FalconFeeds

Democratising Cybersecurity
www.falconfeeds.io

# Europe Threat Intelligence Report

## Cyber Attacks Analysis

**November 1 – 30, 2025**

Europe's cyber front is shifting from silent breaches to sustained disruption. This report uncovers where attacks are rising, who is being targeted, and how threat actors are coordinating in real time.

# 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

Europe entered November 2025 under sustained cyber pressure.

The region recorded **926 cyber incidents**, rising from **861 in October**, a **7.5% month-over-month** increase. While the growth was moderate, the **nature of attacks shifted sharply toward disruption.** Distributed Denial of Service (DDoS) campaigns dominated activity, accounting for **more than half of all recorded incidents**, signalling coordinated efforts to interrupt public services rather than quietly compromise networks.

Alongside disruption, **ransomware, data breaches, and access brokerage** continued at scale, reinforcing a hybrid threat model where hacktivist pressure and criminal monetisation operate in parallel. Government bodies, critical infrastructure operators, and transport-linked organisations were the most impacted, placing Europe's public-facing systems squarely in the crosshairs.

Operational coordination and claims were overwhelmingly routed through **Telegram**, confirming its role as the central command-and-propaganda channel for Europe-focused threat actors.

# Incident Volume & Monthly Trend

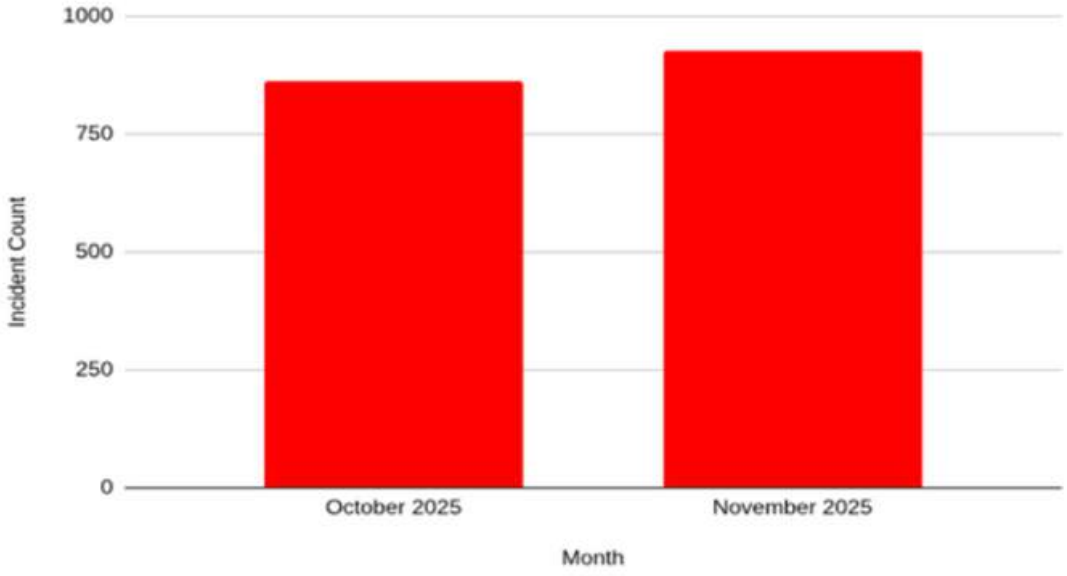
**Think Box**

This is an active campaign, not a spike.

Are you tracking how long attacks persist, or just how often they appear?

- **October 2025:** 861 incidents
- **November 2025:** 926 incidents

November's increase was not driven by isolated spikes, but by **persistent, high-volume pressure** across the month. This pattern points to **extended campaign execution**, not reactive retaliation.




