FalconFeeds

Democratising Cybersecurity
www.falconfeeds.io

European Cyber Threat Landscape

September 2025

Tracking Emerging Threats, Ransomware Campaigns, and Targeted Cyber Activity Across Europe

The Deepest Watch on the Darkest Web

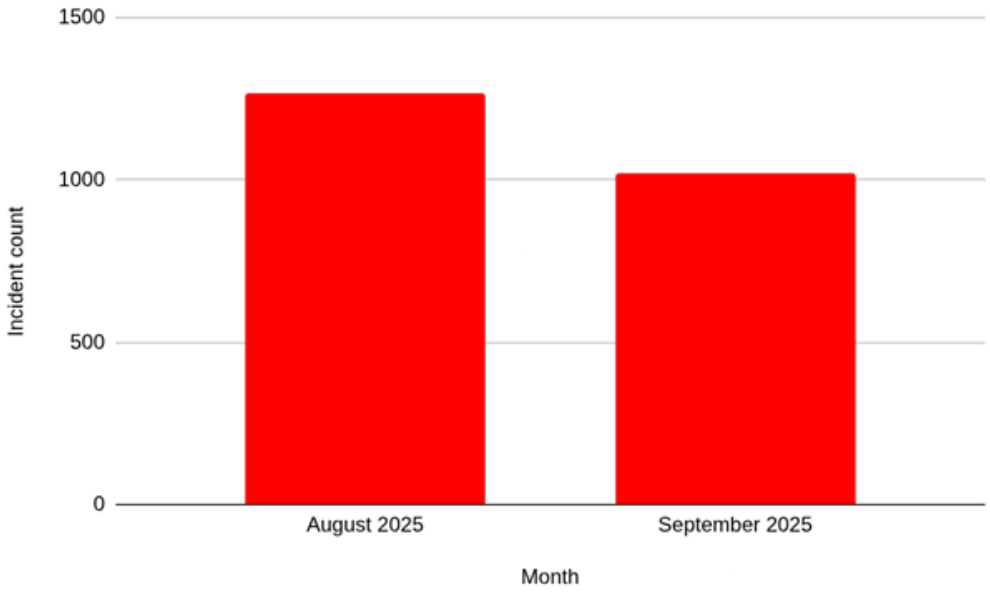
FalconFeeds.io delivers the largest real-time monitoring of deep and dark web activity—from ransomware gangs to Telegram dumps and access marketplaces.

Executive Summary

Think Box:

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.

Even as overall incident volume drops, targeted attacks on high-value sectors can cause disproportionate disruption. A small number of attacks can have large-scale impact.



Critical sectors, including government, manufacturing, and transportation, faced sustained pressure from cybercriminals, while ransomware groups like Qilin, Akira, and Everest continued to disrupt industrial and public infrastructure.

This report breaks down threat types, geographic impact, industrial targeting, attacker infrastructure, and ransomware campaigns, offering actionable insights for cybersecurity teams and decision-makers.

September at a Glance

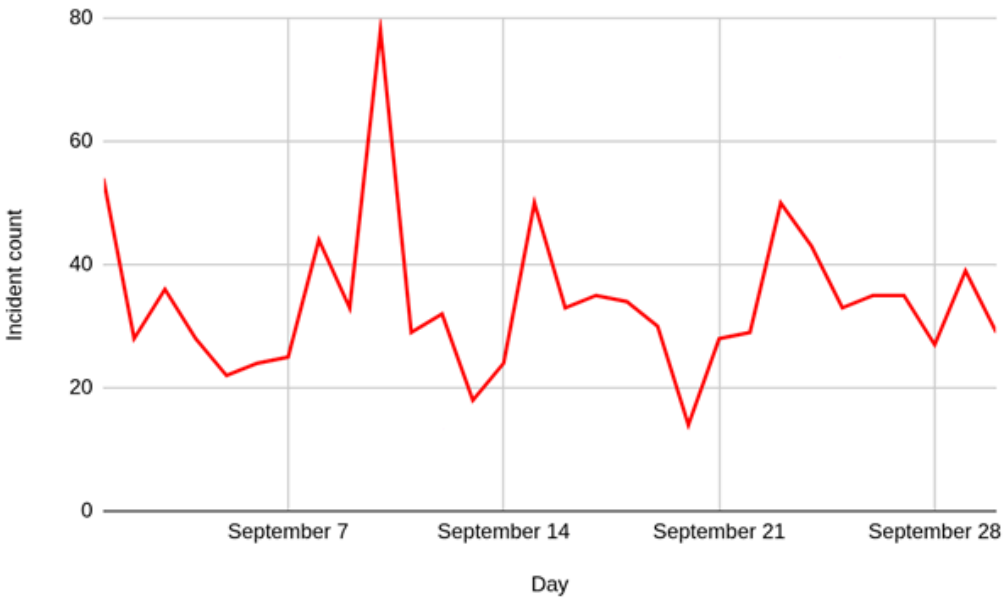
Point to Ponder:

