RANSOM WARE IN 2025

A FRAGMENTED, DATA DRIVEN EXTORTION ECONOMY

phish tank DIGITAL

EXECUTIVE SUMMARY

Ransomware in 2025 was defined not by a single dominant cartel but by a crowded, professionalized ecosystem exploiting the same systemic weaknesses at scale. A diffuse set of groups – including Qilin, Akira, CL0P, PLAY, SAFEPAY, INC Ransom, and others – collectively drove roughly **7,900 known victims**, with an estimated **65% experiencing data leakage**. Extortion has now fully shifted from encryption centric disruption to **data centric coercion**.

Three converging forces shaped the year:

1

Small business exposure at unprecedented levels

2

Windows and appliance centric attack paths

3

Heavy reliance on classic injection and deserialization vulnerabilities

The result is a threat landscape where operational resilience alone is no longer sufficient. Ransomware has become a **data governance, legal, and third party risk problem**, not merely a backup or disaster recovery issue.

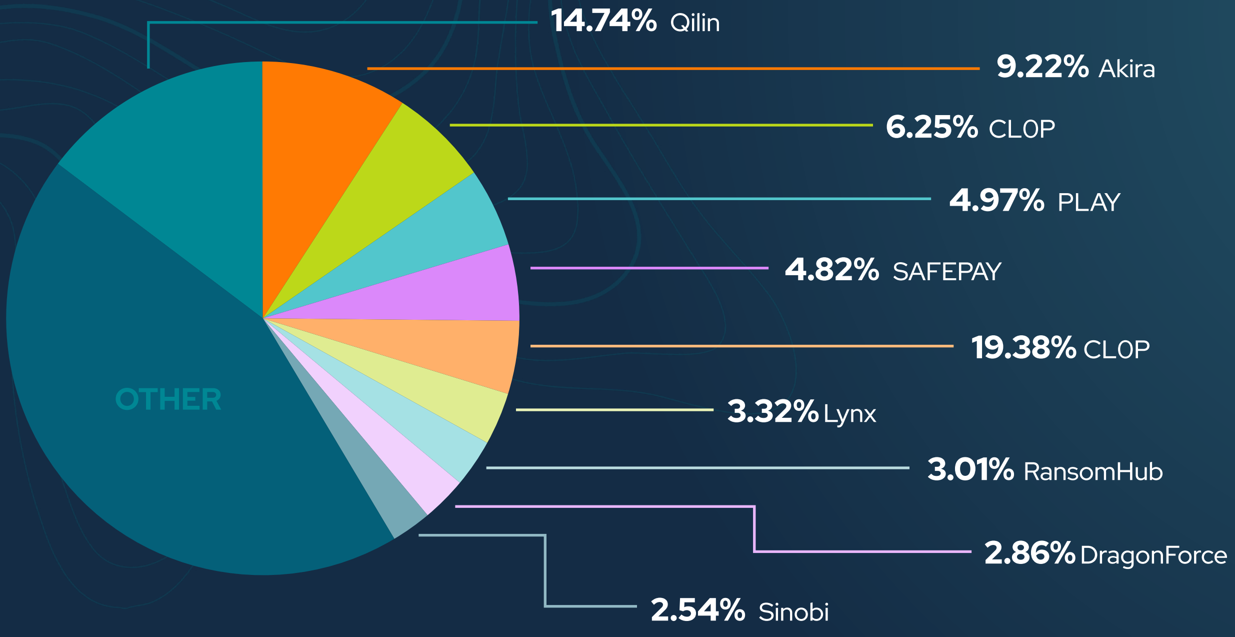
1 | THE RANSOMWARE ECOSYSTEM IN 2025

A fragmented but highly active top tier

No single group dominated the landscape. Qilin led with ~15% of observed incidents, while Akira, CL0P, PLAY, SAFEPAY, and INC Ransom each held mid–single digit shares. This fragmentation reflects:

- **Rapid brand churn** — rebrands, splinters, and "new" groups with familiar TTPs
- **Reduced dependence on mega brands** like LockBit
- **A resilient ecosystem** where disruption of one group barely dents overall activity

