TLP:CLEAR

CYBER THREAT LANDSCAPE AND ACTIONS TAKEN IN BELGIUM – 2025

CYBER THREAT INTELLIGENCE REPORT

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: 09 March 2026
Version: 1.1 EN
Author: Centre for Cybersecurity Belgium (CCB) – CyTRIS department

Target audience:
This report is intended for cybersecurity practitioners, organizational decision-makers, and policymakers seeking to understand the evolving cyber threat landscape in Belgium and the strategic actions required to mitigate risks in 2026.

Permitted distribution of TLP CLEAR:
Recipients can spread this to the world, there is no limit on disclosure.

More information: https://ccb.belgium.be/tlp

Table of Contents

EXECUTIVE SUMMARY

Threat overview

- The **number of notifications** received by the CCB **continued to increase**, since the beginning of 2025.
- The **top cyber risk**s to Belgian entities were **operational disruption and data theft,** which is similar to other European countries.
- The most **prevalent threats** remain account compromise, ransomware, and DDoS, followed by spear-phishing and system compromises.
- **Social-engineering-related threats** remained a key driver of account compromise. In 2025, **ClickFix** and **FileFix** were among the techniques most frequently observed.
- The **most affected sector** in 2025 was **public administration**. Other largely impacted sectors included manufacturing, transportation, healthcare, energy.
- Both state-sponsored threat actors and ransomware groups rapidly weaponised and exploited known and zero-day vulnerabilities.
- Most of the **malware families** observed were **infostealers, remote access trojans (RATs) and ransomware** strains, while phishing, exploitation of vulnerabilities and use of compromised account credentials were the most frequently observed attack vectors.

Actions taken

- The CCB was directly involved in **103 emergency response interventions**, providing forensic support and expert investigative advice.
- As part of the Active Cyber Protection program, the CCB sent **32.005 spear warnings** containing threat information and remediation guidance.
- In response to DDoS campaigns, the CCB developed the Red Button procedure, in order to prevent, address, and mitigate the impact.
- In 2025, the CCB published **568 reports** and **14 Flash Alerts** on EWS portal, **264** technical advisories on its website, **693** technical posts on X, and **1.075 events in MISP**.
- As part of the **Connect & Share initiative**, in 2025, the CCB organised **15 events**, with more than 13.000 participants from 87 countries.

Outlook for 2026

- We assess with high confidence that the main categories of cyber threat activity observed in 2025 will persist in 2026. Evolving geopolitical dynamics and technological change will sustain elevated cyber risk for Belgian organisations.
- Belgian organisations are expected to remain under sustained pressure from ransomware, DDoS attacks, and account compromise.
- Automation, AI, and as-a-Service ecosystems will further increase the speed and scale of cyber operations. In 2026, the use of AI by threat actors is expected to become commonplace.
- Key threat enablers, such as phishing, credential abuse, vulnerability exploitation, and supply-chain compromise, will persist, reinforcing the need for strong prevention, detection, response, and recovery capabilities to sustain national cyber resilience.

SCOPE AND METHODOLOGY

This report provides an assessment of the cyber threat landscape affecting Belgium in 2025 and outlines the actions undertaken by the Centre for Cybersecurity Belgium (CCB) in response to observed threats.

Its scope covers incidents, trends, and metrics recorded throughout the year, based on notifications received from Belgian organisations, investigations conducted by the CCB, and threat intelligence from commercial CTI platforms and open sources. However, as it is based on the data available to the CCB in the reporting period, it may not be exhaustive and there is always a probability of incomplete information.

The methodology combines quantitative analysis of reported incidents with qualitative threat assessment and contextualisation, enabling trend validation and impact analysis. The report concludes with recommendations aligned with the MITRE ATT&CK and CyFun® 2025 frameworks, to support organisations in strengthening their cyber resilience.

THREAT OVERVIEW

Trends & Impact

In 2025, the CCB received **635 notifications** from Belgian organisations (almost 70 % increase compared to 2024), of which 556 were cyber related (almost 58 % increase compared to 2024). The **cyber threat landscape in Belgium remained largely unchanged throughout the year**, with recurring threats observed consistently across all quarters.

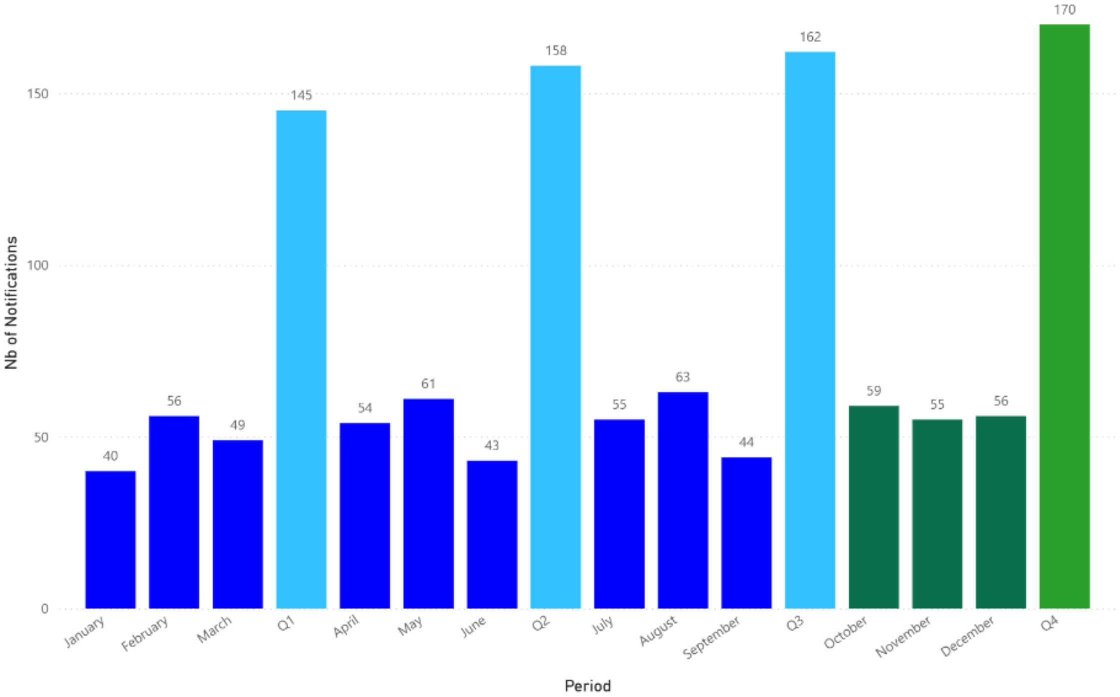


Figure 1: Number of notifications received by the CCB in 2025

As shown in Figure 1, since the beginning of 2025, the CCB observed a **continued increase** in the number of cyber incident **notifications**.

> The trend is partly driven by increased digital activity, evolving regulatory frameworks such as NIS2 and DORA, which have broadened the scope of reporting entities and enforced stricter incident disclosure obligations, but also by enhanced CCB detection capabilities and greater public reporting awareness. It also reflects increased trust in the CCB, with more companies now voluntarily reporting incidents, a significant shift from previous years.

While the monthly figures fluctuate, with some months showing more reports from NIS2-regulated organisations and others from non-NIS2 organisations, the overall distribution remained nearly equal between the two groups.

This underlines that **cybersecurity risks** are **shared across sectors** and not limited to regulated organisations and highlights the need for broader cyber resilience across all sectors, with unregulated organisations encouraged to adopt NIS2-style controls to better manage cyber threats.

Of the NIS2-defined organisations, we observed that **public administration** sector remained the primary target, followed by **energy**, **transportation** and **healthcare**, suggesting a broadening attacker focus on essential service providers with high operational dependency on digital infrastructure. This trend aligns with observations at the European level, where the same sectors continue to face sustained and increasingly sophisticated threat activity.

> Threat actors continue to prioritise critical public services, where successful attacks can rapidly translate into real-world disruption. Energy sector entities are especially attractive due to the potential cascading effects on other services, while healthcare, transportation and public administration organisations remain exposed because of sensitive data holdings and, in some cases, limited cybersecurity resources and outdated systems.

Most common threats

As observed from the beginning of 2025, the top cyber risks to Belgian organisations were operational disruption and data theft, consistent with trends observed in other European countries.

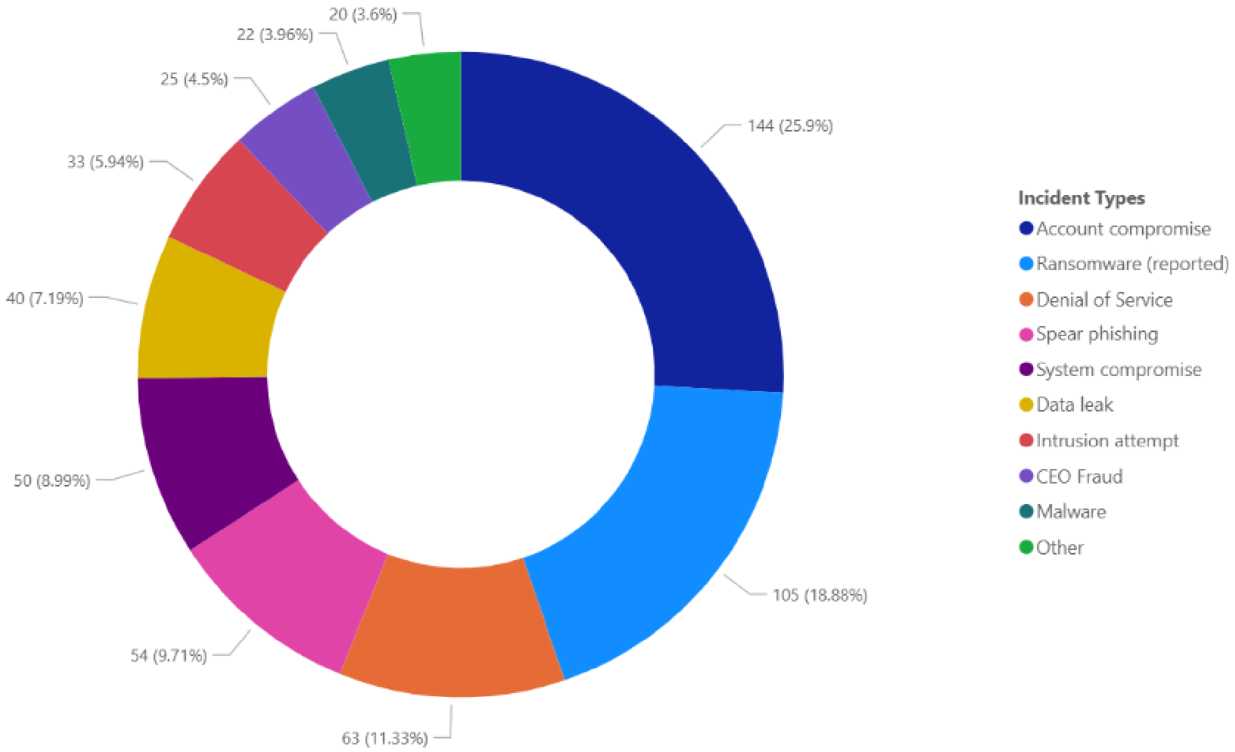


Figure 2: Type of incidents reported in the notifications received by the CCB in 2025

The **most common threats** in 2025 were **account compromise, ransomware, DDoS attacks, spear-phishing,** and **system compromise** (as illustrated in Figure 2). Although these categories consistently accounted for most incidents, their prominence varied monthly or quarterly.

Social-engineering-related threats, such as spear-phishing and CEO fraud, consistently ranked among the most reported incident types and remained a key driver of account compromise incidents.

