BRANDEFENSE COUNTRY REPORT · FRANCE 2026

Brandefense France : rapport sur le paysage des cybermenaces 2026

Vol de données par abus d'identité, incidents chez les prestataires et perturbation des services connectés

Odin by Brandefense
Période de recherche: du 1er janvier au 22 novembre 2026, selon la date des publications
Version 1.0 · Édition publique de recherche · TLP:CLEAR · 22 novembre 2026

120 sur 249
domaines évalués avec une offre actuelle d'identifiants

7757
enregistrements de forum conservés, sur une période partielle

295
inscriptions étiquetées France d'extorsion réparties entre de nombreux noms

20
actions avec un responsable, un déclencheur et une preuve d'achèvement

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 parcours de lecture	09
02	Contexte numérique et sécuritaire français	10
03	Exposition nationale : l'ensemble de domaines sélectionné	14
04	Ce que montrent les publications conservées du dark web	26
05	Incidents et revendications par secteur	44
06	Hacktivisme, DDoS et perturbation industrielle	57
07	Acteurs et campagnes	62
08	L'économie de la fraude	73
09	Banque et finance	78
10	Réponse réglementaire et nationale	83
11	Perspectives et scénarios conditionnels	88
12	Plan d'action	92
A	Annexe A. Périmètre, méthode et confiance	99
B	Annexe B. Registre des éléments	102
C	Annexe C. Sources	103
D	Annexe D. Glossaire	107
	À propos de ce rapport	109

Direction et RSSI	01 05 11 12
SOC et réponse	04 06 07 12
Identité et applications	03 05 07 12
Exploitation et sécurité physique	05 06 12
Fraude et finance	08 09 12
Juridique et achats	05 10 12

À propos de cette édition

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

Recherche et rédaction assistées par l'IA. Les observations, les revendications, les déclarations officielles et les interprétations restent distinctes. L'annexe A précise le périmètre et le niveau de confiance de chaque ensemble de données.

Des identités volées peuvent ouvrir l'accès aux données des organisations françaises. Un incident chez un prestataire peut toucher de nombreux clients, et un accès distant peut affecter les opérations physiques.

CHAPITRE 01

Synthèse

01

CE CHAPITRE RÉPOND À LA QUESTION

Quelles décisions découlent des éléments français disponibles à la clôture ?

4

décisions avec un responsable et un test d'achèvement

Quatre décisions pour la direction 06

L'année en chiffres 06

CHAPITRE 01

Synthèse

EN BREF

Les éléments français relient vol de données, abus d'identité et perturbation des services. Ransompedia recense 295 inscriptions étiquetées France sur la période, contre 182 sur toute l'année 2025. Les enquêtes officielles décrivent des comptes volés, des droits excessifs et des dépendances aux prestataires. Les divulgations de novembre concernent aussi des contrôleurs de froid. Des offres actuelles d'identifiants concernent 120 domaines sur 249 ; l'indicateur national Atlas vaut 63. Donnez la priorité aux comptes, aux exports, aux notifications des prestataires, à la reprise indépendante et aux accès industriels distants.

Ce rapport associe des contenus conservés de Brandefense, des inscriptions de Ransompedia, des observations passives et des informations publiques vérifiées. Ces chiffres décrivent des ensembles différents. Une publication n'est pas un incident, une inscription n'est pas une confirmation, et une sélection d'organisations ne mesure pas la prévalence nationale [S1][S2][S3][S4].

1. Les contrôles d'identité doivent encadrer l'usage des données après la connexion. L'enquête de l'ANSSI sur l'administration fiscale décrit des identifiants valides, un cloisonnement insuffisant et des lacunes de détection. Son bilan opérationnel d'octobre décrit encore la réutilisation de secrets volés pour atteindre des applications contenant des données. L'authentification multifacteur compte, mais les droits, les sessions et les exports doivent aussi être contrôlés [S7][S8].

2. La visibilité des rançongiciels justifie des moyens de reprise dans plusieurs secteurs. Les 295 inscriptions étiquetées France se comparent à 457 pour l'Allemagne, 286 pour l'Italie, 221 pour l'Espagne et 46 pour la Belgique. Qilin représente 48 inscriptions étiquetées France et The Gentlemen 44. Il s'agit de revendications publiques enregistrées, pas d'incidents confirmés ni d'un classement du risque national [S3].

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.

3. Un incident chez un prestataire peut multiplier les décisions de notification. Un prestataire de courrier professionnel a divulgué en novembre un incident de septembre. La presse cite ses déclarations sur les noms et adresses postales et indique une population de 22 millions de destinataires. La taille du prestataire n'établit pas quels autres systèmes ont été consultés [S12][S13].

4. Les opérations physiques exigent une réponse distincte. L'évaluation française du C4 décrit des changements de paramètres de contrôleurs de froid sur environ 700 sites de distribution les 11–12 octobre. Elle fait état de départs de feu dans au moins 15 cas. L'attribution à une unité iranienne est celle des autorités ; elle ne découle pas des publications étudiées dans ce rapport [S10].

5. Une publication peut décrire un incident bien antérieur. Le bilan du CERT-FR du 12 novembre décrit des incidents d'octobre et des enquêtes en cours. Les sanctions annoncées en janvier portent sur des événements antérieurs. La date d'une annonce ne suffit pas à compter une nouvelle intrusion en novembre ou en janvier [S7] [S14][S15].

Quatre décisions pour la direction

1. **Encadrez les comptes valides avant une extraction massive.** Confiez aux responsables de l'identité et des applications la revue des accès privilégiés, des prestataires et des partenaires. Vérifiez si un utilisateur légitime peu privilégié peut consulter les dossiers d'autrui. Faites remonter les accès massifs inattendus avec le contexte du compte, de la session et de l'export.
1. **Testez la notification avec les prestataires qui traitent des données sensibles.** Exigez un contact d'incident identifié, une première alerte rapide et des mises à jour du périmètre. Exercez un cas où le prestataire connaît l'incident mais ne peut pas encore identifier tous les clients concernés.
1. **Démontrez la reprise et la sécurité industrielle de manière indépendante.** Restaurez un service critique avec des identifiants de reprise distincts. Pour les équipements connectés, vérifiez l'isolement des accès distants, les procédures locales et la remise en service sûre avec le responsable opérationnel.
1. **Réunissez fraude, juridique et communication.** Préparez des messages précisant les faits connus, les investigations en cours et les mesures possibles pour les personnes concernées. La connaissance de données personnelles ne doit jamais autoriser à elle seule un paiement.

L'année en chiffres

Chaque chiffre a sa propre unité et sa propre période d'observation.

295

Inscriptions françaises de rançongiciels datées de la période étudiée [S3]

CE QU'IL NE MESURE PAS

Attaques confirmées, victimes distinctes ou activité nationale totale

182

Inscriptions françaises sur toute l'année 2025 dans le même état des données [S3]

CE QU'IL NE MESURE PAS

Une comparaison sur une durée identique

48 / 44

Inscriptions sous les noms Qilin et The Gentlemen [S3]

CE QU'IL NE MESURE PAS

L'attribution de chaque intrusion à un opérateur unique

7 757

Enregistrements de forum conservés [S1]

CE QU'IL NE MESURE PAS

Le total national de la période ou des incidents distincts

162 sur 237

Domaines observés avec politique DMARC de rejet ou quarantaine [S2]

CE QU'IL NE MESURE PAS

Protection vérifiée de tous les expéditeurs ou adoption nationale

63

Indicateur national Atlas pour 249 domaines évalués [S2]

CE QU'IL NE MESURE PAS

Prévalence nationale ou note sectorielle

120 sur 249

Domaines évalués avec offre actuelle d'identifiants [S2]

CE QU'IL NE MESURE PAS

Intrusions confirmées ou ventes conclues

250

Domaines candidats dans douze groupes sectoriels sélectionnés [S2]

CE QU'IL NE MESURE PAS

Un échantillon représentatif ou un classement officiel d'organisations

Environ 700

Sites de distribution dans le récit officiel de l'incident de froid [S10]

CE QU'IL NE MESURE PAS

Un décompte vérifié indépendamment par Brandefense

Au moins 15

Cas de départs de feu signalés dans ce récit officiel [S10]

CE QU'IL NE MESURE PAS

L'ensemble des conséquences physiques

64 / 5

Nouveaux événements de sécurité des données / ceux concernant des ministères ou organismes sous tutelle dans le bilan d'octobre [S7]

CE QU'IL NE MESURE PAS

Soixante-quatre nouveaux incidents ministériels confirmés indépendamment

22 millions

Destinataires mentionnés dans la presse sur le prestataire de courrier [S13]

CE QU'IL NE MESURE PAS

Une population à additionner aux autres fuites pour compter les résidents français distincts

POINTS À RETENIR

01

Protégez l'usage des comptes valides autant que la connexion.

02

Traitez les données des prestataires, la reprise et la sécurité industrielle comme des responsabilités opérationnelles distinctes.

03

Séparez les inscriptions, les estimations officielles d'incidents et les nombres de personnes concernées.

Carte du rapport

Partez de votre décision, puis suivez les éléments disponibles, leurs limites et le test d'achèvement.

Direction et RSSI	Quelles dépendances justifient un investissement immédiat ?	01 05 11 12
SOC et réponse	Quand une revendication exige-t-elle une investigation ?	04 06 07 12
Identité et applications	Un accès valide permet-il de récupérer trop de données ?	03 05 07 12
Exploitation et sécurité physique	Peut-on isoler les équipements distants sans danger ?	05 06 12
Fraude et finance	Que peut réellement autoriser un interlocuteur convaincant ?	08 09 12
Juridique et achats	Qui doit informer qui, et quand ?	05 10 12

Ensemble étudié	Question traitée	Limite
Publications clandestines	Ce que des personnes proposent, demandent ou annoncent	Authenticité, actualité et résultats à établir séparément
Inscriptions de rançongiciels	Ce qui apparaît dans l'état des inscriptions	Une publication peut suivre l'intrusion et répéter une organisation
Observations passives	Ce que montrent certaines configurations publiques	Aucune démonstration d'intrusion réussie ou d'efficacité globale
Déclarations officielles	Ce qu'un responsable de traitement ou une autorité indique	Estimations et enquêtes susceptibles d'évoluer
Avis techniques	Quels produits et versions nécessitent une action	Un avis n'établit pas une exploitation dans une organisation française

Sommaire et parcours de lecture

Les douze chapitres relient les éléments disponibles aux décisions. Commencez par la synthèse, puis suivez le parcours correspondant à vos responsabilités.

Chapitre	Question	Premier lecteur
1. Synthèse	Quelles décisions faut-il attribuer immédiatement ?	Direction et RSSI
2. Contexte numérique	Quelles dépendances structurent les risques ?	Direction
3. Exposition des organisations	Que permet d'établir l'ensemble sélectionné ?	Infrastructure
4. Éléments du dark web	Que proposent les annonces, et que reste-t-il à vérifier ?	Renseignement
5. Cas par secteur	Quels mécanismes divulgués changent les priorités ?	Responsables de services
6. Hacktivisme et perturbations	Qu'est-ce qui distingue la publicité d'un effet démontré ?	Exploitation
7. Acteurs et campagnes	Quels liens et quelles attributions sont étayés ?	Renseignement
8. Économie de la fraude	Comment des données personnelles peuvent-elles faciliter la tromperie ?	Équipes fraude
9. Banque et finance	Quels contrôles d'accès et de paiement exigent une responsabilité commune ?	Finance et identité
10. Réponse réglementaire	Quelles obligations s'appliquent à la date de clôture ?	Juridique et conformité
11. Perspectives	Quels signaux feraient évoluer l'évaluation ?	Direction
12. Plan d'action	Qui agit, et comment vérifier l'achèvement ?	Tous les responsables

Parcours direction : chapitres 1, 5 et 10–12. **Parcours exploitation** : chapitres 4, 6, 7 et 12. **Parcours identité et fraude** : chapitres 3, 8, 9 et 12.

Observé désigne un contenu conservé ou une mesure enregistrée. **Revendiqué** désigne ce qu'affirme une publication ou une inscription. **Signalé officiellement** désigne la description d'un responsable de traitement ou d'une autorité, dans son périmètre déclaré.

Une interprétation relie les éléments disponibles à une décision. Elle ne peut établir des faits manquants sur l'accès, les personnes concernées, l'attribution, une vente réalisée ou une perte financière.

CHAPITRE 02

Contexte numérique et sécuritaire français

02

CE CHAPITRE RÉPOND À LA QUESTION

Quelles dépendances nationales doivent guider la défense ?

95,7%

pénétration d'Internet dans l'observation de fin 2026

2.1 Une population connectée et des interactions répétées 11
2.2 Services publics, données et accès délégués 11
2.3 La portée d'un prestataire dépend du service 12
2.4 Les opérations connectées ajoutent une dimension de sécurité physique 12
2.5 Discours politique et attribution étatique 12
2.6 Plusieurs volets institutionnels 13

CHAPITRE 02

Contexte numérique et sécuritaire français

EN BREF

La France associe un usage étendu des services numériques à de grands ensembles de données d'identité, des prestataires connectés et des équipements administrés à distance. Ces caractéristiques créent des risques différents. Un compte valide peut exposer des dossiers sans faille logicielle. Un incident chez un prestataire peut imposer plusieurs évaluations clients. Un changement de paramètres peut affecter les opérations physiques. Cartographiez ensemble identités, données et services avant de choisir les priorités.

2.1 Une population connectée et des interactions répétées

L'édition Digital 2027 France de DataReportal présente des estimations de fin 2026 : 63.9 millions d'internautes et une pénétration de 95,7%. Elle indique 77.4 millions de connexions mobiles et 53.5 millions d'identités d'utilisateurs des réseaux sociaux en octobre. Connexions et identités ne représentent pas des personnes distinctes [S5].

L'enjeu de sécurité tient aux interactions répétées. Une personne peut employer les services fiscaux, l'emploi, la santé, le commerce, les télécommunications et la banque. Chacun peut détenir des informations exactes qui rendent ensuite une usurpation plus convaincante. Ces détails ne doivent pas autoriser seuls une action sensible.

La même logique vaut au sein des organisations. Un salarié peut employer une application partenaire, un support externalisé et un fournisseur d'identité dans un même processus. Ce parcours franchit des limites qu'un inventaire isolé de serveurs peut manquer.

Reliez la personne à l'application, l'application aux données et les données à chaque prestataire. Identifiez qui peut réinitialiser un accès, exporter des dossiers, modifier des instructions de paiement ou agir sur un processus physique. Ce sont des décisions opérationnelles, au-delà de simples champs d'inventaire.

2.2 Services publics, données et accès délégués

Les incidents officiels concernent la fiscalité, l'éducation, l'emploi, les prestations et les services administratifs [S6] [S7][S8]. Leur question commune est l'usage autorisé des informations par une identité valide. Les éléments ne démontrent pas qu'un même acteur a mené tous ces incidents.

Une application peut authentifier correctement un utilisateur et lui exposer trop d'informations. Le problème peut venir de droits excessifs, d'un défaut d'autorisation au niveau d'un objet ou d'un contrôle insuffisant des extractions automatisées. Changer le mot de passe ne corrige pas ces situations.

Le rapport associe donc les contrôles d'identité aux responsables applicatifs. Les équipes de sécurité doivent comprendre le sens métier d'un export, d'une consultation et d'un identifiant de dossier. Sans ce contexte, une opération légitime volumineuse peut ressembler à un abus, et un abus à une opération courante.

2.3 La portée d'un prestataire dépend du service

La divulgation du prestataire de courrier illustre la dépendance de nombreuses organisations à un service de traitement commun [S12][S13]. Un responsable de traitement peut devoir évaluer ses données sans preuve d'intrusion dans ses propres systèmes. Les enquêtes du prestataire et du client peuvent avancer à des rythmes différents.

Un registre utile décrit les données détenues, les accès autorisés, les sous-traitants, la reprise et les contacts d'incident. Les garanties contractuelles doivent être testées. Le prestataire peut-il identifier les ensembles clients concernés, et le client peut-il décider d'une notification avant la fin de l'enquête ?

Ce rapport ne suppose pas que toute organisation utilisant un prestataire a été touchée. Il ne confond pas non plus la clientèle totale du prestataire avec la population concernée par l'incident. Ces nombres répondent à des questions différentes.

2.4 Les opérations connectées ajoutent une dimension de sécurité physique

L'incident des contrôleurs de froid intègre les opérations physiques au paysage étudié [S10]. Les équipes doivent savoir qui peut modifier les paramètres, comment les accès distants sont contrôlés et quelles alarmes indépendantes détectent un état dangereux.

La reprise informatique et la reprise physique ne sont pas interchangeables. Restaurer une configuration ne prouve pas automatiquement la sécurité des denrées, des équipements ou des locaux. Les responsables opérationnels décident quand reprendre et quelles preuves sont nécessaires.

Le même principe vaut pour l'énergie, l'eau, la logistique et l'industrie. Le rapport emploie ces secteurs pour préparer la défense. Il n'affirme ni qu'ils ont tous subi le même mécanisme, ni qu'une interface publique démontre un accès non autorisé.

2.5 Discours politique et attribution étatique

Le rapport ne reprend un motif politique que lorsqu'une source le formule et qu'il aide à comprendre les éléments disponibles. Les slogans ne démontrent ni causalité, ni commanditaire, ni véracité d'un grief. Les descriptions chargées et les insultes sont omises.

L'attribution de novembre par les autorités françaises reste leur évaluation [S10][S11]. Elle n'est pas étendue aux vendeurs de données, aux annonces DDoS ou aux groupes de rançongiciels sans lien établi. Une proximité temporelle ou un discours commun ne démontre pas un opérateur commun.

L'analyse ne prend position ni sur les questions territoriales, ni sur les débats politiques internes, ni sur les élections, les décisions publiques ou les relations extérieures. Ses recommandations concernent les éléments de sécurité et les responsabilités opérationnelles.

2.6 Plusieurs volets institutionnels

Les bilans de l'ANSSI décrivent l'assistance aux ministères et la coordination de la communication technique de crise [S6][S7]. Les décisions de la CNIL concernent les obligations relatives aux données personnelles et les contrôles de sécurité [S14][S15][S16][S17]. Les enquêtes policières et judiciaires ont un rôle distinct.

Ces volets se recoupent mais répondent à des questions différentes. Un rapport technique peut décrire une voie d'intrusion sans établir une responsabilité pénale. Une décision réglementaire peut concerner un incident ancien. Une annonce d'enquête peut présenter des allégations non jugées.

Conservez des contacts actuels et une chronologie commune des éléments. Distinguez découverte, prise de connaissance, endiguement, première notification et mises à jour. Le chapitre 10 précise les limites juridiques ; le chapitre 12 attribue les responsabilités opérationnelles.

POINTS À RETENIR

01

Reliez personnes, applications, dossiers et prestataires dans chaque processus critique.

02

Donnez à la sécurité des opérations physiques sa propre décision de remise en service.

03

Limitez attributions officielles, constats réglementaires et allégations pénales au périmètre de leur source.

CHAPITRE 03

Exposition nationale : l'ensemble de domaines sélectionné

CE CHAPITRE RÉPOND À LA QUESTION

Quels signaux mesurés justifient la validation des comptes, appareils ou services ?

120 sur 249

domaines évalués avec une offre actuelle d'identifiants

3.1 Périmètre étudié 15
3.2 Offres actuelles et indicateur national 16
3.3 Associations d'appareils et enregistrements d'identifiants 18
3.4 Documents, domaines similaires et mentions 21
3.5 Politiques de messagerie et certificats 22
3.6 DNS, TLS et pages d'accueil 24
3.7 Responsables et preuves d'achèvement 25

CHAPITRE 03

Exposition nationale : l'ensemble de domaines sélectionné

EN BREF

120 domaines évalués sur 249 avaient un identifiant proposé à la vente. L'indicateur national Atlas vaut 63 pour la partie évaluée des 250 domaines sélectionnés. Un domaine sélectionné reste sans résultat d'exposition. Au moins 1051618 associations d'appareils et 480908523 enregistrements d'identifiants sont recensés. Ces observations se recoupent et ne confirment pas des intrusions. Confiez aux responsables concernés la validation des offres actuelles, des appareils salariés et des configurations.

3.1 Périmètre étudié

La sélection décrit des institutions et services importants. Ce n'est pas un classement officiel, et plusieurs domaines appartiennent à des groupes liés [S2].

Élément	Définition
Population sélectionnée	250 domaines candidats dans douze groupes sectoriels
Sélection	Choix raisonné de services publics, finance, infrastructures, grandes entreprises, éducation et santé
Unité	Un domaine principal de service ; pas nécessairement une entité juridique indépendante
Recoupements	Maisons mères, filiales, marques ou services distincts peuvent apparaître séparément
Population d'exposition	249 domaines évalués ; un domaine sélectionné sans résultat
Population passive	237 domaines observés ; 13 domaines sélectionnés hors dénominateur
État de l'exposition	21 novembre 2026
Fenêtre des domaines similaires	19 octobre–18 novembre 2026
États des mentions et configurations	22 novembre 2026
Publication sectorielle	Nombres de signaux observés
Résultats publics	Agrégats anonymes et indicateur national Atlas
Limite	Aucune estimation de prévalence nationale, d'efficacité ou d'organisation typique

La validation des entités juridiques et de la propriété reste nécessaire avant un classement d'organisations indépendantes. Un domaine reconnaissable et un service joignable ne démontrent pas l'indépendance de chaque entrée.

3.2 Offres actuelles et indicateur national

120 domaines évalués sur 249 avaient un identifiant proposé à la vente. L'ensemble sélectionné comprend 250 domaines, dont un sans résultat d'exposition. Une donnée absente n'est pas un zéro observé [S2].

L'indicateur national Atlas vaut **63 sur une échelle de 0–100**. Une valeur plus élevée indique une exposition observée plus forte. Il décrit cet ensemble évalué, pas toutes les organisations françaises. Seul l'indicateur national est publié ; les notes sectorielles et individuelles sont retirées.

63

indicateur national Atlas pour 249 domaines évalués

Les populations sélectionnées, évaluées et passives gardent des dénominateurs distincts

Le nombre sélectionné figure dans chaque libellé. Les fractions d'exposition et d'observation passive utilisent les domaines sélectionnés ; les offres actuelles d'identifiants utilisent les domaines évalués et sont en corail.

	Sélectionnés	Exposition évaluée	Observations passives	Offre actuelle
Administration (50)	50/50	50/50	49/50	19/50
Banque et finance (30)	30/30	30/30	27/30	16/30
Éducation (30)	30/30	30/30	26/30	18/30
Industrie (30)	30/30	30/30	30/30	11/30
Énergie et services collectifs (20)	20/20	20/20	20/20	6/20
Commerce et groupes (20)	20/20	19/20	20/20	14/19
Transport et logistique (20)	20/20	20/20	19/20	9/20
Télécommunications et technologie (10)	10/10	10/10	10/10	9/10
Santé (10)	10/10	10/10	7/10	1/10
Assurance (10)	10/10	10/10	10/10	5/10
Hôtellerie et tourisme (10)	10/10	10/10	10/10	6/10
Médias et divertissement (10)	10/10	10/10	9/10	6/10

Source : observations d'exposition de 249 domaines évalués parmi 250 candidats sélectionnés, 21 novembre 2026. Associations cumulatives pouvant se chevaucher ; aucune mesure des personnes uniques, des intrusions confirmées ou de la prévalence nationale [S2].