TOP RANSOMWARE IN 2025



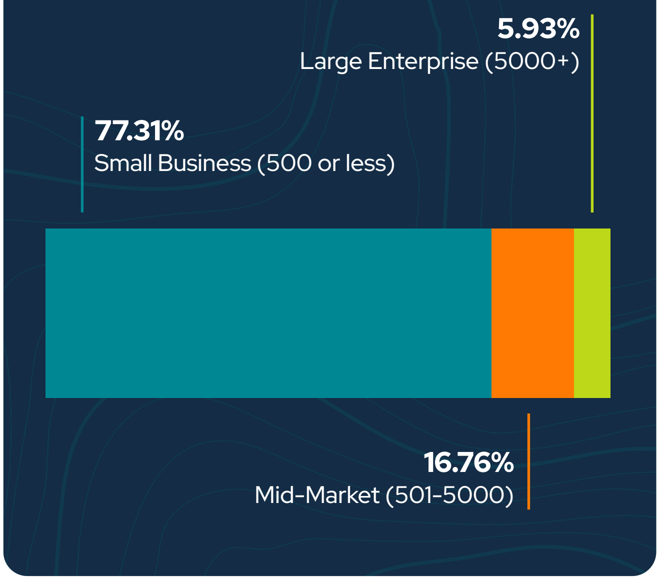
Double extortion as the default

With ~65% of cases involving data leakage, encryption now serves primarily as a pressure tactic. The business model is data theft, publication, and multi party extortion. Regulatory, legal, and reputational consequences increasingly outweigh operational downtime.

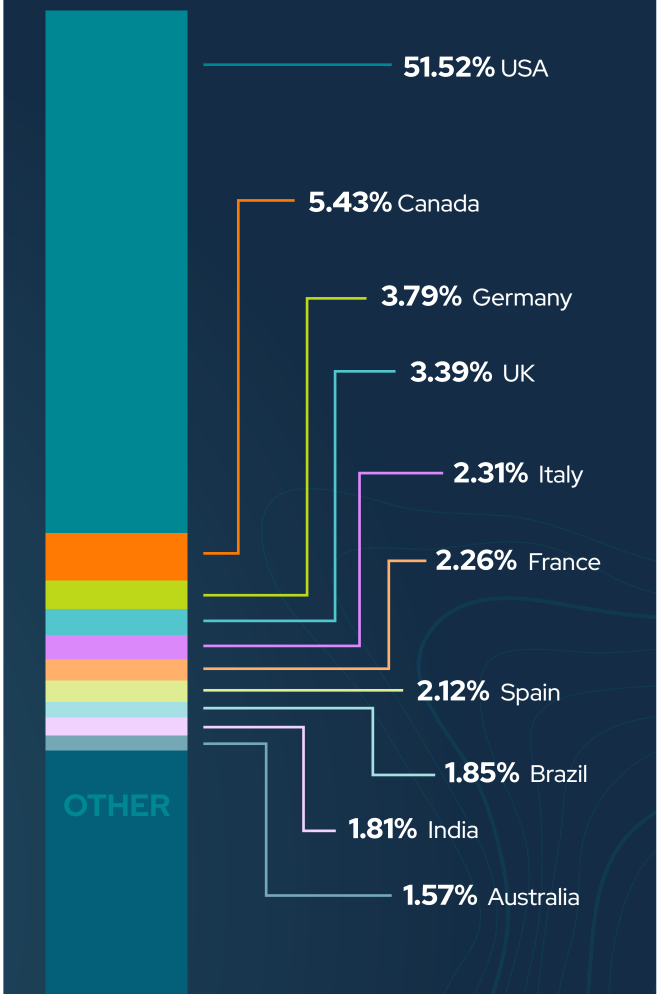
Executive implication: Ransomware cannot be treated as a backup problem. It is fundamentally a **data risk and supply chain risk problem.**

2 | WHO WAS HIT: VICTIMS, SECTORS, & GEOGRAPHY

VICTIM DISTRIBUTION IN 2025



VICTIM LOCATIONS



Small businesses bore the brunt

- **Small businesses (≤500 staff):** ~77%
- **Mid market (501–5,000):** ~17%
- **Large enterprises (5,000+):** ~6%

Attackers **optimized for volume and low resistance**, not prestige. The impact is now concentrated in organizations with limited security staffing, weaker vendor oversight, and constrained budgets.