We recorded also a **slight increase** in **system compromise notifications**, indicating sustained levels of post-intrusion activity. Once initial access is achieved, threat actors continue to successfully exploit compromised environments, highlighting persistent challenges related to timely detection, patch management, and incident response capabilities.

THREAT ACTIVITY

Cybercrime threat

Account compromises and social engineering related threats

Account compromise continued to be the **most frequently reported** incident type in 2025, with **144 notifications** received, confirming a sustained upward trend, as shown in Figure 3 below.

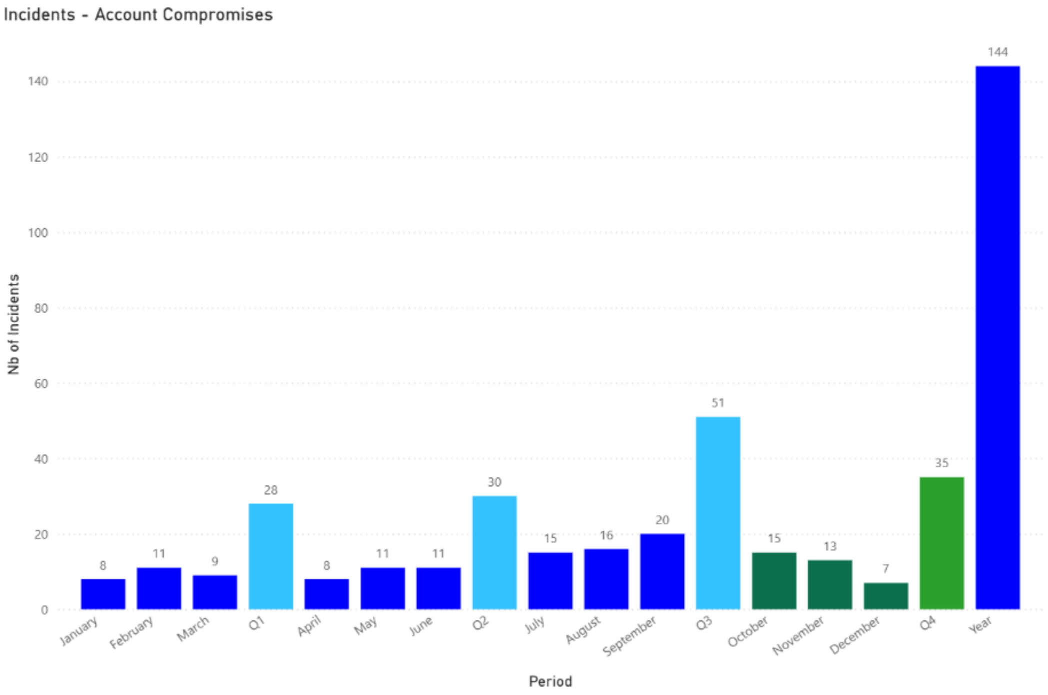


Figure 3: Number of account compromise related notifications received in 2025

This indicates that credential-based attacks remain a primary initial access vector used by threat actors against Belgian organisations. These attacks represent **a systemic risk in Belgium**, as trust-based digital interactions and interconnected ecosystems allow individual account compromises to scale across sectors, amplifying the operational and financial impact.

Most account compromise incidents originated from **phishing** and **spear-phishing**, underlining the persistent effectiveness of social engineering techniques despite existing awareness efforts and technical controls.

> Spear-phishing activity reached its highest quarterly level to date in Q4, with 20 notifications, including campaigns targeting customers and partners through compromised accounts or spoofed domains.
>
> In most reported cases, attackers exploit the trust associated with a legitimate identity to send phishing emails. Employees clicking on malicious links contained in phishing emails is one of the most common entry points observed for such incidents.

Account compromise and spear-phishing are **closely interconnected** and **reinforce each other**, significantly increasing success rates: spear-phishing enables credential theft and account takeover, while compromised accounts are subsequently abused to conduct further spear-phishing or e-fraud from trusted sources. This dynamic was observed in several reported incidents.

From a technical perspective, this confirms that **identity has become the primary security boundary being bypassed**. By abusing valid stolen credentials, attackers can operate within legitimate authentication flows, reducing detection risks and enabling persistent, low-noise access. Moreover, when privileged or business-critical accounts are compromised, the resulting blast radius can expand rapidly, enabling lateral movement, access to sensitive systems and data, and direct financial impact.

If not mitigated, this threat will continue to:

- drive a high volume of incidents across sectors, as identity-based attacks bypass perimeter and endpoint controls and scale rapidly through credential reuse;
- increase financial losses linked to e-fraud;
- undermine trust in digital communications between organisations, customers, and partners;
- extend attacker dwell time and blast radius[1], enabling lateral movement, persistent access, and delayed detection with higher remediation and recovery costs.

Bolster Your Cyber Defenses: 3 Key Recommendations

1. Strengthen Identity Security as a Baseline

Enforce Multi-Factor Authentication (MFA)

Apply to all external-facing and privileged accounts to secure access.

IMPACT: Reduces Credential Theft

Limits an attacker's ability to escalate privileges after an initial compromise.

2. Improve Detection of Anomalous Behaviour

Monitor for Unusual Account Activity – Use behavioral analytics, centralized logging, and rapid response capabilities.

IMPACT: Reduces Attacker Dwell Time

Enables faster incident containment and prevents misuse of trusted accounts.

3. Reinforce User Awareness and Training

Conduct Targeted Cybersecurity Training

Focus on common threats like spear-phishing, CEO fraud, and abuse scenarios.

IMPACT: Reduces Human-Enabled Attacks

Minimizes successful social engineering and prevents financial or reputational damage.

Figure 4: Key recommendations – account compromise and social engineering threats

[1] In cybersecurity, dwell time and blast radius are used to describe the impact and severity of an incident, especially after a compromise. **Dwell time** describes how long an attacker remains undetected; **blast radius** reflects how widely the compromise can spread across systems and operations.

Ransomware

Despite a relative stability in reported incidents in 2025 (105 cases, compared to 109 in 2024, representing a 3.7% decrease), ransomware continued to represent a **significant threat** to Belgian organisations due to its **high operational, financial,** and **reputational impact**, increasingly amplified by the use of **multiple extortion techniques**.

> Belgium is not among the most targeted European countries. This can largely be explained by structural factors, as countries such as the United Kingdom, Germany, and Italy have larger populations, economies, and numbers of enterprises, resulting in a higher concentration of high-value targets. Ransomware groups also apply broad targeting criteria, including an organisation's ability and willingness to pay, expected ransom value, technical maturity, and the potential monetary value of exfiltrated data.

As illustrated in Figure 5, ransomware activity fluctuated monthly throughout the year, while overall remaining persistent and stable.

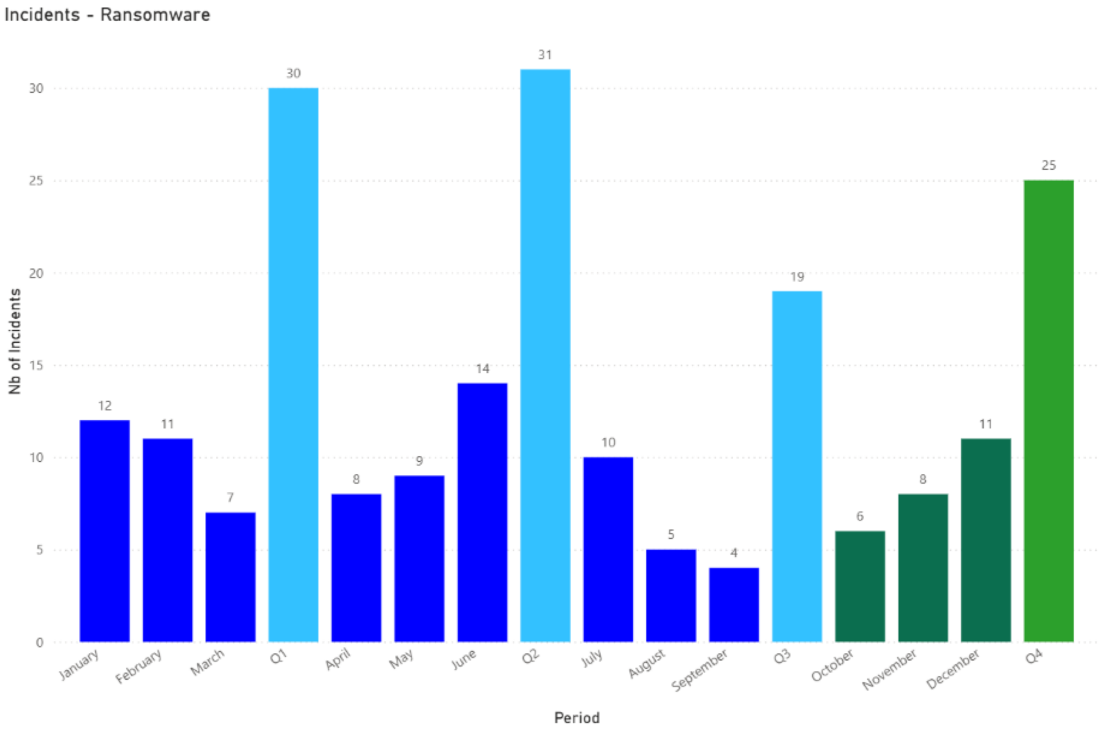


Figure 5: Number of ransomware related notifications received in 2025

Alongside well-established groups previously observed targeting Belgian entities, including Qilin, Clop, Akira, INC Ransom, Warlock, LockBit 3.0, Warlock Group, WorldLeaks, and Everest, several newer or less mature groups, such as Lynx, SafePay Coinbase Cartel, Wirebit, Nova, TridentLocker, Radar, Ghost (Cring), Crypto24, Cinnamon Tempest, and Morpheus, were also observed targeting Belgian organisations in 2025.

This confirms the diversity and dynamism of the ransomware ecosystem observed in 2025, characterised by frequent rebranding, splintering, and the emergence of new groups.

Following the takedown of LockBit, which accounted for most of the Belgian victims, the groups now active against Belgian targets represent a very fragmented and less predictable threat environment. No successor group filled the gap in 2025.

Notably, Qilin, Akira, and Clop, were also among the most active ransomware groups targeting Europe and globally, indicating strong alignment between national and broader European threat trends.

In 2025, **Qilin** rapidly emerged as the dominant and technically mature ransomware operator, targeting organisations globally and accounting for approximately 18% of all claimed victims. The group significantly enhanced its tooling and operational sophistication, including the introduction of advanced extortion mechanisms, such as data analysis audits designed to maximise pressure on victims.

Akira remained a highly active and adaptable ransomware group throughout 2025, increasingly shifting its operational focus from double extortion campaigns, combining data exfiltration and encryption to put pressure on victims toward only data exfiltration.

CLOP distinguishes itself through the systematic exploitation of zero-day vulnerabilities in file transfer solutions. According to the *Akamai Ransomware Report 2025*[2], the group operates through intermittent, high-impact campaigns aligned with zero-day disclosures, enabling the compromise of high-value targets while keeping overall victim numbers relatively low. CLOP also employs triple and, at times, quadruple extortion tactics, including direct pressure on customers through threatened data disclosure.

Ransomware continued to cause **operational disruption** and **financial impact**, particularly for essential service providers and organisations with a low tolerance for downtime, both in Belgium and across other European countries. Multiple incidents recorded in 2025 were followed by **data leaks**, significantly amplifying their impact through the exposure of sensitive information and increased reputational damage.

