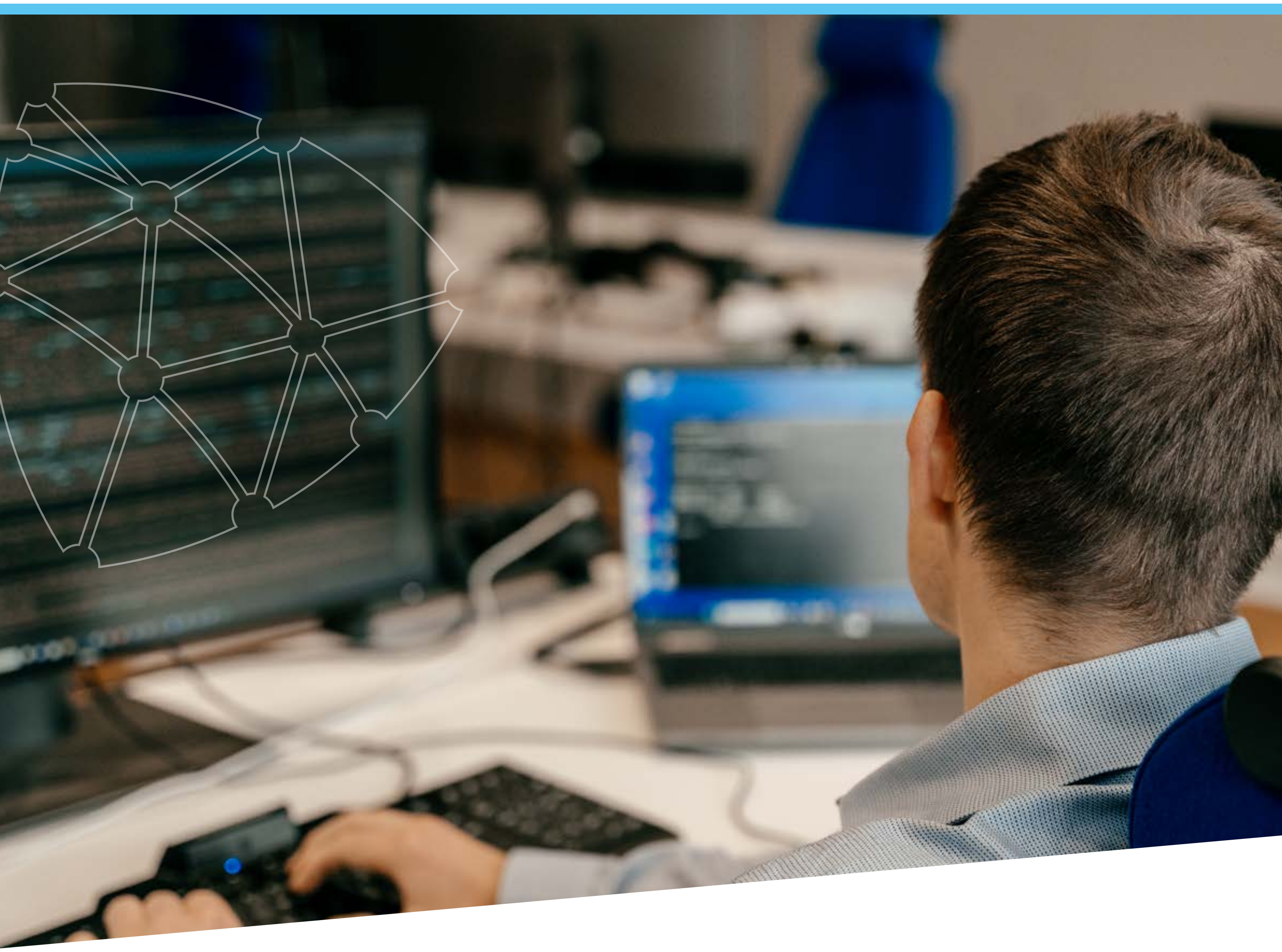
CENTRE FOR
CYBERSECURITY
BELGIUM



# EMPOWERING CYBERSECURITY

## CCB REPORT 1/1/2023 - 30/9/2023

**Centre for Cybersecurity Belgium**
*Under the authority of the Prime Minister*

.be

# Table of Contents

Director’s Brief 3

National Projects and International Priorities 5

The rotating Presidency of the Council of the EU 6

NIS2: Impact on Belgian sectors and entities 7

The CyberFundamentals framework 8

Safeonweb @work 9

Safeonweb Browser Extension 10

Promoting innovation in cybersecurity for Belgian SMEs: Financial Support for Third Parties (FSTP) 11

Cyber Threat Landscape in 2023 13

The current Cyber Threat Level 14

The Anti-Phishing Project 18

Active Cyber Protection - spear warnings 22

Critical Vulnerabilities 27

Critical vulnerabilities that have sharped the cyber threat landscape between January and September 2023 28

Belgium Cyber Metrics in 2023 30

Overview of Belgium Cyber Metrics in 2023 30

Connect & Share Events 32

Raising awareness and building a strong community of cybersecurity experts 32

Belgium in the World 35

Belgian cybersecurity ranking 36

Belgium’s cyber champions: The Red Daemons at the ECSC 2023 37

Cyber Spotlight: AI & Cybersecurity 39

Who are we? 43

# Director’s Brief

Improving national cybersecurity and reducing a country’s vulnerability is a very challenging mission. Cyberspace is almost entirely a private environment, making it difficult for government services to protect, detect and respond to threats and incidents.

As in most countries, the Centre for Cybersecurity Belgium (CCB) is working to build resilience through national and international collaboration, public-private partnerships, information sharing, capacity building and training, awareness raising, research, AI driven detection and response, Quantum ready crypto, national cybersecurity exercises, etc. All these actions are necessary and useful, but not enough. Despite all these measures, cybercrime and online fraud are on the rise.

These measures seem to be too high level and often do not lead to concrete actions and results without being translated into smaller, more concrete, targeted projects and services. You have not run a marathon until you have run the last mile! And that is what we want to do at the CCB, to run that last mile for all these important concepts and initiatives. We want to ask ourselves each time:

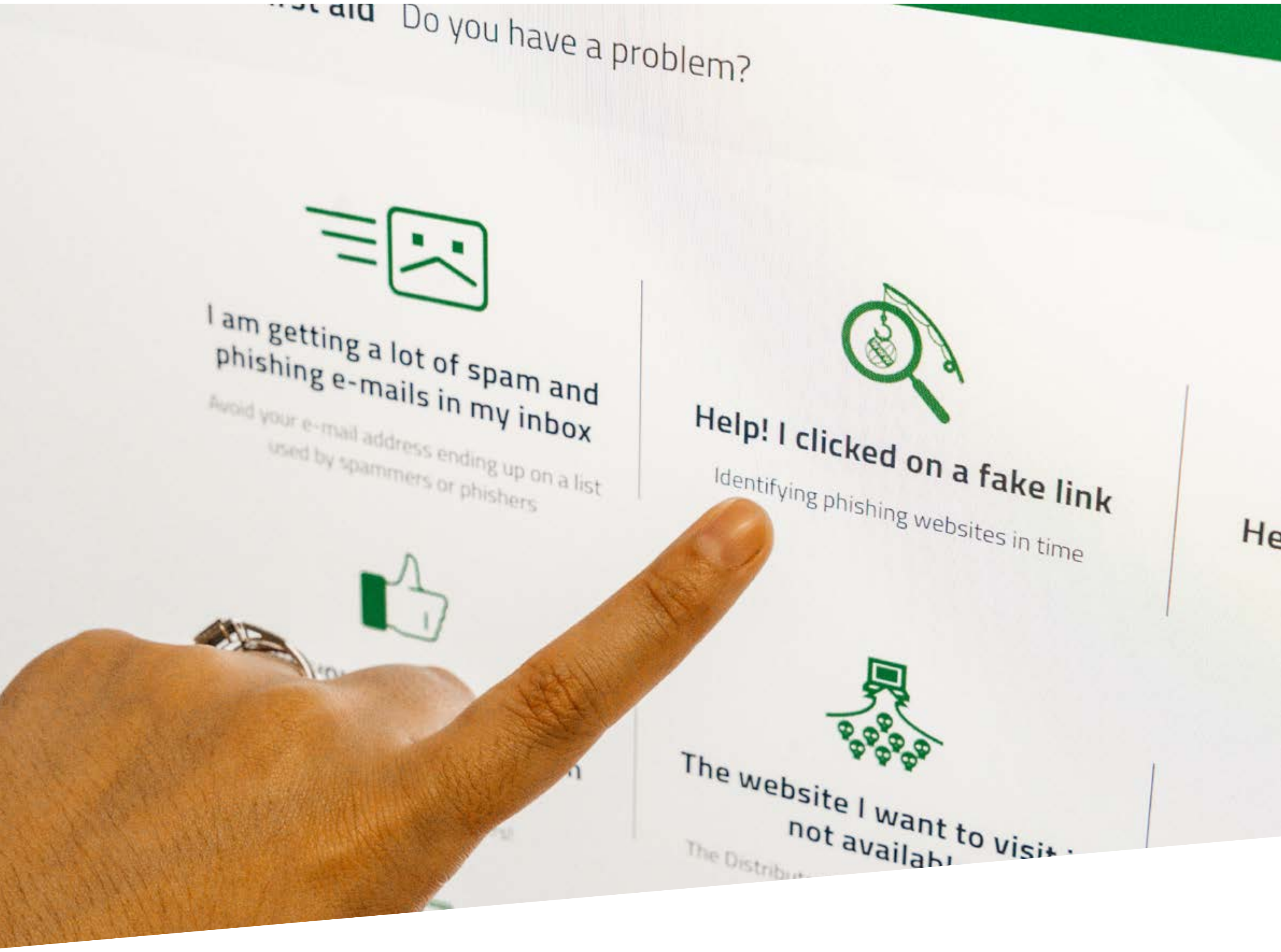
> What does this really mean for citizens, businesses, government or critical infrastructure?

Running the last mile has been translated into an Active Cyber Protection (ACP) policy with five sub-areas. We want to involve the owners of the threatened systems or accounts, filter communications with 100% malicious infrastructure at national level, make cybersecurity a routine domain accessible to all companies, identify vulnerable systems in Belgium and warn the owners directly (Spear Warning) and finally encourage the development of validated services so that anyone receiving information via the Internet can see whether the identity of the sender has been validated or not.

Assessing the evolving cyber threat landscape and responding with concrete projects together with our partners is the core business of the CCB. We have to make sure that our customers see us coming, running the last mile.

**Miguel De Bruycker**
Director General
Centre for Cybersecurity Belgium

Brussels, December 2023



st aid Do you have a problem?

I am getting a lot of spam and phishing e-mails in my inbox

Avoid your e-mail address ending up on a list used by spammers or phishers

Help! I clicked on a fake link

Identifying phishing websites in time

He

The website I want to visit not availabl

The Distribu

# NATIONAL PROJECTS AND INTERNATIONAL PRIORITIES

Through its projects and initiatives aimed at increasing the level of cybersecurity and resilience of public institutions, companies, academia and end users, the Centre for Cybersecurity Belgium, as the national authority for cybersecurity, is actively involved in making Belgium one of the least vulnerable countries in Europe in terms of cybersecurity by 2025.

