modify SSH Authorised Keys: Establishing durable access by adding authorised keys on network infrastructure and jump points.

T1136 Create Account: Creating local users on network devices or management planes to maintain access even after initial credentials are rotated.

T1562.004 Disable or Modify System Firewall: Modifying access controls and filtering rules to reduce visibility and preserve attacker access paths.

ADDITIONAL SERVICES

GOVERNMENT

Security must be embedded into infrastructure foundations and not treated as an afterthought. Threat actors are targeting multiple infrastructure layers to penetrate networks and establish persistent access. AC3 provides comprehensive services to strengthen critical security areas through red and blue team operations, advanced threat hunting and mature vulnerability management programmes.

AC3 OFFER THE FOLLOWING SERVICES TO CUSTOMERS ACROSS THE CYBER LANDSCAPE:

Cyber Consulting - Strategic cybersecurity advisory

Virtual CISO (vCISO) - Executive cybersecurity leadership

Solution Architecture - Security-first infrastructure planning with financial compliance

Digital Forensics and Incident Response - Specialised financial breach investigation

Penetration Testing - Comprehensive infrastructure security assessments

Supply Chain Security Assessment - Third-party vendor risk management

Business Continuity Planning - Critical operations resilience strategies

IRP Exercises - Crisis management training for senior leadership

Security Regulations Compliance - Meeting government security

INDUSTRY SECTOR:

PRIVATE

PRIVATE SECTOR THREAT INTEL - REPORT

PRIVATE

KEY JUDGEMENTS

Across Q2–Q4 2025, ransomware remained the most disruptive threat to the APAC private sector, driven by mature double-extortion models and Ransomware-as-a-Service ecosystems led by groups such as LockBit, Medusa, Qilin and Chaos. Exploit-driven intrusions intensified as attackers increasingly targeted exposed infrastructure and enterprise applications, often outpacing patch cycles and enabling rapid credential theft and data staging. Service-desk compromise, particularly through vishing and social manipulation techniques popularized by groups like Scattered Spider, became a major intrusion vector, allowing attackers to gain privileged access without heavy malware use. Third-party and supply-chain breaches continued to amplify impact, exposing weaknesses in vendor segregation and trust relationships. Heightened regulatory scrutiny and mandatory reporting raised accountability and legal risk, underscoring that exploit-led access, service-channel abuse and supply-chain exposure now define the core of enterprise cyber risk across APAC.

THREAT LANDSCAPE UPDATE

The private sector remains a highly contested environment where criminal extortion, credential-driven fraud and state-sponsored espionage occur in parallel. Criminal activity continues to be dominated by ransomware and extortion, with data theft now the primary lever and encryption increasingly used to amplify disruption rather than serve as the core objective. Initial access patterns have shifted toward faster, more reliable pathways, with threat actors prioritising exploitation of exposed services such as VPNs, firewalls and file-transfer platforms alongside identity compromise, reducing dependence on traditional email-led intrusion. Social engineering has also increased in impact as service desk targeting and vishing, became repeatable routes to privileged access, supported by readily available tooling that improves the credibility, consistency and scale of lures. Overall, the threat landscape is defined by compressed time-to-compromise, theft-first outcomes and a growing convergence where both financially motivated groups and state-aligned actors exploit the same exposure and governance gaps to achieve either disruption or long-dwell access.

TOP SECTOR THREATS

Private sector threat activity centred around theft-led extortion, exploit-first intrusions, service desk compromise and credential abuse that enabled fraud and steady state-aligned successful espionage against critical-adjacent industries, with Ransomware remaining the leading driver of disruption. Operators increasingly treated data theft as the primary lever and used encryption to amplify pressure rather than define the outcome. Initial access shifted toward more direct pathways. Rapid exploitation of exposed VPNs, firewalls, file-transfer platforms and public-facing applications compressed patch windows. In parallel, vishing and helpdesk workflow abuse became a dependable route to bypass MFA and gain privileged access. Stolen credentials remained a consistent driver of cybercriminal activity and were frequently used for account takeover, then leveraged to pivot into internal systems, escalate privileges, move laterally and stage data for theft or extortion.

COMMON ATTACK PATHS AND EXPOSURE POINTS

A number of recurring exposure points continued to account for a large share of intrusions. Attackers repeatedly access by probing VPNs, firewalls and remote access gateways, then moving quickly once an opportunity appears. In parallel helpdesk-driven password resets and MFA changes often undermined by weak verification and reliance on SMS or voice recovery. Where customer-facing services lacked strong authentication, credential stuffing and account takeover continued to translate directly into targeted attacks. Stolen and reused credentials also increased downstream risk, as prior breach data and info-stealer logs enabled quiet valid-account access without obvious malware activity. Finally, shared providers amplified impact, with call centres, SaaS platforms and other third parties creating a wider blast radius when compromised.

OPERATIONAL AND BUSINESS IMPACT

Operational and business impact most often identified as a mix of downtime, data exposure and financial loss that kept compounding after the initial intrusion. Supplier-side incidents and ransomware events regularly disrupted services and day-to-day operations and restoration was rarely quick, once core systems and dependencies were affected. Extortion pressure added a long tail, with theft of sensitive data driving notifications, remediation work and ongoing identity-misuse risk even when encryption was not the main feature of the attack. Credential-driven intrusions and business email compromise also continued to generate immediate financial loss, most often through account takeover and fraudulent payment diversion.