Peaks in activity often align with major vulnerabilities or geopolitical events. Awareness of these patterns helps teams anticipate surges.

September saw a mix of persistent low-level campaigns and sharp spikes in activity:

- **Peak days:**
  September saw a mix of persistent low-level campaigns and sharp spikes in activity:

- **Average day:**
  33–35 incident



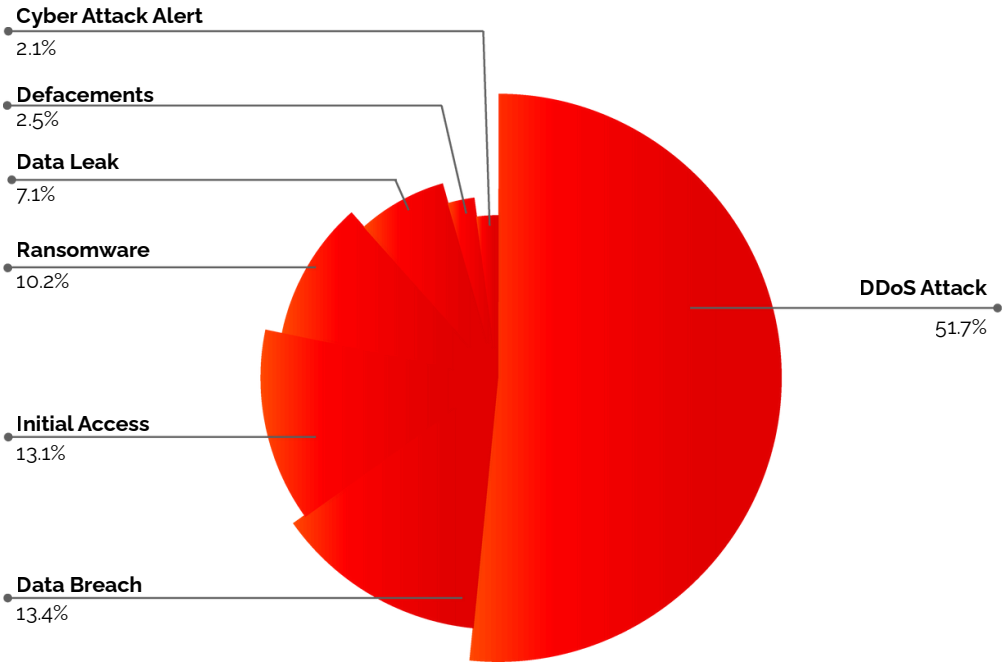
These peaks suggest coordinated campaigns exploiting either recent vulnerabilities or seasonal attack opportunities, while lower-volume days reflect ongoing reconnaissance, initial access sales, and low-intensity disruption.

Category-Wise Threat Landscape

Risk Radar:

DDoS attacks may not steal data but can paralyse services, causing reputational damage and economic loss.

DDoS attacks dominated September, accounting for **527 incidents** (over 50% of total), targeting government portals and transport systems.



Other key categories included:

Data breaches:
137 incidents, often involving customer, employee, or corporate data.

Initial access listings:
133 incidents, showing increasing specialization among cybercriminals selling network footholds.

Ransomware attacks:
104 incidents, using encryption and extortion to maximize impact.

