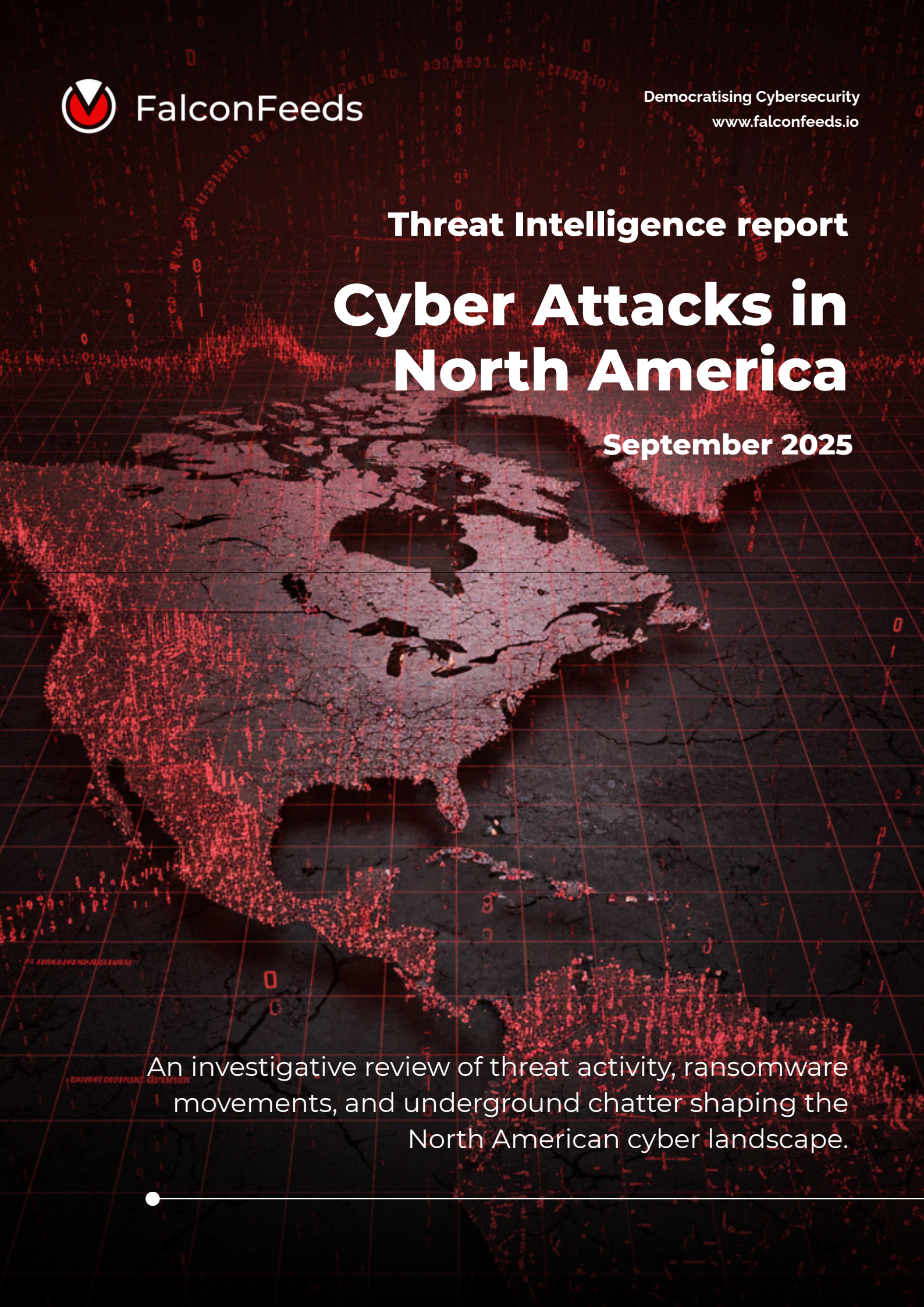
FalconFeeds

Democratising Cybersecurity
www.falconfeeds.io

Threat Intelligence report

Cyber Attacks in North America

September 2025



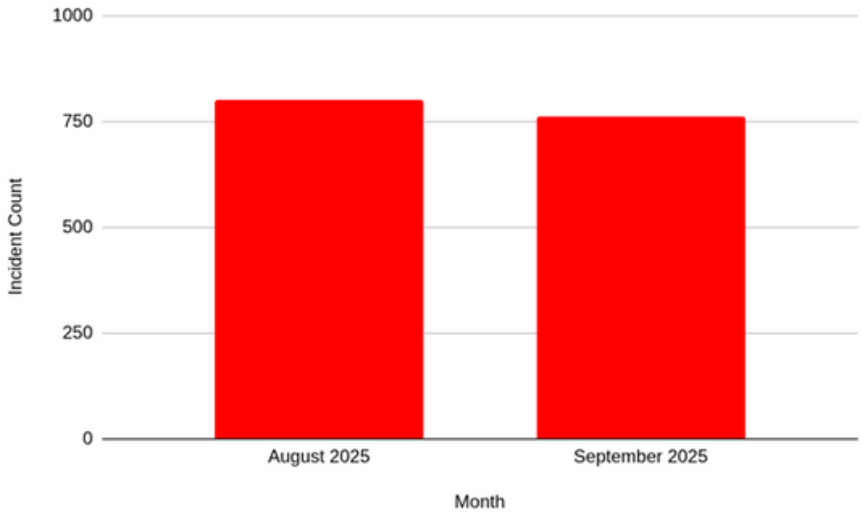
An investigative review of threat activity, ransomware movements, and underground chatter shaping the North American cyber landscape.

The Deepest Watch on the Darkest Web

FalconFeeds.io delivers the largest real-time monitoring of deep and dark web activity—from ransomware gangs to Telegram dumps and access marketplaces.

Executive Overview

September 2025 brought a brief lull in cyber hostilities across North America — but not calm.
A total of 762 confirmed incidents were recorded across the region, a modest drop from 802 in August 2025. Yet the apparent dip belied the intensity and persistence of ransomware operations that continued to wreak havoc across critical sectors.



Ransomware remained the dominant weapon, driving 42% of all incidents (323 cases). Among the most active groups were PLAY, Akira, Qilin, and INC RANSOM — each continuing to expand its reach and refine its tactics.

High-value targets once again sat at the intersection of finance, technology, manufacturing, and construction — industries that form the backbone of North America's economy. The United States absorbed the majority of hits, while Canada and Mexico experienced steady spillover.

Across the digital underworld, Ransomware Data Leak Sites (DLS), dark forums, and Telegram channels operated as the central arteries of cybercrime — fuelling extortion, credential sales, and stolen data dissemination.