## The rotating Presidency of the Council of the EU

From 1 January to 30 June 2024, Belgium will hold the rotating Presidency of the Council of the EU.

During this period, the CCB will assume its international responsibilities and play a leading role in promoting the Belgian priorities and the Presidency's program in the field of cybersecurity to other Member States and abroad, with the aim of promoting Objective 6 of our National Cybersecurity Strategy: maintaining Belgium's clear international engagement and commitment in the field of cybersecurity.

### THE CHAIRMANSHIP COMES WITH OBLIGATIONS AND OPPORTUNITIES

The CCB will ensure the rotating chairmanship of several official European cybersecurity networks in which it is the officially appointed representative of Belgium (such as the NIS Cooperation Group, the EU Cybercrisis Liaison Network - EU-CyCLONe, and the EU-CSIRTs Network). The CCB will follow up on the legal responsibilities of these networks and will chair, set the agenda and host meetings of all these groups in different locations in Belgium, also to showcase our country.

At a time when the transposition of the NIS2 Directive into national legislation is entering its final stage, the need for coordination within all these networks will be essential. Within the EU CyCLONe network, it will also be up to Belgium and the CCB to finalise the first report to the Council and the EU Parliament.

In the event of major cybersecurity incidents, the CCB will also have to play a leading role in coordinating the European response, both within the EU CyCLONe network and the EU CSIRTs network.

### AND THE ELECTIONS

It should be noted that the Belgian Presidency will be marked not only by national and regional elections, but also by the European elections, to be held on 6-9 June 2024. Given the geopolitical context, these elections may result in cybersecurity-related events or increased threats with an impact on the EU, which will require enhanced cooperation at crisis management level, as well as at technical level.

The CCB will also play a leading role in the legislative and policy work within the Council Working Group on Cybersecurity Issues. We will support the Belgian attachés in the Council to achieve the Belgian objectives and to advance or finalise the work on important files such as the Cyber Resilience Act, the Cyber Solidarity Act or the amendments to the Cybersecurity Act. We will also support them holding a European stock taking on of the state of EU cybersecurity policy, leading to Council Conclusions on the future of cybersecurity.

## NIS2: Impact on Belgian sectors and entities

In order to address the expanding cyber threat landscape and the emergence of new challenges, the European Union has adopted a new piece of legislation concerning measures for a high common level of cybersecurity across the Union (Directive 2022/2555 of 14 December 2022 - the so-called "NIS2 Directive"), which replaces the "NIS1 Directive" (Directive 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union).

The NIS2 Directive has introduced some important changes compared to the NIS1 Directive: expansion of the sectors and entities covered, new selection and registration methods, more cybersecurity requirements, new deadlines for reporting incidents, strengthening of monitoring mechanisms.

The NIS2 Directive also aims to improve national capacities and cybersecurity policies. In terms of national policies, this includes the national cybersecurity strategy, national cyber crisis management frameworks, the roles of competent authorities and national or international cooperation.

### COORDINATION AND IMPLEMENTATION OF THE NIS2 DIRECTIVE

As the national cybersecurity authority, the CCB will play a key role in the coordination and implementation of this Directive. The CCB will ensure the tasks of competent authority for all sectors (in cooperation with potential sectoral authorities), national CSIRT, national single point of contact, representative in the cooperation group, CSIRT network and CyCLONe.

With regard to cybersecurity risk management measures, essential and important entities must take appropriate and proportionate technical, operational and organisational measures to manage the risks to the security of the network and information systems that those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on the recipients of their services. These measures are based on an all-hazards approach, for which the CCB has provided clear guidance through the adoption of the CyberFundamentals Framework. To this end, organisations will benefit from a presumption of compliance if they obtain a CyberFundamentals or ISO/IEC 27001 certification/label.

As a national CSIRT, the CCB will receive notification of significant incidents from NIS entities in order to mitigate the potential spread of incidents, enable entities to seek assistance, manage crisis situations in the best possible way and share relevant technical information with other entities.

Finally, the CCB, through its inspection service (in cooperation with potential sectoral authorities), will also play a role in the supervision of the entities concerned.

## The CyberFundamentals framework

In the field of cybersecurity, there are international frameworks and various international standards. Organisations in Belgium are aware of these frameworks, but they generally lack a specific interpretation for the Belgian situation and remain at a high level. This means that the measures that organisations can take have to be determined in a risk-based manner, which poses specific difficulties for organisations that do not necessarily have or employ cyber specialists.

In order to give substance to the mission of the Belgian National Cybersecurity Strategy 2.0, which is also the mission of the Belgian Centre for Cybersecurity – Belgium must be one of the least vulnerable countries in Europe in the cyber domain by 2025 – the CCB Certification Authority has developed the ‘CyberFundamentals’ framework.

### REDUCE THE RISK OF CYBER ATTACKS

This framework aims to protect our data, significantly reduce the risk of cyber attacks and increase the resilience of Belgian organisations.

With this holistic, risk-based approach, we want to increase trust in the digitalisation of society by sharing our knowledge and providing insight into various cyber threats. We do this by incorporating real data we receive from the Belgian Cyber Emergency Response Team (CERT) into the framework and using this, along with other methodologies, to validate the framework.

The framework is based on the globally recognised NIST-CSF framework and incorporates various elements of the ISO 27001 and ISO 62443 standards, which are widely used in Belgium, as well as elements of the CIS Security Framework. The Identify, Protect, Detect, Respond and Recover functions form the common thread throughout the framework, which is written as a conformity assessment scheme to demonstrate compliance or non-conformity with the measures in the framework.

### LEVELS OF ASSURANCE

In addition, the framework is aligned with the levels of assurance in the Cyber Security Act and includes three levels of assurance: ‘Basic’, ‘Important’ and ‘Essential’, supplemented by an entry level ‘Small’. In this way, and partly by incorporating a maturity approach, the framework aims to provide a proportionate response to the needs of small to large organisations so that they can incrementally improve their cybersecurity.

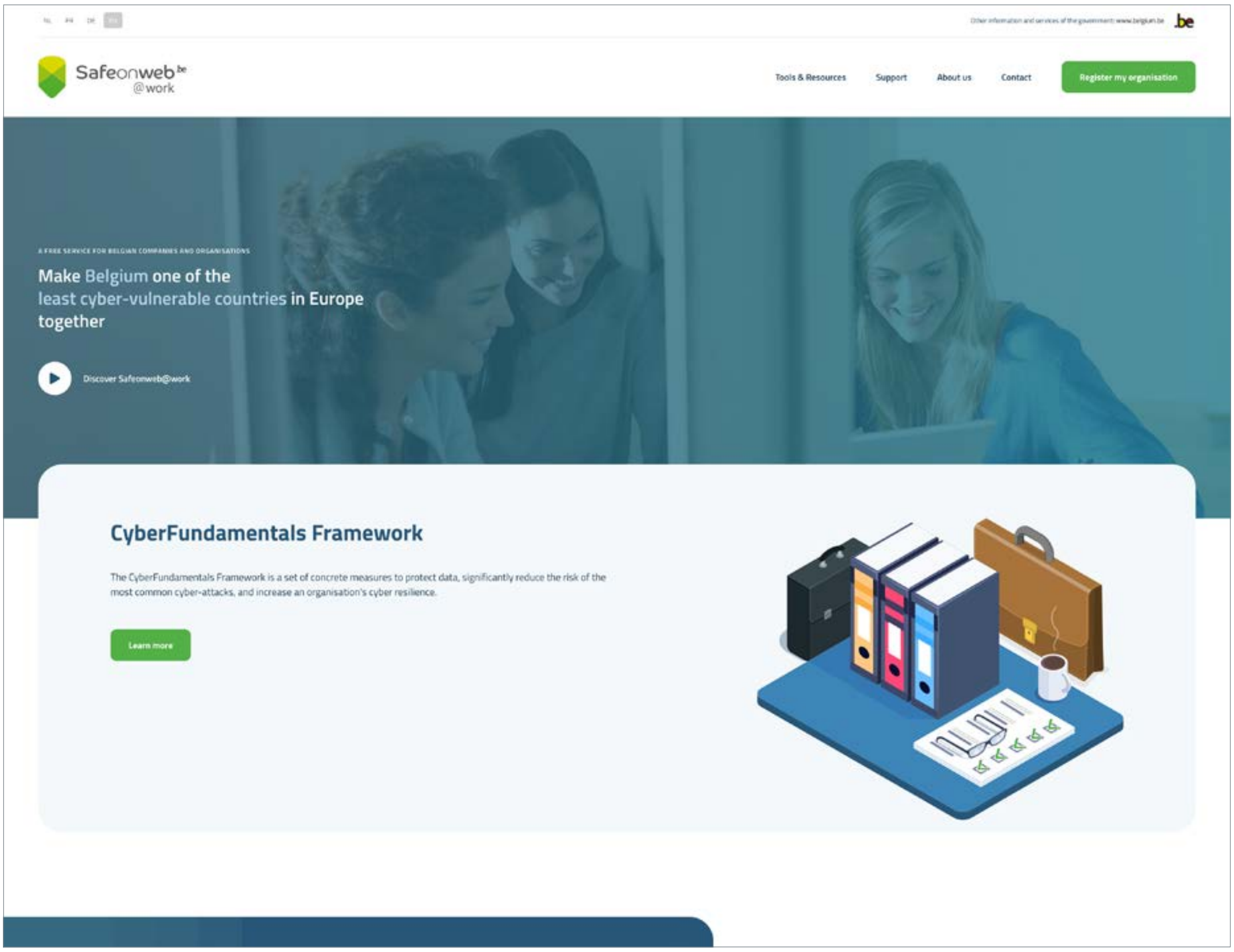
Finally, to support the implementation of this framework, the CCB offers several tools, ranging from a risk analysis to determine the level of assurance required under NIS2, to a self-assessment tool and a mapping to the various frameworks and standards that form the basis of the framework.

The framework and tools are freely available.

www.cyfun.be

## Safeonweb @work

**Safeonweb@work** is an initiative aimed at Belgian organisations and companies. Its objective is to strengthen their cybersecurity by providing them with advice, recommendations, and tools to identify and mitigate the vulnerabilities of their systems and to be alerted to cyber threats. Through its various services, organisations can pro-actively implement the appropriate measures to significantly reduce the risk of cyber attacks, and ultimately participate in our objective of making Belgium one of the least cyber vulnerable countries in Europe by 2025.



A FREE SERVICE FOR BELGIAN COMPANIES AND ORGANISATIONS

Make Belgium one of the least cyber-vulnerable countries in Europe together

CyberFundamentals Framework

The CyberFundamentals Framework is a set of concrete measures to protect data, significantly reduce the risk of the most common cyber-attacks, and increase an organisation's cyber resilience.

### SAFEONWEB@WORK SERVICES INCLUDE:

**Cyber Threat Alerts**
A service providing early warning of threats to the network. Safeonweb@work sends a specific alert if a vulnerability or an infection has been reported on the registered network in the platform.

**Quick Scan Report**
A service allowing you to receive a report that will give an overview of the organisation's assets, identify potential vulnerabilities and recommendations for remediation.

**Policy templates**
A set of customizable and editable cybersecurity policy documents to facilitate the implementation of information security management within an organisation.

**Self-assessment**
A self-assessment form allowing to evaluate an organisation's cybersecurity maturity level and benefit from our practical recommendations to fill any gaps identified.

