# Express Attack Brief (EAB) v2.0: Q2 2025 Threat Landscape Report

### 1.0. Strategic Overview & Executive Summary

#### 1.1. Foreword from the Analyst

The second quarter of 2025 has been a period of significant strategic transition and dynamic reshuffling within the global cyber threat landscape. On the surface, data might suggest a period of reduced activity; however, a deeper analysis reveals a complex and paradoxical environment. The threat ecosystem is not receding but rather adapting, becoming more fragmented and resilient. This report, the Express Attack Brief (EAB) v2.0, is designed to synthesize this complex intelligence into a single, comprehensive document that bridges the gap between high-level strategic concerns and granular technical details. The objective is to provide senior leadership with the context necessary for informed decision-making and to equip technical teams with the actionable intelligence required to defend against these evolving threats.

#### 1.2. The Q2 2025 Threat Landscape: Fragmentation & Resurgence

The most defining trend of the second quarter of 2025 is a fragmentation paradox. Publicly disclosed ransomware attacks, as tracked by data leak sites, experienced a 23% decline from the previous quarter, a dip that may seem to indicate a reduction in overall threat capacity.1 However, this metric is deceptive. Concurrently, the number of active ransomware groups increased by 45% year-over-year, from 41 groups in Q2 2024 to 71 groups in Q2 2025.1 This surge in the number of actors demonstrates that disruption against major players, such as law enforcement action against LockBit and the dissolution of Alphv/BlackCat, did not diminish the total threat capacity. Instead, it redistributed it among a more numerous and less centralized collection of smaller, more agile actors.1 This decentralization makes the threat landscape more difficult to monitor and defend against, as new groups continuously emerge to fill the void left by their predecessors.

The quarter was further characterized by the success of sophisticated human-centric attacks. Threat actors increasingly bypassed robust technical defenses by targeting the human element through refined social engineering campaigns. The collaboration between the groups known as Scattered Spider and ShinyHunters exemplifies this approach, as they successfully compromised highly secured organizations like Google and Allianz Life not by exploiting technical vulnerabilities in the core infrastructure but by deceiving employees and gaining initial access through third-party platforms.3 This highlights a critical shift away from solely technological exploits toward a blended attack model that prioritizes the psychological manipulation of personnel.

An additional, significant trend that emerged in Q2 2025 is the shift from traditional ransomware-to-extortion, where groups skip the encryption phase entirely. The rebranding of the Hunters International ransomware gang into "World Leaks" and its subsequent exfiltration and public leakage of 1.3 TB of data from Dell Technologies illustrates this evolving monetization strategy.7 By focusing on pure data exfiltration, these actors circumvent the need to deploy and manage complex encryption routines, and they render traditional ransomware defenses, such as robust data backups, less effective. This strategy changes the calculus for victims, forcing them to consider a ransom payment primarily to prevent public exposure and the ensuing reputational damage, rather than to regain access to critical systems.

These incidents underscore the primacy of supply chain risk as a critical and highly vulnerable attack vector. Major breaches at Qantas, Google, and Allianz Life all exploited weaknesses not in the primary infrastructure of the affected organizations but in their third-party platforms and vendors.3 These incidents serve as a stark reminder that an organization's security posture is only as strong as its weakest vendor link. The interconnectedness of modern business operations means that a compromise within one small, less-resourced vendor can have cascading and severe consequences for a large, well-defended corporation.

### 2.0. Comprehensive Victim Analysis & Targeting Patterns

#### 2.1. Major Breach Overview

The second quarter of 2025 was marked by several high-profile cyber incidents, each providing a unique perspective on the evolving tactics of threat actors.

**The Qantas Incident: A Case Study in Supply Chain Flank Attacks.** In early July, Qantas Airways confirmed a major data breach that exposed the personal information of up to 6 million customers.11 The vulnerability was not found within Qantas's core network but rather within a third-party platform used for customer support operations.10 The data compromised included names, phone numbers, email addresses, dates of birth, and frequent flyer numbers.11 Despite the crucial absence of financial or passport data, the exposure of this Personally Identifiable Information (PII) created a significant legal and reputational risk. The incident exemplifies a "flank attack" on the supply chain, where threat actors target a less-defended vendor to gain a foothold that compromises a larger, more resilient parent organization.