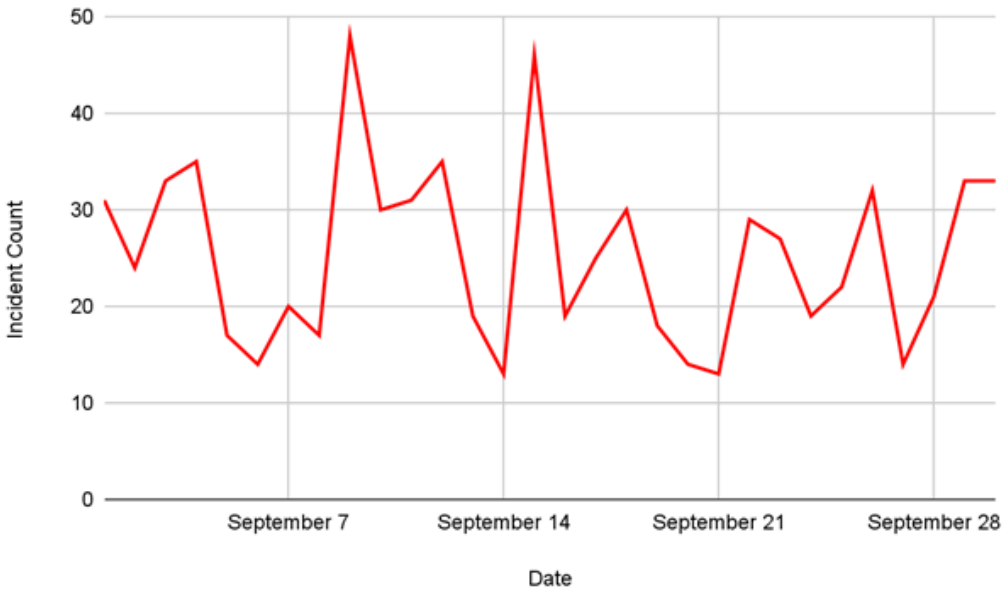
Date-wise Activity Trends

The Ebb and Flow of September's Threat Landscape

Point to Ponder:

Behind every spike lies a trigger — a disclosure, a new vulnerability, or a misstep in defence. The challenge for security leaders is not just to react, but to read the pulse early.

While the overall incident curve showed small fluctuations, the rhythm of September's attacks painted a more complex picture. Activity peaked several times during the month — notably on 1st September (31 incidents), 9th September (48), 15th September (46), 26th September (32), and the closing days, 29th and 30th September (33 each).



Each of these peaks aligned with specific patterns: ransomware disclosures, mass data leaks, and coordinated DDoS offensives targeting public-facing infrastructure.

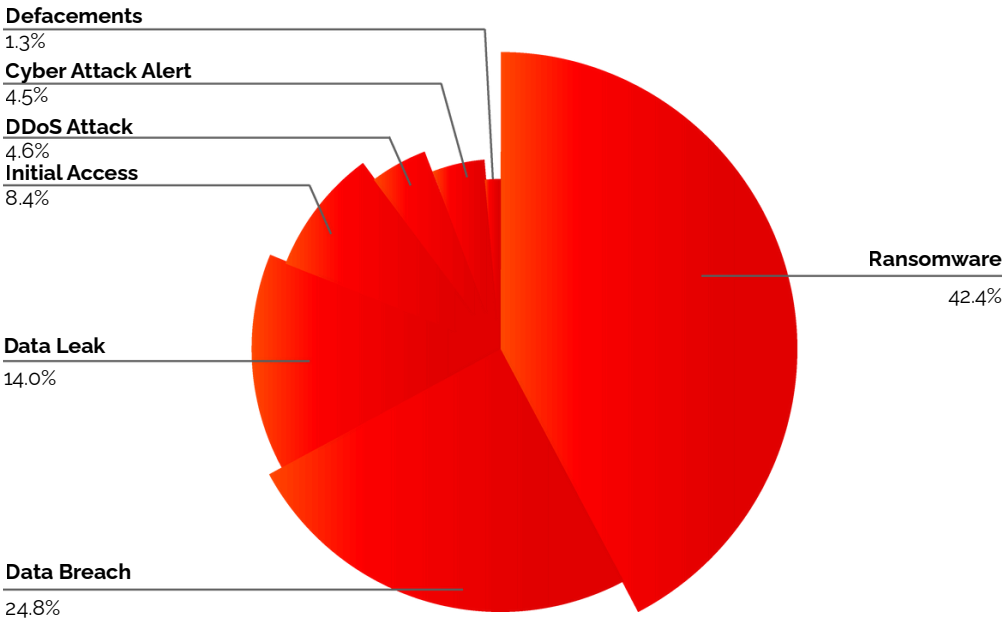
Category-wise Breakdown

The Anatomy of Attacks

Think Box:

If your organisation's name appeared on a leak site tomorrow, would your response plan be ready within the hour or would chaos precede clarity?

Ransomware continued its reign as the most disruptive force, accounting for 323 incidents in September. Attackers increasingly adopted double-extortion models, where encryption is only the opening act — followed by data leaks, public shaming, and negotiation pressure.



- Data breaches followed at 189 incidents, spanning everything from corporate server infiltrations to mass credential dumps.
- Initial Access Sales, the underground trade of compromised entry points, recorded 64 incidents, reflecting a slight decline but remaining an essential supply chain for ransomware affiliates.
- Data leaks (107 incidents) and DDoS attacks (35) persisted as staple tactics.
- While defacements, though fewer (10), carried symbolic value for hacktivist and ideological groups.