Key drivers included:

- Escalated DDoS campaigns, particularly against government and transport systems
- Steady ransomware operations, avoiding dramatic peaks but maintaining continuity
- Ongoing access brokerage and data exposure, feeding downstream attacks

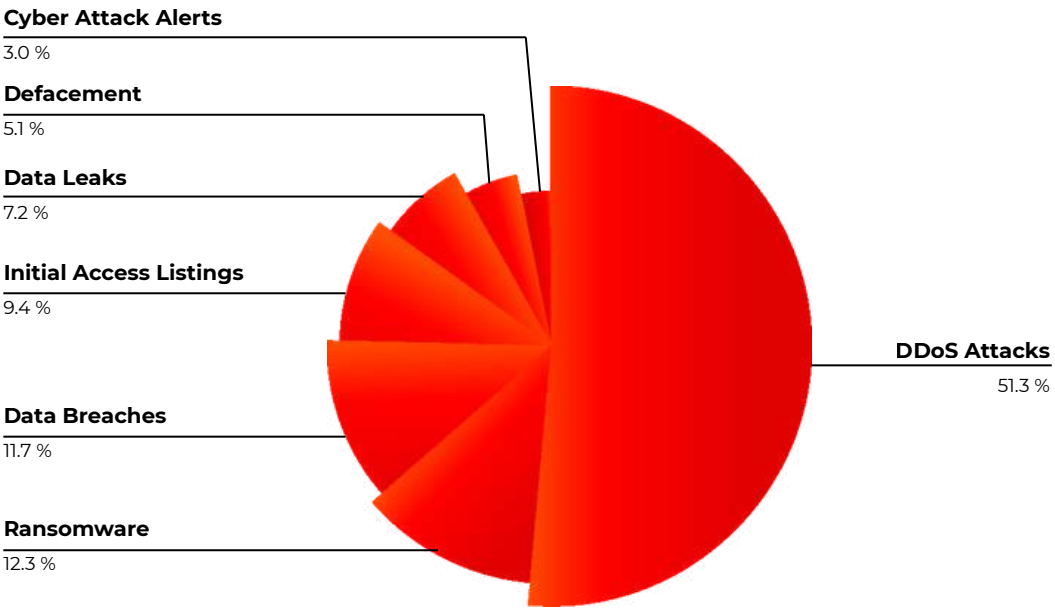
# Category-Wise Threat Landscape

**Point to Ponder**

When DDoS dominates the headlines, are teams missing the quieter signals of access sales, data theft, and monetisation already in motion?

Europe's November threat profile was defined by service disruption and extortion:

- **DDoS Attacks:** 475
- **Ransomware:** 114
- **Data Breaches:** 108
- **Initial Access Listings:** 87
- **Data Leaks:** 67
- **Defacement:** 47
- **Cyber Attack Alerts:** 28




DDoS alone represented **over 51%** of all activity—underscoring a strategic preference for visibility and disruption. Yet the combined weight of ransomware, leaks, and access sales confirms a **fully active cybercriminal economy running alongside hacktivism.**

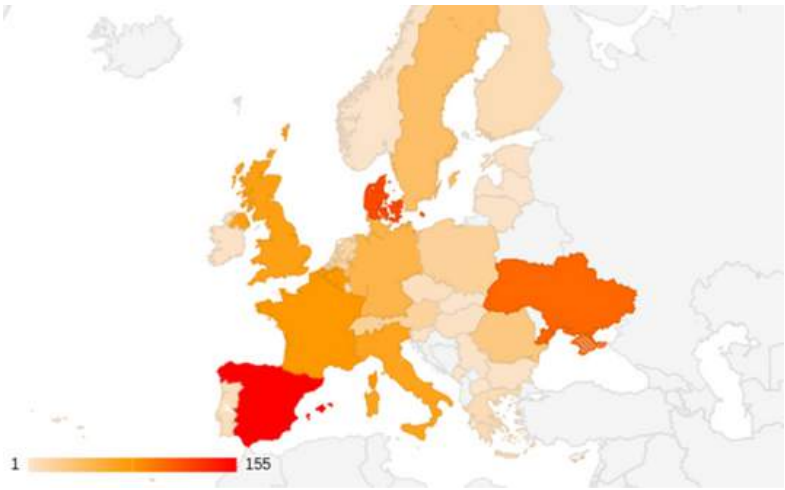
# Country-Wise Distribution

**Think Box**

Campaigns bleed across borders. If pressure concentrates on one country, are neighbours already adjusting defenses—or waiting to become the next target?