Implication: Security programs, insurance models, and government policy remain calibrated for large enterprises, while the real blast radius sits in **SME dominated supply chains**.

Geography: US centric but globally distributed

- **USA: ~51% of victims**
- Next tier (low single digits each): Canada, Germany, UK, Italy, France, Spain, Brazil, India, Australia
- Long tail across Asia, the Middle East, and Latin America

Implication: US organizations remain the default target set for most RaaS operations, but non US regions are firmly in the "steady growth" phase as digitization outpaces security maturity.

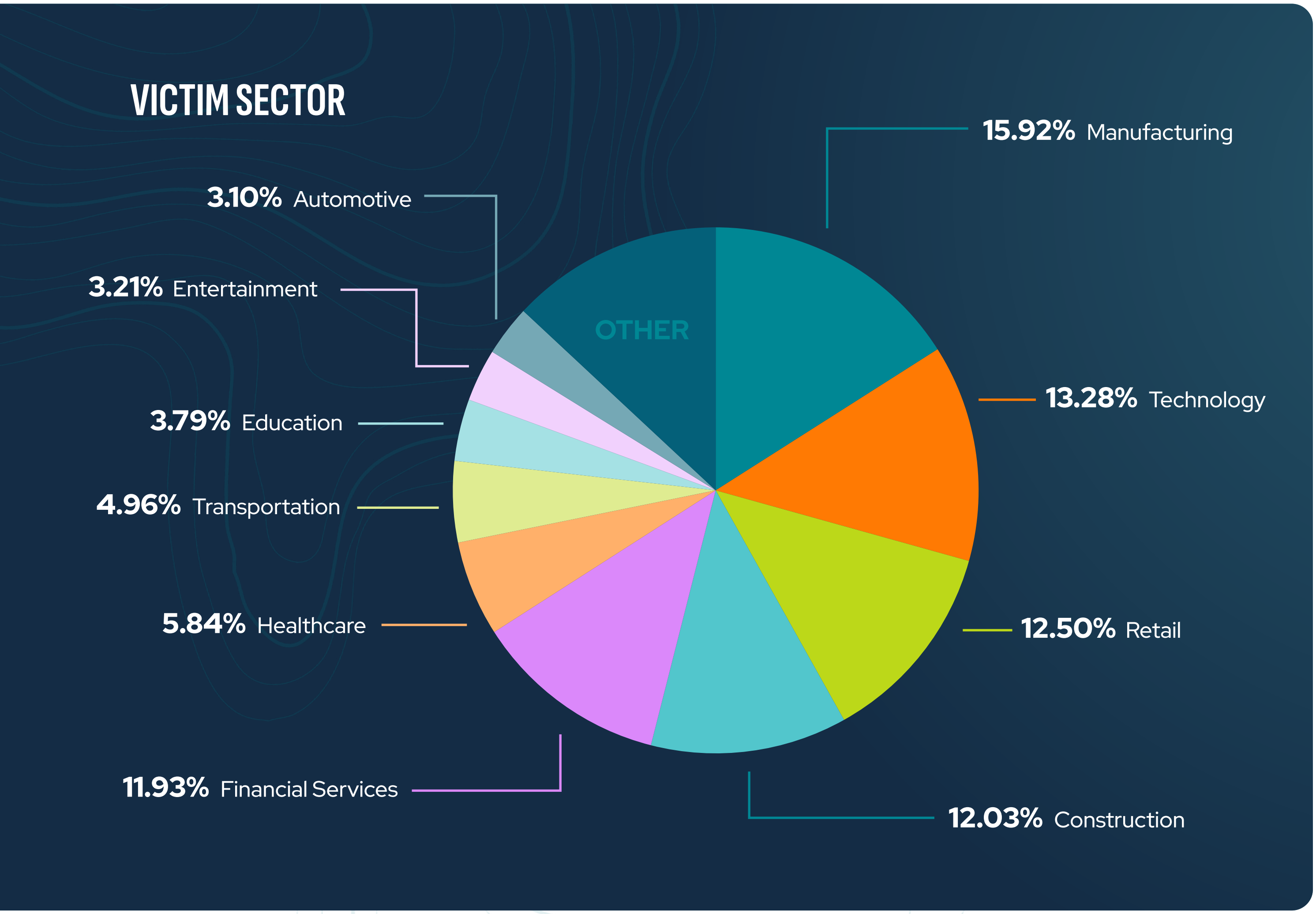
Sector exposure: manufacturing and digital backbone services