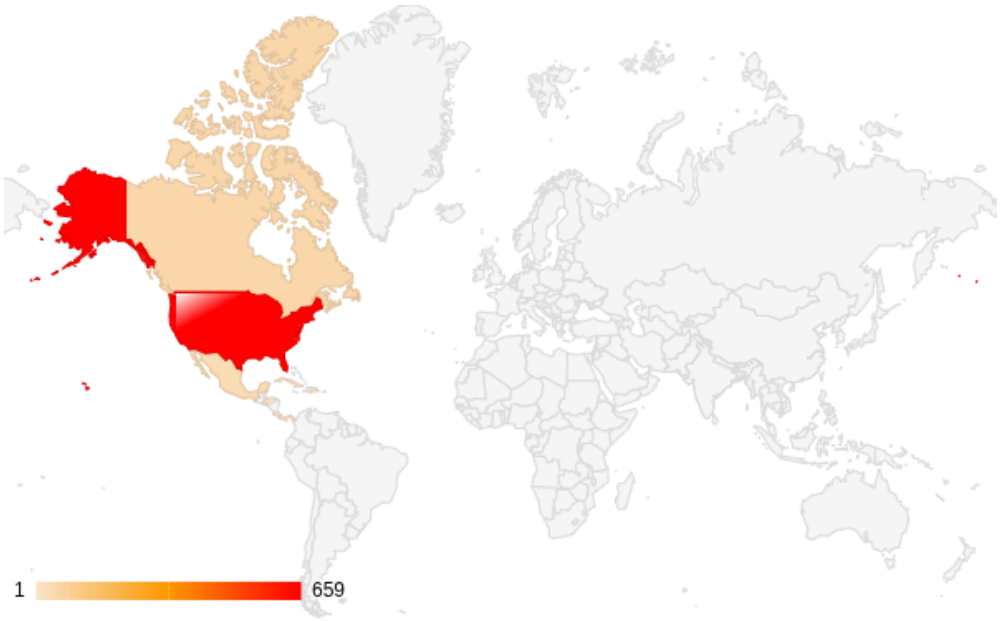
Country-wise Distribution

Mapping the Region's Exposure

Point to Ponder:

Cybercrime respects no borders. It travels through the same cables that connect our businesses. The weakest link in the region can become everyone's problem.

The United States remained the undisputed epicentre of cyber activity, absorbing 659 of the 762 recorded incidents — a staggering 86.5% share.
Canada followed with 50 cases, and Mexico with 39.



Beyond these three, smaller economies across the Caribbean and Central America were also caught in the net. This includes Panama, Costa Rica, the Dominican Republic, El Salvador, Cuba, and Trinidad and Tobago.

This expanding geographical footprint highlights a clear evolution: attackers are no longer confined to major economies but are probing adjacent markets for weaker digital borders.