**Content**
News, tips, warning, webinars, recommendations on cybersecurity best practices and main threats, as well as various tools aiming to improve the level of cybersecurity of an organisation.

atwork.safeonweb.be

## Safeonweb Browser Extension

The CCB developed the Safeonweb Browser Extension which helps citizens and organisations in assessing whether the identity of the website owner has been thoroughly validated or not. Website reliability could result from this. The Extension is free of charge and provides information regarding the verification of the ownership of the website, not its content.

### HOW DOES THE SAFEONWEB BROWSER EXTENSION WORK?

The Extension allocates a score to the websites:

**Green (OK)**
score of 4 out of 4: the website owner has an Extended Validation Certificate issued by a Certificate Authority or the site owner is registered on atwork.safeonweb.be (for Belgian organisations only).

Therefore:

- It should be OK to continue surfing on this website.
- It should be OK to share data on this website.

**Amber ( ! )**
scores from 1 to 3 out of 4: the website owner has an Organisation Validation Certificate, or a Domain Validation Certificate issued by a Certificate Authority, and the website is not registered on atwork.safeonweb.be

Therefore:

- It should be OK to continue surfing on this website.
- If any doubts, refrain from sharing data on this website.

**Red (X)**
score of 0 out of 4: the website lacks basic security features or is known as malicious. The website owner has no Certificate and therefore has not been validated.

Therefore:

- We advise against browsing this website and sharing any data.

More information about the project and about how to install instructions are available at:

- https://safeonweb.be/en/safeonweb-browser-extension
- https://atwork.safeonweb.be/protect-my-organisation/safeonweb-browser-extension

## Promoting innovation in cybersecurity for Belgian SMEs: Financial Support for Third Parties (FSTP)

Financial Support for Third Parties (FSTP) is a project implemented by the **Belgian National Coordination Centre** (NCC-BE) within the CCB. This initiative focuses on leveraging EU investments, such as FSTP, to enable start-ups, SMEs and mid-cap companies to strengthen their cybersecurity capabilities, thus contributing to a safer digital environment.

### BOOSTING CYBER RESILIENCE FOR SMES

FSTP isn't just a fancy acronym, it's your passport to cyber resilience!

Known as 'cascading funding', FSTP is a key mechanism used by the European Commission to support start-ups and SMEs in promoting cybersecurity. NCC-BE is using FSTP to disseminate cutting-edge cybersecurity solutions, thereby strengthening Belgium's cybersecurity.

### FSTP IMPACT: STRONGER, SAFER, SMARTER!

The FSTP initiative is expected to deliver significant results that will positively impact Belgian cybersecurity in the following ways:

- Increased cyber resilience: SMEs will have greater access to innovative cybersecurity solutions, increasing their resilience to evolving cyber threats.
- Fostering innovation: Encouraging innovation within the SME sector will lead to the development of cutting-edge cybersecurity technologies, significantly improving Belgium's ability to combat sophisticated cyber threats.
- Public-private cooperation: Collaboration between the NCC-BE and private SMEs will enhance information sharing and promote a cohesive approach to cybersecurity, benefiting the nation's overall cyber resilience.
- Economic growth: By strengthening the cybersecurity posture of SMEs, the FSTP will contribute to economic growth by protecting critical digital assets and fostering an enabling environment for business operations.

The FSTP, led by the NCC-BE, is central to maintaining Belgian cybersecurity in line with European cyber-security objectives. Stay tuned for further updates on the CCB and NCC-BE channels.

Funding & tenders (europa.eu)

# CYBER THREAT LANDSCAPE IN 2023

# The current Cyber Threat Level

## THE GLOBAL CYBER THREAT LANDSCAPE

The global cyber threat landscape in 2023 continued to be marked by cyberattacks carried out by different threat actors, as hacktivist groups, ransomware groups and state-sponsored hacking groups. While cyber-criminals are mostly interested by financial gains, a strong link exists between geopolitics and cyber attacks conducted by hacktivist and state-sponsored actors.

### The Ukraine-Russia conflict

The Ukraine-Russia conflict, started in 2022, reactivated hacktivism and showed that hacktivist groups could represent an important capability and a way to attract attention in support of the physical and ideological activities during a conflict time. The hacktivist activity in 2023 was mostly related to the Russia – Ukraine conflict. From the beginning of the conflict, many hacktivist groups appeared on the online scene and highly increased their activity to support interests and politics of one of the sides involved in conflicts. Their favorite modus operandi was represented by disruptive Distributed Denial-of-Service (DDoS) attacks, web defacements and by hack-and-leak operations.

The pro-Russia hacktivist groups targeted not only Ukraine but also a lot of other countries in Europe, including Belgium. Their targets were mostly government and military entities, but also organisations in the energy, transportation (ports and airports), logistics, banking, telecommunication and even healthcare sectors. The attacks were conducted in retaliation for national military, financial, humanitarian, or political support offered by European countries to Ukraine and consistently mirrored Russian strategic objectives. Except from the hacktivist activity related to the Ukraine-Russia conflict, hacktivism has also been on the rise in different zones of the world, as these groups continue to respond to changing political societal issues and conflicts occurring worldwide. Political issues and social tensions, as well as ongoing conflicts in different zones of the world influenced the hacktivist activity in 2023.

### Ransomware

The cybercriminal activity was influenced by the macro-economic changes and saw significant transformations and developments as regards both the increase of capabilities and tactics used and the addition of new type of targets, such as governmental bodies, public institutions, and organisations in critical sectors.

Ransomware attacks remained the most important cybercriminal activity affecting organisations, including critical infrastructures, in Europe and the U.S. Ransomware operators primarily targeted the following industries: manufacturing, software and information technology (IT), healthcare, education, business and consulting services, law, finance and banking. Since the onset of the war in Ukraine it was observed an increase in ransomware attacks against municipalities and public sector institutions in European countries, including Belgium.

### APT campaigns and cyber espionage

Geopolitics remains the most important driver of APT campaigns development, whose prime goal continue to be cyber espionage (exfiltration and collection of sensitive data). APT attacks were mostly conducted by state-sponsored hacking groups and had a significant impact on the targeted infrastructure. Cybersecurity companies and national authorities reported through the entire year about multiple cyber espionage campaigns targeting mainly the governmental environment, but also some strategic sectors.

Well-known state-sponsored hacking groups, such as APT 28 (Fancy Bear), APT 29 (Cozy Bear), Emissary Panda, APT 33, Charming Kitten or Lazarus Groups, to name just some of them, continued to be globally active. There were also reports indicating intense activity against different European targets from new groups such as Storm-0978 that was reporting by Microsoft conducting a phishing campaign against the North Atlantic Treaty Organisation (NATO) Summit this year or Storm-0558 a threat actor also tracked by Microsoft, which primarily targets government agencies in Western Europe and focuses on espionage, data theft, and credential access. The state-sponsored threat actors were also observed developing and deploying new tools and capabilities against their targets, to maintain their persistence, to avoid detection and to complete their objectives.

## THE BELGIAN CYBER THREAT LANDSCAPE

In 2023, Belgian organisations were mainly victims of ransomware and DDoS attacks but were also affected by other categories of cyber incidents, as: data leaks, CEO frauds, threat leads on dark web and special forums with advertised stolen data and compromised Belgian IPs used in cyber operations.

### Ransomware

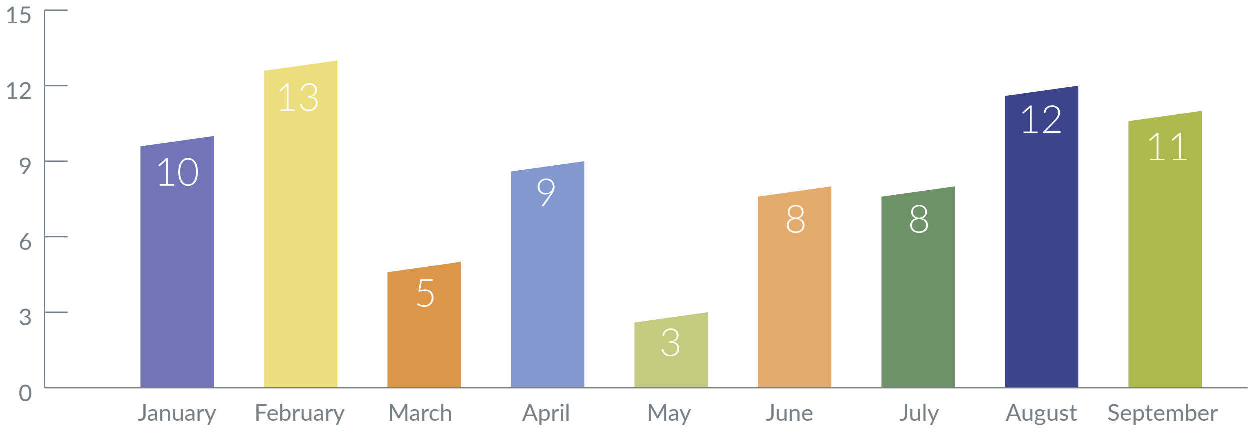
The same as in other European countries, ransomware remained the most important and constant cyber threat, as regards both the number and the impact. Ransomware attacks were conducted against Belgian organisations by different ransomware groups, including the most notorious ones as LockBit, Play or Cl0p.

According to our data, LockBit extorted the highest number of Belgian victims, which is consistent with the group's operations on a global scale.

Also, Cl0p ransomware gang's mass exploit of the MOVEit critical vulnerability has made it to the top of the ransomware threat actor hierarchy.

The targets were both private and public entities from different sectors, including government, local administration, healthcare, manufacturing, IT, food, and beverage. The impact varied from low to high depending on the targeted organisation, its cybersecurity infrastructure and the practices and policies in place. In some cases, cybercriminals engaged in double extortion and ransomware attacks were followed by data leaks and their exposure on the DLS belonging to the ransomware groups. In these situations, the impact is always higher as the attacks are affecting not only the availability of the infrastructures but also the public image of the targeted companies. **During the first three quarters of the year, 79 ransomware cases were reported to CCB by public or private entities in Belgium.** The figures in this report cover the period from 1/1/2023 to 30/09/2023.

Ransomware attacks: January – September 2023



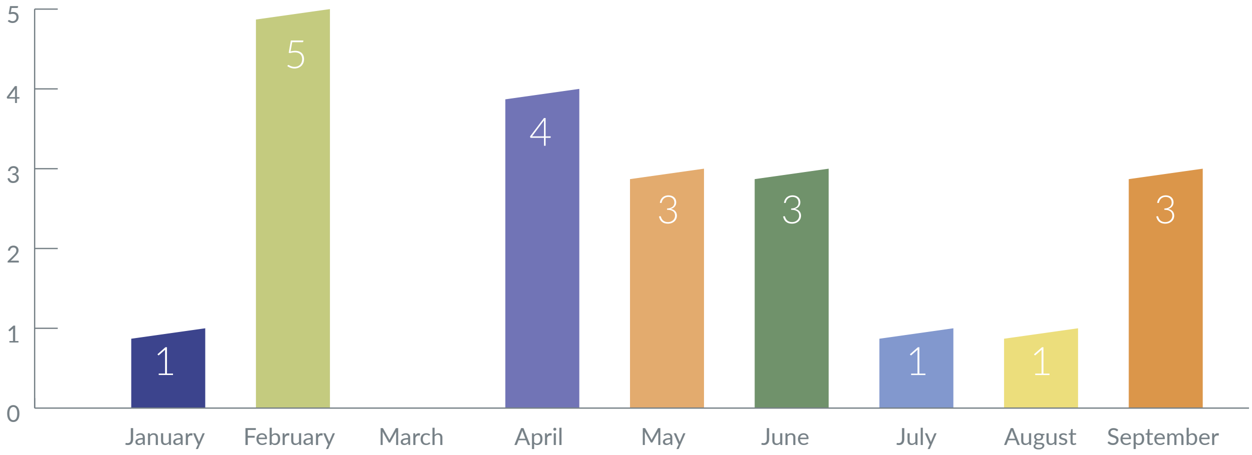
## DDoS

DDoS attacks conducted against Belgian entities were a constant but low impact threat. The attacks temporarily obstructed the availability of some resources or services of the targeted organisations. Usually, the situations were properly managed, and the services were again available and functional. Some of the attacks were claimed by the pro-Russia hacktivist groups KillNet, NoName057(16) and NET-WORKER ALLIANCE and were related to the official positions of the Belgian state regarding the evolution of the Ukraine-Russia conflict or to the military support offered by our country to Ukraine.