**The Google & Allianz Life Breaches: The Vishing Vector.** These incidents, both occurring in the quarter, demonstrate the effectiveness of a sophisticated vishing campaign. The ShinyHunters group, tracked as UNC6040, compromised a corporate Salesforce CRM instance at Google in June, affecting an estimated 2.55 million business contacts.3 Similarly, Allianz Life confirmed a breach in July that exposed data for the majority of its 1.4 million customers via a cloud-based CRM system, which is suspected to be Salesforce.15 These attacks were successful not due to a zero-day exploit in the Salesforce platform itself, but through a social engineering technique where attackers impersonated IT staff to trick employees into granting unauthorized access to their cloud environments.4

**The Dell Incident: The Business of Pure Extortion.** The Dell Technologies breach in July provides a clear illustration of the shift toward pure data exfiltration and extortion.7 A group known as World Leaks, identified as a rebranding of the Hunters International ransomware gang, exfiltrated a massive 1.3 TB trove of data from Dell's Customer Solution Center platform.7 This incident is notable because the threat actor skipped the traditional encryption phase of a ransomware attack, opting instead to immediately leak the data online.8 While Dell claimed the data was "primarily synthetic, publicly available or Dell systems/test data" 7, the files reportedly included infrastructure scripts, employee folders, and tools, suggesting the data may have been more sensitive than initially claimed.

#### 2.2. Quantified Operational & Financial Impacts

The fallout from these attacks extends far beyond technical remediation. The operational and financial impacts highlight the severe consequences of a successful compromise.

* **Qantas's Financial & Legal Fallout:** The Qantas breach had an immediate and visible financial impact. The airline's shares dropped by as much as 4.1% following the incident's confirmation.19 More significant are the potential legal repercussions under Australia's strengthened Privacy Legislation Amendment. Under this legislation, Qantas could face a maximum penalty of up to AUD$6.6 billion, a figure derived from 30% of its annual Australian turnover.20 The incident also introduces the prospect of civil litigation, as new statutory tort provisions allow affected individuals to sue for damages.20
* **Other Financial Impacts:** The financial repercussions of cyberattacks are not limited to large-scale enterprises. The report from a UK retailer in April attributed a compromise to the DragonForce group, with an expected impact on this year's profits of approximately $400 million.2 This demonstrates the significant and business-threatening financial consequences that can arise from targeted cybercrime.

#### 2.3. Victim Targeting & Sectoral Analysis

An analysis of the quarter's most significant incidents reveals consistent targeting patterns and commonalities among victims. While manufacturing, technology, legal services, and construction remained the top targets for overall ransomware activity, the most high-profile and disruptive breaches consistently targeted organizations with a heavy reliance on cloud-based, third-party platforms.1 The victims in these prominent cases—Qantas (aviation), Allianz Life (insurance), and Google (technology)—all had their initial compromise rooted in a shared vulnerability: the human element interacting with a cloud-based vendor service. This trend shows a strategic focus by threat actors on exploiting the weakest point in an organization's defense perimeter, which is often its extended digital supply chain.

**Table 2.1: Q2 2025 Victim Analysis: Confirmed & Suspected Organizations**

| Organization | Country | Sector | Incident Type | Compromised Records/Data | Attributed Threat Actor(s) | Confidence Score | Key Operational/Financial Impact | Supply Chain/Third-Party Link |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Confirmed Victims** |  |  |  |  |  |  |  |  |
| Qantas | Australia | Aviation | Data Breach (Third-Party) | 5.7M unique customer records 11 | Scattered Spider, ShinyHunters 13 | High | 4.1% stock drop 19; Potential AUD$6.6B fine 20 | Yes (third-party contact center platform) 10 |
| Google | USA | Technology | Data Theft (CRM) | 2.55M business contacts 3 | ShinyHunters (UNC6040) 3 | High | No financial impact on products; Data exfiltration 3 | Yes (corporate Salesforce instance) 3 |
| Allianz Life | USA | Insurance | Data Theft (CRM) | Majority of 1.4M customer records 15 | Suspected ShinyHunters, Scattered Spider 15 | High | FBI notified; 24 months free identity protection offered 17 | Yes (third-party cloud CRM) 16 |
| Dell Technologies | USA | Technology | Data Extortion | 1.3 TB of data (synthetic/test) 7 | World Leaks (rebranded Hunters International) 7 | High | Public data leak; No reported operational impact 18 | Yes (Customer Solution Center platform) 7 |
| **Suspected Victims** |  |  |  |  |  |  |  |  |
| Air France | France | Aviation | Data Breach (Third-Party) | Names, contact details, loyalty numbers 3 | ShinyHunters 3 | Medium | Customer notification; Ongoing investigation 3 | Yes (third-party customer support tool) 3 |
| KLM | Netherlands | Aviation | Data Breach (Third-Party) | Passenger names, contact details 3 | ShinyHunters 3 | Medium | Customer notification; Ongoing investigation 3 | Yes (third-party customer support tool) 3 |
| Adidas | Global | Retail | Data Theft (CRM) | Undisclosed | ShinyHunters 3 | Low | Unconfirmed details; Listed as victim of broader campaign 24 | Yes (Salesforce platform) 25 |
| LVMH Brands | Global | Retail | Data Theft (CRM) | Undisclosed | ShinyHunters 3 | Low | Unconfirmed details; Listed as victim of broader campaign 24 | Yes (Salesforce platform) 25 |
| Chanel & Pandora | Global | Retail | Data Theft (CRM) | Undisclosed | ShinyHunters 4 | Low | Unconfirmed details; Disclosed breach of customer data 25 | Yes (Salesforce platform) 24 |

