BRANDEFENSE COUNTRY REPORT · BELGIUM 2026

Brandefense Belgique : rapport sur le paysage des cybermenaces 2026

Exposition des identités, fournisseurs communs et continuité des activités

Odin by Brandefense
Période de recherche: 1 janvier–22 novembre 2026
Version 1.0 · Édition publique de recherche · TLP:CLEAR · 9–22 novembre 2026

63 sur 250
domaines d'organisations sélectionnés avaient un identifiant proposé à la vente lors du contrôle

1025
publications de forum distinctes conservées, avec couverture limitée au-delà de ces espaces

22
noms de groupes de rançongiciels dans les publications belges conservées

11 sur 25
domaines sélectionnés de banque et finance avaient une annonce actuelle d'identifiant

TABLE DES MATIÈRES

Table des matières

Translated with AI

Cette édition a été traduite avec l'aide de l'intelligence artificielle à partir de l'original anglais; la version anglaise fait foi.

01	Synthèse	04
	Carte du rapport	08
	Sommaire et guide de lecture	09
02	Contexte numérique et menaces en Belgique	10
03	Exposition nationale : organisations et domaines sélectionnés	13
04	Ce que nous observons sur le dark web	22
05	Incidents confirmés et revendications par secteur	36
06	Hacktivisme, perturbations et systèmes opérationnels	49
07	Acteurs de la menace et liens entre les preuves	53
08	L'économie de la fraude	61
09	Analyse du secteur bancaire et financier	66
10	Réglementation et réponse nationale	69
11	Perspectives	74
12	Plan d'action	77
A	Annexe A. Méthode et limites	83
B	Annexe B. Registre des preuves	86
C	Annexe C. Sources	87
D	Annexe D. Glossaire	90
	À propos du rapport	92

CISO et direction	01 05 10 11 12
SOC et identités	03 04 07 09 A–B
Opérations et achats	02 05 06 12
Finance et protection clients	04 08 09
Vie privée et communication	05 06 10 A–C

À propos de cette édition

Traduit avec l'IA. En cas de différence, l'édition anglaise fait foi.

Recherche et rédaction assistées par l'IA. Les catégories de preuve et les limites de couverture s'appliquent à l'ensemble du rapport. L'édition anglaise fait foi en cas de différence entre les traductions.

CHAPITRE 01

Synthèse

01

CE CHAPITRE RÉPOND À LA QUESTION

Quels sont les enjeux prioritaires pour les organisations belges en 2026 et que doivent faire les dirigeants en premier ?

4

décisions relatives aux identités, aux fournisseurs, aux activités et à la communication d'incident

Quatre décisions pour les dirigeants 06

L'année en chiffres 06

CHAPITRE 01

Synthèse

EN BREF

Les éléments belges soulignent la protection des identités et la continuité des services. Le CCB a reçu 588 signalements jusqu'au 28 septembre. Les sites de rançongiciels comptaient 46 publications belges dans la période étudiée. Les forums conservés annonçaient des données clients, des documents d'identité, des accès et des outils frauduleux. Des incidents publics ont touché soins, adhésions, enseignement et administration. Ces populations mesurent des réalités différentes. Validez les identités actives, cartographiez les fournisseurs, limitez les accès opérationnels distants et exercez notification et reprise.

Le rapport associe observations clandestines, données d'exposition et informations publiques vérifiées. Brandefense Blackhole compte 96 265 publications étiquetées pour le pays sur les plateformes. Le contenu conservé comprend 1025 publications de forum distinctes, dont 480 portent une étiquette nationale. Ces populations se chevauchent et décrivent la visibilité, sans compter les attaques nationales. [S1][S2][S3]

1. Les sources officielles soutiennent surtout la protection des identités. Dans son évaluation du 9 novembre, le CCB situe les incidents liés aux comptes autour de 30% des signalements des deux premiers trimestres. La police décrit séparément la réutilisation d'identifiants de messagerie, la modification de factures et l'usurpation d'employés bancaires. Aucune source ne mesure l'exposition actuelle de chaque organisation belge. [S5][S31][S32]

2. Les revendications d'extorsion couvrent de nombreux noms de groupes. Ransompedia a enregistré 46 publications acceptées dans la période, sous 22 noms de groupes. Qilin en compte 9 et The Gentlemen 7. Ce total partiel dépasse les 42 publications de toute l'année 2025. Il ne s'agit ni d'un taux annuel de croissance ni de la preuve de 46 intrusions distinctes. [S1]

3. Les fournisseurs communs imposent des décisions sur les services. Les cas de l'enseignement, des soins et des administrations locales montrent les effets possibles d'une dépendance sur la communication, la disponibilité et l'évaluation des données. Une clientèle ne correspond pas au nombre de victimes touchées. Exigez une analyse d'impact propre au fournisseur et à chaque client. [S8][S13][S22]

4. Les annonces mêlent anciennes données, revendications actuelles et capacités non testées. Une annonce télécom renvoie à juillet 2025. L'auteur d'une importante annonce de données citoyennes reconnaît ignorer leur source. Des publications récentes proposent des tickets d'assistance, des outils d'usurpation bancaire et une liste de clients liée aux casinos. Elles n'établissent ni accès fonctionnel ni transaction réalisée. [S3]

5. La reprise opérationnelle exige un responsable distinct. Les perturbations frigorifiques de novembre posent un autre problème qu'une panne de site web. L'attribution publique restait contestée dans les sources conservées. La question défensive immédiate concerne la maîtrise des accès distants et le retour des équipements à un état sûr. [S25][S26][S27]

6. Les annonces actuelles exigent une vérification ciblée des identités. 63 des 250 domaines d'organisations sélectionnés avaient un identifiant proposé à la vente lors du contrôle. La valeur nationale Atlas est de 48 sur 100. Au moins 296 591 associations d'appareils et 26 236 674 identifiants enregistrés décrivent des populations qui se chevauchent, sans confirmer d'intrusions. [S2]

Quatre décisions pour les dirigeants

1. **Validez les identités avant d'imposer une réponse perturbatrice.** Demandez aux responsables identités et SOC de distinguer un ancien identifiant, un compte actif et une session suspecte. Consignez le traitement de chaque constat pertinent.
2. **Reliez les fournisseurs aux effets sur les données et les services.** Exigez de chaque fournisseur critique des conditions de notification précises et une solution de remplacement testée. Exercez une panne alors que la confidentialité reste incertaine.
3. **Maîtrisez les accès opérationnels distants.** Donnez aux équipes opérationnelles une liste d'accès vérifiée, une procédure locale sûre et le pouvoir de limiter les accès fournisseurs. Testez la reprise sans le canal distant habituel.
4. **Préparez des notifications et des décisions de reprise claires.** Désignez les responsables juridiques, techniques, communication et vie privée. Distinguez délais légaux et objectifs internes. Préservez les incertitudes dans les avis français et néerlandais.

L'année en chiffres

Nombre	Ce qu'il représente	Ce qu'il ne représente pas
588	Signalements reçus par le CCB, 1 janvier–28 septembre 2026 [S4]	Total annuel, victimes uniques ou estimation de prévalence nationale
46	Publications belges acceptées de rançongiciels dans la période [S1]	Chiffrement confirmé, intrusions distinctes ou pertes mesurées
22	Noms de groupes associés à ces publications [S1]	Organisations criminelles distinctes et vérifiées
1025	Publications de forum distinctes conservées dans les ensembles collectés [S3]	Ensemble des publications concernant la Belgique ou incidents uniques
480	Publications portant une étiquette nationale dans cette population [S3]	Population supplémentaire à ajouter aux 1025
31	Publications conservées datées du 9–22 novembre [S3]	Pas de nouvelles intrusions vérifiées
250	Domaines candidats sélectionnés de manière raisonnée [S2]	Recensement économique classé ou échantillon national représentatif
245	Domaines candidats ayant répondu au DNS à la date d'observation [S2]	Personnes morales indépendantes validées ou notation de sécurité
63	Domaines d'organisations sélectionnés avec une annonce actuelle d'identifiant [S2]	Accès fonctionnel, comptes actifs ou intrusions confirmées

Nombre	Ce qu'il représente	Ce qu'il ne représente pas
48	Valeur nationale Atlas pour les 250 domaines sélectionnés [S2]	Prévalence nationale ou notation sectorielle
96 265	Publications étiquetées pour le pays sur les plateformes [S3]	Ciblage belge vérifié, pertinence criminelle ou incidents nationaux

POINTS À RETENIR

01

Privilégiez la validation des comptes et la capacité de reprise des services.

02

Distinguez annonces, publications d'extorsion et incidents confirmés.

03

Désignez les responsables des décisions concernant fournisseurs, activités et notifications.

Carte du rapport

Commencez par la décision qui vous appartient, puis suivez les preuves et leurs limites.

CISO et direction	Financer identités, continuité et notification	01 05 10 11 12
SOC et identités	Valider annonces, sessions et activité actuelle	03 04 07 09 A–B
Opérations et achats	Maintenir des services sûrs pendant un incident fournisseur	02 05 06 12
Finance et protection clients	Interrompre usurpation et modifications de paiement	04 08 09
Vie privée et communication	Préserver périmètre des preuves et obligations de signalement	05 06 10 A–C

Sommaire et guide de lecture

Chapitre	Question
1 Synthèse	Quelles décisions les dirigeants doivent-ils prendre en premier ?
2 Contexte	Quelles dépendances structurent la situation belge ?
3 Exposition nationale	Que permet d'établir l'évaluation des domaines sélectionnés ?
4 Dark web	Qu'est-ce qui était annoncé et qu'est-ce qui reste non vérifié ?
5 Incidents	Quels effets sur les services et les données sont étayés ?
6 Perturbations	En quoi les revendications diffèrent-elles des effets opérationnels ?
7 Acteurs	Quels liens reposent sur des preuves ?
8 Fraude	Comment des informations exposées pourraient-elles faciliter la tromperie ?
9 Banque	Que doivent vérifier les équipes chargées des identités et de la fraude ?
10 Réglementation	Quelles obligations et échéances s'appliquent ?
11 Perspectives	Quels scénarios conditionnels faut-il tester ?
12 Plan d'action	Qui est responsable des prochains 30/60/90 jours ?
Annexes A–D	Périmètre, registre des preuves, sources et glossaire

Les dirigeants peuvent commencer par les chapitres 1, 5, 10 et 12. Les équipes SOC et identités devraient lire les chapitres 3, 4, 7 et 9. Les équipes opérationnelles, achats et protection des clients utiliseront les chapitres 5, 6 et 8.

Observé signifie qu'une annonce, une publication d'extorsion ou une déclaration publique conservée existe. **Revendiqué** restitue les propos de l'annonceur sans valider leur résultat. **Évalué** désigne une interprétation mesurée, son explication alternative et l'action qu'elle justifie.

CHAPITRE 02

Contexte numérique et menaces en Belgique

02

CE CHAPITRE RÉPOND À LA QUESTION

Quelles particularités belges comptent pour la réponse aux incidents et quelles conclusions faut-il éviter ?

588

signalements reçus par le CCB jusqu'au 28 septembre, sans équivalence avec un nombre national de victimes

2.1 Une dépendance numérique peut franchir plusieurs frontières 11

2.2 Les rapports officiels soulignent l'exposition des identités et des systèmes 11

2.3 Les fournisseurs créent des dépendances de service 12

2.4 Les activités à discours politique exigent une attribution prudente 12

CHAPITRE 02

Contexte numérique et menaces en Belgique

EN BREF

Services publics, plateformes commerciales et fournisseurs partagent des dépendances numériques au-delà des frontières organisationnelles et nationales. Le CCB a reçu 588 signalements jusqu'au 28 septembre. Son rapport de novembre sur les identités place la protection des comptes au centre de la réponse. Les cas montrent aussi comment une interruption fournisseur devient un problème de service client. Identifiez les dépendances de comptes, de fournisseurs et d'activités nécessaires au fonctionnement de votre organisation.

2.1 Une dépendance numérique peut franchir plusieurs frontières

Le portail officiel belge décrit un État fédéral comprenant trois communautés et trois régions. Le néerlandais, le français et l'allemand sont les langues officielles. Ce sont des faits administratifs, sans explication des performances de sécurité. [S6]

Pour les défenseurs, la question utile concerne le contrôle d'un service et de ses données. Un contrat central peut soutenir plusieurs administrations locales. Une plateforme étrangère peut détenir des données clients belges. Un incident sur cette plateforme n'établit pas une intrusion dans le réseau propre de chaque client belge.

Le rapport distingue donc incidents organisationnels nationaux, incidents de services partagés et contexte de services étrangers. Il ne classe ni communautés linguistiques, ni régions, ni administrations selon leur sécurité. Les observations des domaines sélectionnés ne permettent pas de telles comparaisons.

La communication doit suivre les utilisateurs concernés. Préparez des avis clairs dans les langues du service. Conservez les mêmes périmètres, incertitudes et conseils de protection. La traduction ne doit pas transformer une divulgation possible en vol confirmé.

2.2 Les rapports officiels soulignent l'exposition des identités et des systèmes

Le CCB a reçu 588 signalements entre 1 janvier et 28 septembre 2026, contre 556 sur toute l'année 2025. Les périodes diffèrent. Le précédent total annuel est dépassé ; ce n'est pas un taux annuel de croissance. [S4]

Les rapports trimestriels décrivent une évolution des types d'incidents. Le premier trimestre compte 154 cyberincidents ; le deuxième en compte 188 au sein d'une population plus large de notifications. Ces chiffres ne sont pas interchangeables avec l'ensemble des notifications. [S7][S8]

Le troisième rapport trimestriel souligne les intrusions dans les systèmes et les vulnérabilités exposées. L'évaluation des identités du CCB de novembre situe les incidents liés aux comptes autour de 30% des signalements des deux premiers trimestres. Chaque chiffre conserve sa population et sa période. [S9][S5]

Cela justifie deux travaux parallèles. Les équipes identités doivent vérifier sessions, récupération et privilèges. Les équipes infrastructure doivent connaître les systèmes exposés nécessitant une correction urgente. Aucune ne peut clore son travail en remplissant seulement la liste de l'autre.

2.3 Les fournisseurs créent des dépendances de service

Le deuxième rapport trimestriel du CCB traite des chaînes logicielles touchant la Belgique. Les cas publics concernent des logiciels de santé, des plateformes pédagogiques et un service de signature utilisé par des administrations locales. Leur point commun est la dépendance, sans preuve d'un attaquant coordonné unique. [S8][S13][S22]

Pour le fournisseur, le premier livrable utile est une analyse d'impact propre à chaque client. Pour le client, c'est l'inventaire des données, comptes et processus dépendants. Le nombre de clients n'est pas celui des clients dont les données ont été prises.

Distinguez continuité commerciale et confidentialité. Un service peut être indisponible parce qu'il a été volontairement isolé. Un autre peut rester disponible alors que des données personnelles sont exposées. Le chapitre 5 consigne ces résultats séparément.

2.4 Les activités à discours politique exigent une attribution prudente

Le CCB considère les activités soutenues par des États et l'hacktivisme géopolitique comme des menaces pertinentes. Cette évaluation n'attribue pas chaque incident belge à un État. Les sources publiques de la campagne frigorifique illustrent cette distinction. [S8][S9][S26]

Reuters a rapporté des évaluations ministérielles différentes le 13 novembre. Le ministre de l'Intérieur jugeait l'implication iranienne très probable. Le ministre des Affaires étrangères estimait les informations insuffisantes pour une attribution officielle. Une enquête se poursuivait. [S26]

Ce rapport ne formule aucune attribution indépendante pour cette campagne. Il ne prend position ni sur les décisions gouvernementales, ni sur les différends internationaux, les questions linguistiques ou les relations historiques. Le discours d'un acteur n'établit ni motivation, ni responsabilité technique, ni impact.

Les institutions européennes apparaissent uniquement comme contexte public. Une implantation bruxelloise, une marque liée à l'UE ou une publication multilingue ne suffit pas à inclure un incident dans la population des organisations nationales belges.

POINTS À RETENIR

01

Reliez chaque chiffre officiel à sa population et à sa période.

02

Cartographiez les dépendances fournisseurs selon le service et les données réellement touchés.

03

Préservez l'incertitude dans les attributions et les traductions d'avis.

CHAPITRE 03

Exposition nationale : organisations et domaines sélectionnés

CE CHAPITRE RÉPOND À LA QUESTION

Que signifient les signaux mesurés pour les organisations sélectionnées ?

63 sur 250

domaines d'organisations sélectionnés avaient un identifiant proposé à la vente lors du contrôle

3.1 Fiche de périmètre 14
3.2 Signaux d'exposition par secteur 15
3.3 Appareils et identifiants 17
3.4 Traiter un constat actuel lié à une identité 18
3.5 Contrôles de messagerie et du web 19

CHAPITRE 03

Exposition nationale : organisations et domaines sélectionnés

EN BREF

63 des 250 domaines d'organisations sélectionnés avaient un identifiant proposé à la vente lors du contrôle. La valeur nationale Atlas est de 48 sur 100. Le portefeuille contient au moins 296 591 associations d'appareils et 26 236 674 identifiants enregistrés. Ces observations ne comptent ni personnes uniques, ni comptes actifs, ni intrusions confirmées. Les contrôles passifs concernent 245 de ces domaines. Vérifiez les annonces actuelles, les appareils associés aux salariés et les voies de récupération.

3.1 Fiche de périmètre

Attribut	Périmètre
Population	250 domaines principaux sélectionnés dans dix secteurs ; 245 avec observations passives
Unité	Un domaine principal ; le DNS n'établit ni indépendance juridique ni propriété
Sélection	Fonctions publiques et économiques ; portefeuille raisonné, sans recensement national classé
Date d'exposition	Observations cumulées d'appareils, identifiants, annonces et documents : 21 novembre 2026
Autres périodes	Mentions : 365 jours jusqu'au 22 novembre 2026 ; ressemblances : 30 jours ; observations passives : 22 novembre 2026
Chevauchement	Les sources, domaines, appareils et personnes peuvent se chevaucher ; les totaux ne comptent pas des utilisateurs uniques
Interprétation	Résultats limités aux domaines sélectionnés, sans prévalence nationale ni couverture de tous les actifs

La portée nationale du rapport ne rend pas le portefeuille représentatif. Un domaine peut servir salariés, étudiants, clients ou plusieurs unités opérationnelles. Une association de domaine n'établit ni propriété d'appareil ni intrusion dans le réseau d'entreprise. [S2]

3.2 Signaux d'exposition par secteur

La valeur nationale Atlas pour les 250 domaines sélectionnés est de 48 sur une échelle de 0–100. Une valeur plus élevée décrit davantage d'exposition externe observée dans ce portefeuille. Le tableau présente les nombres de signaux par secteur. [S2]

Annonces actuelles, associations d'appareils salariés et références documentaires décrivent des populations différentes

Chaque cellule indique les domaines présentant le signal sur 25 domaines sélectionnés par secteur. Les annonces actuelles d'identifiants sont en corail.

	Annonce actuelle	Historique	Appareils salariés	Références documentaires
Banque et finance	11/25	11/25	18/25	18/25
Gouvernement et services publics	3/25	3/25	11/25	11/25
Administration locale	2/25	2/25	23/25	18/25
Éducation et recherche	6/25	6/25	21/25	19/25
Santé et soins	2/25	2/25	19/25	13/25
Énergie et services publics	2/25	2/25	16/25	9/25
Transport et logistique	8/25	8/25	18/25	13/25
Industrie et entreprises	2/25	2/25	20/25	20/25
Commerce et services aux consommateurs	18/25	18/25	16/25	14/25
Télécoms, technologie et médias	9/25	9/25	17/25	18/25

Source : observations d'exposition de 250 domaines d'organisations sélectionnés, 21 novembre 2026. Associations cumulatives et chevauchantes, sans preuve d'intrusion ou de prévalence nationale [S2].

