FalconFeeds

Democratising Cybersecurity
www.falconfeeds.io

North America Under Digital Siege

June 2025 Cyber Threat Intelligence Report

What's driving the sharpest surge in cyberattacks this year?

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.

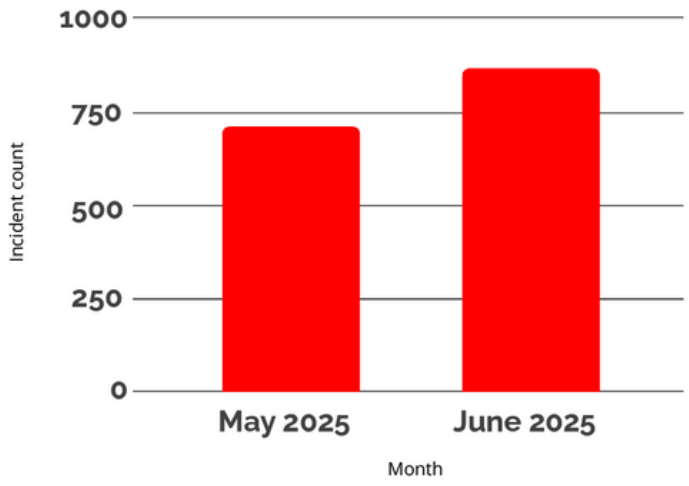
A Surge That Can't Be Ignored

North America's digital defenses crumble. Uncover the unprecedented surge in cyberattacks.

862 cyber incidents. A 21.9% spike in just one month.

North America witnessed a sharp escalation in cyber threats this June — **155 more attacks** than in May. The month closed with **862 recorded incidents**, signaling a relentless push by both ransomware operators and access brokers.

May 2025: 707 incidents
June 2025: 862 incidents
+21.9% increase



This growth coincides with two alarming developments:

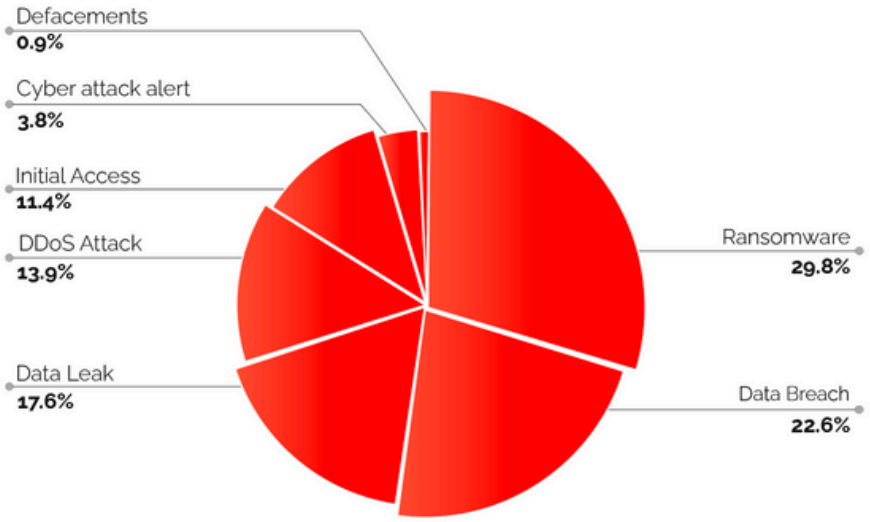
- A rise in ransomware-as-a-service (RaaS) campaigns
- A surge in initial access sales and dark web trading

The data tells a story of persistence, coordination, and bold expansion.

Anatomy of an Attack

What They're Doing

Breakdown of Attack Types (June 2025):



Beyond frequency: Cyberattacks are engineered for maximum, multi-stage disruption.

Dive into the anatomy.