Secteur	Sélectionnés	Exposition évaluée	Observations passives	Domaines avec une offre actuelle d'identifiants
Administration	50	50	49	19
Banque et finance	30	30	27	16
Éducation	30	30	26	18
Industrie	30	30	30	11
Énergie et services collectifs	20	20	20	6
Commerce et groupes	20	19	20	14
Transport et logistique	20	20	19	9
Télécommunications et technologie	10	10	10	9

Secteur	Sélectionnés	Exposition évaluée	Observations passives	Domaines avec une offre actuelle d'identifiants
Santé	10	10	7	1
Assurance	10	10	10	5
Hôtellerie et tourisme	10	10	10	6
Médias et divertissement	10	10	9	6
Total	250	249	237	120

Une offre actuelle établit qu'un identifiant associé au domaine est annoncé. Elle n'établit ni validité du compte, ni vente conclue, ni personnes concernées, ni intrusion dans l'organisation. Validez le compte et le service avec les éléments autorisés avant de décider.

Dans les graphiques téléchargeables, `domains_with_current_credential_listing` compte les domaines associés à des identifiants annoncés à la vente. Ce champ n'établit pas la mise en vente d'une organisation ou d'un accès à ses systèmes.

3.3 Associations d'appareils et enregistrements d'identifiants

Des associations d'appareils concernent 236 domaines évalués et des enregistrements d'identifiants en concernent 243. L'ensemble contient au moins 1051618 associations d'appareils, dont 82775 classées salariées. Ces dernières sont comprises dans la vue appareils et ne doivent pas y être ajoutées [S2].

Les associations d'appareils et enregistrements d'identifiants sectoriels exigent des validations différentes



Source : observations d'exposition de 249 domaines évalués parmi 250 candidats sélectionnés, 21 novembre 2026. Associations cumulatives pouvant se chevaucher ; aucune mesure des personnes uniques, des intrusions confirmées ou de la prévalence nationale [S2].

Secteur	Évalués	Appareils, au moins	Appareils salariés	Enregistrements d'identifiants
Administration	50	247 177	1 292	759 163
Banque et finance	30	115 930	701	373 568

Secteur	Évalués	Appareils, au moins	Appareils salariés	Enregistrements d'identifiants
Éducation	30	65 836	4 464	814 866
Industrie	30	60 555	3 704	1 525 751
Énergie et services collectifs	20	51 288	2 496	513 681
Commerce et groupes	19	228 916	3 529	916 117
Transport et logistique	20	59 024	828	329 948
Télécommunications et technologie	10	106 139	64 087	474 979 471
Santé	10	2 531	317	300 911
Assurance	10	60 544	325	200 959
Hôtellerie et tourisme	10	4 114	52	15 568
Médias et divertissement	10	49 564	980	178 520
Total	249	1 051 618	82 775	480 908 523

Les enregistrements d'identifiants comprennent 170 231 515 enregistrements de bases divulguées, 21 992 886 issus de journaux de voleurs d'informations et 288 684 122 de listes combinées (combolists). Leur somme atteint 480 908 523.

Une liste combinée réunit des identifiants de compte et des mots de passe ; elle peut compiler ou répéter des données anciennes [S77]. Ces enregistrements peuvent se recouper entre domaines et ne dénombrent pas des comptes actifs distincts.

Les télécommunications et la technologie représentent 474 979 471 associations d'enregistrements d'identifiants, soit 98,8% du total. Domaines employés par les clients et contenus historiques répétés peuvent y contribuer. Cette concentration ne démontre pas la même part de personnes touchées ou d'intrusions confirmées [S2].

Un appareil associé à un service client n'appartient pas automatiquement au prestataire. La classification salariée exige aussi du contexte lorsque salariés, étudiants ou clients partagent un domaine. Vérifiez actualité, propriété et corrections antérieures avant toute action perturbatrice.

3.4 Documents, domaines similaires et mentions

Secteur	Évalués	Offres actuelles	Associations de documents
Administration	50	19	2 807
Banque et finance	30	16	327
Éducation	30	18	418
Industrie	30	11	1 675
Énergie et services collectifs	20	6	1 089
Commerce et groupes	19	14	532
Transport et logistique	20	9	487
Télécommunications et technologie	10	9	2 549
Santé	10	1	75
Assurance	10	5	55
Hôtellerie et tourisme	10	6	19
Médias et divertissement	10	6	171
Total	249	120	10 204

Des documents sont associés à 210 domaines évalués, avec 10 204 associations au total. Cela n'établit ni confidentialité, ni divulgation illicite, ni accès adverse. Des documents publics et des répétitions restent des explications possibles [S2].

La vue des domaines similaires datée du 19 octobre–18 novembre 2026 contient 171 947 candidats pour 229 domaines évalués. Leur propriété et leur usage restent à examiner ; ce ne sont pas des sites d'hameçonnage confirmés. Ils peuvent désigner des services liés, autorisés ou sans rapport.

Des mentions apparaissent pour 125 domaines évalués dans les conversations clandestines et 96 sur le web clandestin, pendant la fenêtre annuelle terminant le 22 novembre 2026. Elles peuvent refléter informations, liens, clients ou publicité. Leur présence ne démontre pas seule une activité hostile [S2].

Ces nombres ne sont pas additifs. Un domaine peut cumuler appareils, identifiants, offres et documents. Une somme sectorielle élevée ne décrit pas non plus l'organisation typique du secteur.

3.5 Politiques de messagerie et certificats

Les observations passives couvrent 237 domaines sélectionnés. La politique DMARC est de rejet pour 107 et de quarantaine pour 55. Ensemble, 162 domaines, soit 68,4%, publient une de ces politiques. Pour 65 autres, elle est de surveillance ; aucune n'est observée pour 10 [S2].

Une politique publiée ne prouve ni la bonne configuration de chaque expéditeur ni le respect du traitement par chaque destinataire. Vérifiez la politique effective du domaine d'envoi et les messages sortants avant de modifier la politique [S27].

Messagerie et certificats utilisent la population passive

	DMARC reject / quarantine	SPF	DNSSEC	TLS valide
Administration	27/49	48/49	11/49	47/49
Banque et finance	23/27	26/27	5/27	20/27
Éducation	8/26	24/26	3/26	22/26
Industrie	25/30	29/30	9/30	29/30
Énergie et services collectifs	17/20	20/20	4/20	19/20
Commerce et groupes	16/20	20/20	0/20	19/20
Transport et logistique	14/19	18/19	5/19	17/19
Télécommunications et technologie	8/10	9/10	2/10	10/10
Santé	5/7	7/7	1/7	5/7
Assurance	8/10	10/10	0/10	10/10
Hôtellerie et tourisme	4/10	7/10	3/10	9/10
Médias et divertissement	7/9	8/9	0/9	9/9

Source : observations passives de 237 domaines, 22 novembre 2026. HSTS repose sur 184 pages d'accueil enregistrées. Les validations infructueuses et les résultats TLS non résolus restent distincts ; les politiques ne prouvent pas leur application à chaque message [S2].

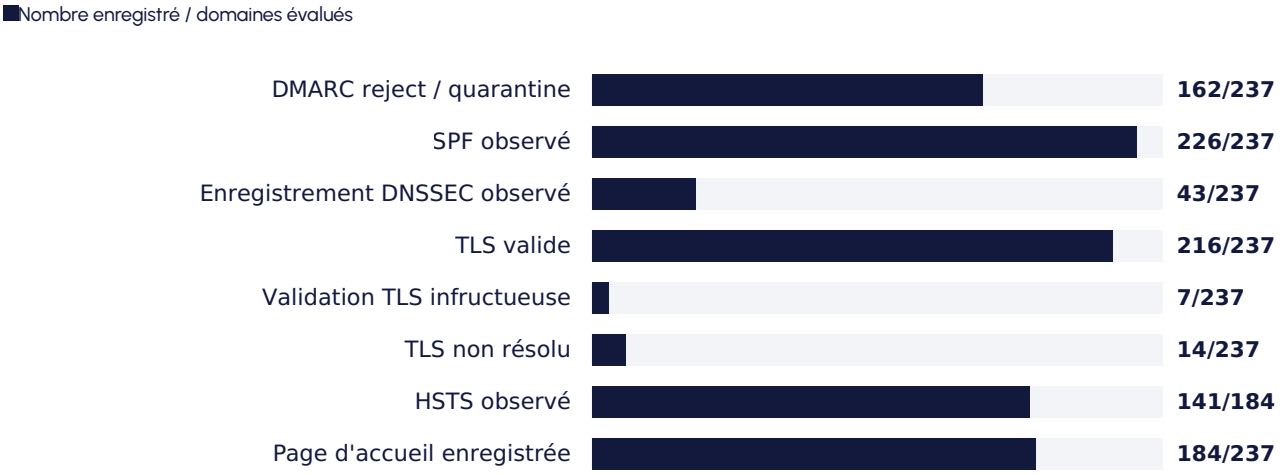
Secteur	Observés	Rejet ou quarantaine	SPF observé	Certificat valide
Administration	49	27	48	47

Secteur	Observés	Rejet ou quarantaine	SPF observé	Certificat valide
Banque et finance	27	23	26	20
Éducation	26	8	24	22
Industrie	30	25	29	29
Énergie et services collectifs	20	17	20	19
Commerce et groupes	20	16	20	19
Transport et logistique	19	14	18	17
Télécommunications et technologie	10	8	9	10
Santé	7	5	7	5
Assurance	10	8	10	10
Hôtellerie et tourisme	10	4	7	9
Médias et divertissement	9	7	8	9
Total	237	162	226	216

SPF est observé pour 226 domaines. Cela ne démontre ni l'inclusion de tous les expéditeurs autorisés ni le rejet des autres. L'absence d'enregistrement DKIM observé n'établit pas davantage l'absence de signature ; vérifiez les en-têtes réels [S2][S27].

3.6 DNS, TLS et pages d'accueil

Les résultats passifs préservent les observations inconclusives



Source : observations passives de 237 domaines, 22 novembre 2026. HSTS repose sur 184 pages d'accueil enregistrées. Les validations infructueuses et les résultats TLS non résolus restent distincts ; les politiques ne prouvent pas leur application à chaque message [S2].

Observation	Nombre	Population évaluée
Enregistrement de délégation DNSSEC observé	43	237 domaines observés
Vérification du certificat réussie	216	237 domaines observés
Validation du certificat infructueuse	7	237 domaines observés
Vérification du certificat non résolue	14	237 domaines observés
Réponse de page d'accueil enregistrée	184	237 domaines observés
Observation de page inconclusive	53	237 domaines observés
HSTS observé	141	184 pages enregistrées

La somme des résultats de certificats atteint 237. Celle des pages enregistrées et inconclusives atteint également 237. Les résultats inconclusifs ne sont pas comptés comme absences d'en-têtes ou défauts confirmés [S2].

Un certificat valide ne démontre pas la sécurité applicative. Un enregistrement lié à DNSSEC ne démontre pas la validation de chaque application. HSTS décrit la réponse enregistrée, pas tous les sous-domaines ou parcours [S27].

3.7 Responsables et preuves d'achèvement

Confiez la validation des comptes actifs à l'identité, les appareils salariés aux équipes terminaux et les signaux clients pertinents à la fraude. La sensibilité documentaire relève du propriétaire des données ; les domaines similaires, du responsable de marque et de service.

Clôturez chaque élément comme actif, historique, sans rapport ou non résolu, avec une date justificative. Faites remonter l'activité non autorisée corroborée par le processus de réponse interne. L'indicateur national ne remplace pas les preuves sur le compte, l'appareil ou le service précis.

POINTS À RETENIR

01

Validez les offres actuelles de 120 domaines sur 249 sans annoncer des intrusions confirmées.

02

Séparez appareils, identifiants, documents et observations passives.

03

Confiez chaque signal crédible à son responsable opérationnel avec une décision datée.

CHAPITRE 04

Ce que montrent les publications conservées du dark web

CE CHAPITRE RÉPOND À LA QUESTION

Quelles offres justifient une validation, et quelles conclusions restent indisponibles ?

7757

enregistrements de forum conservés, sur une période partielle

4.1 Périmètre étudié 27
4.2 Plateformes, langues et dernière quinzaine 28
4.3 Objets proposés et sens défensif 29
4.4 Six études de cas 30
4.5 Quatre autres fiches de prudence 40
4.6 Liens, prix et revendications 41
4.7 Autres revendications conservées séparément 41

CHAPITRE 04

Ce que montrent les publications conservées du dark web

EN BREF

L'ensemble conservé compte 7757 enregistrements de forum, dont 432 datés de la dernière quinzaine. Les offres sélectionnées concernent les accès privilégiés, la santé, des fichiers d'identité, les télécommunications, une série attribuée à un prestataire et des documents d'ingénierie. Certaines dates et authenticités restent incertaines. Ces exemples n'établissent ni répartition criminelle nationale ni nouveaux incidents vérifiés. Validez provenance, accès actuel et champs réels avant de choisir la réponse.

4.1 Périmètre étudié

La vue étiquetée France contient 841760 enregistrements datés dans la période nominale. Ce total ne dénombre ni publications malveillantes, ni ciblages, ni victimes, ni incidents. L'ensemble de forums conservé contient 7757 identifiants d'enregistrement, dont 432 datés du 9–22 novembre [S1]. Il constitue un sous-ensemble des 7758 enregistrements de forums de la vue étiquetée : octobre conserve 1849 des 1850 enregistrements de forums étiquetés, une entrée d'octobre n'étant pas conservée.

Élément	Définition
Population étiquetée France	841760 enregistrements associés à la France dans la période
Forums conservés	7757 identifiants d'enregistrement, dont échanges et réponses
Dernière quinzaine	432 identifiants conservés datés du 9–22 novembre
Temps	Date de publication enregistrée ; dernier jour civil partiel
Limite géographique	Une association au pays n'établit ni ciblage ni localisation des victimes
Répétitions	Des identifiants peuvent représenter un même message sous-jacent
Incertitude des dates	Certaines dates de publication contredisent d'autres dates conservées ; elles ne datent ni vol ni première circulation
Validation	Accès, fichiers, état des cartes et populations annoncés non testés
Usage analytique	Cas sélectionnés et questions défensives, sans estimation nationale des familles criminelles

Étiquettes nationales et forums conservés décrivent des populations différentes

Données de chaque population observée



Source : contenus retenus liés à la France, 1 janvier-22 novembre 2026 ; dernier jour partiel. Les données étiquetées France et les forums conservés sont des populations distinctes ; la quinzaine finale est un sous-ensemble des forums. Les publications ne sont pas des incidents [S1].

Le volume étiqueté ne fournit pas une fourchette nationale d'activité criminelle pertinente. Informations, échanges et associations géographiques sans rapport peuvent y contribuer. Les cas conservés n'établissent pas la répartition des activités criminelles dans cet ensemble plus large.

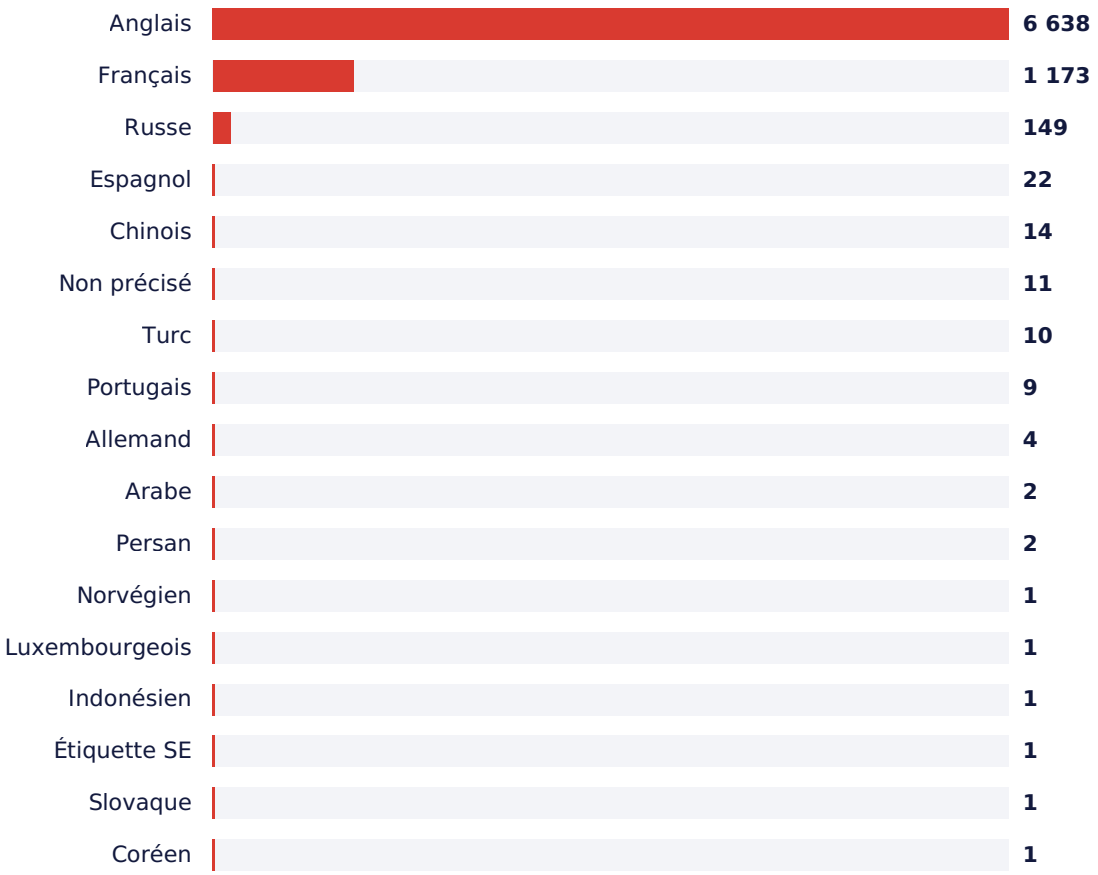
4.2 Plateformes, langues et dernière quinzaine

La vue étiquetée compte 833 822 enregistrements Telegram, 7 758 de forums, 109 Discord, 71 de partage de texte et 0 de sources onion. Sur ces 7 758 enregistrements de forums étiquetés, 7 757 figurent dans l'ensemble conservé, une entrée étiquetée d'octobre n'étant pas conservée (1 849 sur 1 850) [S1].

L'ensemble conservé porte 6 638 étiquettes anglaises, 1 173 françaises et 149 russes. Les autres langues ou l'absence de langue représentent 80 occurrences. Ces étiquettes se recoupent et ne répartissent pas les 7 757 enregistrements en groupes disjoints [S1].

Les étiquettes de langue se recoupent dans les seuls forums conservés

Étiquettes linguistiques de 7 757 données de forum conservées ; chevauchements possibles



Source : contenus retenus liés à la France, 1 janvier-22 novembre 2026 ; dernier jour partiel. Les données étiquetées France et les forums conservés sont des populations distinctes ; la quinzaine finale est un sous-ensemble des forums. Les publications ne sont pas des incidents [S1].

La langue n'établit ni nationalité, ni localisation, ni affiliation étatique. Une réponse peut contester une revendication, demander un accès ou n'apporter aucun élément nouveau. Réponse et republication ne doivent pas automatiquement devenir des incidents supplémentaires.

Les 432 enregistrements de la dernière quinzaine apportent une population de forums datée. Ils n'établissent ni date de vol, ni première apparition d'une offre, ni couverture complète de l'activité criminelle française. Les divulgations publiques récentes restent distinctes au chapitre 6.

Une revendication du 15 novembre concernant un prestataire local dit que plusieurs ressources prétendument accessibles n'ont jamais été téléchargées. Une offre du 21 novembre vise des accès privilégiés dans la construction. Aucune n'établit accès actuel ou copie des données. Une offre hôtelière du 10 novembre décrit une extraction ancienne : publicité récente ne signifie pas nouvel incident [S1].

4.3 Objets proposés et sens défensif

Les exemples sont qualitatifs. Leur sélection n'estime pas la taille relative des marchés criminels français [S1].

Objet proposé	Exemple	Ce qui est observé	Ce qui n'est pas établi
Accès privilégié	Organisation culturelle	Capacités administratives étendues et prix demandé	Accès actuel, maîtrise de tous les systèmes ou vente

Objet proposé	Exemple	Ce qui est observé	Ce qui n'est pas établi
Données de santé et accès optionnel	Grand ensemble de santé	Fichiers, secrets et accès présentés séparément	Source unique, patients distincts ou accès valide
Fichiers d'identité	Attributions et volumes concurrents	Offres et contestation de provenance par un participant	Intrusion confirmée dans l'institution nommée par le vendeur
Données clients télécoms	Plusieurs offres et une republication explicite	Champs d'identité, contact et banque proposés	Nouveau vol, opérateur commun ou clients distincts
Plateforme métier partagée	Diffusions avec une même étiquette de série	L'auteur revendique un lien de plateforme	Cause générale vérifiée ou tous les clients touchés
Documents de projets	Archives d'un prestataire avec noms de projets clients	Fichiers proposés sous ces noms	Intrusion chez les clients ou dans leurs systèmes industriels

4.4 Six études de cas

A

CAS A

Une offre d'accès privilégié étendu

Fiche de preuve B01 | 19 mars 2026 | Forum de fuites | Accès

Accès revendiqué non vérifié

REVENDICATION

Un pseudonyme proposait l'accès à une organisation culturelle : identité, infrastructure virtuelle, administration cloud, messagerie et sécurité des postes. Le prix demandé était de 2.5K USD [S1].

OBSERVATION

Deux annonces presque identiques sous le même pseudonyme partagent un long inventaire de privilèges. B01 conserve le prix ; B02 conserve la revendication sur la sécurité des postes.

ÉTABLI

La même identité de forum a publié deux offres similaires. Cela ne démontre ni seconde intrusion ni second opérateur.

ALTERNATIVES

Vendeur d'accès authentique, revendeur, promotion copiée ou fabrication. La liste des capacités ne les distingue pas.

LIMITES

L'accès n'a pas été testé et l'organisation victime n'est pas établie. Le pseudonyme public est généralisé car l'original contient une formulation inadaptée.

RÉPONSE

En cas de correspondance interne, examinez ensemble identité privilégiée, infrastructure virtuelle et administration de sécurité. Validez les accès de reprise indépendamment de cet ensemble administratif revendiqué.

En définitive

Validez privilèges et reprise avant de prendre une liste de capacités pour un fait.