The most targeted European countries in November:

- **Spain: 155**
- **Denmark: 119**
- **Ukraine: 103**
- **France: 78**
- **Belgium: 77**
- **United Kingdom: 70**
- **Italy: 67**
- **Germany: 50**
- **Sweden: 39**
- **Romania: 29**




Additional activity spanned Switzerland (21), Poland (20), Austria (18), Netherlands (17), Finland (10), Greece (9), Portugal (7), and others.

Southern and Western Europe absorbed the heaviest pressure, while **Ukraine's continued presence** reflects sustained geopolitical targeting. Elevated activity in **Spain and Denmark** suggests focused disruption against public-facing infrastructure.

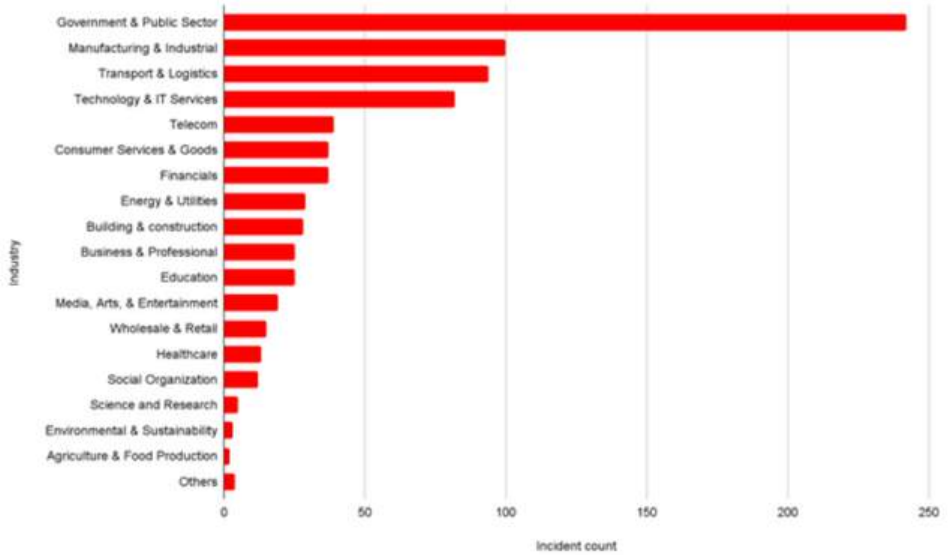
# Industry-Wise Impact

**Point to Ponder**

Are your sector controls built for real downtime, or only written for audits?

Most affected sectors:

- **Government & Public Sector:** 242
- **Manufacturing & Industrial:** 100
- **Transport & Logistics:** 94
- **Technology & IT Services:** 82
- **Telecom:** 39
- **Consumer Services & Goods:** 37
- **Financial Services:** 37
- **Energy & Utilities:** 29
- **Building & Construction:** 28
- **Business & Professional Services:** 25
- **Education:** 25




Other affected industries included Media (19), Retail (15), Healthcare (13), Social Organisations (12), and Research (5).

The data highlights a **dual targeting strategy:**

- **Disruption-first** attacks on government, transport, telecom, and energy
- **Extortion-driven** ransomware against manufacturing, construction, and professional services