A wide range of **sectors** were affected in 2025, highlighting ransomware's cross-sector impact and systemic relevance. Notably, many of these fall directly under the **NIS2 scope:**

- administrative and support service activities
- human health and social work activities
- manufacturing
- scientific and technical activities
- transportation and storage
- education
- and water supply
- waste management and remediation activities
- financial and insurance activities
- information and communication
- professional
- public administration and defence
- wholesale and retail trade
- construction
- sewerage

From a technical perspective, ransomware groups were observed increasingly de-prioritising encryption in favour of data theft and extortion, exploiting the growing reliance on regulatory

[2] https://www.akamai.com/lp/soti/ransomware-trends-2025

pressure, reputational harm, and third-party exposure. Ransomware extortion tactics continued to evolve, and, while double extortion was still the most common tactic, some ransomware groups, such as CLOP, tried also the quadruple extortion[3]. The integration of AI and large language models (LLMs) further increased the scale, efficiency, sophistications and personalisation of their operations, while hybrid ransomware-hacktivist models blurred the boundary between cybercrime and ideologically motivated activity.

If insufficiently diminished, ransomware will continue to:

- cause severe operational disruption, particularly for essential and time-critical services;
- amplify financial and reputational damage through data leaks and multi-layered extortion;
- increase systemic risk, as attacks propagate across interconnected sectors and supply chains;
- exploit regulatory and compliance pressure as an additional extortion lever.

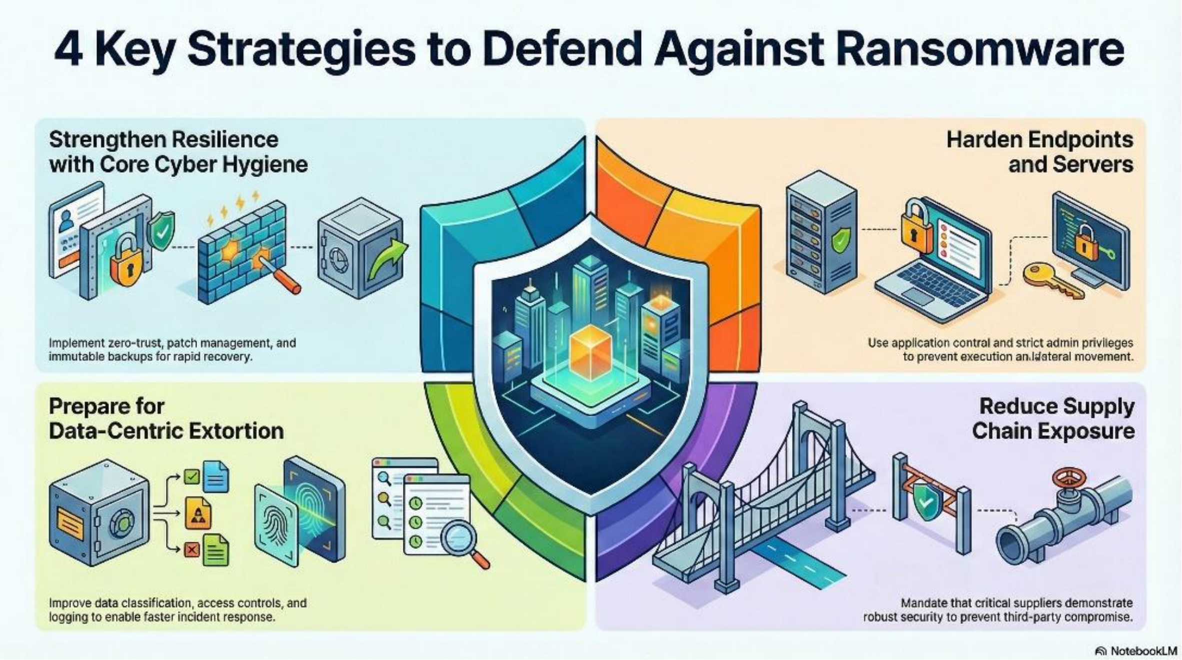

4 Key Strategies to Defend Against Ransomware
Strengthen Resilience with Core Cyber Hygiene
Implement zero-trust, patch management, and immutable backups for rapid recovery.
Harden Endpoints and Servers
Use application contral and strict admin privileges to prevent execution an.lateral movement.
Prepare for Data-Centric Extortion
Improve data classification, access controls, and logging to enable faster incident response.
Reduce Supply Chain Exposure
Mandate that critical suppliers demonstrate robust security to prevent third-party compromise.
NotebookLM

Figure 6: Key recommendations - ransomware

Other type of incidents

Over the past year, the CCB was notified of a range of **other incident types**, including system compromises, data leaks unrelated to ransomware, attempted intrusions, exposed or vulnerable services, malware detections, and phone-based scams.

[3] **Double extortion** involves both the encryption of systems and the threat of data exfiltration and public disclosure if the ransom is not paid. While **triple extortion** ads the use of DDoS attacks to disrupt business operations, the **quadruple extortion** adds the sending of messages to harass business partners, employees, customers, high-level executives, and media to inform of the breach and pressure the primary victim.

Notably, the number of reported **system compromise** incidents remained high throughout the year.

> In several instances, these compromises resulted from the exploitation of known vulnerabilities, including Ivanti and SAP NetWeaver, which have also been publicly reported as being exploited by Chinese state-sponsored threat actors. These vulnerabilities were rapidly weaponised, enabling attackers to gain unauthorised access to affected networks.
>
> Additional system compromise notifications involved malware infections originating from counterfeit AppSuite PDF Editor installers, promoted through malicious Google Ads as part of a large-scale campaign observed in Q3 2025 that distributed the TamperedChef infostealer.

Regarding **vulnerable services**, several notifications received in 2025 were related to the exploitation of known SharePoint vulnerabilities, CVE-2025-53770 and CVE-2025-53771, further reinforcing the persistent risk associated with exposed and insufficiently patched internet-facing services.

These highlight the risk posed by widely deployed technologies with unpatched weaknesses, which can be exploited at scale and lead to serious security breaches. It also highlights the growing role of malvertising and fake software distribution in expanding initial access beyond traditional phishing, and underscores the need for timely patching, effective vulnerability management, and layered cybersecurity defences for Belgian organisations.

Another form of social engineering reported to the CCB was **CEO fraud**, in which employees, typically within finance or administrative functions, received emails impersonating senior executives. These attacks frequently led to e-fraud or the disclosure of sensitive information. The financial and reputational consequences of CEO fraud can be severe, resulting in direct monetary losses, data exposure, and, in some cases, operational disruption.

> An emerging trend amplifying this threat is the increased use of messaging platforms such as WhatsApp in CEO fraud schemes. Attackers increasingly combine compromised email accounts with phone-based communication, applying real-time pressure on victims by invoking urgency or confidentiality in order to bypass established verification and control procedures.

Several data leak notifications reported to the CCB appeared to be associated with account compromises originating from third-party data breaches. This emphasises that organisations should consider their third-party risk management practices and maintain visibility into what data is stored and processed by external providers.

Hacktivist threat and DDoS attacks

In 2025, **Belgium** was among the **European countries most frequently targeted** by pro-Russian hacktivist groups, primarily through distributed denial-of-service (DDoS) attacks. These campaigns were closely linked to geopolitical developments, including public statements by Belgian officials, financial and military support to Ukraine, and discussions around the potential use of frozen Russian assets held by Euroclear to finance Ukrainian support measures.

Throughout 2025, NoName057(16) was the most active pro-Russian hacktivist group targeting Belgian entities, leveraging the DDoSia botnet to conduct **5 distinct campaigns**.

- **24th of March - 4th of April**, around 130 organisations were added on the DDoSia targets list in retaliation for Belgium's announced €1 billion military aid package to Ukraine, but not all of them were targeted;
- **25th - 27th of July**, as part of the #FuckEastwood[4] #TimeOfRetribution campaign, Belgian domains were added to the DDoSia list and DDoS attacks were carried out against the publicly accessible websites of 16 Belgian organisations;
- **18th - 24th of August**, 122 Belgian organisations were added on the DDoSia list of targets, with a focus on several clusters of targets, including government entities, municipalities, and ports;
- **3rd - 11th of November**, 84 organisations were targeted;
- **8th - 14th of December**, 85 organisations were targeted.

Targeted organisations spanned a wide range of **sectors**, including government and public administration, transportation, infrastructure, water utilities, energy, telecommunications, aerospace and defence, hospitality, construction, banking and finance, retail, and manufacturing.

> Consistent with trends observed across other European countries, government and public administration entities were the most frequently targeted. By focusing on regional and local government services, NoName057(16) appears to seek indirect pressure on national decision-makers, aiming to deter continued support for Ukraine through perceived public disruption.

While threat actors frequently updated and publicised target lists to maximise perceived **impact** and media attention, not all announced targets were attacked. Most observed DDoS incidents resulted in temporary service disruption, with limited long-term operational impact.

> A bigger impact was typically observed during morning hours, with service availability usually stabilising by midday following coordination between victims, ISPs, hosting providers, and the CCB. Over weekends, previously used target lists were sometimes reused, and reduced staffing levels at affected organisations occasionally resulted in longer disruption periods.

Overall, **most organisations responded effectively**, supported by the CCB's proactive notification and coordination procedures under the Red Button project, including the sharing of technical indicators and mitigation advice.

However, websites with limited protective measures, particularly those of local municipalities hosted by third-party providers outside Belgium, experienced more significant downtime. Centralised hosting within the national government infrastructure, which has a proven track record in protecting critical services, would substantially improve resilience.

[4] Between the 14th and the 17th of July 2025, a joint international operation (coordinated by Europol and Eurojust) known as Eastwood targeted the pro-Russian hacktivist group NoName057(16). Belgium supported the investigation, alongside ENISA, 6 other countries, and 2 private entities (ShadowServer and abuse.ch).

Notably, in the final campaigns of 2025, NoName057(16) appeared less successful in achieving one of its key strategic objectives: generating sustained media attention.

Other pro-Russian hacktivist groups, including Desinformador Ruso, Dark Storm Team, Server Killers, and Mr Hamza, also claimed responsibility for DDoS attacks against Belgian entities, predominantly within the public sector. In parallel, the CCB received notifications of DDoS attacks by unidentified actors affecting organisations in sectors such as government, banking, and transport.

While current activity in Belgium remains largely limited to DDoS and service disruption, developments observed elsewhere in Europe indicate a **potential escalation**, with some hacktivist groups expanding into **ransomware** and **attacks against critical infrastructure** and **OT environments**.

