**Reporting Window**
March 28 – April 27, 2026

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

**Data Source**
Ransomware.live · BlackFog · ZeroFox · FBI IC3 · CSIS

# M&A CYBER THREAT INTELLIGENCE REPORT

## ■ EXECUTIVE SUMMARY

The final 30 days of March–April 2026 confirmed what sophisticated capital already suspects: ransomware is no longer an IT nuisance—it is a **valuation event**. Ransomware.live and corroborating intelligence feeds tracked **2,318 confirmed incidents globally in Q1 2026** across 70 active threat groups. Manufacturing absorbed nearly **one in five attacks**; healthcare, professional services (legal/accounting), construction, and financial services rounded out the top five—exactly the sectors that fill PE and family-office portfolios. Double-extortion (encrypt + exfiltrate) now defines **77% of all intrusions**, meaning ransom payment does not end exposure. The United States remained the primary target at **64.7% of all recorded victims**, with Germany in second place. For deal teams, the lesson is clear: an undisclosed breach is undisclosed debt.

| 2,318 | 77% | $3M | 5–7× | 70 |
|---|---|---|---|---|
| Q1 2026 Incidents (Ransomware.live) | Attacks Include Data Exfiltration | Median Ransom Financial Sector | True Cost vs. Ransom Demand | Active Threat Groups |

## ■ DOMINANT THREAT ACTORS

**Qilin** — **338 victims Q1**
8 attacks in March alone; led global activity; targeted Die Linke (political), Dow Chemical, and NHS-linked entities. Credential theft primary vector.

**Akira** — **197 victims Q1**
Manufacturing-heavy focus. Engineering designs exfiltrated. Swiss firm Gericke AG hit; IP theft primary damage.

**The Gentlemen** — **~130 victims Q1**
New entrant that scaled rapidly via RaaS model. Targeted professional services and healthcare across EU and North America.

**INC Ransom / Cl0p** — **~120 combined**
Supply-chain and SaaS platform exploitation. Attacking vendors to reach portfolios of downstream victims simultaneously.

**LockBit 5 / DragonForce** — **Active Apr 2026**
LockBit 5 resurgent—logistics (Heinrichs, Germany) and machinery (Merlo) hit April 24–26. DragonForce struck FGV Brazil: 1.52 TB exfiltrated.

**Lapsus$** — **Re-emerged Apr 25**
Checkmarx breach: source code, employee DB, API keys, and database credentials stolen. Software supply-chain risk.

## ■ SECTOR RISK HEATMAP

| SECTOR | THREAT LEVEL | Q1 SHARE | DEAL RISK |
|---|---|---|---|
| **Manufacturing** | ■ CRITICAL | ~20% | Hidden IP loss |
| **Healthcare** | ■ CRITICAL | ~18% | HIPAA liability |
| **Professional Svcs (Legal/Accounting)** | ■ HIGH | ~15% | Client file breach |
| **Construction** | ■ HIGH | ~12% | Project doc theft |
| **Financial Services** | ■ HIGH | ~10% | Max ransom demands |
| **Technology/SaaS** | ■ HIGH | ~9% | Supply chain vector |
| **Retail/Distribution** | ■ ELEVATED | ~8% | Logistics disruption |
| **Energy/Utilities** | ■ ELEVATED | ~5% | OT/SCADA risk |

## ■ ACTIVE ACCESS BROKER MARKET

In March 2026, CRIL tracked **20 unauthorized network access listings** on cybercrime forums within a single month—a critical pre-incident indicator. Access brokers sell credentials to your portfolio companies *before* ransomware deploys, often 30–90 days ahead of the visible attack. The top three brokers—**vexin, holyduxy, and algoyim**—controlled over 55% of listings. For M&A teams: if a target appears in broker markets, ransomware deployment is imminent.

## ■ NOTABLE INCIDENTS — MARCH 28 TO APRIL 27, 2026 | 5Ws + HOW

| WHO / WHERE | WHAT | WHEN | WHY TARGETED | HOW (VECTOR) | EST. IMPACT |
|---|---|---|---|---|---|
| **Stryker Corp (Medical Devices, US)** | Handala (Iran-linked) wiped 200k+ devices; 50 TB data theft claimed; simultaneous factor resets across 79 countries | Mar 11–12, 2026 | Retaliation for US geopolitical action; high-value IP & global device footprint | Nation-state intrusion; credential compromise; EDR neutralization via BYOVD technique | **CRITICAL — Massive operational disruption; order/production/shipping halted** |

