TLP:CLEAR

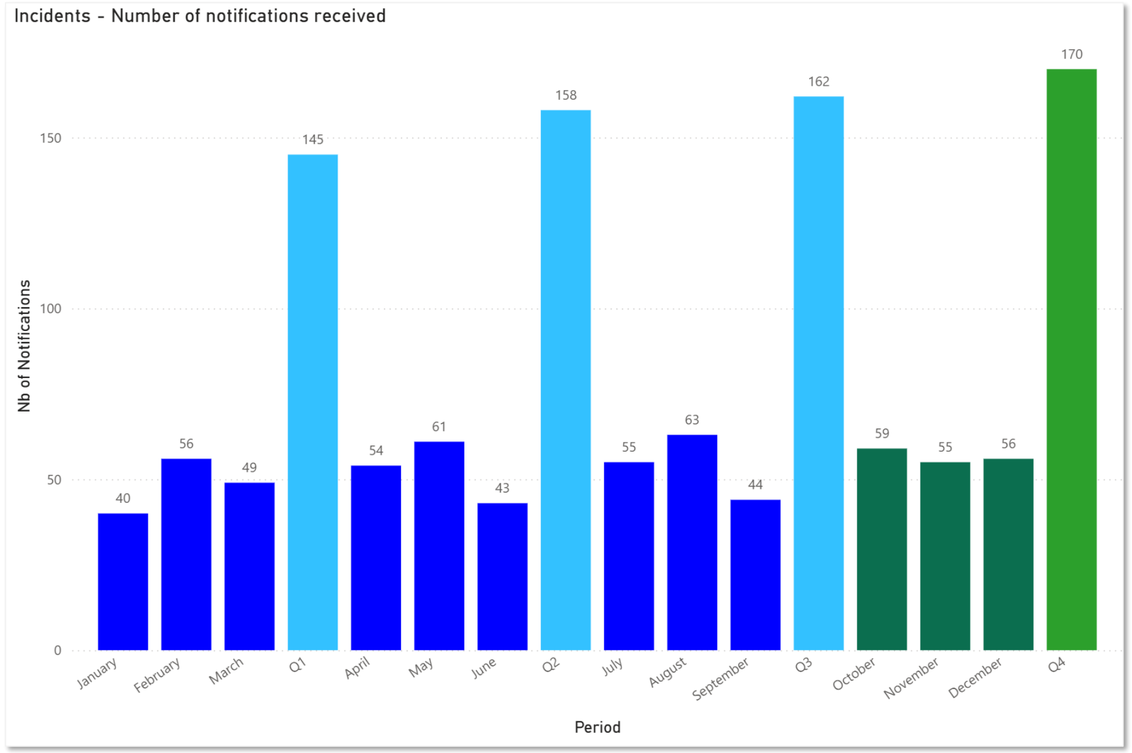
The cyber threat landscape in Belgium

Quarterly Cyber Threat Report Q1 2026 – 22 April 2026

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

A (rather) stable threat landscape

- The number of incidents reported to the CCB **continues to grow**.
- Especially true for **cyber-related incidents**: 149 (Q4 2025) and 154 (Q1 2026)
- A roughly **equal number of NIS2 and non-NIS2 entities** reported incidents this past quarter.



