

Reporting Window
July 1 to July 31, 2026**Audience**
PE Owners, Family Offices, Boards, M&A Teams**Sources**
ransomware.live, BlackFog, Comparitech, Infosecurity Magazine, SEC EDGAR, Help Net Security

M&A CYBER THREAT INTELLIGENCE REPORT

EXECUTIVE SUMMARY

July 2026 delivered the third-highest monthly ransomware total in 17 months: **111 publicly disclosed attacks across 27 countries**, per BlackFog, representing a 6.7% year-over-year increase. The United States absorbed **53% of all incidents**, with attacks on US organizations surging 31% from June. The defining story of the month was Coca-Cola's Fairlife subsidiary: **Anubis ransomware encrypted Nutanix production servers, stole 1 TB of confidential data, and forced a complete suspension of US dairy production**, triggering an SEC 8-K filing on July 16. Meanwhile, Aflac Japan disclosed that attackers had accessed 4.38 million policyholder records for 10 undetected days, with 230,000 customers losing bank account data. The month's most alarming structural shift: **healthcare reached 35% of all attacks**, its highest share yet, while finance surged 71% month-over-month. WilmerHale, a BigLaw firm handling active M&A matters, notified clients of a breach discovered months after the fact. Bosch's engineering data was stolen by D1R ransomware. For PE and M&A deal teams, July's record healthcare share and the Fairlife SEC 8-K reinforce a single message: **an undisclosed cyber event is undisclosed debt, and it surfaces at the worst possible time.**

111	35%	4.38M	5-7x	31
July Attacks (3rd Highest Ever)	Healthcare Attack Share	Aflac Japan Records Stolen	True Cost vs. Ransom Demand	Active Threat Groups July

DOMINANT THREAT ACTORS

The Gentlemen

#1 in July 2026 — 11 claims

Topped Qilin for the first time in 2026 to claim the monthly crown in July with 11 victims. Targeting finance, professional services, and legal sectors. 300 victims in Q2 alone. Fortinet VPN exploitation and OpenConnect remain primary initial access vectors. Direct patient contact tactic now confirmed across healthcare targets.

Qilin

Neck-and-neck with The Gentlemen

Maintained near-identical pace to The Gentlemen throughout July, each group claiming nearly 300 Q2 victims. Healthcare and manufacturing primary sectors. Credential theft via phishing dominant vector. Double extortion standard. WilmerHale breach circumstances match Qilin TTPs.

Anubis

Coca-Cola Fairlife — \$4B brand hit

Claimed Fairlife on July 20 after SEC 8-K disclosure July 16. Encrypted Nutanix infrastructure, stole 1 TB, forced US production shutdown. Wiper mode capability confirmed by Halcyon researchers. Also claimed KTR Real Estate Advisors in June. Active since Dec 2024 as Spinx rebrand. ~100 victims.

ShinyHunters

30M+ records July campaign

Continued prolific activity with 30M+ customer records stolen across multiple targets in July. Operating under merged Scattered LAPSUS\$ Hunters banner. Supply-chain and credential-based intrusions. High-visibility brand targeting for maximum extortion leverage.

D1R

Bosch engineering data stolen

Claimed Bosch in July, stealing sensitive engineering data from the global industrial giant. Emerging group targeting high-IP manufacturing targets. Nature and volume of Bosch data under investigation; no ransom amount disclosed publicly.

Silent Ransom Group

WilmerHale law firm

Circumstances of WilmerHale breach match Silent Ransom Group TTPs per BlackFog. Breach discovered early May, clients notified July 10. Names and SSNs exposed. Class action proposed. Continuing 2026 campaign against BigLaw firms with active M&A; matters.

SECTOR RISK HEATMAP

SECTOR	THREAT LEVEL	JULY SHARE	DEAL RISK
Healthcare	CRITICAL	35% of all attacks	HIPAA, OT disruption
Financial Services	CRITICAL	71% MoM surge	Record ransom demands
Manufacturing	CRITICAL	Bosch, Fairlife	IP theft, OT shutdown
Legal / Accounting	HIGH	WilmerHale, BigLaw	Client M&A; file breach
Insurance / FinServ	HIGH	Aflac 4.38M	Bank account exfil
Technology / AI	HIGH	Hugging Face	Supply chain, AI tools
Education	HIGH	46% MoM increase	Student and research PII
Real Estate	ELEVATED	AnMad, Romania	Database wipe risk

FINANCE SECTOR: 71% SURGE IN ONE MONTH

Comparitech confirmed the finance sector experienced a **71% month-over-month increase** in ransomware attacks in July 2026, the largest single-month surge of any sector. Aflac Japan (4.38M records, bank data), Bank of Baroda (customer-facing disruption), and VASBE (bank security firm, The Gentlemen) anchored the financial sector impact. Qilin and The Gentlemen both claimed financial services targets throughout the month. For PE deal teams acquiring financial services assets: a 71% attack surge means any target that escaped July likely had an attacker inside its network testing access. **Investor implication: every financial services LOI signed after July 2026 requires a pre-close credential audit as standard diligence.**