If insufficiently addressed, hacktivist DDoS activity will:

- disrupt public-facing services, particularly at regional and local government level
- erode public trust in institutions, especially when attacks coincide with sensitive political events
- create systemic operational risk, as repeated low-impact disruptions accumulate across sectors
- increase escalation risk, as hacktivist groups adopt more destructive or financially motivated techniques

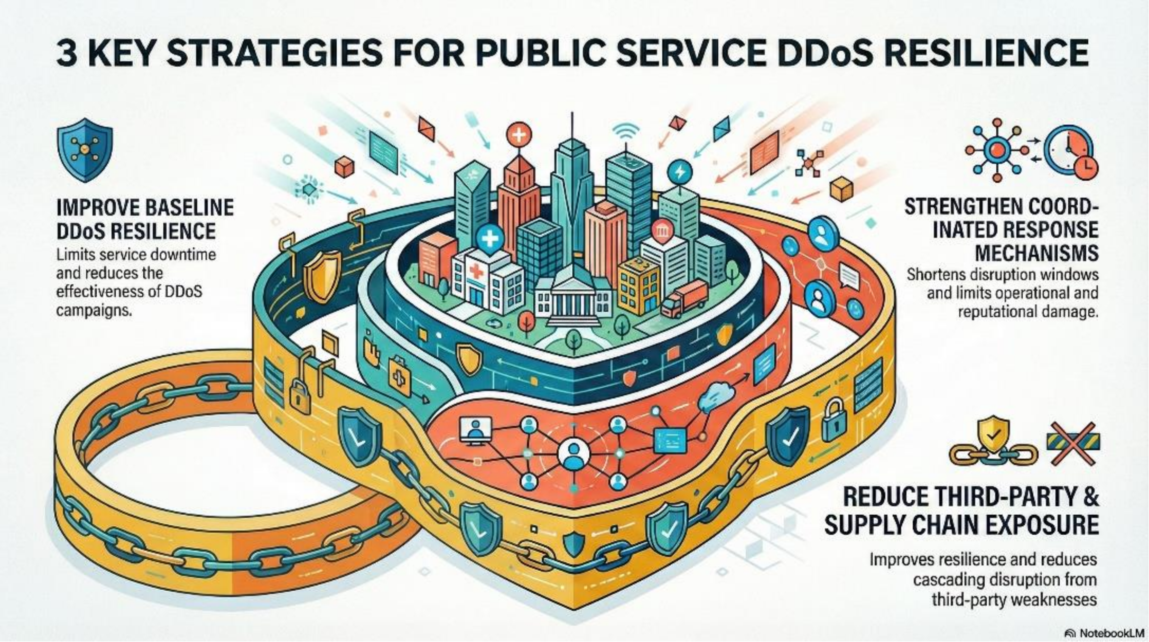

3 KEY STRATEGIES FOR PUBLIC SERVICE DDoS RESILIENCE
IMPROVE BASELINE DDoS RESILIENCE
Limits service downtime and reduces the effectiveness of DDoS campaigns.
STRENGTHEN COORDINATED RESPONSE MECHANISMS
Shortens disruption windows and limits operational and reputational damage.
REDUCE THIRD-PARTY & SUPPLY CHAIN EXPOSURE
Improves resilience and reduces cascading disruption from third-party weaknesses
NotebookLM

Figure 7: Key recommendations – DDoS attacks

State-sponsored threat

The analysis of state-sponsored cyber activity observed throughout 2025 highlights several **key aspects** shaping the threat landscape in Belgium:

Persistent exploitation of known vulnerabilities

The CCB observed a sustained interest by state-sponsored threat actors in exploiting known vulnerabilities to gain rapid access to high-value systems, particularly by Chinese state-sponsored groups.

> Among the vulnerabilities disclosed in 2025 and actively exploited by state-linked actors were the ToolShell vulnerabilities (CVE-2025-53770 and CVE-2025-53771), a stack-based buffer overflow in Ivanti Connect Secure (CVE-2025-0282), remote code execution vulnerabilities affecting multiple end-of-life Ivanti devices, SAP NetWeaver Visual Composer Metadata Uploader (CVE-2025-31324), Citrix Bleed 2 (CVE-2025-5777), a memory disclosure vulnerability in Citrix NetScaler ADC, and Cisco Identity Services Engine (CVE-2025-20337). These cases demonstrate the speed at which publicly disclosed vulnerabilities are weaponised for espionage operations.

Increased targeting of diplomatic and foreign affairs entities

A noticeable rise in cyber operations targeting foreign affairs ministries, diplomatic missions, and related entities was observed, reflecting the strategic intelligence value of these institutions.

> Threat actors linked to China were observed targeting diplomats and hijacking web traffic to deploy PlugX malware variants for cyber-espionage purposes. In this context, the CCB identified a Belgian IP address potentially infected with PlugX.
>
> In addition, the Chinese-affiliated threat actor UNC6384 (also known as Mustang Panda or Red Delta) conducted a cyber-espionage campaign between September and October 2025 targeting diplomatic entities in Belgium, Hungary, and other European countries. This campaign demonstrated UNC6384’s rapid adoption of the zero-day vulnerability ZDI-CAN-25373 (CVE-2025-9491) affecting Windows shortcut files, disclosed in March 2025.
>
> Separately, the Iranian-nexus threat actor Homeland Justice (overlapping with MuddyWater, Seedworm, and TA450), associated with Iran’s Ministry of Intelligence and Security (MOIS), carried out a multi-wave spear-phishing campaign targeting foreign diplomatic missions and international organisations. In Europe, 10 countries, including Belgium, were targeted.

Continued activity by North Korean remote IT worker campaigns

The CCB continued to observe North Korean remote IT workers seeking employment in Western companies, including in Belgium, to generate foreign revenue for the Pyongyang regime. In some cases, this activity has been linked to malware deployment, ransomware activity, or theft of corporate and customer data. These operations are coordinated, long-running, and supported by intermediaries, including proxies and so-called “laptop farms”, designed to obscure the workers’ true geographic location.

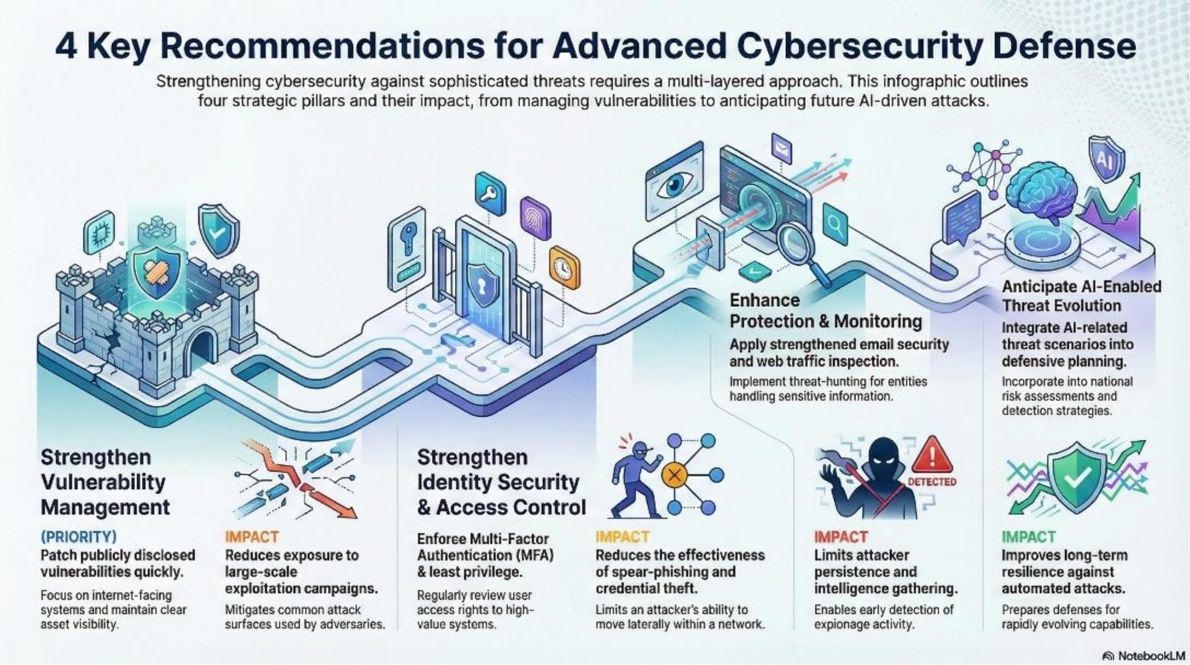
Growing use of AI and LLMs by state-sponsored actors

State-sponsored threat actors increasingly explored and leveraged artificial intelligence and large language models to enhance the speed, scale, and sophistication of their cyber operations. Beyond tactical use, several actors were observed pursuing long-term strategies to integrate AI into cyber-espionage, influence, and information operations, thereby increasing the precision and impact of future campaigns.

Although many cyber campaigns observed in 2025 did not directly target Belgium or Europe, recurring global patterns, such as common target profiles, threat actor behaviour, and shared malware capabilities, suggest that these activities should be factored into risk assessments and mitigation planning, as they can rapidly extend to European countries, including Belgium.

If insufficiently mitigated, state-sponsored cyber activity will continue to:

- expose sensitive governmental and diplomatic information, undermining national security interests;
- increase systemic risk, as widely exploited vulnerabilities enable rapid compromise across sectors;
- erode trust in public institutions, particularly when governmental entities are affected;
- amplify future threat capability, as AI-enabled operations increase speed, scale, and precision.



4 Key Recommendations for Advanced Cybersecurity Defense

Strengthening cybersecurity against sophisticated threats requires a multi-layered approach. This infographic outlines four strategic pillars and their impact, from managing vulnerabilities to anticipating future AI-driven attacks.

Strengthen Vulnerability Management

(PRIORITY)
Patch publicly disclosed vulnerabilities quickly.
Focus on internet-facing systems and maintain clear asset visibility.

IMPACT
Reduces exposure to large-scale exploitation campaigns.
Mitigates common attack surfaces used by adversaries.

Strengthen Identity Security & Access Control

Enforce Multi-Factor Authentication (MFA) & least privilege.
Regularly review user access rights to high-value systems.

IMPACT
Reduces the effectiveness of spear-phishing and credential theft.
Limits an attacker's ability to move laterally within a network.

Enhance Protection & Monitoring

Apply strengthened email security and web traffic inspection.
Implement threat-hunting for entities handling sensitive information.

IMPACT
Limits attacker persistence and intelligence gathering.
Enables early detection of expionage activity.

Anticipate AI-Enabled Threat Evolution

Integrate AI-related threat scenarios into defensive planning.
Incorporate into national risk assessments and detection strategies.

IMPACT
Improves long-term resilience against automated attacks.
Prepares defenses for rapidly evolving capabilities.

NotebookLM

Figure 8: Key recommendations - state-sponsored activity

MALWARE & ATTACK VECTORS

Malware families

The malware families observed in 2025 were predominantly **infostealers** and **RATs.** These included Xloader, Agent Tesla, AsyncRAT, Remcos, Xworm, Snake Keylogger, Stealerium, 404 Keylogger, DarkCloud, VIPKeylogger, CloudEye, Dbatloader, and Mass Logger.

> Many of the infostealers have keylogging capabilities, which highlights the focus of threat actors on data exfiltration. RATs pose a serious threat to Belgian infrastructure by enabling threat actors to remotely control an infected network throughout the entire attack lifecycle.

Among the top observed malware, there were also **loaders** such as DonutLoader, Cloudeye and DarkTortilla, which attackers use to deliver and execute other malicious payloads, including infostealers and RATs.

Ransomware strains were also among the most reported types of malware in this quarter.

Attack vectors

Phishing and spear-phishing campaigns, exploitation of known vulnerabilities, and the use of valid account credentials that had previously been compromised were the most used attack vectors observed in 2025, remaining reliable entry points across sectors for threat actors.

This confirms that threat actors continue to rely on established and effective techniques rather than introducing fundamentally new methods. At the same time, these techniques are being progressively refined and scaled, supported in part by the increasing use of AI-enabled tools to improve the quality, personalisation, and volume of attacks.

In 2025, the supply chain attacks represent a significant attack vector, as they allow threat actors to compromise a large number of downstream victims by targeting a single trusted component, service, or provider.

Phishing

Phishing attacks remain both **widespread** and **challenging**. Often serving as the initial entry point for more significant security breaches, these attacks enable cyber threat actors to impersonate trusted entities, steal credentials and personal data, and severely disrupt organisational operations.

> Generative AI tools have improved the quality of phishing schemes, business email compromise (BEC) lures and voice phishing (vishing) scripts. However, they currently function more as an efficiency upgrade than the core enabler of cyber related operations. QR codes were also used in phishing emails (quishing), as they are not detected by traditional email filters. When scanned by a mobile phone, these malicious QR codes either redirect users to phishing websites or trick

> them into downloading malware.