| WHO / WHERE | WHAT | WHEN | WHY TARGETED | HOW (VECTOR) | EST. IMPACT |
|---|---|---|---|---|---|
| **Dow Chemical (Manufacturing, US)** | Qilin claimed unauthorized access; internal data allegedly exfiltrated; Dow has not confirmed scope | Mar 2026 | Chemical manufacturing = high-leverage extortion; OT/IT boundary vulnerability | Phishing + credential theft; lateral movement to corporate systems | **HIGH — IP and trade-data exposure; unconfirmed ransom demand** |
| **Die Linke Party (Government/Political, DE)** | Qilin claimed ransomware + data theft; IT systems partially shut down; hybrid-warfare framing | Mar 2026 | Political entity with sensitive communications; Russian-aligned threat group | Spear-phishing; remote desktop exploitation | **HIGH — Reputational and political damage; data publication threatened** |
| **Foster City, CA (Municipal Gov, US)** | Ransomware forced suspension of all non-emergency public services; personal data potentially compromised | Mar 19, 2026 | Under-resourced municipal IT; no group claimed; opportunistic targeting | Likely phishing or exposed RDP; weeks-long recovery | **HIGH — Public service disruption; PII exposure for residents** |
| **Bladex Bank (Finance, Latin America)** | LockBit 5 listed Bladex (multinational bank from central bank consortium); attack estimated Apr 22 | Apr 22–26, 2026 | Multinational financial institution; cross-border data = high ransom leverage | Credential theft; likely supply-chain or third-party vendor access | **CRITICAL — Banking data; inter-bank records; regulatory exposure** |
| **Checkmarx (SaaS/DevSec, Global)** | Lapsus$ stole source code, employee database, API keys, and MongoDB/MySQL credentials | Apr 24–25, 2026 | DevSecOps platform = supply-chain multiplier; keys enable downstream compromise | Insider access or social engineering; API key exfiltration | **CRITICAL — Every customer using Checkmarx APIs is at downstream risk** |
| **Heinrichs Logistic (Logistics, DE)** | LockBit 5 listed German logistics provider; attack estimated Apr 24 | Apr 24–26, 2026 | Port logistics = supply chain bottleneck; high disruption leverage | Unknown; LockBit 5 typical vectors: phishing + RDP | **HIGH — Supply chain disruption; client data exposure** |
| **Getulio Vargas Fdn (Education/Gov, BR)** | DragonForce exfiltrated 1.52 TB including names, IDs, and banking data from leading Brazilian institution | Mar 2026 | Government-linked educational data = personal + financial records at scale | Credential theft + lateral movement; double extortion | **HIGH — 1.52 TB of sensitive records; Brazilian data regulation exposure (LGPD)** |

## ■ INTELLIGENCE SPOTLIGHT — TRENDS THAT MOVE DEAL VALUATIONS

### ① Manufacturing: Sustained #1 Target Since 2021

Manufacturing absorbed **419 incidents in Q1 2026** (~20% of all attacks), per ZeroFox. OT/IT convergence creates a single-point-of-failure where a ransomware hit stops the production floor immediately. Engineering designs and production data are primary exfiltration targets, destroying IP value long after remediation. **Investor implication:** Any manufacturer without documented network segmentation between OT and IT represents an unpriced liability.

### ② Healthcare: 460 FBI-Reported Incidents; HIPAA Fines Escalate

The FBI's 2025 IC3 report recorded **460 ransomware incidents in healthcare**—the highest of any sector. This month, HHS OCR fined four entities a combined **$1.7M** for HIPAA violations enabling ransomware. Exposed ePHI of 427,000 individuals. Healthcare organizations that cannot evidence a current, documented risk analysis carry hidden regulatory liability that surfaces post-close. **Investor implication:** Request risk-analysis documentation as part of every healthcare LOI package.

### ③ Financial Services: Record $3M Median Ransom

Financial services now carries the **highest median ransom demand of any sector at $3M**, with 59% of attacked firms reporting successful encryption (up from 49%). The Marquis Software breach (Aug 2025) continued to surface in March 2026 regulatory filings, exposing **672,000–1.35M individuals** across 74 banks. Third-party vendor risk is the defining attack vector—attackers compromise a shared platform and pivot into multiple portfolio companies simultaneously. **Investor implication:** Map every fintech vendor relationship before close.

### ④ Construction & Legal: The Quiet Targets

Construction and professional services (legal, accounting) consistently rank **3rd and 4th** in U.S. attack frequency. Construction firms hold project plans, contracts, and lien data—all highly sensitive in M&A contexts. Law firms hold client files that may include pending litigation, deal memos, and transaction documents. A breach of outside counsel during a live deal is a material event. **Investor implication:** Due diligence should extend to key professional-service vendors, not just the target company itself.

### ⑤ Supply-Chain Intrusion: One Compromise, Many Victims

The VECT & TeamPCP campaign this period exploited a **global travel platform** to deploy ransomware across its entire customer base—a single breach with cascading downstream impact. Similarly, Checkmarx's API key theft puts every customer's DevOps pipeline at risk. The FBI confirmed that ransomware groups increasingly breach **SaaS and authentication platforms** to reach a wider network of victims. **Investor implication:** Shared-service providers used by portfolio companies must be included in cyber due diligence scope.

### ⑥ Nation-State Actors Now Targeting Commercial Entities

The Stryker attack by Iran-linked **Handala** (200k+ devices wiped; geopolitical retaliation) and Qilin's attack on Germany's Die Linke party illustrate that geopolitical risk now translates directly into commercial enterprise risk. ODNI's 2026 Annual Threat Assessment confirmed that **China, Russia, Iran, and North Korea** are actively embedding access in critical infrastructure for future disruption. **Investor implication:** Companies with government contracts, sensitive IP, or overseas operations carry elevated nation-state exposure.

## ■ DEAL TEAM ACTION FRAMEWORK — WHAT SOPHISTICATED CAPITAL DOES DIFFERENTLY

 

| DEAL STAGE | CYBERSWEEP ACTION | WHAT IT PREVENTS | FINANCIAL BENEFIT |
|---|---|---|---|
| **Pre-LOI Screening** | QuickSweep: dark web access-broker check + external attack surface scan | Bidding on a company already inside an attacker's queue | Avoids inherited breach; walk-away clarity |
| **LOI / QofE Stage** | DeepSweep: full security posture assessment with dollar-risk quantification | Hidden cyber debt inflating EBITDA; undisclosed incidents | Renegotiate price; fund escrow for remediation |
| **Pre-Close / Integration** | TotalSweep: vendor risk mapping + OT/IT gap analysis + pen test | Supply-chain inherited breach; rep & warranty disputes | Lower R&W; insurance premiums; clean close |
| **Post-Close Portfolio** | Continuous monitoring via CyberSweep weekly threat-intel brief | Silent post-close breach destroying hold-period value | Protects exit valuation; maintains EBITDA integrity |

**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



 