*Confidence Score:* ***High*** *- Supported by multiple, independent, authoritative sources;* ***Medium*** *- Supported by consistent TTPs and initial reporting from a single, authoritative source;* ***Low*** *- Speculative, uncorroborated claim from a single source or actor.*

### 3.0. Threat Actor Profiles & Thematic Connections

#### 3.1. The New Power Players: Qilin, Akira, and DragonForce

The fragmentation of the ransomware ecosystem has led to the emergence of new, dominant actors who have quickly filled the vacuum left by defunct operations.

* **Qilin's Dominance:** Qilin has rapidly ascended to become the most active and dominant ransomware group of the quarter. The group conducted more than 200 attacks, nearly double the volume of the next most active groups.1 This surge in activity is attributed to its reliance on the mass exploitation of critical vulnerabilities, such as those found in Fortinet/FortiGate products, to achieve initial access.21
* **Akira's Exponential Growth:** The Akira ransomware group demonstrated remarkable consistency and effectiveness, listing approximately 130 organizations on its data-leak site this quarter alone.21 The group has shown staggering growth, with a 348% year-over-year increase in victim posts in Q2 2025 compared to the same period last year, indicating its sustained and escalating threat capacity.21
* **DragonForce's Cartel Strategy:** DragonForce, which holds the fifth spot in attack volume, has adopted an aggressive cartel strategy.1 The group attempted a hostile takeover of the RansomHub operation and actively recruits affiliates, demonstrating a desire to consolidate power within the ecosystem. A key part of its strategy involves partnering with initial access brokers, such as Scattered Spider, to facilitate attacks.2

#### 3.2. Threat Convergence: Scattered Spider & ShinyHunters

One of the most concerning developments of the quarter is the observed convergence of tactics and victims between the highly sophisticated social engineering group Scattered Spider and the data extortion group ShinyHunters. Scattered Spider is an elite threat actor known for its initial access prowess, specializing in social engineering, SIM swapping, and help-desk impersonation to infiltrate target networks.6 ShinyHunters has demonstrated a specific and highly effective method for targeting Salesforce environments through vishing, an attack method that mimics IT support to trick employees into granting access.4

The operational overlap between these groups is significant and suggests a potential collaboration. Multiple authoritative sources confirm that both groups were tied to breaches at Qantas, Google, and Allianz Life, all of which leveraged similar tactics and targeted cloud-based CRM systems.5 The appearance of the alias "Sp1d3rHunters" on cybercriminal forums further substantiates the connection, as it appears to be a portmanteau of the two groups' names, linking them directly to this ongoing campaign.5

This partnership represents an evolutionary leap in the cybercrime business model. Scattered Spider provides the initial human-centric compromise—a highly refined and scalable skill. ShinyHunters, in turn, provides the specific post-exploitation capability to exfiltrate data from a common and valuable target, such as a Salesforce instance. This specialized division of labor allows the combined entity to rapidly scale its operations, bypass the strongest technical defenses by exploiting the weakest link—the human—and then leverage a specific, widespread cloud-based platform for maximum data theft. Consequently, an organization must defend against a blended attack model that combines disparate tactics, forcing a shift from a reactive, signature-based defense to a more holistic, identity-focused security posture.