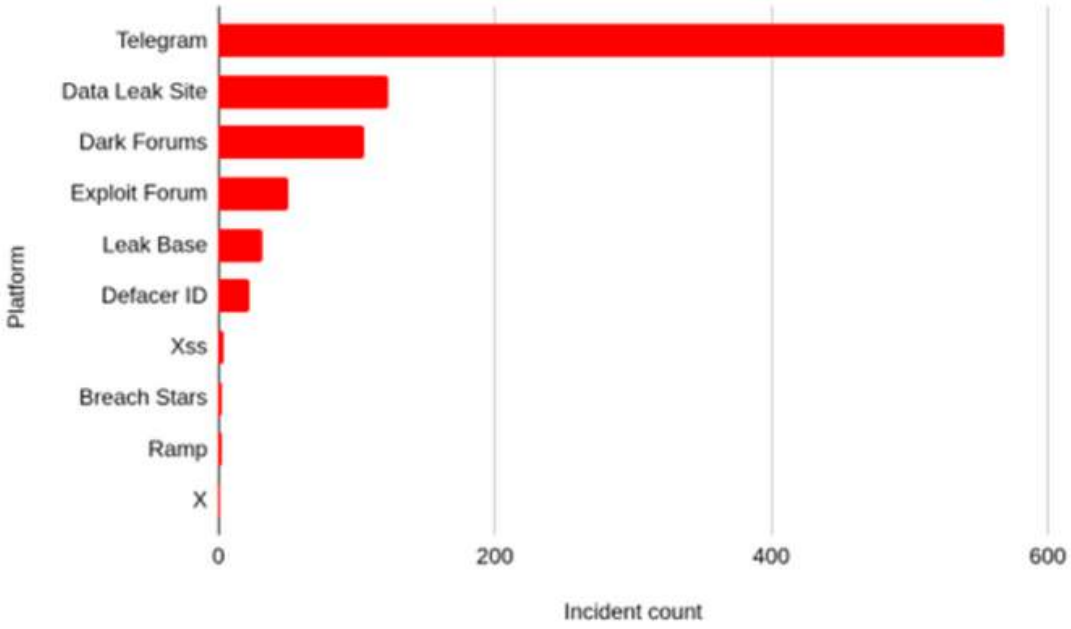
# Platform & Underground Ecosystem Activity

**Think Box**

If most attacks surface on Telegram first, are your teams monitoring it in real time—or learning after damage is done?

Threat coordination and disclosure channels:

- **Telegram:** 568
- **Data Leak Sites:** 123
- **Dark Forums:** 105
- **Exploit Forums:** 51
- **LeakBase:** 32
- **Defacer ID:** 22




Telegram functioned as the **central nervous system—** hosting coordination, claims, and amplification.

Data Leak Sites sustained extortion pressure, while forums supported access sales and vulnerability trade.