KEY EVIDENCE HIGHLIGHTS

Evidence from the period shows a familiar pattern rather than new tradecraft. Ransomware and extortion remained the main disruption driver, with data theft increasingly used to create leverage and encryption used to raise urgency and recovery cost. Exploit-led compromise of internet-facing services stayed a repeat entry point as attackers moved quickly from disclosure to scanning, outpacing patch cycles.
Concentration risk in shared providers also remained high, with one incident often creating spillover across multiple customers through trusted access and identity pathways.
Credential abuse continued to underpin account takeover, fraud and payment-process manipulation, while regulatory pressure increased the cost of weak governance through stricter reporting, investigation and remediation expectations.

NOTEABLE ACTOR TRADECRAFT & TECHNIQUES

PRIVATE

Akira

Threat Type: Financially motivated ransomware and data-extortion group targeting private sector organisations, prioritising fast monetisation and disruption.

Tech Profile: Intrusions commonly begin via exposed VPN services or stolen credentials, followed by rapid domain discovery and privilege escalation. Operators deploy remote tooling and Cobalt Strike-style beacons, dump credentials and stage data with rclone before encryption. They disable security controls, delete backups and leverage scheduled tasks and PsExec to spread payloads

Lazarus Group

Threat Type: DPRK linked sponsored intrusion and theft actor targeting finance and crypto firms, plus tech providers.

Tech Profile: Operators gain access through spearphishing, trojanised software and credential harvesting, then deploy malware for persistence and remote execution. They pivot using stolen admin tokens, collect data and target payment flows. A parallel tradecraft is the fraudulent remote IT worker scheme, maintaining low-noise access via company-issued laptops and routine admin tools.

Medusa Ransomware

Threat Type: Ransomware as a service group using theft and leak pressure to extort private sector victims.

Tech Profile: Affiliates enter via phishing, stolen credentials, or exploitation of exposed VPN services. They escalate privileges, run discovery and deploy remote management tools for persistence and lateral movement. Data is staged and exfiltrated first, then systems are encrypted to drive downtime. Negotiations are reinforced by leak site threats and selective releases.

Earth Kasha

Threat Type: PRC-aligned state-sponsored cyber espionage, assessed as part of the broader APT10 umbrella, focused on stealthy access and long-dwell collection against APAC targets.

Tech Profile: Activity has used spear-phishing with cloud-hosted links to deliver a refreshed ANEL backdoor and deploy NOOPDOOR as a second stage. Operators favour low-noise discovery and credential access, then keep persistence through normal administrative behaviour. Command-and-control is engineered to blend into common enterprise traffic and has been observed using DNS over HTTPS to hide lookups, supporting staged collection and data exfiltration.

MALWARE TREND

PRIVATE

Credential Stealers - Theft-First Payloads

Trend Level: Rising

Mechanism: Stealer families harvest browser credentials, cookies, autofill data and other authentication artefacts to enable rapid account takeover and follow-on access.

Common Delivery: Phishing attachments and links, trojanised installers, cracked software and loader-led payload chains.

Common Tooling/Strains: Lumma, Stealc, Vidar, Blank Grabber.

Observed: Credential theft remained a primary attacker objective despite a relative decline in stealer activity.

Remote Access Trojans and Persistent Access

RATs and Persistent Access Tooling

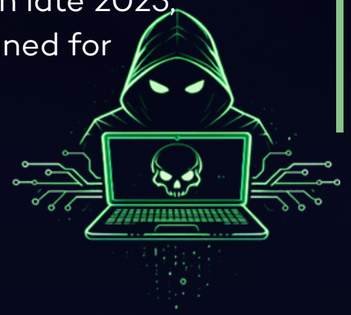
Trend Level: High

Mechanism: RATs provide interactive control and persistence, enabling discovery, credential access and long-lived footholds that support follow-on theft and extortion.

Common Delivery: Phishing-lure payloads, malicious downloads, loader hand-offs and staged execution after initial access.

Common Tooling/Strains: XWorm, AsyncRAT, Quasar RAT, Remcos.

Observed: RAT activity increased strongly through late 2025, alongside broader momentum in tooling designed for persistence and modular access.



Loaders and Dropper Chains

Loaders and Initial-Stage Malware

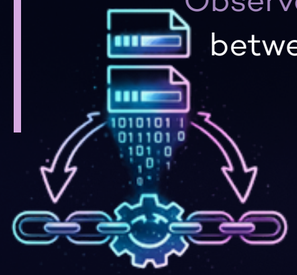
Trend Level: High

Mechanism: Loaders establish execution, perform environment checks and deliver second-stage payloads such as stealers or RATs while attempting to reduce defender visibility.

Common Delivery: Phishing and malvertising traffic, fake updates, drive-by downloads and bundled “installer” workflows.

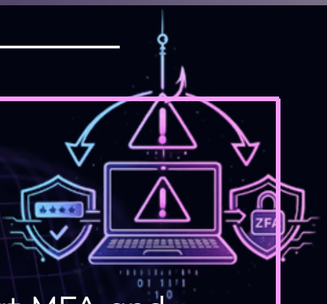
Common Tooling/Strains: Smoke Loader, PureCrypter, HijackLoader.

Observed: Loader activity stayed prominent as a reliable bridge between initial delivery and high-value payload deployment.



MALWARE TREND

PRIVATE



AiTM and 2FA Bypass Phishing - Adversary-in-the-Middle Phishing and 2FA Bypass

Trend Level: High

Mechanism: Reverse-proxy phishing kits capture sessions and tokens in real time, often pairing with workflow manipulation to defeat MFA and maintain access without deploying noisy malware.

Common Delivery: Branded credential lures, SMS/email delivery and service-desk social engineering to push victims into “approved” sign-in flows.