### 4.0. Technical Analysis & Incident Deep-Dive

#### 4.1. The Salesforce Vishing Campaign: A Technical Breakdown

The series of breaches linked to the ShinyHunters/Scattered Spider collaboration provides a blueprint for how sophisticated actors are compromising cloud-based platforms. The initial access vector is a highly refined vishing scheme. Attackers impersonate IT support personnel via a phone call and deceive an employee into authorizing a malicious application.3 This is often achieved by instructing the employee to enter a seemingly benign 8-digit code, which, when entered, connects the attacker's data exfiltration program to the company's Salesforce instance. The attackers often masquerade their malicious application as a legitimate Salesforce tool, such as "Data Loader," which is used for importing or exporting bulk data.4

Once the malicious application is authorized, the attacker gains access to the company's Salesforce "instance" and is free to exfiltrate large volumes of data.4 This attack method was responsible for the theft of 2.55 million business contacts from Google and the personal information of the majority of Allianz Life's 1.4 million customers.3 In some cases, the threat actors reportedly expanded their access to other cloud applications, such as Microsoft 365, to further their reconnaissance and data theft objectives.4 The success of this campaign demonstrates that even organizations with robust internal security can be compromised by a threat actor who meticulously targets the human element to bypass technical controls.

#### 4.2. Pure Data Extortion: The Dell Incident as a New Model

The Dell Technologies breach serves as a powerful case study for an emerging monetization strategy in the cybercrime world. The threat actor, World Leaks, explicitly adopted a pure data exfiltration model, bypassing the traditional ransomware step of encrypting files and holding them hostage.7 Instead, the group’s leverage was solely the threat of publicly leaking the 1.3 TB of stolen data.7 This strategic pivot has several profound implications.

By eliminating the encryption phase, the threat actor streamlines their operation, making the process faster and less technically demanding.7 More critically, it changes the defensive paradigm for victims. For a group like World Leaks, which has reportedly provided free decryption tools to previous victims, the value of the stolen data lies not in its ability to lock down a network but in its potential for public exposure and reputational damage. This strategy renders traditional ransomware defense measures, such as maintaining robust, segmented backups, far less effective. The incident forces organizations to recognize that data exfiltration and public extortion are a separate and potent threat that requires a dedicated Data Loss Prevention (DLP) strategy in addition to existing ransomware defenses. The focus shifts from operational recovery to mitigating legal and reputational risk.

### 5.0. Threat Actor TTPs & Forensic Artifacts

#### 5.1. Initial Access Techniques: A New Dominance of Social Engineering

The attack patterns of Q2 2025 reveal two primary initial access techniques: sophisticated social engineering and vulnerability exploitation. Threat actors, particularly Scattered Spider and ShinyHunters, have honed their social engineering prowess.5 Their methods include vishing (voice phishing), which involves impersonating IT help desk staff to manipulate employees into divulging credentials or authorizing malicious applications.5 The use of custom, brand-impersonating domains, such as

dashboard-salesforce[.]com, and phishing pages mimicking legitimate single sign-on (SSO) portals like Okta, further enhances the credibility of these attacks and increases their success rate.5

In parallel, other dominant groups like Qilin and Akira continue to rely on the mass exploitation of critical vulnerabilities.21 They leverage public proof-of-concept (PoC) exploits and automated discovery tools to scan for and compromise systems with vulnerable edge devices like firewalls and VPNs.21 The continued targeting of technologies from vendors such as Fortinet, SonicWall, and Cisco, with a focus on both new and legacy vulnerabilities, demonstrates that this remains a highly effective initial access vector for large-scale operations.29

#### 5.2. Post-Exploitation & Lateral Movement

After gaining initial access, threat actors employ a mix of legitimate tools and custom malware to establish persistence, elevate privileges, and exfiltrate data. Scattered Spider, for instance, is known for its extensive use of legitimate remote access tools, including Fleetdeck, Atera, AnyDesk, and Ngrok.6 By using these trusted applications, the group can maintain covert access and operate under the radar of conventional security monitoring tools, as the activity can blend in with expected administrative traffic.6

The group also employs specialized reconnaissance frameworks, such as ADRecon and Rubeus, to enumerate domain controllers and user accounts, and it utilizes Windows management tools to map the target environment.6 This intelligence is used to carefully plan lateral movement, often by abusing misconfigured Microsoft Certificate Services templates to request and issue their own certificates, which provides stealthy privilege escalation.6 The reliance on these legitimate or "living-off-the-land" tools and social engineering forces defenders to shift their focus from signature-based detection to a more proactive, behavioral monitoring approach to spot anomalous activities.