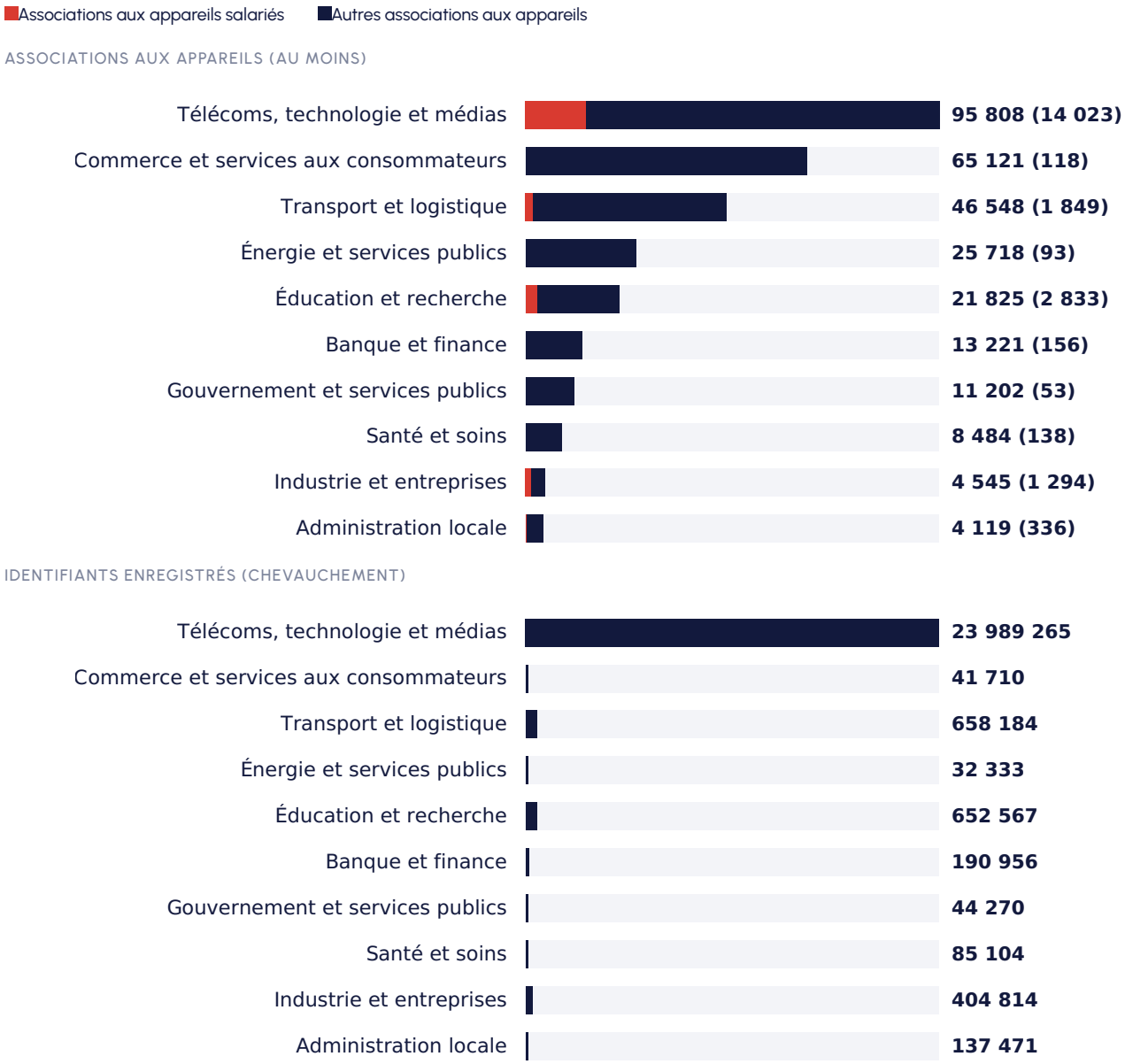
Secteur	Domaines	Annonces actuelles	Historique d'annonces	Avec appareils salariés	Avec documents
Banque et finance	25	11	11	18	18
Administration et services publics	25	3	3	11	11
Administration locale	25	2	2	23	18

Secteur	Domaines	Annonces actuelles	Historique d'annonces	Avec appareils salariés	Avec documents
Enseignement et recherche	25	6	6	21	19
Santé et soins	25	2	2	19	13
Énergie et services collectifs	25	2	2	16	9
Transport et logistique	25	8	8	18	13
Industrie et entreprises	25	2	2	20	20
Commerce et services aux consommateurs	25	18	18	16	14
Télécommunications, technologie et médias	25	9	9	17	18
Tous les domaines sélectionnés	250	63	63	179	153

Les deux dernières colonnes comptent les domaines ayant une association d'appareil salarié ou une référence documentaire, sans compter appareils ou documents. Chaque secteur contient 25 domaines sélectionnés. Une annonce actuelle justifie une vérification de compte, sans prouver qu'il fonctionne. [S2]

3.3 Appareils et identifiants

Les associations d'appareils et d'identifiants diffèrent entre les secteurs sélectionnés



Source : observations d'exposition de 250 domaines d'organisations sélectionnés, 21 novembre 2026. Associations cumulatives et chevauchantes, sans preuve d'intrusion ou de prévalence nationale [S2].

Secteur	Domaines	Appareils, au moins	Appareils salariés	Identifiants enregistrés
Banque et finance	25	13 221	156	190 956
Administration et services publics	25	11 202	53	44 270
Administration locale	25	4 119	336	137 471

Secteur	Domaines	Appareils, au moins	Appareils salariés	Identifiants enregistrés
Enseignement et recherche	25	21825	2833	652567
Santé et soins	25	8484	138	85104
Énergie et services collectifs	25	25718	93	32333
Transport et logistique	25	46548	1849	658184
Industrie et entreprises	25	4545	1294	404814
Commerce et services aux consommateurs	25	65121	118	41710
Télécommunications, technologie et médias	25	95808	14023	23989265
Tous les domaines sélectionnés	250	296591	20893	26236674

Le portefeuille contient au moins 296591 associations d'appareils, dont 20893 classées comme liées aux salariés. Les identifiants comprennent 9869372 enregistrements de bases compromises, 1488704 enregistrements de logiciels voleurs et 14878598 entrées de combolists. Ces sources se chevauchent ; leur total ne compte pas des comptes uniques. [S2]

Certains totaux d'appareils sont des minimums. Le classement salarié constitue une piste d'enquête, sans confirmer emploi ni propriété. Les domaines éducatifs ou destinés aux clients nécessitent une vérification des rôles avant intervention.

Le portefeuille contient aussi 38774 domaines ressemblants candidats et 1333 références documentaires exposées. La ressemblance n'établit pas un usage malveillant ; une référence documentaire ne prouve pas une divulgation confidentielle. Des mentions de discussions clandestines concernent 39 domaines et des mentions du dark web 31. La visibilité n'établit pas l'hostilité. [S2]

3.4 Traiter un constat actuel lié à une identité

Confiez le constat à un responsable des identités. Vérifiez si le compte existe, reste actif et a déjà fait l'objet de mesures correctives. Comparez l'ancienneté du constat aux activités récentes d'authentification et de récupération.

Si une session suspecte actuelle est vérifiée, révoquez-la. Examinez persistance, méthodes d'authentification enregistrées et modifications de messagerie. Si l'enregistrement est ancien et inactif, consignez cette conclusion. Préservez les preuves avant suppression ou réinitialisation d'un compte.

Les 63 annonces actuelles d'identifiants concernent le portefeuille de domaines sélectionnés. Les demandes et annonces de capacités des forums sont des observations distinctes. Ni annonce actuelle ni demande d'acheteur ne prouve un accès fonctionnel ou une intrusion organisationnelle confirmée. [S2][S3]

3.5 Contrôles de messagerie et du web

Observation	Nombre	Dénominateur
DMARC reject ou quarantine	188	245
Politique DMARC de surveillance	46	245
Aucune politique DMARC valide observée	11	245
SPF observé	234	245
Informations DKIM observées	204	245
Enregistrement DS (signataire de délégation) observé	65	245
Certificat TLS validé	240	245
Erreur de certificat TLS	1	245
Résultat TLS indéterminé	4	245
Réponse de page d'accueil obtenue	213	245
HSTS (HTTP Strict Transport Security) dans la réponse obtenue	164	213
CSP (Content Security Policy) dans la réponse obtenue	91	213

Une politique DMARC publiée indique le traitement demandé aux destinataires pour les messages non authentifiés. Une politique de surveillance diffère d'une politique contraignante. Même contraignante, elle ne prouve ni alignement de chaque expéditeur légitime ni application par chaque destinataire. [S2]

SPF et DKIM contribuent à l'authentification des courriels, sans constituer une évaluation complète de la sécurité. Une configuration de signature non observée n'est pas nécessairement inexistante. Les responsables doivent vérifier leurs véritables services d'envoi.

L'observation d'un enregistrement DS ne valide pas DNSSEC de bout en bout. Une observation TLS réussie concerne l'hôte évalué à cet instant. Examinez les observations manquantes ou échouées avant d'y voir un défaut de configuration organisationnel. [S2]

Les en-têtes de page d'accueil décrivent la réponse conservée, sans couvrir toutes les applications ou tous les chemins. Un en-tête absent peut justifier une vérification. Il n'établit ni exploitabilité, ni exposition de données sensibles, ni intrusion réussie.

Les observations de messagerie concernent les domaines sélectionnés

	DMARC reject / quarantine	SPF	TLS
Banque et finance	23/25	25/25	25/25
Gouvernement et services publics	21/25	20/25	24/25
Administration locale	20/23	22/23	22/23
Éducation et recherche	13/24	23/24	24/24
Santé et soins	16/24	21/24	23/24
Énergie et services publics	21/25	25/25	25/25
Transport et logistique	16/24	23/24	24/24
Industrie et entreprises	22/25	25/25	23/25
Commerce et services aux consommateurs	19/25	25/25	25/25
Télécoms, technologie et médias	17/25	25/25	25/25

Source : observations passives, 22 novembre 2026. Chaque cellule indique les domaines observés/évalués ; les politiques publiées ne prouvent pas leur application à chaque message [S2].

Secteur	Observés	DMARC reject/quarantine	SPF observé	TLS valide
Banque et finance	25	23	25	25
Administration et services publics	25	21	20	24
Administration locale	23	20	22	22
Enseignement et recherche	24	13	23	24
Santé et soins	24	16	21	23
Énergie et services collectifs	25	21	25	25
Transport et logistique	24	16	23	24
Industrie et entreprises	25	22	25	23

Secteur	Observés	DMARC reject/quarantine	SPF observé	TLS valide
Commerce et services aux consommateurs	25	19	25	25
Télécommunications, technologie et médias	25	17	25	25

POINTS À RETENIR

01

Vérifiez annonces actuelles et associations d'appareils salariés avec les responsables.

02

Distinguez enregistrements qui se chevauchent, personnes et intrusions confirmées.

03

Examinez les contrôles passifs selon le domaine et la date évalués.

CHAPITRE 04

Ce que nous observons sur le dark web

04

CE CHAPITRE RÉPOND À LA QUESTION

Que prouvent les annonces conservées concernant la demande de données, d'accès et de fraude en Belgique ?

1025

publications de forum distinctes conservées, avec couverture limitée au-delà de ces espaces

4.1 Fiche de périmètre 23
4.2 Volume et langue 25
4.3 Les produits annoncés 27
4.4 Études de cas 27
4.5 Cartes de preuve supplémentaires 33
4.6 Activité récente dans les forums conservés 35
4.7 L'apport des forums 35

CHAPITRE 04

Ce que nous observons sur le dark web

EN BREF

Les forums conservés montrent un marché de données clients, d'images d'identité, d'accès et d'outils frauduleux. Certaines annonces renvoient explicitement à d'anciens incidents. D'autres reconnaissent une provenance incertaine ou décrivent des structures de données proposées. Les dernières semaines ajoutent des revendications de tickets d'assistance, de modèles bancaires et de données de casinos. Le fait observé est l'annonce. Vérifiez pertinence, fraîcheur et accès avec des preuves organisationnelles fiables avant d'y voir un incident actuel.

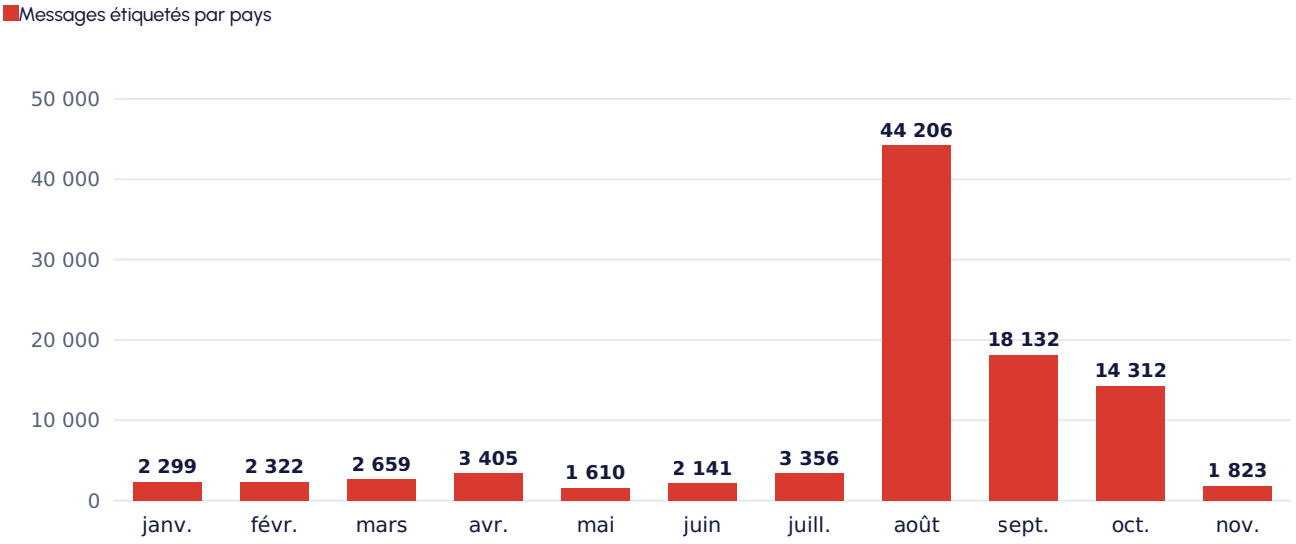
4.1 Fiche de périmètre

Attribut	Périmètre
Période	Dates des publications : 1 janvier–22 novembre 2026
Population conservée	1025 publications distinctes dans les observations de forums conservées
Sous-ensemble national	480 publications, comprises dans la population conservée
Sous-ensemble récent	31 publications datées du 9–22 novembre, également comprises dans la population
Espace	Le contenu conservé provient de forums ; les décomptes portant une étiquette nationale couvrent aussi d'autres plateformes.
Unité	Publication, sans équivalence avec un fichier, vendeur, achat, victime ou incident unique
Limite de couverture	Certains enregistrements annoncés restent indisponibles ; totaux étiquetés et forums conservés sont des populations distinctes

Les ensembles conservés se recoupent. Leurs totaux ne doivent pas être additionnés. Une étiquette nationale ou la pertinence d'un mot-clé ne valide pas indépendamment le ciblage, la provenance ou la nationalité d'une victime. [S3]

Brandefense Blackhole compte 96 265 publications étiquetées pour le pays sur les plateformes pendant la période. Une étiquette n'établit ni ciblage belge, ni pertinence criminelle, ni incident. Ces nombres incluent discussions et annonces ; ils diffèrent des 1025 publications de forums conservées. [S3]

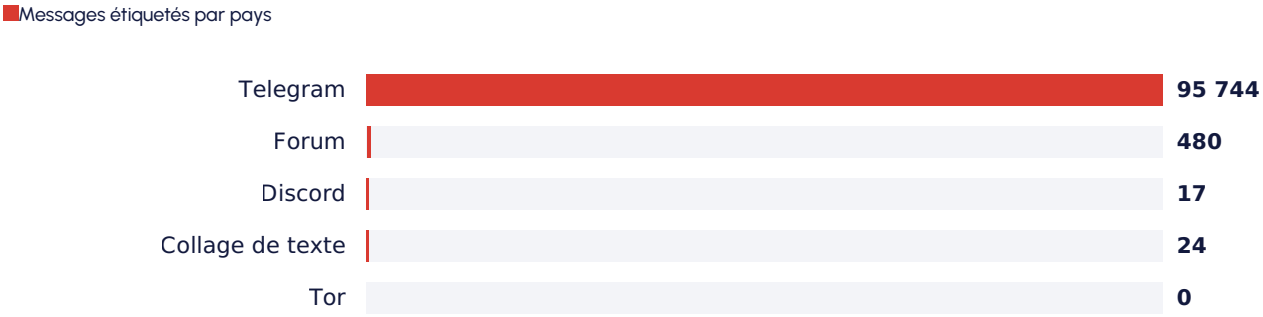
Les nombres mensuels étiquetés mesurent la visibilité enregistrée, pas les attaques



Source : Brandefense Blackhole, 1 janvier–22 novembre 2026 ; novembre partiel. Les messages étiquetés et les messages de forum conservés sont des populations distinctes, pas des incidents confirmés [S3].

Mois	Publications étiquetées
2026-01	2 299
2026-02	2 322
2026-03	2 659
2026-04	3 405
2026-05	1 610
2026-06	2 141
2026-07	3 356
2026-08	44 206
2026-09	18 132
2026-10	14 312
2026-11	1 823

Les nombres par plateforme décrivent la visibilité, pas des victimes



Source : Brandefense Blackhole, 1 janvier-22 novembre 2026 ; novembre partiel. Les messages étiquetés et les messages de forum conservés sont des populations distinctes, pas des incidents confirmés [S3].