Common Tooling/Strains: Tycoon, EvilProxy, Sneaky2FA, Mamba2FA, Salty2FA.

Observed: 2FA-bypass phishing remained a major access enabler, with Tycoon and EvilProxy leading activity and newer kits accelerating.

Threat Shift: Stealth and Persistence

Stealers continue to underpin a large share of real-world compromise, but late-2025 activity shows a clear shift toward durable access. More intrusions now favour RATs, backdoors and loader chains that keep options open after the first foothold and support follow-on actions over time. In parallel, AiTM phishing is reducing the need for malware-heavy tradecraft by capturing sessions and tokens directly. The result is faster time-to-impact, increased reliance on valid accounts, high-signal indicators that defenders can easily spot.

RECOMMENDATIONS & ADDITIONAL SERVICES

PRIVATE

Security needs to be integrated into the core of infrastructure design and operations rather than applied reactively. Adversaries are exploiting weaknesses across multiple infrastructure layers to gain initial access and maintain persistence. AC3 helps organisations reduce this risk through integrated security services that include proactive red and blue team operations, advanced threat hunting and mature vulnerability management programs designed to strengthen resilience across critical systems.

AC3 OFFER THE FOLLOWING SERVICES TO CUSTOMERS ACROSS THE CYBER LANDSCAPE

Cyber Consulting - Strategic cybersecurity advisory
Virtual CISO (vCISO) - Executive cybersecurity leadership
Solution Architecture - Security-first infrastructure planning with financial compliance
Digital Forensics and Incident Response - Specialised financial breach investigation
Penetration Testing - Comprehensive infrastructure security assessments
Supply Chain Security Assessment - Third-party vendor risk management
Business Continuity Planning - Critical operations resilience strategies
IRP Exercises - Crisis management training for senior leadership
Security Regulations Compliance - Meeting government security

USER AWARENESS AND TRAINING PROGRAMMES

The widespread use of spear phishing techniques across threat actors emphasises the critical importance of user education as a primary defence. AC3's security awareness training specifically addresses social engineering methodologies used by groups.

Industry-specific threat scenarios for the financial sector targeting, Interactive modules on cryptocurrency-focused social engineering, Executive briefings on nation-state threat actor methodologies and Continuous awareness programmes reflecting evolving threats.

CORE SECURITY SERVICES

Red Teaming
Realistic defensive posture assessments through controlled adversarial emulation, Threat actor TTP replication, White box and black box testing

Blue Teaming
IRAP-certified SOC addressing systematic security circumvention techniques, Expert guidance on defensive system configuration

Threat Hunting
Proactive and retrospective hunting services, Ongoing exercises to stay ahead of threat actors

Vulnerability Management
Structured programmes aligned with Essential Eight Maturity Levels 1-3, Service level agreements ensuring timely remediation, Specialised assessment of APAC-specific financial software platforms

VULNERABILITY LANDSCAPE

TOP 5 VULNERABILITIES

SharePoint Tool Shell Zero-Day
CVE-2025-53770
9.8

Mechanism: Multi-stage attack bypassing authentication and exploiting unsafe deserialization
Impact: Full system control, data theft and lateral movement. Confirmed active exploitation against government/finance sectors.
Published: July 19, 2025

React Server Components Code Injection
CVE-2025-10035
10.0

Mechanism: Unsafe payload deserialization leading to prototype pollution and RCE.
Impact: Pre-authentication RCE affecting major web frameworks like Next.js. Requires only a single HTTP request.
Published: Sept 18, 2025

Citrix-Bleed 2
CVE-2025-5777
9.3

Mechanism: Out-of-bounds memory read (buffer over-read) in the authentication handler of NetScaler ADC and Gateway.
Impact: Session hijacking and MFA bypass. The leaked memory contains valid session tokens, allowing attackers to bypass multi-factor authentication

Docker Desktop Inadequate Access Control
CVE-2025-9074
9.8

Mechanism: Unauthenticated Docker Engine API exposure to containers via a hardcoded subnet.
Impact: Container escape, host system compromise (Windows) and control of Docker infrastructure.
Published: August 20, 2025

TOP 5 VULNERABILITIES

Forti Web Remote Code Execution Chain
CVE-2025-64446, 58034
9.8

Mechanism: Authentication bypass via path traversal to legacy CGI interfaces, followed by RCE.

Impact: Full control of WAF devices, enabling network pivot, traffic interception and defence disablement. Actively exploited.