Industry-wise Impact

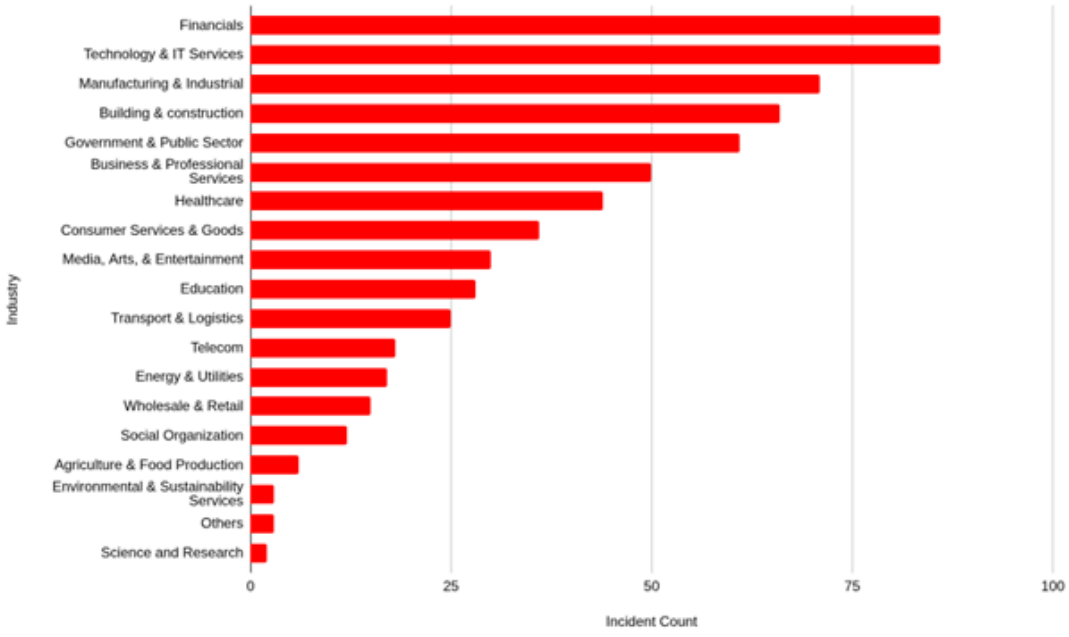
Who is in the Firing Line

Think Box:

Would your sector survive three days of digital paralysis? For many industries, downtime now costs more than ransom.

The pattern of targeting stayed consistent, underscoring adversaries' fixation on sectors with both financial leverage and operational dependency.
Top among them were:

- **Financials** – 86 incidents
- **Technology & IT Services** – 86 incidents
- **Manufacturing & Industrial** – 71 incidents
- **Building & Construction** – 66 incidents
- **Government & Public Sector** – 61 incidents



Others in the line of fire included healthcare, education, energy, logistics, media, and telecom — collectively revealing how attackers diversify to test defences across essential infrastructure.

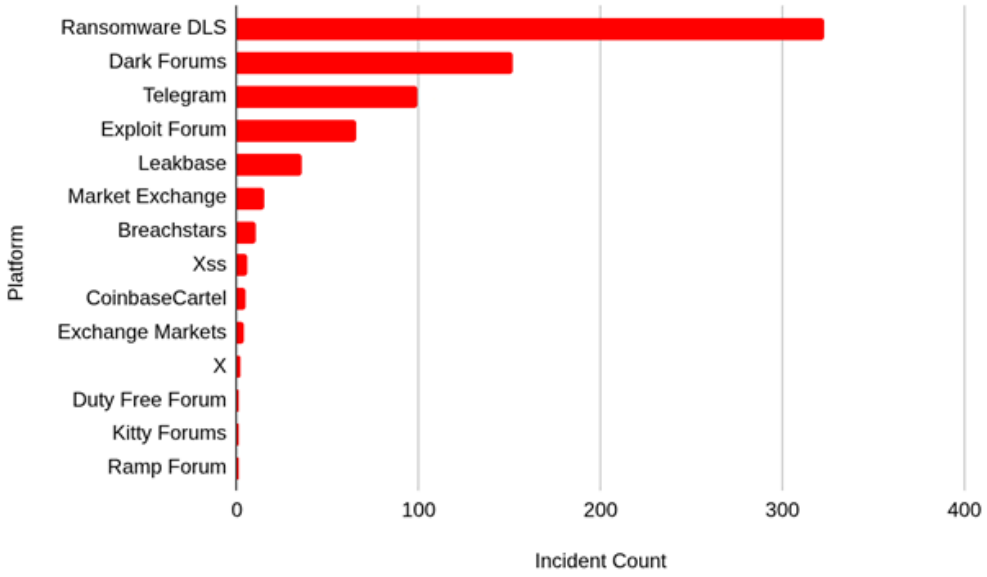
Platform-wise Analysis

Inside the Underground Exploitation

Point to Ponder:

The dark web is not a place — it's a process. Its decentralisation makes it almost impossible to shut down, but entirely possible to monitor intelligently.