Plateforme	Publications étiquetées
telegram	95744
forum	480
discord	17
paste	24
tor	0

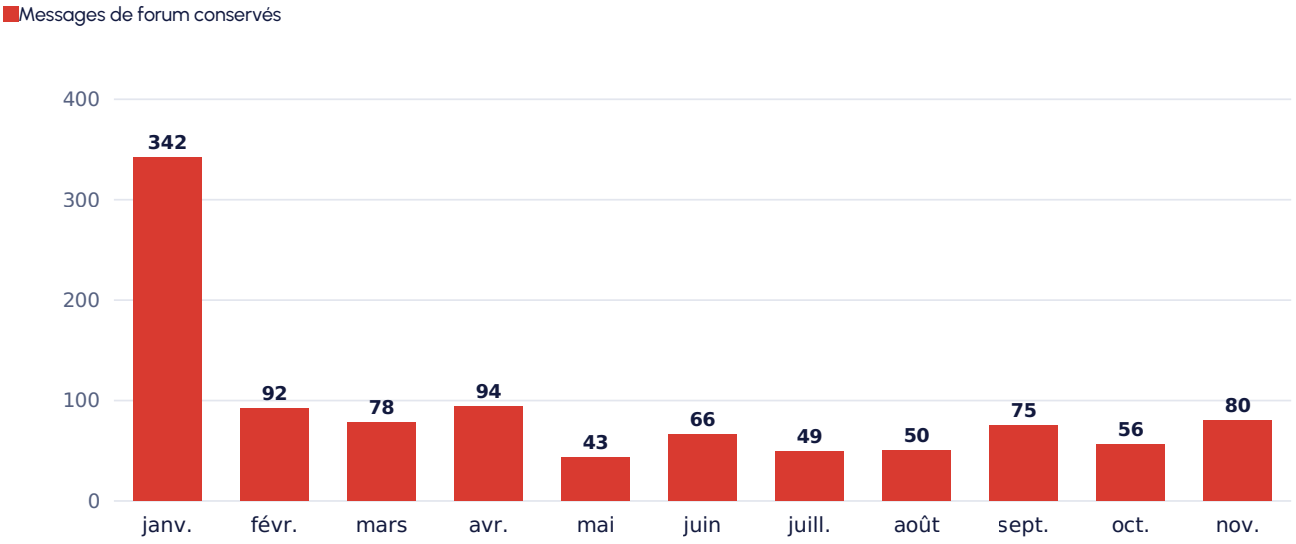
Telegram représente 95744 des 96265 publications étiquetées. Les preuves conservées des cas proviennent de forums ; la messagerie est représentée ici par des nombres. Ceux-ci ne valident ni les revendications ni la fréquence des attaques. Le contenu des forums n'établit pas les parts criminelles sur toutes les plateformes. [S3]

4.2 Volume et langue

Mois	Messages conservés
2026-01	342
2026-02	92
2026-03	78
2026-04	94
2026-05	43
2026-06	66
2026-07	49
2026-08	50

Mois	Messages conservés
2026-09	75
2026-10	56
2026-11	80

Les chiffres mensuels décrivent les messages conservés, pas la fréquence nationale des attaques



Source : Brandefense Blackhole, 1 janvier–22 novembre 2026 ; novembre partiel. Les messages étiquetés et les messages de forum conservés sont des populations distinctes, pas des incidents confirmés [S3].

Les chiffres mensuels décrivent cette population conservée. Ils n'établissent pas une hausse ou une baisse parallèle de la menace belge. Publicité, republications, discussions et visibilité peuvent chacune modifier le décompte. [S3]

La recherche a couvert les publications en anglais, français, néerlandais et russe, ainsi que d'autres contextes régionaux pertinents. La langue d'une annonce n'établit ni nationalité de son auteur ni langue des utilisateurs concernés.

4.3 Les produits annoncés

Famille	Ce que montrent les éléments conservés	Ce qu'ils n'établissent pas
Données clients et citoyennes	Offres liées aux télécoms, à la formation, aux services juridiques et aux consommateurs	Authenticité, personnes uniques ou intrusion récente
Documents d'identité	Demandes d'images de documents d'identité belges	Document fourni ou ouverture de compte réussie
Accès et sessions	Revendications d'accès administrateur et demandes de cookies	Accès actuel valide ou achat réalisé
Identifiants bancaires	Identifiants annoncés et prix demandés	Contrôle du compte ou autorisation de paiement
Outils frauduleux	Annonces de modèles d'hameçonnage propres à certaines banques	Outil fonctionnel, campagne déployée ou interception d'authentification réussie

Ce sont des thèmes observés, sans constituer des catégories d'incidents exclusives ou des parts d'une économie clandestine nationale. Une annonce peut proposer plusieurs produits. L'affichage d'un prix ne prouve pas une transaction. [S3]

4.4 Études de cas

A

CAS A

Une annonce de télécommunications renvoie à 2025

Fiche de preuve B01 | 24 janv. 2026 | Forum de fuites | Télécommunications

Revendication non vérifiée

REVENDICATION	La personne propose un échantillon de données qui concernerait plus de 300k personnes. Elle situe explicitement l'incident initial en juillet 2025.
CHRONOLOGIE	L'annonce conservée date du 24 janvier 2026. Des titres similaires et des republications ne prouvent pas que les fichiers sont identiques.
ÉLÉMENTS ÉTABLIS	L'annonce et sa référence historique sont conservées. Le nombre de données, leur source et leur authenticité ne sont pas vérifiés.
AUTRE EXPLICATION	Des données anciennes peuvent être copiées, renommées ou revendues. Une publication en 2026 ne prouve pas une nouvelle intrusion.

RÉPONSE	Vérifiez les comptes concernés et les corrections antérieures avant de décrire un nouvel incident. Préparez des conseils proportionnés si des données anciennes circulent de nouveau. [S3]

En définitive

Une annonce de janvier mentionne une date d'incident antérieure et propose un échantillon de données clients.

Fiche de preuve B01 — 24 janv. 2026

kazutlg | Forum de fuites | Forum | English

ORIGINAL

At the end of July 2025, [a telecom operator] detected a cyberattack on one of its IT systems [...] Here is a sample from this parsed database containing over 300k individuals.

TRADUCTION

Fin juillet 2025, [un opérateur de télécommunications] a détecté une cyberattaque [...] Voici un échantillon de cette base, qui contiendrait plus de 300k personnes.

Ce que nous pouvons établir

Une annonce de janvier mentionne une date d'incident antérieure et propose un échantillon de données clients.

Ce qui n'est pas établi

Le nombre et l'authenticité des données, une nouvelle intrusion en 2026 ou une transaction.

B

CAS B

La personne qui publie les données ignore leur origine

Fiche de preuve B02 | 21 janv. 2026 | Forum de fuites | Données de citoyens

Revendication non vérifiée

REVENDICATION	Un compte annonce 3,1M de dossiers de citoyens belges et suggère une origine publique, tout en reconnaissant que la source est inconnue.
CHRONOLOGIE	Le message du 21 janvier reçoit une réponse évoquant des données anciennes d'un réseau social. Le compte initial accepte cette possibilité.
ÉLÉMENTS ÉTABLIS	L'incertitude apparaît dans la discussion. Ni la revendication initiale ni la réponse ne valident la source des données.
AUTRE EXPLICATION	Des données historiques de réseaux sociaux, des sources publiques ou un changement d'étiquette restent plausibles. La discussion ne prouve pas un accès à une base publique.

RÉPONSE	Exigez une provenance validée et des échantillons pertinents avant d'alerter l'organisme supposé à l'origine des données. Un grand nombre associé à un pays ne remplace pas la vérification. [S3]

En définitive

Un message revendique une vaste base de population tout en reconnaissant une origine inconnue.

Fiche de preuve B02 — 21 janv. 2026

xmlrpc | Forum de fuites | Forum | English

ORIGINAL

Today, I leak data from 3.1M Belgian citizens. I don't have a source for this database [...] It's probably a government department scrape.

TRADUCTION

Aujourd'hui, je publie des données de 3,1M de citoyens belges. Je n'ai pas de source pour cette base [...] Il s'agit probablement de données extraites d'un service public.

Ce que nous pouvons établir

Un message revendique une vaste base de population tout en reconnaissant une origine inconnue.

Ce qui n'est pas établi

Une provenance publique, le nombre de personnes distinctes ou une intrusion dans un système public en 2026.

CAS C

C

Une offre de formation peut remettre des données anciennes en circulation

Revendication non vérifiée

Fiche de preuve B03 | 2 oct. 2026 | Forum de fuites | Formation

REVENDICATION	L'annonce propose plus de 700K personnes et +85 K IBAN, ainsi qu'un accès. Il s'agit de propositions distinctes.
CHRONOLOGIE	L'offre conservée date du 2 octobre. Des réponses de février et un autre lot d'octobre évoquent la même cible. La presse décrit séparément une republication. [S20]
ÉLÉMENTS ÉTABLIS	L'annonce est conservée. Le nombre de personnes distinctes et l'existence d'un accès actuel ne sont pas établis indépendamment.
AUTRE EXPLICATION	Un lot ancien peut être republié ou proposé par un autre compte. Un nom similaire ne prouve ni des fichiers identiques ni une intrusion distincte en octobre.

RÉPONSE	Vérifiez l'accès actuel aux comptes séparément de l'exposition historique. Prévenez les utilisateurs d'une reprise des usurpations lorsque l'organisme a établi la pertinence des données. [S3]

En définitive

Une annonce d'octobre revendique des données et un accès. Des réponses de février évoquent déjà le même sujet.

Fiche de preuve B03 2 oct. 2026

yneov18 Forum de fuites Forum English

ORIGINAL

I am selling the complete [vocational-training network] database from belgium containing more than 700K different people and +85 K IBAN [...] also selling the access.

TRADUCTION

Je vends la base complète [d'un réseau de formation professionnelle] en Belgique : plus de 700K personnes différentes et +85 K IBAN [...] je vends aussi l'accès.

Ce que nous pouvons établir

Une annonce d'octobre revendique des données et un accès. Des réponses de février évoquent déjà le même sujet.

Ce qui n'est pas établi

Le nombre de personnes distinctes, un accès encore valide ou une nouvelle intrusion en octobre.

D

CAS D

Une offre d'accès décrit plusieurs tables proposées

Fiche de preuve B04 8 nov. 2026 Forum de fuites Identité numérique

Revendication non vérifiée

REVENDICATION	Un vendeur revendique un accès administrateur à un service de vérification d'identité, environ 412k dossiers et un prix de USD 4 550.
CHRONOLOGIE	L'offre date du 8 novembre. Les descriptions des tables de contact, de contrôle d'identité et de récupération les présentent à plusieurs reprises comme proposées.
ÉLÉMENTS ÉTABLIS	Les descriptions de structure et la revendication d'accès sont conservées. Elles ne démontrent pas l'existence d'un compte, d'un environnement client ou d'une base validés.
AUTRE EXPLICATION	Les structures pourraient être hypothétiques, copiées ou synthétiques. Leur formulation soulève des questions sans prouver à elle seule une fabrication.

RÉPONSE	Vérifiez l'environnement client par les canaux fiables du fournisseur. Conservez les traces d'administration et de récupération avant d'imposer une réinitialisation générale. [S3]

En définitive

L'offre et ses descriptions de structure existent. Le titre revendique environ 412k enregistrements.

Fiche de preuve B04 — 8 nov. 2026

DataJava | Forum de fuites | Forum | English

ORIGINAL

Access: full admin account in [identity-verification portal] [...] Proposed contact table [...] Proposed identity verification case table [...] Proposed account recovery case table [...] Price: $4,550

TRADUCTION

Accès : compte administrateur complet dans [un portail de vérification d'identité] [...] Table de contacts proposée [...] Table de vérification d'identité proposée [...] Table de récupération de compte proposée [...] Prix : $4 550

Ce que nous pouvons établir

L'offre et ses descriptions de structure existent. Le titre revendique environ 412k enregistrements.

Ce qui n'est pas établi

Un accès valide, des données réellement stockées, le nombre annoncé, une vente ou un incident chez un fournisseur.

CAS E

E

Une annonce de phishing présente des modèles bancaires

Fiche de preuve B05 | 20 nov. 2026 | Forum de fuites | Fraude bancaire

Revendication non vérifiée

REVENDICATION	L'annonce SALTA3 propose des modèles pour certaines banques, dont des marques belges, et revendique des fonctions d'authentification interactives.
CHRONOLOGIE	Le message du 20 novembre appartient aux deux dernières semaines. C'est une publicité pour un outil, pas une trace d'attaque conservée.
ÉLÉMENTS ÉTABLIS	L'annonce et la liste de marques revendiquées existent. Une marque bancaire dans une liste de modèles indique un thème d'usurpation, pas un accès aux systèmes bancaires.
AUTRE EXPLICATION	Les fonctions peuvent être exagérées ou copiées. Le document ne prouve ni leur fonctionnement, ni leur déploiement, ni une interception d'authentification réussie.

RÉPONSE	Testez le signalement client et le traitement des ajouts d'appareils ou validations de paiement inhabituels. Examinez l'authentification résistante au phishing en distinguant publicité et attaque observée. [S3]

En définitive

Une annonce du 20 novembre propose des modèles bancaires, dont des marques belges, et revendique des fonctions interactives.

Fiche de preuve B05 — 20 nov. 2026

0xcasper | Forum de fuites | Forum | English

ORIGINAL

SALTA3 is a live panel phishing kits customized to target specific banks [...] OTP/TAN/2FA support including QR Codes and PhotoTAN method.

TRADUCTION

SALTA3 est un panneau de phishing avec des kits adaptés à certaines banques [...] prise en charge OTP/TAN/2FA, dont les codes QR et PhotoTAN.

Ce que nous pouvons établir

Une annonce du 20 novembre propose des modèles bancaires, dont des marques belges, et revendique des fonctions interactives.

Ce qui n'est pas établi

Un outil fonctionnel, une interception réussie, un déploiement, des victimes, un accès aux systèmes bancaires ou des pertes.

CAS F

F ■ Une revendication vise des tickets et pièces jointes de support

Revendication non vérifiée

Fiche de preuve B06 | 13 nov. 2026 | Forum de fuites | Technologie d'entreprise

REVENDICATION	Un compte affirme détenir tous les tickets et pièces jointes et annonce 6 028 utilisateurs. Ses déclarations sur les clients et des contacts antérieurs ne sont pas vérifiées.
CHRONOLOGIE	Le message date du 13 novembre. Aucune preuve conservée ne confirme indépendamment le contact antérieur revendiqué avec le fournisseur.
ÉLÉMENTS ÉTABLIS	La déclaration est conservée. Elle ne démontre ni la possession de chaque pièce jointe ni l'effet sur un client particulier.
AUTRE EXPLICATION	Les données pourraient être partielles, anciennes, copiées ou fabriquées. Le nom d'un client dans une annonce ne valide pas son exposition.

RÉPONSE

Demandez au fournisseur une déclaration propre à votre organisation. Limitez les pièces jointes sensibles et examinez les accès administratifs aux portails contenant des informations opérationnelles. [S3]

En définitive

Un acteur revendique des tickets et pièces jointes. Le message annonce 6 028 utilisateurs.

Fiche de preuve B06 13 nov. 2026

updap Forum de fuites Forum English

ORIGINAL

some random internet group has your every support ticket and every attachment [...] We urge your customers to review what they shared with you.

TRADUCTION

Un groupe sur Internet possède chacun de vos tickets de support et chaque pièce jointe [...] Nous invitons vos clients à vérifier ce qu'ils vous ont transmis.

Ce que nous pouvons établir

Un acteur revendique des tickets et pièces jointes. Le message annonce 6 028 utilisateurs.

Ce qui n'est pas établi

La possession de tous les tickets, les clients concernés, un accès actuel ou un effet technique.

4.5 Cartes de preuve supplémentaires

Les autres cartes montrent des annonces d'identifiants, des demandes d'images d'identité, des achats de sessions et une offre récente liée aux casinos. Les extraits originaux proviennent d'annonces conservées dont les éléments identifiants ont été retirés. Ce ne sont ni des instructions ni des descriptions de produits validées. [S3]

Fiche de preuve B07 — 13 avr. 2026

[alias withheld] | Forum de fuites | Forum | English

ORIGINAL

I SELL 40K+ BELGIUM IBANS PRICE : 1000 IBANS = 1,75$ (USD) ALL IBANS = 70,19$ (USD)

TRADUCTION

JE VENDS 40K+ IBAN BELGES PRIX : 1 000 IBAN = 1,75$ (USD) TOUS LES IBAN = 70,19$ (USD)

Ce que nous pouvons établir
Une personne propose des identifiants de compte associés à la Belgique et affiche des prix.

Ce qui n'est pas établi
Un accès aux comptes, une autorisation de paiement, un incident bancaire ou une vente.

Fiche de preuve B08 — 24 févr. 2026

Crazy88 | Forum de fuites | Forum | English

ORIGINAL

Hello i'm looking for a seller that can provide belgium ids i need a lot of them 500+

TRADUCTION

Bonjour, je cherche un vendeur pouvant fournir des pièces d'identité belges, il m'en faut beaucoup, 500+

Ce que nous pouvons établir
Une demande d'achat de documents d'identité belges.

Ce qui n'est pas établi
Un document fourni, un achat, une vérification d'identité réussie ou une fuite à l'origine des images.

Fiche de preuve B09 — 3 nov. 2026

buylogs | Forum de fuites | Forum | English

ORIGINAL

I will buy requests from your logs EXPENSIVELY - cookies with active email [...] 250-2500 (fixed and percentage possible)

TRADUCTION

J'achète CHER des éléments de vos journaux : cookies avec messagerie active [...] 250$-2 500$ (montant fixe et pourcentage possibles)

Ce que nous pouvons établir
Une demande d'achat vise des plateformes logistiques et des cookies de messagerie actifs, avec une fourchette de prix.

Ce qui n'est pas établi
Une réponse, des sessions achetées, des comptes valides, une vente ou une intrusion dans la plateforme.

Fiche de preuve B10 — 21 nov. 2026

WSdatabase | Forum de fuites | Forum | English

ORIGINAL

Belgium Casino User Database 2026

TRADUCTION

Base d'utilisateurs de casino Belgique 2026

Ce que nous pouvons établir
L'annonce du 21 novembre et un échantillon affiché de coordonnées avec des champs de dépôt annoncés.

Ce qui n'est pas établi
Le casino d'origine, la fraîcheur des données, les dépôts, un accès actuel ou une nouvelle intrusion.

Une offre d'IBAN affiche USD 1,75 pour 1000 identifiants et USD 70,19 pour l'ensemble annoncé. Les quantités ne constituent pas un inventaire exact vérifié. Un IBAN n'autorise pas à déplacer des fonds. [S3]

Une demande de sessions logistiques affiche une fourchette de USD 250–2 500. Elle établit une demande et une fourchette souhaitée, sans valider compte ou transaction. L'enjeu défensif concerne la récupération des sessions et la vérification indépendante des modifications de paiement. [S3]

4.6 Activité récente dans les forums conservés

Date de publication	Carte	Annonce	Limite
2026-11-13	B06	Tickets d'assistance fournisseur et pièces jointes	Nommer des clients dans une revendication n'établit pas leur impact
2026-11-20	B05	Modèles d'hameçonnage propres à des banques	La publicité ne prouve ni déploiement ni incident du système bancaire
2026-11-21	B10	Données clients liées aux casinos	Une publicité similaire de septembre ne prouve ni fichiers identiques ni nouvel incident

L'offre de service d'identité B04 est datée du 8 novembre et se situe hors de la période récente. Sa proximité avec des avis ultérieurs ne crée aucun lien. Aucun opérateur commun ni incident commun n'est déduit. [S3]

Une annonce du 22 novembre proposait encore des modèles d'usurpation bancaire et revendiquait des fonctions d'authentification interactives. Une autre annonce multinationale incluait la Belgique dans ses tarifs. Ces observations n'établissent ni accès fonctionnel, ni validité des cartes, ni nouvelle intrusion bancaire. [S3]

4.7 L'apport des forums

Les forums rendent visibles la formulation et la date des revendications. Un annonceur de données démographiques reconnaît l'incertitude de leur provenance. Un annonceur télécom donne une ancienne date d'incident. Un vendeur d'accès décrit à plusieurs reprises ses tableaux comme proposés.

Ces détails aident l'enquêteur à poser de meilleures questions. Ils ne tranchent pas l'authenticité. Un titre, un nombre de lignes ou un schéma peut être copié, partiellement exact, périmé ou inventé. Le rapport conserve ces possibilités au lieu de traiter toutes les annonces comme des violations équivalentes.