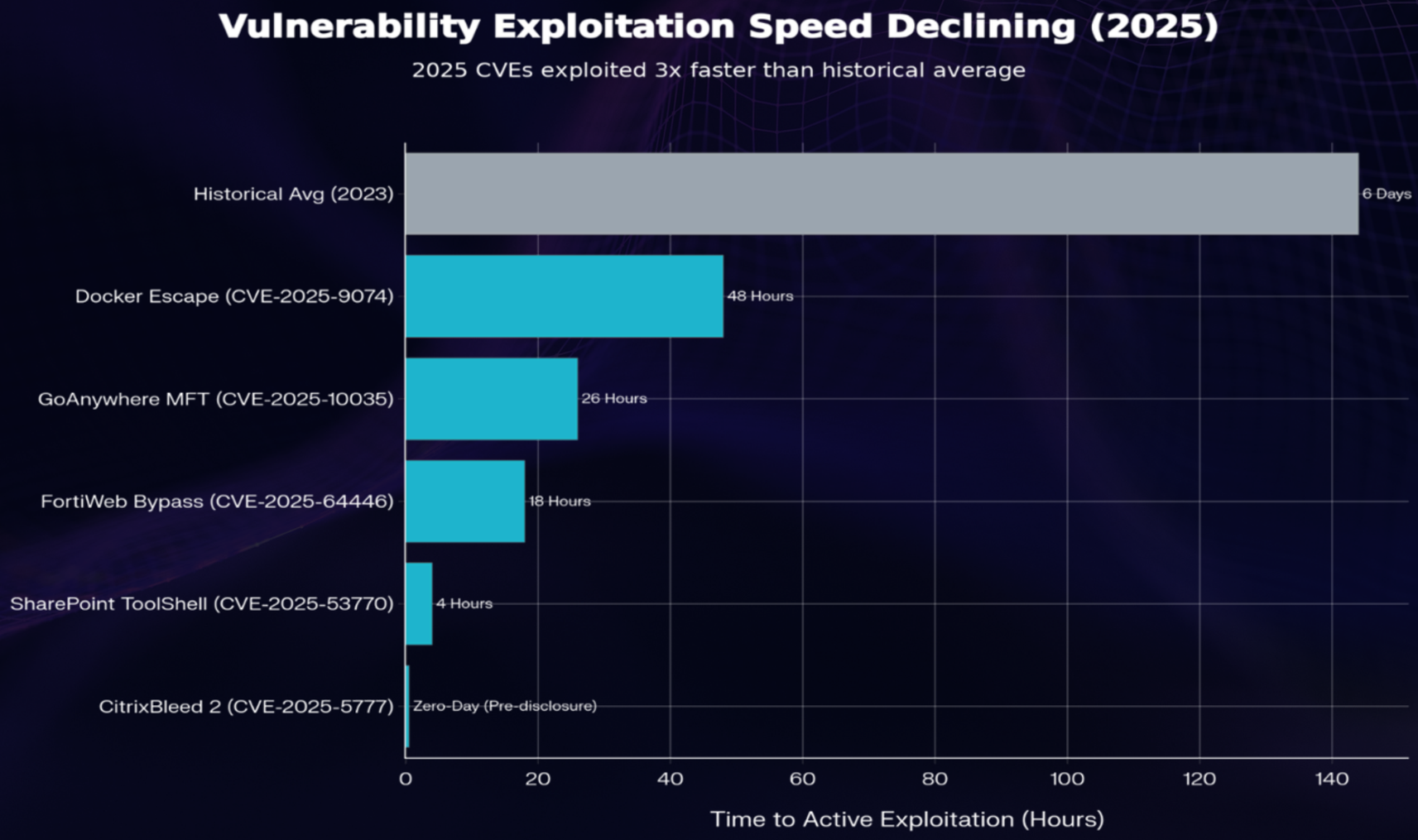
Published: November 13, 2025

VULNERABILITY LANDSCAPE

CRITICAL EDGE SERVICES UNDER SIEGE

Late 2025 saw a surge in zero-day exploitation of unauthenticated edge services, including rapid weaponization of CitrixBleed 2 (CVE-2025-5777) and FortiWeb (CVE-2025-64446), enabling initial access without credentials and bypassing perimeter defences. The fast turn from disclosure to exploitation for SharePoint ToolShell (CVE-2025-53770) shows threat actors are compromising major collaboration platforms within hours. After entry, adversaries have leveraged vulnerabilities such as GoAnywhere MFT (CVE-2025-10035) and Docker (CVE-2025-9074) to enable ransomware deployment, container escape and rapid lateral movement across hybrid environments, reinforcing the need to harden internet facing management interfaces and rely on behaviour based detection when patching lags.

VULNERABILITY LANDSCAPE



DOCUMENT REFERENCES

REFERENCES

Insurance Sources

https://securitybrief.com.au/story/ransomware-attacks-surge-in-australia-new-zealand-on-holidays
https://anziif.com/professional-development/articles/2025/07/how-apac-insurers-can-tackle-ai-powered-cyber-threats
https://securitybrief.com.au/story/2025-ransomware-business-as-usual-business-is-booming
https://www.cyberdaily.au/security/11833-exclusive-kiwi-insurance-broker-confirms-it-is-investigating-a-ransomware-attack
https://reliaquest.com/blog/ransomware-cyber-extortion-threat-intel-q2-2025/
https://securitybrief.com.au/story/quadruple-extortion-ransomware-rises-in-asia-pacific-region
https://www.cyfirma.com/research/tracking-ransomware-june-2025/
https://borderlesscs.com.au/2024-data-breach-lists/
https://www.qbe.com/media/qbe/apac/new-zealand/files/qbe-cyber-report-click-breach-repeat-2025.pdf
https://www.rapid7.com/blog/post/2025/04/08/2025-ransomware-business-as-usual-business-is-booming/
https://www.insurancebusinessmag.com/au/news/cyber/cyber-insurance-claims-steady-but-risk-environment-remains-complex-551115.aspx
https://www.insurancebusinessmag.com/au/news/cyber/australia-and-new-zealand-trail-in-ransomware-recovery-speed-555503.aspx
https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025
https://www.webberinsurance.com.au/data-breaches-list
https://www.abc.net.au/news/2024-06-22/medibank-alerts-australia-cybersecurity-breach/104003576
https://www.ebminsurance.com.au/resources/news/washing-woes/
https://cyble.com/blog/ai-powered-cyberattacks-surge-in-australia/
https://www.ajg.com/au/-/media/files/gallagher/au/news-and-insights/gallagher-cyber-insurance-market-update.pdf
https://www.aic.gov.au/sites/default/files/2020-05/tandi408.pdf
https://cisoonline.com.au/cyber-attacks-and-data-breaches/the-2024-data-breach-notifications-in-australia/
https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html
https://securitybrief.com.au/story/australian-firms-face-surge-in-ai-driven-cyber-attacks-scams
https://www.upguard.com/blog/biggest-data-breaches-australia
https://www.pwc.com.au/cyber-security-digital-trust/global-threat-intelligence-year-in-retrospect.html
https://www.cm-alliance.com/cybersecurity-blog/september-2024-major-cyber-attacks-data-breaches-ransomware-attacks
https://www.hsfkramer.com/notes/cybersecurity/2025-posts/cyber-security-a-month-in-retrospect-august-september-2025
https://www.ransomware.live/map/AU https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-australia-and-new-zealand/
https://attack.mitre.org/groups/
https://www.oaic.gov.au/news/media-centre/data-breach-report-highlights-supply-chain-risks
https://redpiranha.net/news/threat-intelligence-report-august-5-august-11-2025
https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024
https://cyberpeaceinstitute.org/wp-content/uploads/2025/10/APAC-Financial-Inclusion-Report.pdf
https://www.halcyon.ai/raas-mq/power-rankings-ransomware-malicious-quartile-q1-2025 https://www.wipro.com/blogs/ganesha-rajanaidu/cyber-threats-in-healthcare/
https://research.checkpoint.com/2025/17th-march-threat-intelligence-report/ Cl0p - https://www.theregister.com/2025/11/10/allianz_uk_joins_growing_list/?utm_source=chatgpt.com - Threat Intel brief highlighting Cl0p's CVE-2025-61882