It is still important to mention that the DDoS attacks conducted by pro-Russian hacktivists are meant to intertwined with information operations and to easily got media attention and thus the exposed unavailability of services or the exaggerated impact could damage the company's reputation and have a far more severe effect in the long run.

Other DDoS attacks, not claimed by pro-Russian hacktivist groups, were conducted primarily against public entities, **bringing to 21 the total number of attacks reported between January and September 2023**.

**DDos attacks: January - September 2023**



### And 2024?

Ransomware attacks will continue to be one of the most frequent and impactful cyber threats against Belgium.

In line with the evolution of ongoing conflicts and the geopolitical situation, as well as decisions and actions taken by Belgium, there will continue to be a risk of DDoS attacks by hacktivist groups against Belgian targets.

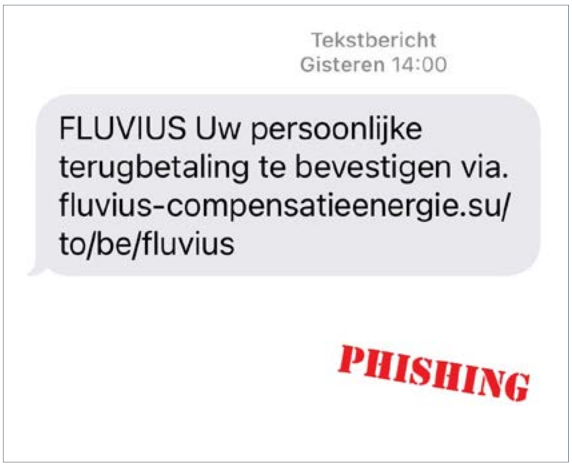
Belgium will remain a target of interest for cyber espionage, with Brussels as capital and home to many international companies and organisations
and EU institutions.

### Examples of attacks against Belgian organisations: January – October 2023

| | Type | Description or Activity |
|---|---|---|
| 12/03/2023 | Ransomware | Entity in the healthcare sector hit by ransomware |
| 11/05/2023 | Ransomware | Entity in the healthcare sector was victim of ransomware |
| 20/06/2023 | DDoS | Pro-Russian conducted DDoS attack against Belgian entities in the maritime sector. NoName057(16) is behind the attack. |
| 27/06/2023 | DDoS | The Belgian federal government was the target of DDoS attack |
| 14/07/2023 | Ransomware | Belgian municipality was victim of a cyberattack |
| 2/08/2023 | Ransomware | Association in Belgium was hit by a ransomware attack |
| 22/08/2023 | Ransomware | Cyberattack against infrastructure related to a Belgian municipality |
| 24/08/2023 | Cyberattack | The government was hit by a distributed denial of service (DDoS) attack |
| 12/10/2023 | DDoS | NoName057(16) targeted Belgian governmental entities in retaliation for promised military and financial support for Ukraine |

# The Anti-Phishing Project

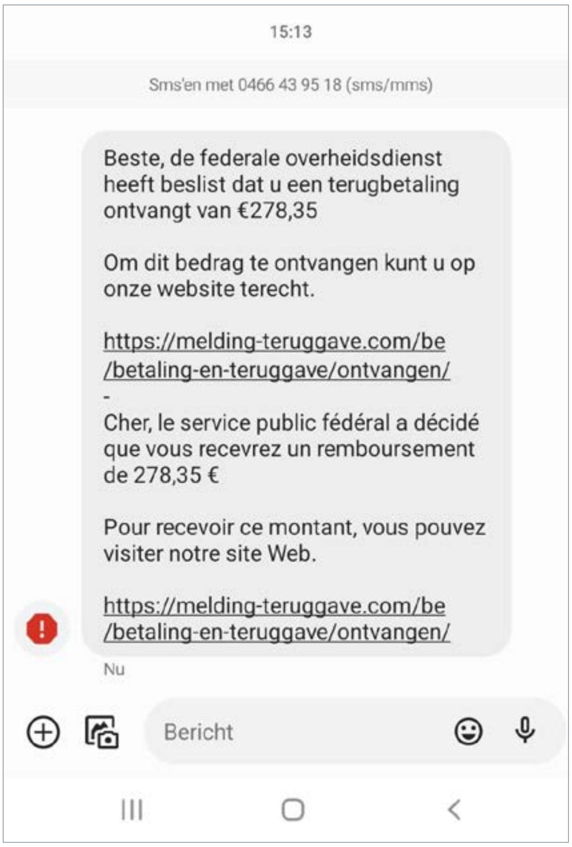
**Phishing** remained one of the main **attack vectors** used by threat actors to install malware in a targeted system, but also one of the most **used type of attacks to steal data**, such as personal information and credentials, and to conduct cyber fraud activities. Phishing attacks largely leverage **social engineering techniques** that rely on human error rather than technical vulnerabilities and represents **a risk both for Belgian organisations and for individuals**.



Tekstbericht
Gisteren 14:00

FLUVIUS Uw persoonlijke terugbetaling te bevestigen via. fluvius-compensatieenergie.su/to/be/fluvius

PHISHING



15:13

Sms'en met 0466 43 95 18 (sms/mms)

Beste, de federale overheidsdienst heeft beslist dat u een terugbetaling ontvangt van €278,35

Om dit bedrag te ontvangen kunt u op onze website terecht.

https://melding-teruggave.com/be/betaling-en-teruggave/ontvangen/

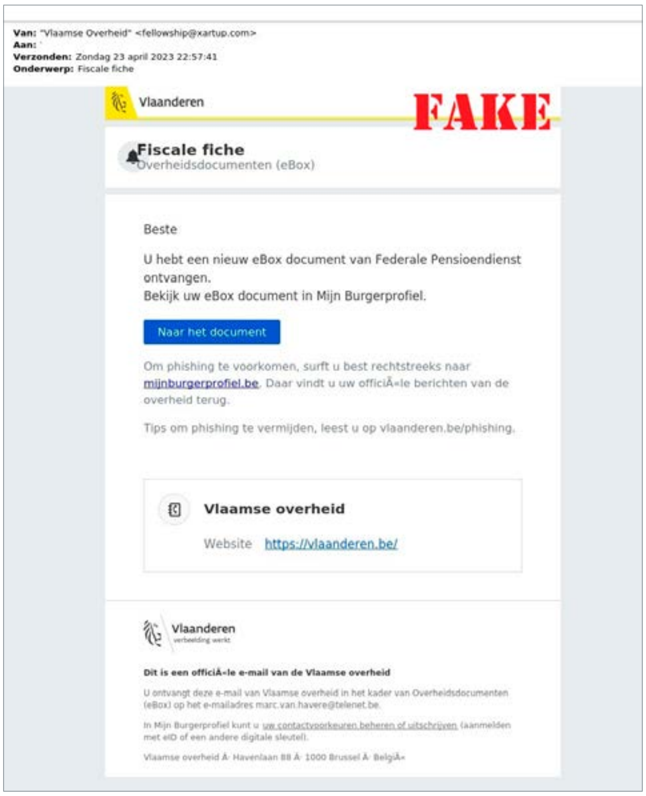
-

Cher, le service public fédéral a décidé que vous recevrez un remboursement de 278,35 €

Pour recevoir ce montant, vous pouvez visiter notre site Web.

https://melding-teruggave.com/be/betaling-en-teruggave/ontvangen/

Nu



**Van:** "Vlaamse Overheid" <fellowship@xartup.com>
**Aan:**
**Verzonden:** Zondag 23 april 2023 22:57:41
**Onderwerp:** Fiscale fiche

Vlaanderen

FAKE

**Fiscale fiche**
Overheidsdocumenten (eBox)

Beste

U hebt een nieuw eBox document van Federale Pensioendienst ontvangen.
Bekijk uw eBox document in Mijn Burgerprofiel.

Om phishing te voorkomen, surft u best rechtstreeks naar mijnburgerprofiel.be. Daar vindt u uw officiÃ«le berichten van de overheid terug.

Tips om phishing te vermijden, leest u op vlaanderen.be/phishing.

**Vlaamse overheid**

Website https://vlaanderen.be/

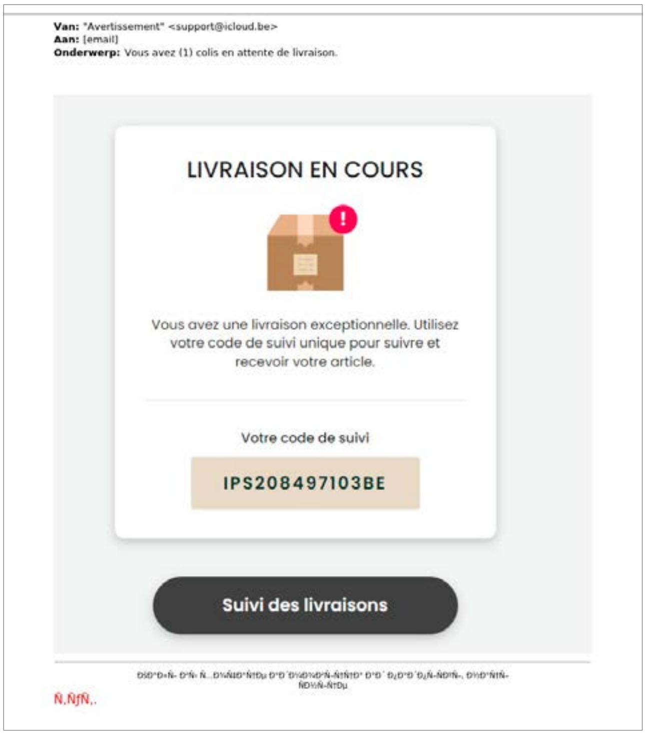
Vlaanderen
verbeelding werkt

**Dit is een officiÃ«le e-mail van de Vlaamse overheid**

U ontvangt deze e-mail van Vlaamse overheid in het kader van Overheidsdocumenten (eBox) op het e-mailadres marc.van.havere@telenet.be.

In Mijn Burgerprofiel kunt u uw contactvoorkeuren beheren of uitschrijven (aanmelden met eID of een andere digitale sleutel).