As part of the **BePhish project**, the CCB registered **9.929.354** (a 9.31%. increase compared to last year) **suspicious phishing emails** sent to the dedicated suspicious@safeonweb.be address in 2025.

> In addition to generic phishing subject lines concerning delivery status or login details, we observed subjects relating to a pension bonus available on *mypension[.]be*, financial assistance requests, new documents available in eBox, or criminal offense in 2025. Additionally, threat actors **tailor the lures** of the phishing emails to subjects relevant for a **specific period of time**, such as energy allowance, vacation credits and tax returns available in *MyMinfin* for the period before the end of the year. Most of the messages insist on **short deadlines** to create a sense of **urgency** and pressure victims into resolving issues or complying with threats of fines.

ClickFix and FileFix

Threat actors are continuously innovating and finding ways to simplify phishing operations, such as ClickFix and FileFix.

> The primary difference between these tactics lies in where the command is executed. In ClickFix, attackers persuade victims to open the Windows Run dialog box and paste a malicious command. In contrast, FileFix involves manipulating victims into pasting a command into the Windows File Explorer address bar.

In 2025, malware tactics underwent a significant transformation, with a notable shift toward high-volume social-engineering techniques exemplified by the **ClickFix** attack. This technique, often used alongside malvertising, operates at the traffic layer, focusing on clicks and conversions. Since the rise of ClickFix, multiple iterations of phishing pages have emerged.

> Unit42[5] observed that attackers are even packaging the ClickFix technique into easy-to-use phishing kits, making it accessible to a wider range of threat actors. A new phishing kit named the IUAM ClickFix Generator automates the creation of these attacks.

The ClickFix technique was observed being used by both ransomware groups and state-sponsored threat actors and affects multiple platforms, including Windows, macOS and Linux. Moreover, ClickFix campaigns have a global reach and distribute malicious files under the guise of tools or urgent fixes, tricking users into downloading and executing them. As the lures are generic and easily adaptable, these campaigns are not limited to a specific geography or sector and can impact organisations and individuals in any country.

Although not as extensively observed in the wild as ClickFix, **FileFix** is another social engineering technique that threat actors started to leverage. This technique was disclosed publicly in June 2025 and has since been observed in threat-actor activity, including reported use by the **Interlock** ransomware group. The adoption of FileFix aligns with established threat behaviour, as adversaries quickly operationalise newly disclosed techniques that enhance and

[5] https://unit42.paloaltonetworks.com/clickfix-generator-first-of-its-kind/

optimise techniques for initial access, execution, or user-assisted payload delivery.

Acronis[6] discovered a FileFix campaign with a global targeting strategy, having victims in numerous countries. The observed campaign used a highly convincing, multilingual phishing site (e.g., fake Facebook Security page), with anti-analysis techniques and advanced obfuscation to evade detection. The attack uniquely employs steganography to conceal malicious code, and the infection chain is built around a multistage payload delivery system. The campaign delivers the StealC infostealer, which targets browsers, cryptocurrency wallets, messaging apps and cloud credentials.

Both techniques highlight the limitations of purely technical defences and underscore the critical need for user awareness and training. Raising awareness through targeted campaigns is essential in order to prepare users and ultimately strengthen the first line of cyber defence.

Exploitation of vulnerabilities

Exploited vulnerabilities remain one of the most common and effective attack vectors. A critical issue is the significantly reduced time between the public disclosure of a vulnerability and its weaponisation and exploitation by both state-sponsored threat actors and cybercriminals, including ransomware groups. This significantly increased the risk of unauthorised access to affected networks, as the traditional “safe window” for patching has **been significantly reduced.**

In 2025, the average Time-to-Exploit (TTE) dropped sharply to just five days, with nearly one-third of vulnerabilities being exploited within 24 hours of public disclosure. Moreover, a substantial share of known exploited vulnerabilities showed evidence of exploitation on or before the day a CVE was officially issued. This acceleration leaves organisations little room to rely on scheduled patching cycles and instead necessitates a shift toward continuous, risk-based vulnerability management focused on exploitability and real-world threat activity[7].

At global level, the vulnerability threat landscape in 2025 presented **an important challenge for defenders**. The US National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) recorded **45.425 vulnerabilities** in 2025, an increase of about 14% compared to 2024 (Figure 9).

The US Cybersecurity and Infrastructure Security Agency (CISA) added 238 vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog, with 146 of these linked to CVE-2025 identifiers.

[6] https://www.acronis.com/en/tru/posts/filefix-in-the-wild-new-filefix-campaign-goes-beyond-poc-and-leverages-steganography/

[7] https://go.crowdstrike.com/2025-global-threat-report.html?utm_campaign=brand&utm_content=crwd-brand-eur-bnlx-en-psp-x-x-x-tct-x_x_x_reports-x&utm_medium=sem&utm_source=goog&utm_term=crowdstrike%202025%20global%20threat%20report&utm_language=en-gb&cq_cmp= , https://services.google.com/fh/files/misc/m-trends-2025-en.pdf, https://wwv.vulncheck.com/1h2025-state-of-exploitation

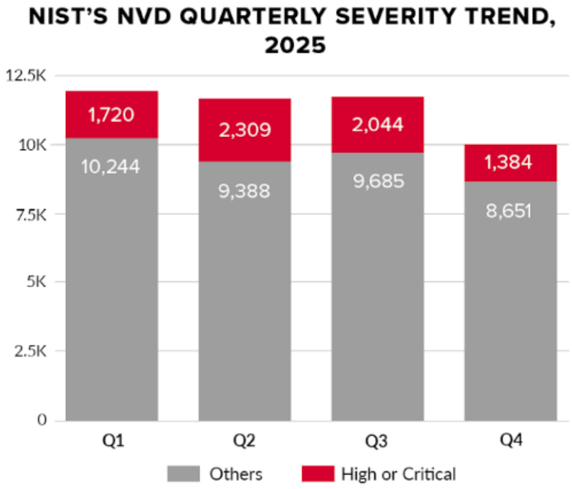


Figure 9: Number of vulnerabilities recorded quarterly by NIST's NVD (source: Intel 471)

According to Intel 471 data, the top 5 most impacted vendors in 2025 were Microsoft, CISCO, D-Link, Apache, and Fortinet. This is also **confirmed by the analysis** of the product vendors associated with the CVEs also addressed **by the CCB** in its actions.

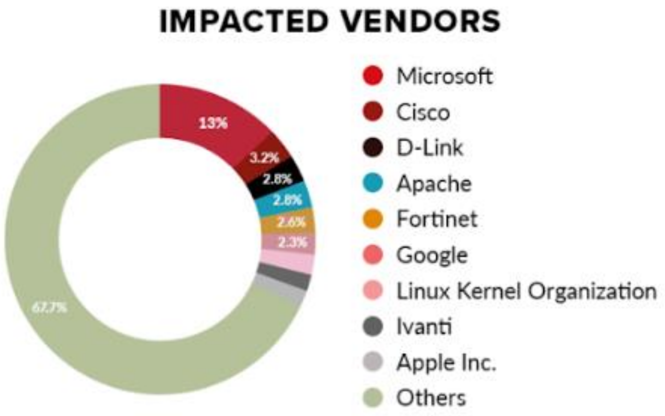


Figure 10: Most impacted vendors in 2025 (source: Intel 471)

Among the vulnerabilities that required **significant effort from operational teams** in 2025 were **CVE-2025-5777, CVE-2025-53770** and **CVE-2025-53771,** and **CVE-2025-55182.** Given the critical nature of these vulnerabilities and their exploitation in the wild, as well as the large number of unpatched instances exposed, the **CCB published advisories** and **sent urgent spear warnings** to help Belgian organisations enhance their protection and response, improve their situational awareness across sectors, and identify exploitation trends more quickly.

CVE-2025-5777, a critical out-of-bounds vulnerability in the Citrix NetScaler application delivery controller that stems from insufficient input validation, allowing an unauthenticated attacker to read sensitive memory contents, including session tokens and credentials. Due to its similarity to the original CitrixBleed vulnerability, security researchers warned early in 2025 of the high likelihood of abuse, and by mid-year organisations such as ReliaQuest had reported active exploitation in the wild against internet-exposed instances, prompting its addition to the CISA Known Exploited Vulnerabilities (KEV) catalog and urgent patching guidance. CVE-2025-5777 has since served as a vector for initial access and session takeover in targeted campaigns.

CVE-2025-53770, CVE-2025-53771, aka *ToolShell*, a critical chain of vulnerabilities in Microsoft SharePoint actively exploited in the wild by multiple threat actors, including Chinese threat actors and ransomware groups. These vulnerabilities allow threat actors to perform unauthenticated RCE and bypass authentication mechanisms to exfiltrate sensitive data from on vulnerable on-premises SharePoint servers. Most concerning, exploitation of these two vulnerabilities grants attackers access to cryptographic keys within SharePoint, specifically the Validation Key and the Decryption Key. Possession of these keys enables long-term persistence, allowing re-entry into systems even after patches are applied. As SharePoint is integrated with Outlook, Teams and OneDrive, compromise could spread rapidly across the Microsoft ecosystem, resulting in data breaches, disruption or espionage.

CVE-2025-55182 aka *React2Shell*, a deserialization of untrusted data vulnerability which was rapidly exploited in December within hours of public disclosure by multiple China state-nexus threat groups, including Earth Lamia and Jackpot Panda, as well as by opportunistic attackers. CVE-2025-55182 has a maximum CVSS severity score of 10. According to the manufacturer, apps that do not implement React Server Function endpoints may still be vulnerable if they support React Server Components. It also has downstream impacts across popular frameworks including Next.js. Malicious proof of concept was also observed circulating to deliver malware.

Other 5 key vulnerabilities in 2025 were **actively exploited in large campaigns** by a range of threat actors from state-sponsored clusters, underground actors, to extortion and ransomware operators: CVE-2025-0282 - Ivanti, CVE-2025-64446 - Fortinet FortiWeb, CVE-2025-53770 - Microsoft SharePoint, CVE-2025-31324 - SAP NetWeaver, and CVE-2025-61882 - Oracle EBS.

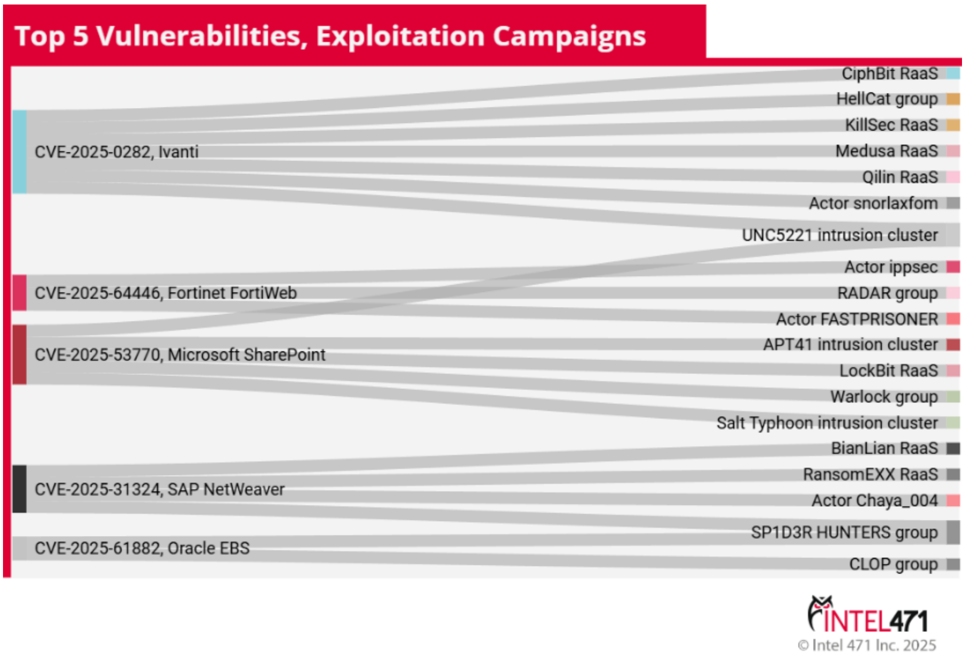


Figure 11: Top 5 most exploited vulnerabilities in 2025 (source: Intel 471)

The CCB published advisories and posted tweets for all the 5 vulnerabilities mentioned: CVE-2025-0282, CVE-2025-64446, CVE-2025-53770, CVE-2025-31324, and CVE-2025-61882.