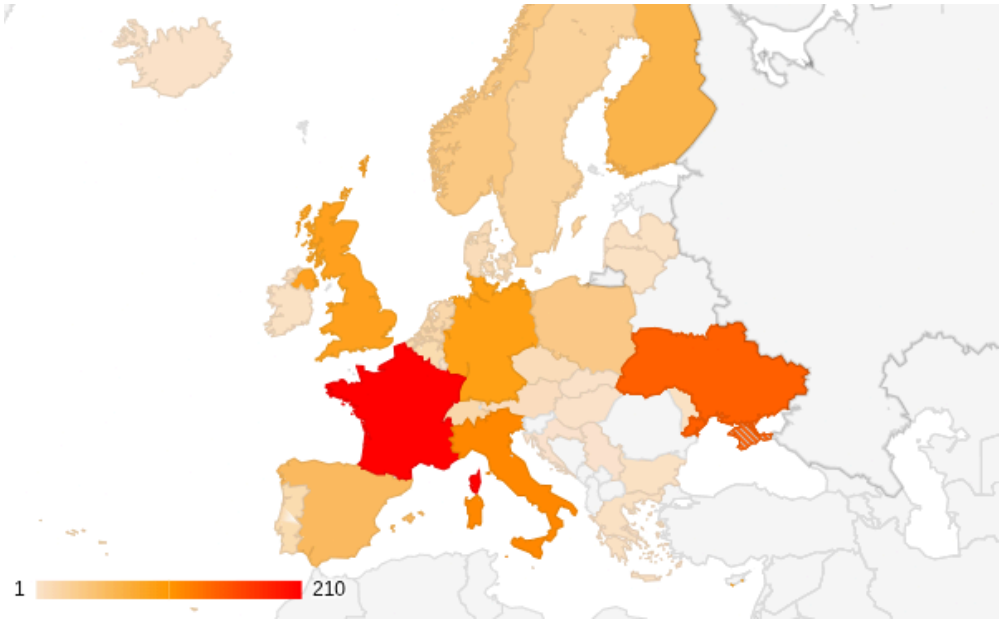
Other attacks:
Defacements, general alerts, and data leaks made up the remainder.

Country-Level Distribution

Quick Take:

Even countries with fewer incidents should remain vigilant; targeted attacks can be catastrophic regardless of total numbers.

France (210 incidents), Ukraine (145), and Italy (116) were the hardest hit, reflecting their geopolitical relevance and dense digital infrastructure.



Other affected countries:

Germany: 95 incidents

United Kingdom: 90 incidents

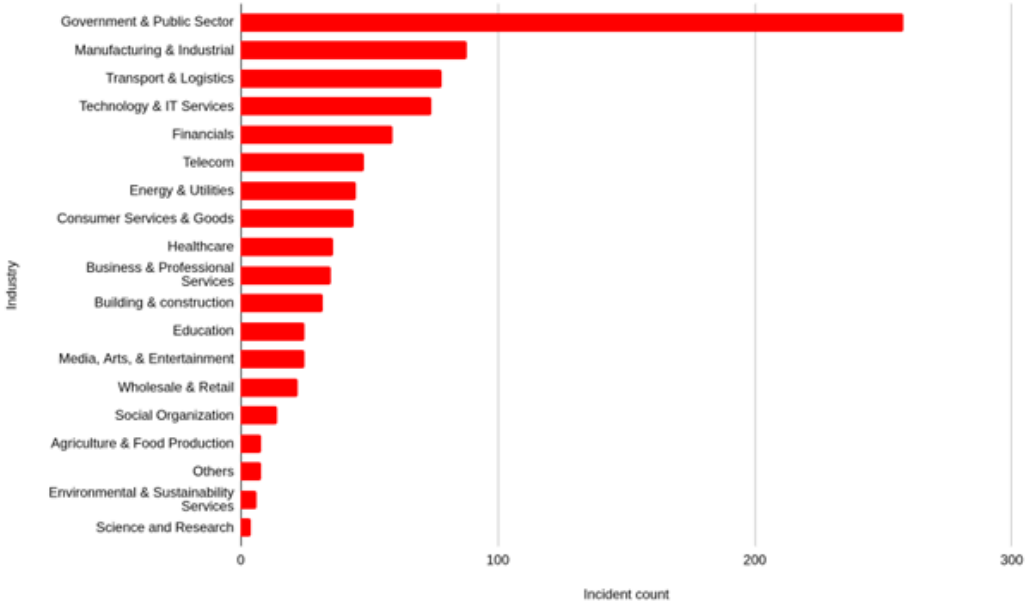
Finland: 65 incidents, showing a notable regional spike

The broader Nordic, Baltic, and Central European nations saw consistent activity, underlining that cybercriminals target networks continent-wide, not just high-profile countries.