POINTS À RETENIR

01
Les dates des publications datent la publicité, pas les intrusions.

02
Vérifiez séparément la provenance et le fonctionnement d'un accès.

03
La publicité récente d'outils frauduleux justifie la préparation, sans prouver des attaques réussies.

CHAPITRE 05

Incidents confirmés et revendications par secteur

CE CHAPITRE RÉPOND À LA QUESTION

Quels effets sont établis et quels chiffres restent ceux d'un revendiquant ?

3

questions distinctes : disponibilité, exposition des données et attribution

5.1 Lire le registre des incidents 37
5.2 Soins et services pédagogiques 38
5.3 Services communaux et services publics partagés 40
5.4 Données d'adhésion, clients et activités 42
5.5 Autres incidents consignés et revendications rapportées 44
5.6 Autres cas d'entreprises, de recherche et de services locaux 45
5.7 Ce que ces cas établissent 47

CHAPITRE 05

Incidents confirmés et revendications par secteur

EN BREF

Les sources publiques belges couvrent soins interrompus, données d'adhésion exposées, plateformes pédagogiques, systèmes communaux et fournisseurs partagés. Plusieurs organisations ont confirmé un incident sans arrêter le nombre de personnes concernées. La restauration et l'analyse des pertes de données ont parfois évolué à des dates différentes. Les fiches conservent ces distinctions. Utilisez l'exemple opérationnel le plus proche pour tester confinement, information des clients et reprise.

5.1 Lire le registre des incidents

Un incident confirmé ne valide pas chaque revendication criminelle qui s'y rapporte. Le registre distingue déclarations directes d'organisations, avertissements officiels, reportages attribués et annonces clandestines. Les cas suivants sont des dossiers sélectionnés, sans recensement national.

Certains services étrangers détiennent des données d'utilisateurs belges. Ils font partie des dépendances, mais leur nombre mondial d'utilisateurs n'est pas un nombre de Belges touchés. Les annonces répétées et avis de fédérations liées ne sont pas automatiquement indépendants.

Les noms apparaissent uniquement avec confirmation officielle et couverture médiatique élargie. Les autres organisations sont décrites par leur rôle général. Cette désignation protège l'identité sans masquer l'incertitude concernant l'événement.

5.2 Soins et services pédagogiques

CAS G

G

Un hôpital isole ses systèmes en janvier

Santé

Récit public attribué

ÉVÉNEMENT	Un réseau hospitalier belge a détecté une grave perturbation informatique le 13 janvier. Sa déclaration citée dans la presse décrivait un arrêt préventif sur ses campus. [S10]
CHRONOLOGIE	Des soins programmés ont été interrompus et des patients critiques transférés. Le récit de janvier conservé n'établit ni rançon payée, ni attaquant nommé, ni périmètre complet de perte de données.
ÉTABLI	La continuité clinique dépendait d'un fonctionnement sans systèmes numériques. Une décision d'arrêt peut protéger les systèmes tout en créant des coûts opérationnels immédiats.
ALTERNATIVES ET LIMITES	Une perturbation seule ne distingue pas chiffrement, confinement ou autre cause technique. Les revendications criminelles ultérieures exigent leurs propres preuves.
RÉPONSE	La direction clinique doit exercer documentation manuelle, transferts de patients et échanges avec les établissements voisins. Consignez les systèmes nécessaires avant le retour à la programmation normale.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

CAS H

H

Basic-Fit confirme un incident transfrontalier de données clients

Services aux consommateurs

Récit public attribué

ÉVÉNEMENT	Safeonweb a relayé le 13 avril la confirmation de l'entreprise : des membres belges étaient concernés par un incident de données clients. Reuters a également rapporté la déclaration. [S11][S12]
CHRONOLOGIE	La divulgation décrivait des informations de membres de plusieurs pays. Le chiffre d'environ un million concerne la population internationale plus large, sans se limiter à la Belgique.

ÉTABLI	Les données potentiellement touchées incluaient coordonnées, dates de naissance et informations bancaires. L'entreprise indiquait que mots de passe et documents d'identité n'avaient pas été pris. [S11]
ALTERNATIVES ET LIMITES	Un identifiant de compte bancaire ne prouve pas un accès au compte de son titulaire. Les sources conservées n'établissent pas le nombre de personnes touchées en Belgique.
RÉPONSE	Avertissez les clients des messages citant de véritables informations d'adhésion. L'assistance doit vérifier l'identité par une procédure fiable distincte avant de modifier coordonnées ou données de paiement.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

CAS I

Un incident pédagogique soulève la question des dépendances belges

Récit public attribué

Enseignement

ÉVÉNEMENT	L'avis Safeonweb du 6 mai décrivait un incident confirmé par l'éditeur d'une plateforme pédagogique utilisée en Belgique. La confirmation de l'éditeur datait du 1 mai. [S13]
REVENDICATION	Un groupe criminel annonçait une population mondiale de 275 millions d'utilisateurs. Safeonweb qualifiait explicitement ce nombre de non confirmé. Ce n'est pas un chiffre belge.
ÉTABLI	Les catégories possibles comprenaient noms, adresses électroniques, identifiants étudiants et messages. À cette date, l'éditeur ne signalait aucune indication concernant mots de passe, dates de naissance, identifiants officiels ou données financières.
ALTERNATIVES ET LIMITES	Une revendication portant sur la plateforme n'établit pas les données prises dans un établissement précis. Notifications institutionnelles et rétablissement du service répondent à des questions différentes.
RÉPONSE	Les établissements doivent demander une analyse d'impact ciblée, préparer les avis étudiants et revoir l'assistance du personnel. Les messages pédagogiques inattendus relèvent aussi de la protection des utilisateurs.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

Le deuxième rapport trimestriel du CCB traite également d'un incident chez un fournisseur de logiciels de santé pertinent pour la Belgique. Cela établit une dépendance, sans prouver un vol de données dans chaque hôpital client. [S8]

5.3 Services communaux et services publics partagés

J

CAS J

Machelen révise son évaluation des données après l'incident initial

Administration locale

Récit public attribué

ÉVÉNEMENT	La commune a identifié un cyberincident le 11 septembre. Sa propre mise à jour indique que des analyses supplémentaires ont confirmé un vol de données personnelles le 22 septembre. [S15][S16]
CHRONOLOGIE	Les services numériques ont été affectés. L'avis communal conservé indique leur retour opérationnel, avec retards possibles, alors que l'enquête sur les données se poursuivait.
ÉTABLI	Date d'incident, date de confirmation et état de restauration sont des faits différents. L'incertitude initiale n'a pas empêché des mises à jour ultérieures.
REVENDICATION	Une publication d'extorsion ultérieure figure dans la population de rançongiciels du rapport. Elle n'établit indépendamment ni données complètes, ni méthode d'attaque, ni identité de l'intrus. [S1]
RÉPONSE	Maintenez une page de suivi avec modifications datées. Donnez aux habitants des conseils utiles tout en précisant les catégories de données et personnes encore examinées.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

L

CAS L

Un fournisseur de signature numérique affecte les processus locaux

Services publics partagés

Récit public attribué

ÉVÉNEMENT	Un reportage du 26 octobre citait un directeur général décrivant un accès non autorisé au service de signature. Une activité suspecte avait été détectée le 23 octobre. [S22]

CHRONOLOGIE	Le fournisseur a mis le service hors ligne, puis l'a rétabli le soir suivant avec restrictions. Des analyses d'impact propres à chaque client étaient en préparation.
ÉTABLI	Le fournisseur évoquait surtout des métadonnées et déclarait qu'aucune signature frauduleuse n'avait été créée. Ce sont des déclarations attribuées, sans conclusion forensique indépendante.
ALTERNATIVES ET LIMITES	Plus de 120 autorités locales utilisaient le module. Cette clientèle n'est pas un décompte d'autorités touchées. Une population d'intégration distincte ne doit pas lui être ajoutée.
RÉPONSE	Demandez l'impact propre à vos documents, identités et intégrations. Examinez les autorisations remplacées et vérifiez les avis de paiement par un canal officiel connu.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

M

CAS M

Les services fiscaux fédéraux rétablissent les applications par étapes

Récit public attribué

Administration

ÉVÉNEMENT	SPF Finances/FOD Financiën a confirmé une cyberattaque le 28 octobre. Son avis de reprise indique un confinement en quelques heures et une mise hors ligne temporaire des applications. [S23][S24]
CHRONOLOGIE	Les principaux services sont revenus le 31 octobre. Une fonction de précompte mobilier est revenue le 6 novembre, puis e604 le 12 novembre. Ce sont des étapes de restauration, sans intrusions distinctes.
ÉTABLI	L'autorité indiquait que son enquête n'avait trouvé ni exfiltration ni contrôle d'applications par l'attaquant. Attribuez cette conclusion à l'autorité et à son enquête. [S23]
ALTERNATIVES ET LIMITES	Un arrêt préventif affecte réellement la disponibilité. Il ne prouve pas un vol de données ; la restauration seule n'en établirait pas non plus l'absence.
RÉPONSE	Exercez la reprise progressive et indiquez les fonctions encore indisponibles. Séparez confinement technique, effets utilisateurs et constats de confidentialité dans le dossier d'incident.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

5.4 Données d'adhésion, clients et activités

K

CAS K

Un incident d'adhésion et un décompte criminel plus élevé

Services aux consommateurs

Récit public attribué

ÉVÉNEMENT	Une chaîne de salles de sport a reconnu un incident touchant les adhésions. Sa porte-parole décrivait dans la presse des dossiers liés à au plus 31 de ses 85 clubs belges. [S18]
REVENDICATION	Le chiffre largement repris de 150 000 membres était attribué aux annonceurs des données. Il ne doit pas devenir un nombre de personnes touchées confirmé par l'entreprise.
ÉTABLI	Les catégories rapportées comprenaient identité, coordonnées, adhésion et certains identifiants bancaires. L'entreprise déclarait que mots de passe et données de santé n'étaient pas concernés. [S18]
ALTERNATIVES ET LIMITES	Clubs, membres, prospects et enregistrements annoncés sont des unités différentes. Diviser un décompte revendiqué par les clubs n'établirait pas l'exposition par club.
RÉPONSE	Informez les personnes identifiées par l'enquête de l'entreprise et préparez l'assistance aux usurpations ciblées. Ne validez pas un appelant parce qu'il connaît une donnée d'adhésion ou bancaire.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

N

CAS N

Les perturbations frigorifiques font des accès distants un enjeu opérationnel

Opérations commerciales

Récit public attribué

ÉVÉNEMENT	Les avertissements officiels et reportages décrivent un incident de novembre touchant des installations frigorifiques commerciales. Les changements de fonctionnement ont eu des conséquences pour les magasins et leurs stocks. [S25][S27]

CHRONOLOGIE	Les perturbations belges ont été rapportées le 2 novembre, suivies de conseils techniques et déclarations attribuées. Les sources comptaient des magasins, des équipements et des clientèles de fournisseurs différentes.
ÉTABLI	Les équipes doivent maîtriser l'accès distant et pouvoir rétablir des réglages sûrs. Les sources ne justifient pas l'addition de tous les équipements et magasins annoncés.
ATTRIBUTION	Reuters a rapporté des évaluations ministérielles contradictoires le 13 novembre. Le rapport ne tranche pas ce désaccord et n'attribue pas indépendamment la campagne. [S26]
RÉPONSE	Supprimez immédiatement l'accès internet public direct aux interfaces de gestion frigorifique. Opérations et sécurité doivent coordonner continuité sûre et maintenance distante protégée, limiter les comptes aux besoins approuvés et exercer un mode local sûr. Vérifiez les réglages sûrs et conservez la preuve que les interfaces ne sont plus directement accessibles. [S25]

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

CAS O

Un avis récent concernant des chèques-cadeaux

Services aux consommateurs

Récit public attribué

ÉVÉNEMENT	Safeonweb a averti le 20 novembre d'un accès non autorisé à une plateforme de chèques-cadeaux. L'avis relayait le constat de l'entreprise et précisait que l'enquête continuait. [S29]
ÉTABLI	Des noms et adresses électroniques ont pu être consultés. Selon l'entreprise, mots de passe et données de carte n'étaient pas touchés à ce stade.
ALTERNATIVES ET LIMITES	Aucun nombre de clients belges touchés n'était fourni. Des messages de suivi convaincants constituent un risque plausible, sans preuve qu'une fraude précise ait déjà utilisé ces données.
RÉPONSE	Les équipes clients doivent publier un avertissement court sur les canaux habituels. Conseillez l'ouverture directe de l'application ou du site officiel pour vérifier un message inattendu.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

5.5 Autres incidents consignés et revendications rapportées

Ces lignes préservent la couverture d'autres incidents sans transformer chaque récit de presse en constat technique vérifié.

Période	Rôle général	Preuve et limite	Conséquence défensive
juin	Une agence publique sensible	Un reportage décrit un incident de gestion mobile entre 2025 et printemps 2026 ; confirmation officielle et attribution restaient non résolues [S14]	Examinez l'accès au plan de gestion sans supposer que le réseau de renseignement interne a été atteint
septembre	Une fédération sportive	La presse cite la confirmation d'un incident de base d'adhérents ; périmètre complet non établi indépendamment [S17]	Préparez les avis et examinez l'administration externalisée
septembre	Une administration sportive liée	Une fédération et son aile sont traitées ensemble ; les nombres annoncés restent des revendications [S17]	Gardez un dossier de campagne unique lorsque les systèmes sont liés
octobre	Un groupe scolaire	Un directeur confirme un incident concernant élèves et personnel ; 3 550 plus 650 donnent 4 200 personnes dans la population rapportée [S19]	Examinez accès du personnel et assistance, avec attention aux adresses privées
octobre	Un réseau de formation professionnelle	La presse décrit la republication de données attribuées à un incident de février ; 700 000 enregistrements et 85 000 données bancaires sont des chiffres rapportés [S20]	Une republication peut renouveler le risque d'hameçonnage sans nouvelle intrusion
octobre	Une plateforme pédagogique publique	La presse décrit une fermeture du service et un décompte de données annoncé séparément [S21]	Vérifiez séparément disponibilité et revendication de données

Période	Rôle général	Preuve et limite	Conséquence défensive
novembre	Un service de paiement d'avantages salariés	L'avis officiel décrit une possible exposition des comptes ; l'entreprise ne constatait ni problème de paiement ni transactions suspectes [S28]	Avertissez les titulaires sans annoncer des pertes non vérifiées
Avril	Un service de réservation en ligne	Safeonweb a signalé un possible accès aux réservations et un changement des codes PIN ; l'entreprise a indiqué que les données financières n'avaient pas été consultées [S11]	Aucun total belge d'utilisateurs concernés établi

5.6 Autres cas d'entreprises, de recherche et de services locaux

R

CAS R

Un institut confirme des données copiées et maintient ses services

Recherche médicale

Récit public attribué

RÉCIT OFFICIEL

L'avis d'un institut médical et scientifique décrit accès non autorisé et copie d'une base après détection le 12 octobre. L'avis a été actualisé le 10 novembre. [S49]

ÉTABLI

L'institut indique que la majorité des informations copiées étaient codées, et une part plus petite directement identifiable. Ses constats actuels n'identifiaient pas d'effets sur d'autres systèmes ; soins et enseignement continuaient.

LIMITES

Des données codées ne sont pas automatiquement anonymes. Un nombre de personnes notifiées, rapporté séparément, ne mesure pas toute la base copiée. Le rapport ne fournit aucun total combiné de personnes concernées.

RÉPONSE

Recherche et vie privée doivent évaluer ensemble codage et identification. Identifiez le détenteur des informations de correspondance, documentez les projets concernés et préparez une communication proportionnée aux participants.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

CAS S

S

Les contacts d'un organisme professionnel exigent un dénominateur précis

Services professionnels

Récit public attribué

RÉCIT OFFICIEL	Dans sa mise à jour du 6 novembre, un organisme juridique indique avoir été informé de l'incident le 29 octobre. L'avis décrit un accès à une application administrative et des coordonnées proposées à la vente. [S50]
ÉTABLI	L'avis identifie environ 27 500 contacts non avocats, en plus des dossiers d'avocats. Il ne donne pas un total unique de personnes touchées.
LIMITES	L'organisme indique que son analyse n'a identifié ni données bancaires ni catégories particulières de données personnelles concernées. C'est son évaluation, sans vérification indépendante de chaque fichier annoncé.
RÉPONSE	Distinguez populations professionnelles et contacts externes. Avertissez des messages utilisant de vraies coordonnées et vérifiez le périmètre avant de reprendre un décompte supérieur d'annonceur.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

Les cas suivants élargissent la vue des services. Ils n'établissent pas tous un vol de données ou un rançongiciel.

Période	Rôle général	Ce que la source étaye	Limite
avril	Une commune	Le bourgmestre décrit perturbation et vol de données ; reprise progressive [S53]	Déclaration municipale originale non conservée ; aucun décompte complet des personnes
mai	Un fabricant chimique	Sa clarification décrit un accès non autorisé ; les analyses ne trouvent aucune preuve d'exfiltration ou de rançongiciel [S47]	La publicité ultérieure concerne le même événement de mai
mai	Un exploitant de parc de recyclage	Le suivi limite l'incident à un ordinateur fournisseur ; activités isolées par précaution [S48]	Aucune indication d'exfiltration dans l'enquête décrite
juillet	Un fournisseur externe de données clients de supermarché	La presse cite une déclaration sur des coordonnées détenues sur un serveur fournisseur distinct [S51]	Ne pas généraliser aux paiements ou à tous les clients

Période	Rôle général	Ce que la source étaye	Limite
août	Un vendeur de meubles	Un porte-parole décrit une brève perturbation et l'accès aux coordonnées et commandes clients [S52]	L'attribution criminelle reste une revendication
octobre	Un voyagiste	Un porte-parole confirme un incident de données et un avertissement clients [S56]	Origine des messages frauduleux personnalisés non résolue
octobre, rapporté en novembre	Un négociant en métaux précieux	La presse cite une confirmation d'accès aux systèmes clients [S54]	Le lien supposé avec des cambriolages n'est pas établi
novembre	Un site communal public	Un bourgmestre décrit accès au site et exposition possible de comptes du personnel [S55]	Aucun constat d'exposition citoyenne ou d'accès aux services distincts

Un service de comptes de recharge fournit un contexte transfrontalier récent. Sa FAQ décrit une attaque le 8 novembre, découverte le 10 novembre et corrigée le 12 novembre. Les utilisateurs ont été informés le 18 novembre. Aucun décompte belge n'est établi. [S46]

VRT rapporte plus de 3,5 millions d'utilisateurs en Europe ; cette population n'est pas un nombre de comptes touchés. [S71] L'entreprise identifie des données de compte et de profil, dont des empreintes de mots de passe. Son avis exclut d'autres catégories. Chaque prestataire belge doit vérifier sa dépendance et ses utilisateurs. [S46]

5.7 Ce que ces cas établissent

Le mécanisme répété le mieux étayé est le décalage entre frontière du service et frontière de l'organisation. Les membres utilisent une plateforme, le personnel dépend d'un fournisseur et les habitants d'une application administrative. La réponse doit identifier la véritable dépendance.

Les cas montrent aussi l'importance d'informations claires. Une confirmation peut restreindre une revendication criminelle sans éliminer tous les risques. Un avis de reprise aide à travailler tandis que l'enquête sur les données continue.

Le rapport n'additionne pas clients, enregistrements revendiqués, organisations et magasins dans un chiffre unique. Un tel total n'aurait pas d'unité cohérente. Les dirigeants doivent demander quel service, quelle donnée et quelle personne nécessitent une action immédiate.

POINTS À RETENIR

01

Distinguez restauration, exposition des données et attribution.