The cyber underground continued to thrive as a dynamic ecosystem of trade, coordination, and exposure.



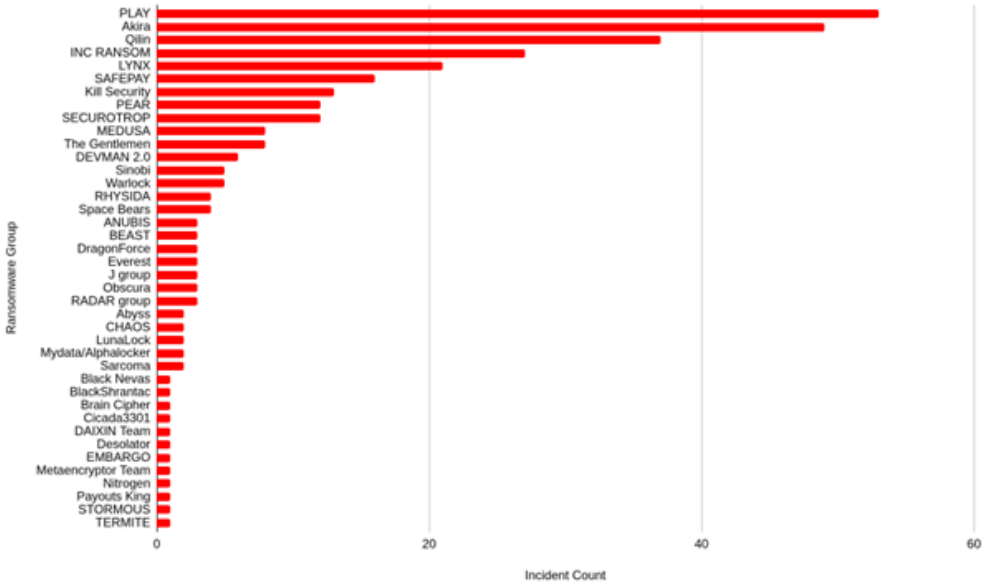
- Ransomware Data Leak Sites (DLS) hosted 323 victim disclosures, often paired with countdowns or auction-style extortion threats.
- Dark forums saw 152 incidents of activity — with threat actors trading access credentials, databases, and exploit kits.
- Telegram followed closely with 99 incidents, cementing its status as a preferred hub for coordination, victim shaming, and real-time leaks.
- Exploit forums (66 incidents) and niche leak platforms like LeakBase (36) facilitated distribution of stolen logs and zero-day exploits.
- Others — such as Market Exchange, Breachstars, CoinbaseCartel, Ramp Forum, and even X (formerly Twitter) — played smaller but significant roles in the information supply chain.

Ransomware Groups on the Offensive

Think Box:

If ransomware has become a business, is your defence structured like one — with budget, metrics, and accountability to match?

September witnessed activity from 40 active ransomware groups across North America. Among them, five stood out for both volume and aggression.



- **PLAY (53 incidents):** Continued to dominate the construction, manufacturing, and technology verticals.
- **Akira (49 incidents):** Targeted U.S. construction and manufacturing sectors with precision and persistence.
- **Qilin (37 incidents):** Spread across construction and healthcare, demonstrating adaptive targeting.
- **INC RANSOM (27 incidents):** Maintained a reputation for ruthless negotiation tactics and affiliate expansion.
- **Emerging players:** LYNX, SAFEPAY, Kill Security, PEAR, and SECUROTROP displayed sharp upward momentum.