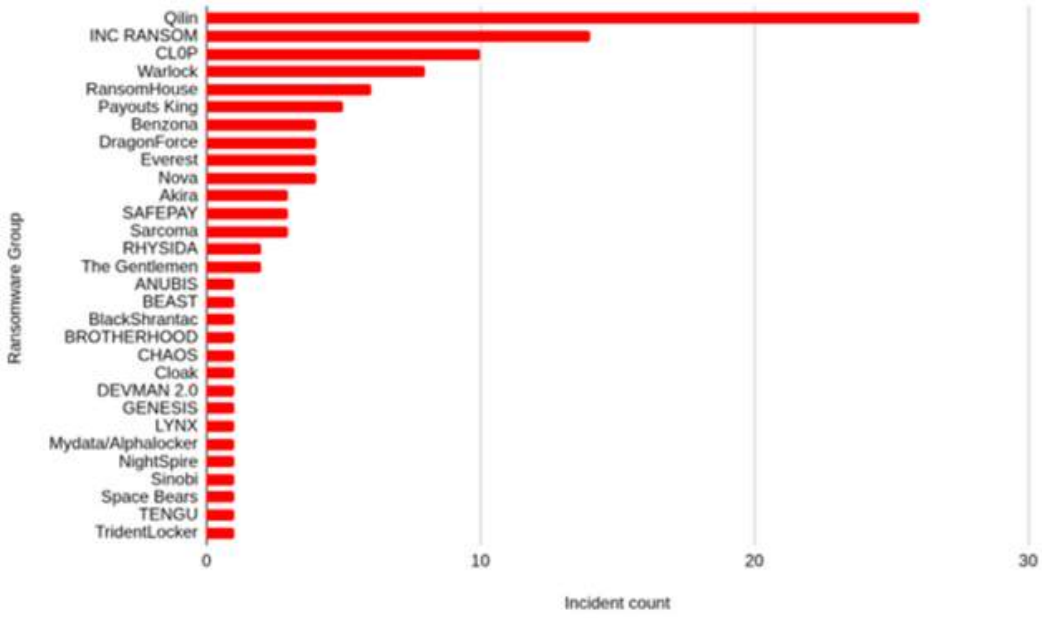
# Ransomware Group Landscape

**Point to Ponder**

When attackers change brands often, how reliable is name-based threat tracking?

Most active groups:

- **Qilin:** 26
- **INC RANSOM:** 14
- **CL0P:** 10
- **Warlock:** 8
- **RansomHouse:** 6
- **Payouts King:** 5




Mid-tier activity included Benzona, DragonForce, Everest, Nova (4 each), with a long tail of single-digit operators.

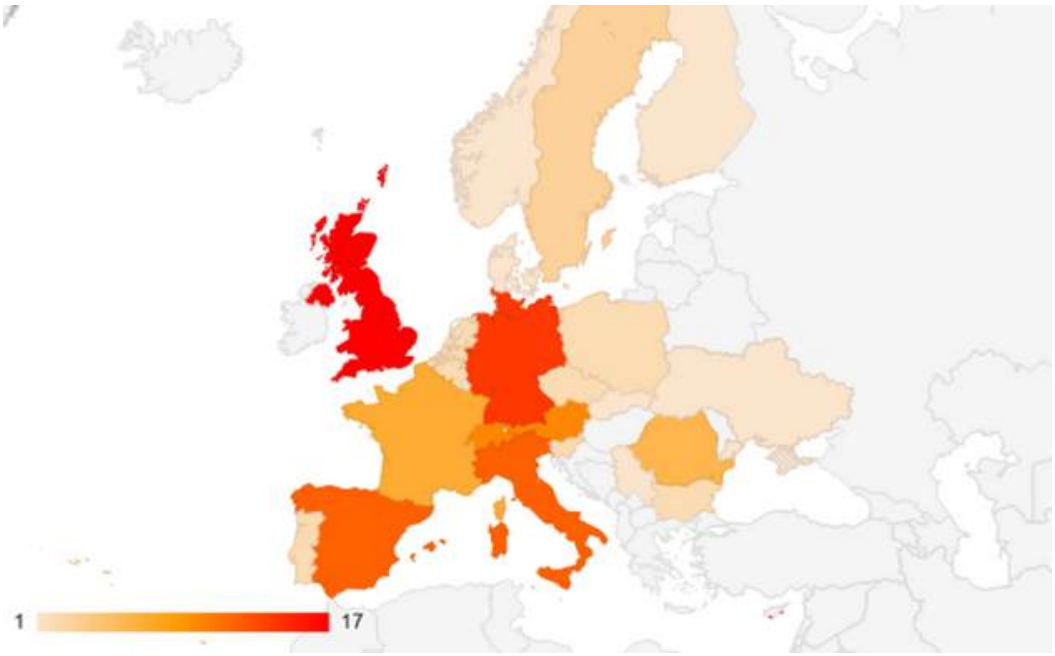
No group dominated. Europe's ransomware ecosystem remains **fragmented, competitive, and affiliate-driven.**

# Ransomware-Affected Countries

**Think Box**

Are ransomware preparedness metrics aligned with actual victim distribution?