02

La clientèle fournisseur n'est pas le total des victimes touchées.

03

Des données republiées peuvent renouveler la fraude sans prouver une nouvelle intrusion.

CHAPITRE 06

Hacktivisme, perturbations et systèmes opérationnels

CE CHAPITRE RÉPOND À LA QUESTION

Qu'a-t-on observé ou revendiqué et comment maintenir les services pendant une perturbation ?

9–22 novembre

période récente au sein de la fenêtre annuelle plus large

6.1 Chronologie 50
6.2 Revendication et récit public 51
6.3 Un incident de site n'est pas un incident d'équipement 51
6.4 Activité récente : 9–22 novembre 52
6.5 Décider pendant une courte perturbation 52

CHAPITRE 06

Hacktivisme, perturbations et systèmes opérationnels

EN BREF

Les sources publiques justifient la préparation aux perturbations de sites et aux conséquences opérationnelles. Le CCB n'a rapporté aucun DDoS hacktiviste au premier trimestre, puis un retour limité au deuxième. Les incidents frigorifiques de novembre posent un autre problème de continuité. Déclarations d'acteurs et explications politiques n'établissent pas l'impact technique. Préparez communication de situation, solutions de service alternatives et accès distant contrôlé avant la prochaine perturbation.

6.1 Chronologie

13 janv. 2026	**Déclaration hospitalière citée dans la presse** Arrêt préventif des systèmes et soins interrompus [S10]
22 avr. 2026	**Rapport trimestriel du CCB** Aucun DDoS hacktiviste rapporté au premier trimestre [S7]
15 juill. 2026	**Rapport trimestriel du CCB** Retour limité du DDoS sur une journée au deuxième trimestre [S8]
11 sept. 2026	**Avis d'incident communal** Interruption numérique, puis confirmation ultérieure de vol de données [S15]
28 oct. 2026	**Administration fiscale fédérale** Applications temporairement mises hors ligne après un incident [S23]
2 nov. 2026	**Reportages frigorifiques commerciaux** Perturbations d'équipements rapportées en Belgique [S25][S27]
9 nov. 2026	**Évaluation des identités du CCB** La protection des comptes reste prioritaire [S5]
10 nov. 2026	**Institut de recherche médicale** Mise à jour de la déclaration, sans nouvelle intrusion établie [S49]
12 nov. 2026	**Administration fiscale fédérale** Mise à jour sur le rétablissement d'e604 [S23]
13 nov. 2026	**Reuters** Évaluations ministérielles divergentes sur l'attribution frigorifique [S26]
17 nov. 2026	**Safeonweb** Alerte sur les fausses offres de pellets et de bois de chauffage [S45]
18 nov. 2026	**Service de comptes de recharge**

Utilisateurs informés après détection et correction ; nombre belge concerné indisponible [S46]

20 nov. 2026 **Safeonweb**
L'avertissement chèques-cadeaux relaie une enquête en cours [S29]

Une ligne officielle indique la source du récit. Elle ne signifie pas que cette source a vérifié indépendamment chaque déclaration d'attaquant citée. Une ligne de relais désigne un reportage plutôt qu'une publication originale d'acteur.

6.2 Revendication et récit public

Point	Revendication ou interprétation	Récit officiel	Évaluation
Disponibilité web	Un acteur peut annoncer un site indisponible	Les rapports du CCB décrivent leur population d'incidents observée [S7][S8]	Une capture ou publication n'établit ni durée ni impact national
Arrêt fiscal	L'indisponibilité peut être présentée comme un accès réussi	L'autorité dit avoir isolé les applications, sans exfiltration ni contrôle applicatif constaté [S23]	Attribuez les conclusions à son enquête
Responsabilité frigorifique	Un État peut être nommé dans le commentaire politique	Reuters rapporte des évaluations ministérielles divergentes et une enquête en cours [S26]	L'attribution reste non résolue dans ce rapport
Échelle frigorifique	Équipements, magasins et clients figurent dans des récits différents	Les avis officiels décrivent le risque opérationnel [S25] [S27]	Ne combinez pas des dénominateurs incompatibles

6.3 Un incident de site n'est pas un incident d'équipement

Un site peut être indisponible tandis que les activités internes continuent. Une interface opérationnelle peut modifier un équipement alors que le site de l'entreprise reste accessible. Leurs traces, responsables et décisions de reprise diffèrent.

Pour les sites publics, convenez des demandes de protection du trafic et de l'accès maintenu pour les utilisateurs légitimes. Conservez mesures de disponibilité et fuseau horaire. N'inférez pas un accès aux données d'une revendication de déni de service.

Pour les équipements frigorifiques, supprimez immédiatement l'accès internet public direct aux interfaces de gestion. Opérations et sécurité doivent coordonner continuité sûre et maintenance distante protégée. Vérifiez que les interfaces de gestion ne sont plus directement accessibles. [S25]

Pour les équipements opérationnels, impliquez les responsables des réglages sûrs. Testez le retrait du canal distant fournisseur. Vérifiez que la récupération locale reste sûre et que les accès d'urgence sont consignés.

Le cas frigorifique n'établit pas une exposition identique pour tous les appareils ménagers connectés. Les conseils de Safeonweb distinguent protection générale des appareils et incidents commerciaux précis. [S27]

6.4 Activité récente : 9–22 novembre

La fenêtre récente est une période d'observation, sans prévision. Le rapport CCB du 9 novembre sur les identités décrit des priorités actuelles à partir de populations antérieures. Sa date de publication ne déplace pas ces incidents en novembre. [S5]

Le 12 novembre, l'avis fiscal consignait une autre application restaurée après l'incident d'octobre. Le 13 novembre, Reuters rapportait l'incertitude d'attribution frigorifique. Aucun de ces éléments ne compte comme nouvelle attaque indépendante. [S23][S26]

L'avertissement Safeonweb du 20 novembre ajoute un risque de données clients pour les chèques-cadeaux. Il décrit une divulgation possible et une enquête en cours, sans décompte belge. Utilisez-le pour déclencher une communication ciblée. [S29]

Les éléments clandestins récents sont évalués séparément au chapitre 4. Une nouvelle annonce peut concerner d'anciennes données ou promouvoir un outil dont l'utilisation n'est pas établie. La date mesure l'annonce, sans dater l'incident sous-jacent. [S3]

6.5 Décider pendant une courte perturbation

Définissez les informations minimales pour protéger le trafic, isoler une intégration fournisseur ou activer un processus manuel. Attendre l'attribution peut prolonger la perturbation sans améliorer le confinement initial.

Utilisez un canal public de suivi unique avec heures explicites. Indiquez les services disponibles, les indisponibilités et les actions utilisateurs. Décrivez les accès aux données uniquement si les preuves les étayent.

Préservez la distinction entre précaution et constat. Une organisation peut isoler un système parce qu'elle n'exclut pas encore un risque. Cela ne signifie pas que tous les systèmes connectés ont été touchés.

POINTS À RETENIR

01

Mesurez la disponibilité séparément des revendications criminelles.

02

Les équipes opérationnelles doivent porter la reprise sûre des équipements.

03

Une publication récente ne transforme pas un ancien incident en nouvelle attaque.

CHAPITRE 07

Acteurs de la menace et liens entre les preuves

07

CE CHAPITRE RÉPOND À LA QUESTION

Quels noms d'acteurs sont observés et quel lien chaque élément étaye-t-il réellement ?

22

noms de groupes de rançongiciels dans les publications belges conservées

7.1 Comment les preuves se relient 54

7.2 Extorsion : des publications réparties entre plusieurs groupes 55

7.3 Pseudonymes publicitaires 59

7.4 Espionnage et récits d'intrusion non résolus 59

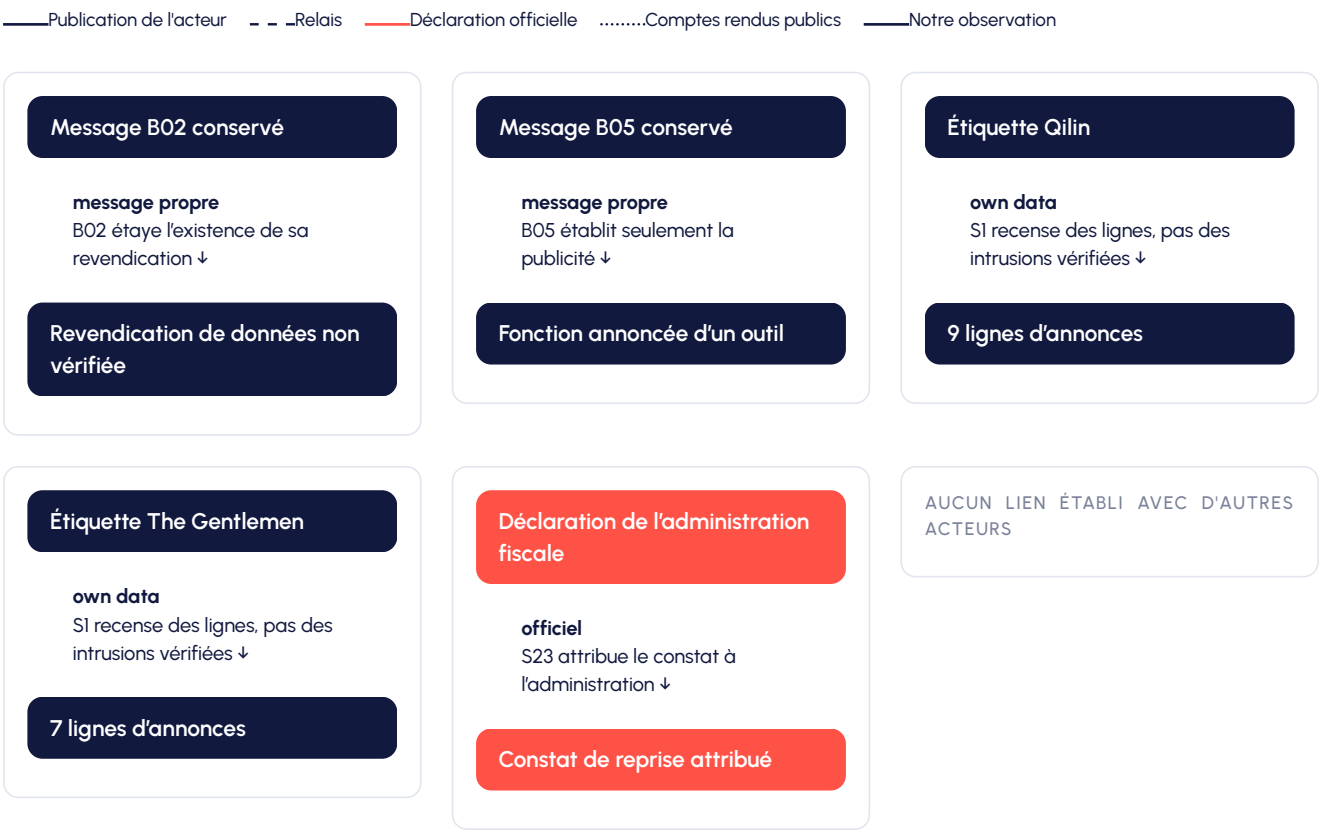
CHAPITRE 07

Acteurs de la menace et liens entre les preuves

EN BREF

Les preuves comprennent noms d'extorsion, pseudonymes publicitaires et campagnes décrites par les autorités. Ce sont des identités de nature différente. Secteur, langue ou thème politique commun ne relient pas les opérateurs. La carte associe une preuve à une proposition sans unir des groupes sans lien. Fondez la réponse sur l'accès validé, l'impact du service et la reprise. Utilisez l'attribution lorsqu'elle améliore ces décisions.

7.1 Comment les preuves se relient



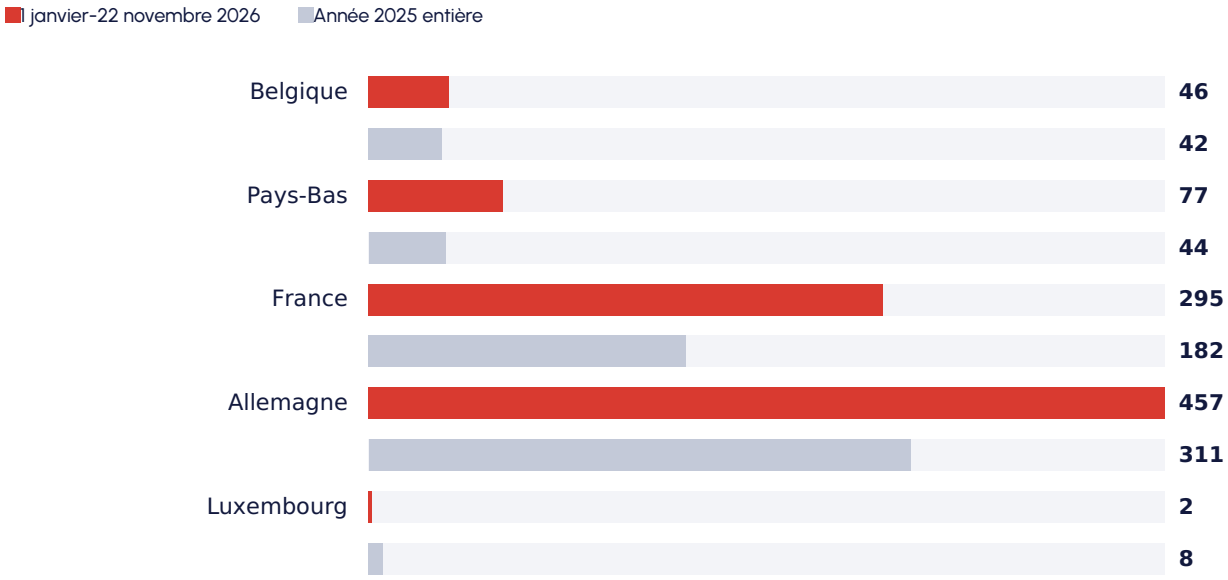
La carte montre une annonce conservée soutenant sa propre revendication, une publication soutenant une assertion d'extorsion et des sources publiques étayant un résultat déclaré. Elle ne déduit pas d'opérateur commun entre ces populations.

Des titres identiques peuvent établir des publicités similaires. Un pseudonyme répété peut établir l'usage de cette identité. Aucun ne prouve fichiers identiques, transfert réalisé ou personne derrière le compte. Aucune organisation criminelle commune n'en est déduite. [S3]

Le lien entre identifiants réutilisés, abus de comptes et fraude constitue un modèle analytique d'un mécanisme possible. La police décrit ce mécanisme dans certaines enquêtes. Cela ne signifie pas que les vendeurs du rapport ont fourni ces campagnes. [S31][S32]

7.2 Extorsion : des publications réparties entre plusieurs groupes

La Belgique compte 46 publications dans la période annuelle partielle, avec des totaux différents chez quatre voisins



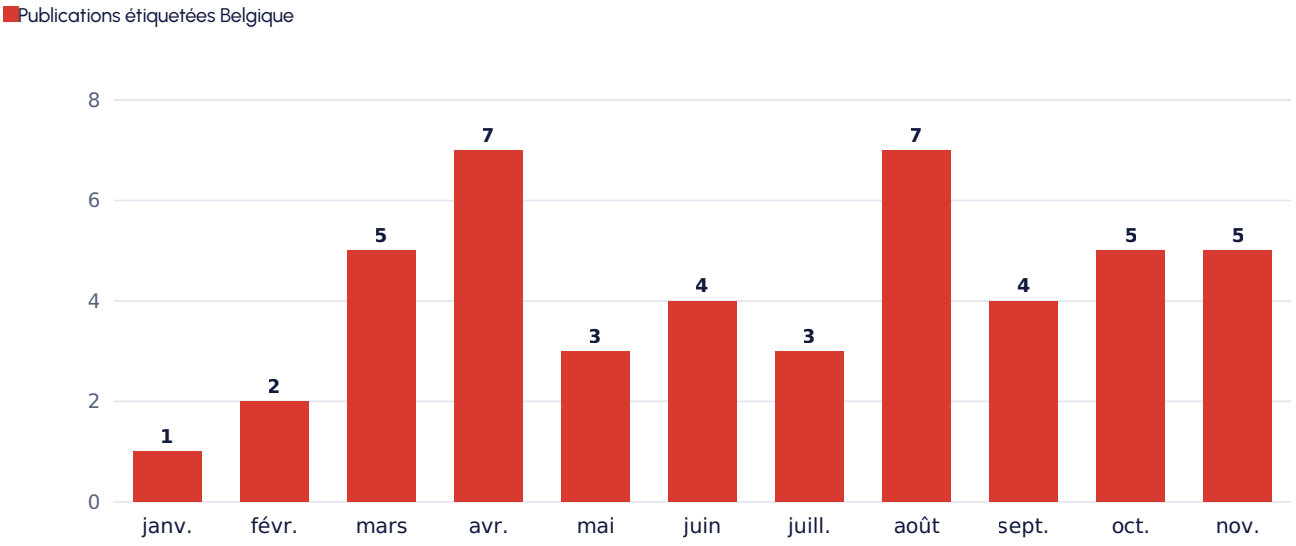
Périodes inégales ; pas de classement national des risques. Source : publications Ransompedia acceptées avec étiquette de pays, 1 janvier-22 novembre 2026 ; novembre partiel. Les dates de publication ne sont pas des dates d'incident [S1].

Les pays de comparaison ont été choisis à titre d'exemples uniquement pour apporter du contexte ; leur sélection n'implique ni classement ni appréciation politique.