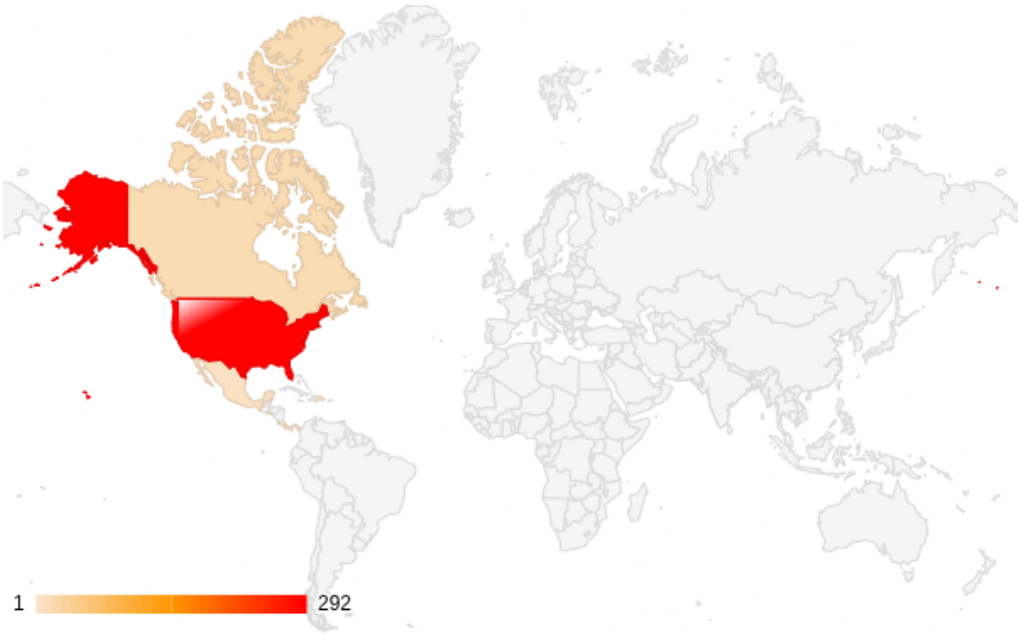
Collectively, these actors illustrate the industrial maturity of Ransomware-as-a-Service (RaaS) — an ecosystem where crime has become an outsourced business model.

Mapping Ransomware's Geographic Reach

Point to Ponder:

The ransomware map is no longer national — it's networked. Your partners' breach can become your headline tomorrow.

The United States recorded 292 ransomware incidents, followed by Canada (19) and Mexico (6). Other countries, including the Dominican Republic, Costa Rica, El Salvador, Panama, and Trinidad and Tobago, faced smaller yet noteworthy campaigns.



The data reinforces a troubling trend — ransomware operators are expanding laterally, exploiting shared suppliers and technology vendors to infiltrate multiple economies simultaneously.

Industries Hit the Hardest by Ransomware

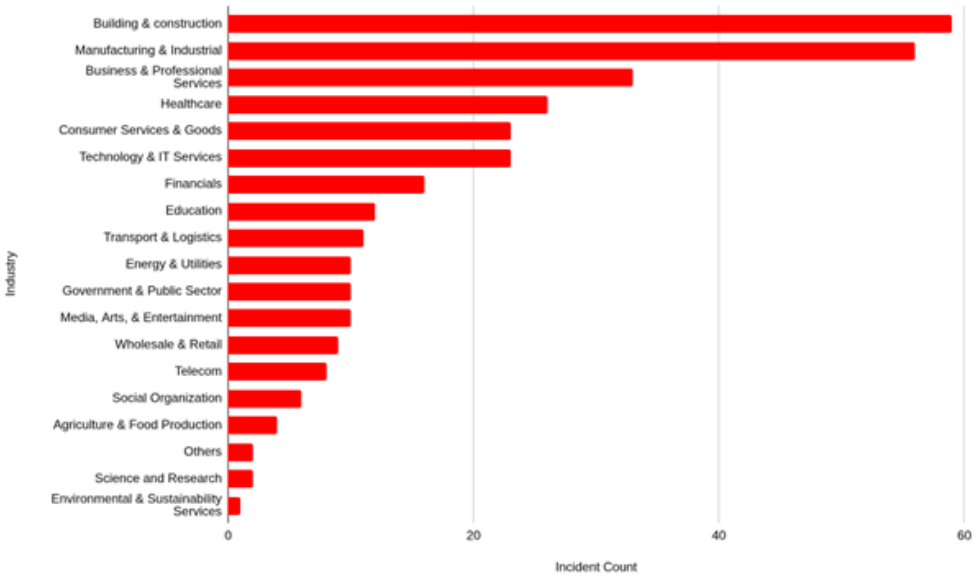
Think Box:

Could your organisation operate offline for a week without losing clients, compliance, or credibility?