Fiche de preuve B01 — 19 mars 2026

Persona A | Forum de fuites | Forum | Anglais

ORIGINAL

Price: 2.5K USD

TRADUCTION

Prix : 2 500 USD

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Le vendeur proposait un accès prétendument actif à l'administration des identités, aux serveurs virtuels, à la messagerie et à la sécurité des postes. Le prix est un montant demandé, sans preuve de transaction.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B02 — 19 mars 2026

Persona A | Forum de fuites | Forum | Anglais

ORIGINAL

Full access to the EDR Security Center

TRADUCTION

Accès complet au centre de sécurité EDR

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Une seconde publication presque identique sous le même pseudonyme annonçait le contrôle de l'administration de la sécurité des postes. Elle montre une republication, sans établir une autre compromission ou un second opérateur.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Persona A

Pseudonyme d'origine généralisé

Identité de forum proposant un accès | Non établi

EN FRANCE, 2026

19 mars

Date enregistrée d'annonces similaires d'accès privilégié, B01–B02

CIBLES REVENDIQUÉES

Une organisation culturelle, selon la revendication

DANS LEURS PROPRES MOTS

"Full access to the EDR Security Center" B02

VU DANS LES SOURCES PUBLIQUES

NOTRE ÉVALUATION

Deux annonces similaires sous une identité de forum. Accès, vente et identité de la victime ne sont pas vérifiés. Aucune corroboration publique n'est citée dans cette édition.

DEGRÉ DE CONFIANCE

Élevée pour la conservation des annonces ; capacités et chronologie incertaines

B

CAS B

Fichiers de santé et accès d'entreprise vendus séparément

Fiche de preuve B03 | 17 juin 2026 | Forum de fuites | Santé

Données et accès non vérifiés

REVENDICATION	Un vendeur annonçait 533 GB et 1167076 fichiers : santé, code source, certificats et identifiants. Un accès d'entreprise était proposé moyennant un supplément [S1].
OBSERVATION	L'annonce distingue un ensemble de données d'une capacité d'accès supposée. Un nombre de fichiers et un accès actif sont des objets différents.
ÉTABLI	Le vendeur a formulé ces revendications. Fichiers, institutions sources, volumes et accès n'ont pas été authentifiés indépendamment.
ALTERNATIVES	Fichiers anciens mélangés, données de plusieurs parties, archives d'un revendeur, contenu gonflé ou extraction récente authentique.
LIMITES	Le nombre de fichiers n'est pas celui des patients. Aucun lien n'est établi avec les divulgations officielles distinctes de logiciels médicaux du chapitre 5.
RÉPONSE	Examinez séparément documents exposés, certificats ou autres secrets et accès actuel. Associez le responsable des données avant de déduire ce que contient réellement un fichier de santé.

En définitive

Fichiers, patients et accès actuel exigent des validations distinctes.

Fiche de preuve B03 — 17 juin 2026

Zab26 | Forum de fuites | Forum | Anglais

ORIGINAL

I can include corporate access if you pay extra.

TRADUCTION

Je peux inclure un accès à l'entreprise moyennant un supplément.

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Le vendeur revendiquait 533 Go répartis dans 1 167 076 fichiers, dont des documents de santé et des identifiants, avec un accès d'entreprise proposé en supplément. La validité de l'accès, l'exhaustivité et les volumes annoncés n'ont pas été vérifiés.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

CAS C

C

Noms de services d'identité et volumes incompatibles

Fiche de preuve B04 | 7 janv. 2026 | Forum de fuites | Services d'identité

Attribution contestée

REVENDICATION	Deux annonces reprenaient des noms apparentés de services d'identité, avec 127 millions et 13 millions d'enregistrements. Un participant contestait séparément une attribution institutionnelle [S1].
OBSERVATION	B04 conserve la contestation ; B05 et B06 les offres concurrentes. Une contestation reste aussi une déclaration non vérifiée.
ÉTABLI	Un thème commun et des descriptions contradictoires. Ces publications ne démontrent ni fichiers identiques, ni opérateur commun, ni institution réelle d'origine.
ALTERNATIVES	Informations anciennes renommées, sources fusionnées, sous-ensembles différents, lignes répétées ou fichier authentique présenté de façon trompeuse.
LIMITES	Les deux volumes ne peuvent être rapprochés ni additionnés. Un grand nombre n'est pas automatiquement impossible : il peut compter des lignes et non des personnes.
RÉPONSE	Vérifiez en privé la provenance et la pertinence des champs. Des détails d'identité statiques ne suffisent pas pour récupérer un compte ; le nom institutionnel donné par le vendeur n'est pas une confirmation.

En définitive

Un nom institutionnel commun ne démontre pas l'origine.

Fiche de preuve B04 — 7 janv. 2026

suicid | Forum de fuites | Forum | Anglais

ORIGINAL

its attributed name may simply be false

TRADUCTION

le nom qui lui est attribué peut tout simplement être faux

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Un participant contestait l'attribution d'un fichier présenté comme issu d'un service d'identité et avertissait qu'un exfiltrateur pouvait lui donner le nom d'un organisme plus connu. Il s'agit de son appréciation, sans conclusion officielle.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B05 — 17 avr. 2026

RubiconH4ck | Forum de fuites | Forum | Anglais

ORIGINAL

the price is $4K negotiable

TRADUCTION

le prix est de 4 000 dollars, négociable

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Un vendeur proposait un fichier présenté comme provenant d'un service municipal d'identité, avec 127 millions d'enregistrements datés de 2025. La publication établit une offre de vente et une liste de champs, sans prouver l'origine revendiquée.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B06 — 12 sept. 2026

lauraallen | Forum de fuites | Forum | Anglais

ORIGINAL

13 Million

TRADUCTION

13 millions

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Une autre annonce reprenait cette attribution institutionnelle tout en revendiquant 13 millions d'enregistrements. Les publications conservées ne permettent pas de rapprocher ces volumes ; ils ne doivent pas être additionnés.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

CAS D

D

Données télécoms et republication explicite

Fiche de preuve B07 | 9 janv. 2026 | Forum de fuites | Télécommunications

Revendications et republication explicite

REVENDICATION	Des annonces distinctes décrivaient des dossiers clients et des coordonnées bancaires. L'une annonçait 150 782 lignes, une autre des archives de 80.9 GB. Une troisième disait explicitement republier des données de fin 2025 [S1].
OBSERVATION	B07, B08 et B09 sont regroupées par secteur, pas par incident commun démontré. L'ancienneté indiquée dans B09 est celle de l'auteur.
ÉTABLI	Des informations télécoms ont été proposées et un auteur a décrit une republication. Cela n'authentifie pas indépendamment l'âge ou la provenance.
ALTERNATIVES	Anciens dossiers, données d'un autre service, archives se recoupant, annonces copiées ou incident récent distinct.
LIMITES	Pseudonymes et tailles différents ne comptent pas des incidents ou clients uniques. Aucun lien n'est affirmé avec l'événement ancien à l'origine de la sanction télécoms de janvier.
RÉPONSE	Validez actualité et recoupements avant d'agir sur les comptes. Préparez les équipes clients à des appels convaincants connaissant opérateur, identité ou coordonnées bancaires.

En définitive

Validez ancienneté et recoupements avant de compter un nouvel incident.

Fiche de preuve B07 — 9 janv. 2026

near | Forum de fuites | Forum | Français

ORIGINAL

Après plusieurs demandes, voici 150 000 IBAN provenant de [victim domain].

TRADUCTION

After several requests, here are 150,000 IBANs from [victim domain].

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation. La traduction fournie est en anglais ; l'original est en français.

Ce que nous pouvons établir
L'auteur affirmait partager 150 782 lignes associant identité, coordonnées et données de compte bancaire. Il s'agit du contenu annoncé ; les enregistrements et leur provenance n'ont pas été authentifiés.

Ce qui n'est pas établi
Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B08 — 4 mai 2026

OverSec | Forum de fuites | Forum | Anglais

ORIGINAL

We have the honor of unveiling our first claim

TRADUCTION

Nous avons l'honneur de présenter notre première revendication

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir
Un vendeur attribuait à un opérateur un fichier JSONL de 80,9 Go et indiquait une date de mai 2026 dans l'annonce. La date de publication et celle attribuée au fichier sont deux informations distinctes, non vérifiées.

Ce qui n'est pas établi
Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B09 — 9 mai 2026

NormalLeVrai | Forum de fuites | Forum | Anglais

ORIGINAL

I'm just reposting 27.471.090 clients dating from the end of 2025.

TRADUCTION

Je ne fais que republier 27 471 090 clients datant de fin 2025.

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir
L'auteur présentait explicitement le fichier comme une republication d'archives clients de fin 2025. Il relève de la circulation observée en 2026, sans établir une nouvelle intrusion en 2026.

Ce qui n'est pas établi
Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Une réponse de forum décrivait une collection télécom annoncée comme des données de 2024. C'est une contre-revendication sur la provenance, pas une date d'acquisition établie indépendamment [S1].

CAS E

E

Une série revendiquée sur une plateforme partagée

Fiche de preuve B10 | 3 sept. 2026 | Forum de fuites | Prestataires

Série revendiquée : attribution corrigée

REVENDICATION	Un pseudonyme présentait plusieurs diffusions dans le matériel professionnel comme une série issue d'une plateforme CRM commune. Une publication corrigeait explicitement une attribution à une entreprise [S1].
OBSERVATION	B10 et B13 conservent le lien revendiqué ; B11 la correction ; B12 un nombre de fichiers. Cela étaye le récit de l'auteur, pas une cause vérifiée.
ÉTABLI	Le pseudonyme employait une étiquette commune et a changé une attribution. L'organisation nommée par erreur ne doit pas devenir une victime supplémentaire.
ALTERNATIVES	Incident réel chez un prestataire commun, étiquette copiée, exports clients sans lien ou mélange de contenus authentiques et mal attribués.
LIMITES	Volumes et nombres de fichiers ne sont pas vérifiés. Le même pseudonyme reste une identité de forum, pas un individu établi ni une intrusion générale dans la plateforme.
RÉPONSE	Suivez séparément l'exposition réelle et les corrections de chaque client. Examinez la dépendance commune uniquement si des éléments indépendants du prestataire ou du client l'étayent.

En définitive

Conservez les corrections et vérifiez chaque dépendance client.

Fiche de preuve B10 — 3 sept. 2026

updap | Forum de fuites | Forum | Anglais

ORIGINAL

This leak is part of a many leaks

TRADUCTION

Cette fuite fait partie de nombreuses fuites

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

La publication rattachait explicitement une diffusion annoncée de 44 Go à une série nommant une plateforme partagée. Elle atteste l'étiquette employée par l'auteur, sans vérifier une compromission de la plateforme ou de chaque client.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B11 — 3 sept. 2026

updap | Forum de fuites | Forum | Anglais

ORIGINAL

Old thread is deleted.

TRADUCTION

L'ancien fil est supprimé.

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

L'auteur corrigeait l'attribution à une entreprise et indiquait qu'un fil antérieur avait été supprimé. Cette correction doit accompagner la diffusion annoncée de 22,25 Go ; l'organisme nommé par erreur ne doit pas devenir une victime supplémentaire.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B12 — 3 sept. 2026

updap | Forum de fuites | Forum | Anglais

ORIGINAL

Files: 323 388

TRADUCTION

Fichiers : 323 388

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Une autre publication sous le même pseudonyme annonçait 13,48 Go et 323 388 fichiers pour une entreprise de location de matériel, avec la même étiquette de série. Les volumes sont déclaratifs et peuvent comprendre des doublons ou des pièces jointes.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B13 — 28 sept. 2026

updap | Forum de fuites | Forum | Anglais

ORIGINAL

Size: 200 GB

TRADUCTION

Taille : 200 Go

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Le même pseudonyme annonçait une diffusion de 200 Go pour un fournisseur de matériel, également présentée comme faisant partie de cette série. Cette étiquette commune ne suffit pas à établir un mécanisme d'intrusion partagé.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

CAS F

F

Fichiers d'un prestataire et accès industriel sont distincts

Fiche de preuve B14 | 4 janv. 2026 | Forum de fuites | Ingénierie

Vente documentaire non vérifiée

REVENDICATION	Un vendeur annonçait environ 340 GB de fichiers d'un prestataire d'ingénierie, avec des dossiers de projets clients dans la construction et l'énergie. Il disait aussi proposer ces données sur un autre forum [S1].
OBSERVATION	L'annonce contient des noms de projets et une affirmation de diffusion ailleurs. Ni l'un ni l'autre n'authentifie les fichiers ou leur premier détenteur.
ÉTABLI	Une revendication de vente de documents. Un nom de dossier ne démontre pas une intrusion chez le client correspondant.
ALTERNATIVES	Archives anciennes, export d'un service de partage de projets, annonce copiée ou divulgation actuelle authentique.
LIMITES	L'actualité de l'intrusion n'est pas établie. L'offre ne démontre aucun accès à des installations, contrôleurs ou systèmes opérationnels.
RÉPONSE	Revoyez accès documentaires, droits d'export et conservation chez les prestataires. Séparez confidentialité et sécurité industrielle tant qu'aucun élément technique ne les relie.

En définitive

Un dossier de projet ne démontre pas l'accès au client ou à ses installations.

Fiche de preuve B14 — 4 janv. 2026

Angel_Batista | Forum de fuites | Forum | Anglais

ORIGINAL

This data is also sold on the other breach by me

TRADUCTION

Ces données sont également vendues par moi sur l'autre forum

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Le vendeur annonçait environ 340 Go de fichiers d'un prestataire, avec des dossiers prétendument liés à des projets de clients dans l'énergie et la construction. Les noms de dossiers et les volumes revendiqués n'établissent ni une compromission des clients ni celle de systèmes industriels.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

4.5 Quatre autres fiches de prudence

Une offre d'accès à une plateforme publique prétend s'appuyer sur un contact interne, sans preuve d'accès validée. Son rôle est généralisé. La revendication ne confirme pas l'existence d'un complice [S1].

Une autre annonce regroupe des adresses par domaines de service public, avec des champs relevant d'un contexte d'adhésion différent. Une adresse professionnelle dans un fichier ne démontre pas une intrusion dans le réseau de l'employeur [S1].

Fiche de preuve B15 — 30 janv. 2026

kazutlg | Forum de fuites | Forum | Anglais

ORIGINAL

With the help of my insider, we propose a full access on government panel

TRADUCTION

Avec l'aide de mon contact interne, nous proposons un accès complet à un panneau gouvernemental

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

Le vendeur revendiquait un accès à un panneau grâce à un contact interne et des informations financières personnelles à la demande. Le texte conservé ne fournit ni preuve d'accès validée ni confirmation officielle ; il peut seulement illustrer une revendication commerciale non vérifiée.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B16 — 20 févr. 2026

HexDex | Forum de fuites | Forum | Anglais

ORIGINAL

Totally 8861 Unique Email agents

TRADUCTION

Au total, 8 861 adresses électroniques uniques d'agents

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir

L'auteur regroupait les adresses selon des domaines de messagerie gouvernementaux. Des champs visibles renvoient à des adhésions et licences sportives ; un domaine de messagerie ne prouve pas une intrusion dans un réseau public. Les sous-totaux annoncés ne doivent pas être ajoutés au total présenté comme unique.

Ce qui n'est pas établi

Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Une annonce de registre professionnel mentionne elle-même des coordonnées publiques ou administratives. Elle ne doit pas devenir une fuite de patients sans contrôle de provenance. Une autre offre revendique des dossiers d'aide aux ménages couvrant environ 2012–2026 ; durée historique et nombres non vérifiés comptent [S1].

Fiche de preuve B17 — 23 juin 2026

Edric | Forum de fuites | Forum | Anglais

ORIGINAL

Public or administrative contact fields (where applicable)

TRADUCTION

Coordonnées publiques ou administratives, le cas échéant

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir
La publication décrivait un registre professionnel d'environ 12 millions d'entrées, avec identifiants d'établissements et champs administratifs. Elle mentionnait elle-même des coordonnées publiques. Sans vérification de provenance, elle ne doit pas être présentée comme une fuite confirmée de données de patients.

Ce qui n'est pas établi
Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Fiche de preuve B18 — 4 mars 2026

HexDex | Forum de fuites | Forum | Anglais

ORIGINAL

over the period from ~2012 to 2026.

TRADUCTION

sur la période allant approximativement de 2012 à 2026.

Note. Date de publication enregistrée ; chronologie incertaine. L'extrait est une revendication, pas une confirmation.

Ce que nous pouvons établir
Le vendeur revendiquait des informations sur 659 658 familles et 1 462 485 personnes, couvrant une longue période. Ce sont des volumes déclaratifs, sans validation du nombre de personnes touchées ni du caractère nouveau des données en 2026.

Ce qui n'est pas établi
Authenticité, accès actuel, origine, personnes distinctes et vente réalisée non établis.

Ces exemples montrent des problèmes d'attribution, d'unité et d'âge plus importants que le volume affiché. Ils ne démontrent pas que chaque offre contestée est fausse.

4.6 Liens, prix et revendications

Une longue phrase commune peut étayer un lien entre annonces. Elle ne prouve ni identité des fichiers, ni auteur du vol, ni transfert réalisé. Un vendeur disant proposer ailleurs ses données formule une revendication de circulation, jusqu'à corroboration indépendante.

Les exemples de 2.5K USD et $4K négociables sont des prix demandés [S1]. Ils ne constituent ni indice français des prix, ni valeur des données, ni somme payée, ni perte métier estimée.

La réponse adaptée est une tâche de validation avec un critère de clôture. Consignez correspondance des données, activité du compte, besoin de révocation des sessions et provenance vérifiée. Les éléments anciens ou sans correspondance nécessitent aussi une décision documentée.

4.7 Autres revendications conservées séparément

Le corpus contient aussi les revendications non vérifiées ci-dessous. Elles élargissent les questions défensives sans établir de nouvelles victimes confirmées ni d'opérateurs communs [S1].

Objet revendiqué	Contenu annoncé	Incertitude	Question défensive
Dossiers immobiliers	Un pseudonyme se présentant comme hacktiviste annonçait images de biens, contrats et données d'identité ou de contact	Motif et fraîcheur restent les assertions du posteur ; aucun fichier ou accès validé	Quels dossiers immobiliers et clients les utilisateurs externes peuvent-ils exporter ?
Registre d'entreprises	Accès privilégié au transfert et grande collection de représentants	Les champs décrits peuvent recouper des informations publiques	Peut-on distinguer données confidentielles et données publiques par leur provenance ?
Logiciel d'ameublement	Données clients, commandes, comptabilité, courriels et empreintes de secrets	Périmètre du vendeur et validité actuelle non vérifiés	Quels comptes couvrent commerce et comptabilité ?
Service culturel et médiatique	Profils, liens d'accès, facturation et journaux d'audit	Objet annoncé plus large qu'une liste clients, mais non vérifié	Peut-on révoquer séparément liens et sessions ?
Collection étiquetée commerce	Étiquette du vendeur associée à des champs professionnels	Le schéma n'étaye pas clairement l'origine commerciale annoncée	Le schéma interne correspond-il réellement ?
Collection étiquetée service mobile	Champs de prospects, appels, équipes et sites sources	Ils peuvent décrire la prospection plutôt qu'un système d'abonnés	Quel prestataire ou quelle campagne détient les champs correspondants ?
Compilation de contacts français	Affirmation explicite d'agrégation de plusieurs bases	L'agrégation n'établit pas une intrusion d'origine commune	Peut-on reconnaître en privé répétitions et provenance historique ?
Applications sportives et de logement	Un auteur alléguait une faiblesse commune de gestion de contenu dans deux services	Ni la faille ni les résultats d'accès n'ont été validés indépendamment	Des contrôles internes autorisés retrouvent-ils une dépendance commune ?
Données d'abonnés mobiles	Abonnés, déverrouillage, facturation et jetons potentiellement actifs	Jetons et origine non testés ; une ligne n'est pas nécessairement un client	Peut-on révoquer anciens jetons et liens de facturation ?
Données liées à l'assurance	Accès employé, données et demande d'extorsion	Accès et délai restent les assertions du demandeur	Les sessions employées et exports tiers sont-ils visibles ensemble ?
Fichiers d'un fournisseur aéronautique	Commandes, expédition, données de gestion et fichiers internes	Aucun accès aux systèmes d'ingénierie ou d'exploitation démontré	Quels comptes commerciaux exposent le contexte des projets fournisseurs ?
Accès chez un fournisseur cloud	Compte parent supposé avec portée étendue en aval	Les populations annoncées n'établissent pas l'accès à chaque client	Peut-on vérifier séparément délégation administrative et séparation des clients ?

Une autre annonce proposait des services d'identité d'appelant et de messagerie pour des destinations françaises. C'est un signal de services facilitant la fraude, sans preuve d'intrusion dans une organisation française. Ces observations n'autorisent ni tests de systèmes tiers ni contact avec un vendeur [S1].

POINTS À RETENIR

01

Utilisez ces forums pour des validations précises, pas pour estimer un taux national de menace.

02

Séparez source, âge, unité et validité de l'accès dans chaque annonce.

03

Une étiquette commune ou un dossier client ne démontre ni opérateur commun ni intrusion chez un client.

CHAPITRE 05

Incidents et revendications par secteur

05

CE CHAPITRE RÉPOND À LA QUESTION

Quels cas sectoriels établissent un mécanisme que les défenseurs peuvent tester ?

10

contextes sectoriels et de services avec des limites différentes

5.1 Lire les cas sélectionnés 45
5.2 Administration : identité et accès applicatif 46
5.3 Autres services administratifs : des événements distincts 48
5.4 Éducation et recherche : dates et ancienneté 49
5.5 Santé : périmètre du prestataire et chiffres revendiqués 50
5.6 Courrier, prestataires et disponibilité 52
5.7 Banque, identité et tourisme 53
5.8 Services professionnels et scripts tiers 53
5.9 Autres divulgations de prestataires et de services clients 53
5.10 Les autres revendications récentes 54
5.11 Autres divulgations et limites 54

CHAPITRE 05

Incidents et revendications par secteur

EN BREF

Les déclarations officielles décrivent abus de comptes, accès excessifs, faiblesses logicielles, prestataires et perturbations physiques. Elles conservent aussi des exclusions. Les dossiers de comptes ne dénombrent pas les personnes, les dossiers de support n'établissent pas une exposition plus large, et un historique privé protégé n'est pas un échec général de messagerie. Choisissez une réponse proportionnée selon le mécanisme et le périmètre réellement divulgués.

5.1 Lire les cas sélectionnés

Les cas distinguent déclaration d'une organisation, enquête d'autorité, presse citant une déclaration et marché non vérifié. Une publication dans la période n'établit pas un début d'incident en 2026.

Les cas sélectionnés incluent aussi des revendications de moniteurs et des éléments encore évalués. Une décision enregistrée ne rend pas une revendication vraie. Aucun total n'est un recensement d'incidents français ou de personnes distinctes.