REFERENCES

Insurance Sources

https://www.wipro.com/blogs/ganesha-rajanaidu/cyber-threats-in-healthcare/
https://research.checkpoint.com/2025/17th-march-threat-intelligence-report/
Cl0p - https://www.theregister.com/2025/11/10/allianz_uk_joins_growing_list/?utm_source=chatgpt.com - Threat Intel brief highlighting Cl0p's CVE-2025-61882
Allianz Life – Salesforce / ShinyHunters / Scattered Spider campaign
https://www.obsidiansecurity.com/resource/allianz-data-leaked-in-major-wave-of-salesforce-attacks
https://apnews.com/article/12b991a141c24d3a060642c0d173e0be
https://www.reuters.com/legal/government/hack-allianz-life-impacts-11-million-customers-breach-notification-site-says-2025-08-18/
https://www.ft.com/content/ae99065b-a2e9-4dc0-8ef4-0280a2c8a739
https://www.bleepingcomputer.com/news/security/farmers-insurance-data-breach-impacts-11m-people-after-salesforce-attack/?utm_source=chatgpt.com
Qilin - https://businessinsights.bitdefender.com/korean-leaks-campaign-targets-south-korean-financial-services-qilin-ransomware
https://www.breachsense.com/breaches/samera-health-data-breach/?utm_source=chatgpt.com
Vercoe Insurance Brokers (New Zealand) – DragonForce
https://www.cyberdaily.au/security/11833-exclusive-kiwi-insurance-broker-confirms-it-is-investigating-a-ransomware-attack?utm_source=chatgpt.com
https://www.insurancenews.com.au/the-broker/nz-brokerage-suffers-cyberattack?utm_source=chatgpt.com
https://socautomation.com/nz_insurance_cyberattack/?utm_source=chatgpt.com
Scattered Spider vs insurers (Aflac, Erie, etc.) - Global (US Insurance)
https://www.cybersecuritydive.com/news/aflac-cyber-crime-spree-insurance/751175/
https://cyberscoop.com/aflac-cyberattack-insurance-sector-scattered-spider/
https://pushsecurity.com/blog/key-takeaways-from-the-scattered-spider-attacks-on-insurance-firms/
https://ar.casact.org/caught-in-the-web-targeted-cyber-attacks-on-insurers/
Coordinated credential-stuffing attack on major Australian super funds. Multi-fund attack against AustralianSuper, Rest, Hostplus, Australian Retirement Trust, Insignia/MLC, Cbus etc. No public APT/ransomware group attribution
https://www.theguardian.com/australia-news/2025/apr/04/australian-super-funds-compromised-cybersecurity-data-breach-hack
https://www.afr.com/companies/financial-services/cyberattack-launched-on-major-australian-superannuation-funds-20250404-p5lp4l
https://www.news.com.au/national/crime/mass-superannuation-cyber-attack-overdue-inevitable-expert-says-after-aussie-funds-targeted/news-story/b28405f9a2c383ae1f149e8db09d2d9c
https://www.theaustralian.com.au/business/australiansuper-says-passwords-potentially-compromised-in-a-coordinated-attack-on-super-funds/news-story/a76c29501e99623577a367ad7dec04c2
https://www.choice.com.au/data-protection-and-privacy/protecting-your-data/data-privacy-and-safety/articles/superannuation-funds-data-breach
https://cyberwardens.com.au/super-fund-breach-what-happened-and-how-to-protect-your-account/
https://blog.stockspot.com.au/australian-super-cyber-attack/
https://secure-iss.com/australias-super-fund-breach-the-password-problem/
https://www.superguide.com.au/super-booster/super-news-for-april-2025
https://www.abc.net.au/news/2025-04-08/customers-warned-australian-super-fund-weakness-cyberattacks/105147170

https://www.theaustralian.com.au/business/australiansuper-says-passwords-potentially-compromised-in-a-coordinated-attack-on-super-funds/news-story/a76c29501e99623577a367ad7dec04c2
https://www.news.com.au/national/crime/mass-superannuation-cyber-attack-overdue-inevitable-expert-says-after-aussie-funds-targeted/news-story/b28405f9a2c383ae1f149e8db09d2d9c