Client-side exploitation was also observed in 2025, with attackers leveraging vulnerabilities in PDF readers through specially crafted documents. Threat actors increasingly exploit familiar file formats and trusted applications as attack vectors to bypass traditional security controls, increase user trust, and achieve higher infection rates.

> Earlier activity observed in 2025 included the distribution of a trojanized AppSuite PDF Editor via spoofed websites and malicious advertisements to deploy the TamperedChef infostealer. This continued with the use of the MatrixPDF toolkit, which enables the abuse of legitimate PDF documents to deliver phishing or malware while bypassing traditional security controls.

Widespread awareness and the implementation of the CCB's CVDP[8] play a critical role in reducing cyber risk by enabling the early identification and responsible reporting of security flaws.

Compromised valid account credentials

The reliance of cyber threat actors on **compromised valid account credentials** was a **persistent threat** throughout 2025, not only in Belgium, but also in other countries in Europe and the rest of the world.

The use of compromised valid account credentials as an attack vector presents **significant risks**, as it enables attackers to bypass perimeter defences and operate under the guise of legitimate users. This often results in delayed detection, prolonged dwell time, and increased opportunities for lateral movement within affected environments. Once access is established, threat actors can exfiltrate sensitive data, disrupt critical services, deploy additional malware, or escalate privileges, amplifying the overall impact of an incident.

Considering this, leaked compromised credentials were one of the **main topics** covered in the **spear warnings** sent by the CCB throughout the year, as shown in Figure 12.

[8] https://atwork.safeonweb.be/tools-resources/coordinated-vulnerability-disclosure-policy

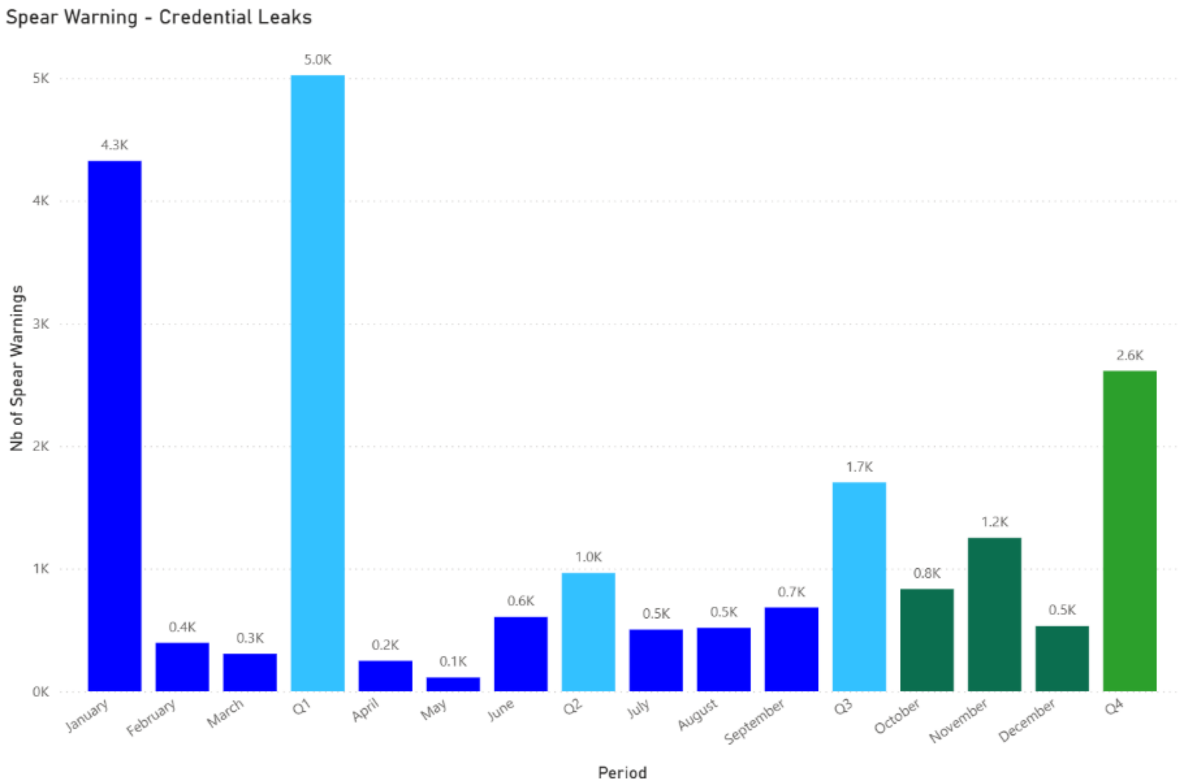


Figure 12: Number of credential leaks in 2025

Based on the number of leaked compromised credentials observed, the sectoral analysis of 2025 indicates that the **manufacturing sector** is the **most impacted** by credential leaks**, closely followed by public administration**. ICT service management, transportation, financial markets and healthcare sectors were also among the most impacted ones. All these sectors face elevated exposure, as their highly sensitive data, operational dependencies and essential service functions make them prime targets for exploitation.

Furthermore, on the dark web forums, initial access brokers (IAB) continued to sell access to different organisations, including Belgian ones. This comprises various forms of initial access, including RDP, Windows NetSupport, and network access.

An effective defence against credential-compromise attacks requires a layered approach, including:

- Robust identity and access management (IAM) and the systematic use of multi-factor authentication (MFA);
- Continuous monitoring of account activity and rapid response to anomalous login patterns;
- Enforcement of least-privilege access and regular review of access rights to reduce unnecessary exposure;
- Security awareness training and strong password hygiene policies;
- Adaptive authentication mechanisms to strengthen resilience against evolving threats.

Supply chain attacks

Supply chain attacks pose a **significant systemic risk**, particularly for organisations that rely on outsourced IT services and shared digital platforms. By compromising widely used software, managed services, or trusted third-party providers, threat actors can bypass direct security controls and trigger data breaches across interconnected environments, significantly amplifying the scale and impact of an attack.

In 2025, supply chain attacks remained a **key driver of large-scale data breaches**, enabling threat actors to compromise multiple downstream organisations through a single upstream weakness.

> Several major incidents illustrated this dynamic, including CLOP's exploitation of zero-day vulnerabilities in Cleo Harmony managed file transfer (MFT) SaaS and Oracle EBS instances, the compromise of CRM provider Salesloft Inc. by the SP1D3R HUNTERS (also known as SCATTERED LAPSUS$ HUNTERS), and the ransomware attack against US-based IT supplier Collins Aerospace, which disrupted airport operations across several EU member states, including Belgium. In the second half of 2025, a series of *npm* supply chain compromises, collectively referred to as Shai-Hulud, further highlighted the risk through worm-like propagation, large-scale package trojanization, and credential theft.

The **impact** of supply-chain and data breaches extends beyond individual victims, resulting in systemic financial, operational, and reputational damage, as well as increased regulatory and legal exposure. Such incidents undermine trust in digital services and complicate incident response, attribution, and remediation efforts. As reliance on shared platforms and external providers continues to grow, **strengthening supply chain security** has become essential to reducing both the likelihood and severity of data breaches, rather than a peripheral risk management consideration.

ACTIONS TAKEN

Response measures: Emergency response interventions

The CCB implemented response measures aimed at limiting the impact of active cyber incidents. These included **emergency response interventions**, technical coordination with affected organisations, and close collaboration with ISPs, hosting providers, and other partners to contain ongoing attacks and restore services.

On an annual perspective, the CCB was involved in 103 emergency response interventions, providing forensic support and expert investigative advice. Of these 8 were related to incidents classified as national.

> Most of the emergency response interventions (70) involved NIS2 entities and addressed incidents related to network intrusion, credential leaks, business email compromise (BEC), insider threats, ransomware, malware infections and phishing.

Proactive measures: Intelligence sharing and spear warnings

Intelligence sharing

In 2025, the CCB further strengthened its **proactive measures** in line with Belgium's Cybersecurity Strategy and its Active Cyber Protection (ACP) approach, focusing on prevention, early detection, and coordinated response and thereby contributing to national cyber resilience.

Through enhanced intelligence sharing and early warning capabilities, the CCB issued timely alerts and targeted notifications to affected and potentially affected organisations, by **sharing timely actionable intelligence on emerging threats and IoCs**, as well as **recommended mitigation measures** to reduce exposure and prevent potential incidents.

These efforts were supported by internal operational procedures, such as **Red Button**, the use of intelligence-sharing platforms including **MISP**, and the dissemination of information via portals, websites, and dedicated services, notably the **Access Journey Program (AJP)**. Drawing on information from international partners and CTI platforms, these actions supported early detection, rapid mitigation, and strengthened overall resilience against emerging and recurring cyber threats.

Red Button procedure

In **response to the DDoS attack campaigns** carried out by the pro-Russian hacktivist groups in 2025, the CCB acted in accordance with its mission by prioritising coordinated action, timely information exchange, and proactive cyber protection measures to prevent and mitigate the impact of these cyberattacks under **Red Button**, a comprehensive national anti-DDoS procedure.

The procedure follows a **four-phase continuous process** aimed at enhancing protection against DDoS attacks.

It begins with proactive monitoring of potential DDoS threats to detect suspicious activity at an early stage. When an incident is identified, a rapid response is initiated to mitigate the attack and provide support to affected victims. Following containment, attack logs are analysed to update the collection of IOCs and related reports. The cycle concludes with documenting lessons learned to drive continuous improvement, ensuring that detection, response, and resilience capabilities are constantly enhanced. This stage is also used to develop new methodologies, detection rules, and data sources to further strengthen the procedure.

The procedure is highly automated and includes automated data collection, standardised processing, and historical tracking. It also maintains consolidated, specialised blocklists composed of highly processed and verified IP address datasets. These lists contain hundreds of thousands of IPs associated with threat actors known to conduct DDoS attacks and are cross-checked against whitelists to reduce false positives. The resulting datasets, together with reports and remediation guidelines, are delivered to victims in a format ready to be deployed directly into their firewalls without disrupting operations.

In 2025, under the **Red Button procedure** and in response to the DDoS campaigns against Belgian organisations, the CCB:

- monitored the threat in real time, exchanging information with partners, targeted organisations, ISPs, and hosting providers[9];
- frequently informed the government, the intelligence community, and the security services about the situation;
- conducted research and analysis on previously reported DDoS incidents using these insights to develop and apply targeted mitigation recommendations;
- stayed in permanent contact with the targeted organisations[10];
- shared CTI to collectively increase resilience (providing detailed reports, target URLs, block lists and mitigation advice.

As a result, the impact of DDoS attacks in 2025 was significantly reduced. Many victims emphasized that the Red Button procedure was highly effective in mitigating these attacks, providing rapid support and actionable measures that helped restore and protect their services.