Pays	Période 2026	Année 2025	Limite de comparaison
Belgique	46	42	Publications, sans intrusions confirmées
Pays-Bas	77	44	Marché logistique voisin et néerlandophone
France	295	182	Marché voisin francophone et d'entreprises
Allemagne	457	311	Économie industrielle et commerciale voisine
Luxembourg	2	8	Marché financier voisin avec peu de publications

Tous les chiffres 2026 couvrent la même période. Ils ne sont pas ajustés selon le nombre d'entreprises, la taille économique, la propension au signalement ou la visibilité des sources. Le tableau ne classe pas la sécurité ou l'exposition comparative d'une organisation belge. [S1]

Les publications belges se répartissent sur l'année plutôt que sur un seul mois

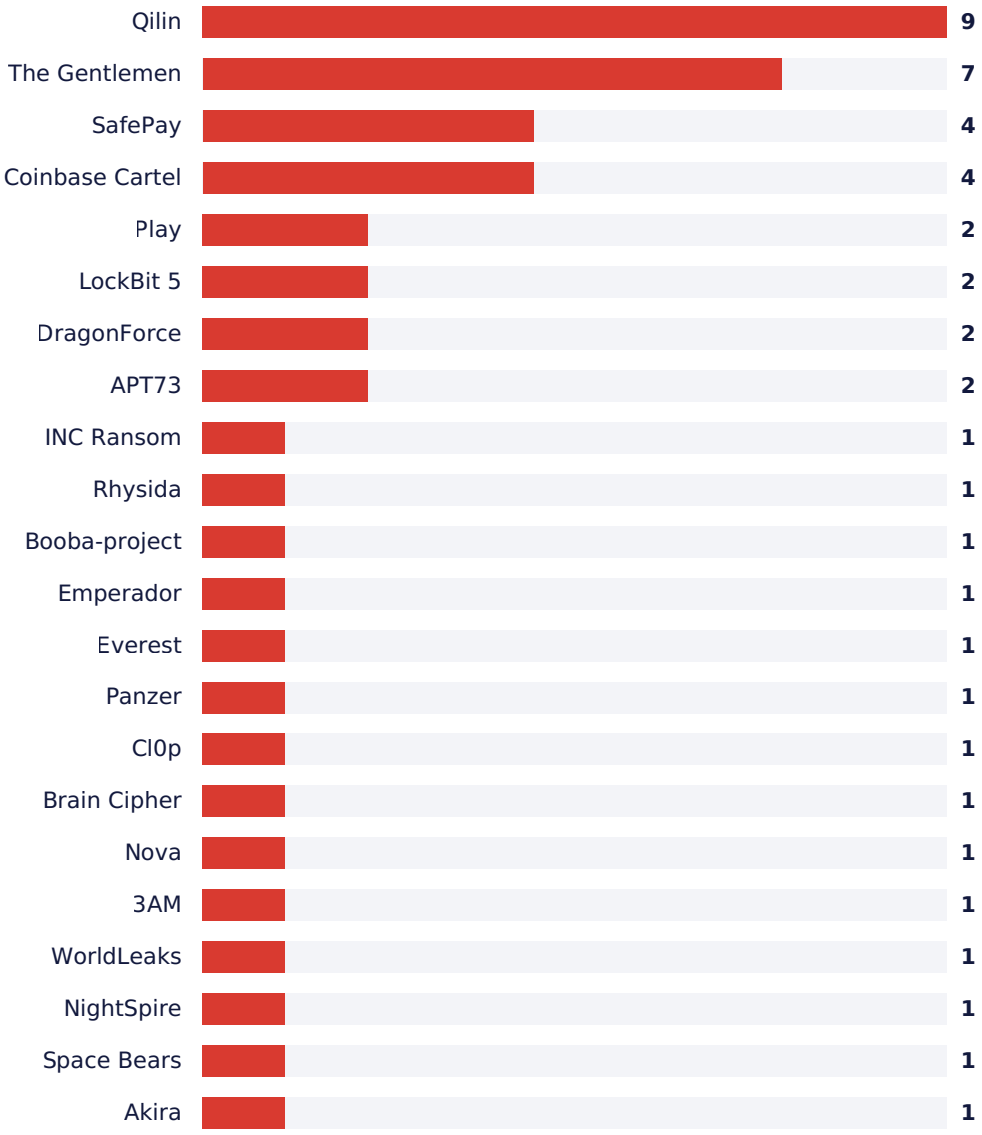


Source : publications Ransompedia acceptées avec étiquette de pays, 1 janvier-22 novembre 2026 ; novembre partiel. Les dates de publication ne sont pas des dates d'incident [S1].

Les décomptes mensuels sont 1, 2, 5, 7, 3, 4, 3, 7, 4, 5 et 5 de janvier à la coupure de novembre. Leur somme est 46. novembre partiel ne doit pas être comparé à un mois complet pour prévoir une tendance. [S1]

Quatre noms de groupes représentent 24 des 46 publications belges





Source : publications Ransompedia acceptées avec étiquette de pays, 1 janvier-22 novembre 2026 ; novembre partiel. Les dates de publication ne sont pas des dates d'incident [S1].

Qilin compte 9 publications, The Gentlemen 7, SafePay 4 et Coinbase Cartel 4. Ensemble, ils représentent 24 publications sur 46. Les 22 restantes sont réparties sous 18 autres noms. [S1]

Qilin

Étiquette d'annonces d'extorsion | Aucune attribution étatique

EN BELGIQUE, 2026

2026

9 · Annonces associées à la Belgique pendant la période ; pas des intrusions confirmées

CIBLES REVENDIQUÉES

Les étiquettes de secteur et de pays doivent être vérifiées ; aucune liste de victimes publiée

VU DANS LES SOURCES PUBLIQUES

[S1] Agrégat d'annonces conservées, sans attribution indépendante

NOTRE ÉVALUATION

Préparer la reprise et vérifier toute revendication sans se fier à l'étiquette de l'acteur

DEGRÉ DE CONFIANCE

Confiance élevée dans le nombre de lignes conservées ; résultats des intrusions non vérifiés

The Gentlemen

Étiquette d'annonces d'extorsion | Aucune attribution étatique

EN BELGIQUE, 2026

2026

7 · Annonces associées à la Belgique pendant la période ; pas des intrusions confirmées

CIBLES REVENDIQUÉES

Les étiquettes de secteur et de pays doivent être vérifiées ; aucune liste de victimes publiée

VU DANS LES SOURCES PUBLIQUES

[S1] Agrégat d'annonces conservées, sans attribution indépendante

NOTRE ÉVALUATION

Préparer la reprise et vérifier toute revendication sans se fier à l'étiquette de l'acteur

DEGRÉ DE CONFIANCE

Confiance élevée dans le nombre de lignes conservées ; résultats des intrusions non vérifiés

L'étiquette nationale reste un attribut de publication, sans preuve de juridiction nationale. La population comprend des descriptions de marques répétées et une unité d'exploitation étrangère. Les chevauchements organisationnels possibles restent des lignes distinctes ; aucun total de victimes uniques n'est affirmé. [S1]

7.3 Pseudonymes publicitaires

Pseudonyme	Cartes	Proposition observée	Limite
kazutlg	B01	Annonce de données clients télécoms	L'annonceur date lui-même l'incident de 2025
xmlrpc	B02	Revendication de données citoyennes avec incertitude reconnue sur la source	Provenance gouvernementale non vérifiée
yneov18	B03	Revendications de données et d'accès de formation	Accès actuel et personnes uniques non vérifiés
DataJava	B04	Administration revendiquée d'un service d'identité	Des descriptions de tableaux proposés ne valident pas l'accès
0xcasper	B05	Publicité de panneaux d'hameçonnage bancaire	Fonctionnement et déploiement non vérifiés
updap	B06	Revendication de tickets d'assistance fournisseur	Impact clients et possession complète non vérifiés

Ce sont des pseudonymes de comptes conservés. Ils n'identifient pas des personnes et n'authentifient pas une annonce. Un pseudonyme lié à un élément exact ne validerait pas chaque revendication ultérieure. [S3]

7.4 Espionnage et récits d'intrusion non résolus

Le CCB traite l'espionnage soutenu par des États dans le contexte des menaces. Un incident rapporté dans une agence publique sensible n'est pas confirmé indépendamment dans les sources officielles conservées. Le rapport retient donc un rôle général et attribue le récit à la presse. [S8][S9][S14]

Le rapport du troisième trimestre du CCB décrit des activités isolées qu'il rattache à la Russie, à la Chine et à l'Iran. Il signale aussi une campagne de spear-phishing sur Teams observée en Belgique. Il s'agit des appréciations de l'autorité. [S9]

Les documents publics de l'éditeur et de NVD sur deux vulnérabilités de gestion mobile établissent un risque produit. Ils n'établissent pas quelle vulnérabilité, quel acteur ou quel effet sur les données concerne l'incident belge rapporté. [S41][S42][S43]

Référence	Périmètre affecté	Versions corrigées de l'éditeur	Limite
CVE-2026-1281	NVD cite les versions jusqu'à 12.5.0.0 et certaines versions ultérieures vulnérables, dont 12.5.1.0, 12.6.0.0, 12.6.1.0 et 12.7.0.0	Voir le registre des versions ci-dessous	Vérifiez la branche du produit et les consignes actuelles de l'éditeur
CVE-2026-1340	NVD cite les versions EPMM affectées jusqu'à 12.7.0.0	Voir le registre des versions ci-dessous	Aucune conclusion sur un déploiement belge individuel

Versions corrigées d'Ivanti EPMM indiquées par le fournisseur [S41] :

`12.6.1.1, 12.7.0.1, 12.8.0.1`

L'avis Ivanti décrit deux risques d'injection de code sans authentification. Les exclusions comprennent Sentry et son produit cloud de gestion mobile. La correction doit correspondre au produit et à la branche installés. Les deux fiches NVD ont été vérifiées pour ce rapport. [S41][S42][S43]

Aucune matrice ATT&CK propre à l'incident n'est fournie pour le récit d'agence non confirmé. Une correspondance technique générique risquerait de transformer une capacité produit en séquence d'attaque observée en Belgique.

POINTS À RETENIR

01

Noms de groupes et pseudonymes ne sont pas des identités d'opérateurs vérifiées.

02

Les totaux régionaux ne mesurent pas une probabilité d'attaque comparative.

03

Les vulnérabilités produit n'attribuent pas indépendamment un incident belge rapporté.

CHAPITRE 08

L'économie de la fraude

08

CE CHAPITRE RÉPOND À LA QUESTION

Comment données, documents et accès annoncés pourraient-ils soutenir la fraude, et où l'interrompre ?

2

cas de campagnes policières avec enseignements concrets

8.1 Des détails exacts peuvent soutenir une fausse instruction 62

8.2 Fiches des campagnes policières 62

8.3 Images d'identité, sessions et ouverture de comptes 64

8.4 Cartes de paiement dans les publications : une vue limitée 64

8.5 Les prix affichés sont des prix demandés 64

8.6 Avertissements publics au fil de l'année 65

CHAPITRE 08

L'économie de la fraude

EN BREF

Les annonces conservées proposent identifiants, images d'identité, sessions et outils bancaires. Police et Safeonweb décrivent usurpation, factures modifiées et applications malveillantes. Ces campagnes publiques ne sont pas attribuées aux pseudonymes des forums. Les observations de cartes de paiement restent très limitées. Protégez récupération, modifications de paiement et communication clients par une vérification indépendante et une voie claire pour les signalements urgents.

8.1 Des détails exacts peuvent soutenir une fausse instruction

De vraies informations personnelles rendent un message frauduleux crédible, sans authentifier l'expéditeur. Les cas de formation, d'adhésion et de fournisseurs expliquent l'utilité des contrôles de l'assistance et de la finance, même lorsque les mots de passe sont déclarés intacts. [S13][S18][S22]

L'avertissement policier de mai décrit des criminels utilisant d'anciens identifiants divulgués, surveillant les messages et modifiant les factures. Il décrit une automatisation croissante du schéma observé. Ce rapport ne mesure pas indépendamment la part de l'IA dans cette activité. [S31]

Le contrôle décisif est la vérification indépendante de l'instruction. Utilisez un contact déjà connu avant d'accepter un changement de bénéficiaire ou un virement urgent. Une messagerie familière, un montant exact ou le nom correct du client ne suffisent pas.

8.2 Fiches des campagnes policières

P

CAS P

Une enquête vise un fournisseur de panneaux d'hameçonnage

Récit public attribué

Services de fraude

RÉCIT OFFICIEL	La Police fédérale a annoncé le 22 avril une enquête sur un suspect présumé concevoir et vendre des panneaux d'hameçonnage. Elle décrit leur utilisation frauduleuse en Belgique et ailleurs en Europe. [S30]
CHRONOLOGIE	La police décrit une perquisition en janvier et une remise du suspect à la Belgique en avril. Ces dates de procédure diffèrent de l'annonce.

ÉTABLI	La déclaration étaye un service criminel : un fournisseur propose des outils utilisables par d'autres. Elle ne relie pas ce suspect à B05 ou aux pseudonymes des forums conservés.
LIMITES	Une arrestation et des allégations policières ne sont pas une condamnation. N'en déduisez pas un total national de victimes ou de pertes.
RÉPONSE	Intégrez authentification résistante à l'hameçonnage et vérification des paiements dans le même exercice. Consignez comment un utilisateur signale une interaction d'authentification interceptée.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

CAS Q

Q De faux employés bancaires combinent messages, appels et accès distant

Récit public attribué

Usurpation bancaire

RÉCIT OFFICIEL	Une déclaration policière du 2 juillet décrit des dizaines de victimes belges et des gains présumés supérieurs à EUR 500 000. L'enquête se poursuivait. [S32]
CHRONOLOGIE	La police situe le début de l'enquête en mars et l'arrestation d'un suspect principal au 29 juin. La publication de juillet ne date pas le début de toutes les infractions.
MÉCANISME	Le récit officiel décrit des messages usurpant des organismes publics, un appel de faux employé bancaire, puis une incitation à installer un logiciel de contrôle distant.
LIMITES	Les gains sont présumés, sans estimation nationale des pertes frauduleuses. Aucun opérateur commun avec les annonces clandestines du rapport n'est établi.
RÉPONSE	Conseillez aux clients de terminer les appels inattendus et de contacter leur banque indépendamment. Préparez une escalade urgente pour les risques d'accès distant et de nouveau bénéficiaire.

En définitive

Respecter le périmètre indiqué et conserver les questions non résolues.

8.3 Images d'identité, sessions et ouverture de comptes

La demande B08 recherche plus de 500 images d'identité belges. Elle établit uniquement une demande. Elle ne prouve ni réponse d'un fournisseur, ni vérification d'identité réussie, ni vol dans un registre public. [S3]

La demande B09 recherche des sessions actives de services logistiques. Une session peut nécessiter une réponse différente d'un simple mot de passe. Examinez sessions et récupération lorsque l'organisation a validé un constat pertinent. [S3]

Ne faites pas de la possession d'un document une preuve d'identité unique. Testez les abus possibles d'une vraie image, de coordonnées ou d'un ancien identifiant lors de l'ouverture ou de la récupération. Prévoyez une escalade pour les cas incertains.

8.4 Cartes de paiement dans les publications : une vue limitée

PORTÉE DES CHIFFRES DES FICHES

Ces observations limitées n'estiment ni le vol total de cartes, ni les cartes actives, ni les intrusions dans les systèmes bancaires, ni les pertes frauduleuses.

Les éléments conservés associent 3 numéros de carte distincts à la Belgique, dans 9 publications et 17 apparitions. Aucun émetteur belge nommé n'est établi pour ces trois cartes. Les répétitions ne sont pas des cartes supplémentaires. [S3]

Ces observations n'établissent ni carte toujours active ni paiement tenté avec succès. Les émetteurs doivent utiliser leurs propres preuves avant blocage ou remplacement. Cette population ne doit pas être ajoutée aux identifiants ou aux enregistrements clients.

8.5 Les prix affichés sont des prix demandés

Produit annoncé	Prix affiché	Limite des preuves
Identifiants de comptes bancaires	USD 1,75 pour 1000 ; USD 70,19 pour l'ensemble annoncé	Quantité, provenance et autorité de paiement non vérifiées
Administration revendiquée d'un service d'identité	USD 4 550	Accès fonctionnel et population annoncée non vérifiés
Sessions liées à la logistique	USD 250–2 500	Fourchette d'achat, sans transaction réalisée

Les prix décrivent les annonces conservées. Ils n'établissent ni prix de transaction, ni revenu, ni rentabilité, ni taille d'un marché clandestin belge. Les périmètres revendiqués diffèrent et empêchent une comparaison simple. [S3]

8.6 Avertissements publics au fil de l'année

Période	Avertissement officiel	Décision justifiée
janvier	Usurpation d'invitations et parrainages de personnalités [S65]	Vérifier les demandes auprès d'un contact professionnel établi
février	Usurpation de connexion à un service public [S62]	Ouvrir directement le service officiel
mars	Faux messages d'indemnisation et de récupération [S63]	Ne pas envoyer de documents à un interlocuteur de récupération non vérifié
juin	Messages hôteliers contenant des réservations exactes [S61]	Vérifier indépendamment le paiement auprès de l'hébergement
septembre	Usurpation de dirigeants sur un logiciel collaboratif [S60]	Vérifier l'identité organisationnelle, même familière
septembre	Application malveillante et relais mobile de carte [S59]	Refuser l'installation non sollicitée et contacter séparément la banque
octobre	Liaison de compte de messagerie par faux votes [S64]	Vérifier les demandes inattendues, même issues d'un contact connu
novembre	Faux vendeurs de combustibles et offres à paiement anticipé [S45]	Vérifier vendeur et modalités de paiement avant commande

Ces avis concernent la prévention et des campagnes. Ils ne forment pas huit populations de victimes disjointes. L'avertissement hôtelier n'établit pas que l'incident précédent de réservation a fourni les données utilisées dans ces messages. [S61]

POINTS À RETENIR

01

Des informations personnelles exactes n'authentifient pas une demande de paiement.

02

Une annonce d'outil diffère d'une campagne de fraude observée.

03

Apparitions de cartes et prix demandés ne mesurent ni pertes ni transactions réalisées.

CHAPITRE 09

Analyse du secteur bancaire et financier

09

CE CHAPITRE RÉPOND À LA QUESTION

Quels signaux d'identité et de protection des clients faut-il vérifier en priorité ?

11 sur 25

domaines sélectionnés de banque et finance avaient une annonce actuelle d'identifiant

9.1 Ce que les preuves disent et ne disent pas 67

9.2 Distinguer compte, session et décision de paiement 67

9.3 Fournisseurs et coordination réglementaire 68

CHAPITRE 09

Analyse du secteur bancaire et financier

EN BREF

11 des 25 domaines sélectionnés de banque et finance avaient une annonce actuelle d'identifiant. Le secteur contient au moins 13 221 associations d'appareils, dont 156 classées salariés, et 190 956 identifiants enregistrés. Les trois cartes observées dans les publications n'ont pas d'émetteur nommé attribué. Ces observations mesurent des populations différentes. Coordonnez identité, fraude et assistance autour de comptes, sessions et paiements vérifiés.

9.1 Ce que les preuves disent et ne disent pas

Population	Résultat disponible	Interprétation
Domaines sélectionnés de banque et finance	25	Inclut des services financiers ; aucun recensement des émetteurs de cartes agréés
Associations d'appareils	Au moins 13 221 ; 156 classées salariés	Le classement ne prouve ni propriété ni intrusion d'entreprise
Identifiants enregistrés	190 956	Sources historiques qui se chevauchent, sans comptes actifs uniques
Annonces actuelles d'identifiants	11 domaines sur 25	Vérifier actualité, validité et corrections antérieures
Sous-ensemble de domaines d'émetteurs	7 domaines correspondants ; 6 avec annonces actuelles	86 associations d'appareils salariés et 4 306 non salariés ; sous-ensemble sectoriel
Annonces de modèles bancaires	Observées dans B05	Revendication de produit d'usurpation, sans intrusion bancaire établie
Éléments de cartes	3 cartes ; 9 publications ; 17 apparitions	Sans attribution à un émetteur nommé ni estimation de pertes ou d'intrusions

Aucune carte conservée n'a été attribuée à un émetteur nommé. Cela ne prouve pas l'absence de cartes volées. Les associations non salariées ne prouvent pas une propriété cliente. [S2][S3]

9.2 Distinguer compte, session et décision de paiement

Un identifiant exposé peut personnaliser un appel. Une session valide peut permettre une activité de compte. Une instruction de paiement ne déplace des fonds que dans le processus d'autorisation applicable. Examinez ces propositions séparément sans faire d'une preuve celle des trois.

Si l'équipe fraude reçoit un signalement de contrôle distant ou d'authentification inattendue, orientez-le rapidement vers la protection des comptes. Vérifiez bénéficiaires et modifications de récupération par un canal indépendant connu. Conservez décision et traces justificatives. [S32]

L'annonce B05 revendique des modèles bancaires et des fonctions d'authentification interactive. Elle ne prouve ni fonctionnement ni contournement des contrôles d'une banque. Elle peut servir à tester la réponse de l'équipe fraude à l'usurpation. [S3]

9.3 Fournisseurs et coordination réglementaire

DORA s'applique depuis 17 janvier 2025 à une large population d'entités financières. La NBB décrit la supervision des risques TIC et cyber, comprenant informations d'incidents, tests et dépendances tierces. [S38]

Pour chaque service bancaire essentiel, identifiez fournisseur d'identité, télécommunications, prestataire principal et dépendances de reprise. Un message général de restauration fournisseur ne prouve pas que votre propre service est sûr, complet et réconcilié.