Ransomware's impact was not evenly spread. Some industries bore disproportionate damage due to their reliance on continuous digital operations.

The worst affected were:

- **Building & Construction** – 59 incidents
- **Manufacturing & Industrial** – 56 incidents
- **Business & Professional Services** – 33 incidents
- **Healthcare** – 26 incidents
- **Consumer Services & Goods** – 23 incidents
- **Technology & IT Services** – 23 incidents
- **Financials** – 16 incidents



Other sectors, including education, energy, government, media, telecom, and agriculture, also suffered sporadic hits.

The message is clear — ransomware groups target dependency. Wherever downtime hurts most, that's where they strike.

Key Trends and Takeaways

Threat actors adapt faster than most corporate strategies. Intelligence isn't about prediction — it's about readiness.

The September data paints a story of evolution, not reduction.

- PLAY and Akira alone accounted for over a hundred ransomware cases, showing their dominance in the regional ecosystem.
- Initial Access Brokers (IABs) — though slightly quieter — remained the indispensable middlemen enabling these attacks.
- Telegram and dark forums continued as preferred communication channels, and the rise of groups such as SECUROTROP, RADAR, and The Gentlemen highlighted an ongoing churn of affiliates seeking new revenue models.

What Organisations Must Do Now

In cyber defence,
hope is not a strategy.

Visibility is.

Defence in this environment demands depth, not just detection.

Security teams should:

Harden initial access points

Enforce multi-factor authentication, restrict RDP exposure, and monitor login anomalies.

Segment networks and deploy EDR

Contain impact zones and enhance visibility.

Secure backups

Keep encrypted, offline copies and test recovery regularly.

Track threat actors

Follow ransomware and access broker patterns relevant to your sector.

Invest in awareness

Train employees to recognise phishing, social engineering, and credential scams.

Monitor the dark web

Detect credential leaks or brand mentions early to reduce response lag.

How FalconFeeds.io Strengthens Defence

Threat intelligence is not about information — it's about anticipation.

The earlier you see the wave, the better you surf it.

FalconFeeds.io empowers enterprises and MSSPs in North America with actionable, high-fidelity intelligence.

Key capabilities include:

Real-time threat actor tracking:
Monitoring ransomware operators, access brokers, and data-stealer gangs.

Ransomware Leak Intelligence:
Mapping victim sectors and timelines from DLS portals.

Platform Monitoring:
Continuous observation of Telegram, Exploit, and Dark forums.

Initial Access Alerts:
Correlating sale listings with the digital footprint of target organisations.

IOC & Platform Intelligence:
Delivered via the FalconFeeds MCP Server, seamlessly integrating into SIEM and XSOAR pipelines.

With this intelligence layer, defenders gain the context and foresight needed to pre-empt attacks, triage incidents faster, and make decisions rooted in data — not panic.

Conclusion

A Battle of Adaptation

September 2025 reminded us that a drop in incident count does not equal a drop in threat. North America's cyber ecosystem remains under siege — not from volume alone, but from the sophistication of its adversaries.

As ransomware groups industrialise their operations, defenders must do the same. The future of cybersecurity in the region depends on intelligence-led decision-making, early detection, and an unwavering commitment to resilience.

Cybercriminals will continue to evolve. So must we — one alert, one feed, and one informed choice at a time.


FalconFeeds
Stay Ahead of Cyber Threats with FalconFeeds.io
FalconFeeds.io delivers real-time intelligence, automates monitoring, and reduces manual effort—helping organizations stay proactive against evolving cyber threats. With seamless integrations and an efficient alerting system, we empower teams to detect, analyze, and respond faster.
Don't just react—stay ahead. Strengthen your defenses with FalconFeeds.io.
Start Your Free 14-Day Trial Today
support@falconfeeds.io
Democratising Cybersecurity
www.falconfeeds.io