#### 5.3. Q2 2025 Critical Vulnerabilities

The second quarter of 2025 saw a number of high-severity vulnerabilities patched, many of which are known to be actively exploited in the wild. The Microsoft August 2025 security update alone addressed 107 vulnerabilities, including one publicly disclosed zero-day and 13 Critical vulnerabilities.31

**Table 5.1: Critical Q2 2025 Vulnerabilities & Attributed Exploitation**

| CVE ID | Vulnerability Type | CVSS Score | Affected Component | Known Exploitation Methods | Attributed Threat Actor/Campaign |
| --- | --- | --- | --- | --- | --- |
| CVE-2025-53779 | Elevation of Privilege (EoP) | 7.2 (Moderate) | Windows Kerberos | Relative path traversal over network connection; Allows high-privilege actors to gain domain administrator access 31 | Publicly disclosed zero-day 31 |
| CVE-2025-50165 | Remote Code Execution (RCE) | 9.8 (Critical) | Windows Graphics Component | Untrusted pointer dereference and use of uninitialized resources triggered by malicious JPEG images 31 | Unauthenticated remote attackers 31 |
| CVE-2025-53766 | Remote Code Execution (RCE) | 9.8 (Critical) | GDI+ | Heap-based buffer overflow via specially crafted metafiles in documents; Possible without user interaction on web services 31 | Unauthenticated remote attackers 31 |
| CVE-2025-53778 | Elevation of Privilege (EoP) | 8.8 (Critical) | Windows NTLM | Improper authentication leading to privilege escalation from low-privileged access 31 | Authenticated attackers with low privileges 31 |
| CVE-2025-8875 | Insecure Deserialization | N/A | N-able N-central | Active exploitation in the wild 32 | Unknown 32 |
| CVE-2025-8876 | Command Injection | N/A | N-able N-central | Active exploitation in the wild 32 | Unknown 32 |
| CVE-2024-55591 | Remote Code Execution | N/A | Fortinet/FortiGate | Active exploitation for initial access 21 | Qilin ransomware group 21 |
| CVE-2024-21762 | Remote Code Execution | N/A | Fortinet/FortiGate | Active exploitation for initial access 21 | Qilin ransomware group 21 |

### 6.0. Evidence-Based Analysis & Documentation

#### 6.1. Forensic Confidence Scoring Framework

All claims and attributions within this report are assigned a confidence score based on a defined framework. This methodology is designed to provide an objective assessment of the reliability of the intelligence.

* **High Confidence:** This score is reserved for claims supported by multiple, independent, authoritative sources, such as government agencies (e.g., CISA, FBI), major commercial threat intelligence firms (e.g., GuidePoint, Rapid7, ReliaQuest), and direct public disclosures from the affected organization.33
* **Medium Confidence:** This score is used when a claim is plausible and supported by consistent, circumstantial evidence, such as overlapping tactics, techniques, and procedures (TTPs) and initial reporting from a single authoritative source.33
* **Low Confidence:** This score is assigned to speculative or uncorroborated claims, such as those made by the threat actor themselves or unverified reports from a single non-authoritative source.

#### 6.2. Chain of Custody & Source Attribution

The integrity of this report relies on a meticulous and transparent process of source attribution. The intelligence has been compiled exclusively from publicly available sources, with the provenance of each data point carefully tracked and cited. The methodology for this analysis aligns with professional standards for digital evidence handling, which emphasizes the preservation and non-alteration of original data points, with all analysis performed on duplicated copies to maintain the integrity of the information.35 This documentation ensures that the report's conclusions are verifiable and defensible.

