



Reporting Window

August 1 to August 31, 2026

Audience

PE Owners, Family Offices, Boards, M&A Teams

Sources

ransomware.live, BlackFog, Breachsense, SEC EDGAR,
CM-Alliance, SharkStriker

M&A CYBER THREAT INTELLIGENCE REPORT

EXECUTIVE SUMMARY

August 2026 was the highest-volume ransomware month of the year: **964 victims posted across ransomware leak sites**, per Breachsense, up 19% from July's 811 and 58% above the 2025 monthly average, with **83 distinct groups active**, up from 66 in July. Qilin held the top spot with 157 claimed victims, trailed by The Gentlemen with 127; five of the ten most active groups were new entrants to that ranking, reflecting rapid churn in the ransomware-as-a-service ecosystem. The defining incident was McKesson: **ShinyHunters claimed roughly 284 million patient records** after breaching third-party applications at the Texas-based pharmaceutical distributor, the largest healthcare-adjacent exposure CyberSweep has tracked in 2026. The Medusa gang separately disclosed a rolling campaign against **500+ critical-infrastructure organizations**, with intrusions dating back to June 2021 only now surfacing. Government, energy, and data-center infrastructure all saw marquee claims: Berlin's Senate network (5.79 TB), a disputed 89 GB claim against Shell, and CyrusOne's 640 GB Salesforce-adjacent breach. Healthcare (91 victims), construction (65), and finance (59) led sector volume, each up double digits month-over-month. For PE and M&A; deal teams, August's headline lesson is **dwell time**: Medusa's multi-year intrusions and McKesson's third-party exposure both show the attacker was often inside long before anyone outside the company knew it.

964	91	284M	5-7x	83
August Attacks (2026 High)	Healthcare Victims (Leading Sector)	McKesson Records Claimed	True Cost vs. Ransom Demand	Active Threat Groups August



DOMINANT THREAT ACTORS

Qilin

#1 in August 2026 — 157 claims

Extended its 2026 lead with 157 claimed victims in August, the highest single-group monthly total CyberSweep has tracked this year. Healthcare, legal, and manufacturing remain primary targets. Phishing and credential theft dominant vectors; double extortion standard.

The Gentlemen

127 claims — construction & real estate

Held second place with 127 victims, sustaining July's momentum. Fortinet VPN exploitation remains the group's signature initial-access vector; construction and real estate saw concentrated targeting in August.

ShinyHunters

McKesson, CyrusOne — 284M+ records

Claimed two of August's largest breaches: McKesson (284M patient records) and CyrusOne (12.9M Salesforce records). Operating under the merged Scattered LAPSUS\$ Hunters banner, the group continues targeting high-visibility brands and third-party SaaS platforms.

Medusa

500+ critical-infrastructure orgs

Surfaced a rolling disclosure of breaches across 500+ healthcare, defense, manufacturing, government, IT, and financial-services organizations, with intrusions dating back to June 2021 — illustrating how long a ransomware actor can hold dormant access before detonation.

CI0p

Shell — disputed 89GB claim

Claimed roughly 89 GB of engineering data from Royal Dutch Shell on August 17; Shell disputes a breach occurred. CI0p's pattern of large-enterprise, supply-chain-adjacent claims continued through August regardless of the dispute's outcome.

Rhysida

Berlin Senate — 5.79TB government data

Claimed 5.79 TB from Berlin's Senate government network, including roughly 46,500 contracts and staff credentials — continuing a 2026 pattern of targeting European government networks for high-sensitivity, low-security-budget data.

SECTOR RISK HEATMAP

SECTOR	THREAT LEVEL	AUG SHARE	DEAL RISK
Healthcare	CRITICAL	91 victims (+20 MoM)	HIPAA, patient-data exfil
Construction	CRITICAL	65 victims (+16 MoM)	Project IP, bid data
Financial Services	CRITICAL	59 victims (+22 MoM)	Regulatory, customer PII
Technology / SaaS	HIGH	58 victims; CyrusOne	Downstream customer exposure
Legal / Accounting	HIGH	43 victims (+17 MoM)	Client-file confidentiality
Government	HIGH	Berlin Senate (5.79TB)	Classified / regulatory exposure
Energy / Industrial	ELEVATED	Shell (disputed)	OT disruption, IP theft
Transportation	ELEVATED	Manchester Airports Grp	Passenger-data exposure

FINANCE SECTOR: 59% SURGE

Breachsense recorded a **59% month-over-month increase** in finance-sector ransomware victims in August 2026, the sector's largest jump of the year to date. The month's clearest financial-sector case was **U.S. Bancorp**: LockBit claimed a data breach on August 21 and threatened a leak by September 4; authenticity remains unconfirmed as of publication. Qilin and The Gentlemen both claimed additional financial-services targets through August. **Investor implication: an unconfirmed claim is not a reason to stand down diligence** — 2026's pattern shows claims frequently precede confirmed, material breaches by weeks, not the reverse.