Secteur ou service	Éléments de cette édition	Limite	Première réponse
Administration	Abus de comptes, défauts d'autorisation et extractions dans les rapports officiels	Services et dates distincts ; aucun acteur commun déduit	Valider accès, droits et exports [S6][S7][S8]
Éducation et recherche	Personnel, élèves, annuaires et anciens dossiers de paie	Données anciennes et actuelles peuvent se recouper	Revoir accès délégués et conservation [S6][S34][S38][S39]
Santé	Incidents de logiciels médicaux et de radiologie	Notes administratives et dossier médical complet diffèrent	Identifier les champs chez le prestataire et les accès distants [S36][S51]
Banque et finance	Accès aux données financières et opérations frauduleuses distincts	Les dossiers financiers ne démontrent pas une intrusion dans chaque banque	Associer validation d'identité et paiements [S35][S49][S50][S78]
Courrier et services métiers	Mises à jour DDoS et incident distinct de destinataires	Disponibilité et confidentialité sont deux cas	Exercer continuité et notification du sous-traitant [S12][S13][S31]
Commerce et alimentaire	Constats officiels sur les contrôleurs de froid	Effets signalés par les autorités	Vérifier accès distants et alarmes indépendantes [S10]
Tourisme et loisirs	Divulgation de réservations citée par la presse	Dossiers de réservation et voyageurs distincts diffèrent	Protéger accès partenaires et communications de réservation [S41]

Secteur ou service	Éléments de cette édition	Limite	Première réponse
Sport et associations	Incidents d'adhésion et de permis	Organisations et populations différentes	Revoir exports et accès des comptes [S32][S6][S7]
Services professionnels et technologie	Déclaration de système interne et scripts tiers	Exposition possible et vol établi diffèrent	Revoir dépendances et sessions [S52][S53]
Énergie et infrastructures connectées	Ciblage hydroélectrique concomitant dans le récit officiel	Effet différent du froid	Associer exploitation et sécurité physique [S10]

5.2 Administration : identité et accès applicatif

CAS G

Données fiscales sur des périmètres distincts

Administration

Enquête officielle

DIVULGATION

L'ANSSI publie son enquête le 29 septembre sur des activités de mai à août. Elle distingue le périmètre fiscal du périmètre cadastral [S8].

ÉTABLI

L'enquête décrit des identifiants valides volés, des applications sensibles accessibles au-delà des frontières prévues et des lacunes de détection. Elle relève un accès latéral depuis une autre administration.

UNITÉS

Le bilan de septembre indique environ 353 000 usagers fiscaux particuliers, 252 000 professionnels et 434 000 usagers du cadastre. Ces populations ont des recoupements inconnus [S6].

ALTERNATIVES ET LIMITES

Ces chiffres ne s'additionnent pas pour compter des résidents uniques. Une annonce ultérieure n'établit pas indépendamment un nouvel accès ou une nouvelle extraction.

RÉPONSE

Testez si un compte externe ou partenaire valide peut franchir sa limite prévue. Corrélez connexion, activité applicative et exports, y compris sur les systèmes absents de la surveillance courante.

En définitive

Encadrez l'usage des données après connexion et au-delà des frontières de confiance.

Un identifiant légitime et une action légitime sont différents. Le récit officiel dit que les identifiants étaient valides. Il ne dit pas que les responsables des données avaient autorisé les extractions [S8].

CAS H

H ■ Annuaire professionnel après validation du second facteur

Administration

Récit officiel : second facteur validé

DIVULGATION	Le bilan du 12 novembre décrit une annonce du 8 octobre et une extraction du 26 septembre. L'offre concernait plus de 60 000 dossiers d'agents et professionnels [S7].
ÉTABLI	Le récit officiel indique l'usage abusif du compte d'un agent avec validation du second facteur SMS. Il décrit la révocation et la poursuite de l'enquête.
ALTERNATIVES ET LIMITES	Il ne précise pas exactement comment le second facteur a été obtenu ou approuvé. Il n'établit pas une attaque contre tous les comptes du personnel.
RÉPONSE	Examinez validations MFA, récupération, sessions et accès à l'annuaire. Un changement de mot de passe ne suffit pas à clôturer le cas.

En définitive

Examinez sessions et récupération autant que les mots de passe.

Ce cas diffère de l'ancien événement touchant les demandeurs d'emploi derrière la sanction de janvier. Annuaires professionnels, demandeurs d'emploi et populations historiques ne doivent pas être fusionnés [S7][S15].

CAS I

I ■ Aides aux vacances, accès partenaires et défaut d'autorisation

Administration

Récit officiel : dossiers et personnes distincts

DIVULGATION	Le bilan d'octobre indique qu'une vente a déclenché la détection le 9 octobre. L'extraction automatisée est datée du 8 au 10 octobre [S7].
ÉTABLI	Le récit associe identifiants partenaires volés sans MFA et défaut d'autorisation sur les objets. Il indique près de 1.2 million de dossiers, avec prestations et identités d'enfants.
EXCLUSIONS	La source exclut données bancaires et mots de passe. Les dossiers ne sont pas des personnes uniques ; un ménage peut apparaître plusieurs fois.
LIMITES	Le service était hors ligne dans l'attente de protections. Cela ne signifie pas que toutes les applications de l'organisation élargie étaient touchées.
RÉPONSE	Testez les droits par dossier avec un compte partenaire de test approuvé. Examinez les extractions automatisées, imposez une authentification forte et vérifiez les protections avant réouverture.

En définitive

Testez autorisations par objet et accès partenaires avant réouverture.

5.3 Autres services administratifs : des événements distincts

Les bilans officiels décrivent les services supplémentaires suivants. Le tableau conserve les formulations provisoires et les unités mixtes [S6][S7].

Rôle du service	Contexte	Ce que dit la source	Limite
Bibliothèque administrative	Octobre ; publication le 12 novembre	Des comptes techniques volés pourraient exposer les données d'environ 100 utilisateurs ; élévation de privilèges bloquée	Enquête en cours
Inscription à un examen de permis	4 octobre ; publication le 12 novembre	Défaut d'autorisation exposant plus de 1 000 personnes, dont des mineurs	Distinct de la fédération de janvier
Portails de gestion d'aides	Août ; mise à jour en novembre	Deux portails avec extraction et corrections	Aucun lien établi avec les autres incidents de l'agence
Rémunération de stagiaires	30 septembre ; revendication en octobre	Compte usurpé et faille ; 30 500 usagers	Portail et incident distincts
Application de service public A	Août ; publication en septembre	Abus de compte professionnel exposant des coordonnées	Les coordonnées ne dénombrent pas des personnes distinctes
Application de support d'un service public	Fin juin–juillet ; publication en septembre	Sous-traitant : 136 usagers et 213 demandes de support	Aucune exposition plus large des données opérationnelles établie
Messagerie et échanges douaniers	Lien établi en août ; publication en septembre	Trois boîtes professionnelles et un service d'échange associé	Pas d'affirmation sur tous les systèmes douaniers
Contrôle technique environnemental	Bilan de septembre	Compte abusé et faiblesse permettant d'énumérer 22 000 agents ou organismes habilités	Unité mixte, pas des personnes distinctes
Espace ministériel partagé	Détection en août	Plus de 300 comptes et contenus accessibles de messagerie ou fichiers	Contenu encore analysé
Service destiné aux jeunes	Revendication signalée en septembre	Revendication de 275 000 usagers	Périmètre et enquête provisoires
Application liée au logement B	Revendication signalée en août	Revendication non vérifiée d'extraction de données	Périmètre et voie d'accès non confirmés

Rôle du service	Contexte	Ce que dit la source	Limite
Application de service public C	Bilan de septembre	Incident encore évalué	Aucune extraction, voie ou population établie
Correspondance parlementaire	Bilan de septembre	Extraction possible de correspondance	Conditionnel, sans population confirmée
Analyse de recharge électrique	Bilan de septembre	102 000 sessions et environ 100 comptes techniques extraits	Aucune unité n'est un propriétaire de véhicule
Urbanisme	Revendication signalée en août	Extraction revendiquée et accès analytique suspecté	Origine et dates encore examinées
Analyse d'innovation publique	Bilan de septembre	118 comptes applicatifs touchés	Application restreinte, pas toute l'agence
Services d'analyse publics	Bilan de septembre	Deux instances touchées ; données déjà publiques	L'accès applicatif reste pertinent
Qualification professionnelle	Août ; publication en septembre	Exploitation d'une instance analytique et extraction de dossiers	Aucun total de personnes distinctes
Formation agricole	Revendication de début septembre	Données revendiquées sur 5 265 personnes	Enquête en cours

Certaines applications partagent un produit ou une faiblesse générale. Cela n'établit ni opérateur commun ni sensibilité identique. Une instance de données publiques et une application de prestations peuvent nécessiter des décisions de notification différentes.

Le bilan de septembre décrit une exploitation massive touchant neuf instances analytiques ministérielles et nomme CVE-2026-72898 [S6]. La faille et les correctifs ont été vérifiés séparément [S21][S22]. Cela ne valide pas toutes les annonces qui citent le même produit.

Le bilan de novembre donne aussi un exemple d'accès empêché. Des certificats VPN volés ont été identifiés, mais la MFA a empêché la connexion et aucune autre activité malveillante n'a été établie. Il s'agit d'une tentative bloquée, pas d'une intrusion VPN réussie [S7].

En janvier, la presse citait un organisme de cotisations sociales sur l'abus d'identifiants partenaires dans un service de déclarations d'embauche. Elle évoquait 12 millions de salariés potentiellement concernés. L'avis original n'a pas été lu directement ici ; le cas reste attribué avec cette limite [S33].

5.4 Éducation et recherche : dates et ancienneté

Une déclaration ministérielle de mars décrit l'extraction de données d'environ 243 000 agents après usurpation d'un compte externe. Elle précise identité, coordonnées, périodes d'absence sans détail médical et coordonnées professionnelles de tuteurs. Elle n'établit pas l'exposition de dossiers médicaux complets [S38].

Une déclaration d'avril concerne des élèves dans un service auxiliaire d'administration de comptes. L'incident date de fin 2025 et la population exacte restait évaluée. Il ne doit pas devenir un incident vérifié de plusieurs millions de personnes en 2026 [S39].

Le récit estival concerne des incidents dans 25 des 30 académies. Il décrit identifiants valides, comptes privilégiés, nouveaux accès et extractions. Le bilan de novembre signale la poursuite des corrections et aucune nouvelle violation observée depuis septembre dans ce périmètre [S7].

Ces populations ne sont pas automatiquement indépendantes. Un dossier peut apparaître dans une application de personnel, un annuaire et une annonce ultérieure. Le rapport conserve donc les cas sans additionner les chiffres.

En février, la presse technique cite un organisme de recherche sur des personnes payées avant janvier 2007. L'ancienneté est importante. L'incident ne démontre pas que les systèmes de recherche actuels ou tous les salariés actuels ont été touchés [S34].

Une déclaration de messagerie publique en juin décrit un compte abusé et une exposition possible des salons publics et profils de 73 467 agents. Elle indique que l'historique privé chiffré restait protégé. Ce cas est distinct de celui de l'été [S42].

La presse éducative cite en janvier un établissement public d'agronomie sur des perturbations système et messagerie, avec l'impact sur les données encore évalué [S59]. La presse spécialisée cite un autre établissement sur une extraction de septembre dans une application de stages, excluant mots de passe, identifiants de connexion et données bancaires [S60].

La conservation historique est un contrôle actuel. Un ancien fichier de paie peut toujours contenir des informations d'identité utiles. Examinez pourquoi il reste accessible, à qui et selon quelle justification de conservation.

5.5 Santé : périmètre du prestataire et chiffres revendiqués

J

CAS J

Logiciel médical divulgué en février, détecté l'année précédente

Santé

Divulgation officielle d'un incident antérieur

DIVULGATION	La presse technique cite la déclaration du 26 février d'un éditeur médical sur une détection fin 2025. Elle attribue à l'éditeur le constat de consultation ou d'extraction illégale de données de patients [S36].
ÉTABLI	La presse cite l'éditeur sur 1500 médecins utilisateurs touchés. Elle évoque une population de patients bien supérieure : c'est une autre unité et une autre déclaration [S36].

DONNÉES	Des notes administratives non structurées peuvent contenir des informations sensibles. Cela diffère de l'extraction de dossiers médicaux structurés complets, d'ordonnances et de résultats d'analyses.
LIMITES	La publication appartient à la période ; l'incident a commencé avant. Multiplier les médecins ne produit pas un total vérifié de patients.
RÉPONSE	Demandez les champs et les clients concernés. Évaluez les notes non structurées autant que les tables cliniques, et conservez la distinction de dates.

En définitive

Conservez champs, unités et distinction entre incident et divulgation.

Un reportage du 27 février attribue au ministère chargé de la santé une population de près de 15 millions de personnes. C'est un chiffre ministériel rapporté, distinct du nombre de médecins utilisateurs déclaré par l'éditeur et des affirmations sur des dossiers cliniques complets [S75].

K

CAS K

Accès de radiologie et annonce de marché ultérieure

Santé

Mise à jour de l'éditeur ; volume criminel supérieur

DIVULGATION	Un éditeur de radiologie publie une première déclaration le 8 novembre et une mise à jour le 18. Celle-ci décrit une revendication du soir du 17 novembre [S51].
ÉTABLI	L'éditeur indique que les premiers éléments semblent correspondre à l'incident antérieur, avec un périmètre encore examiné. Il décrit l'usage frauduleux d'identifiants clients pour des accès distants.
LIMITE DE REVENDICATION	Selon l'éditeur, l'évaluation actuelle place la population nettement sous le chiffre criminel. Le rapport n'adopte pas les 18 millions de personnes annoncées.
LIMITES	L'éditeur dit n'avoir détecté ni nouvelle intrusion ni nouvelle fuite après endiguement. Cela ne valide pas indépendamment chaque champ annoncé.
RÉPONSE	Identifiez les données réelles, examinez identifiants distants et sessions, puis coordonnez les évaluations individuelles. Des avis clients sans fournisseur nommé ne sont pas automatiquement le même incident.

En définitive

Identifiez les données réelles et accès distants sans adopter les totaux du vendeur.

Plusieurs entrées récentes de moniteurs concernent l'imagerie ou d'anciens fichiers de patients. Leurs liens de source diffèrent. Un avis ne nommant pas l'éditeur doit rester distinct jusqu'à ce que des éléments plus forts établissent la dépendance [S54].

La sanction hospitalière de septembre par la CNIL concerne un incident antérieur. Elle est utile pour les contrôles mais n'ajoute pas une nouvelle intrusion hospitalière survenue en 2026 [S55].

5.6 Courrier, prestataires et disponibilité

CAS L

L

Incident de septembre d'un prestataire de courrier divulgué en novembre

Services métiers

Entreprise et parquet cités par la presse

DIVULGATION	En novembre, la presse cite l'organisation et le parquet de Paris sur un incident de septembre chez un prestataire de courrier professionnel. La population annoncée est de 22 millions de destinataires [S12][S13].
ÉTABLI	Les champs signalés sont noms et adresses postales. La presse cite l'exclusion des coordonnées bancaires et l'information des organisations clientes.
LIMITES	Les destinataires ne sont pas les clients professionnels du prestataire. Son activité documentaire ne démontre pas l'extraction de tous les contenus des documents.
ALTERNATIVES	Un avis client peut décrire cet incident sans intrusion distincte dans ses systèmes. Ces avis n'établissent pas des incidents distincts lorsque la dépendance au prestataire est explicitement établie.
RÉPONSE	Les responsables de traitement doivent identifier leurs dossiers, évaluer le risque et préparer les usurpations postales ou numériques convaincantes. Conservez les mises à jour successives du périmètre prestataire.

En définitive

Un incident prestataire peut imposer plusieurs décisions aux responsables de traitement.

La presse nationale cite un prestataire postal sur une nouvelle perturbation en ligne le 1 janvier et décrit un précédent incident DDoS en décembre 2025. Elle cite le prestataire sur l'absence de fuite. Ce cas de disponibilité n'établit ni n'explique l'incident de septembre sur les destinataires [S31].

5.7 Banque, identité et tourisme

Une notification officielle de février décrit l'accès à un service de données financières avec des identifiants volés, depuis fin janvier. Environ 1.2 million de comptes pourraient être concernés. La source exclut explicitement la consultation de l'identifiant fiscal [S35].

Un service de données financières et les systèmes bancaires sont des surfaces différentes. L'incident peut exposer des identifiants de comptes sans démontrer une intrusion dans la banque du titulaire. Le chapitre 9 développe les questions de fraude et de vérification.

Une mise à jour d'avril du portail de titres indique que 11.7 millions de comptes individuels pourraient être touchés, sous réserve de l'enquête. La source distinguait identité et contact des pièces jointes et données biométriques exclues à ce stade. Le conditionnel doit rester partout [S40].

La divulgation de mai d'un groupe touristique, citée par la presse nationale, concerne 1.6 million de dossiers de réservation. Une revendication criminelle employait un chiffre supérieur et une autre unité. L'exclusion bancaire annoncée ne rend pas les réservations anodines, mais celles-ci ne sont pas des voyageurs uniques [S41].

Le cas bancaire coopératif de novembre figure au chapitre 9. La déclaration du 4 novembre signalait des opérations frauduleuses et des virements retardés, avec des avoirs clients déclarés non affectés [S49]. Son amendement du 18 novembre indiquait que l'attaque provenait de la plateforme d'un prestataire externe et touchait le compte propre de la banque [S78]. Il estimait l'effet sur le résultat à environ 100 millions d'euros [S78]. Ce n'est pas une extension du cas du service de données financières [S49][S50][S78].

5.8 Services professionnels et scripts tiers

La déclaration de novembre d'un groupe d'études confirme un incident interne, une plainte et une enquête externe. Les opérations sont dites non affectées ; les effets possibles sur clients, projets et partenaires restent évalués. Aucun total de vol ni acteur n'est établi [S52].

Un chercheur rapporte séparément du JavaScript malveillant livré à 178 organisations par une plateforme internationale d'expérimentation le 16 novembre. Certaines entreprises françaises apparaissent dans sa recherche. Le nombre est mondial, et la livraison du script ne démontre pas un vol chez chaque visiteur [S53].

Inventoriez les scripts tiers, identifiez qui peut les modifier et examinez les sessions et éléments applicatifs pertinents. Le rapport ne transforme pas une marque citée par un chercheur en victime française officiellement confirmée.

5.9 Autres divulgations de prestataires et de services clients

L'avis d'octobre d'un fournisseur d'énergie concerne un accès inhabituel chez un partenaire commercial, avec un périmètre clients français. Il indique que ses propres systèmes et les données bancaires ne sont pas touchés. Ce cas de données et de partenaire n'est pas industriel [S57].

L'avis de septembre d'un organisme de formation concerne l'extraction possible de données d'environ 1.7 million de personnes via un outil externe d'hébergement. Ses systèmes et services sont déclarés non affectés. Le périmètre reste étudié, avec des données bancaires et de sécurité sociale apparemment exclues [S58].

L'évaluation d'un prestataire doit donc suivre les données et le service réels. Le nom d'une grande maison mère ne démontre pas que tous ses services, opérations industrielles ou entités juridiques ont été touchés.

5.10 Les autres revendications récentes

La clôture conserve d'autres annonces et signalements par rôle. Authenticité, localisation ou déclaration originale restent insuffisamment établies pour nommer ces parties [S54].

Ensemble	Exemples conservés	Limite de statut	Prochaine question
Commerce et consommation	Électronique, plein air, repas, spécialistes et rénovation	Revendications ou avis reproduits ; périmètres variables	Un avis authentique ou une correspondance interne confirme-t-il la source ?
Logiciels professionnels	Recrutement, métiers, tourisme et services web	Certains articles citent des avis non lus directement ici	Quel service et quels dossiers sont réellement impliqués ?
Adhésion et éducation	Soutien scolaire, sport, associations et communauté	Les lignes peuvent concerner d'anciens membres	Les données sont-elles actuelles et les doublons compris ?
Logement et immobilier	Location, société immobilière alléguée et rénovation	Certaines provenances se contredisent	L'échantillon correspond-il à l'organisation revendiquée ?
Services municipaux	Messagerie de déchets et revendication d'extorsion	Consultation possible chez un prestataire et extraction confirmée diffèrent	L'exploitant confirme-t-il et la dépendance est-elle vérifiée ?
Extorsion	Mesure, ingénierie, alimentaire, optique et pharmacie	Pays ou correspondance avec le registre non résolus dans plusieurs cas	L'entité juridique exacte et le pays sont-ils étayés ?
Contenus anciens ou contestés	Archives hospitalières reconstituées, adhésions et communautés	Republication ou attribution contestée, pas nouvelle intrusion établie	Quels éléments établissent l'âge et l'origine ?

Cette section résume une sélection de récits non résolus ; elle n'est pas un registre détaillé des incidents. Ces éléments ne sont pas comptés comme incidents confirmés. Les questions ouvertes portent sur les sources, les entités et l'actualité, sans supposer que toutes les revendications sont fausses.

5.11 Autres divulgations et limites

Ces entrées conservent d'autres divulgations vérifiées à la source. La presse citant une organisation reste un récit attribué lorsque l'avis original n'était pas directement disponible. Les lignes ne sont pas additionnées pour compter les incidents ou personnes touchées en France.

Rôle du service	Divulgation et éléments	Limite et réponse
Plateforme d'anciens étudiants	En avril, la presse régionale cite police et université sur 127 400 dossiers consultés [S63]	Avis universitaire original non lu ; les dossiers ne sont pas des personnes distinctes. Vérifier les droits de la plateforme.
Boutique d'édition universitaire	En septembre, la presse locale décrit un script malveillant de paiement et 1 332 acheteurs contactés [S64]	Exposition possible depuis 2023 ; aucun total de paiements frauduleux établi. Examiner scripts et dépendances de paiement.
Institut de recherche	En août, la presse technique cite l'avis de l'institut sur une exposition de données après une intrusion externe [S65]	Exfiltration non confirmée dans l'avis cité. Séparer exposition et vol établi.
Éditeur de logiciel métier	Déclaration originale : 13 instances avec extraction de contacts/courriels, cinq avec documents et scénario distinct d'usurpation de comptes dans trois instances [S66]	Jour initial exact non résolu ; ne pas additionner les scénarios ni déduire une atteinte aux infrastructures de tous les clients. Examiner chaque instance et ses sessions.
Opérateur externe de services d'intégration	En janvier, la presse technique cite le directeur de l'agence sur un incident prestataire [S67]	Original direct non lu ; aucune intrusion directe des serveurs de l'agence ni population du vendeur retenue. Préserver les périmètres du prestataire et du responsable de traitement.
Visualiseur d'imagerie hospitalière	En novembre, la presse spécialisée cite l'hôpital sur une exposition de données patients liée au fournisseur et la poursuite de l'imagerie [S68]	L'avis cité exclut résultats médicaux et données financières/de facturation. Lien avec un produit non établi indépendamment ici ; aucun total retenu. Examiner la conservation chez les anciens fournisseurs.
Rendez-vous d'aide étudiante	En mars, la presse technique cite l'organisme sur 774 000 personnes en dix ans : 139 000 avec pièces jointes et 635 000 avec champs limités de rendez-vous, identité ou contact [S69]	Sous-ensembles disjoints égaux au total rapporté ; il ne s'agit pas uniquement d'étudiants actuels. Examiner conservation des pièces et accès.
Informations de détenteurs réglementés	En mars, une agence de presse cite une autorité sur une extraction par un compte d'entreprise [S70]	Système central déclaré non atteint ; aucun total ni avis original direct lu. Vérifier séparément les comptes professionnels autorisés.
Commandes de documents de prévention	En août, une agence de presse cite l'agence : coordonnées d'environ 80 000 personnes dans une plateforme externalisée [S71]	Données de santé exclues ; ne pas déduire un accès aux systèmes centraux de santé publique. Examiner les contacts détenus par le sous-traitant.
Administration des écoles primaires	En mars, la presse technique cite un avis sur l'accès aux informations d'utilisateurs et aux coordonnées d'élèves, familles et enseignants [S72]	Aucun total retenu de la presse. Vérifier périmètre des comptes et conservation des données familiales.