Vlaamse overheid Â· Havenlaan 88 Â· 1000 Brussel Â· BelgiÃ«



**Van:** "Avertissement" <support@icloud.be>
**Aan:** [email]
**Onderwerp:** Vous avez (1) colis en attente de livraison.

LIVRAISON EN COURS

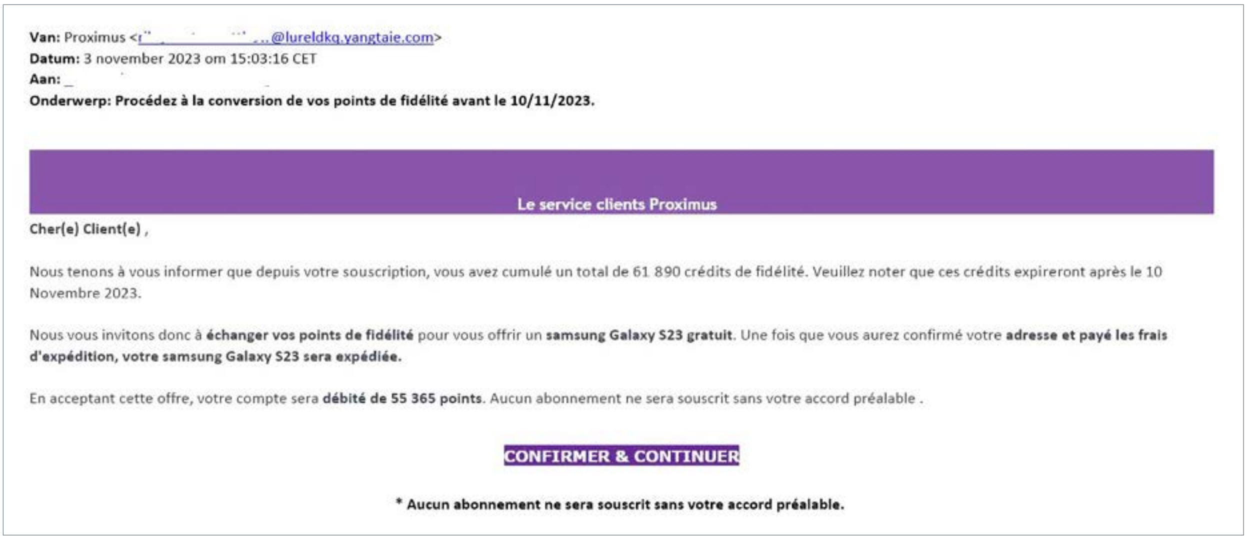
Vous avez une livraison exceptionnelle. Utilisez votre code de suivi unique pour suivre et recevoir votre article.

Votre code de suivi

IPS208497103BE

[illegible]

Ñ‚ÑƒÑ‚.



**Van:** Proximus <[redacted]@lureldkq.yangtaie.com>
**Datum:** 3 november 2023 om 15:03:16 CET
**Aan:** [redacted]
**Onderwerp: Procédez à la conversion de vos points de fidélité avant le 10/11/2023.**

**Le service clients Proximus**

**Cher(e) Client(e) ,**

Nous tenons à vous informer que depuis votre souscription, vous avez cumulé un total de 61 890 crédits de fidélité. Veuillez noter que ces crédits expireront après le 10 Novembre 2023.

Nous vous invitons donc à **échanger vos points de fidélité** pour vous offrir un **samsung Galaxy S23 gratuit**. Une fois que vous aurez confirmé votre **adresse et payé les frais d'expédition, votre samsung Galaxy S23 sera expédiée.**

En acceptant cette offre, votre compte sera **débité de 55 365 points**. Aucun abonnement ne sera souscrit sans votre accord préalable .

**CONFIRMER & CONTINUER**

*** Aucun abonnement ne sera souscrit sans votre accord préalable.**

The **subjects** and **lures** for messages and phishing emails used by attackers to steal data from Belgium victims were mostly related to topics of interest for citizens (bank communications, parcels, and other postal services) and were influenced by the social-economic context, the time of the year or the geopolitical circumstances.

The threat actors were very often impersonating official authorities and public institutions, with some phishing being very professionally realised while there are still a lot easy to spot phishing emails and messages. For **example**, alongside the already “traditional” subjects related to delivery packages, final remainders for different payments needed, new subjects in 2023 were related to the **energy subventions** and **tax contribution**, while old subjects related to COVID-19 were no longer used.

As the main purpose of the phishing campaigns is to collect data form the victims, **the top 5 most used malware** were **information stealers**: Agent Tesla, xloader, remcos, snake keylogger, Loki password stealer.

## TOP 10 Malware Family

| Malware Family | Count |
|---|---|
| agent tesla | 545 |
| xloader | 124 |
| remcos | 68 |
| snake keylogger | 57 |
| loki password stealer (pws) | 46 |
| cloudeye | 41 |
| blustealer | 40 |
| dbatloader | 29 |
| upatre | 25 |
| ave maria | 22 |

Source: CCB, 2023

**Agent Tesla**[1], the most observed malware in 2023, is an advanced **remote access trojan (RAT)** that specializes in the theft and of sensitive information from infected machines **(information stealer)**. It first appeared in 2014 and in the 2020s was largely leveraged for COVID-19 themed phishing campaigns.

Agent Tesla delivers emails attached with *.zip*, *.gz*, *.cab*, *.msi* and *.img* files and Microsoft Office documents with malicious Visual Basic Application (VBA) macros to compromise victim systems. Its phishing campaigns are notorious for precisely replicating a legitimate company’s communication tone and visual template, including logos and fonts.

The malware can collect various types of data, including keystrokes, login credentials used in browsers, email clients, wireless profiles, and other valuable information.

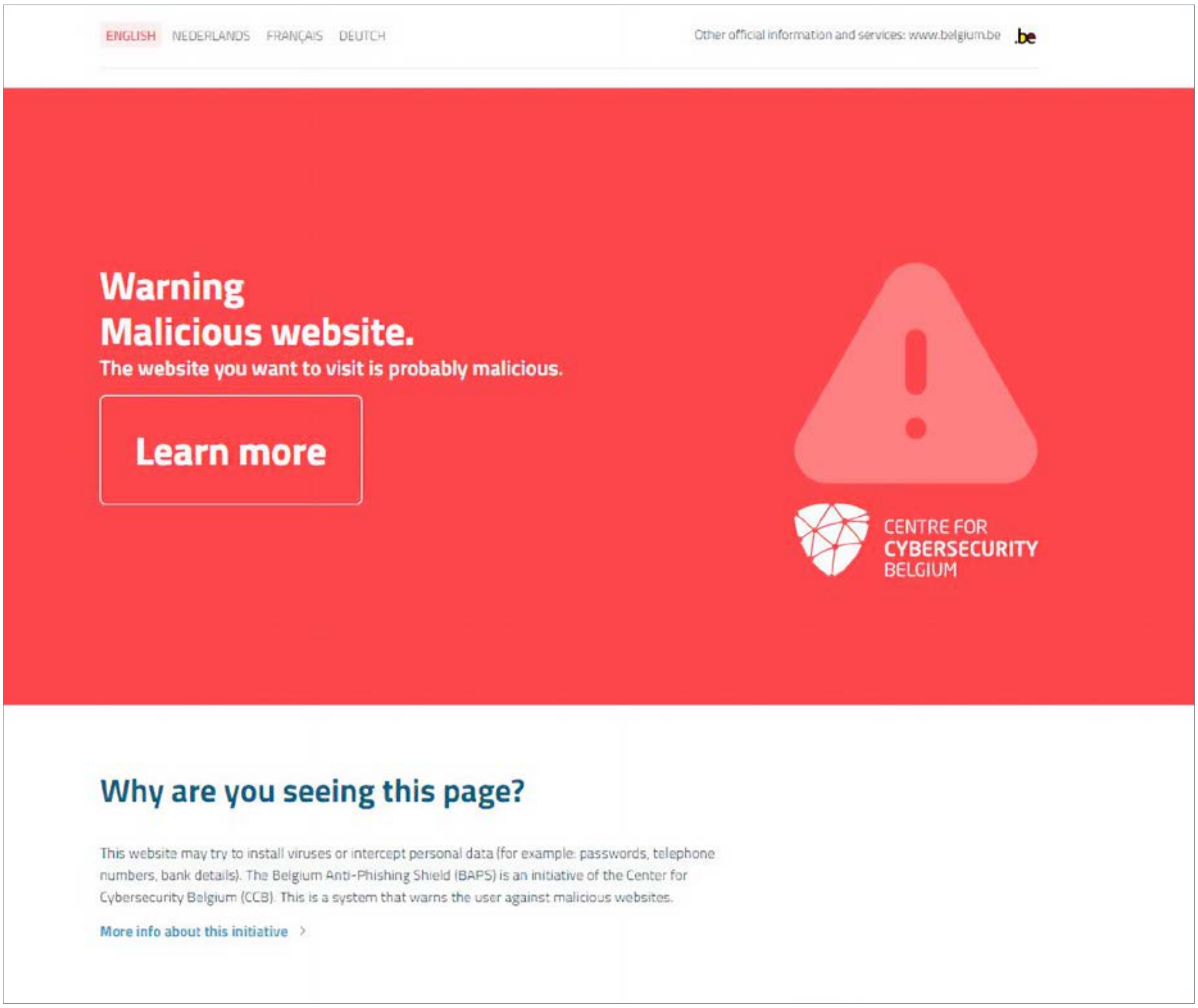
[1] https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/agent-tesla
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/agent-tesla-malware

## SAFEONWEB AND THE BELGIAN ANTI-PHISHING SHIELD

To help keep the Belgian public safe online and better protected against cyber threats and vulnerabilities, the CCB provides a service called Safeonweb that presents the necessary updated information and special campaigns about a specific topic. The Belgium Cyber Security Strategy 2.0 states that "The internet belongs to and is for everyone. Its safety is also a shared effort. Therefore, the population is urged to participate in security."

Safeonweb is a very good example of constructive cooperation of the public institutions with the citizens and the private sector, as it offers the possibility to fight phishing activities by reporting suspicious links and messages to suspicious@safeonweb.be. Based on this service, the CCB created, as part of Active Cyber Protection approach, the Belgian Anti-Phishing Shield (BAPS) initiative, which warns Internet users in Belgium about dangerous websites (such as those used in phishing attempts) and get the reported suspicious links redirected on our warning page.

**In the first three quarters of 2023, more than 7 million messages (7.207.167) were received at suspicious@safeonweb.be compared to almost 4 million messages received during the same period last year (3.954.641 in 2022)**, which shows the broad outreach and civil commitment. Thanks to these messages, the CCB was able to redirect 633.361 unique URLs and 163.736 unique domains tagged as malicious. Between January and September 2023, the BAPS system warned Belgian citizens 5.736.374 times that they were trying to visit a malicious website or server.


ENGLISH
NEDERLANDS
FRANÇAIS
DEUTCH
Other official information and services: www.belgium.be
.be
Learn more
CENTRE FOR
CYBERSECURITY
BELGIUM
More info about this initiative ›

Warning
Malicious website.

The website you want to visit is probably malicious.

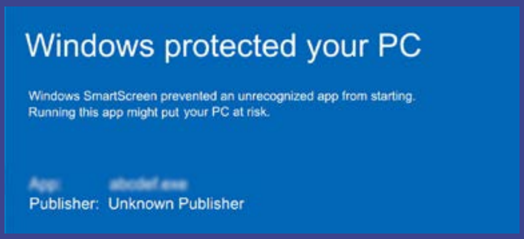
Why are you seeing this page?