Conservez une chronologie commune et des décisions distinctes pour signalement opérationnel, vie privée, information clients et fraude. L'existence d'un régime ne clôt pas automatiquement l'évaluation d'un autre. [S36] [S37][S38]

POINTS À RETENIR

01

Traitez les annonces actuelles par une vérification des comptes.

02

Examinez séparément identifiants, sessions et autorisation de paiement.

03

Distinguez sous-ensembles d'émetteurs, associations sectorielles et cartes des publications.

CHAPITRE 10

Réglementation et réponse nationale

10

CE CHAPITRE RÉPOND À LA QUESTION

Quelles obligations de signalement et étapes de supervision les dirigeants belges doivent-ils déjà avoir organisées ?

18 avril 2027

étape de conformité traitée dans la communication du CCB d'août

10.1 Les règles applicables aujourd'hui 70
10.2 Conformité NIS2 : preuves et corrections 71
10.3 Sanctions et exclusions exigent un périmètre précis 71
10.4 Une décision distincte pour les données personnelles 72
10.5 Coordination nationale des crises 72

CHAPITRE 10

Réglementation et réponse nationale

EN BREF

Les obligations NIS2 belges sont déjà en vigueur. L'étape documentaire d'avril 2026 et la communication de supervision d'août demandent une préparation concrète. Les incidents de données personnelles nécessitent une évaluation RGPD distincte. Les entités financières doivent déterminer le régime DORA applicable. Les fabricants ont des obligations de signalement CRA depuis septembre. Désignez un responsable par régime et exercez la première notification avant l'incident.

10.1 Les règles applicables aujourd'hui

Le tableau distingue déclencheur, délai et contexte de supervision. C'est une aide à la préparation, sans conseil juridique. L'autorité compétente et le périmètre dépendent de l'entité, de l'activité et de l'incident. [S33][S35][S36][S37][S38][S39]

Régime	Champ d'application	Délai	Canal responsable
Loi NIS2 belge	Entités essentielles et importantes concernées ; incidents significatifs touchant les services couverts	Sans retard injustifié après prise de connaissance d'un incident significatif : alerte précoce au plus tard sous 24 heures ; notification au plus tard sous 72 heures. Rapport final dans le mois suivant la notification, sauf incident en cours (voir ci-dessous)	CSIRT national au CCB ; exception de notification sous 24 heures pour les prestataires de services de confiance
RGPD	Responsables du traitement d'une violation de données, sauf risque peu probable pour les droits et libertés des personnes	Sans retard injustifié et, si possible, sous 72 heures après prise de connaissance	Autorité de protection des données compétente ; l'APD/GBA n'est pas compétente pour tous les secteurs
DORA	Entités financières dans le champ du règlement	Applicable depuis 17 janvier 2025 ; suivre le classement des incidents et le processus de déclaration appropriés	Superviseur financier et canal de déclaration applicables
Signalement CRA	Fabricants de produits comportant des éléments numériques et vulnérabilités ou incidents graves à signaler	Obligations depuis 11 septembre 2026. Après prise de connaissance d'une vulnérabilité activement exploitée ou d'un incident grave : alerte précoce sous 24 heures et notification sous 72 heures	Plateforme européenne unique de signalement, CSIRT compétent et ENISA

Si l'incident est toujours en cours à l'échéance d'un mois, fournissez alors un rapport d'avancement. Transmettez le rapport final dans le mois suivant le traitement définitif de l'incident. [S36]

Les délais des rapports finaux CRA diffèrent. Pour une vulnérabilité activement exploitée, le CCB décrit un délai de 14 jours après disponibilité d'une correction ou atténuation. Pour un incident grave, il indique un mois après notification. [S39]

N'appliquez pas le délai d'un régime à chaque incident. Informer un fournisseur, un assureur ou la police ne vaut pas automatiquement notification au régulateur compétent. Conservez l'heure de prise de connaissance et une décision distincte pour chaque obligation.

10.2 Conformité NIS2 : preuves et corrections

La loi du 26 avril 2024 est entrée en vigueur le 18 octobre 2024. La communication du CCB d'avril précisait les preuves attendues des entités essentielles pour le 18 avril 2026. Leur contenu dépendait de la voie de conformité choisie. [S33][S36]

Pour CyberFundamentals, le CCB décrivait une vérification ou une démarche active, comprenant un accord d'évaluation signé. Pour ISO/IEC 27001, il demandait périmètre, applicabilité et audit interne. L'inspection directe nécessitait une autoévaluation et des justificatifs. [S33]

La communication d'août concerne l'étape du 18 avril 2027. Les entités essentielles ne démontrant pas des mesures équivalentes au niveau Essential doivent fournir des preuves équivalentes à Important et un plan visant Essential pour le 18 avril 2028. [S34]

Aucun plan de remédiation n'est requis si, au 18 avril 2027, l'entité démontre des mesures équivalentes à Essential ou justifie un niveau équivalent inférieur par son analyse des risques. [S34]

Le CCB précise que cette approche ne modifie ni les obligations ni les délais légaux. Traitez-la comme une exigence de supervision imposant un parcours crédible documenté, sans prolongation générale. Consignez voie, périmètre, responsable des preuves et écarts non résolus. [S34]

10.3 Sanctions et exclusions exigent un périmètre précis

L'article 59 distingue plusieurs manquements à la loi NIS2 belge. Pour la gestion des risques et la notification, les fourchettes diffèrent selon les entités essentielles et importantes. D'autres manquements ont des fourchettes distinctes. [S36]

Disposition	Fourchette légale	Rappel du champ
Entités importantes	EUR 500 à EUR 7 000 000 ou 1,4% du chiffre d'affaires annuel mondial précédent de l'entreprise, selon le montant le plus élevé	Obligations concernées de gestion des risques ou de notification
Entités essentielles	EUR 500 à EUR 10 000 000 ou 2% du chiffre d'affaires annuel mondial précédent de l'entreprise, selon le montant le plus élevé	Obligations concernées de gestion des risques ou de notification
Récidive	L'amende administrative double pour les mêmes faits dans un délai de trois ans	Application soumise aux conditions légales de récidive
Secteur de l'administration publique	L'article 62 exclut ces entités des amendes et mesures administratives prévues aux articles 59–60	Évaluez séparément les obligations applicables de cybersécurité et de notification [S36]

Ces fourchettes légales ne prédisent pas une amende. La loi prévoit aussi des exclusions sectorielles et une articulation avec des règles européennes équivalentes. Les dispositions financières se lisent avec DORA ; une liste NIS2 générique ne suffit pas. [S36][S38]

10.4 Une décision distincte pour les données personnelles

L'APD/GBA oriente les responsables du traitement vers son portail. Ses instructions exigent une notification dans une langue nationale ; les annexes techniques peuvent être en anglais. Elle désigne d'autres autorités fédérales compétentes dans certains domaines, notamment l'information policière. [S37]

Préparez compte du portail et analyse de compétence avant l'incident. Consignez faits connus, incertitudes et prochaine mise à jour. L'absence d'un nombre final de victimes demande d'expliquer l'incertitude, sans reporter toutes les décisions de notification.

L'équipe incident doit fournir aux responsables vie privée une synthèse d'impact. Incluez catégories de données, traitements concernés, destinataires possibles, protections et preuves étayant chaque conclusion. Distinguez nombres revendiqués par des criminels et évaluation propre au responsable du traitement.

10.5 Coordination nationale des crises

Le CCB présente un cadre national révisé de crise cyber. Ses indications publiques précisent une application depuis le 7 mai 2026. Le plan coordonne les autorités sans remplacer leurs mandats ; son contenu opérationnel détaillé n'est pas public. [S40]

Chaque organisation doit néanmoins connaître sa chaîne de décision. Désignez qui peut isoler un service, demander une aide externe, activer les processus manuels et publier un état de situation. Testez ces décisions avec un fournisseur indisponible et une perte de données incertaine.

POINTS À RETENIR

01

Distinguez les décisions NIS2, vie privée, finance et signalement produit.

02

L'approche corrective du CCB n'efface pas les échéances légales.

03

Préparez accès de notification, responsables des preuves et décisions de crise avant l'alerte.

CHAPITRE 11

Perspectives

11

CE CHAPITRE RÉPOND À LA QUESTION

Quelles hypothèses de préparation sont étayées et quels signaux les modifieraient ?

3

scénarios conditionnels de continuité, d'identités et de réponse fournisseurs

11.1 Principaux jugements 75

11.2 Ce qui modifierait l'évaluation 75

11.3 Scénarios conditionnels 76

CHAPITRE 11

Perspectives

EN BREF

Les priorités les mieux étayées sont la protection des identités, l'assurance fournisseurs et la reprise des services. Les rapports officiels et les cas justifient ces priorités sans établir la probabilité d'un incident futur. Les publications d'extorsion restent réparties entre de nombreux noms de groupes. Les perturbations récentes renforcent l'urgence de maîtriser les accès distants. Testez les décisions avec ces scénarios, puis révisez-les lorsque vos propres preuves évoluent.

11.1 Principaux jugements

Jugement	Confiance	Fondement	Limite
La protection des comptes mérite une attention immédiate	Élevée pour la priorité	Évaluation du CCB et rapports policiers sur la fraude [S5][S31][S32]	Ne mesure pas l'exposition d'un employeur particulier
Une défaillance fournisseur peut devenir un problème de service local	Élevée pour le mécanisme	Cas pédagogiques, sanitaires et de signature [S8][S13] [S22]	Une dépendance commune ne signifie pas que chaque client est touché
La préparation à l'extorsion doit couvrir plusieurs noms d'acteurs	Élevée pour la répartition visible	46 publications sous 22 noms [S1]	Les publications n'établissent ni intrusions distinctes ni pertes
Les accès opérationnels distants méritent un examen	Élevée pour la priorité de contrôle	Perturbation frigorifique et conseils officiels [S25][S27]	N'établit pas la cause de chaque dysfonctionnement signalé

La confiance porte sur ces propositions. Elle ne certifie ni honnêteté d'un acteur, ni catalogue complet d'un vendeur, ni authenticité de chaque ligne d'un fichier.

11.2 Ce qui modifierait l'évaluation

Un compte privilégié actuel vérifié augmenterait l'urgence de la réponse identités. Un ancien identifiant inactif avec correction documentée la réduirait. Les preuves pertinentes concernent la validité du compte et l'activité récente, plutôt que le volume des annonces.

Un rapport fournisseur vérifié, propre au client, pourrait réduire ou élargir la population de données concernée. Une déclaration générale de reprise établirait la disponibilité, sans résoudre la confidentialité. Documentez ces deux états indépendamment.

Une enquête officielle ou des preuves techniques reproductibles pourraient modifier l'attribution frigorifique. La répétition d'allégations, les captures d'écran et le calendrier politique ne suffiraient pas seuls. Révisez le jugement lorsque la proposition elle-même reçoit de nouveaux appuis.

11.3 Scénarios conditionnels

Ces scénarios sont des hypothèses de préparation. Ils ne prévoient ni fréquence d'attaque, ni perte financière, ni auteur probable.

Scénario	Déclencheur	Première décision	Preuve d'achèvement
Une identité actuelle est utilisée abusivement	Compte actif et session suspecte vérifiés	Le responsable identités révoque les sessions et préserve les traces d'accès	Récupération confirmée par le titulaire ; accès et récupération examinés
Un fournisseur commun isole sa plateforme	Un avis correspond à une dépendance documentée	Le responsable du service active l'alternative testée et demande une analyse d'impact ciblée	Service manuel fonctionnel ; données et décisions de notification documentées
Un équipement distant se comporte anormalement	Les équipes opérationnelles valident une modification ou une perte de contrôle	Le responsable applique la procédure locale sûre et restreint l'accès distant	État sûr confirmé ; comptes distants et historique examinés

POINTS À RETENIR

01

Les scénarios testent des décisions ; ce ne sont pas des prévisions.

02

Adaptez l'urgence identités à la validité des comptes et à l'activité actuelle.

03

Modifiez l'attribution uniquement lorsque des preuves plus solides étayent la proposition.

CHAPITRE 12

Plan d'action

12

CE CHAPITRE RÉPOND À LA QUESTION

Qui agit en premier et quelles preuves montrent l'achèvement ?

30/60/90

jours pour valider les identités, exercer les dépendances et vérifier la reprise

12.1 Les premiers 30/60/90 jours 78

12.2 Responsabilités par rôle 80

12.3 Comment Brandefense peut aider 80

CHAPITRE 12

Plan d'action

EN BREF

Commencez par les faits vérifiables dans votre organisation : comptes actifs, services exposés, dépendances fournisseurs et capacité de restauration. Donnez à chaque action un responsable et une preuve de clôture. Associez vie privée, assistance clients, finance et opérations. L'objectif est un service capable de reprendre et une équipe capable d'expliquer les événements. Examinez l'avancement à partir des preuves ci-dessous lors de chaque réunion de direction.

12.1 Les premiers 30/60/90 jours

1Immédiat

Supprimez l'accès internet public direct aux interfaces de gestion frigorifique ; coordonnez continuité sûre et maintenance distante protégée

RESPONSABLE

Responsables opérations et sécurité avec les mainteneurs

PREUVE D'ACHÈVEMENT

Tests d'accessibilité confirmant l'absence d'accès public direct ; réglages sûrs et maintenance protégée vérifiés [S25]

230 jours

Si un identifiant ou une session actuels concernent votre service, vérifiez le compte, révoquez les sessions suspectes et examinez la récupération

RESPONSABLE

Responsables identités et SOC

PREUVE D'ACHÈVEMENT

Traitement du compte, analyse d'activité et dossier de récupération

Inventoriez la gestion distante accessible sur internet et les applications critiques ; privilégiez les corrections urgentes confirmées par l'éditeur

RESPONSABLE

Responsable infrastructure

PREUVE D'ACHÈVEMENT

Inventaire attribué, preuves des correctifs et exceptions documentées

Reliez les fournisseurs critiques aux données, accès administratifs et processus

RESPONSABLE

Achats et responsables de service

PREUVE D'ACHÈVEMENT

Registre des dépendances, contact incident et processus alternatif

Préparez un dossier de décision couvrant déclencheurs de notification et heures de prise de connaissance

RESPONSABLE

Juridique, vie privée et responsable incident

PREUVE D'ACHÈVEMENT

Accès aux canaux requis testé et suppléants désignés

360 jours

Exercez une panne fournisseur avec impact incertain sur les données clients

RESPONSABLE

Continuité et vie privée

PREUVE D'ACHÈVEMENT

Alternative fonctionnelle, projet d'avis utilisateurs et décisions réglementaires séparées

Testez la vérification des modifications de paiement par un canal déjà connu

RESPONSABLE

Finance et fraude

PREUVE D'ACHÈVEMENT

Échantillons de rappels consignés et traitement des divergences de bénéficiaire

Examinez comptes et chemins d'accès aux équipements distants avec les mainteneurs

RESPONSABLE

Responsable opérationnel

PREUVE D'ACHÈVEMENT

Liste approuvée, procédure locale sûre et preuve d'examen des changements

490 jours

Restaurez un service essentiel depuis des sauvegardes protégées sous contraintes réalistes de dépendance

RESPONSABLE

Responsable reprise

PREUVE D'ACHÈVEMENT

Résultat mesuré, validation des données et points d'exercice clos

Testez la détection des sessions suspectes, nouvelles méthodes d'authentification et transferts de courriels non autorisés

RESPONSABLE

SOC et identités

PREUVE D'ACHÈVEMENT

Alertes examinées, responsable désigné et preuves d'exercice conservées

Présentez à la direction voie de conformité, écarts fournisseurs et résultats d'exercices

RESPONSABLE

CISO

PREUVE D'ACHÈVEMENT

Décisions signées, corrections financées et dates des points ouverts

Ces horizons sont des objectifs internes de préparation. Ils ne remplacent ni délais légaux de signalement, ni confinement urgent, ni réponse immédiate à un incident actif.

12.2 Responsabilités par rôle

Direction de la sécurité. Demandez des preuves de reprise et de maîtrise des identités, plutôt qu'une liste d'outils achetés. Clarifiez les responsabilités lorsqu'application, fournisseur et service traversent plusieurs équipes. Datez l'expiration des risques résiduels acceptés.

SOC et réponse aux incidents. Commencez par le compte, le service touché et le type de preuve. Conservez notification originale et chronologie claire. Distinguez annonce suspecte, identité valide et session observée avant de décrire un résultat.

Informatique et infrastructure. Vérifiez que les mises à jour urgentes ont atteint le système réellement exposé. Une tâche de déploiement réussie ne prouve pas la couverture de chaque équipement, environnement intégré ou serveur secondaire. Séparez accès de reprise et administration courante.

Vie privée et communication. Rédigez des avis courts indiquant faits connus, incertitudes et actions demandées aux utilisateurs. Préparez ensemble versions française et néerlandaise lorsque nécessaire. Utilisez un canal officiel stable pour les mises à jour.

Finance et protection des clients. Vérifiez indépendamment les nouvelles instructions de paiement. Formez l'assistance aux appelants citant de vraies informations personnelles. Des détails clients exacts rendent la fraude crédible, sans authentifier l'appelant.

Opérations et fournisseurs. Définissez un mode local sûr avant de restreindre l'accès distant. Convenez de qui peut modifier les réglages, autoriser un accès d'urgence et confirmer la reprise. Réexaminez les accès après changement de personnel ou de contrat.

12.3 Comment Brandefense peut aider

Brandefense fournit du renseignement externe sur les menaces et une surveillance des risques numériques. Le service peut soutenir l'examen d'identifiants exposés, de fuites et d'usurpations de marque. Une alerte doit rejoindre le processus de validation et de réponse décrit ici. [S44]

Apportez à une démonstration Brandefense les domaines, marques et services que vous êtes autorisés à évaluer. Demandez comment un constat atteint son responsable, comment l'incertitude est représentée et quelle preuve clôt le cas. [S44]

POINTS À RETENIR

01

Donnez à chaque action un responsable et une preuve d'achèvement vérifiable.

02

Testez la reprise avec les dépendances fournisseurs et identités indisponibles.

03

Distinguez objectifs internes, réponse immédiate et obligations de notification.

ANNEXES

Annexes

A–D

CE CHAPITRE RÉPOND À LA QUESTION

Comment interpréter les preuves sans confondre leurs populations ?

4

types de preuve : observation, revendication, corroboration publique et évaluation

Annexe A. Méthode et limites 83

Annexe B. Registre des preuves 86

Annexe C. Sources 87

Annexe D. Glossaire 90

Annexe A. Méthode et limites

Les pays de comparaison ont été choisis à titre d'exemples uniquement pour apporter du contexte ; leur sélection n'implique ni classement ni appréciation politique.

A.1 Période et sens des dates

Le rapport couvre la période du 1 janvier au 22 novembre 2026. Les observations clandestines utilisent les dates de publication, sans présumer la date d'intrusion. Les observations d'exposition datent du 21 novembre ; les observations de forums et contrôles passifs datent du 22 novembre. La coupure du jour reflète les informations disponibles lors de la capture, sans couvrir les heures suivantes.

L'activité récente est indiquée comme 9–22 novembre. Un rapport officiel publié alors peut décrire des événements antérieurs. Une restauration, une republication ou l'annonce nouvelle d'un fichier historique ne sont pas par défaut de nouvelles intrusions.