Rôle du service	Divulgation et éléments	Limite et réponse
Module administratif d'admission	Avis d'avril divulguant une extraction d'octobre 2025 concernant environ 705 000 candidats de sessions achevées 2023/2025 [S73]	Module régional historique, sans atteinte établie aux candidatures 2026. Examiner accès légitimes des agents et anonymisation.
Licences du sport scolaire	En mars, la presse technique cite la fédération sur l'extraction de novembre 2025 puis publication ; mesures sur comptes et liens d'images décrites [S74]	Aucun total officiel de personnes ou photos retenu ; l'analyse initiale citée exclut données financières et de handicap. Révoquer aussi les liens résiduels.

POINTS À RETENIR

01

Conservez dates d'incident et de publication, champs et unités pour chaque cas.

02

Testez droits des comptes valides et dépendances selon les mécanismes divulgués.

03

Gardez visibles les revendications provisoires sans les promouvoir en incidents nationaux confirmés.

CHAPITRE 06

Hacktivisme, DDoS et perturbation industrielle

06

CE CHAPITRE RÉPOND À LA QUESTION

Qu'est-ce qui distingue une revendication d'un effet démontré sur le service ou les équipements ?

2

réponses distinctes : disponibilité numérique et sécurité physique

6.1 Chronologie et niveaux de preuve 58
6.2 Froid : conséquences officielles et publicité publique 59
6.3 Les DDoS exigent un contexte de service 59
6.4 Une interface industrielle revendiquée a une autre limite 60
6.5 Activité récente : 9–22 novembre 60
6.6 Enseignements pour l'exploitation et la communication 61

CHAPITRE 06

Hacktivisme, DDoS et perturbation industrielle

EN BREF

Une annonce, une panne et un état dangereux exigent des éléments différents. Le cas officiel du froid d'octobre décrit des effets physiques et une attribution étatique en novembre. Les annonces DDoS et captures d'interfaces ne démontrent pas un effet comparable. Conservez les mesures de l'exploitant, attribuez les conclusions à leur source et confiez isolement et remise en service aux responsables de sécurité industrielle.

6.1 Chronologie et niveaux de preuve

La chronologie distingue incident et divulgation. Une publication officielle peut actualiser un événement ancien sans établir une nouvelle attaque ce jour-là.

12 août 2026	**Enquête fiscale** Premier périmètre d'extraction revendiqué ; l'enquête officielle ultérieure décrit la voie d'accès [S8].
1er sept. 2026	**Réponse des services de l'État** L'ANSSI date de ce jour la demande de capacité renforcée [S6][S7].
26 sept. 2026	**Données des professionnels de l'emploi** Le bilan d'octobre date l'extraction de ce jour [S7].
4 oct. 2026	**Service administratif de permis** Le bilan décrit un défaut d'autorisation sur les objets et des dossiers exposés [S7].
8 oct. 2026	**Annonce de données professionnelles** Le récit distingue l'annonce de l'extraction antérieure [S7].
9 oct. 2026	**Plateforme d'aides aux vacances** Une vente déclenche la détection ; l'extraction signalée couvre le 8–10 octobre [S7].
11 oct. 2026	**Contrôleurs de froid** Les autorités datent les changements de la nuit du 11–12 octobre [S10].
9 nov. 2026	**Évaluation française du C4** Le rapport attribue l'incident antérieur et décrit ses effets physiques [S10].
12 nov. 2026	**Bilan du CERT-FR** Publication de cas d'octobre et des corrections en cours [S7].
14 nov. 2026	**Divulgation du prestataire de courrier** France 24 cite la confirmation de l'entreprise concernant un incident de septembre [S12].
18 nov. 2026	**Décision de sécurité CNIL** Sanction anonyme sur mots de passe, accès partagés et conservation [S16].

La chronologie ne signifie pas qu'un acteur commun a mené ces événements. Elle réunit des éléments différents pour orienter chaque validation.

6.2 Froid : conséquences officielles et publicité publique

Le C4 indique environ 700 sites de distribution français affectés au niveau des contrôleurs de froid en octobre. Il décrit des paramètres de dégivrage modifiés, des pertes importantes de marchandises et des départs de feu dans au moins 15 cas. Ce sont des constats officiels rapportés [S10].

Le rapport mentionne séparément le ciblage concomitant d'équipements de petites installations hydroélectriques, avec des effets modérés. Il n'indique pas les mêmes conséquences que pour le froid. Les deux ensembles ne doivent pas former un total national vérifié d'équipements [S10].

Point	Revendication ou publicité	Récit officiel	Limite de cette édition
Événement	Des canaux publics ont relayé l'incident selon le C4	Le C4 rapporte des changements de paramètres les 11–12 octobre [S10]	Aucune télémétrie d'exploitant détenue ici
Échelle	Une revendication ne mesure pas indépendamment les sites	Environ 700 sites selon le récit officiel [S10]	Aucun recensement distinct de Brandefense
Effets physiques	Une capture ne démontre ni incendie ni perte de denrées	Pertes et au moins 15 départs de feu signalés [S10]	Pas de reconstitution indépendante de chaque site
Attribution	Pseudonymes et discours politique ne suffisent pas	Le C4 attribue l'activité à Shahid Kaveh dans la structure cyber iranienne [S10] [S11]	Attribution des autorités, pas issue des annonces de marché
Réponse	Une annonce de reprise ne démontre pas la sécurité physique	Exploitants et autorités décrivent leur périmètre	Chaque exploitant doit vérifier une remise en service sûre

Le tableau compare des preuves de nature différente. Il ne calcule aucun ratio entre chiffre d'un acteur et récit officiel. Attribution et conséquences physiques répondent aussi à deux questions distinctes : responsable évalué et faits signalés.

6.3 Les DDoS exigent un contexte de service

Une annonce DDoS établit une revendication. Une capture de disponibilité externe peut montrer l'échec d'une requête. Ni l'une ni l'autre n'établit durée, étendue géographique ou effet métier.

Les exploitants doivent conserver leurs mesures et les dossiers du prestataire d'atténuation. Un service peut bloquer une région ou modifier sa protection tout en servant d'autres clients. Cette possibilité ne signifie pas que toute panne signalée est anodine.

La question pratique est la fonction critique perdue, sa durée et sa dépendance. Les mesures du service peuvent guider atténuation et communication sans résoudre l'identité de l'auteur.

6.4 Une interface industrielle revendiquée a une autre limite

Une interface photographiée peut être réelle, ancienne, simulée ou copiée. Elle ne démontre pas que l'auteur peut changer un paramètre. Même un accès démontré ne prouverait pas seul un effet physique.

Le cas officiel du froid est plus étayé : les autorités décrivent paramètres modifiés et conséquences [S10]. Cela ne valide pas les revendications sans lien sur des pompes, réseaux d'eau, usines ou transports.

Confiez chaque revendication au responsable opérationnel. Vérifiez la propriété en privé, examinez les sessions distantes et comparez la configuration à l'état approuvé. Ne reproduisez pas publiquement interfaces, adresses ou identifiants de tiers.

6.5 Activité récente : 9–22 novembre

La dernière quinzaine apporte des évolutions différentes. L'attribution du 9 novembre concerne un incident physique d'octobre. Le bilan du 12 novembre traite d'événements d'octobre et de corrections en cours. La divulgation du courrier concerne septembre [S7][S10][S12][S13].

Le 9 novembre, la CNIL annonce aussi les sanctions de collectivités. Le 18, elle publie la décision sur les mots de passe et le CERT-FR l'alerte NGINX. Constats réglementaires et alertes de failles sont récents, mais ne sont pas des intrusions confirmées supplémentaires [S16][S17][S23].

Le 17 novembre, la chambre basse adopte en première lecture le projet modifié sur la résilience et la cybersécurité. Cette étape appartient à l'activité récente ; son statut diffère d'une loi nationale en vigueur [S61].

La section suit donc l'évolution des connaissances pendant la quinzaine. Elle ne présente pas chaque élément comme une attaque survenue à ces dates. Cette distinction compte pour les effectifs, les avis clients et l'urgence des corrections.

La couverture des 20–21 novembre sur un logiciel touristique apporte un cas récent de disponibilité. Dans un entretien direct avec la presse professionnelle, le dirigeant décrit des accès illicites, l'arrêt préventif de plateformes de réservation connectées et une reprise progressive. La fuite de données restait non résolue ; les réservations illicites étaient un risque redouté, pas un résultat établi. L'éditeur déclarait ne pas héberger de données bancaires [S76].

6.6 Enseignements pour l'exploitation et la communication

Déclencheur	Premier responsable	Éléments à conserver	Première décision
Service nommé dans une annonce	SOC et responsable de service	Revendication, dates et mesures réelles	Renforcer la préparation et valider l'effet client
Interruption numérique confirmée	Exploitation et fournisseur	Disponibilité, trafic et atténuation	Activer la réponse convenue et les messages factuels
Accès industriel revendiqué	Sécurité opérationnelle	Propriété vérifiée en privé et accès distants	Évaluer avec le propriétaire de l'équipement
Paramètre modifié sans autorisation	Exploitation et sécurité physique	État approuvé, état réel et alarmes indépendantes	Isoler sans danger et contrôler la reprise
Nouvelle attribution étatique	Renseignement et communication	Source exacte, acteur évalué et confiance	Actualiser sans étendre aux cas sans lien

La communication doit distinguer disponibilité, confidentialité et sécurité physique. Restaurer un service ne démontre pas l'absence de vol. Une offre de données ne démontre pas non plus une panne prolongée.

POINTS À RETENIR

01

Adaptez la force de chaque conclusion aux éléments officiels ou de l'exploitant.

02

Séparez disponibilité numérique, sécurité physique et reprise.

03

Présentez la dernière quinzaine comme une actualisation, avec des dates d'incident distinctes.

CHAPITRE 07

Acteurs et campagnes

07

CE CHAPITRE RÉPOND À LA QUESTION

Quels liens et quels mécanismes de campagne sont étayés ?

295

inscriptions étiquetées France d'extorsion réparties entre de nombreux noms

7.1 Lire la carte des liens 63
7.2 Rançongiciels et extorsion 64
7.3 L'attribution industrielle officielle 67
7.4 Turla : évaluation d'espionnage publiée par le C4 français 69
7.5 Campagnes d'identité sans acteur commun établi 70
7.6 Correspondances de techniques pour les défenseurs 70
7.7 Les avis techniques sont un signal distinct 71
7.8 Persistance dans une petite entreprise : un cas distinct 72

CHAPITRE 07

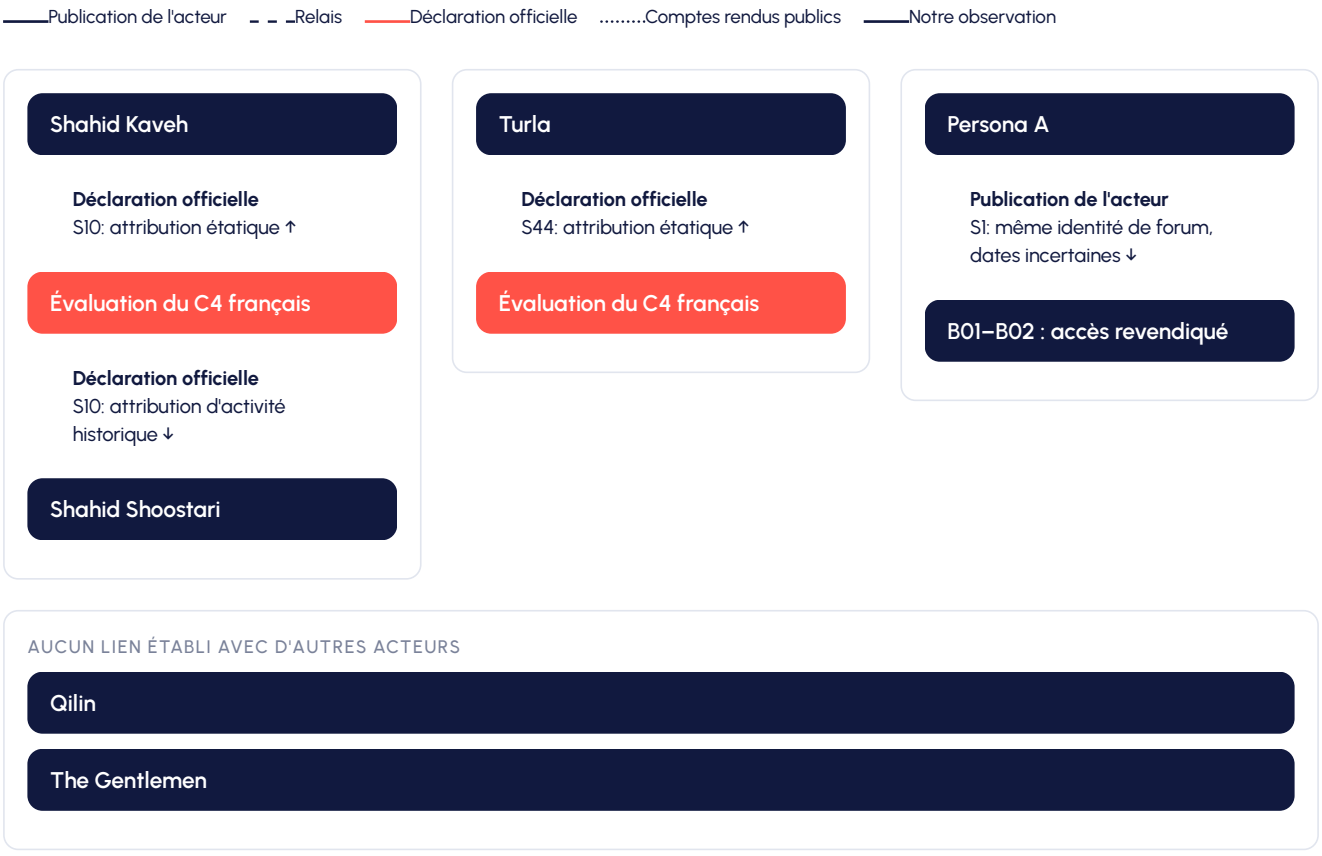
Acteurs et campagnes

EN BREF

Les marques d'extorsion sont visibles dans les inscriptions. Le cas industriel officiel apporte une attribution étatique distincte. Vendeurs de données et d'accès restent des personas non vérifiées sans éléments plus forts. Formulation, calendrier ou discours politique similaires ne démontrent pas une direction commune. Gardez l'attribution liée à sa source et préparez la reprise selon le mécanisme observé plutôt que le nom d'un groupe.

7.1 Lire la carte des liens

La carte présente les liens d'attribution officielle et un lien entre un pseudonyme et ses publications. Les marques d'extorsion apparaissent comme des nœuds sans lien. Chaque lien précise son type. Un pseudonyme réutilisé n'établit pas une personne unique, et une cible annoncée n'établit pas l'accès.



Aucun élément ici ne réunit les marques d'extorsion, l'activité industrielle attribuée et les personas de marché dans une même organisation. Tout lien de préparation entre données volées et fraude est présenté comme modèle analytique.

7.2 Rançongiciels et extorsion

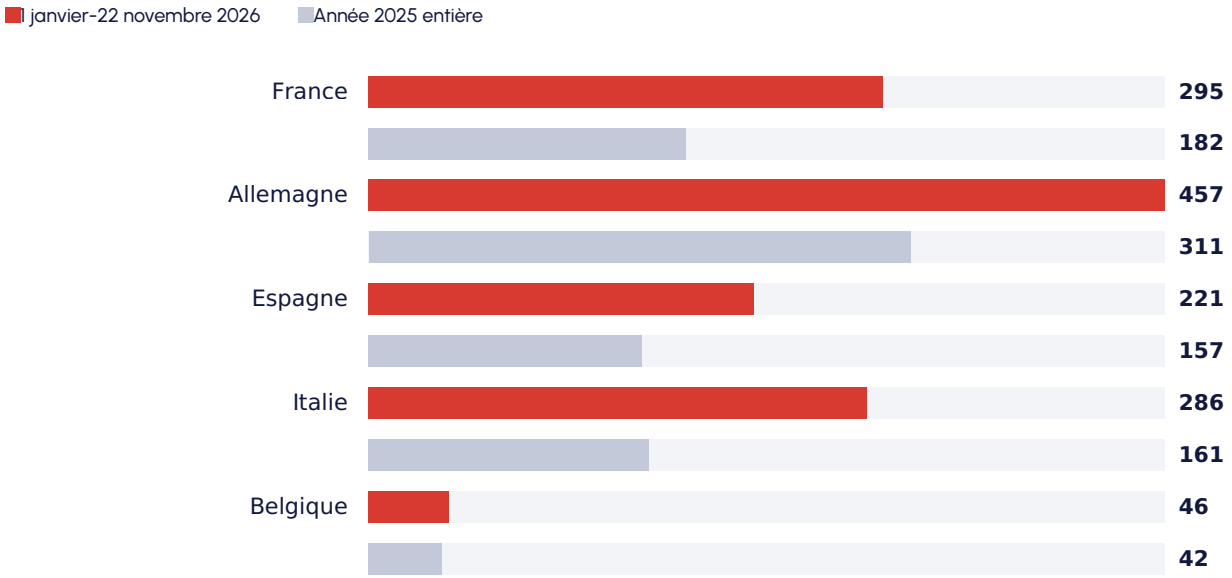
Ransompedia compte 295 inscriptions étiquetées France datées de la période. Dans le même état des données, toute l'année 2025 en compte 182. Les durées diffèrent, et le chiffre supérieur d'une année partielle ne mesure pas l'évolution de l'incidence nationale [S3].

À titre de série officielle distincte et non comparable, le panorama 2025 de l'ANSSI recense 1366 incidents traités ou signalés en 2025 contre 1361 en 2024 [S79]. Dans cette série officielle, les incidents d'exfiltration de données signalés passent de 130 en 2024 à 196 en 2025 [S79].

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.

La comparaison suivante porte sur la même période actuelle pour les cinq pays. Elle couvre des économies industrielles et de services voisines ; la Belgique ajoute des liens francophones et institutionnels. La visibilité n'est ajustée ni à la population, ni à l'économie, ni aux pratiques de divulgation.

Les 295 inscriptions étiquetées France et les quatre comparateurs décrivent la visibilité, pas le risque national



Source : inscriptions Brandefense Ransompedia étiquetées par pays. 2026 : 1 janvier-22 novembre ; 2025 : année entière. Périodes inégales ; les dates d'inscription ne sont ni des dates d'incident ni un classement national des risques [S3].

Pays	Inscriptions sur la période	Toute l'année 2025	Interprétation
France	295	182	Pays étudié
Allemagne	457	311	Grande économie industrielle voisine
Espagne	221	157	Grande économie voisine de l'UE
Italie	286	161	Grande économie industrielle et financière
Belgique	46	42	Économie voisine avec liens francophones

Qilin et The Gentlemen représentent ensemble 92 des 295 inscriptions, soit 31,2%. Les autres marques représentent 203, soit 68,8%. Cette répartition couvre plusieurs marques d'extorsion et étiquettes d'inscription, sans établir des personnes distinctes derrière chaque marque.

Marque d'inscription	Inscriptions françaises	Part
Qilin	48	16,3%
The Gentlemen	44	14,9%
Coinbasecartel	13	4,4%
Lapsus$	12	4,1%
Autres noms	178	60,3%
Total	295	100,0%

Ces noms restent des étiquettes d'inscription. Une marque historique connue n'établit pas une continuité d'opérateurs, de logiciels ou de voies d'accès. Pays et secteurs exigent aussi une corroboration au niveau du cas avant de décrire une organisation comme affectée.

Qilin

Agenda

Marque d'inscriptions de rançongiciel et d'extorsion | Revendications d'extorsion à but financier

EN FRANCE, 2026

2026

48 inscriptions françaises sur la période

CIBLES REVENDIQUÉES

Organisations décrites dans les revendications publiques

VU DANS LES SOURCES PUBLIQUES

[S3] Ransompedia compte 48 inscriptions françaises sous ce nom

NOTRE ÉVALUATION

Étiquette fréquente. Le nombre établit des revendications publiques, sans confirmer chiffrement, vol ou opérateur unique. Préparez reprise et réponse sur les données indépendamment de la marque.

DEGRÉ DE CONFIANCE

Élevée pour le nombre conservé ; résultats des incidents non vérifiés

The Gentlemen

Marque d'inscriptions de rançongiciel et d'extorsion | Revendications d'extorsion à but financier

EN FRANCE, 2026

2026

44 inscriptions françaises sur la période

CIBLES REVENDIQUÉES

Organisations décrites dans les revendications publiques

VU DANS LES SOURCES PUBLIQUES

[S3] Ransompedia compte 44 inscriptions françaises sous ce nom

NOTRE ÉVALUATION

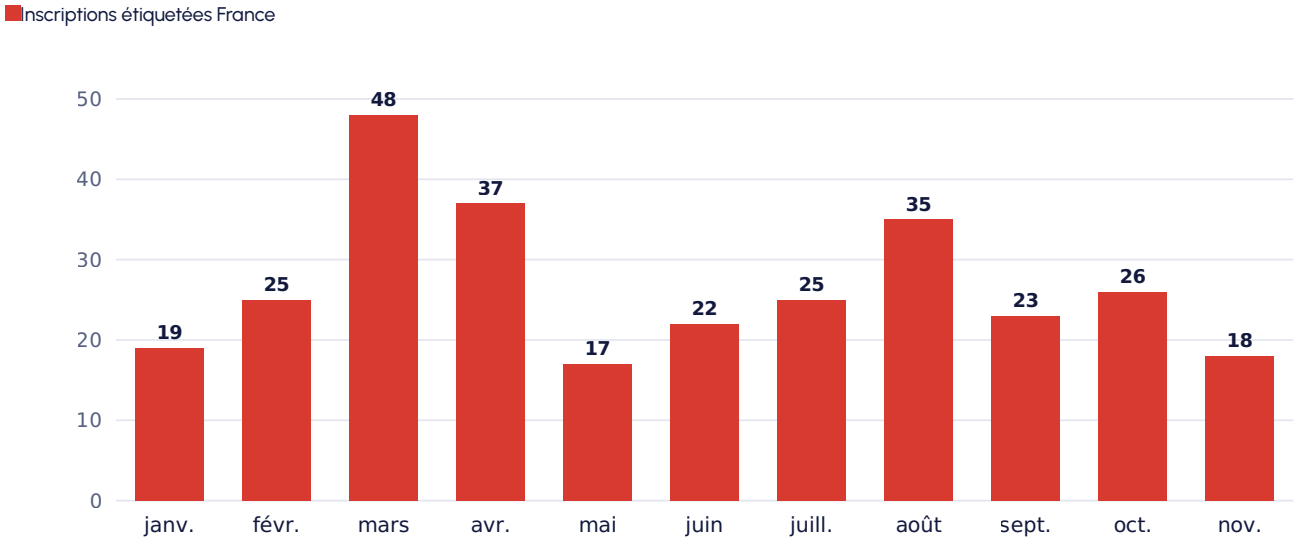
Deuxième étiquette française de cet état des données. Aucune voie d'accès n'est déduite du nom du groupe.

DEGRÉ DE CONFIANCE

Élevée pour le nombre conservé ; résultats non vérifiés

Les nombres mensuels français vont de 17 en mai à 48 en mars. Novembre apporte 18 inscriptions à la clôture et reste partiel. Les dates d'inscription ne donnent ni la date d'intrusion ni l'unicité d'une organisation [S3].

Les inscriptions étiquetées France couvrent la période, avec un mois de novembre partiel



Source : inscriptions Brandefense Ransompedia étiquetées par pays. 2026 : 1 janvier-22 novembre ; 2025 : année entière. Périodes inégales ; les dates d'inscription ne sont ni des dates d'incident ni un classement national des risques [S3].

Les étiquettes fréquentes comprennent conseil, administration, technologie, commerce, construction et industrie. Elles concernent des revendications. Elles ne correspondent pas directement aux secteurs de la sélection d'organisations et ne démontrent pas des contrôles plus faibles.

Séparez publication des données et reprise du service. Un test de restauration peut démontrer la continuité tout en laissant la confidentialité non résolue. L'extorsion doit donc réunir reprise, protection des données, juridique et communication.

7.3 L'attribution industrielle officielle

Le 9 novembre, le CERT-FR publie l'évaluation du C4 sur des attaques contre des intérêts français. Elle attribue le cas des contrôleurs de froid d'octobre à l'unité Shahid Kaveh, dans la structure électronique et cyber des Gardiens de la révolution iraniens. Cette attribution est celle des sources [S10][S11].

Le rapport décrit aussi Shahid Shoostari, associée aux noms Emennet Pasargad et Iliyanet. Les cas français discutés pour cette unité sont antérieurs. Leur présence dans une publication de 2026 ne les transforme pas en nouveaux incidents de 2026 [S10].

Shahid Kaveh

Pseudonymes publics selon le C4

Activité industrielle attribuée par les autorités françaises | Attribuée par le C4 français à la structure cyber des Gardiens de la révolution iraniens

EN FRANCE, 2026

11–12 oct.
Incident des contrôleurs de froid dans le récit officiel

9 nov.
Publication de l'attribution du C4

CIBLES REVENDIQUÉES

Équipements de froid et autres équipements industriels connectés, selon le C4

VU DANS LES SOURCES PUBLIQUES

[S10] Le C4 décrit des changements de paramètres, pertes de denrées et départs de feu

[S11] Déclaration d'attribution du ministère français des Affaires étrangères

NOTRE ÉVALUATION

L'attribution appartient aux sources officielles. Validez accès distants, autorité de configuration et remise en service sûre ; n'étendez pas cette attribution à des revendications sans lien.

DEGRÉ DE CONFIANCE
Attribution officielle ; aucune attribution indépendante de Brandefense

Shahid Shoostari

Emennet Pasargad ; Iliyanet, selon le C4

Activité antérieure décrite dans un rapport officiel de 2026 | Attribuée par le C4 français à la structure cyber iranienne

EN FRANCE, 2026

9 nov.
Le C4 décrit des cas français antérieurs et le lien avec l'unité

CIBLES REVENDIQUÉES

Cas antérieurs de médias et d'affichage décrits par la source

VU DANS LES SOURCES PUBLIQUES

[S10] Le rapport officiel traite d'événements d'années antérieures

NOTRE ÉVALUATION

Une publication de 2026 ne transforme pas ces cas historiques en incidents nouveaux de 2026. Aucun lien avec les vendeurs des forums n'est établi.

DEGRÉ DE CONFIANCE
Attribution de la source ; dates historiques conservées

Le récit officiel relie plusieurs pseudonymes publics à Shahid Kaveh. Ce lien reste une attribution officielle. Le rapport n'attribue pas un autre événement français à cette unité à partir d'un pseudonyme, d'une langue ou d'une republication seuls.

La conséquence défensive est indépendante de l'évaluation politique. Les exploitants doivent connaître les accès permettant de changer des paramètres physiques, les alarmes indépendantes et l'autorité de remise en service. Le chapitre 6 sépare le récit officiel des interfaces revendiquées non vérifiées.

7.4 Turla : évaluation d'espionnage publiée par le C4 français

Le 13 juillet, le CERT-FR publie une évaluation du C4 sur le ciblage et les accès non autorisés à des entités françaises avec Turla. Elle attribue l'activité au 16e Centre du FSB russe [S44].

La source mentionne administration stratégique, diplomatie, défense, justice et technologie. Son récit historique remonte au moins à 2004. La publication ne démontre pas que chaque opération décrite s'est déroulée dans la période 2026 étudiée.

Turla

Mode opératoire nommé par le C4 français

Espionnage attribué par les autorités françaises | Attribué par le C4 français au 16e Centre du FSB russe

EN FRANCE, 2026

13 juillet
Le CERT-FR publie son évaluation de ciblage et d'attribution

CIBLES REVENDIQUÉES

Contextes stratégiques publics, diplomatiques, de défense, de justice et technologiques, selon la source

VU DANS LES SOURCES PUBLIQUES

[S44] Le C4 rapporte ciblage et accès non autorisés à des entités françaises

NOTRE ÉVALUATION

La campagne historique couvre des années antérieures. Ne datez pas toutes les opérations de 2026 et n'étendez pas l'attribution aux contenus russophones sans lien.

DEGRÉ DE CONFIANCE
Attribution officielle ; dates de chaque événement non entièrement précisées

L'attribution reste celle des autorités françaises. Elle ne s'étend pas aux publications russophones, aux revendications DDoS ou aux marques d'extorsion sans lien. La langue seule ne démontre pas un commanditaire étatique.

Conservez une investigation sur les accès persistants aux services stratégiques. Une offre de marché et un rapport de campagne étatique peuvent justifier des questions différentes, même s'ils évoquent le même secteur général.

Au-delà de l'avis sur Turla, le panorama 2025 de l'ANSSI décrit un espionnage soutenu contre des intérêts institutionnels, diplomatiques et industriels français [S79][S80]. L'agence rattache principalement ces campagnes à des modes opératoires liés à la Russie et à la Chine [S79][S80]. Cette édition ne profilant que les acteurs liés à un avis français spécifique de 2026 ou au corpus conservé, ces autres ensembles étatiques ne figurent pas séparément ici.

7.5 Campagnes d'identité sans acteur commun établi

L'enquête fiscale, l'annuaire professionnel et les aides aux vacances impliquent tous des comptes légitimes dans le récit officiel [S7][S8]. Cela n'établit ni acteur commun ni voie initiale unique.

Le cas fiscal décrit identifiants volés et franchissements de frontières de confiance. Le cas professionnel indique la validation d'un second facteur. Les aides associent identifiants partenaires et autorisation par objet. Dire que la MFA seule aurait empêché tous les cas dépasserait ces éléments.

La réponse couvre donc protection et récupération des comptes, sessions, droits de rôle, autorisations par objet et surveillance des exports. Un contrôle à une étape ne doit pas masquer l'absence d'un autre.

7.6 Correspondances de techniques pour les défenseurs

Cette correspondance analytique rapproche les comportements publics des concepts ATT&CK. Elle ne dit ni que les autorités emploient ces étiquettes, ni que chaque technique apparaît dans chaque incident [S29].

CORRESPONDANCE ANALYTIQUE DES COMPORTEMENTS DÉCRITS AVEC LES TECHNIQUES MITRE

Initial Access	Impair Process Control
T1078 Valid Accounts	T0836 Modify Parameter

Correspondance analytique des comportements décrits, pas une matrice originale des sources. S7, S8, S10 et S29. [S10]

Comportement décrit	Concept de technique	Limite de source	Question défensive
Identifiants légitimes volés utilisés	T1078, Valid Accounts	Décrit dans les rapports fiscaux et opérationnels [S7] [S8]	Une session apparemment valide atteint-elle des données sensibles sans contrôle ?
Paramètres industriels modifiés	T0836, Modify Parameter	Le récit officiel du froid décrit les changements [S10]	Une alarme indépendante détecterait-elle un état dangereux ?

Le premier concept concerne l'accès d'entreprise, le second les systèmes industriels. Leur présence commune dans une matrice de préparation n'implique ni chaîne d'intrusion unique ni lien entre acteurs.

Pour l'identité, reliez utilisateur, session, action applicative et dossiers récupérés. Pour les contrôleurs, reliez opérateur autorisé, configuration approuvée et état physique indépendant. Ce sont deux surfaces d'investigation différentes.

7.7 Les avis techniques sont un signal distinct

L'alerte NGINX du 18 novembre identifie deux failles HTTP/2. Le NVD et F5 décrivent déni de service et exécution possible de code sous conditions. Aucune de ces sources n'établit une exploitation dans une organisation française de ce rapport [S23][S24][S25][S26].

Le NVD et l'avis Metabase établissent une injection SQL critique et des correctifs. L'éditeur indique une exploitation active. Cette déclaration n'établit pas qu'une annonce française particulière résulte de cette faille [S21][S22].

Produit et CVE	Périmètre affecté vérifié	Versions corrigées ou action	Limite de réponse
Metabase, CVE-2026-72898	Six plages affectées répertoriées par l'éditeur, reproduites ci-dessous	Correctifs recommandés ci-dessous ; x désigne l'édition	Suivre la branche exacte ; examiner activités antérieures et secrets connectés [S21][S22]
NGINX Open Source, CVE-2026-123633	F5 indique 1.19.7–1.30.6 et 1.31.0–1.31.8 avec la configuration HTTP/2 concernée	1.30.7 ou 1.31.9	Consulter le tableau complet pour les autres produits [S24] [S26]
NGINX Open Source, CVE-2026-123007	F5 indique 1.9.5–1.30.6 et 1.31.0–1.31.8 avec HTTP/2	1.30.7 ou 1.31.9	Corriger ne prouve pas l'absence d'activité antérieure [S25][S26]

Les plages affectées et les correctifs recommandés pour Metabase sont reproduits séparément, tels que répertoriés par l'éditeur [S22].

Plage affectée	Correctif recommandé
>= x.58.0, < x.58.23	x.58.24
>= x.59.0, < x.59.20	x.59.21
>= x.60.0, < x.60.16	x.60.17
>= x.61.0, < x.61.10	x.61.11
>= x.62.0, < x.62.8	x.62.9
>= x.63.0, < x.63.3	x.63.5

Pour NGINX Plus, les deux tableaux donnent des correctifs de branche différents. La synthèse numérique se limite volontairement à Open Source. Les responsables de Plus et des produits intégrés doivent lire leur ligne, sans transposer la version d'un autre produit [S26].

Le CERT-FR recommande de désactiver HTTP/2 provisoirement avant correction [S23]. Testez l'effet opérationnel et vérifiez la configuration. Le rapport ne fournit ni exploitation, ni commande de test en production, ni validation d'atténuation chez un tiers.

7.8 Persistance dans une petite entreprise : un cas distinct

L'étude de Cato CTRL du 16 juin décrit l'activité de Poisson du 30 mars–1 mai contre des particuliers français et une petite entreprise automobile. Elle rapporte un vol de secrets et des accès distants indépendants ayant survécu à l'interruption de l'infrastructure de commande. Ses descriptions des victimes se contredisent ; aucun total n'est retenu [S62].

Il faut examiner postes, outils distants autorisés et persistance avant de déclarer le confinement. La source n'établit aucun lien avec les vendeurs ou groupes de rançongiciel de ce rapport [S62].

POINTS À RETENIR

01

Séparez marques d'extorsion, personas criminelles et attributions étatiques officielles.

02

Reliez le mécanisme observé à une investigation réalisable par le responsable concerné.

03

Vérifiez branches affectées et activité antérieure sans faire d'un avis un incident français confirmé.

CHAPITRE 08

L'économie de la fraude

CE CHAPITRE RÉPOND À LA QUESTION

Comment des informations exposées peuvent-elles rendre une demande frauduleuse convaincante ?

4

sections de mécanismes couvrant cinq exemples officiels de campagnes

8.1 Offres de données et fraude ultérieure sont distinctes 74
8.2 Cartes dans les publications : un aperçu limité 74
8.3 Fausse assistance après une violation 75
8.4 Remboursements fiscaux et fausse autorité 75
8.5 Association d'appareils et confiance dans les comptes 75
8.6 Services de crypto-actifs et menaces physiques 76
8.7 L'action judiciaire reste un ensemble distinct 76
8.8 Prix et services annoncés 76

CHAPITRE 08

L'économie de la fraude

EN BREF

Des détails personnels exacts peuvent faciliter une usurpation sans donner le contrôle d'une banque ou d'un service public. Cinq alertes officielles décrivent fausse aide à la suppression, remboursement fiscal, convocation judiciaire, association d'appareils de messagerie et usurpation liée aux crypto-actifs. Les cartes des publications n'apportent qu'un aperçu supplémentaire limité. Considérez ces détails comme potentiellement connus, vérifiez par un canal indépendant fiable et testez les actions sensibles au-delà de la simple reconnaissance.

8.1 Offres de données et fraude ultérieure sont distinctes

Une annonce établit qu'une information ou un accès est proposé. Elle ne démontre ni acquisition par un acheteur, ni authenticité, ni emploi de ces dossiers dans une fraude ultérieure. Le rapport ne relie pas un vendeur à une campagne sans éléments supplémentaires [S1].

Le lien est utile comme modèle analytique. Si des informations exactes deviennent disponibles, un interlocuteur peut les employer pour rendre son prétexte crédible. La question est de savoir si le processus exige encore une autorité indépendante pour l'action demandée.

Les détails varient selon le service. Un message fiscal peut citer un contexte administratif. Un message touristique peut citer une réservation réelle. Un appel bancaire peut connaître l'établissement et le titulaire. Les informations familières ne remplacent pas la vérification de la demande.

8.2 Cartes dans les publications : un aperçu limité

PORTÉE DES CHIFFRES DES FICHES

Cette section présente un aperçu limité des observations de cartes de paiement associées à la France. Ces chiffres ne mesurent ni le vol national, ni les cartes actives, ni des transactions réalisées, ni les pertes de fraude.

L'agrégat comprend 11 cartes distinctes associées à la France dans 5 enregistrements conservés. Parmi elles, 1 est associée à un émetteur et 10 au seul pays. Ces catégories disjointes totalisent 11 [S4]. Les mêmes limites s'appliquent au chapitre bancaire et à la méthode. Une absence dans cet aperçu ne démontre pas l'absence d'exposition d'une banque, d'un émetteur ou de clients.

L'affirmation d'un auteur sur la validité d'une carte ou la réussite d'un paiement reste une revendication. La validité des cartes et la réalisation des paiements ne sont pas établies. La réponse nécessite la validation et les transactions propres à l'émetteur.

8.3 Fausse assistance après une violation

L'alerte de la CNIL du 24 juin décrit des organisations non sollicitées prétendant aider les personnes touchées par une fuite. Certains messages emploient des détails exacts et proposent de retirer les informations d'Internet. La CNIL précise qu'ils ne viennent pas d'elle et n'agissent pas en partenariat avec elle [S43].

Le mécanisme réemploie la connaissance d'un incident antérieur par la victime. Une personne attendant des conseils protecteurs peut recevoir une offre semblant résoudre le même problème. L'alerte ne démontre pas que toute offre non sollicitée emploie des données volées.

Les responsables de traitement doivent prévoir un canal officiel reconnaissable dans leur avis. Expliquez quelles informations seront demandées et comment vérifier le contact. Ne dirigez pas une personne vers un intermédiaire non vérifié parce qu'il connaît des détails exacts.

8.4 Remboursements fiscaux et fausse autorité

L'alerte de Cybermalveillance.gouv.fr sur les remboursements décrit courriels, SMS et appels menant vers des pages frauduleuses pour obtenir données personnelles, identifiants fiscaux et informations bancaires. Elle a été publiée le 15 juillet 2026 et mise à jour le 8 septembre 2026 [S46].

La personne peut-elle vérifier la demande dans son service habituel, sans suivre le lien ou le numéro fourni ? Une vraie période de remboursement n'authentifie pas chaque message.

Le 11 août, la Gendarmerie alerte sur une hausse de fausses convocations judiciaires demandant un prétendu règlement. L'article évoque des arrestations antérieures, dont une opération de 2023. Ce n'est pas un nouveau démantèlement de 2026 [S47].

Le rapport omet les menaces et contenus personnels des messages. Le mécanisme pertinent associe fausse autorité et pression au paiement. Finance et service client doivent reconnaître la demande sans reproduire l'intimidation.

8.5 Association d'appareils et confiance dans les comptes

L'alerte de Cybermalveillance.gouv.fr sur les faux votes, publiée le 27 octobre 2026 et mise à jour le 3 novembre 2026, décrit des liens incitant à associer un appareil supplémentaire à une messagerie. Les contacts peuvent ensuite recevoir des messages paraissant venir d'une connaissance. Cela abuse d'une fonction légitime, sans établir une faille logicielle [S56].

L'alerte du CERT-FR, publiée le 20 mars 2026 et actualisée le 18 juin 2026, décrit l'accès à des comptes sensibles via les fonctions légitimes d'association et l'usurpation du support. Son périmètre dépasse une messagerie commerciale. Elle ne démontre pas une défaite du chiffrement ou une intrusion dans les téléphones [S37].

Examinez appareils liés, récupération et faux supports. Pour les processus sensibles, déterminez les demandes exigeant une vérification hors de la conversation. Un échange existant et un compte familier n'autorisent pas seuls un paiement ou un changement d'accès.

8.6 Services de crypto-actifs et menaces physiques

L'alerte de Cybermalveillance.gouv.fr décrit de faux salariés, services antifraude ou forces de l'ordre après des divulgations de données. Elle mentionne une enquête dirigée par Paris J3. Elle a été publiée le 22 janvier 2026 et mise à jour le 8 juin 2026 [S45].

Le risque dépasse le seul mot de passe. Des informations sur le service peuvent désigner des personnes pour des demandes ciblées. Le rapport ne reprend aucun détail personnel et ne suppose pas un risque identique pour tous les usagers.

Sécurité, fraude, protection des données et sécurité physique doivent convenir d'une escalade pour les menaces crédibles. Le message client doit expliquer vérification et assistance sans suggérer que les connaissances d'un interlocuteur prouvent son autorité.

8.7 L'action judiciaire reste un ensemble distinct

Le 8 octobre, la publication de police judiciaire de la Gendarmerie décrit la fermeture de trois sites diffusant des contenus intimes volés. Elle indique une enquête dirigée par Paris J3, deux suspects arrêtés en France et plus de 17 000 victimes dans plusieurs pays [S48].

Le total multinational n'est pas celui des victimes françaises. Une arrestation n'est pas une condamnation. L'annonce ne démontre pas que toutes les personas proposant des comptes appartenaient à cette opération.

La sécurité des comptes a donc aussi une dimension de vie privée et de sécurité personnelle. Préservez les éléments et soutenez les personnes sans publier d'identifiants ou de contenus sensibles pour montrer qu'une revendication existe.

8.8 Prix et services annoncés

Les prix demandés sont des caractéristiques des annonces conservées [S1]. Ils n'établissent ni prix de marché, ni authenticité, ni transaction, ni valeur de l'information.

Lorsqu'une offre mélange fichiers, accès et promesses de service, conservez les unités séparées. Un prix bas ne démontre pas une fabrication ; un prix haut ne démontre pas la qualité. Commencez par la provenance, l'actualité et la pertinence interne.

POINTS À RETENIR

01

Des détails personnels exacts ne suffisent pas à autoriser une demande sensible.

02

Gardez le lien entre données proposées et fraude comme modèle analytique sans preuve supplémentaire.

03

Examinez messagerie, récupération et support avec les contrôles de paiement.

CHAPITRE 09

Banque et finance

09

CE CHAPITRE RÉPOND À LA QUESTION

Quelles décisions financières exigent ensemble identité, prestataire et transactions ?

3

surfaces distinctes : identité client, accès aux données financières et opérations de paiement

9.1 L'ensemble bancaire sélectionné 79
9.2 Les dossiers financiers n'établissent pas l'accès à toutes les banques 80
9.3 Opérations frauduleuses et interruption de service 80
9.4 Validation commune 81
9.5 DORA et éléments opérationnels 81
9.6 Priorités des équipes financières 81

CHAPITRE 09

Banque et finance

EN BREF

Le risque financier vient de surfaces différentes. L'avis officiel sur un service de données financières concerne l'accès aux données. Une banque coopérative divulgue des opérations frauduleuses et des virements retardés. Les cartes des publications ont un périmètre bien plus limité. 16 domaines financiers évalués sur 30 ont une offre actuelle d'identifiants. Réunissez identité et fraude, vérifiez indépendamment l'autorité de paiement et testez les dépendances des services financiers critiques.

9.1 L'ensemble bancaire sélectionné

La sélection comprend trente domaines de banque, paiement, investissement et infrastructure financière, tous avec observations d'exposition [S2]. Ce n'est pas une liste de trente banques de dépôt indépendantes agréées. Des entités liées et des services différents peuvent apparaître séparément.

16 domaines financiers évalués sur 30 avaient un identifiant proposé à la vente. Les appareils représentent au moins 115 930 associations, dont 701 classées salariées. Aucun de ces ensembles n'établit seul une intrusion bancaire.

Signal	Population bancaire et financière sélectionnée
Domaines évalués pour l'exposition	30
Offres actuelles d'identifiants	16 domaines
Associations d'appareils, au moins	115 930
Associations d'appareils salariés	701
Enregistrements d'identifiants	373 568
Associations de documents	327
Domaines avec observations passives	27
DMARC rejet ou quarantaine	23 sur 27

Source : observations d'exposition et passives [S2]. Aucune note bancaire ou individuelle n'est publiée.

Les chiffres limités des cartes ne dénombrent ni cartes actives, ni paiements réussis, ni intrusions bancaires [S4]. Une absence d'attribution ne démontre pas l'absence d'exposition.

Un identifiant associé au domaine bancaire peut concerner salariés, messagerie client ou autre contexte. Validez les offres actuelles avec les équipes identité et fraude. Examinez les appareils classés salariés avec leur responsable avant de déduire la propriété des autres appareils associés.

9.2 Les dossiers financiers n'établissent pas l'accès à toutes les banques

L'avis de février décrit l'accès à un service de données financières avec les identifiants volés d'un fonctionnaire. Il date les accès de fin janvier et estime qu'environ 1.2 million de comptes pourraient être concernés. Les champs indiqués comprennent références de compte, identité du titulaire et adresse [S35].

L'avis exclut explicitement la consultation de l'identifiant fiscal. Cette exclusion prime sur une formulation secondaire plus large. La synthèse ne doit pas ajouter un identifiant exclu par la source primaire.

Il s'agit d'accès aux données financières. Cela n'établit ni intrusion dans chaque banque, ni modification de soldes, ni population identique de personnes distinctes. Une personne peut détenir plusieurs comptes.

La conséquence concerne les contacts persuasifs. Un interlocuteur connaissant la banque ou un identifiant de compte peut sembler crédible. Testez si la vérification du client repose encore sur des informations qui ne peuvent plus être considérées comme secrètes.

9.3 Opérations frauduleuses et interruption de service

La déclaration du 4 novembre de Crédit Mutuel Arkéa confirme une attaque ayant permis des opérations frauduleuses. Elle décrit suspension temporaire, reprise progressive et exécution retardée de certains virements. La banque indique que les avoirs des clients ne sont pas affectés, sans préciser la voie initiale dans ce premier communiqué [S49].