Top targeted sectors:

- **Manufacturing** (~16%) — reflecting OT adjacent exposure and just in time supply chain leverage
- **Technology** (~13%)
- **Retail** (~12%)
- **Construction** (~12%)
- **Financial services** (~12%)

These sectors share characteristics: complex, heterogeneous IT; internet facing portals; and deep supply chain integrations.

Healthcare, transportation, education, entertainment, automotive, local government, and energy all appear meaningfully but without sectoral dominance — reinforcing that **targeting remains broad and opportunistic.**

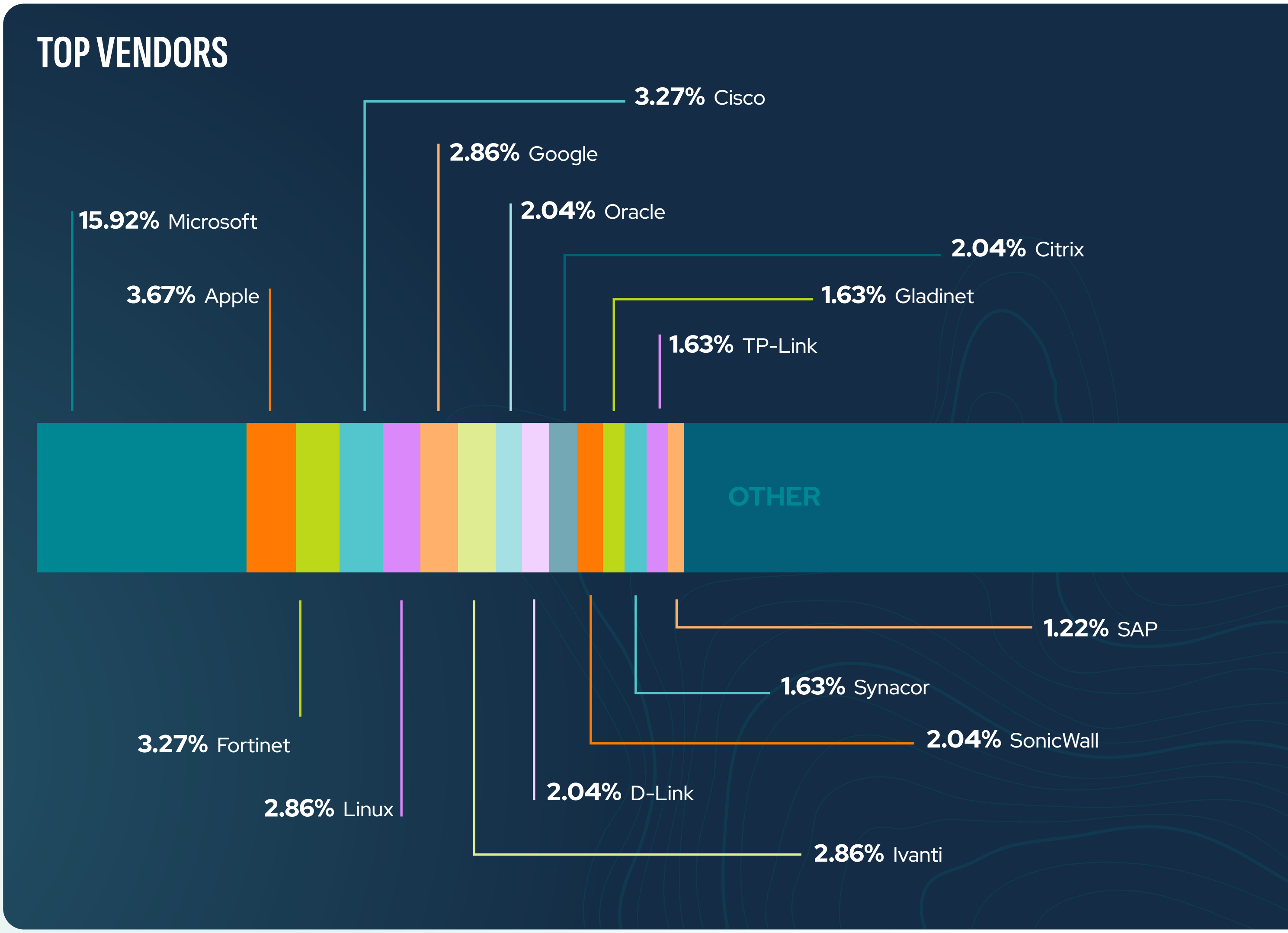


3 TECHNICAL THEMES: HOW ATTACKERS GAINED ACCESS

Vendor and product patterns: Windows and edge appliances

Top vendors associated with exploited products:

- **Microsoft (~16%), with Windows (~12%)** as the single most referenced product
- A long tail including Apple, Fortinet, Cisco, Google, Linux, Ivanti, Citrix, Oracle, D Link, SonicWall, TP Link, SAP, and others



MOST NOTABLE PRODUCTS

11.84% Windows	**2.86%** Linux Kernel	**1.63%** Chromium V8	**1.63%** Zimbra Collaboration Suite (ZCSI)

Notable product categories:

- **Core OS / Linux kernel paths**
- **Security appliances and edge devices** (VPNs, firewalls, routers, email gateways)
- **Enterprise collaboration and management platforms** (Zimbra, SharePoint, NetWeaver, Craft CMS, Apriso, Endpoint Manager)

The prevalence of "multiple products/devices/chipsets" categories highlights **portfolio-wide exposure** within vendors.