- **United Kingdom:** 17
- **Germany:** 14
- **Italy:** 12
- **Spain:** 12
- **Austria:** 10
- **Switzerland:** 10



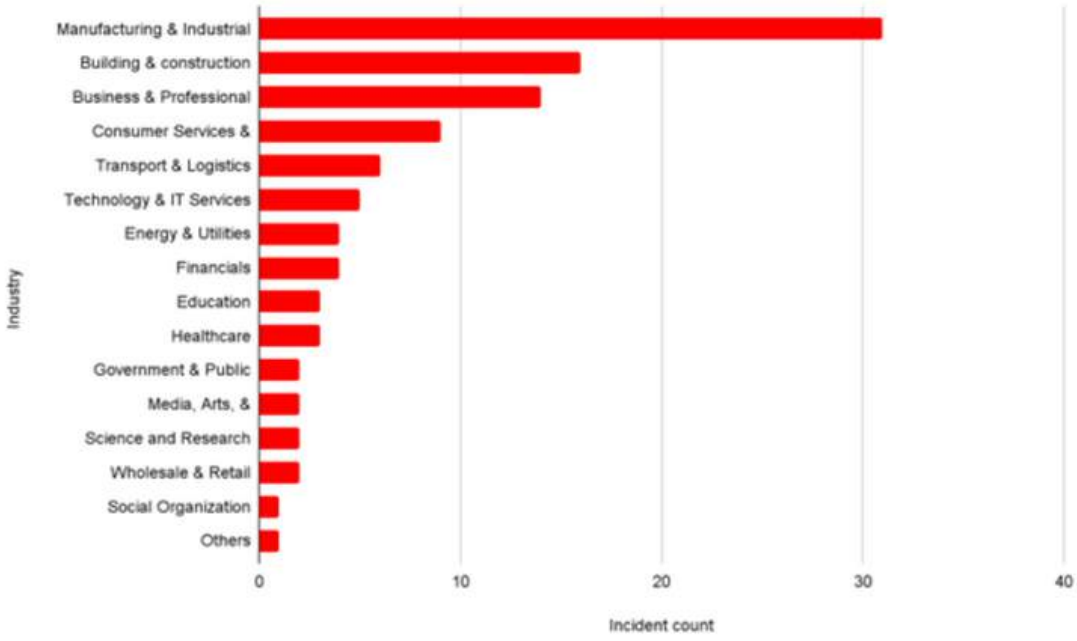

Additional cases spanned France, Romania, Sweden, Belgium, the Netherlands, Poland, Portugal, and others.

# Ransomware-Affected Industries

**Point to Ponder**

These targets aren't random. Why are the same industries still exposed month after month?

- **Manufacturing & Industrial:** 31
- **Building & Construction:** 16
- **Business & Professional Services:** 14
- **Consumer Services & Goods:** 9
- **Transport & Logistics:** 6
- **Technology & IT Services:** 5
- **Energy & Utilities:** 4
- **Financial Services:** 4




Attackers continued to favour industries where **downtime equals leverage.**

# Key Observations

- DDoS dominated, exceeding **50%** of all incidents
- Government and transport sectors faced sustained pressure
- Ransomware remained active but decentralised
- Telegram emerged as the primary operational hub
- Access brokerage continued feeding downstream attacks

# Recommendations

- Strengthen **DDoS resilience** through scrubbing, WAF tuning, and ISP coordination
- Prioritise **government and transport infrastructure protection**
- Reinforce ransomware defences with **immutable backups and EDR**
- Monitor **Telegram, Data Leak Sites, and Exploit Forums** for early signals
- Apply **sector-specific controls** for manufacturing, energy, and logistics

# How FalconFeeds.io Can Help

FalconFeeds.io delivers **real-time, actionable intelligence** for European defenders by:

- Monitoring **Telegram, Dark Web, and closed forums**
- Tracking **active ransomware campaigns and DLS activity**
- Identifying **initial access brokers** before compromise
- Mapping **threat actors to industries and regions**

This enables **earlier detection, faster prioritisation, and intelligence-led defence** across Europe.

# Conclusion

Europe's November 2025 cyber landscape reflects a **shift toward sustained disruption**, supported by parallel criminal operations. DDoS campaigns, ransomware extortion, and access brokerage now operate as a **blended threat** model, pressuring public trust, economic continuity, and national resilience.

In this environment, **reactive security is insufficient.** Only proactive, intelligence-driven defence, grounded in underground visibility and sector-specific readiness, can counter the next phase of escalation.