Le suivi de Reuters du 5 novembre rapporte une estimation bancaire d'environ 100 millions d'euros [S50]. Dans son amendement déposé le 18 novembre, la banque indique que l'attaque est passée par la plateforme d'un prestataire externe et a touché le compte propre de l'établissement [S78]. Ce document estime l'effet sur le résultat à environ 100 millions d'euros, ce qui reste une estimation attribuée à ce cas et non une perte nationale ou une perte client [S50][S78].

Ces publications datées distinguent le premier communiqué du 4 novembre et l'amendement du 18 novembre sur la plateforme du prestataire externe et le compte propre de la banque [S49][S78]. Ce dépôt ne nomme pas le prestataire externe ; aucun nom de fournisseur ni aucune faille logicielle n'est donc ajouté ici.

Séparez intégrité des transactions, avoirs clients et disponibilité. Une banque peut retarder des virements légitimes pour contenir l'incident tout en examinant les mouvements frauduleux. Ces résultats nécessitent des preuves et communications différentes.

9.4 Validation commune

Signal	Ce qu'il peut justifier	Ce qu'il n'établit pas seul	Premier responsable
Divulgation de données financières avec références de comptes	Préparation aux usurpations convaincantes	Intrusion dans chaque banque associée	Fraude et opérations clients
Offre d'identifiants ou d'accès	Validation du compte et de la session	Connexion fonctionnelle ou incident général bancaire	Identité et réponse
Carte dans le périmètre limité du rapport	Validation par l'émetteur si justifiée indépendamment	Carte active, paiement réussi ou perte	Fraude cartes
Instruction de paiement inattendue	Vérification indépendante et revue	Autorité légitime parce que l'expéditeur connaît le client	Finance et fraude
Incident prestataire	Évaluation du périmètre, des dépendances et des déclarations	Intrusion dans les systèmes du client	Achats, réponse et protection des données
Virement retardé pendant l'endiguement	Évaluation de service et communication	Perte des avoirs clients	Exploitation et communication

9.5 DORA et éléments opérationnels

DORA s'applique aux entités concernées depuis le 17 janvier 2025. Les documents de l'ACPR identifient risque TIC, déclaration d'incidents, tests de résilience et risque des prestataires [S19]. Vérifiez l'applicabilité et le canal de déclaration actuel.

Reliez les fonctions critiques aux fournisseurs TIC réels, aux flux et aux chemins de reprise. Un registre de fournisseurs n'est utile que si l'institution peut relier une notification à un service et à une décision métier.

Testez si un même dossier peut alimenter réponse technique, classification prudentielle, protection des données et communication client. Les faits peuvent être partagés, les critères juridiques restent distincts. Une formule générique de 72 heures ne remplace pas l'analyse de chaque texte.

9.6 Priorités des équipes financières

Validez les accès. Rapprochez un signal d'un compte actif et examinez les sessions avant une action perturbatrice. Un contenu ancien ou sans correspondance appelle une décision documentée, pas une réinitialisation générale automatique.

Vérifiez les instructions. Exigez une autorité indépendante pour nouveau bénéficiaire, nouvelles coordonnées ou transfert exceptionnel. Récit convaincant, coordonnées connues et conversation existante peuvent tous participer à la tromperie.

Protégez la continuité. Exercez l'effet d'un endiguement sur virements, accès clients et institutions dépendantes. Convenez du droit de suspension, des solutions alternatives et des éléments permettant la reprise.

Exercez les prestataires. Demandez une première alerte au périmètre incertain. Mesurez si les équipes financières, de protection des données et de réponse peuvent décider sans attendre le rapport final.

POINTS À RETENIR

01

Séparez accès aux données financières, intégrité des paiements et disponibilité.

02

Limitez pertes estimées et observations de cartes à leur périmètre réel.

03

Réunissez identité, fraude et prestataires avant d'attribuer les actions.

CHAPITRE 10

Réponse réglementaire et nationale

10

CE CHAPITRE RÉPOND À LA QUESTION

Quelles règles et quels constats officiels doivent changer les opérations actuelles ?

3

décisions distinctes : protéger les données, évaluer la notification et documenter les corrections

10.1 Les obligations déjà applicables 84
10.2 NIS2 : une première lecture n'est pas une entrée en vigueur 85
10.3 Les sanctions de janvier concernent des incidents antérieurs 85
10.4 Les constats de novembre rendent les accès partagés actuels 86
10.5 Coordination et conservation des éléments 86
10.6 Ce que les RSSI doivent faire maintenant 87

CHAPITRE 10

Réponse réglementaire et nationale

EN BREF

Les obligations de sécurité des données personnelles s'appliquent déjà. Les entités financières relèvent aussi de DORA dans son périmètre. L'ANSSI décrit toujours la transposition française de NIS2 et présente son référentiel comme un document de travail. Les décisions récentes de la CNIL portent sur l'authentification, les accès des prestataires, les journaux et la conservation. Attribuez chaque texte à un responsable juridique et testez la notification avec les intervenants et les prestataires.

10.1 Les obligations déjà applicables

Le tableau distingue les obligations actuelles de la préparation d'un futur cadre national. Il s'agit d'une synthèse opérationnelle, pas d'un avis juridique.

Texte	Périmètre et statut	Exigence opérationnelle	Éléments à conserver
RGPD, article 32	Responsables de traitement et sous-traitants concernés	Mesures de sécurité adaptées au risque	Décisions d'accès, tests, détection et reprise [S18]
RGPD, article 33	Notification à l'autorité, sauf si la violation est peu susceptible de présenter un risque pour les droits et libertés des personnes physiques	Informer sans retard injustifié et, si possible, dans les 72 heures après en avoir pris connaissance	Chronologie, évaluation du risque, notification et mises à jour [S18]
RGPD, article 34	Information des personnes si la violation est susceptible d'engendrer un risque élevé, sous réserve des exceptions prévues	Informer sans retard injustifié dans un langage clair	Décision, population concernée, message et conseils [S18]
RGPD, article 33(2)	Sous-traitant ayant connaissance d'une violation de données	Informer le responsable de traitement sans retard injustifié	Alerte du prestataire, premier périmètre et évolutions [S18]
DORA	Entités financières concernées ; applicable depuis le 17 janvier 2025	Risque informatique, déclaration d'incidents, tests de résilience et risque lié aux prestataires TIC	Classification, déclarations, tests et informations contractuelles [S19]
Préparation française de NIS2	L'ANSSI décrit une transposition en cours et un référentiel de travail	Préparer le périmètre et les contrôles ; vérifier les textes adoptés avant de traiter un projet comme une obligation	Analyse d'applicabilité et texte officiel actuel [S20]

Les 72 heures ne constituent pas un délai universel pour tout événement cyber. L'article 33 exige une notification à l'autorité, sauf si la violation est peu susceptible de présenter un risque pour les droits et libertés des personnes physiques. Documentez la décision même si la notification n'est pas requise [S18].

L'information des personnes repose sur un autre critère. Le risque élevé pour leurs droits et libertés compte, et le message doit expliquer la nature, les conséquences probables et les mesures de protection. Un message rassurant ou un numéro d'assistance ne fournit pas nécessairement les informations requises [S14][S18].

Un prestataire ne devrait pas attendre un rapport complet avant une première alerte. Une information incomplète peut déjà aider le responsable de traitement. Consignez les faits connus à chaque décision et actualisez l'évaluation lorsque les éléments évoluent [S18].

10.2 NIS2 : une première lecture n'est pas une entrée en vigueur

À la clôture, la page de l'ANSSI décrit la transposition nationale et invite les futures entités essentielles et importantes à se préparer. Elle indique que le Référentiel Cyber France est disponible depuis le 17 mars 2026 comme document de travail [S20].

Le dossier législatif indique l'adoption d'un projet modifié en première lecture par la chambre basse le 17 novembre 2026. Il présente toujours un projet, pas une loi promulguée. C'est une évolution importante de la dernière quinzaine [S61].

La page de l'ANSSI présente son référentiel comme non obligatoire par défaut. Le rapport ne transforme donc pas une version de travail en obligation nationale adoptée. Il ne suppose pas non plus que le secteur d'une société suffit à déterminer sa catégorie juridique.

La préparation reste concrète. Identifiez les entités juridiques potentiellement concernées, les services critiques, les responsabilités de direction, les contacts de déclaration et les dépendances. Comparez les contrôles au référentiel officiel pendant que le conseil juridique vérifie les exigences et dispositions transitoires applicables.

Le programme de contrôle peut avancer malgré l'évolution du calendrier. La protection des identités, la gestion des incidents et celle des prestataires sont déjà justifiées par les cas décrits ici. Leur intérêt métier n'exige pas de présenter un projet comme une loi.

10.3 Les sanctions de janvier concernent des incidents antérieurs

L'annonce de la CNIL du 14 janvier décrit des amendes de 27 millions et 15 millions d'euros contre deux entités de télécommunications. Elle concerne un incident d'octobre 2024 touchant les données de 24 millions de contrats d'abonnement. Les contrats ne sont pas des personnes distinctes, et la sanction n'est pas une nouvelle intrusion de 2026 [S14].

La CNIL relève des faiblesses d'authentification des accès distants et de détection des comportements anormaux. Elle constate aussi des insuffisances dans l'information des personnes. Pour l'entité mobile, la décision porte également sur une conservation excessive [S14].

Un programme d'accès doit donc produire des preuves à plusieurs niveaux. Un service distant configuré, un outil déployé et un avis envoyé ne démontrent pas séparément que les contrôles ont atteint leur objectif.

L'annonce du 29 janvier concernant le service de l'emploi porte sur le premier trimestre 2024. La CNIL décrit l'ingénierie sociale visant des comptes de conseillers partenaires, des droits trop larges et une journalisation insuffisante [S15].

La CNIL indique aussi que des mesures adéquates avaient largement été identifiées sans être mises en œuvre. Ce constat justifie un test de clôture pour la direction : qui vérifie que le contrôle promis fonctionne réellement [S15] ?

10.4 Les constats de novembre rendent les accès partagés actuels

Le 9 novembre, la CNIL annonce dix sanctions simplifiées concernant des collectivités et un établissement public. Les constats comprennent une authentification administrative insuffisante, des accès permanents de prestataires, des comptes partagés, une journalisation inefficace, un cloisonnement faible et des systèmes obsolètes [S17].

Les amendes vont de 3 000 à 20 000 euros dans cette procédure. Ces montants ne sont ni un plafond général du RGPD, ni un tarif de non-conformité. Ils ne prouvent pas dix nouvelles intrusions en novembre [S17].

Le régulateur traite aussi l'homologation des systèmes administratifs et les analyses d'impact pour la vidéoprotection. Ces constats doivent rester dans leur contexte juridique. L'équipe de sécurité doit associer les responsables administratifs et de la protection des données, plutôt qu'appliquer une liste générique [S17].

Le 18 novembre, la CNIL annonce une sanction de 5 millions d'euros contre une société non nommée. Elle décrit des mots de passe clients en clair, des identifiants salariés partagés et une conservation excessive. La CNIL choisit de ne pas identifier la société ; le rapport respecte ce choix [S16].

La décision justifie une vérification immédiate du stockage des mots de passe et de la responsabilité individuelle. Elle n'établit pas un nouveau vol divulgué de mots de passe clients. Un constat de contrôle et une intrusion confirmée restent distincts.

10.5 Coordination et conservation des éléments

Les bilans de l'ANSSI décrivent l'assistance technique, les corrections et la communication de crise centralisée pour les services de l'État [S6][S7]. Ces activités ne remplacent ni l'évaluation de protection des données ni l'enquête judiciaire.

Créez une chronologie commune distinguant découverte, prise de connaissance, endiguement, restauration, notification et confirmation ultérieure. Désignez un responsable capable d'expliquer chaque horodatage. Ne substituez pas la date d'un article à celle de la prise de connaissance.

Conservez les faits nécessaires aux différents intervenants. La réponse technique a besoin des comptes, sessions, actions applicatives et exports. Les équipes de protection des données ont besoin des catégories de données et du risque. Les responsables de services ont besoin de preuves de continuité et de reprise.

La communication doit conserver des versions de l'état des connaissances. Le chiffre d'un acteur doit rester présenté comme tel jusqu'à confirmation indépendante. Une correction doit préciser quelle mesure évolue, plutôt que remplacer silencieusement un nombre.

10.6 Ce que les RSSI doivent faire maintenant

Décision	Responsable	Premier test	Preuve d'achèvement
Cartographier les obligations	Juridique et conformité	Classer un incident réaliste chez un prestataire selon chaque texte applicable	Matrice approuvée des obligations et contacts
Valider les corrections annoncées	RSSI et audit	Choisir un risque accepté antérieurement et démontrer le contrôle promis	Résultat technique et validation métier
Exercer la notification	Protection des données et réponse	Déclencher l'exercice à la prise de connaissance avec un périmètre prestataire incomplet	Journal de décision et projet de notification utilisable
Tester la communication	Communication et protection des données	Demander à un lecteur extérieur ce qu'il comprend des mesures à prendre	Avis clair révisé
Revoir la conservation	Responsables des données	Repérer les exports historiques inutiles et les dossiers arrivés à échéance	Preuves de suppression et registre d'exceptions

POINTS À RETENIR

01

Appliquez les obligations actuelles de sécurité et de résilience financière tout en vérifiant le calendrier national NIS2.

02

Traitez les décisions réglementaires dans les dates réelles des incidents concernés.

03

Testez notification, responsabilité individuelle et corrections, au-delà des documents de politique.

CHAPITRE 11

Perspectives et scénarios conditionnels

11

CE CHAPITRE RÉPOND À LA QUESTION

Quels jugements guident la préparation, et qu'est-ce qui les ferait évoluer ?

5

jugements avec une limite et un signal de changement

11.1 Jugements clés 89
11.2 Ce qui ferait évoluer l'évaluation 90
11.3 Scénarios conditionnels 90
11.4 Éviter les certitudes injustifiées 91

CHAPITRE 11

Perspectives et scénarios conditionnels

EN BREF

L'accès aux données par abus d'identité, la concentration des prestataires et la reprise restent prioritaires. Les inscriptions publiques justifient aussi la continuité dans plusieurs secteurs. L'incident industriel exige une réponse de sécurité physique distincte de la restauration informatique. Ces jugements sont conditionnels, sans probabilité d'attaque. Réévaluez-les lorsque des activités de comptes validées, de nouveaux constats officiels ou des effets opérationnels mesurés changent les éléments disponibles.

11.1 Jugements clés

La confiance s'applique à chaque proposition, pas à un acteur ou à un chapitre entier. Une priorité de contrôle bien étayée peut coexister avec une attribution incertaine.

Jugement	Confiance et fondement	Limite	Signal de changement
L'usage des données par des comptes valides mérite une attention immédiate	Élevée pour la priorité ; mécanismes répétés dans les enquêtes officielles [S7][S8] [S9]	Ne démontre pas la voie dominante de tous les incidents français	Des cas vérifiés montrent une autre voie ou les contrôles empêchent la même extraction
La notification des prestataires mérite des exercices communs	Élevée pour la gestion des dépendances ; divulgation du courrier et constats officiels sur les prestataires [S12] [S13][S17]	Aucune estimation nationale de prévalence	Un sous-traitant ne peut préciser le périmètre client ou un exercice manque une obligation
Les investissements de reprise restent justifiés	Élevée pour la préparation ; 295 inscriptions étiquetées France sur la période [S3]	Les revendications ne prouvent ni chiffrement, ni perte métier, ni victimes distinctes	Une interruption confirmée ou un échec de restauration change la priorité d'un service
Les accès industriels distants exigent un responsable de sécurité physique	Élevée pour ce besoin précis ; conséquences physiques signalées par les autorités [S10]	Ne démontre pas la même exposition chez tous les industriels	Paramètres non autorisés ou alarmes dangereuses exigent une escalade opérationnelle
Les nouvelles annonces exigeront un contrôle d'actualité	Moyenne comme jugement de préparation ; revendications conservées et avertissements officiels sur les republications [S1][S9]	La date d'une annonce n'est pas celle du vol	Des dossiers actuels, des sessions ou une déclaration indépendante établissent l'actualité

Un canal peu volumineux peut compter s'il propose un accès valide. Inversement, un grand volume étiqueté par pays peut contenir des promotions répétées ou des listes internationales. La capacité à changer une décision compte davantage que le seul nombre.

11.2 Ce qui ferait évoluer l'évaluation

Éléments de compte. Une correspondance avec un compte privilégié actif, une session inhabituelle et un export inexpliqué justifierait une escalade. Un ancien mot de passe déjà invalidé justifierait une autre décision documentée.

Éléments du prestataire. Une première notification peut s'élargir ou se réduire avec l'enquête. Un changement de catégories de données peut compter davantage qu'une hausse de population, notamment si apparaissent des données financières, de santé ou de mineurs.

Éléments opérationnels. Une revendication sur des équipements ne prouve pas un effet physique. Une configuration non autorisée, une alarme indépendante ou une interruption confirmée par l'exploitant changerait l'évaluation et le responsable de la réponse.

Éléments d'attribution. Un slogan commun ou des annonces simultanées ne démontrent pas une direction commune. Une attribution officielle nouvelle ou un lien technique étayé doit actualiser la carte avec sa source et son niveau de confiance.

Éléments de couverture. La validation des comptes et de leur propriété peut modifier les priorités dans l'ensemble évalué. Les domaines sélectionnés ne deviennent pas un échantillon national ; des données historiques n'établissent pas un accès actuel.

11.3 Scénarios conditionnels

Ces scénarios sont des hypothèses de préparation. Ils ne comportent ni probabilité numérique, ni résultat promis, ni estimation nationale de perte financière.

Scénario	Signal à surveiller	Première réponse	Preuve de clôture
Une nouvelle annonce concerne des clients actifs	Une correspondance interne confirme des dossiers actuels ou une déclaration officielle confirme la source	Conserver l'annonce, délimiter les données et examiner les accès	Décisions sur les comptes, applications et notifications
Un compte partenaire récupère un ensemble inhabituellement large	Consultations et exports sortent de la tâche métier autorisée	Limiter l'accès, conserver les sessions et associer le responsable applicatif	Frontière d'autorisation reproduite et activité d'export expliquée
Un prestataire critique signale un incident incertain	La première notification identifie le service mais pas la population	Réunir protection des données, achats et responsable de service	Mises à jour du périmètre et décision de notification
Une annonce politique désigne un service public	La revendication est suivie d'une interruption confirmée par l'exploitant	Activer l'atténuation et une communication factuelle	Mesures du service et dossier du fournisseur
Des paramètres distants changent sur un équipement	L'exploitant confirme un état non autorisé ou dangereux	Isoler l'accès selon le plan de sécurité	État sûr, accès revus et remise en service approuvée

11.4 Éviter les certitudes injustifiées

Une même annonce peut correspondre à plusieurs explications : vendeur initial, revendeur, promotion copiée, données historiques mélangées ou fabrication. Cherchez ensuite les éléments qui permettent de distinguer ces hypothèses.

Un rapport officiel peut aussi rester provisoire. La poursuite d'une enquête est une limite importante. Conservez-la dans la synthèse, la fiche de cas et l'action recommandée, surtout lorsqu'un acteur propose un chiffre supérieur.

Réévaluez les conclusions quand les éléments changent, sans attendre l'édition annuelle suivante. Une validation de compte ou une mise à jour d'un prestataire peut modifier une décision plus vite qu'un graphique national.

POINTS À RETENIR

01

Attribuez la confiance à une proposition précise et consignez ses limites.

02

Utilisez des signaux observables pour changer la réponse, le responsable et l'urgence.

03

Gardez les scénarios conditionnels jusqu'à ce que les comptes, les services ou une source officielle permettent de conclure davantage.

CHAPITRE 12

Plan d'action

12

CE CHAPITRE RÉPOND À LA QUESTION

Qui agit pendant les trois prochains mois, et comment démontrer les progrès ?

20

actions avec un responsable, un déclencheur et une preuve d'achèvement

12.1 Les étapes à 30/60/90 jours 93
12.2 Ce que signifie l'achèvement 96
12.3 Par rôle 96
12.4 Comment Brandefense peut aider 97

CHAPITRE 12

Plan d'action

EN BREF

Commencez par les accès permettant de récupérer des dossiers sensibles ou de modifier des opérations essentielles. Testez ensuite les prestataires, la restauration et les décisions antifraude. Terminez par une validation indépendante et le retrait des accès obsolètes. Le plan comporte 20 actions réparties sur 30, 60 et 90 jours. Attribuez chacune à un responsable métier et exigez la preuve du comportement obtenu, plutôt qu'un décompte de politiques ou d'outils.

12.1 Les étapes à 30/60/90 jours

Ces périodes sont des intervalles de préparation proposés, pas des délais légaux. Un incident actif ou une obligation de notification applicable reste prioritaire.

Agir immédiatement pour tout déploiement exposé et affecté, ou toute vulnérabilité applicable dont l'exploitation est signalée. Les responsables infrastructure et applications doivent corriger ou appliquer les mesures temporaires de l'éditeur et rechercher des activités antérieures [S22][S23]. Consigner les preuves de version déployée, les mesures appliquées et la conclusion de l'investigation. L'étape à 60 jours couvre le rapprochement de l'inventaire plus large avec les avis.