Implication: Security appliances and edge devices — often implicitly trusted — are functioning as **high value single points of failure.**

Vulnerability patterns: classic injection and unsafe data handling

Top CWEs linked to incidents:

- **CWE 78 / CWE 77** — OS & command injection (~11% combined)
- **CWE 502** — Deserialization of untrusted data (~6.5%)
- **CWE 22** — Path traversal (~5.7%)
- **CWE 787 / CWE 416** — Out of bounds write & use after free (~9.5% combined)
- **CWE 79, CWE 94, CWE 306/288** — XSS, code injection, auth bypass (~8–9% combined)

Attackers continue to profit from decades old bug classes in modern products.

Implication: You don't need exotic 0 days to suffer a breach — one missed injection or deserialization flaw in an exposed component is enough.

COMMON WEAKNESS ENUMERATION

CVE	DESCRIPTION	PERCENTAGE
CWE-78	OS Command Injection	7.83%
CWE-502	Deserialization of Untrusted Data	6.52%
CWE-22	Path Traversal	5.65%
CWE-787	Out-of-bounds Write	4.78%
CWE-416	Use After Free	4.78%
CWE-79	Cross-site Scripting	3.04%
CWE-77	Command Injection	3.04%
CWE-94	Code Injection	2.61%
CWE-306	Missing Authentication for Critical Function	2.61%
CWE-288	Authentication Bypass Using an Alternate Path or Channel	2.61%

4 | PRACTICAL PRIORITIES FOR DEFENDERS HEADING INTO 2026

1

Treat SME and mid market security as systemic risk

ACTIONS

- Establish baseline controls: MFA, EDR, centralized logging, and vulnerability management
- Embed security expectations into supplier contracts: patching, MFA, backup testing, IR readiness