NOTABLE INCIDENTS | AUGUST 1 TO AUGUST 31, 2026 | 5Ws + HOW

WHO / WHERE	WHAT	WHEN	WHY TARGETED	HOW (VECTOR)	EST. IMPACT
McKesson (Healthcare / Pharma Distribution, US)	ShinyHunters claimed unauthorized access to third-party applications; asserted theft of ~284 million patient records. Scope and authenticity under investigation.	Disclosed mid-August 2026	Major US pharmaceutical distributor; patient data spans practices and payers nationwide — high resale and extortion value.	Third-party application compromise; exact vector not publicly confirmed.	CRITICAL: Largest healthcare-adjacent claim of 2026 to date. HIPAA notification exposure at scale if confirmed. Severe downstream-provider liability.



WHO / WHERE	WHAT	WHEN	WHY TARGETED	HOW (VECTOR)	EST. IMPACT
Medusa Campaign (Critical Infrastructure, Global)	Medusa gang disclosed breaches across 500+ organizations spanning healthcare, defense, manufacturing, government, IT, and financial services, with intrusions dating to June 2021.	Disclosed Aug 2026; since Jun 2021	Multi-sector critical-infrastructure targeting maximizes ransom leverage and cross-sector disruption.	Multi-year dwell time; initial-access vector not disclosed publicly for the full victim set.	CRITICAL: Scale reflects a multi-year campaign, not a single incident. This dwell time means diligence-period breaches can be effectively undetectable without direct threat-intel review.
Shell / Royal Dutch Shell (Energy, Global)	CI0p claimed ~89 GB of engineering drawings, facility reports, photos, and project plans.	Reported August 17, 2026	Major energy operator; engineering and facility data carries both competitive and safety-sensitive value.	Not confirmed; CI0p's typical pattern favors edge-device and file-transfer exploitation.	HIGH: Shell disputes a breach occurred. Authenticity and scope unconfirmed; OT/engineering data claims warrant diligence regardless of dispute outcome.
Berlin Senate Network (Government, Germany)	Rhysida claimed 5.79 TB of data including ~46,500 contracts, emails, passwords, phone numbers, and other classified records.	Late August 2026	Central government network; classified and administrative data carries diplomatic and regulatory sensitivity.	Not publicly confirmed; Rhysida typically favors phishing and exposed remote-access services.	HIGH: Large-scale government data exposure. Regulatory and diplomatic sensitivity; credential exposure creates follow-on intrusion risk.
CyrusOne (Data Center / Tech, US)	ShinyHunters claimed 640 GB of data including ~12.9 million Salesforce records.	August 2026	Data-center operator hosting infrastructure for many enterprise customers; third-party CRM exposure multiplies downstream risk.	Third-party CRM (Salesforce-linked) compromise; direct vector not confirmed.	HIGH: Downstream exposure for every enterprise customer whose data transited CyrusOne-hosted or -linked infrastructure. Supply-chain multiplier consistent with 2025-26 SaaS breaches.
Manchester Airports Group (Transportation, UK)	FulcrumSec claimed ~86 GB of data including ~200,000 records tied to upcoming traveler itineraries.	August 2026	Operator of Manchester, Stansted, and East Midlands airports; traveler and operational data is high-sensitivity, high-disruption-potential.	Not publicly confirmed.	HIGH: Passenger-privacy exposure at a critical transport-sector target. Operational disruption risk at three major UK airports.
Fidelity Services Group (Private Security, South Africa)	Ransomhouse compromised systems and stole data after a failed extortion attempt; data leaked despite company denial of customer-data exposure.	Disclosed August 7, 2026	South Africa's largest private security company; operational and client-contract data has resale and reputational value.	Not publicly confirmed; extortion attempt preceded the data leak.	ELEVATED: Company isolated affected systems and disputes customer-data exposure. Data was leaked publicly regardless, creating reputational exposure irrespective of the dispute.
McDonald's Corporation (Consumer / Retail, US)	TheHatman claimed an Azure-infrastructure attack yielding ~1.7 million records, including employee contact information.	Jul 31 – Aug 16, 2026	High-visibility consumer brand; employee HR data valuable for follow-on phishing and identity fraud.	Cloud (Azure) infrastructure compromise; specific technique not publicly disclosed.	ELEVATED: Continued targeting of cloud-hosted HR/identity infrastructure at large consumer brands. Employee, not customer, data primarily affected.