### 7.0. Comprehensive References

* 1  
  <https://www.hipaajournal.com/ransomware-attacks-fall-q2-2025/>
* 2  
  <https://securitybrief.co.uk/story/q2-2025-ransomware-trends-analysis-boom-and-bust>
* 3  
  <https://www.brightdefense.com/resources/recent-data-breaches/>
* 9  
  <https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-july-2025>
* 32  
  <https://www.cisa.gov/news-events/alerts/2025/08/13/cisa-adds-two-known-exploited-vulnerabilities-catalog>
* 31  
  <https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-august-2025/>
* 10  
  <https://www.gerrishlegal.com/blog/qantas-data-breach-puts-six-million-customer-profiles-at-risk>
* 11  
  <https://www.cnet.com/tech/services-and-software/qantas-data-breach-impacts-5-7-million-customers-heres-what-we-know/>
* 13  
  <https://nguard.com/qantas-breach-personal-info-of-5-7m-customers-compromised/>
* 22  
  <https://www.bankinfosecurity.com/scattered-spider-shinyhunters-next-move-leaking-data-a-29170>
* 37  
  <https://exchange.xforce.ibmcloud.com/osint/guid:5838492cf88d423c95e9861b4279ad26>
* 25  
  <https://www.infosecurity-magazine.com/news/google-salesforce-data-theft/>
* 4  
  <https://www.malwarebytes.com/blog/news/2025/08/how-google-adidas-and-more-were-breached-in-a-salesforce-scam>
* 14  
  <https://www.kaseya.com/blog/the-week-in-breach-news-08-13-25/>
* 15  
  <https://www.bleepingcomputer.com/news/security/allianz-life-confirms-data-breach-impacts-majority-of-14-million-customers/>
* 16  
  <https://www.infosecurity-magazine.com/news/third-party-breach-allianz/>
* 17  
  <https://www.cbsnews.com/news/allianz-life-insurance-data-breach/>
* 23  
  <https://www.ampcuscyber.com/shadowopsintel/customer-records-compromised-in-allianz-life-breach/>
* 7  
  <https://tech.co/news/world-leaks-just-leaked-files-dell-data-breach>
* 8  
  <https://www.esecurityplanet.com/security/dell-data-breach-world-leaks-ransomware/>
* 38  
  <https://www.criticalstart.com/resources/dell-data-breach-2024/>
* 18  
  <https://therecord.media/hackers-hit-dell-product-demo-platform-limited-impact>
* 39  
  <https://www.webberinsurance.com.au/data-breaches-list>
* 19  
  <https://www.investing.com/news/stock-market-news/qantas-sayscyber-breach-exposed-customer-data-shares-drop-4-4120252>
* 20  
  <https://idm.net.au/article/0015231-qantas-faces-potential-aud66b-fine-data-breach>
* 12  
  <https://www.qantasnewsroom.com.au/media-releases/update-on-qantas-cyber-incident-wednesday-9-july-2025/>
* 4  
  <https://www.malwarebytes.com/blog/news/2025/08/how-google-adidas-and-more-were-breached-in-a-salesforce-scam>
* 14  
  <https://www.kaseya.com/blog/the-week-in-breach-news-08-13-25/>
* 5  
  <https://reliaquest.com/blog/threat-spotlight-shinyhunters-data-breach-targets-salesforce-amid-scattered-spider-collaboration/>
* 26  
  <https://securitybrief.com.au/story/shinyhunters-scattered-spider-escalate-attacks-on-salesforce>
* 40  
  <https://www.infosecurity-magazine.com/news/financial-services-next-line/>
* 24  
  <https://nationalcioreview.com/articles-insights/extra-bytes/shinyhunters-data-theft-campaign-grows-as-new-corporate-victims-emerge/>
* 28  
  <https://www.silentpush.com/blog/scattered-spider-2025/>
* 6  
  <https://www.halcyon.ai/blog/scattered-spider-tactics-observed-amid-shift-to-us-targets>
* 27  
  <https://www.malwarebytes.com/blog/news/2025/07/allianz-life-says-majority-of-1-4-million-us-customers-info-breached>
* 17  
  <https://www.cbsnews.com/news/allianz-life-insurance-data-breach/>
* 33  
  <https://www.cyware.com/resources/security-guides/cyber-threat-intelligence/what-is-confidence-scoring-in-threat-intelligence>
* 34  
  <https://www.cisa.gov/sites/default/files/publications/AIS%2520Scoring%2520Framework%2520Used%2520for%2520Indicator%2520Enrichment%2520V1.0_508.pdf>
* 35  
  <https://online.champlain.edu/blog/chain-custody-digital-forensics>
* 36  
  <https://techfusion.com/chain-of-custody-in-digital-forensics/>
* 41  
  <https://www.picussecurity.com/resource/blog/tracking-scattered-spider-through-identity-attacks-and-token-theft>
* 30  
  <https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf>
* 1  
  <https://www.hipaajournal.com/ransomware-attacks-fall-q2-2025/>
* 42  
  <https://www.cybermaxx.com/q2-2025-ransomware-research-report/>
* 21  
  <https://reliaquest.com/blog/ransomware-cyber-extortion-threat-intel-q2-2025/>
* 29  
  <https://security.pditechnologies.com/resources/q2-2025-threat-landscape-report/?utm_source=pdi&utm_medium=press-release&utm_campaign=q2-threat-report-2025>
* 3  
  <https://www.brightdefense.com/resources/recent-data-breaches/>
* 9  
  <https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-july-2025>
* 9  
  <https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-july-2025>