This website may try to install viruses or intercept personal data (for example: passwords, telephone numbers, bank details). The Belgium Anti-Phishing Shield (BAPS) is an initiative of the Center for Cybersecurity Belgium (CCB). This is a system that warns the user against malicious websites.

**Belgian Anti-Phishing Shield**

How it works

1. The CCB receives information about potentially malicious websites when Internet users forward suspicious messages to suspicious@safeonweb.be.
2. From the suspicious messages, attachments and links are extracted. URLs are also extracted from screenshots and QR codes.
3. It analyses the URL/link/attachment and if the analysis shows it is malicious, a list of malicious sites is forwarded to our partners (such as ISPs; Google Safe Browsing and Microsoft SmartScreen).



Windows protected your PC

Windows SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

[redacted]

Publisher: Unknown Publisher

4. When an internet user clicks on a link to a malicious site, the relevant ISP compares the DNS request with the list of malicious sites.
5. The user is redirected to a warning page thus the user doesn't visit the malicious site.

# Active Cyber Protection – spear warnings

The Centre for Cybersecurity Belgium (CCB) introduced the concept of Spear Warning at the beginning of 2021. The main purpose of spear warnings is to inform companies and individuals about a cyber threat in a timely manner so that they can act in a timely manner and prevent a cyberattack. "Spear Warning" (SW) is a wordplay related to "Spear Phishing", a modus operandi used by cyber criminals to send very targeted phishing emails to potential victims, usually with the intention of tricking them into handing over personal details. Spear Warnings also fall under the concept of Active Cyber Protection (ACP), which is now included as a term in the EU NIS2 Directive.

The concept of spear warnings aimed to contact Internet users (companies or end users) in an “active way”, by e-mail, letter, or even telephone (the most rapid and efficient contact method in case of an imminent threat. Thus, they can be timely and pro-actively informed about cyber threats or vulnerabilities. The fact that this personal message comes directly from the CCB should, in principle, attract even more attention.

## PREVENT THE THREAT ACTOR TO ACHIEVE ITS ACTIONS

Through sending spear warnings, the CCB seeks to prevent the threat actor to achieve its actions on objectives, such as compromising systems, making them unavailable or exfiltrating data.

The CCB’s spear warnings are often part of long-term campaigns and are mostly related to:

- vulnerable IT systems that are connected to the internet and can be easily compromised/attacked/exploited by cybercriminals;
- critical vulnerabilities that could impact Belgian organisations;
- credential leaks and unauthorized access from Belgian companies that are offered for sale on cybercrime forums and that can be used for further spear phishing campaigns.
- systems infected with malware that could be used for a larger cyberattack as is the case when Belgian infrastructure are compromised with malware that is used as precursor for ransomware attacks;
- suspicious certificate and domain registrations;
- compromised assets notifications.

## THE PROCESS

One of the most important parts of the spear warning concept is to detect cyber threats and vulnerabilities for the entire Belgian cyberspace, and this is one of the CCB’s statutory missions. The CCB uses various techniques and processes for the "collection processes": technical solutions, information sources (open and commercial) and partnerships. When talking about vulnerabilities, the CCB has started a national "Vulnerability Management" project to prioritize vulnerabilities and determine which ones will be issued spear warnings. After a vulnerability has been selected, the spear warning process starts that results in informing the organisations involved with the following elements:

- a risk and impact analysis of the vulnerability,
- recommended actions,
- active exploitation by cybercriminals.

Another version of the spear warning concept is to send automated messages about vulnerabilities and infections on the IT infrastructure to organisations that are register for this service and share the IP range with the CCB, as no IP identification is carried out in this case. By launching the safeonweb@work project, any company will be able to register for this service.

Sometimes, such as in case of major incidents, spear warnings are part of a larger escalation procedure that also includes press releases, publishing advisories on the websites, sending alerts through an early warning system and even organising specific webinars. Spear warnings deeply contribute to the CCB's official mission to make Belgium one of the least vulnerable cyberspaces in the EU. By better informing organisations they can greatly increase their cybersecurity. This makes their IT systems less susceptible to attacks by cybercriminals, who invariably choose the path of least resistance.

It often happens that organisations receive a spear warning from the CCB and that they give feedback that they were not aware of the security problem, the vulnerability, the data breach, or the infection of their IT systems. There were situations where the attack was in progress or in full preparation just when the victim received a spear warning from the CCB and could therefore still respond in time.

The Centre for Cybersecurity Belgium (CCB) is proud to announce that it has won the Publica Awards in the 'Security & Safety' category with its pioneering 'Spear Warning' project. The Publica Awards recognise excellence in public projects and the CCB is delighted to be the winner of this prestigious competition, which took place in Brussels on 16 November 2023.

*"We are extremely pleased and grateful for the recognition we have received from the Publica Awards. This award confirms the impact and innovation of the Spear Warning project. It shows that proactive measures like this play a crucial role in strengthening the digital resilience of our society. We will continue our efforts to improve cybersecurity and protect our citizens and businesses from ever-evolving threats."*

Miguel De Bruycker, Director General CCB

## SPEAR WARNING – HAFNIUM: THE FIRST BIG USE CASE

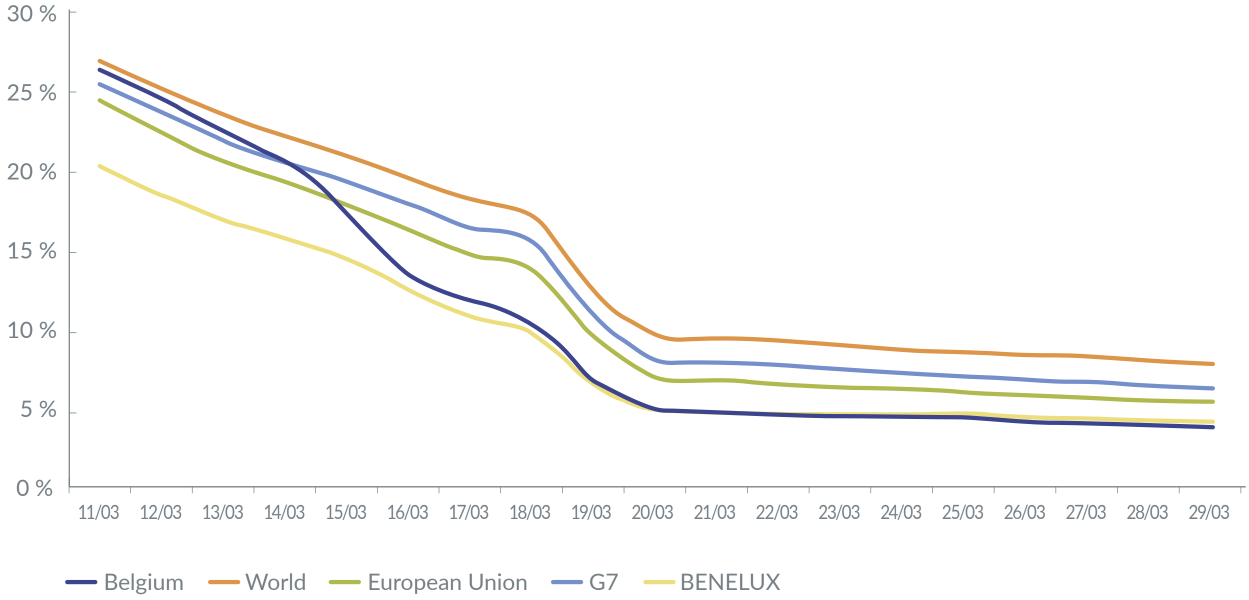
Hafnium. This actor exploited a vulnerability in Microsoft Exchange, and at that time, a large number of Belgian Exchange installations were vulnerable and exposed to the Internet. Belgium had the highest percentage of exposed vulnerable Microsoft Exchange systems. Yet, the introduction of the spear warning system marked the beginning of a positive shift. The first spear warning to potential victims led to a noticeable improvement in the amount of vulnerable systems.

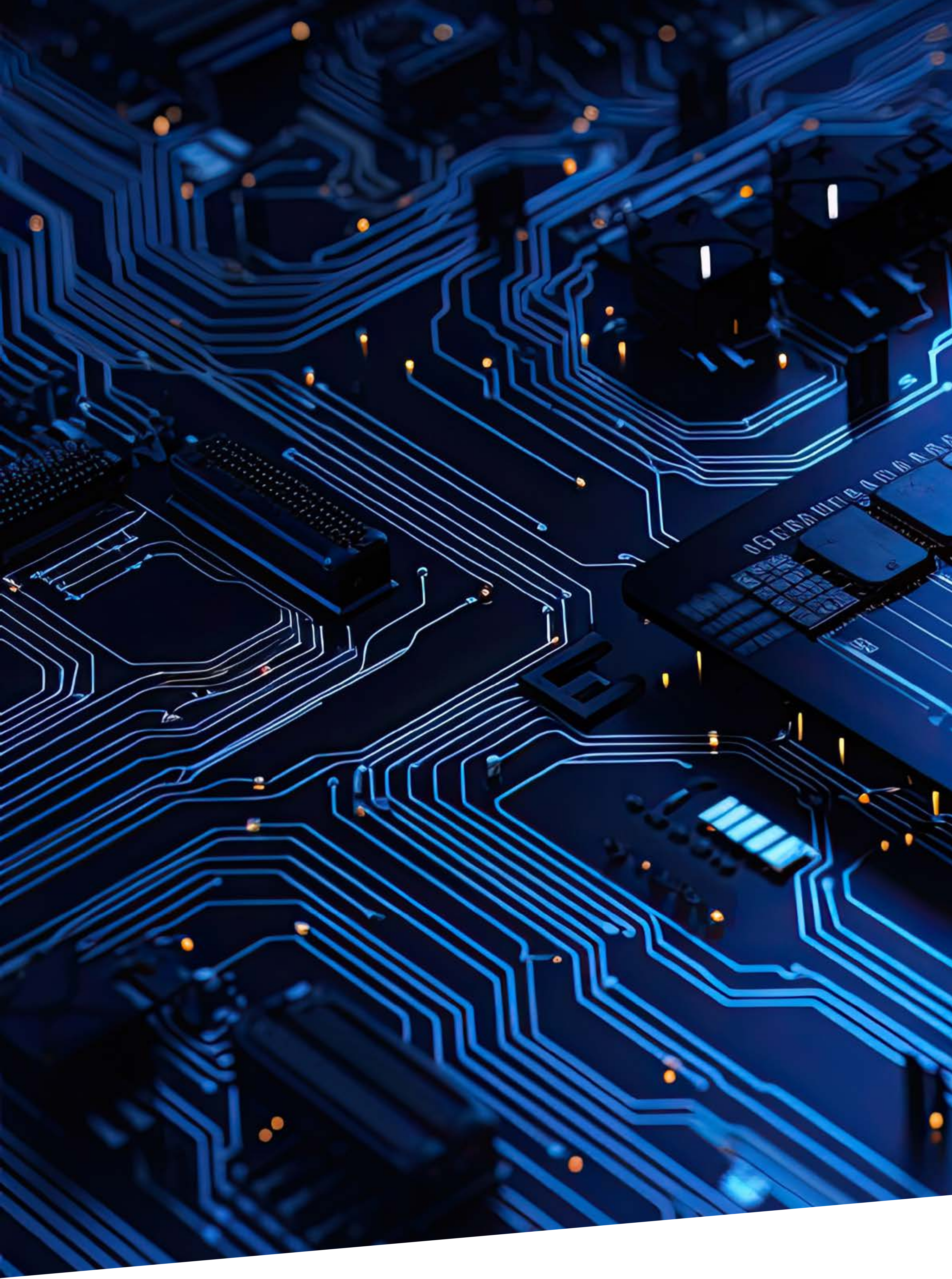
The situation improved even further with the second spear warning, ultimately resulting in a remarkable turnaround. Belgium went from having the highest number of vulnerable systems to the lowest, demonstrating the effectiveness of the spear warning system.