REFERENCES

Insurance Sources

Financial and insurance services are now the most frequently reported non-government sector and also the top CI division for DDoS incidents (32% of CI incidents, 17% of DDoS incidents). -
https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025?utm_source=chatgpt.com
https://www.insurancebusinessmag.com/au/news/cyber/cyber-insurance-claims-steady-but-risk-environment-remains-complex-551115.aspx?utm_source=chatgpt.com - interesting
https://anziif.com/professional-development/articles/2025/07/how-apac-insurers-can-tackle-ai-powered-cyber-threats?utm_source=chatgpt.com - interesting
https://insuranceasia.com/insurance/in-focus/how-cyber-claims-in-asia-were-all-tied-ransomware-in-2025?utm_source=chatgpt.com - interesting

Government Sources

https://www.oaic.gov.au/news/blog/latest-notifiable-data-breaches-statistics-for-july-to-december-2024
https://www.pinsentmasons.com/out-law/news/oaic-data-confirms-cybersecurity-threats-australia-escalating
https://www.counterfraud.gov.au/news/general-news/beware-mind-hackers-growing-threat-social-engineering
https://www.eftsure.com/en-au/blog/cyber-crime/apt40-cyber-threats-to-australia/
https://www.sbs.com.au/news/article/china-backed-cybercrime-group-accused-of-targeting-australia/oqc7wwg8x
https://www.asd.gov.au/news/2024-07-09-prc-state-sponsored-cyber-group-apt40s-expanding-tradecraft-and-tactics
https://www.hsfkramer.com/notes/cybersecurity/2025-posts/cyber-security-a-month-in-retrospect-august-september-2025
https://www.cyberdaily.au/security/7948-chinese-linked-apt-group-targeting-australia-and-south-east-asia
https://www.neweratech.com/au/blog/top-3-cyber-incidents-in-australia-october-2025-update/
https://borderlesscs.com.au/2025-data-breach-lists/
https://securitybrief.com.au/story/ransomware-attacks-surge-in-australia-new-zealand-on-holidays
https://www.hsfkramer.com/notes/cybersecurity/2024-posts/cyber-security-a-month-in-retrospect-australia-october-2024
https://www.abc.net.au/news/2025-10-01/ransomware-attacks-on-small-businesses-cybersecurity/105835708
https://securitybrief.com.au/story/quadruple-extortion-ransomware-rises-in-asia-pacific-region
https://stephens.com.au/data-breach-cybersecurity-and-privacy-law-update-september-2025/
https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-security-act
https://www.homeaffairs.gov.au/cyber-security-subsite/Pages/cyber-security-act.aspx
https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025
https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/apt40-advisory-prc-mss-tradecraft-in-action
https://www.hsfkramer.com/notes/cybersecurity/2025-posts/cyber-security-two-months-in-retrospect-may-june-2025
https://www.webberinsurance.com.au/data-breaches-list
https://www.upguard.com/blog/biggest-data-breaches-australia
https://publicsectornetwork.com/insight/2025-ransomware-holiday-risk-report
https://cybercx.com.au/news/cybercx-2025-threat-report-media-release/
https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

REFERENCES

Government Sources

https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/countering-chinese-state-sponsored-actors-compromise-of-networks-worldwide-to-feed-global-espionage-system
https://cisoonline.com.au/cyber-attacks-and-data-breaches/the-2024-data-breach-notifications-in-australia/
https://www.abc.net.au/news/2024-07-11/australia-accusation-china-cyber-espionage-explained/104082308
https://www.cm-alliance.com/cybersecurity-blog/sept-2025-biggest-cyber-attacks-ransomware-attacks-and-data-breaches
https://www.ottoit.com.au/blog/biggest-australian-cyber-breaches-in-2025/
https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024
https://ami.org.au/knowledge-hub/oaic-reports-record-high-data-breach-notifications-in-2024/
https://attack.mitre.org/groups/G0065/ https://cisoonline.com.au/cyber-attacks-and-data-breaches/the-2025-data-breach-notifications-in-australia/ Muswellbrook Shire Council (Australia – local government) – SafePay ransomware
https://www.cyberdaily.au/security/11596-exclusive-muswellbrook-shire-council-confirms-december-ransomware-attack?utm_source=chatgpt.com
https://www.muswellbrook.nsw.gov.au/cyber-incident/?utm_source=chatgpt.com
https://www.cyberlutions.com.au/copy-of-2025-updated-regularly-data-breach-notifications-in-australia?utm_source=chatgpt.com
https://www.cyberlutions.com.au/copy-of-2025-updated-regularly-data-breach-notifications-in-australia?utm_source=chatgpt.com Legal Practice Board of Western Australia (Australia – statutory authority / regulator) – Dire Wolf ransomware
https://www.cyberdaily.au/security/12158-exclusive-legal-practice-board-of-western-australia-confirms-dire-wolf-ransomware-attack?utm_source=chatgpt.com
https://www.lpbwa.org.au/cyber-incident?utm_source=chatgpt.com
https://www.peteraclarke.com.au/2025/05/29/legal-practice-board-of-western-australia-suffers-significant-data-breach-with-bank-details-and-contact-information-posted-on-the-dark-web/?utm_source=chatgpt.com
https://www.lawyersweekly.com.au/biglaw/43083-legal-practice-board-of-wa-begins-notifying-data-breach-victims?utm_source=chatgpt.com
https://databreaches.net/2025/10/02/legal-practice-board-of-western-australia-begins-notifying-data-breach-victims/?utm_source=chatgpt.com New Zealand government & critical infrastructure organisations – ServerKillers (pro-Russia hacktivist DDoS)
https://cybercx.co.nz/blog/active-ddos-threat-against-new-zealand-government-and-critical-infrastructure-organisation/?utm_source=chatgpt.com https://www.ncsc.govt.nz/insights-and-research/cyber-threat-reports/cyber-threat-report-2025/judgement-3?utm_source=chatgpt.com
https://www.ncsc.govt.nz/assets/insights/cyber-threat-report/NCSC-CyberReport2025-FINAL.pdf?utm_source=chatgpt.com
https://securitybrief.co.nz/story/new-zealand-urged-to-boost-cyber-security-as-threats-diversify?utm_source=chatgpt.com Government of Samoa / Pacific government networks – APT40 (China-backed)
https://www.abc.net.au/news/2025-02-12/china-backed-apt40-blamed-for-cyber-attacks-on-samoa/104927412?utm_source=chatgpt.com https://industrialcyber.co/ransomware/samoa-warns-of-apt40-hackers-targeting-organizations-in-blue-pacific-region-urges-immediate-action/?utm_source=chatgpt.com
https://www.samoaobserver.ws/category/editorial/113230?utm_source=chatgpt.com
https://www.aspistrategist.org.au/the-pacific-needs-greater-cyber-resilience-as-malicious-actors-break-into-networks/?utm_source=chatgpt.com Asia–Pacific government & foreign affairs entities – Mysterious Elephant (APT)
https://www.kaspersky.com/about/press-releases/an-elephant-in-the-room-kaspersky-detects-new-mysterious-elephant-activity-in-asia-pacific?utm_source=chatgpt.com
https://securelist.com/mysterious-elephant-apt-ttps-and-tools/117596/?utm_source=chatgpt.com
https://www.darkreading.com/cyberattacks-data-breaches/mysterious-elephant-recycled-malware?utm_source=chatgpt.com