#### Works cited

1. Ransomware Attacks Fall in Q2 as Ecosystem Reshuffles - The HIPAA Journal, accessed August 16, 2025, <https://www.hipaajournal.com/ransomware-attacks-fall-q2-2025/>
2. Q2 2025 ransomware trends analysis: Boom and bust, accessed August 16, 2025, <https://securitybrief.co.uk/story/q2-2025-ransomware-trends-analysis-boom-and-bust>
3. List of Recent Data Breaches in 2025 - Bright Defense, accessed August 16, 2025, <https://www.brightdefense.com/resources/recent-data-breaches/>
4. How Google, Adidas, and more were breached in a Salesforce scam - Malwarebytes, accessed August 16, 2025, <https://www.malwarebytes.com/blog/news/2025/08/how-google-adidas-and-more-were-breached-in-a-salesforce-scam>
5. ShinyHunters Targets Salesforce Amid Clues of Scattered Spider Collaboration - ReliaQuest, accessed August 16, 2025, <https://reliaquest.com/blog/threat-spotlight-shinyhunters-data-breach-targets-salesforce-amid-scattered-spider-collaboration/>
6. Scattered Spider Tactics Observed Amid Shift to US Targets - Halcyon, accessed August 16, 2025, <https://www.halcyon.ai/blog/scattered-spider-tactics-observed-amid-shift-to-us-targets>
7. World Leaks Just Leaked 1.3 TB of Files From Its Dell Data Breach - Tech.co, accessed August 16, 2025, <https://tech.co/news/world-leaks-just-leaked-files-dell-data-breach>
8. Dell Confirms Security Breach by Extortion Group, Calls Stolen Data 'Fake', accessed August 16, 2025, <https://www.esecurityplanet.com/security/dell-data-breach-world-leaks-ransomware/>
9. Global Data Breaches and Cyber Attacks in July 2025 - IT ..., accessed August 16, 2025, <https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-july-2025>
10. Qantas Data Breach Puts Six Million Customer Profiles at Risk - Gerrish Legal, accessed August 16, 2025, <https://www.gerrishlegal.com/blog/qantas-data-breach-puts-six-million-customer-profiles-at-risk>
11. Qantas Data Breach Impacts 5.7 Million Customers. Here's What We Know - CNET, accessed August 16, 2025, <https://www.cnet.com/tech/services-and-software/qantas-data-breach-impacts-5-7-million-customers-heres-what-we-know/>
12. UPDATE ON QANTAS CYBER INCIDENT: WEDNESDAY 9 JULY 2025, accessed August 16, 2025, <https://www.qantasnewsroom.com.au/media-releases/update-on-qantas-cyber-incident-wednesday-9-july-2025/>
13. Qantas Breach: Personal Info of 5.7M Customers Compromised - nGuard, accessed August 16, 2025, <https://nguard.com/qantas-breach-personal-info-of-5-7m-customers-compromised/>
14. The Week in Breach News: August 13, 2025 | Kaseya, accessed August 16, 2025, <https://www.kaseya.com/blog/the-week-in-breach-news-08-13-25/>
15. Allianz Life confirms data breach impacts majority of 1.4 million customers, accessed August 16, 2025, <https://www.bleepingcomputer.com/news/security/allianz-life-confirms-data-breach-impacts-majority-of-14-million-customers/>
16. Third-Party Breach Impacts Majority of Allianz Life US Customers - Infosecurity Magazine, accessed August 16, 2025, <https://www.infosecurity-magazine.com/news/third-party-breach-allianz/>
17. Allianz Life data breach affects majority of 1.4 million U.S. customers, insurance company says - CBS News, accessed August 16, 2025, <https://www.cbsnews.com/news/allianz-life-insurance-data-breach/>
18. Hackers hit Dell product demo platform, but impact is limited - The Record, accessed August 16, 2025, <https://therecord.media/hackers-hit-dell-product-demo-platform-limited-impact>
19. Qantas says cyber breach exposed customer data; shares drop 4% - Investing.com, accessed August 16, 2025, <https://www.investing.com/news/stock-market-news/qantas-sayscyber-breach-exposed-customer-data-shares-drop-4-4120252>
20. Qantas Faces Potential $AUD6.6B Fine for Data Breach | IDM Magazine, accessed August 16, 2025, <https://idm.net.au/article/0015231-qantas-faces-potential-aud66b-fine-data-breach>
21. Ransomware and Cyber Extortion in Q2 2025 - ReliaQuest, accessed August 16, 2025, <https://reliaquest.com/blog/ransomware-cyber-extortion-threat-intel-q2-2025/>