- Planning and Direction: Formulating a strategic plan and preparing to pinpoint the vulnerabilities that have the most significant impact on Belgium's cyberspace.
- Collection: Conducting a comprehensive scan to detect vulnerable systems across Belgium.
- Processing and Exploitation: Identifying the proprietors of these vulnerable systems.
- Analysis and Production: Initiating communication to inform the system owners about their vulnerabilities.
- Dissemination: After a certain period, reassessing to determine if systems remain vulnerable.
- Feedback: Dispatching reminders to the system owners as necessary.

**2021**

**Notifications sent to 1259 vulnerable organizations**
**Notifications sent to 355 compromised organizations**
**Multiple reminders were sent afterwards**





# CRITICAL VULNERABILITIES

# Critical vulnerabilities that have sharped the cyber threat landscape between January and September 2023

Threat actors with different interests exploit critical vulnerabilities in their attacks. They become increasingly faster at weaponizing zero-day vulnerabilities to their advantage, than organisation updating their cyber-security measures. It was also observed that threat actors continue to successfully exploit pre-existing vulnerabilities in unpatched software where enterprises enforce lax or inadequate security measures.

CVEs refer to Common Vulnerability Exposures. Whenever security researchers or organisations find new vulnerabilities, they add them to the CVE list maintained by MITRE Corporation. The vulnerability is assigned a CVE ID so that it is easy to identify and protect against the said vulnerability.

**Five of the most critical vulnerabilities that were also exploited by cyber threat actors in 2023 were:**

**CVE-2023-0669**

CVE-2023-0669, a zero-day vulnerability in Fortra's GoAnywhere Managed File Transfer (MFT) tool, a platform centralizing control over internal and external file transfers, has been actively exploited by threat actors, including ransomware groups. This vulnerability allows for remote code execution (RCE), potentially leading to compromise of the affected systems, extensive data breaches and financial extortion. The managed file transfer software from a victim can be used to infect other victims by sending malicious files and successful intrusion could lead to a serious supply chain attack. The Clop ransomware group specifically targeted around 490,000 individuals, compromising their personal information through the exploitation of this vulnerability.

**CVE-2023-2868**

CVE-2023-2868 vulnerability in the Barracuda Email Security Gateway devices permits user inputs to be executed as a system command, which grants attackers the ability to remotely manipulate system commands with significant privileges. The flaw was exploited in wide campaigns, from October 2022 until May 2023, by a highly skilled threat actor, tracked by Mandiant as UNC4841. Almost a third of identified affected organisations were government agencies across all regions. Mandiant assessment was that it is a China-nexus activity and that, based on the observed targeting profile, it could be an espionage campaign.

**CVE-2023-34362**

CVE-2023-34362 is a critical zero-day vulnerability in the MOVEit Transfer, a file transfer solution. The vulnerability, that could lead to escalated privileges and unauthorized access to the environment, was mass-exploited by Cl0p ransomware group to steal data from organisations. The operators behind Cl0p ransomware claimed to have gained access to information of "hundreds" of companies that use the MOVEit software and started to list the victims on their Data Leak Site (DLS).

**CVE-2023-23397**

Another vulnerability that was highly exploited by cyber threat actors was CVE-2023-23397, a critical elevation of privilege vulnerability in all supported versions of the Microsoft Outlook email client for Windows. This flaw allows attackers to bypass authentication measures, facilitating unauthorized access to confidential data and enabling user impersonation within organisations.

**CVE-2023-38831**

CVE-2023-38831 a security flaw in the WinRAR archiver tool for Windows, allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive. The vulnerability has been largely exploited to achieve remote code exploitation both by cybercriminal organisations and State-sponsored threat actors, like APT 28, Sandworm, DarkPink or APT40.

The CCB always publishes technical advisories, warning about the possible exploitation of vulnerabilities and recommending the right actions to mitigate the risks, including patching.

In the case of critical vulnerabilities with a high risk of impacting Belgium, CCB issues spear alerts, directly informing Belgian organisations of the threat and the urgent need for patching. This proactive approach helps to protect Belgian victims and successfully prevent imminent attacks, such as ransomware attacks using exploitable vulnerabilities.

# Overview of Belgium Cyber Metrics in 2023

| 2023 | Q1 | Q2 | Q3 |
|---|---|---|---|
| **PHISHING** | | | |
| E-mails received | 2.695.345 | 2.381.106 | 2.130.716 |
| Unique URLs tagged as malicious by Netcraft | 186.792 | 237.740 | 211.031 |
| Unique domains tagged as malcious by Netcraft | 12.382 | 93.481 | 59.727 |
| **BAPS** | | | |
| Amount of hits on the landing page | 2.031.888 | 2.464.489 | 1.239.997 |
| **WARNINGS** | | | |
| Technical advisories published on www.cert.be | 35 | 39 | 41 |
| Technical tweets | 67 | 67 | 79 |
| **Spear warnings** | | | |
| Automated processed | 1.193 | 863 | 1.221 |
| Manually processed | 1.653 | 946 | 1.255 |
| Total | 2.846 | 1.809 | 2.476 |
| **INCIDENTS** | | | |
| Ransomware (reported) | 28 | 20 | 31 |
| Denial of Service | 6 | 10 | 5 |
| **COMMUNICATION** | | | |
| **Websites** | | | |
| Sessions www.safeonweb.be | 674.243 | 615.379 | 450.365 |
| News items SOW | 22 | 19 | 16 |
| **CCB Events** | | | |
| Connect & Share events | 2 | 2 | 0 |

# BELGIUM CYBER METRICS IN 2023

# Raising awareness and building a strong community of cybersecurity experts

As part of the CCB Connect & Share initiative, which aims to raise awareness and build a community by bringing together cybersecurity professionals to share their thoughts on the various cyber threats in Belgium and around the world, several events were organised in 2023, with high attendance, live or hybrid:

### 12 JANUARY 2023 – QUARTERLY CYBER THREAT REPORT Q4 2022 EVENT

The CCB experts, together with experts from cybersecurity companies, examined the cyber threat with a focus on cloud security and the energy sector.

### 19 JANUARY 2023 – ICS RAPID RESPONSE EVENT

The event was organised by SANS and the CCB and provided an opportunity for experienced ICS specialists, as well as non-ICS specialists, to hear presentations on a range of topics including: Five Critical Controls, Defensible Architecture, OT Visibility, Threat Intelligence and OSINT.

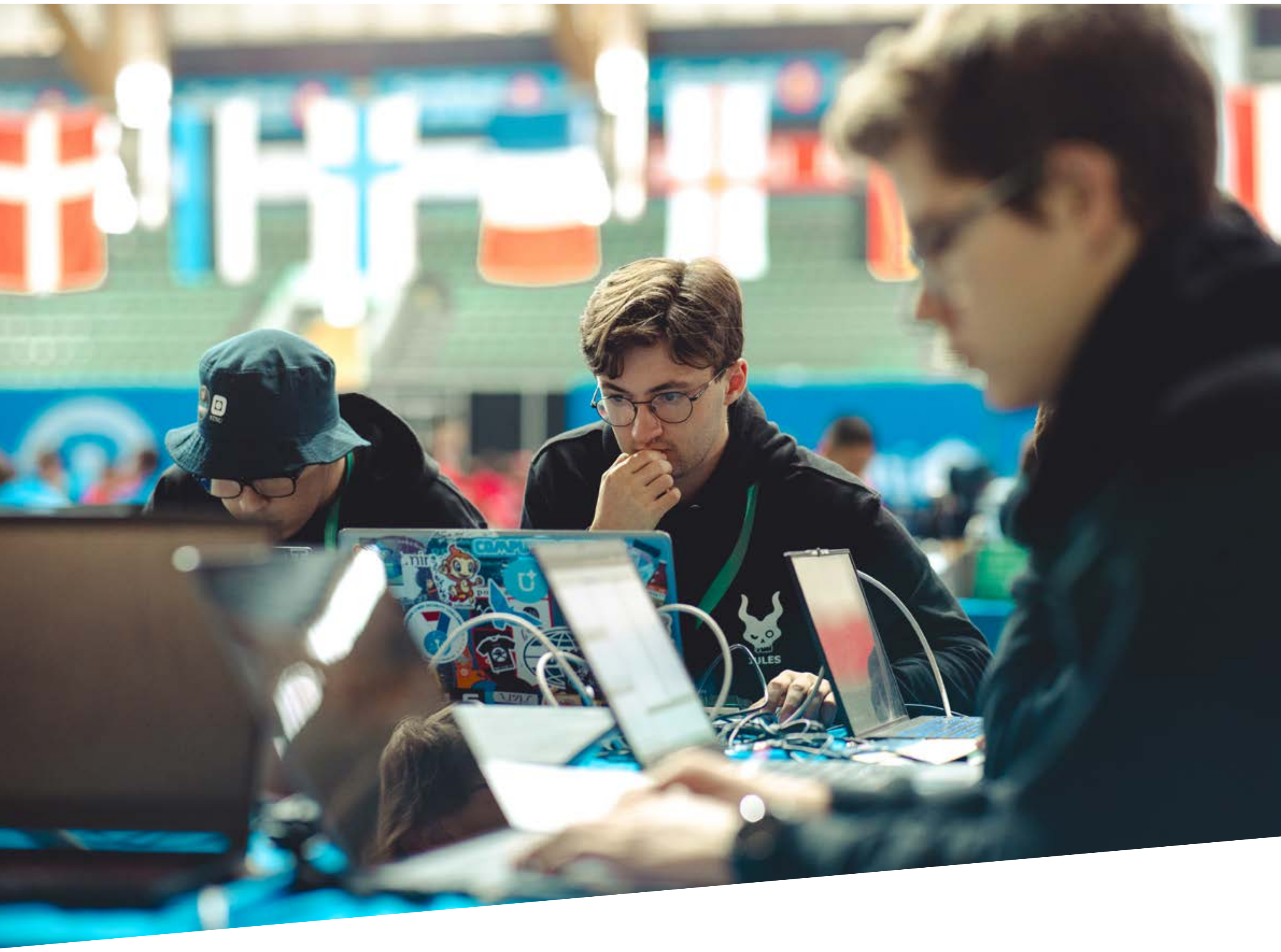
### 20 APRIL 2023 – QUARTERLY CYBER THREAT REPORT Q1 2023 EVENT

The CCB organised a new event to review the observations from the first quarter of 2023 and discuss topics such as DDoS attacks, Wi-Fi security, malware and the latest observations on espionage and hacktivism. It was also an opportunity for experts to share their latest research.