2

Harden internet facing infrastructure and security appliances

ACTIONS

- Maintain an authoritative inventory of exposed services
- Prioritize rapid patching for Microsoft, Fortinet, Cisco, Ivanti, Citrix, SonicWall, TP Link, and similar edge products
- Enforce network segmentation to prevent appliance compromise from becoming full internal access

3

Assume data theft and prepare for extortion

ACTIONS

- Identify and protect systems holding high value data
- Build and rehearse data breach playbooks (legal, comms, regulatory, third party coordination)
- Encrypt sensitive data and monitor for abnormal data movement

4

Focus on the “boring but critical” bug classes

ACTIONS

- Mandate secure coding controls for injection, deserialization, and path traversal
- Adopt secure by default frameworks and tuned static analysis
- Prioritize patches and virtual patching for these classes

5

Improve detection of lateral movement and privilege abuse

ACTIONS

- Strengthen detections for credential theft, suspicious remote access, and abnormal process execution
- Implement tiered admin access and audited privileged accounts

4 | SIGNALS AND PREDICTIONS FOR 2026

1

Continued fragmentation and rebranding

Expect ongoing churn in group names. Operators and TTPs will remain familiar even as brands shift. Technique focused intelligence will outperform brand focused tracking.

2

Increased pressure on manufacturing, OT adjacent, and logistics environments

Attackers have discovered the leverage of production and supply chain disruption. Expect:

- Higher ransom demands tied to business interruption
- IT side ransomware used to pressure OT owners, even without deep OT compromise

3

Expansion of data centric extortion and leak aggregation

With data leakage already at ~65%:

- Multi party extortion will grow
- Marketplaces and search tools for historical leak data will expand
- Long term privacy and fraud risks will increase

4

Continued exploitation of edge devices and security stacks

Expect:

- New waves of mass exploitation in VPNs, firewalls, email gateways, and device management platforms
- Increased focus on firmware and chipset flaws with slow patch cycles

5

Gradual shift toward memory safe and hardened stacks

Regulatory pressure and repeated exploitation of memory unsafe code will drive:

- Adoption of memory safe languages for new development
- Systematic vendor efforts to address injection and deserialization risks

TL;DR

Ransomware in 2025 was driven by a fragmented ecosystem of many mid tier groups rather than a single dominant cartel. Attackers overwhelmingly targeted small and mid sized businesses, exploited Windows and internet facing appliances, and relied on classic vulnerabilities like injection and deserialization bugs. Around 7,900 known victims were recorded, with ~65% experiencing data theft, confirming that extortion is now fundamentally data centric, not encryption centric.

The most targeted sectors were manufacturing, technology, retail, construction, and financial services, with the US remaining the primary hunting ground. Attackers focused on edge devices, security appliances, and enterprise platforms, taking advantage of long standing software weaknesses rather than exotic 0 days.

For defenders, the priorities heading into 2026 are clear: treat SME security as systemic risk, harden internet facing infrastructure, assume data theft in every incident, focus on the "boring but critical" bug classes, and improve detection of lateral movement and privilege abuse.

Looking ahead, expect continued threat group fragmentation, increased pressure on manufacturing and logistics, expansion of data driven extortion, ongoing exploitation of edge devices, and a slow but real shift toward memory safe and hardened software stacks.

ULTRA-TL;DR

Ransomware in 2025 became a fragmented, data theft driven extortion economy overwhelmingly targeting small and mid sized businesses through old, unpatched vulnerabilities in Windows and internet facing appliances.

phish tank DIGITAL

WHAT DO WE DO?

DIGITAL MARKETING SOLUTIONS
FOR CYBERSECURITY COMPANIES

CONTACT US

PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL

DATA & CO-AUTHOR
JEREMY NICHOLS
Former Director of the Global
Threat Intelligence Center

CO-AUTHOR
GEOFF REHMET
Cybersecurity Expert