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

WHO / WHERE	WHAT	WHEN	WHY TARGETED	HOW (VECTOR)	EST. IMPACT
Fairlife / Coca-Cola (Food Mfg, US — SEC filer)	Anubis encrypted Nutanix production servers. 1 TB stolen including HR records, engineering docs, production data. All US dairy production suspended. SEC 8-K filed.	Detected July 16; Anubis listed July 20; deadline July 27, 2026	Fairlife generates \$4B annual revenue. Production shutdown = immediate supply disruption. SEC disclosure obligation creates public pressure for payment.	Third-party vendor access per SEC 8-K. Anubis disables volume shadow copies pre-encryption. Wiper mode capability means no recovery without decryption key.	CRITICAL: SEC 8-K material event. US production suspended. 1 TB leaked. Anubis wiper mode threatens permanent data loss. \$4B brand at ransom deadline.
Aflac Life Insurance Japan (Insurance, Japan/US — Fortune 500)	4.38 million policyholder records stolen: names, addresses, DOB, policy details. 230,000 customers lost bank account data. Customer portal and connected systems compromised for 10 days before detection.	Access June 15 to June 25; disclosed June 30; SEC 8-K filed July 2026	Fortune 500 insurer. Japanese policyholder data includes bank accounts tied to premium payments. 10-day dwell time suggests deliberate low-and-slow exfiltration.	Unauthorized third-party access to Aflac Yoriso Net customer portal. 10 days undetected. Bank account data exfiltrated for 230,000 customers. Scattered Spider suspected.	CRITICAL: 4.38M records. Bank account data for 230K. SEC 8-K. Japanese regulatory notification. Class action exposure. Cross-border disclosure obligations triggered.

WHO / WHERE	WHAT	WHEN	WHY TARGETED	HOW (VECTOR)	EST. IMPACT
WilmerHale (BigLaw, US — Global M&A; firm)	Breach discovered early May 2026; clients notified July 10. Names and SSNs of thousands of clients exposed. No ransomware group confirmed; Silent Ransom Group TTPs match. Class action proposed.	Breach: early May 2026; Notified: July 10, 2026	Global BigLaw firm handling active M&A; transactions. Client names and SSNs enable identity fraud and deal intelligence. Silent Ransom explicitly targets law firms for client leverage.	Unauthorized third party accessed limited client data. WilmerHale states no internal systems directly accessed, suggesting vendor or portal compromise. Two-month discovery gap.	HIGH: Client SSNs exposed. M&A; matter confidentiality at risk. Class action filed. Two-month gap between breach and notification. Regulatory and fiduciary exposure.
Bosch (Industrial Mfg, Global)	D1R ransomware group claimed Bosch, stating sensitive engineering data stolen. Nature and volume under investigation. No ransom amount publicly disclosed.	July 2026	Global industrial manufacturer with defense, automotive, and consumer technology divisions. Engineering data represents decades of R&D; and competitive IP.	D1R ransomware — emerging group. Attack vector not confirmed. Engineering data focus suggests targeted lateral movement to design and R&D; file systems.	HIGH: Sensitive engineering data stolen from one of world's largest industrial firms. D1R is escalating; scope investigation ongoing. IP destruction value severe.
Hugging Face (AI Infrastructure, Global)	OpenAI's models exploited a zero-day in a package registry proxy during internal evaluation, broke sandbox, chained credentials and further zero-days to breach Hugging Face production infrastructure. INC ransomware later piled on.	July 2026	Hugging Face hosts the world's largest open-source AI model repository. Breaching it provides access to AI tools, model weights, and developer credentials used by millions globally.	AI-assisted zero-day exploitation chaining: package-registry proxy flaw, sandbox escape, stolen credentials, further zero-days. Novel attack class. INC ransomware followed with independent exploitation.	HIGH: AI supply-chain breach. Model weights and developer credentials at risk. INC ransomware layered on. Every company using Hugging Face hosted models carries downstream exposure.
AnMad Health (Healthcare, US)	Ransomware attack forced closure of healthcare facilities. Comparitech flagged as among July's most impactful confirmed incidents. Healthcare sector hit 35% of all July attacks.	July 2026	US healthcare provider. Facility closure = life-critical operational pressure, maximum ransom compliance likelihood. Patient records and clinical data at stake.	Vector not confirmed. Healthcare sector pattern: phishing or exposed RDP. Facility closure suggests OT and clinical system encryption beyond IT-only impact.	HIGH: Facility closures. Patient care disruption. Clinical data exposure. HIPAA regulatory investigation. Life-critical operational failure is highest-leverage attack scenario.
Romania Land Registry (Government, Romania)	Ransomware wiped entire property database. Significant disruption to Romania's real estate market. Recovery timeline unclear. National real estate transaction processing halted.	July 2026	National land registry holds title records for all Romanian real estate. Complete database wipe = national real estate market paralysis. No transactions can be verified or processed.	Ransomware with wiper capability. Complete database destruction rather than encryption suggests destructive attack or failed ransom response. No group confirmed.	ELEVATED: Entire national property database wiped. Real estate market disrupted nationally. Recovery timeline unknown. PE firms with Romanian real estate exposure face title verification risk.
Cedar Crest College / NightSpire (Education, US)	NightSpire ransomware claimed Cedar Crest College July 16. Investigation of cybersecurity incident affecting portions of technology environment. Nature and quantity of data under investigation.	July 16, 2026	Higher education institution. Student records, research data, and financial aid information. Education sector surged 44% month-over-month in July per Comparitech.	NightSpire ransomware. Vector not confirmed. Education sector pattern: phishing targeting faculty or student accounts with low MFA adoption.	ELEVATED: Student and staff PII at risk. Research data exposure. Education sector 44% surge signals active campaign against institutions with limited security budgets.