Industry-Wise Impact

Think Box:

Attackers employ a multi-sector strategy, leveraging each breach to maximize profit, influence, and disruption potential.



Government & Public Sector:
258 incidents, top target for espionage and disruption.

Manufacturing & Industrial:
88 incidents, vulnerable to operational disruptions and supply chain attacks.

Transport & Logistics:
78 incidents, highlighting potential for disruption of critical infrastructure.

Technology & IT Services:
74 incidents

Financial Institutions:
59 incidents

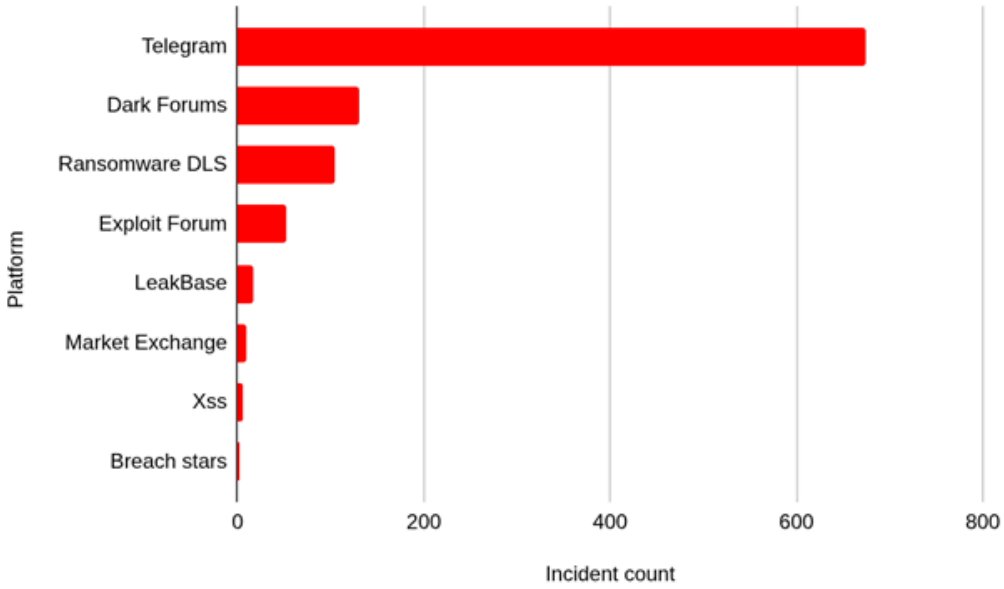
Other notable sectors:
Telecom (48), Energy & Utilities (45), Healthcare (36), Consumer Services & Goods (44).

Platform and Infrastructure Analysis

Point to Ponder:

Monitoring Telegram and dark web activity provides early warning for potential attacks, giving defenders critical lead time.

Threat actors relied heavily on **Telegram (675 incidents)** for coordination, data leaks, and attack announcements.



Dark Web Forums:
131 incidents, serving as marketplaces for access sales, data leaks, and exploit trading.

Ransomware Dedicated Leak Sites (DLS):
Linked to all 104 ransomware incidents.

Traditional exploit markets like **Exploit Forum, LeakBase, Market Exchange** saw niche activity.

Ransomware Operations Overview

Think Box:

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

Ransomware remained a major threat:

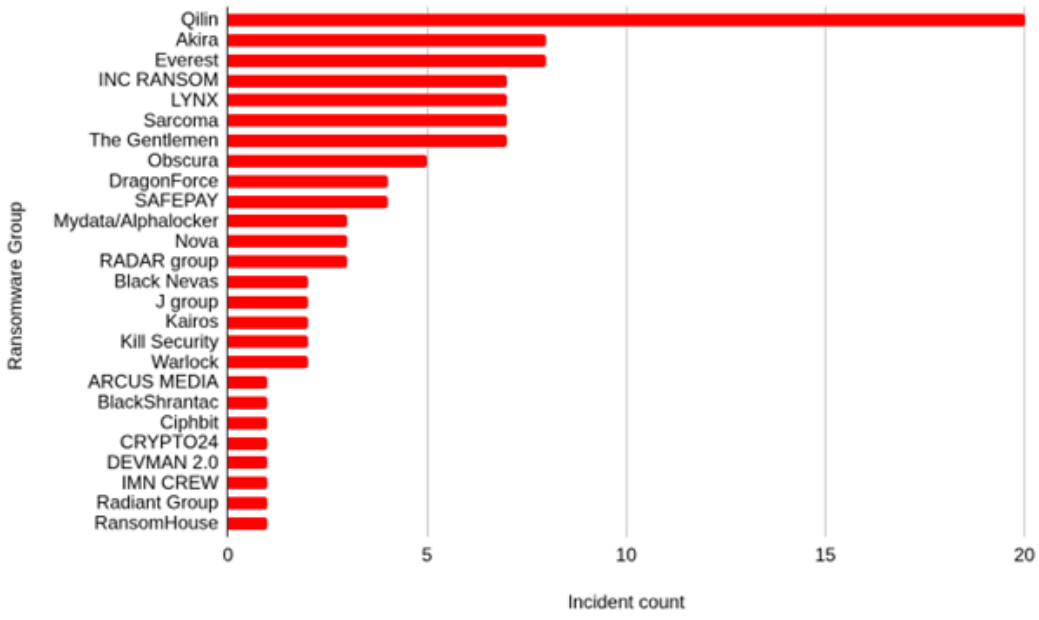
Qilin: 20 attacks

Akira: 8 attacks

Everest: 8 attacks

INC RANSOM: 7 attacks

Other active groups: **LYNX, Sarcoma, The Gentlemen, DragonForce.**



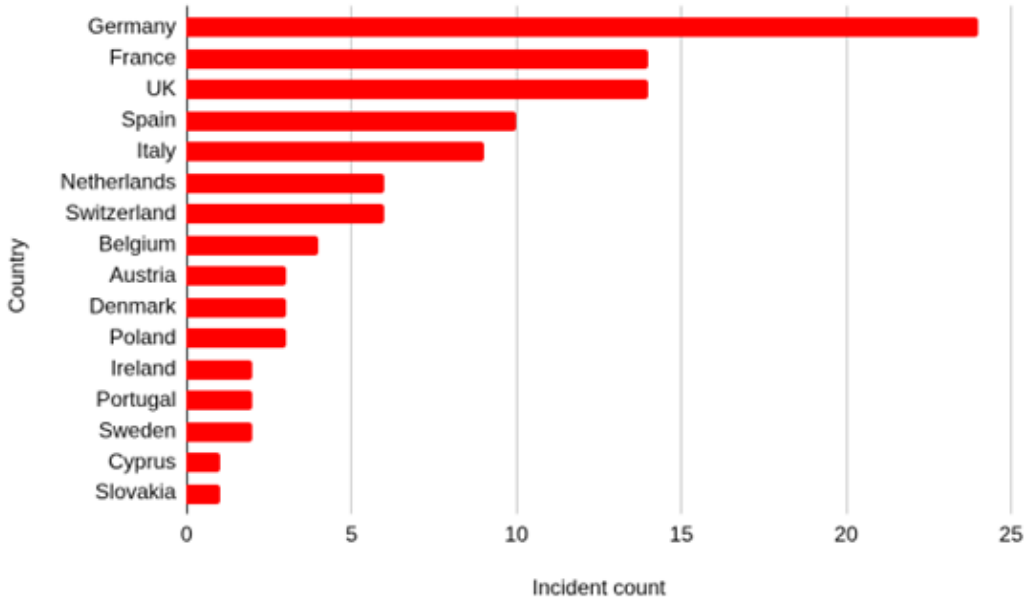
Country-level ransomware:

Germany: 24 attacks

France & UK: 14 each

Spain: 10

Italy: 9



Sector Focus:

Risk Radar:

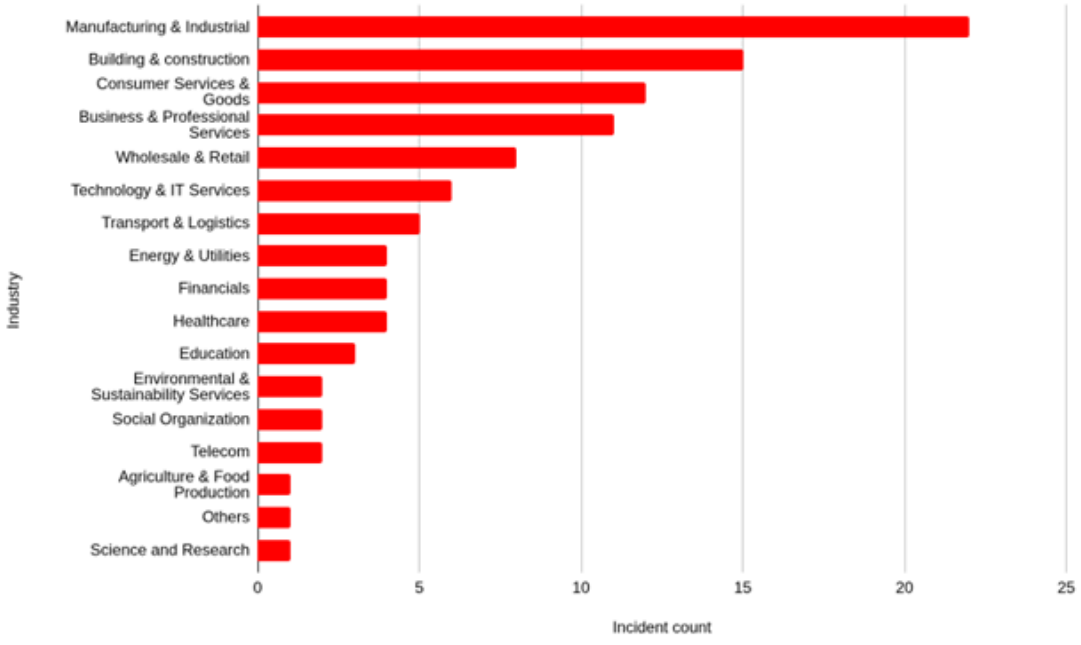
The spread of attacks across varied industries indicates a fragmented ransomware landscape, making it harder for defenders to predict which sector may be hit next.

Manufacturing & Industrial – 22 attacks
Continued to be the most targeted due to high operational dependency and quick-pressure extortion potential.

Building & Construction – 15 attacks
Project-based workflows and vendor dependencies make disruption highly costly, attracting attackers.

Consumer Services & Goods – 12 attacks
Remains an attractive target due to access to consumer data, payment information, and brand reputation leverage.

Other Sectors Impacted:
Healthcare, Technology, Energy, and Education faced smaller but notable clusters of attacks, showing a broad targeting pattern rather than concentrated focus.



Key Observations

DDoS Dominance:
Non-invasive disruptions increasingly favored.

Rise in Access Brokerage:
Specialization in selling access to enterprise networks is growing.

Diversified Ransomware Ecosystem:
Over 25 active groups in Europe; no single dominant actor.

Telegram's Continued Role:
Primary hub for coordination, leaks, and attack announcements.

Recommendations

Strengthen Network Segmentation:
Limit lateral movement post-compromise.

Adopt Anti-DDoS Mechanisms:
Invest in mitigation tools and CDNs.

Monitor Access Sale Listings:
Detect unauthorized access early via threat intel.

Implement Zero Trust Architecture:
Enforce identity verification across all access points.

Accelerate Patch Management:
Target VPNs, RDPs, and legacy systems.

Employee Awareness Training:
Phishing, credential theft, and social engineering prevention.

How FalconFeeds.io Supports Organizations

Point to Ponder:

Staying ahead of threats requires **proactive intelligence,** not just reactive defence.

FalconFeeds.io empowers SOC teams with **actionable intelligence:**

Dark Web & Forum Monitoring:
Telegram, Exploit, and Dark forums

Active Ransomware Tracking:
Real-time DLS updates and group activity analysis

Initial Access Broker Detection:
Prevent exploitation of unauthorized access

Industry Mapping:
Prioritize sector-specific defenses

Automated Alerts:
Seamless integration with SIEM and XSOAR tools

Conclusion

Europe's cyber landscape in September 2025 shows a **shifting but persistent threat environment:**

- Incident volume dropped but complexity and variety increased.
- Government, manufacturing, and transport remain under pressure.
- Distributed ransomware groups and dark web infrastructure amplify risks.

Proactive monitoring, sector-specific defences, and collaboration with specialised platforms like FalconFeeds.io are essential to staying ahead of evolving cyber threats.


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