Category	Count
Ransomware	257
Data Breaches	195
Data Leaks	152
DDoS Attacks	119
Initial Access	98
Cyberattack Alerts	33
Website Defacements	8

This pattern reveals a **layered approach:**

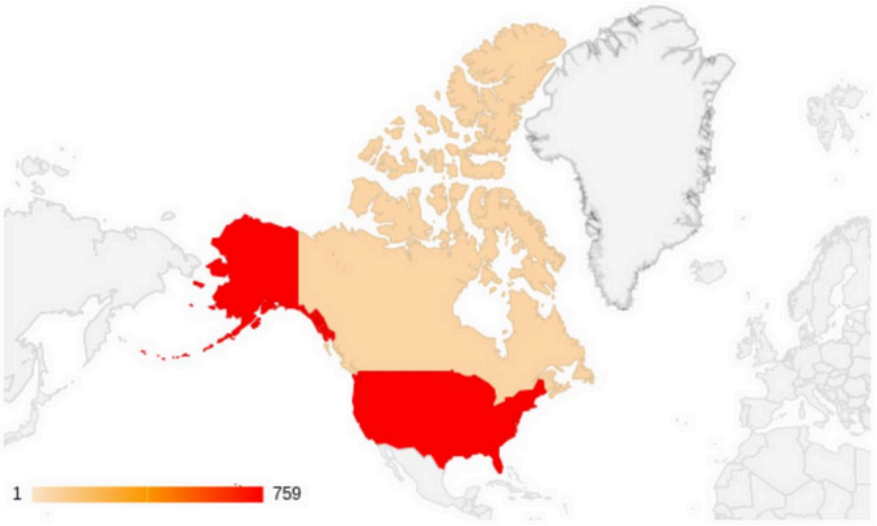
- Initial access → Breach → Encryption or leak
- Many attacks are not single events but **multi-stage operations**

Key Insight: Cyberattacks aren't just happening more often — they're being engineered for maximum disruption.

The Geographic Bullseye

Targeting Patterns by Country

USA at the bullseye with 88% of total attacks.



Country	Incidents
United States	759
Canada	70
Mexico	29
Dominican Republic	4
Belize	3
Costa Rica, Haiti, Honduras, Jamaica, and Panama	1 each

Why is America Ground Zero for cyberattacks?

The alarming strategic reasons revealed.

Despite regional diversity, the U.S. remains the digital epicentre — attracting nearly **9 out of every 10** attacks in North America.

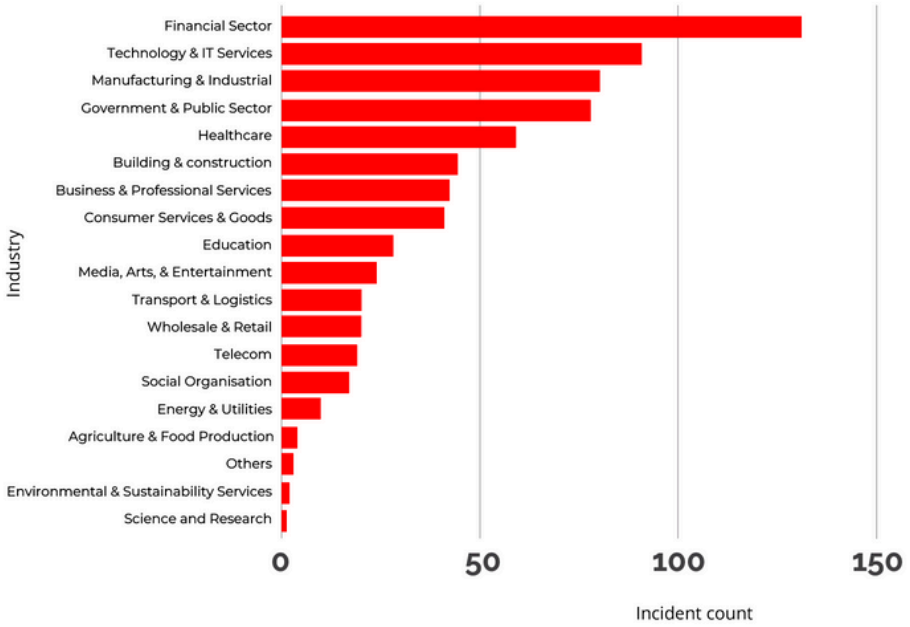
Why

- Global financial footprint
- Dense critical infrastructure
- High probability of ransom payments

Even mid-tier attackers are learning that big risk means bigger reward.

Who's Getting Hit — Sector Analysis

Top Industries Targeted in June:



Threat actors are hitting everything. Discover why every exploitable system is a target.