REFERENCES

Government Sources

https://vietnamnews.vn/advertisement/1724151/kaspersky-apts-haunt-state-secrets-diplomatic-files-and-nuclear-plants-across-apac.html?utm_source=chatgpt.com Noosa Shire Council (QLD local government) – International criminal gangs / AI-enabled payment-redirect fraud
https://www.noosa.qld.gov.au/About-Council/News-and-publications/Media-releases/2025/Council-strengthens-processes-to-safeguard-against-cyber-fraud?utm_source=chatgpt.com
https://www.noosa.qld.gov.au/About-Council/News-and-publications/Media-releases/2025/Message-from-the-CEO-regarding-cyber-fraud-incident?utm_source=chatgpt.com
https://www.abc.net.au/news/2025-10-14/noosa-council-scam-mayor-blames-ai-imitation/105887962?utm_source=chatgpt.com Nation-state / APT activity – Australia (government-adjacent, last quarter)
https://www.abc.net.au/news/2025-11-12/spy-chief-warns-of-china-espionage-threat-to-business/105999522?utm_source=chatgpt.com
https://www.reuters.com/world/china/australia-spy-chief-says-chinese-hackers-probing-telecommunications-critical-2025-11-12/?utm_source=chatgpt.com
https://www.aspistrategist.org.au/chinese-cyber-skirmishes-in-the-indo-pacific-show-emerging-patterns-of-conflict/?utm_source=chatgpt.com
https://industrialcyber.co/reports/acsc-reports-surge-in-cyberattacks-targeting-australias-critical-infrastructure-focus-shifts-to-building-resilience/?utm_source=chatgpt.com
https://unit42.paloaltonetworks.com/threat-brief-ivanti-cve-2025-0282-cve-2025-0283/
https://www.picussecurity.com/resource/blog/cisa-alert-aa25-239a-analysis-simulation-and-mitigation-of-chinese-apts
https://breached.company/massive-chinese-espionage-campaign-targets-global-network-infrastructure/
https://www.eftsure.com/blog/cyber-crime/apt40-cyber-threats-to-australia/
https://www.defenceconnect.com.au/joint-capabilities/15527-nation-state-hackers-continue-to-target-australian-orgs-as-greyzone-operations-intensify-year-on-year
https://www.aspistrategist.org.au/the-pacific-needs-greater-cyber-resilience-as-malicious-actors-break-into-networks/
https://www.landers.com.au/legal-insights-news/cyber-trends-that-will-define-2025-and-beyond
https://www.senatorpaterson.com.au/news/spy-agencies-kept-australian-mps-in-dark-after-they-were-targeted-by-chinese-hackers

Private Sector Sources

https://borderlesscs.com.au/2025-data-breach-lists/
https://cyble.com/blog/australian-data-breaches-2025-surge/
https://securitybrief.com.au/story/anz-firms-face-rising-repeat-ransomware-attacks-executive-threats
https://industrialcyber.co/ransomware/qilin-ransomware-escalates-rapidly-in-2025-targeting-critical-sectors-with-700-attacks-amid-ransomhub-shutdown/
https://securitybrief.com.au/story/australian-organisations-face-rising-threat-from-top-ransomware-groups
https://cyble.com/blog/ransomware-groups-targets-australia-and-new-zealand/
https://cyble.com/blog/ransomware-attacks-surge-october-2025/ https://attack.mitre.org/groups/G1015/
https://australiancybersecuritymagazine.com.au/scattered-spider-insights-observations-and-recommendations/
https://www.ottoit.com.au/blog/biggest-australian-cyber-breaches-in-2025/
https://www.cyberdaily.au/security/11580-exclusive-lynx-ransomware-targets-australian-construction-company-novati
https://www.cyberdaily.au/security/12559-exclusive-south-australian-barristers-chambers-listed-on-lynx-ransomware-s-leak-site
https://www.cyberdaily.au/security/12359-nz-it-hardware-and-infrastructure-firm-breached-inc-ransom-claims-responsibility
https://www.cyberdaily.au/security/12436-exclusive-safepay-ransomware-group-finally-lists-ingram-micro-on-leak-site
https://www.leansecurity.com.au/blog/2025/12/2/daily-threat-briefing-australia-02-december-2025