A.2 Populations de preuves

Population	Unité	Limite de couverture
Éléments clandestins conservés	Publication distincte	1025 publications de forums conservées ; nombres étiquetés présentés séparément
Sous-ensemble national des forums	Publication	480, comprises dans la population conservée
Éléments de rançongiciels	Ligne de publication acceptée	46 lignes étiquetées belges ; prudence sur pays et entités
Inventaire des domaines	Domaine principal candidat	250 sélectionnés ; 245 répondant au DNS
Incidents et campagnes publics	Dossier de preuves	Déclarations, avis officiels et récits attribués ; sans recensement national
Cartes de paiement	Carte distincte et apparitions	3 cartes, 17 apparitions, 9 publications ; sans émetteur nommé

Les fichiers graphiques publics contiennent des agrégats. Les cartes conservent de courts extraits expurgés, sans échantillons personnels, identifiants de victimes ou contacts criminels. Un pseudonyme désigne un personnage de forum, sans personne vérifiée.

A.3 Observations des domaines sélectionnés

Les domaines couvrent services publics et grands rôles économiques. Cet ensemble raisonné n'établit pas un classement des plus grandes organisations indépendantes belges. Les réponses DNS ne valident ni propriété juridique, ni indépendance organisationnelle, ni performance de sécurité.

Les observations passives de messagerie et du web concernent les domaines à la date évaluée. Les observations manquantes ou échouées restent distinctes des constats de configuration établis.

Atlas couvre les 250 domaines sélectionnés. La valeur nationale est de 48 sur 100. Les observations d'appareils, identifiants, documents et annonces actuelles datent du 21 novembre 2026. Ces enregistrements cumulés ne concernent pas exclusivement des événements de 2026.

Les mentions couvrent 365 jours jusqu'au 22 novembre 2026 ; les ressemblances couvrent 30 jours. Aucune notation organisationnelle ou sectorielle n'est publiée. Les observations n'établissent ni comptes actifs, ni personnes uniques, ni intrusions confirmées. [S2]

A.4 Comparaisons de rançongiciels

Les publications des sites d'extorsion sont des assertions criminelles. Elles ne prouvent ni chiffrement, ni vol réussi, ni paiement, ni perte, ni identité juridique unique. Les marques répétées et unités étrangères compliquent les comparaisons nationales.

Les quatre voisins régionaux partagent des frontières avec la Belgique et apportent un contexte logistique, linguistique, industriel ou financier pertinent. Les totaux bruts ne sont pas des taux nationaux de risque ajustés. Année 2026 partielle et année 2025 complète restent distinctes.

A.5 Périmètre des cartes de paiement

Ces observations limitées n'estiment ni le vol total de cartes, ni les cartes actives, ni les intrusions dans les systèmes bancaires, ni les pertes frauduleuses.

Les 3 cartes distinctes ne sont pas attribuées à des émetteurs belges nommés. Dix-sept apparitions ne sont pas dix-sept cartes. Les trois cartes forment une population unique ; aucune population bancaire nommée supplémentaire ne s'y ajoute.

A.6 Sources publiques et désignation des organisations

Les sources comprennent autorité cyber nationale, Safeonweb, autorité de protection des données, police, déclarations organisationnelles et presse dans les langues pertinentes. Chaque source factuelle citée a été lue dans son passage justificatif. La date de vérification ne date pas l'incident.

Nommer une victime exige confirmation officielle et couverture élargie. Les autres organisations reçoivent un rôle général. Si l'adresse de l'article identifie une organisation protégée, le registre public donne la racine de l'éditeur et masque l'adresse de l'article.

Une déclaration originale indisponible limite la désignation et la corroboration. Une citation rapportée reste attribuée à son auteur et à son éditeur. Elle ne devient pas silencieusement un résultat forensique indépendant vérifié.

A.7 Confiance et explications alternatives

La confiance peut être élevée dans l'existence d'une annonce conservée et faible dans son contenu revendiqué. Ces propositions diffèrent. Chaque cas indique ce qui est détenu, ce qui reste ouvert et une explication alternative.

Les modèles analytiques sont signalés. Langue, géographie, secteur, discours politique ou calendrier commun ne suffisent pas à relier des acteurs. Le rapport n'en déduit pas d'opérateur partagé.

A.8 Ce que le rapport exclut

Le rapport ne recense pas toute la cybercriminalité belge. Il ne fournit ni total national de personnes touchées, ni estimation de pertes, ni probabilités d'acteurs. Des avis de prévention ou d'événements anciens publiés en 2026 ne deviennent pas de nouvelles attaques.

Un arrêt préventif de site en octobre et une panne hospitalière de novembre sans indication d'attaque externe sont ainsi exclus des cyberattaques confirmées. Ils montrent pourquoi l'indisponibilité seule ne suffit pas. [S66][S67]

Les affirmations juridiques restent limitées aux autorités et textes cités. Le rapport n'est pas un conseil juridique. Dates de publication et réglementaires diffèrent des dates d'incident ; une décision administrative peut concerner une conduite d'une année antérieure.

Annexe B. Registre des preuves

Carte	Date	Lieu	Pseudonyme	Langue	Chapitre
B01	2026-01-24	Forum de fuites	kazutlg	Anglais	4
B02	2026-01-21	Forum de fuites	xmlrpc	Anglais	4
B03	2026-10-02	Forum de fuites	yneov18	Anglais	4
B04	2026-11-08	Forum de fuites	DataJava	Anglais	4
B05	2026-11-20	Forum de fuites	0xcasper	Anglais	4
B06	2026-11-13	Forum de fuites	updap	Anglais	4
B07	2026-04-13	Forum de fuites	[alias withheld]	Anglais	4
B08	2026-02-24	Forum de fuites	Crazy88	Anglais	4
B09	2026-11-03	Forum de fuites	buylogs	Anglais	4
B10	2026-11-21	Forum de fuites	WSdatabase	Anglais	4

Les cas A–F évaluent les propositions des forums conservés. Les cas G–O et R–S évaluent les récits d'incidents publics. Les cas P–Q évaluent les déclarations policières. Ce sont des dossiers, sans unités nationales d'incidents mutuellement exclusives.

Annexe C. Sources

S1: Odin by Brandefense ransomware-listing aggregate. https://brandefense.io/. Vérifié le 2026-11-22. Données conservées pour le rapport ; l'URL décrit le service et ne publie pas les données sous-jacentes.

S2: Atlas exposure ratings, Brandefense Blackhole domain associations and selected-domain passive observations. https://brandefense.io/. Vérifié le 2026-11-22. Données conservées pour le rapport ; l'URL décrit le service et ne publie pas les données sous-jacentes.

S3: Brandefense Blackhole country-tagged post counts and retained forum and card-material observations. https://brandefense.io/. Vérifié le 2026-11-22. Données conservées pour le rapport ; l'URL décrit le service et ne publie pas les données sous-jacentes.

S4: CCB, Figures show a steady rise in incidents. https://ccb.belgium.be/news/figures-show-steady-rise-incidents-ccb-urges-enterprises-act-immediately. Vérifié le 2026-11-22.

S5: CCB, The growing threat of identity compromise. https://ccb.belgium.be/news/growing-threat-identity-compromise. Vérifié le 2026-11-22.

S6: Belgian federal portal, Belgium, a federal state. https://www.belgium.be/en/about_belgium/government/federale_staat. Vérifié le 2026-11-22.

S7: CCB, Quarterly Cyber Threat Report Q1 2026. https://ccb.belgium.be/nl/open-media/1237/download?inline. Vérifié le 2026-11-22.

S8: CCB, Quarterly Cyber Threat Report Q2 2026. https://ccb.belgium.be/open-media/1427/download?inline. Vérifié le 2026-11-22.

S9: CCB, Quarterly Cyber Threat Report Q3 2026. https://ccb.belgium.be/open-media/1470/download?inline. Vérifié le 2026-11-22.

S10: Security Affairs, hospital service disruption and quoted statement. https://securityaffairs.com/ (URL de l'article omise). Vérifié le 2026-11-22.

S11: Safeonweb, company-confirmed fitness and booking-service incidents. https://safeonweb.be/nl/actueel/opgelet-klantgegevens-gelekt-bij-basic-fit-en-bookingcom. Vérifié le 2026-11-22.

S12: Reuters, Basic-Fit customer-data incident. https://www.reuters.com/business/basic-fit-says-data-breach-exposes-details-200000-members-netherlands-2026-04-13/. Vérifié le 2026-11-22.

S13: Safeonweb, learning-platform incident and phishing warning. https://safeonweb.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S14: RTBF, reported mobile-management incident at a public agency. https://www.rtbf.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S15: Machelen, municipal incident updates. https://www.machelen.be/cyberincident. Vérifié le 2026-11-22.

S16: VRT, municipal confirmation of personal-data theft. https://www.vrt.be/vrtnws/nl/2026/09/23/dan-toch-persoonsgegevens-gestolen-bij-cyberaanval-op-gemeentebe/. Vérifié le 2026-11-22.

S17: RTBF/Belga, sports membership incident accounts. https://www.rtbf.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S18: RTBF, fitness-chain company statement and criminal claim. https://www.rtbf.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S19: VRT, school-group incident and director statement. https://www.vrt.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S20: VRT, vocational-training data republication. https://www.vrt.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S21: L'Avenir, reported public e-learning platform incident. https://www.lavenir.net/ (URL de l'article omise). Vérifié le 2026-11-22.

S22: VRT, digital-signature supplier statement and customer-scope distinction. https://www.vrt.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S23: SPF Finances/FOD Financiën, recovery updates. https://finances.belgium.be/fr/Actualites/eservices-disponibles-apres-cyberattaque. Vérifié le 2026-11-22.

S24: VRT, federal tax administration incident. https://www.vrt.be/vrtnws/nl/2026/10/28/cyberaanval-bij-fod-financien/. Vérifié le 2026-11-22.

S25: CCB, refrigeration-controller security advisory. https://ccb.belgium.be/advisories/warning-six-new-danfoss-vulnerabilities-refrigeration-controllers-risk-immediate-action. Vérifié le 2026-11-22.

S26: Reuters, differing ministerial assessments of refrigeration attribution. https://www.reuters.com/world/belgian-ministers-odds-over-irans-alleged-role-refrigerator-cyberattacks-2026-11-13/. Vérifié le 2026-11-22.

S27: Safeonweb, refrigeration incidents and connected-device advice. https://safeonweb.be/nl/actueel/na-de-incidenten-met-koelkasten-warenhuizen-kan-jouw-slimme-koelkast-een-eigen-leven-gaan. Vérifié le 2026-11-22.

S28: Safeonweb, possible benefits-service data exposure. https://safeonweb.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S29: Safeonweb, possible gift-voucher customer-data exposure. https://safeonweb.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S30: Federal Police, alleged phishing-panel supplier investigation. https://www.police.be/5998/fr/actualites/crime-as-a-service-arrestation-dun-fournisseur-de-panneaux-de-phishing. Vérifié le 2026-11-22.

S31: Federal Police, automated invoice-fraud warning. https://www.police.be/5998/fr/actualites/factures-falsifiees-la-police-judiciaire-federale-danvers-tire-la-sonnette-dalarme. Vérifié le 2026-11-22.

S32: Federal Police, phishing and fake-bank-employee investigation. https://www.police.be/5998/fr/actualites/un-chef-dune-bande-dhameconneurs-arrete-son-retour-de-dubai. Vérifié le 2026-11-22.

S33: CCB, NIS2 evidence milestone in April 2026. https://ccb.belgium.be/news/nis2-18-april-2026-deadline-what-essential-entities-must-have-place. Vérifié le 2026-11-22.

S34: CCB, New communication for NIS2 essential entities. https://ccb.belgium.be/news/new-communication-nis2-essential-entities. Vérifié le 2026-11-22.

S35: CCB, NIS2 Notifications – Howto?. https://ccb.belgium.be/cert/report-incident/nis2-notifications-howto. Vérifié le 2026-11-22.

S36: Justel, Belgian NIS2 law, consolidated text. https://www.ejustice.just.fgov.be/eli/loi/2024/04/26/2024202344/justel. Vérifié le 2026-11-22.

S37: APD/GBA, Notifier et gérer une violation de données. https://www.autoriteprotectiondonnees.be/professionnel/actions/violation-de-donnees-personnelles. Vérifié le 2026-11-22.

S38: National Bank of Belgium, ITA team and DORA. https://www.nbb.be/en/financial-supervision/digital-resilience-and-cyber-risk/ita-team. Vérifié le 2026-11-22.

S39: CCB, CRA reporting obligations take effect. https://ccb.belgium.be/news/cyber-resilience-act-european-reporting-obligations-take-effect. Vérifié le 2026-11-22.

S40: CCB, National Cyber Emergency Plan. https://ccb.belgium.be/vital-sectors/national-cyber-emergency-plan. Vérifié le 2026-11-22.

S41: Ivanti, EPMM security advisory and resolved versions. https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340. Vérifié le 2026-11-22.

S42: NVD, CVE-2026-1281. https://nvd.nist.gov/vuln/detail/CVE-2026-1281. Vérifié le 2026-11-22.

S43: NVD, CVE-2026-1340. https://nvd.nist.gov/vuln/detail/CVE-2026-1340. Vérifié le 2026-11-22.

S44: Brandefense, Request a demo. https://brandefense.io/request-a-demo/. Vérifié le 2026-11-22.

S45: Safeonweb, fake pellet and firewood offers. https://safeonweb.be/nl/actueel/pellets-brandhout-kopen-laat-je-niet-misleiden-door-valse-aanbiedingen. Vérifié le 2026-11-22.

S46: Charging-account service, company incident FAQ. https://help.chargemap.com/nl/articles/11583170. Vérifié le 2026-11-22.

S47: Chemical manufacturer, clarification of the May incident. https://www.christeyns.com/ (URL de l'article omise). Vérifié le 2026-11-22.

S48: Recycling operator, forensic follow-up. https://www.iok.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S49: Medical research institute, statement updated in November. https://www.itg.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S50: Professional legal body, scope update. https://www.avocats.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S51: ITdaily, supermarket supplier incident. https://itdaily.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S52: Wonen360, furniture-retailer company statement. https://www.wonen360.nl/ (URL de l'article omise). Vérifié le 2026-11-22.

S53: Télésambre, municipal incident and restoration reporting. https://www.telesambre.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S54: La Libre, precious-metals customer-data incident. https://www.lalibre.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S55: DH, municipal website incident and scope. https://www.dhnet.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S56: HLN/VTM, travel-operator statement and customer messages. https://www.hln.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S59: Safeonweb, malicious-app and NFC-relay warning. https://safeonweb.be/nl/actueel/pas-op-voor-frauduleuze-telefoontjes-waarin-je-wordt-gevraagd-een-app-te-installeren-en-je. Vérifié le 2026-11-22.

S60: Safeonweb, executive impersonation on Teams. https://safeonweb.be/nl/actueel/pas-op-voor-ceo-fraude-microsoft-teams. Vérifié le 2026-11-22.

S61: Safeonweb, false hotel and B&B reservation messages. https://safeonweb.be/nl/actueel/opgelet-voor-valse-whatsapp-berichten-over-hotel-en-bb-boekingen. Vérifié le 2026-11-22.

S62: Safeonweb, government sign-in impersonation. https://safeonweb.be/nl/actueel/phishing-naam-van-csam. Vérifié le 2026-11-22.

S63: Safeonweb, fraudulent compensation and recovery messages. https://safeonweb.be/nl/actueel/opgelet-voor-fake-dossier-voor-schadevergoeding-na-fraude. Vérifié le 2026-11-22.

S64: Safeonweb, false voting and account-linking messages. https://safeonweb.be/nl/actueel/opgelet-voor-valse-stemwedstrijden-whatsapp. Vérifié le 2026-11-22.

S65: Safeonweb, high-profile invitation impersonation. https://safeonweb.be/nl/actueel/opgepast-voor-berichten-die-van-het-koningshuis-lijken-te-komen. Vérifié le 2026-11-22.

S66: Safeonweb, preventive PHP patching outage. https://safeonweb.be/nl/actueel/php-crisis-waarom-waren-verschillende-websites-niet-bereikbaar. Vérifié le 2026-11-22.

S67: Numerikare/Belga, hospital outage without external-attack indications. https://www.numerikare.be/ (URL de l'article omise). Vérifié le 2026-11-22.

S68: IETF, RFC 6797: HTTP Strict Transport Security. https://www.rfc-editor.org/rfc/rfc6797.html. Vérifié le 2026-11-22.

S69: W3C, Content Security Policy Level 3, abstract. https://www.w3.org/TR/CSP3/. Vérifié le 2026-11-22.

S70: IETF, RFC 4034: Resource Records for the DNS Security Extensions, section 5. https://www.rfc-editor.org/rfc/rfc4034.html. Vérifié le 2026-11-22.

S71: VRT, charging-account service incident and European user population. https://www.vrt.be/vrtnws/nl/2026/11/18/charge-map-cyberaanval/. Vérifié le 2026-11-22.

Annexe D. Glossaire

Terme	Sens simple
Récupération de compte	Processus rétablissant l'accès après perte d'identifiants ou de méthodes d'authentification
Identifiant d'authentification	Information servant à s'authentifier, comme un mot de passe ou un secret
Association d'appareil	Enregistrement reliant une observation d'appareil à un domaine ; la propriété exige une vérification
DMARC	Politique de messagerie aidant les destinataires à évaluer les messages utilisant l'identité d'un domaine
DKIM	Signature numérique d'un courriel vérifiée grâce aux informations publiées par le domaine
DNSSEC	Système de validation des informations DNS signées
Enregistrement DS	Un signataire de délégation relie une zone DNS parente à la clé de signature d'une zone enfant ; son observation ne valide pas toute la chaîne DNSSEC [S70]
HSTS	HTTP Strict Transport Security impose aux navigateurs HTTPS pour un site ; un seul en-tête observé n'évalue pas toutes les applications [S68]
CSP	Content Security Policy contrôle les ressources qu'une page peut charger ou exécuter ; une seule politique observée n'établit pas la sécurité complète de l'application [S69]
Exfiltration	Copie non autorisée de données hors d'un système
Courtier en accès initial	Une personne qui propose un accès aux systèmes d'une organisation ; chaque revendication doit être vérifiée
Métadonnées	Informations décrivant un autre enregistrement, comme son titre, son auteur ou l'heure de traitement
Relais NFC	Transmission à distance de communications de carte à courte portée pendant une transaction frauduleuse
Consentement OAuth	Permission accordée à une application pour des ressources définies d'un compte
Pseudonymisation	Remplacement des identifiants directs conservant une possibilité de rattacher les données aux personnes
Session	Interaction authentifiée pouvant rester utilisable après la connexion initiale

Terme	Sens simple
SPF	Déclaration DNS des services d'envoi autorisés pour un domaine de messagerie
TLS	Protocole protégeant les communications réseau et authentifiant un service

À propos du rapport

Préparé par Odin by Brandefense. Brandefense Country Report · Belgium 2026. Version 1.0, coupure d'observation 22 novembre 2026. TLP:CLEAR.

Le rapport distingue annonces, publications d'extorsion, récits officiels et évaluation. Il ne prend aucune position politique et ne formule aucune attribution étatique indépendante. Les recommandations décrivent des actions à valider ; elles n'accusent pas une organisation nommée de les avoir omises.

Les éditions française et néerlandaise sont traduites avec l'IA depuis le texte anglais de référence. L'édition anglaise fait foi en cas de différence. Revue indépendante de publication, mise en page et diffusion sont des étapes distinctes.

© 2026 Brandefense. Tous droits réservés.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO