Reporting Window
April 28 – May 28, 2026

Audience
PE Owners · Family Offices · Boards · M&A Teams

Data Sources
Ransomware.live · BlackFog · PurpleOps · BleepingComputer · SEC Filings

M&A CYBER THREAT INTELLIGENCE REPORT

■ EXECUTIVE SUMMARY

The 30-day period ending May 28, 2026 delivered the highest single-month ransomware count since tracking began—**105 publicly disclosed attacks in April alone**, per BlackFog, with May threatening to surpass that mark. Healthcare reclaimed the #1 most-targeted sector with **25 confirmed attacks**, while construction, manufacturing, and financial technology absorbed some of the period's most financially consequential hits. The defining story of this window is scale and supply-chain amplification: **ShinyHunters** (now operating under the merged Scattered LAPSUS$ Hunters banner) compromised Instructure's Canvas LMS, breaching **275 million records across 8,800+ institutions**—one intrusion, planetary downstream impact. Simultaneously, **Everest** targeted Fiserv and TSYS—two pillars of global payment infrastructure—while **INC Ransom** escalated across professional services and manufacturing. West Pharmaceutical's SEC 8-K filing confirmed what deal teams often discover post-close: ransomware is now a **material, board-level, disclosure-worthy financial event**. The U.S. remains the primary target at **60% of global incidents**. For PE and M&A teams, any target operating in healthcare, pharma manufacturing, fintech, or legal services without documented, tested security controls carries an unpriced liability on the balance sheet.

105	275M	60%	5–7×	32
April Attacks (Record High)	Records Exposed Canvas/Instructure	US Share of Global Incidents	True Cost vs. Ransom Demand	Active Threat Groups in April

 © 2026 CyberSweep Inc. All rights reserved.

■ DOMINANT THREAT ACTORS

ShinyHunters (Scattered LAPSUS$ Hunters)

Most active Apr 2026 — 15 claims

Merged with Scattered Spider & Lapsus$. Exploited Instructure Canvas XSS flaw: 275M records, 3.65TB. Also hit Medtronic (9M+ records), 7-Eleven, Pitney Bowes, McGraw Hill, Odido, Carnival. Supply-chain multiplier model.

Qilin

Dominant volume; ~50% of May daily claims

Targeted Mayer LLP (May 13), Denso auto-parts (Italy/Morocco ops), Foxstone Financial, Johnson Carter Architects, Australian retailer Bluize. Credential theft + RDP primary vectors. Still #1 by victim count in 2026.

Everest

Critical financial infra focus

Listed Fiserv (May 3) — global payment processing, core banking, Clover POS. Listed TSYS (May 2) — US payment solutions. Russian-speaking group; data theft + extortion without encryption. Systemic downstream risk to every bank using these platforms.

INC Ransom

Professional services escalation

Hit Silergy Corp (450GB+ stolen: financial docs, PII). Active across manufacturing and professional services globally. Strong encryption + exfiltration combo. Growing US healthcare presence.

Akira

Financial advisory targeting

Claimed Moorman Harting (May 6): 21GB — client files, NDAs, passports, financial records, payroll. Classic wealthcare/PE-adjacent target. Also hit Shingle & Gibb Automation (industrial distributor, 25GB exfiltrated).

The Gentlemen

RaaS escalation — 182 Q1 victims

Hit JRK Property Holdings (111k individuals; SSNs; class action filed). Hit Gem Terminal Industry (electronics mfr; shares dropped 3%). Fastest-growing RaaS group since Conti. Fortinet edge gear + OpenConnect VPN initial access.

■ SECTOR RISK HEATMAP

SECTOR	THREAT LEVEL	SHARE	DEAL RISK
Healthcare	■ CRITICAL	25 Apr attacks	HIPAA + op disruption
Pharma Mfg	■ CRITICAL	SEC-reportable	Supply chain + IP theft
Financial Tech	■ CRITICAL	Systemic risk	Cascading bank exposure
Professional Svcs (Legal/Accounting)	■ HIGH	Top 3 US sector	Client file exfiltration
Construction	■ HIGH	#1 US sector	Contract + lien data
Manufacturing	■ HIGH	~20% globally	OT/IT boundary exposure
Education/SaaS	■ HIGH	Record breaches	Supply-chain multiplier
Real Estate	■ ELEVATED	Class actions filed	PII + SSN exposure

■ SEC 8-K: RANSOMWARE IS NOW MATERIAL DISCLOSURE

West Pharmaceutical Services filed an SEC **8-K on May 7** disclosing a material ransomware attack — only the third S&P 500 company in 2026 to do so. Intrusion detected May 4; global systems taken offline; Unit 42 engaged. The filing stated data was **exfiltrated and systems encrypted**, disrupting manufacturing and shipping globally. For M&A deal teams: the SEC's 2023 cybersecurity disclosure rules now require public companies to report material incidents within 4 business days. **A target that experienced a breach and didn't file may have a securities law problem on top of the operational one.** CyberSweep's pre-LOI scan checks dark web broker markets and SEC EDGAR simultaneously.

■ NOTABLE INCIDENTS — APRIL 28 TO MAY 28, 2026 | 5Ws + HOW

WHO / WHERE	WHAT	WHEN	WHY TARGETED	HOW (VECTOR)	EST. IMPACT
West Pharmaceutical Svcs (Pharma Mfg, US — S&P; 500)	Data exfiltrated + global systems encrypted; manufacturing/shipping disrupted worldwide; SEC 8-K filed as material event	Detected May 4; disclosed May 7, 2026	S&P; 500 pharma mfr; injectable drug packaging = life-critical supply chain; high ransom leverage	Unknown vector; Unit 42 (Palo Alto) engaged; language in SEC filing implies ransom negotiation initiated	**CRITICAL — Global ops disruption; SEC material event; $3B+ revenue company; supply chain risk to pharma sector**
Instructure / Canvas LMS (EdTech SaaS, Global)	275M records stolen across 8,800+ institutions (Duke, Harvard, Penn, Wisconsin); 3.65TB exfiltrated; login pages defaced May 7; ransom paid	May 1 disclosed; May 7 escalation; May 12 deadline; agreement reached	Largest LMS platform globally; single breach = 275M downstream victims; Salesforce instance also breached	XSS flaw in Free-for-Teacher support-ticket flow; session hijacking; admin credential theft; lateral pivot to Salesforce	**CRITICAL — 275M PII records; FBI PSA issued; Free-for-Teacher shutdown; ransom paid (undisclosed sum)**
Fiserv (FinTech Infrastructure, US)	Everest posted Fiserv to leak site; data theft claimed; no confirmed encryption; ransom negotiation ongoing as of report date	Listed May 3, 2026	Processes payments for 10,000+ financial institutions; core banking + Clover POS = maximum systemic leverage	Everest's typical vector: credential theft via third-party vendor access; data theft without encryption	**CRITICAL — Every bank/FI using Fiserv APIs is at downstream risk; Fiserv has not confirmed or denied scope**
TSYS / Total System Services (Payments, US)	Everest listed TSYS one day after Fiserv; double-targeting of payment infrastructure suggests coordinated campaign against US FinTech sector	Listed May 2, 2026	Major payment processor; card issuer processing at scale; companion attack to Fiserv hit	Same Everest TTP as Fiserv — data exfiltration focus; no encryption confirmed	**HIGH — Card-issuer and payment network data; cascading downstream bank exposure**

 © 2026 CyberSweep Inc. All rights reserved.

WHO / WHERE	WHAT	WHEN	WHY TARGETED	HOW (VECTOR)	EST. IMPACT
Medtronic (Medical Devices, Global)	ShinyHunters claimed 9M+ PII records + terabytes of corporate data; Medtronic confirmed unauthorized access; listing later removed (possible settlement)	April 2026 (disclosed during period)	Global medical device maker; 9M+ patient/employee records = HIPAA exposure at scale; corporate IP value	ShinyHunters credential-based intrusion; lateral movement to corporate IT; separate from product networks	**HIGH — 9M records; HIPAA regulatory exposure; listing removal suggests quiet settlement; ongoing investigation**
Jones Day (Global Law Firm, US/Global)	Silent Ransom Group phishing attack; older files from ~10 clients accessed and posted; $13M ransom demand with threat to leak all data	April 6, 2026 confirmed	Global BigLaw firm; M&A; deal files, litigation memos, client financials — maximum confidentiality value	Spear-phishing; targeted email access; exfiltration of client-matter files before detection	**HIGH — $13M demand; 10 clients notified; reputational damage; deal confidentiality risk for any active M&A; matters**
Moorman Harting (Wealthcare/Financi al Advisory, US)	Akira claimed 21GB: client financial records, NDAs, passports, payroll, government IDs, contracts — full dossier on wealthy clients	May 6, 2026	Wealthcare firm = HNW client files, retirement plans, tax records; small security footprint vs. data value	Akira typical: phishing or exposed VPN/RDP; no EDR; rapid lateral movement to file servers	**HIGH — NDAs and client financials leaked; identity theft risk for HNW individuals; regulatory exposure**
JRK Property Holdings (Real Estate Investment, US)	The Gentlemen claimed attack; 111,000 individuals notified; SSNs and names exposed; class action lawsuit filed	Early April 2026	Real estate investment firm; tenant/investor PII at scale; litigation magnet post-breach	The Gentlemen's standard vector: Fortinet edge gear exploitation or OpenConnect VPN compromise	**HIGH — Class action filed; SSN exposure for 111k; identity theft liability; deal-time PII = CCPA/state law risk**

■ INTELLIGENCE SPOTLIGHT — TRENDS THAT MOVE DEAL VALUATIONS

① Record April: 105 Attacks, 22 Countries — A New Baseline

BlackFog confirmed April 2026 as the **highest single-month attack count since tracking began**, with 105 publicly disclosed incidents across 22 countries. The U.S. absorbed 60% of all attacks. Healthcare led at 25 incidents, followed by services (16) and government (16). Critically, public disclosures represent only a fraction of total compromise activity — BlackFog estimates the true ratio is **6:1 undisclosed to disclosed**. **Investor implication:** Any portfolio company in the top-5 sectors without continuous monitoring carries statistically near-certain exposure that simply hasn't surfaced yet.

② Supply-Chain Amplification: One Breach, 275 Million Victims

ShinyHunters' Instructure attack is the defining supply-chain event of 2026 so far. A single XSS flaw in a free-tier support flow gave attackers access to **275 million records spanning 8,800+ institutions worldwide**, including Salesforce environment credentials. The FBI issued a PSA warning of follow-on extortion. Instructure confirmed a ransom payment. The same group also hit Medtronic, 7-Eleven, McGraw Hill, and Carnival within the same window. **Investor implication:** Any target using shared SaaS platforms (LMS, ERP, CRM, POS) must have those vendor relationships assessed — not just the core company.

③ FinTech Infrastructure Under Coordinated Attack

Everest listed both Fiserv and TSYS within 24 hours in early May — a coordinated strike against two of the most critical US payment-processing platforms. **Fiserv alone serves 10,000+ financial institutions** with core banking, digital banking, and the Clover POS ecosystem. Neither company has confirmed scope, but the downstream exposure for every bank, credit union, and retailer using these platforms is systemic. PurpleOps confirmed the Fiserv attack represents 'persistent pressure on critical financial infrastructure.' **Investor implication:** Financial services targets must disclose all third-party fintech vendor relationships during diligence. A breach at a vendor is a breach at the portfolio company.

④ Legal Sector: Law Firms Are the New Ransomware Battleground

Jones Day ($13M demand; Silent Ransom), Mayer LLP (Qilin; May 13), Orrick Herrington (Silent Ransom), and multiple unnamed firms were hit in this 30-day window. Law firms hold the most deal-sensitive data in any M&A transaction: NDAs, LOIs, purchase agreements, litigation files, and client financial records. A breach of outside counsel during a live deal is a **direct material event for the transaction itself**. DataBreaches.net noted the Silent Ransom Group is explicitly targeting law firms as a strategy to extract leverage against their clients. **Investor implication:** Include outside counsel in cyber diligence scope on every active deal above $50M.

⑤ The SEC 8-K Signal: Ransomware Is a Board-Level Disclosure Event

West Pharmaceutical's May 7 SEC 8-K is a landmark data point. Under the SEC's 2023 cybersecurity disclosure rules, public companies must report material incidents within **4 business days**. West filed on time, disclosing data exfiltration AND system encryption — both triggers. The language 'steps intended to mitigate the risk of dissemination' is broadly interpreted as code for ransom negotiation. For deal teams acquiring public companies or targets with future IPO intent: **an undisclosed breach that should have been an 8-K is a securities law violation layered on top of an operational one.** CyberSweep's DeepSweep includes SEC EDGAR cross-check as standard.

⑥ Wealthcare & Real Estate: PE-Adjacent Targets Rising Fast

Moorman Harting (Akira; 21GB of HNW client files) and JRK Property Holdings (The Gentlemen; 111k SSNs; class action filed) represent a rising pattern: **PE-adjacent professional services firms** — wealth managers, real estate operators, financial advisors — are being systematically targeted because they hold concentrated, high-value client data with typically thin security postures. These firms often appear in PE roll-up strategies as add-on acquisitions. A class action for a real estate manager exposes the GP to downstream liability. **Investor implication:** Add-on acquisitions carry full inherited liability — diligence must extend to these targets regardless of deal size.

■ DEAL TEAM ACTION FRAMEWORK — WHAT SOPHISTICATED CAPITAL DOES DIFFERENTLY

 © 2026 CyberSweep Inc. All rights reserved.

DEAL STAGE	CYBERSWEEP ACTION	WHAT IT PREVENTS	FINANCIAL BENEFIT
Pre-LOI Screening	QuickSweep: dark web broker check + SEC EDGAR cross-reference + external attack surface	Bidding on a company already breached or in ransom negotiation; 8-K non-disclosure liability	Avoids inherited breach; walk-away clarity before capital at risk
LOI / QofE Stage	DeepSweep: full security posture + third-party vendor map + dollar-risk quantification	Hidden cyber debt in EBITDA; SaaS vendor supply-chain exposure (Fiserv/Instructure model)	Renegotiate price; structure escrow; right-size R&W; insurance
Pre-Close / Integration	TotalSweep: OT/IT gap + pen test + legal/outside counsel vendor sweep	Post-close breach; law firm data exposure during active deal; rep & warranty disputes	Clean close; lower insurance premiums; no post-close surprise 8-Ks
Post-Close Portfolio	Continuous monitoring via CyberSweep weekly threat-intel brief + dark web alerts	Silent hold-period breach destroying exit valuation; pre-exit disclosure obligations	Protects EBITDA; maintains exit multiple; satisfies LP reporting obligations

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

CyberSweep translates hidden cyber risk into dollar figures your deal team can act on — before money changes hands.

Average Risk Identified: **$10M+** | Average Deal Value Protected: **$5M+**

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

 © 2026 CyberSweep Inc. All rights reserved.