- Financial Services – 131 incidents
- Tech & IT – 91
- Manufacturing – 80
- Government – 78
- Healthcare – 59
- Construction – 44
- Professional Services – 42
- Consumer Goods & Services – 41

Additional sectors hit: Education, Media, Telecom, Energy, Logistics, Agriculture

Key takeaway:

Threat actors are no longer focused on single sectors. Their strategy is **diversification** — hit anything with exploitable systems and a high cost of downtime.

Where the Attacks Begin

Digital Infrastructure Under Siege

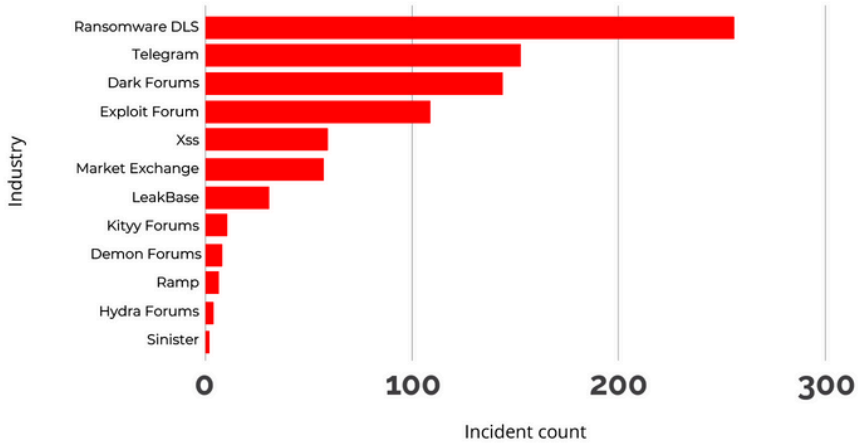
Threat actors aren't hiding.
They're organizing — everywhere

In June 2025, attackers operated across a mix of encrypted messaging apps, data leak portals, and dark web forums. Their activities ranged from **selling initial access** to **negotiating ransoms,** publishing **stolen data**, and broadcasting **campaign announcements.**

Dark forums, Telegram, leak sites. Uncover the unseen hubs of cybercrime coordination.

Top Platforms Used:

Platform Type	Incidents
Ransomware Leak Sites (DLS)	257
Telegram	153
Dark Forums	144
Exploit Forums	109
XSS Exploit Market	59
Market Exchange Sites	57
LeakBase	30
Kitty, Demon, Hydra, and Sinister	26 (total)



Telegram remains a vital nerve centre — enabling fast, anonymous coordination between ransomware affiliates and brokers.

Who's Waging War

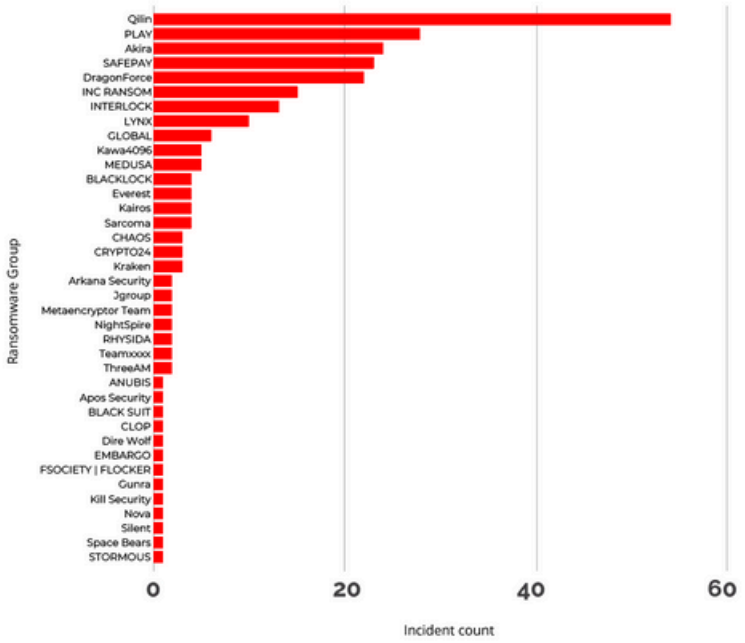
Top Ransomware Actors This Month

New contenders rise.

Discover the relentless groups maximizing ransomware payouts.

The North American threatscape was dominated by **repeat offenders** and rising contenders. At the center: **Qilin**, driving nearly 1 in 5 ransomware attacks this June.

Ransomware Group	Incidents
Qilin	54
PLAY	28
Akira	24
SAFEPAY	23
DragonForce	22
INC RANSOM	15
INTERLOCK	13
LYNX	10



Other notable mentions: **MEDUSA, GLOBAL, Everest, Kairos, Sarcoma** — each operating in low-to-mid volumes, but no less impactful.

These groups aren't just encrypting data — they're leveraging double extortion, dedicated leak sites, and public shaming tactics to maximize payouts.

Where They Struck

Geographic Reach of Ransomware

The U.S. remains the bulls-eye.

The US remains ransomware's bullseye. Discover its relentless geographic reach.

With **232 of 257 ransomware attacks**, the country faces relentless targeting. Even Canada, with 18 incidents, and Mexico with 3, remain active battlefields.

Country	Ransomware Incidents
USA	232
Canada	18
Mexico	3
Dominican Republic, Haiti, Jamaica, Panama	1 each

Attacks are expanding slowly across the Americas, but **North America remains the financial heart of ransomware campaigns.**

Who's Vulnerable

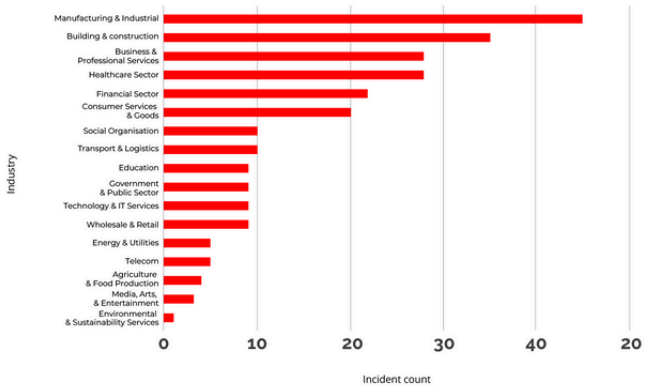
Sector-Wise Ransomware Impact

No sector is safe. Ransomware operations in June hit **every layer** of North American society — from factories and banks to schools and non-profits.

Ransomware isn't selective. Discover the systematic impact across every sector.

Most Affected Industries:

Industry	Incidents
Manufacturing & Industrial	45
Building & Construction	35
Business & Professional Services	28
Healthcare	28
Financial Services	22
Consumer Goods & Services	20
Education & Social Organisations	10+ each
Energy, Media, Retail, Telecom	3–9



Why?

These sectors have:

- Weak segmentation
- Valuable data
- High-pressure operations that make downtime costly

Conclusion Ransomware isn't selective — it's systematic.

Final Takeaways

What June 2025 Taught Us

Ransomware, Telegram, leak sites. Uncover the evolving control rooms of cybercrime.

The threat landscape this month wasn't just about volume. It was about **coordination, speed, and intent.**

- **Ransomware remains the apex threat** — not just for damage, but visibility.
- **Initial access listings** are accelerating attacks. One sale = dozens of victims.
- **Telegram & leak sites** have evolved into real-time control rooms for cybercrime.
- **Healthcare, industrial, and public sector** targets remain in constant crosshairs.

Bottom line:	Attackers are faster. Louder. More organized.

What You Can Do

Strategic Security Recommendations

Stop reacting.
Start anticipating. Essential strategies to outmaneuver the next cyberattack.

Defending your org means thinking like an attacker.
Start with visibility.

- **Monitor** real-time posts from leak sites, Telegram, and forums → Tools like **FalconFeeds.io** are essential.
- **Deploy** EDR & XDR tools → Detect lateral movement, isolate ransomware patterns.
- **Harden RDP, VPNs, Exchange, Fortinet** → Patch known CVEs before threat actors exploit them.
- **Segment your network** → Contain breaches before they spiral.
- **Back up everything** — and test recovery often → Assume encryption. Plan recovery.
- **Train your people** → Phishing and social engineering are still the #1 entry points.

The Final Word

June 2025 defined it. Uncover why adaptive intelligence is your only way forward.

June 2025 was a defining moment.
Not just because of how many attacks landed — but how quickly they evolved.

Ransomware groups aren't just coding malware.
They're building economies. Forging alliances. Learning faster than defenders adapt

The only way forward? Intelligence-led defence.

FalconFeeds.io delivers real-time, high-fidelity CTI, built for defenders who can't afford to be late.

Try FalconFeeds.io free for 14 days.


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