22. Scattered Spider and ShinyHunters' Next Move: Leaking Data - Bank Info Security, accessed August 16, 2025, <https://www.bankinfosecurity.com/scattered-spider-shinyhunters-next-move-leaking-data-a-29170>
23. Allianz Life Breach Exposes 1.4 Million Customer Records - Ampcus Cyber, accessed August 16, 2025, <https://www.ampcuscyber.com/shadowopsintel/customer-records-compromised-in-allianz-life-breach/>
24. ShinyHunters' Data Theft Campaign Grows as New Corporate Victims Emerge, accessed August 16, 2025, <https://nationalcioreview.com/articles-insights/extra-bytes/shinyhunters-data-theft-campaign-grows-as-new-corporate-victims-emerge/>
25. Google Among Victims in Ongoing Salesforce Data Theft Campaign - Infosecurity Magazine, accessed August 16, 2025, <https://www.infosecurity-magazine.com/news/google-salesforce-data-theft/>
26. ShinyHunters & Scattered Spider escalate attacks on Salesforce - SecurityBrief Australia, accessed August 16, 2025, <https://securitybrief.com.au/story/shinyhunters-scattered-spider-escalate-attacks-on-salesforce>
27. Allianz Life says majority of 1.4 million US customers' info breached - Malwarebytes, accessed August 16, 2025, <https://www.malwarebytes.com/blog/news/2025/07/allianz-life-says-majority-of-1-4-million-us-customers-info-breached>
28. Scattered Spider: Still Hunting for Victims in 2025 - Silent Push, accessed August 16, 2025, <https://www.silentpush.com/blog/scattered-spider-2025/>
29. Q2 2025 Threat Landscape Report | PDI Security and Network Solutions - Nuspire, accessed August 16, 2025, <https://security.pditechnologies.com/resources/q2-2025-threat-landscape-report/?utm_source=pdi&utm_medium=press-release&utm_campaign=q2-threat-report-2025>
30. Scattered Spider - CISA, accessed August 16, 2025, <https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf>
31. August 2025 Patch Tuesday: One Publicly Disclosed Zero-Day and 13 Critical Vulnerabilities Among 107 CVEs - CrowdStrike, accessed August 16, 2025, <https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-august-2025/>
32. CISA Adds Two Known Exploited Vulnerabilities to Catalog, accessed August 16, 2025, <https://www.cisa.gov/news-events/alerts/2025/08/13/cisa-adds-two-known-exploited-vulnerabilities-catalog>
33. Confidence Scoring in Threat Intelligence | Cyware, accessed August 16, 2025, <https://www.cyware.com/resources/security-guides/cyber-threat-intelligence/what-is-confidence-scoring-in-threat-intelligence>
34. Automated Indicator Sharing (AIS) Scoring Framework Used for Indicator Enrichment - CISA, accessed August 16, 2025, <https://www.cisa.gov/sites/default/files/publications/AIS%2520Scoring%2520Framework%2520Used%2520for%2520Indicator%2520Enrichment%2520V1.0_508.pdf>
35. What is the Chain of Custody in Digital Forensics? - Champlain College Online, accessed August 16, 2025, <https://online.champlain.edu/blog/chain-custody-digital-forensics>
36. Ultimate Guide - Chain Of Custody In Digital Forensics - TechFusion, accessed August 16, 2025, <https://techfusion.com/chain-of-custody-in-digital-forensics/>
37. IBM X-Force OSINT Advisory Google says hackers stole its customers' data by breaching its Salesforce database, accessed August 16, 2025, <https://exchange.xforce.ibmcloud.com/osint/guid:5838492cf88d423c95e9861b4279ad26>
38. Dell Data Breach Exposes Personal Information of 49 Million Customers - Critical Start, accessed August 16, 2025, <https://www.criticalstart.com/resources/dell-data-breach-2024/>
39. List of Data Breaches and Cyber Attacks in Australia 2018-2025, accessed August 16, 2025, <https://www.webberinsurance.com.au/data-breaches-list>
40. Financial Services Could Be Next in Line for ShinyHunters - Infosecurity Magazine, accessed August 16, 2025, <https://www.infosecurity-magazine.com/news/financial-services-next-line/>
41. Tracking Scattered Spider Through Identity Attacks and Token Theft - Picus Security, accessed August 16, 2025, <https://www.picussecurity.com/resource/blog/tracking-scattered-spider-through-identity-attacks-and-token-theft>
42. Q2 2025 Ransomware Research Report - CyberMaxx, accessed August 16, 2025, <https://www.cybermaxx.com/q2-2025-ransomware-research-report/>