INTELLIGENCE SPOTLIGHT | TRENDS THAT MOVE DEAL VALUATIONS

① McKesson: Healthcare's Largest 2026 Claim

ShinyHunters' 284-million-record claim against McKesson, if confirmed at anything close to that scale, would be the largest healthcare-adjacent exposure CyberSweep has tracked this year, eclipsing even May's Canvas/Instructure breach. Third-party application compromise — not McKesson's core systems — appears to be the entry point, consistent with 2026's dominant healthcare pattern of vendor-adjacent rather than direct intrusion. **Investor implication: healthcare and pharma distribution targets need a documented map of every third-party application with patient-data access, not just their own perimeter.**

③ Shell / ClOp: When a Claim Is Disputed

ClOp's claim against Shell was met with an outright company denial — a reminder that leak-site claims are marketing for the attacker as much as evidence of compromise. Scope and authenticity remain unresolved as of publication. **Investor implication: an disputed claim against a target or counterparty still belongs in the diligence file; unresolved claims frequently resolve toward partial confirmation in the following reporting cycle.**

⑤ Finance's 59% Surge

Financial-services ransomware victims rose 59% month-over-month in August, the sharpest sector acceleration of the year to date. LockBit's unconfirmed U.S. Bancorp claim sits inside a broader pattern of Qilin and The Gentlemen also expanding into financial targets. **Investor implication: every financial-services LOI signed after August 2026 warrants a pre-close credential-exposure audit as standard diligence, not an optional add-on.**

② Medusa's Multi-Year Dwell Time

Medusa's disclosure of intrusions dating to June 2021 across 500+ organizations is the starkest dwell-time data point CyberSweep has seen in 2026. A target could pass every point-in-time security questionnaire during diligence while still hosting a four-year-old dormant compromise. **Investor implication: pre-LOI screening should include dark-web and leak-site historical search, not just current posture — a clean scan today does not rule out a legacy intrusion.**

④ CyrusOne: The Third-Party CRM Multiplier

CyrusOne's 640 GB claim, anchored by 12.9 million Salesforce-linked records, illustrates how a breach at infrastructure and SaaS providers cascades to every downstream customer simultaneously. This is the same pattern that made May's Canvas/Instructure breach reach 8,800+ institutions. **Investor implication: technology diligence must map a target's CRM and data-center dependencies as attack surface, not just its own codebase.**

⑥ Berlin Senate: Government Networks as Soft Targets

Rhysida's 5.79 TB claim against Berlin's Senate network continues 2026's pattern of European government and municipal targets absorbing large, sensitive breaches despite comparatively modest security budgets. **Investor implication: portfolio companies with material government-contract exposure should treat counterparty government-network security as a supply-chain risk, not someone else's problem.**

DEAL TEAM ACTION FRAMEWORK | WHAT SOPHISTICATED CAPITAL DOES DIFFERENTLY

DEAL STAGE	CYBERSWEEP ACTION	WHAT IT PREVENTS	FINANCIAL BENEFIT
Pre-LOI Screening	QuickSweep: dark web broker check, SEC EDGAR 8-K cross-reference, Nutanix and OT patch verification	Bidding on a company with active attacker access or pending SEC disclosure obligation (Fairlife model)	Walk-away clarity before capital at risk; avoids inherited production shutdown
LOI / QofE Stage	DeepSweep: full posture assessment plus subsidiary sweep plus outside counsel security review	Cross-border subsidiary breach (Aflac Japan model); law firm client file exposure (WilmerHale model)	Renegotiate price; structure escrow; right-size R&W; insurance across all entities
Pre-Close / Integration	TotalSweep: OT/IT gap, AI vendor dependency map, pen test, wiper-mode resilience verification	Post-close wiper attack destroying production (Fairlife/Romania model); AI supply-chain breach	Clean close; no post-close 8-K surprise; lower insurance premiums
Post-Close Portfolio	Continuous monitoring via CyberSweep monthly threat intel brief plus dark web credential alerts	Silent hold-period breach with multi-year dwell time (Medusa model) destroying exit valuation	Protects EBITDA; maintains exit multiple; satisfies LP reporting obligations



The most expensive breach is the one you discover after closing.

CyberSweep transforms cyber risk into financial intelligence your deal team can act on before money changes hands.

Avg Hidden Liability Surfaced: **\$6M+** | Avg Deal Value at Risk: **\$400M+**

Schedule a consultation: info@cybersweep.io | www.cybersweep.io | (303) 900-2664