REFERENCES

Private Sector Sources

https://onapsis.com/blog/sap-salesforce-oracle-attacks-rising-2025-report/
https://www.leansecurity.com.au/blog/oracle-ebs-zero-day-cve-2025-61882-australia
https://www.eftsure.com/en-au/blog/cyber-crime/apt40-cyber-threats-to-australia/
https://australiancybersecuritymagazine.com.au/acsc-issues-advisory-warning-of-chinese-state-backed-cyber-threat/
https://cybercx.com.au/blog/managing-cyber-risk-in-the-era-of-volt-typhoon/
https://www.hsfkramer.com/notes/cybersecurity/2025-posts/cyber-security-a-month-in-retrospect-australia-april-2025
https://orca.security/resources/blog/sap-netweaver-cve-2025-31324-vulnerability-exploit/
https://www.reddit.com/r/newzealand/comments/1pifx7e/26000_new_zealanders_devices_infected_with/
https://www.csoonline.com/article/4060101/entra-id-vulnerability-exposes-gaps-in-cloud-identity-trust-models-experts-warn.html
https://securitybrief.com.au/story/ai-driven-cyberattacks-surge-targeting-australian-organisations
https://www.neweratech.com/au/blog/top-3-cyber-incidents-in-australia-october-2025-update/
https://cisoonline.com.au/cyber-attacks-and-data-breaches/the-2025-data-breach-notifications-in-australia/
https://addisons.com/article/federal-court-makes-first-civil-penalty-orders-under-australias-privacy-act/
https://www.oaic.gov.au/news/blog/latest-notifiable-data-breach-statistics-for-january-to-june-2025
https://www.ncsc.govt.nz/assets/insights/cyber-threat-report/NCSC-CyberReport2025-FINAL.pdf
https://borderlesscs.com.au/2024-data-breach-lists/ https://www.aic.gov.au/sites/default/files/2025-11/ti724_ransomware_targeting_individuals_and_small_businesses.pdf
https://www.corbado.com/blog/data-breaches-australia
https://www.dexpose.io/qilin-ransomware-group-strikes-b-dynamic-in-australia/
https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/scattered-spider
https://2631546.fs1.hubspotusercontent-na1.net/hubfs/2631546/Kordia%20NZ%20Business%20Cyber%20Report%202025_2.pdf
https://therecord.media/five-eyes-china-apt40-alert-end-of-life-routers https://tesserent.com/insights/blog/complex-interconnections-understanding-supply-chains-to-manage-risk
https://www.mauriceblackburn.com.au/media-centre/media-statements/2025/compensation-sought-on-behalf-of-aussies-caught-up-in-qantas-data-breach/
https://securitybrief.com.au/story/qantas-data-breach-exposes-5-7-million-in-third-party-cyberattack
https://australianaviation.com.au/2025/07/exclusive-qantas-hacker-gave-airline-72-hour-deadline/
https://therecord.media/qantas-airline-reduces-bonuses-executives-data-breach
https://www.securityweek.com/australian-human-rights-commission-discloses-data-breach/
https://cyberint.com/blog/research/ransomware-annual-report-2024/
https://www.cyberdaily.au/security/12218-report-ddos-attacks-on-financial-institutions-in-apac-surge
https://www.cyberdaily.au/security/12172-exclusive-melbourne-based-3p-corporation-breached-by-space-bears-ransomware
https://www.cyberdaily.au/security/11633-exclusive-cl0p-ransomware-gang-lists-ampol-linfox-and-steel-blue-as-victims
https://cybersecurityasia.net/fs-isac-and-akamai-report-ddos-attacks-apac/
https://thecyberexpress.com/three-firms-hit-by-space-bears-ransomware/
https://peris.ai/post/apac-under-siege-key-cybersecurity-lessons-from-the-2025-x-force-threat-intelligence-report
https://www.cyberdaily.au/security/12262-exclusive-aussie-msp-vertel-confirms-space-bears-ransomware-attack

REFERENCES

Private Sector Sources

https://www.crnasia.com/news/2025/cybersecurity/asia-pacific-had-the-most-cyberattacks-in-2024
https://reliaquest.com/blog/ransomware-and-cyber-extortion-in-q4-2024/
https://blog.qualys.com/vulnerabilities-threat-research/2025/06/18/qilin-ransomware-explained-threats-risks-defenses
https://flashpoint.io/blog/top-threat-actor-groups-targeting-financial-sector/
https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2025/
https://www.proofpoint.com/au/blog/email-and-cloud-threats/evolving-threat-landscape-apac-key-trends-2024
https://www.qbe.com/media/qbe/apac/australia/files/product/cyber-threats-to-the-legal-and-professional-services-sector.pdf
https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/qilin-ransomware/
https://securitybrief.asia/story/southeast-asian-firms-face-surge-in-ransomware-attacks-in-2024