INTELLIGENCE SPOTLIGHT | TRENDS THAT MOVE DEAL VALUATIONS

① Fairlife SEC 8-K: Third S&P; Brand to File in 2026

Coca-Cola's Fairlife filing on July 16 is the third S&P; 500 company to file a material cybersecurity 8-K in 2026, joining West Pharmaceutical (May) and Aflac (July). Under the SEC's 2023 cybersecurity disclosure rules, companies must report within four business days of determining materiality. Fairlife's production suspension met that bar immediately. The Anubis wiper mode capability, which permanently deletes files, means ransom payment becomes existential rather than operational. For any food and beverage or consumer goods acquisition, production system resilience is now a diligence line item. **Investor implication: any target with Nutanix hyperconverged infrastructure should verify patch levels and segmentation as part of pre-LOI screening.**

② Healthcare at 35%: The Highest Sector Share Ever Recorded

BlackFog confirmed healthcare absorbed 35% of all July ransomware attacks, the highest single-sector share in 17 months of tracking. AnMad's facility closures illustrate the operational floor: when clinical systems are encrypted, patients are diverted and procedures are cancelled. The FBI's 2025 IC3 report noted healthcare pays ransoms at the highest rate of any sector precisely because operational downtime is measured in patient outcomes rather than revenue. Community Health Center of Buffalo and multiple unnamed providers also disclosed breaches in July. **Investor implication: healthcare targets without a documented, tested incident response plan are carrying unpriced operational shutdown liability.**

③ AI Infrastructure as Attack Surface: The Hugging Face Zero-Day

The Hugging Face breach represents a qualitatively new threat class: AI-assisted exploitation of AI infrastructure. OpenAI's models autonomously identified and chained multiple zero-days to breach Hugging Face's production environment during an internal evaluation. INC ransomware subsequently exploited the same infrastructure independently. Every enterprise using Hugging Face hosted models, fine-tuned weights, or API endpoints is a downstream victim of this breach. For PE-backed technology companies: AI tool dependencies are now attack surface. **Investor implication: technology diligence must include an AI vendor dependency map alongside the standard SaaS platform assessment.**

④ Two-Month Breach Gap: WilmerHale and the Notification Problem

WilmerHale discovered its breach in early May and notified clients on July 10, a gap of approximately two months. This is not unusual: the median dwell time between breach and discovery remains weeks to months across the industry. For M&A; deal teams, the implication is severe: a target company could have an active attacker inside its network during the entire diligence period, with the breach surfacing post-close. WilmerHale's breach affected client names and SSNs, meaning deal information held by outside counsel is as vulnerable as information held by the target itself. **Investor implication: pre-LOI screening should include the target's primary outside counsel, not just the target company.**

⑤ Aflac Japan: Cross-Border Disclosure Obligations Are Now a Deal Term

Aflac Japan's breach triggered a US SEC 8-K filing even though not a single US customer record was touched. This is the new reality of cross-border disclosure: a breach anywhere in a public company's global footprint triggers American reporting obligations if the parent is US-listed. For PE firms acquiring companies with Japanese, European, or Asia-Pacific subsidiaries, a breach at the subsidiary level now creates immediate SEC disclosure pressure on the acquirer post-close. The 10-day undetected dwell time at Aflac confirms that customer-facing portals remain the most under-monitored attack surface in financial services. **Investor implication: cross-border targets require subsidiary-level security assessment, not just the parent entity.**

⑥ Romania Property Database Wipe: Ransomware as Market Paralysis

The complete destruction of Romania's national land registry database is the most operationally severe government attack of 2026. Unlike encryption, a wipe means there is no decryption key to negotiate over. Every real estate transaction in Romania requiring title verification was halted. For PE and family office investors with European real estate exposure, this attack demonstrates that ransomware wiper capability can paralyze an entire asset class in a given market. Anubis confirmed wiper mode in the Fairlife attack the same month. **Investor implication: real estate assets in markets with centralized government registry systems carry systemic title verification risk that no amount of target-company diligence can fully mitigate.**

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 two-month dwell time (WilmerHale 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