Sharing across platforms

Throughout **2025**, the CCB published: **568** reports and **14** Flash Alerts on the **EWS portal**, **264** technical advisories on its public website https://ccb.belgium.be/, and **693** technical posts on X, informing Belgian organisations about emerging threats, disclosed vulnerabilities and available patches.

[9] The Belgian ISPs and hosting providers of the targeted organisations received daily email messages.

[10] All targeted organisations were contacted daily by telephone and email.

The threat intelligence analysis and detection efforts were supported by the IoCs and context shared through the **published MISP events**, which were related to major observed threats, including ransomware, DDoS attacks, APT state-sponsored threats, PDF editor AppSuite, and different vulnerabilities**.**

> As of 2025, **331 Belgian organisations** were onboarded on the MISP and benefited from shared threat intelligence derived from **1.075 events** created by the CCB in 2025.

Additionally, under the **Access Journey Program (AJP)** [11] the CCB in cooperation with BitSight offer to Belgian organisations a service that focuses on helping organizations gain visibility over their external attack surface. This program enables organisations to obtain temporary free access to BitSight and regular training on the different features and capabilities of the platform, with in mind a focus on remediating issues and minimizing the attack surface.

> **2025 marked a year of strong growth for AJP:** the CCB invited **90 organisations**, 3 times more than in 2024, when 28 organisations joined the program. Of these, **58** were active in the healthcare sector, which was the core focus for 2025, thus demonstrating the success of the CCB's pro-active, targeted campaign towards this industry.

The feedback received by the CCB for the 2024–2025 period indicates a **high level of satisfaction among stakeholders**.

> Overall satisfaction reached 88%, with particularly strong results for advisor satisfaction (91%) and CCB communication (91%), reflecting the perceived quality of engagement and support. Portal satisfaction, while slightly lower at 85%, remains high and suggests a generally positive user experience, with limited scope for further improvement.

Spear warnings

The CCB continued to send spear warnings to Belgian organisations informing them of (potential) security issues and providing recommendations and remediation actions to help them effectively prioritise and mitigate security risks and improve the overall resilience to threats.

For the entire year the CCB kept an upward trend, sending a total of **32.005 spear warnings**, which represent a **42.77% increase** compared to 2024.

> The increase is likely driven by a combination of factors, including the expanding attack surface and greater prevalence of cyber security risks. At the same time, improved monitoring, data sources, and analytical processes have enabled the identification of a larger number of actionable issues. Overall, this trend underscores both the growing complexity of the threat landscape and the critical importance of timely notification as a pro-active cybersecurity measure.

[11] Participants receive up to 90 days of access per year, split into two phases of 45 days each.

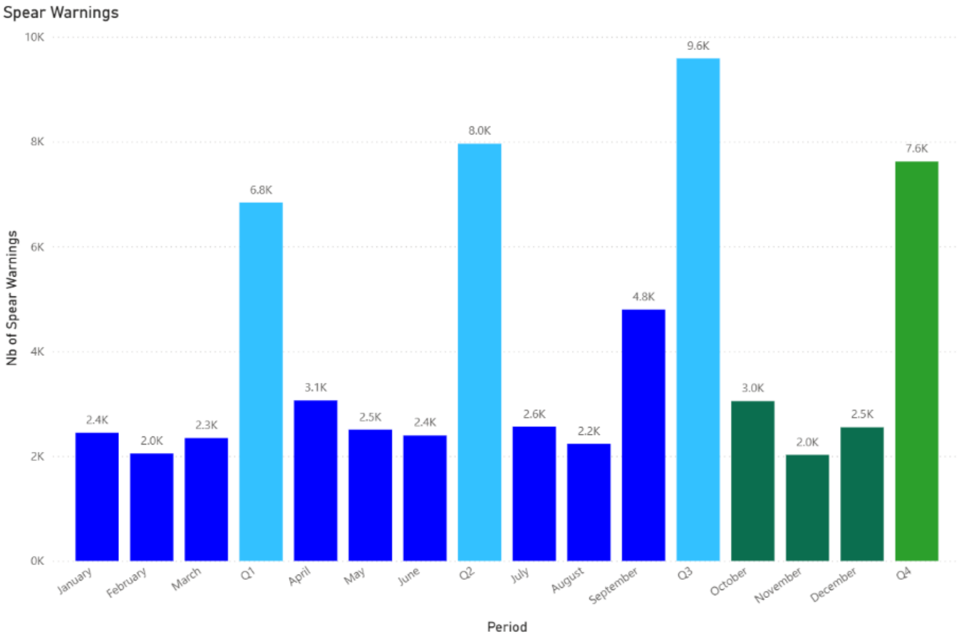


Figure 13: Number of spear warnings sent in 2025

When labelling the spear warnings by security issue, **53.28% (16.521)** of the spear warnings sent in 2025 **relate to vulnerabilities** and **exposures**, while 22.74% concern other security misconfigurations, including TLS certificates, web application headers, and DNS and email configurations. The pattern identified at the annual level is consistently visible across all quarters.

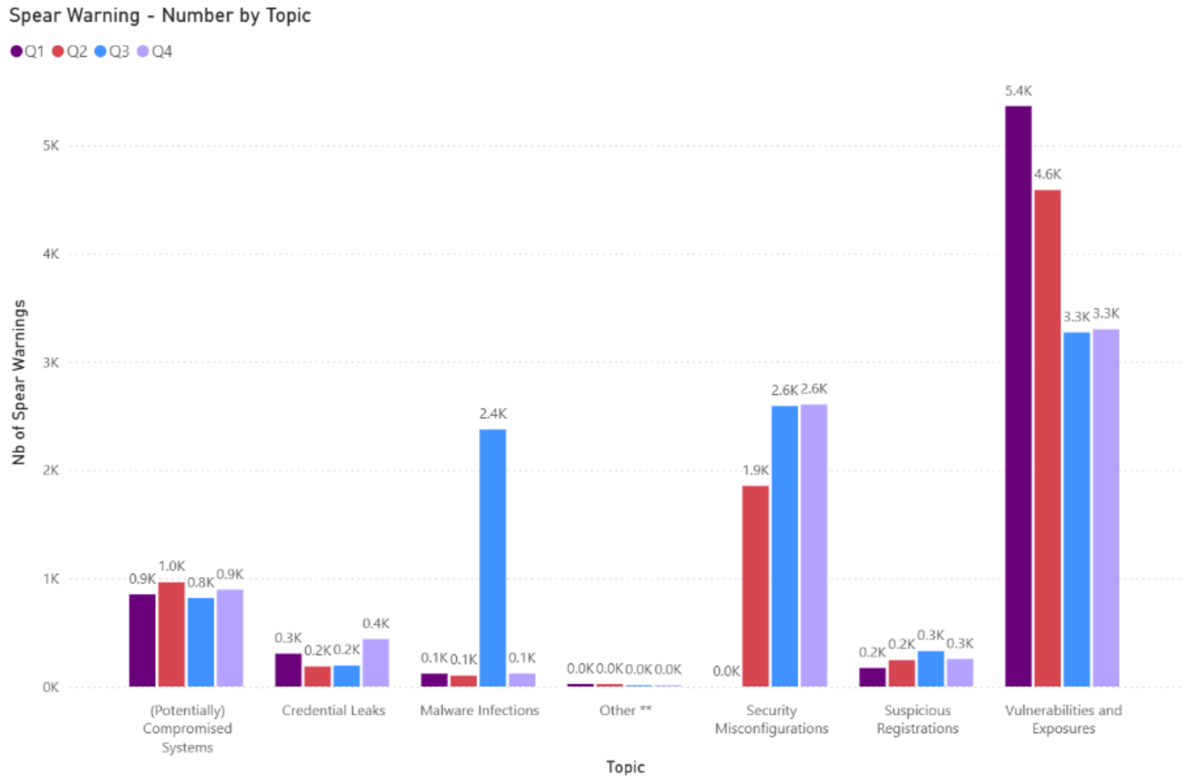


Figure 14: Number of spear warnings sent in 2025 based on the topic

During 2025, the CCB launched multiple **spear warning campaigns** on **vulnerabilities** and **exposures** based on data provided by partners as well as on internally constructed queries for Shodan and Censys. A single campaign, such as one targeting a specific vulnerability, may rely on multiple sources and scan data from several sources is often combined to maximise the effectiveness of the spear warnings.

> The proactive approach of informing organisations about disclosed vulnerabilities and identified vulnerable instances has proven highly effective in preventing potential incidents or mitigating their impact. This approach not only enables organisations to patch critical vulnerabilities in a timely manner but also strengthens overall cybersecurity resilience by reducing the attack surface available to threat actors. The **success** is illustrated by the actions taken in the case of several major vulnerabilities disclosed in 2025, such as **CVE-2025-53770** aka *ToolShell*, **CVE-2025-22457** in Ivanti EoL, or **CVE-2025-55182** aka *React2Shell*.

Additionally, as part of the **Counter Ransomware Initiative (CRI)**, the CCB prioritises the launch of spear warnings for vulnerabilities exploited in ransomware operations, aiming to minimise the impact of ransomware activity in Belgium.

> In 2025, **57 spear warning campaigns** were initiated, **addressing 27 unique vulnerabilities** recognized by CISA as being **exploited by ransomware actors**. In addition to those identified by CISA, other vulnerabilities that are highly likely to be exploited by ransomware groups were also addressed.

In 2025, the CCB tracked **feedback** from recipients of spear warnings, achieving an average response rate of 5.28%. Most responses were positive, with recipients expressing gratitude for the notifications and confirming that they had patched their systems.

> Feedback sentiment was categorized into 3 groups. **Positive feedback** comprised responses where recipients thanked CCB and confirmed actions taken to enhance their security. **Neutral feedback** included those who either viewed the issue as a false positive, sought confirmation of the warning's legitimacy, or informed CCB of actions taken without expressing gratitude, with most responses falling into the latter. **Negative feedback** involved specific criticisms and negative opinions about the spear warning project.

Awareness

Throughout 2025, the CCB further strengthened its Connect & Share initiative as a key platform for cybersecurity awareness, knowledge exchange and community building. Under this umbrella, CCB organized **15 events**, compared to 8 events in 2024, including QCTR events, Cyber Tips webinars, multiple sessions dedicated to the NIS2 regulation, and events in cooperation with external partners such as SANS, MITRE, and Belnet, reaching more than **13.000 participants** from **87 countries**.

Through these activities, Connect & Share continued to support CCB’s mission by bringing together cybersecurity professionals from government, industry, and academia to exchange insights, share best practices, and address emerging cyber threats.

Compared to 2024, which featured several large-scale, high-visibility events, the CCB adopted a **more targeted and cost-efficient approach** in 2025. As a result, CCB organized 88% more events - mostly online - that were tailored to the needs of its constituents and international partners, reaching a wide variety of audiences from advanced cybersecurity experts to IT professionals responsible for cybersecurity in SMEs, from C-level executives to middle management, at national, EU, and global levels.

OUTLOOK

We assess with high confidence that the main categories of cyber threat activity observed in 2025 will persist in 2026. While no fundamental shifts in the cyber threat landscape are anticipated, adversary behaviour is expected to continue evolving in response to geopolitical developments, regulatory and law-enforcement pressure, and technological advances.

Key cross-cutting trends include:

- Increased automation and continued refinement of attack methods;
- Widespread adoption of AI and LLMs, transitioning from exception to norm;
- Further maturation of as-a-Service (aaS) ecosystems, increasing scale and efficiency.

Belgian organisations are expected to remain under sustained pressure from ransomware, DDoS attacks, and account compromise. Ongoing geopolitical developments are likely to influence targeting priorities and sustain elevated levels of cyber activity in Belgium, increasing the risk of state-sponsored compromise for espionage or infrastructure abuse.