### 25 MAY 2023 – 11TH EU MITRE ATT&CK® COMMUNITY WORKSHOP

The CCB co-organised with MITRE Engenuity a hybrid event to present updates on the use of the ATT&CK® framework to advance threat-informed defence. Experts from the CCB, MITRE Engenuity and other developers of systems and tools supporting the ATT&CK® Framework gave presentations during the event.

# CONNECT & SHARE EVENTS


JULES

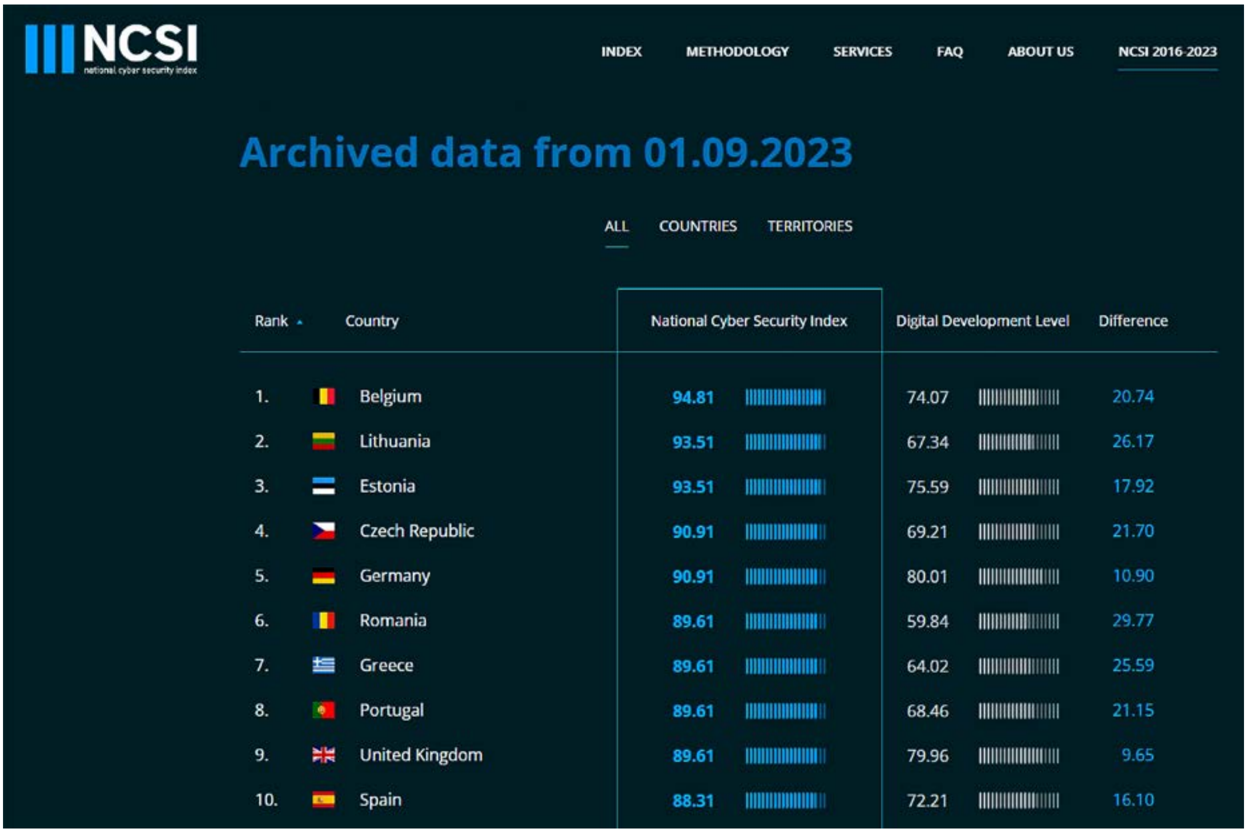
# BELGIUM IN THE WORLD

# Belgian Cybersecurity Ranking

The very good overall cybersecurity posture of Belgium and the preparedness to prevent cyber threats and manage cyber incidents affecting national organisations is reflected also by the cybersecurity ranking of Belgium.

In 2023, Belgium reached the first place in the world according to the National Cyber Security Index, the global live index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents.

The NCSI Score shows the percentage the country received from the maximum value of the indicators considered based on the methodology used.



Archived data from 01.09.2023

| Rank | Country | National Cyber Security Index | Digital Development Level | Difference |
|---|---|---|---|---|
| 1. | Belgium | 94.81 | 74.07 | 20.74 |
| 2. | Lithuania | 93.51 | 67.34 | 26.17 |
| 3. | Estonia | 93.51 | 75.59 | 17.92 |
| 4. | Czech Republic | 90.91 | 69.21 | 21.70 |
| 5. | Germany | 90.91 | 80.01 | 10.90 |
| 6. | Romania | 89.61 | 59.84 | 29.77 |
| 7. | Greece | 89.61 | 64.02 | 25.59 |
| 8. | Portugal | 89.61 | 68.46 | 21.15 |
| 9. | United Kingdom | 89.61 | 79.96 | 9.65 |
| 10. | Spain | 88.31 | 72.21 | 16.10 |

Source: https://ncsi.ega.ee/ncsi-index/?archive=1

# Belgium's Cyber Champions: The Red Daemons at the ECSC 2023

In October 2023, the Belgian Red Daemons team embarked on a journey to Hamar, Norway, to proudly represent Belgium at the 8th annual European Cyber Security Challenge (ECSC). Competing against teams from 29 other European nations, the Red Daemons faced three intense days of security-related challenges, accruing points for their solutions. This marked Belgium's sixth participation in this prestigious international event.

The ten cyber talents were traditionally selected from the victorious teams of the national Cyber Security Challenge Belgium (CSCBE), which was held earlier in March of that year. Over the past seven years, the Cyber Security Challenge Belgium has drawn the interest of thousands of Belgian students eager to test their skills, learn, and engage in the exciting world of cybersecurity.

The demand for cybersecurity experts in companies, organisations, and security and police forces is on the rise. The participation of the Belgian Red Daemons is made possible through a collaborative effort between the CCB and NVISO. These partners are responsible for organizing the event, providing sponsorship, and conducting preparatory workshops each year.

The national challenge, CSCBE, is annually organized by NVISO and receives support from the CCB as well.

Events like the ECSC and the CSCBE play a crucial role in inspiring young individuals to pursue dynamic careers in the field of cybersecurity.

Follow the Belgian Red Daemons on social media:

- X: @BelRedDaemons
- Instagram: @belgianreddaemons
- Facebook: https://www.facebook.com/BelRedDaemons

# CYBER SPOTLIGHT: AI & CYBERSECURITY

# Cyber Spotlight: AI & Cybersecurity

Behind the current hype we see around "AI" in the tech world, there is a real underlying trend of thinking the use of AI in every sector, cybersecurity is no exception and its proximity with innovation and its transversality to many technologies makes it a prime subject for AI applications. To better grasp the interactions between these two subjects it is possible to define 3 major areas of convergence as follows:

- AI 'at the service' of cybersecurity: how can cybersecurity expert use AI to improve the defence of their systems? (e.g. malware analysis and attack detection)
- AI 'against' cybersecurity: how can a hacker take advantage of AI to improves its techniques and tactics? (e.g. deepfake and vulnerabilities discovery)
- The security of AI applications: do AI applications have vulnerabilities and how to protect them? (e.g. data poisoning and model evasion)

These different approaches are rich and in constant evolution, but we will do our best to tackle them in a set of articles. The first one will address the trendy use of chatbots and LLMs, we decided to focus on the third approach, the security of the AI, with the point of view of an average user.

## GENERAL CONSIDERATIONS FOR THE SAFE AND RESPONSIBLE USE OF CONVERSATIONAL ARTIFICIAL INTELLIGENCE (AI) TECHNOLOGIES

Conversational AI technologies such as ChatGPT and Bard, driven by large language models (LLMs), have grown in popularity and many Belgians have adopted them to improve their productivity. Against this backdrop, the CCB has recognized the significance of clearly defining the issues associated with these technologies.

We would like to present here an initial list of "good reflexes" to adopt for the safe and responsible use of these technologies.

As a preamble, even if it seems like common sense, it is vital never to trust blindly the answers provided by conversational agents and always to keep a critical mind. As the answers provided by these tools are imperfect, they should always be reviewed and corrected. Moreover, conversational agents generally lack logical reasoning; they are ‘probabilistic’ in the sense that they are trained to generate sequences of words with a high degree of probability.

Additionally, particular attention must be paid to the following aspects:

- Protect confidential data: avoid sharing sensitive information, as conversational AI agents can store and reuse this data. Deactivate the recording of conversation history whenever possible.
- Error detection: conversational AI agents make mistakes, so only entrust them with tasks for which you have sufficient knowledge (so that you can check and control the results).
- Fact-checking: independently verify the facts (fact-checking), as sources are often omitted from the results proposed by conversational AI agents.
- Automation bias: by using them too much, it is possible to favour the results generated by AI agents and give them excessive confidence when, as we have seen, in many areas humans are more competent.
- Limitations and prejudices: conversational AI agents can be tainted by prejudices and are limited in their knowledge by their training data. Confront them with various sources to obtain an objective and complete context.
- Transparency: favour transparent use of conversational AI agents. Don’t try to hide their use, but rather report it to reinforce trust and responsibility.
- Copyright: the responses provided by conversational AI agents may infringe copyright, so care should be taken when using them for academic or commercial purposes.
- Humanity: don’t forget that conversational AI agents are devoid of consciousness and emotions. Beware of emotional manipulation.

By taking all these aspects into account, we believe users can effectively use conversational AI agents while understanding their limitations and acting responsibly.

P

# WHO ARE WE?

# Who are we?

**The Centre for Cybersecurity Belgium (CCB) is the national authority for cybersecurity in Belgium. Established by Royal Decree of 10 October 2014, the CCB operates under the authority of the Prime Minister.**

Through an optimal exchange of information, companies, the government, providers of essential services and the population can protect themselves adequately.

The CCB also supervises, coordinates and monitors the application of the Belgian Cyber Security Strategy, approved by the country's National Security Council in 2021. Its mission is to make Belgium one of the least vulnerable countries in Europe in terms of cybersecurity by 2025.

The CCB plays a key role in helping Belgium to achieve this goal by carrying out its tasks, such as informing and raising awareness of the main cyber threats and how to protect against them.

Follow the Centre for Cybersecurity Belgium on social media and our website:

- X: @CCBbelgium
- X: @CCBAlerts
- LinkedIn
- www.ccb.belgium.be

**Responsible editor**
Centre for Cybersecurity Belgium
Mr. De Bruycker, General Director
Rue de la Loi, 18
1000 Brussels

**Legal Depot:**
D/2024/14828/001

### Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister. All texts, layouts, designs and other elements of any nature in this document are subject to copyright law. Reproduction of extracts from this document is authorised for non-commercial purposes only and provided the source is acknowledged.

A translation into Dutch, French or German of this brochure is also made available on the CCB website.

The CCB accepts no responsibility for the content of this document.

The information provided:

- are exclusive of a general nature and do not intend to take into consideration all particular situations.
- are not necessarily exhaustive, precise, or up to date on all points.

Photos © Adobe Stock, Emil Nyeng (pixieset.com), iStock, Karakters.be, Mati Mango