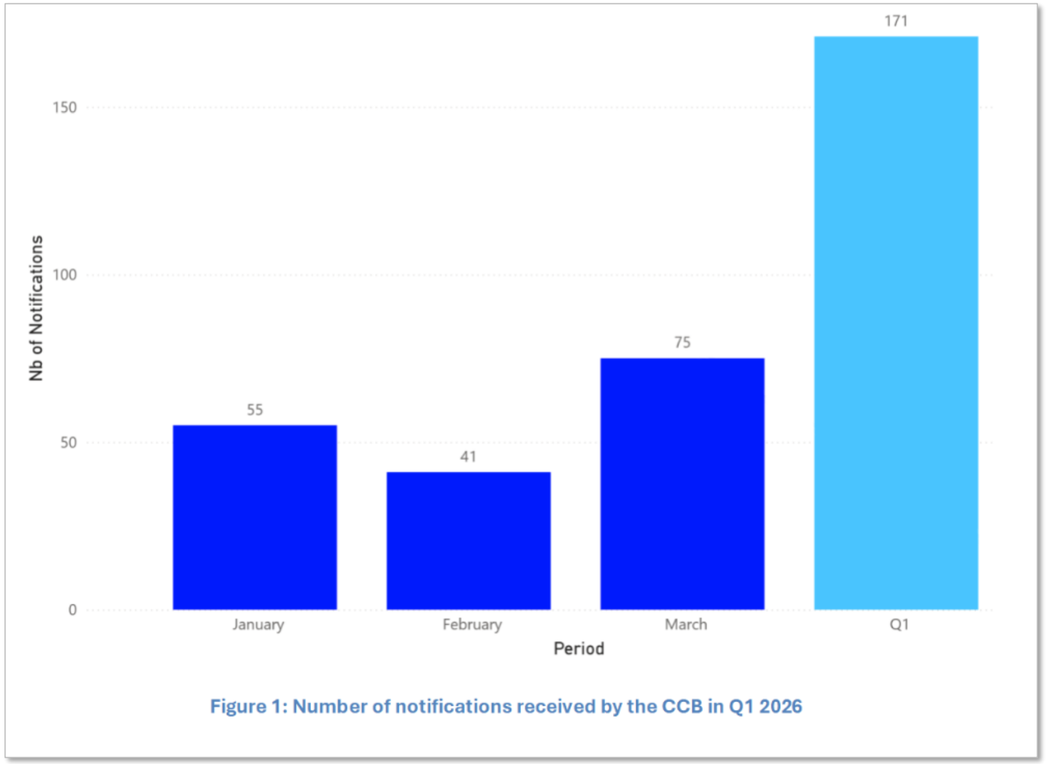
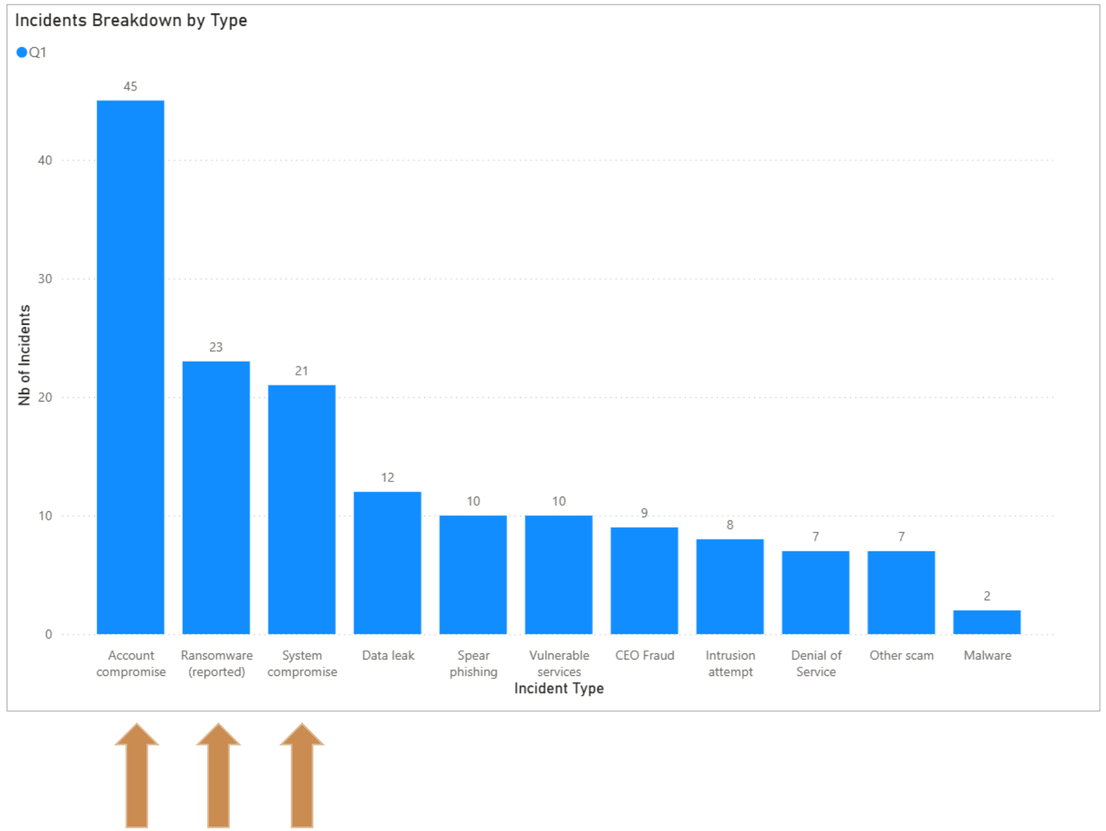


Figure 1: Number of notifications received by the CCB in Q1 2026

Account compromise and ransomware remain the top threats in Belgium

CENTRE FOR CYBERSECURITY BELGIUM

- **Threat 1: account compromise**
  - Closely related to phishing and CEO fraud in Belgium
- **Threat 2: ransomware**
  - Persistent threat
  - A combination of well-established and emerging groups
- **Threat 3: system compromise**
  - Episodic, linked to waves of vulnerability exploitation
- Public administration & healthcare report the most incidents.
- Threat actors appear to target in particular **essential service providers**. This trend is observed in other European countries.



Surprise, surprise

- No DDoS from hacktivists this quarter!

- But likely just a **temporary** shift in threat actor attention.

Source: https://imgflip.com/i/ap9a2t

How attacks were initiated

CENTRE FOR CYBERSECURITY BELGIUM

- **Malware**
  - **Infostealers, loaders, RATs**
  - Multifactor authentication remains a key defense
  - **Enablers** that come before, or along with other malware
- **Phishing**
  - Invoice and e-fraud schemes, data theft and data extortion
- New variants of **ClickFix**:
  - CrashFix (NexShield), InstallFix (fake Claude Code AI Assistant)
  - Connect with the CCB on MISP!
- **Supply chain** attacks
  - Attacks are faster and more mature as organisations' exposure grows
  - Shift **upstream**

Vulnerabilities that have been bugging us this quarter

- Fortinet CVE-2025-59718, CVE-2025-64155, CVE-2026-24858
- Ivanti EPMM CVE-2026-1281 and CVE-2026-1340
- F5 BIG IP APM CVE-2025-53521

- Vulnerability exploitation is **faster** than ever
  - Thanks AI!
- **Episodic** impact: a relatively high number of system compromises in Q1 2026

APTs

CENTRE FOR CYBERSECURITY BELGIUM

- **China** and **Russia** appear to intentionally target **Europe**
- **Iran** focuses on **retaliatory** operations against the US and Israel
  - Blend of disruption and strategic messaging
- **North Korea** remains **opportunistic**
  - Enduring fake job campaign
  - **Developers and IT professionals** are more at risk in Belgium

Outlook for Q2 2026

CENTRE FOR CYBERSECURITY BELGIUM

- The cyber threat landscape will be shaped less by new threats than by the **adaptation, scaling and convergence of existing threats**
- More complex and **hybrid** operations
- **Spillover** effect of geopolitical tensions will drive interest in **disruption**
- **Digital dependencies** expand organisations' attack surface
- **Critical infrastructure** will continue to be attractive targets

CENTRE FOR
CYBERSECURITY
BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be