Threats by actor type

Financially motivated cybercriminals

Financially motivated actors are expected to remain the primary source of cyber risk in 2026.

- **Ransomware, data theft, and multi-layered extortion** will remain the most financially disruptive cybercrime globally;
- **Supply chain attacks** (e.g. CLOP, Qilin) have demonstrated the value of upstream compromise and are likely to be increasingly prioritised;
- Initial access techniques will continue to include **phishing, vishing**, and exploitation of **zero-day vulnerabilities**, including MFA bypass scenarios;
- Declining ransom payment rates may push groups to refine coercion tactics, diversify revenue streams, increase secondary monetisation via data resale and fraud.

Hacktivist collectives

Hacktivism is expected to remain closely aligned with state interests, particularly in the context of ongoing geopolitical conflicts. As long as geopolitical conflicts involving cyber-capable states endure, hacktivist operations are likely to remain an extension of state influence, particularly targeting countries perceived as supporting opposing parties.

- **Pro-Russian DDoS activity** is likely to remain a high-volume threat to Belgium and other European countries;
- Activity is expected to concentrate among a limited number of **operationally mature groups**, such as NoName057(16);
- Hacktivist threats may increasingly extend to **OT environments**, as observed in 2025, increasing the risk associated with the potential impact of such attacks.

State-sponsored threat actors

State-sponsored cyber activity is expected to remain a core instrument of geopolitical strategy.

- Threat actors linked to **China**, **Russia**, **Iran**, and **North Korea** will continue to pursue espionage, disruption, and influence operations;
- Activity will focus on **high-impact vulnerabilities** in widely deployed technologies;
- **Russian** state-sponsored threat actors are likely to target Belgium and other European countries amid heightened European defence rhetoric toward Russia;
- **China**-nexus actors are expected to remain the most persistent and technically advanced, particularly targeting edge devices and zero-day vulnerabilities;
- **Iranian** actors are expected to continue semi-deniable operations that blur espionage, disruption, hacktivism, and financial activity, in the absence of significant geopolitical or domestic changes;
- **North Korean** actors are likely to sustain revenue-generation operations, cyber espionage and attempts to place remote IT workers in European organisations.

Methods and techniques

Phishing and initial access services

- Phishing will remain a keystone initial access vector in 2026;
- Innovations in social engineering are expected to persist, including: ClickFix abuse, malvertising, weaponised documents and PDF editors, or sophisticated BEC lures;
- The availability of Phishing-as-a-Service (PaaS) will continue to lower barriers to entry.

Supply Chain and Third-Party Attacks

- Supply chain compromises are expected to increase in **frequency and sophistication;**
- Likely targets include CI/CD pipelines, developer tooling, managed service providers, widely deployed SaaS platforms;
- **Worm-like automation** and pre-authentication exploitation may enable rapid propagation before detection.

Vulnerability Exploitation

- Vulnerability disclosure volumes are expected to remain high;
- Threat actors will prioritise high-impact initial access vulnerabilities affecting ubiquitous technologies;
- AI-assisted vulnerability research and exploit development is likely to further reduce the time between disclosure and exploitation.

Credential leaks

- The exploitation of leaked and stolen credentials will remain a prominent attack vector;
- Credential abuse will continue to enable account compromise, lateral movement, privilege escalation;

- This activity will remain closely linked to phishing campaigns, MaaS, and RaaS ecosystems, reinforcing its role as a low-cost, high-impact enabler.

APPENDIX 1: KEY RECOMMENDATIONS[12]

Account compromise

Recommendation	MITRE ATT&CK mitigation	CyFun® 2025 alignment[13]	Impact
Strengthen identity security as a baseline control Enforce multi-factor authentication for all external-facing and privileged accounts	Multi-Factor Authentication (M1032) Privileged Account Management (M1026)	**Prevent** (PR.AA-01, PR.AA-05) – reduce exposure to credential-based attacks **Protect** (PR.AA-03) – strengthen identity and access security	Reduces the success rate of credential theft and limits escalation following initial compromise.
Improve detection of anomalous account behaviour Promote behavioural monitoring, centralized identity logging, and rapid response capabilities to identify compromised accounts early.	User Behavior Analytics (M1047) Audit and Log Configuration (M1047)	**Detect** (DE.CM-01, DE.CM-03) – enable early identification of account compromise **Respond** (RS.MA-01) – support rapid containment	Reduces attacker dwell time and prevents secondary abuse of trusted accounts.
Reinforce targeted user awareness and training Focus awareness efforts on spear-phishing, CEO fraud, and customer- and partner-facing abuse scenarios.	User Training (M1017)	**Prevent** (PR.AT-01) – reduce human-enabled attack vectors **Prepare** (PR.AT-01) – increase organisational cyber maturity	Reduces the likelihood of successful social engineering and downstream financial and reputational damage.

[12] mapped to MITRE ATT&CK mitigation areas and CyFun® 2025 objectives.

[13] CyFun® 2025 verbs and control codes refer to the CyFun® 2025 framework and indicate the primary cybersecurity function(s) supported by each recommendation. The codes such as PR.AA-01, PR.DS-11, DE.CM-01, etc., correspond to CyFun® 2025 control definitions derived from the CyFun® 2025 booklet: https://cyfun.eu/en/cyberfundamentals-framework-2025#:~:text=The%20levels%20and%20key%20measures. They follow the Govern / Identify / Protect / Detect / Respond / Recover structure aligned with international standards.

Ransomware

Recommendation	MITRE ATT&CK mitigation	CyFun® 2025 alignment	Impact
Strengthen ransomware resilience through core cyber hygiene Improve patch management, secure configuration, employee awareness, and the adoption of zero-trust principles.	Vulnerability Scanning (M1016) Network Segmentation (M1030)	**Prevent** (ID.RA-01) – reduce exposure to exploitable vulnerabilities **Protect** (PR.DS-01) – strengthen baseline system and network security	Reduces the likelihood of ransomware compromise and limits attack propagation.
Strengthen backup and recovery resilience Implement regular offline or immutable backups and test restoration procedures.	Data Backup (M1053) System Recovery (M1058)	**Protect** (PR.DS-11) – safeguard critical data and services **Recover** (RC.RP-01) – enable timely service restoration	Limits downtime and significantly reduces ransomware extortion leverage.
Harden endpoint and server environments against ransomware execution Apply application control, timely updates, and strict limitation of administrative privileges.	Application Control (M1045) Privileged Account Management (M1026) Update Software (M1051)	**Prevent** (PR.IP-01) – limit ransomware execution paths **Protect** (PR.AA-05) – reduce lateral movement and blast radius	Reduces the likelihood of successful ransomware deployment and spread.
Prepare for data-centric extortion and data leakage scenarios	Data Loss Prevention (M1057) Audit and Log Configuration (M1047)	**Detect** (DE.CM-01) – improve visibility of data theft activity **Respond** (RS.MA-01) – limit	Limits financial, legal, and reputational consequences of ransomware incidents.

Enhance data classification, access controls, and monitoring of anomalous data exfiltration.		regulatory and reputational impact	
Reduce exposure to supply-chain ransomware attacks Require suppliers to demonstrate timely patching, vulnerability management, and incident notification.	Software Supply Chain Security (M1051) Exploit Protection (M1050)	**Prevent** (ID.AM-08) – reduce third-party entry points **Protect** (PR.DS-01) – limit cascading cross-sector impact	Mitigates large-scale, cross-sector ransomware incidents resulting from third-party compromise.

DDoS/Hacktivist activity

Recommendation	MITRE ATT&CK mitigation	CyFun® 2025 alignment	Impact
Improve baseline DDoS resilience for public-facing services Adopt DDoS protection, traffic filtering, and scalable hosting.	Network Traffic Filtering (M1037) Redundancy (M1027) System Recovery (M1058)	**Protect** (PR.DS-01) – strengthen availability of essential services **Recover** (RC.RP-01) – enable rapid service restoration	Limits service downtime and reduces the effectiveness of DDoS campaigns.
Strengthen preparedness and coordinated response mechanisms Define DDoS response procedures and escalation paths with ISPs and hosting providers, building on the CCB's existing coordination framework.	Incident Response (M1046)	**Respond** (RS.MA-01) – enable faster mitigation and coordination **Recover** (RC.RP-01) – reduce duration of service disruption	Shortens disruption windows and limits operational and reputational damage.
Reduce exposure from third-party hosting dependencies Encourage use of trusted and resilient hosting infrastructures.	Network Segmentation (M1030) Redundancy (M1027)	**Prevent** (ID.AM-08) – reduce single points of failure **Protect** (PR.DS-01) – strengthen systemic resilience	Improves continuity of public services and limits cascading disruption.

State-sponsored related activity

Recommendation	MITRE ATT&CK mitigation	CyFun® 2025 alignment	Impact
Strengthen vulnerability management for high-value systems Prioritise patching and mitigation of publicly disclosed vulnerabilities.	Vulnerability Scanning (M1016) Update Software (M1051)	**Prevent** (ID.RA-01) – reduce exploitable attack surfaces **Protect** (PR.IP-01) – limit rapid initial access	Reduces exposure to large-scale exploitation and espionage campaigns.
Strengthen identity security and access control Enforce MFA, least privilege, and regular access reviews.	Multi-Factor Authentication (M1032) Privileged Account Management (M1026) User Account Management (M1018)	**Prevent** (PR.AA-01) – reduce credential-based access **Protect** (PR.AA-05) – limit persistence and lateral movement	Reduces the effectiveness of spear-phishing and long-term espionage.
Enhance protection and monitoring of sensitive entities Apply strengthened email, web, and network monitoring.	Email Filtering (M1021) Network Traffic Filtering (M1037) Audit and Log Configuration (M1047)	**Protect** (PR.DS-01) – safeguard sensitive institutions **Detect** (DE.CM-01) – enable early identification of espionage activity	Limits intelligence collection and attacker persistence.
Anticipate AI-enabled threat evolution Integrate AI-related threat scenarios into planning and detection strategies.	Threat Intelligence Program (M1019)	**Prepare** (GV.RM-03) – anticipate future threat evolution **Detect** (DE.AE-03) – adapt to automated attacks	Improves long-term resilience against evolving state-sponsored capabilities.

ABOUT THE CCB

The **Centre for Cybersecurity Belgium (CCB)** is the national authority for cybersecurity in Belgium. The CCB supervises, coordinates and monitors the application of the Belgian cyber security strategy. Through optimal information exchange, companies, the government, providers of essential services and the population can protect themselves appropriately.

The Centre for Cybersecurity Belgium (CCB) was established by Royal Decree of 10 October 2014 and operates under the authority of the Prime Minister.

The **CyTRIS (Cyber Threat Research and Intelligence Sharing)** Department of the Centre for Cybersecurity Belgium monitors cyber threats and publishes regular reports. The Team collects, analyses and distributes information on threats, vulnerabilities and attacks on the information and communication systems of Belgium's vital sectors (critical infrastructure, government systems, critical data).

CyTRIS is also responsible for the Early Warning System (EWS). The EWS includes the information exchange platforms of the Belgian CSIRT. CyTRIS is responsible for the operational communication and information exchange with other national CSIRT. CyTRIS also provides the "Spear Warning" procedure. A "Spear Warning" is an individual warning about an infection or vulnerability sent to organisations.

The CCB Connect & Share events, such as the Quarterly Cyber Threat Report (QCTR) events organised by CyTRIS, bring together different stakeholders and consultation platforms at least once a quarter and inform all participants about the active cyber threats.

Our events are also offered as a webinar and are open to anyone, for prior editions check out our YouTube channel: https://www.youtube.com/@cybersecuritybelgium.