30 jours

Examiner chaque revendication actuelle d'identifiants ou d'accès correspondant à l'organisation ; distinguer actif, historique et sans correspondance

RESPONSABLE

Identité et réponse

PREUVE D'ACHÈVEMENT

Décision avec validité du compte, revue de session et escalade

Renforcer l'authentification des accès privilégiés, distants, prestataires et partenaires selon le risque métier

RESPONSABLE

Identité et responsables de services

PREUVE D'ACHÈVEMENT

Connexion, récupération et accès d'urgence testés

Retirer les droits de consultation dépassant le rôle métier

RESPONSABLE

Applications et données

PREUVE D'ACHÈVEMENT

Un utilisateur de test valide ne peut récupérer les dossiers non autorisés d'autrui

Alerter sur les extractions massives inattendues avec le contexte applicatif

RESPONSABLE

SOC et applications

PREUVE D'ACHÈVEMENT

Une simulation autorisée produit une alerte exploitable et une trace de réponse

Confirmer contacts d'incident et première alerte des sous-traitants détenant des données sensibles

RESPONSABLE

Achats et protection des données

PREUVE D'ACHÈVEMENT

Test de contact réussi et mises à jour convenues

Revoir les accès industriels distants et les procédures locales sûres

RESPONSABLE

Exploitation et sécurité physique

PREUVE D'ACHÈVEMENT

Carte approuvée, isolement testé et procédure de secours sûre

260 jours

Examiner les identifiants actifs au-delà du changement de mot de passe ; revoir sessions et appareils si justifié

RESPONSABLE

Identité et réponse sur les postes

PREUVE D'ACHÈVEMENT

Révocation des sessions, examen de l'appareil et clôture documentée

Remplacer l'administration partagée des prestataires par des accès individuels approuvés

RESPONSABLE

Infrastructure et prestataires

PREUVE D'ACHÈVEMENT

Comptes nominatifs, autorisations limitées dans le temps et activités revues

Tester les autorisations au niveau des objets sur les applications sensibles, dans une évaluation approuvée

RESPONSABLE

Sécurité applicative

PREUVE D'ACHÈVEMENT

Échec des extractions non autorisées et corrections retestées

Limiter les exports aux données et aux finalités métier nécessaires

RESPONSABLE

Responsables des données

PREUVE D'ACHÈVEMENT

Inventaire des exports, décisions d'accès et test d'extraction inhabituelle

Restaurer un service critique avec des sauvegardes protégées et des identifiants distincts

RESPONSABLE

Infrastructure et responsable de service

PREUVE D'ACHÈVEMENT

Temps de reprise, intégrité vérifiée et acceptation métier

Exercer un incident prestataire dont la population reste incertaine

RESPONSABLE

Protection des données, réponse et achats

PREUVE D'ACHÈVEMENT

Chronologie de prise de connaissance, première décision et réévaluation

Rapprocher l'inventaire applicatif plus large des avis pertinents et des branches déployées ; le déclencheur immédiat ci-dessus reste prioritaire

RESPONSABLE

Infrastructure et applications

PREUVE D'ACHÈVEMENT

Couverture de l'inventaire, versions déployées prouvées et décisions de correction suivies

Simuler un appel convaincant citant de vrais détails clients

RESPONSABLE

Fraude et opérations clients

PREUVE D'ACHÈVEMENT

La vérification indépendante bloque un paiement ou changement de compte non autorisé

Tester communication d'indisponibilité et contacts d'atténuation du fournisseur

RESPONSABLE

Exploitation et communication

PREUVE D'ACHÈVEMENT

Délai d'activation mesuré, canal alternatif testé et message factuel

390 jours

Retirer les accès obsolètes de partenaires, d'urgence et de migration après revue métier

RESPONSABLE

Identité et métiers

PREUVE D'ACHÈVEMENT

Retraits approuvés et exceptions justifiées, limitées dans le temps

Valider les journaux de l'identité jusqu'à l'application et l'export

RESPONSABLE

SOC et assurance

PREUVE D'ACHÈVEMENT

Chronologie complète d'un test avec utilisateurs identifiables

Réduire les dossiers historiques inutiles et les exports incontrôlés

RESPONSABLE

Protection des données et métiers

PREUVE D'ACHÈVEMENT

Suppressions approuvées et exceptions de conservation testées

Retester la restauration industrielle avec une surveillance physique indépendante

RESPONSABLE

Exploitation et sécurité physique

PREUVE D'ACHÈVEMENT

Restauration sûre, alarmes validées et accès prestataires revus

Présenter à la direction les exceptions et les résultats des tests

RESPONSABLE

RSSI et assurance

PREUVE D'ACHÈVEMENT

Décision avec responsable, échéance, risque résiduel et méthode de validation

12.2 Ce que signifie l'achèvement

Une trace de déploiement est un élément, pas un résultat. Testez l'authentification forte par les chemins normaux, la récupération de compte et les procédures d'urgence. Si un chemin alternatif contourne le contrôle, le métier doit comprendre et approuver ce risque résiduel.

Une alerte doit atteindre quelqu'un capable d'agir. Vérifiez qu'elle comporte compte, application, finalité métier et contexte d'extraction nécessaires à la décision. Un événement généré sans responsable ne clôt pas l'action de détection.

Un test de restauration doit démontrer le service métier, pas seulement la récupération d'un fichier. Vérifiez intégrité, dépendances, identifiants, fonctions clients et autorité de remise en service. Précisez ce que le test ne couvre pas.

Un test industriel exige une autorisation opérationnelle et des conditions sûres. Utilisez un exercice contrôlé plutôt qu'un changement de production destiné seulement à démontrer un point de sécurité. Le responsable de sécurité physique définit le test acceptable et les preuves de restauration.

12.3 Par rôle

Rôle	Première question	Éléments utiles	Déclencheur d'escalade
RSSI	Quel service présente la plus grande dépendance non résolue ?	Résultats testés d'accès et de reprise	Échec répété ou exception sans responsable
SOC	Peut-on relier une session valide à une extraction inattendue ?	Chronologie du compte, de l'application et de l'export	Accès sensible inexpliqué ou extraction massive
Identité	Le compte proposé est-il actif et encore fiable ?	État, sessions et récupération	Accès privilégié actif ou usage non autorisé corroboré
Application	Que peut récupérer un utilisateur valide peu privilégié ?	Tests par objet et par export	Données hors périmètre métier approuvé

Rôle	Première question	Éléments utiles	Déclencheur d'escalade
Fraude	Quels faits un interlocuteur convaincant connaît-il déjà ?	Tests de vérification et de transfert	Action sensible fondée sur les seuls détails personnels
Protection des données et juridique	Quand la prise de connaissance a-t-elle eu lieu, et quel risque en découle ?	Versions du périmètre et décisions de notification	Risque ou risque élevé selon l'obligation applicable
Achats	Le prestataire peut-il envoyer une première alerte et des mises à jour ?	Contacts et clauses testés	Responsable injoignable ou information critique absente
Exploitation et sécurité physique	Peut-on isoler l'accès distant sans créer de danger ?	Procédure de secours et restauration approuvées	Paramètres non autorisés ou état dangereux confirmé

12.4 Comment Brandefense peut aider

Utilisez le renseignement externe pour créer une tâche de validation attribuée. Une offre de données, une inscription d'identifiants ou un signal d'usurpation de marque devient utile quand il rejoint les comptes, dossiers, applications et processus de réponse de l'organisation.

Brandefense peut accompagner l'examen de ces signaux externes et de leur contexte métier. Le renseignement seul ne détermine ni si un compte client est actif, ni si une alerte prestataire déclenche une obligation, ni si une installation peut redémarrer sans danger. Ces décisions exigent des éléments internes et des responsables identifiés.

Pour échanger sur les priorités de surveillance et de réponse, emploiez la demande de démonstration Brandefense [S28]. Apportez une carte de service critique et une question concrète à valider.

POINTS À RETENIR

01

Attribuez chaque action à un responsable et à un test d'achèvement mesurable.

02

Validez accès, notification et reprise par des exercices réalistes.

03

Faites remonter les abus corroborés et les états dangereux sans attendre une tendance annuelle.

ANNEXES

Annexes

A–D

CE CHAPITRE RÉPOND À LA QUESTION

Annexe A. Périmètre, méthode et confiance · Annexe B. Registre des éléments · Annexe C. Sources · Annexe D. Glossaire

79
sources

Annexe A. Périmètre, méthode et confiance 99
Annexe B. Registre des éléments 102
Annexe C. Sources 103
Annexe D. Glossaire 107

Annexe A. Périmètre, méthode et confiance

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 ensembles de sources

La période nominale va du 1 janvier au 22 novembre 2026, date de clôture. Les publications emploient la date enregistrée. Inscription, incident, découverte, divulgation et décision d'un régulateur sont des événements différents.

Le dernier jour et les totaux mensuels de novembre sont partiels au moment de l'observation. L'activité récente désigne les informations publiées ou actualisées du 9 au 22 novembre, avec la date réelle de l'incident précisée lorsqu'elle est connue.

Le rapport associe quatre ensembles propres : publications conservées du dark web, inscriptions publiques de rançongiciels, observations d'exposition et passives de domaines sélectionnés et agrégats limités de cartes [S1] [S2][S3][S4]. Déclarations publiques et sources techniques apportent une corroboration ou un contexte distinct.

Ces ensembles ne sont jamais additionnés pour estimer des personnes, organisations ou attaques distinctes. Une publication peut proposer un événement ancien, une inscription répéter une victime et un domaine appartenir à un groupe déjà représenté.

A.2 Publications conservées et fiches

Les 7757 enregistrements de forum permettent des observations sélectionnées sur annonces, demandes et échanges. Ils comprennent 432 enregistrements datés de la dernière quinzaine. Ils forment un sous-ensemble des 7758 enregistrements de forums compris dans les 841760 enregistrements de la vue étiquetée, une entrée étiquetée d'octobre n'étant pas conservée (1849 sur 1850). Aucun ensemble n'établit incidents distincts, ciblage national ou activité malveillante vérifiée [S1].

Certaines dates enregistrées restent incohérentes. Le rapport ne déduit donc ni la date du vol, ni la première apparition d'une offre, ni un intervalle fiable entre annonces. Les fiches indiquent les dates enregistrées avec leur incertitude.

Les citations démontrent les déclarations faites, pas leur véracité. Aucun accès, carte ou fichier proposé n'a été testé ; aucun contact criminel ni achat n'a été effectué.

L'ensemble conservé ne doit pas être lu comme un registre d'incidents entièrement évalué. La couverture publique reste aussi limitée par la disponibilité des sources et par les divulgations originales non retrouvées.

A.3 Observations des domaines sélectionnés

L'ensemble contient 250 domaines de service candidats. Atlas couvre 249 domaines pour l'exposition et les observations passives en couvrent 237. La sélection est raisonnée ; des entités et services liés peuvent apparaître séparément. Propriété et indépendance restent à valider avant un classement indépendant [S2].

L'indicateur national Atlas vaut 63 sur une échelle de 0–100 pour cet ensemble évalué. Seul l'indicateur national est publié. Les tableaux sectoriels contiennent des observations, sans notes sectorielles ou individuelles.

Les observations d'exposition datent du 21 novembre 2026. La vue des domaines similaires couvre le 19 octobre–18 novembre 2026. Les mentions annuelles et observations passives se terminent le 22 novembre 2026. Les appareils constituent des minima ; identifiants, appareils, documents et mentions peuvent se recouper sans établir accès actuel ou intrusion confirmée.

Les observations passives décrivent politiques de messagerie, DNS, certificats et pages d'accueil. Elles ne démontrent pas l'efficacité des contrôles. Les résultats inconclusifs restent distincts des absences observées ou validations infructueuses.

A.4 Inscriptions de rançongiciels

Ransompedia fournit les inscriptions publiques associées à la France et aux quatre pays comparés. Le total emploie les dates de publication des inscriptions. La comparaison précédente couvre toute l'année 2025 et a donc une durée différente [S3].

Une inscription est une revendication. Elle ne démontre pas indépendamment chiffrement, vol, victime distincte, voie d'accès ou perte financière. Les étiquettes de pays et de secteur doivent être corroborées au niveau du cas avant de nommer une victime.

Les pays sont les catégories de la source. Certaines correspondances d'entités restent non résolues ; la comparaison n'établit pas indépendamment le lieu de chaque service ou personne touchée.

A.5 Périmètre des cartes

L'aperçu limité des cartes comprend 11 cartes associées à la France dans 5 enregistrements conservés. Parmi elles, 1 est associée à un émetteur et 10 au seul pays ; ces catégories sont disjointes [S4].

Ces chiffres ne mesurent ni le vol national de cartes, ni leur validité, ni des paiements réussis, ni les pertes de fraude.

A.6 Incidents publics et noms

Le chapitre 5 présente des cas sélectionnés et leurs limites, distinguant déclarations officielles, presse citant une organisation et revendications non vérifiées. La section 5.10 résume une sélection de récits non résolus. Ces tableaux ne sont pas un registre détaillé et ne transforment pas chaque élément conservé en attaque distincte.

Une organisation n'est nommée comme partie touchée que si une confirmation officielle et une couverture plus large étayent son nom dans le registre public. Les autres rôles restent génériques. Les titres et chemins révélant une partie non nommée sont retirés ; la racine du site éditeur est citée.

La couverture des sources publiques est incomplète et certains avis originaux restent indisponibles.

A.7 Confiance et attribution

Confiance élevée concerne une proposition étroite directement étayée par un élément conservé ou une source primaire claire. Conserver une annonce ne valide pas son contenu.

Confiance moyenne concerne une interprétation étayée mais comportant des alternatives importantes. Une hypothèse de préparation reste conditionnelle et indique un signal susceptible de la faire évoluer.

Non vérifié désigne une revendication dont l'authenticité, l'accès actuel, l'origine ou l'effet n'est pas établi. Contestations et démentis restent attribués. L'absence de corroboration ne démontre ni fabrication ni absence d'incident.

Les attributions étatiques restent celles de la source officielle ou de recherche nommée. Langue, discours politique et annonces simultanées ne suffisent pas à les étendre. Un modèle analytique est signalé lorsqu'il relie des observations sans lien concret entre acteurs.

A.8 Limites techniques et réglementaires

Chaque CVE nommé a été vérifié auprès du NVD et de l'éditeur pertinent [S21][S22][S24][S25][S26]. Les branches affectées et corrigées doivent être lues dans leur contexte produit. Un avis n'est pas un incident français confirmé.

La synthèse réglementaire distingue obligations actuelles, propositions, étapes parlementaires et sanctions d'incidents anciens [S14][S15][S16][S17][S18][S19][S20][S61]. Elle aide à préparer les décisions. L'applicabilité et les notifications exigent les faits propres à l'organisation et une analyse juridique actuelle.

Annexe B. Registre des éléments

Les fiches conservent les dates enregistrées et signalent leur incertitude chronologique. B07 conserve un original français avec une traduction anglaise signalée ; les autres originaux sélectionnés sont en anglais [S1].

Fiche	Date enregistrée	Lieu	Pseudonyme	Chapitre
B01	2026-03-19	Forum	Persona A	4
B02	2026-03-19	Forum	Persona A	4
B03	2026-06-17	Forum	Zab26	4
B04	2026-01-07	Forum	suicid	4
B05	2026-04-17	Forum	RubiconH4ck	4
B06	2026-09-12	Forum	lauraallen	4
B07	2026-01-09	Forum	near	4
B08	2026-05-04	Forum	OverSec	4
B09	2026-05-09	Forum	NormalLeVrai	4
B10	2026-09-03	Forum	updap	4
B11	2026-09-03	Forum	updap	4
B12	2026-09-03	Forum	updap	4
B13	2026-09-28	Forum	updap	4
B14	2026-01-04	Forum	Angel_Batista	4
B15	2026-01-30	Forum	kazutlg	4
B16	2026-02-20	Forum	HexDex	4
B17	2026-06-23	Forum	Edric	4
B18	2026-03-04	Forum	HexDex	4

Annexe C. Sources

Les numéros de sources qui n'apparaissent pas ont été retirés lors de la revue et ne sont pas cités. Chaque source externe a été lue et porte sa date de vérification. Les chemins retirés sont conservés en privé ; les citations publiques conservent la racine du site éditeur.

S1: Brandefense Blackhole records associated with France and retained forum evidence, 1 January–22 November 2026. Éléments propres conservés ; agrégats publics et fiches expurgées joints à cette édition. · vérifié le 2026-11-22.

S2: Atlas selected-domain exposure snapshot, 21 November 2026; mention and passive observations, 22 November 2026. Éléments propres conservés ; agrégats publics joints à cette édition. · vérifié le 2026-11-22.

S3: Ransompedia listing snapshot, France and four regional peers. Éléments propres conservés ; agrégats publics et fiches expurgées joints à cette édition. · vérifié le 2026-11-22.

S4: Brandefense payment-card aggregates for the narrow retained-post view. Éléments propres conservés ; agrégats publics joints à cette édition. · vérifié le 2026-11-22.

S5: DataReportal, Digital 2027: France, late-2026 observations. https://datareportal.com/reports/digital-2027-france · vérifié le 2026-11-22.

S6: CERT-FR, September operational update, 30 September 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-006.pdf · vérifié le 2026-11-22.

S7: CERT-FR, October operational update, published 12 November 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-010.pdf · vérifié le 2026-11-22.

S8: ANSSI, investigation of a tax-administration data incident, 29 September 2026; title withheld. https://cyber.gouv.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S9: CERT-FR, lessons from application data breaches, 20 October 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-008.pdf · vérifié le 2026-11-22.

S10: CERT-FR, French C4 attribution and industrial-controller incident, 9 November 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-009.pdf · vérifié le 2026-11-22.

S11: French diplomatic authority, attribution statement, 9 November 2026. https://www.diplomatie.gouv.fr/fr/presse-et-ressources/decouvrir-et-informer/actualites/declaration-d-attribution-a-l-iran-de-cyberattaques-visant-la-france · vérifié le 2026-11-22.

S12: France 24, company confirmation of a business-mailing provider incident, 14 November 2026; title withheld. https://www.france24.com/ (URL de l'article retirée) · vérifié le 2026-11-22.

S13: RFI, postal-services provider incident, 16 November 2026; title withheld. https://www.rfi.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S14: CNIL, mobile and fixed-line operators security sanctions, 14 January 2026; title withheld. https://www.cnil.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S15: CNIL, employment-service security sanction, 29 January 2026; title withheld. https://www.cnil.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S16: CNIL, anonymised password-storage and retention sanction, 18 November 2026. https://www.cnil.fr/fr/conservation-des-mots-de-passe-sanction-5-millions-deuros · vérifié le 2026-11-22.

S17: CNIL, local-authority cybersecurity sanctions, 9 November 2026. https://www.cnil.fr/fr/sanctions-cybersecurite-collectivites-territoriales · vérifié le 2026-11-22.

S18: CNIL, GDPR text, Articles 32–34. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4 · vérifié le 2026-11-22.

S19: ACPR, Digital Operational Resilience Act and supervisory information. https://acpr.banque-france.fr/fr/reglementation/focus-sur-la-reglementation/transverse/digital-operational-resilience-act-dora · vérifié le 2026-11-22.

S20: ANSSI, NIS2 transposition and working reference document. https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/directive-nis-2/ · vérifié le 2026-11-22.

S21: NVD, CVE-2026-72898. https://nvd.nist.gov/vuln/detail/cve-2026-72898 · vérifié le 2026-11-22.

S22: Metabase, security advisory and affected/fixed branches. https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf · vérifié le 2026-11-22.

S23: CERT-FR, NGINX alert, 18 November 2026. https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-017/ · vérifié le 2026-11-22.

S24: NVD, CVE-2026-123633. https://nvd.nist.gov/vuln/detail/cve-2026-123633 · vérifié le 2026-11-22.

S25: NVD, CVE-2026-123007. https://nvd.nist.gov/vuln/detail/cve-2026-123007 · vérifié le 2026-11-22.

S26: F5, security advisories for the two NGINX HTTP/2 vulnerabilities. https://my.f5.com/manage/s/article/K000163928 ; https://my.f5.com/manage/s/article/K000163926 · vérifié le 2026-11-22.

S27: IETF protocol documents for DMARC, SPF, DNSSEC, TLS, DKIM and HSTS. https://www.rfc-editor.org/info/rfc9989/ ; https://www.rfc-editor.org/rfc/rfc7208 ; https://www.rfc-editor.org/rfc/rfc4035 ; https://www.rfc-editor.org/rfc/rfc9846 ; https://www.rfc-editor.org/rfc/rfc6376 ; https://www.rfc-editor.org/rfc/rfc6797 · vérifié le 2026-11-22.

S28: Brandefense, public demo request page. https://brandefense.io/request-a-demo/ · vérifié le 2026-11-22.

S29: MITRE ATT&CK, Valid Accounts and Modify Parameter. https://attack.mitre.org/techniques/T1078/ ; https://attack.mitre.org/techniques/T0836/ · vérifié le 2026-11-22.

S31: National press, postal-group statement quoted on renewed January disruption; title withheld. https://www.leparisien.fr/ (URL de l'article retirée) · contenu vérifié le 2026-11-22 ; disponibilité de la référence variable.

S32: Technology press, sports-federation member-platform statement quoted, January 2026; title withheld. https://www.01net.com/ (URL de l'article retirée) · contenu vérifié le 2026-11-22.

S33: Franceinfo, social-contribution agency statement quoted, 20 January 2026; title withheld. https://www.franceinfo.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S34: Technology press, research-organisation historical payroll-data statement quoted, February 2026; title withheld. https://next.ink/ (URL de l'article retirée) · contenu vérifié le 2026-11-22.

S35: Finance ministry, financial-data service incident, 18 February 2026; title withheld. https://presse.economie.gouv.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S36: Technology press, medical-software provider statement quoted, February 2026; title withheld. https://www.zdnet.fr/ (URL de l'article retirée) · contenu vérifié le 2026-11-22.

S37: CERT-FR, messaging-account campaign alert, 20 March 2026; updated 18 June. https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-003/ · vérifié le 2026-11-22.

S38: Education authority, personnel-data incident, 24 March 2026; title withheld. https://www.education.gouv.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S39: Education authority, pupil-data incident, April 2026; title withheld. https://www.education.gouv.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S40: Interior authority, identity-document portal update, 21 April 2026; title withheld. https://www.interieur.gouv.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S41: Franceinfo, tourism reservation disclosure quoted, 16 May 2026; title withheld. https://www.franceinfo.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S42: Government digital directorate, messaging-account incident, 8 June 2026; title withheld. https://www.numerique.gouv.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S43: CNIL, false assistance after personal-data breaches, 24 June 2026. https://www.cnil.fr/fr/vigilance-accompagnement-violation-de-donnees · vérifié le 2026-11-22.

S44: CERT-FR, Turla targeting and attribution, 13 July 2026. https://cert.cyber.gouv.fr/cti/CERTFR-2026-CTI-004/ · vérifié le 2026-11-22.

S45: Cybermalveillance.gouv.fr, crypto-service disclosure and impersonation warning; published 22 January 2026; updated 8 June 2026. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/violation-de-donnees-secteur-crypto-actifs-202601 · vérifié le 2026-11-22.

S46: Cybermalveillance.gouv.fr, tax-refund phishing warning; published 15 July 2026; updated 8 September 2026. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/remboursement-impot-hameconnage · vérifié le 2026-11-22.

S47: Gendarmerie, false judicial summons warning, 11 August 2026. https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2026/prevention-mefiez-vous-des-escroqueries-a-la-fausse-convocation · vérifié le 2026-11-22.

S48: Gendarmerie, J3-directed international site disruption, 8 October 2026. https://www.gendarmerie.interieur.gouv.fr/unpj/actualites/plus-de-17-000-victimes-dont-des-mineures-trois-sites-de-diffusion-de-contenus-intimes-voles-fermes · vérifié le 2026-11-22.

S49: Crédit Mutuel Arkéa, fraudulent-transactions statement, 4 November 2026. https://www.cm-arkea.com/arkea/banque/upload/docs/application/pdf/2026-11/04112026_-_communique_-_le_credit_mutuel_arkea_annonce_avoir_ete_victime_dune_cyberattaque__2026-11-04_15-40-19_385.pdf · vérifié le 2026-11-22.

S50: Reuters, Crédit Mutuel Arkéa attributed loss estimate, 5 November 2026. https://www.reuters.com/legal/government/french-bank-credit-mutuel-arkea-says-100-million-missing-after-cyberattack-2026-11-05/ · vérifié le 2026-11-22.

S51: Shared publishing platform, radiology-software provider statement on earlier incident and later sale claim, November 2026; title withheld. https://fr.linkedin.com/ (URL de l'article retirée) · contenu vérifié le 2026-11-22 ; disponibilité de la référence variable.

S52: Press-release service, market-research group internal-system incident statement, November 2026; title withheld. https://www.globenewswire.com/ (URL de l'article retirée) · contenu vérifié le 2026-11-22 ; disponibilité de la référence variable.

S53: Report URI, international third-party script incident, 16 November 2026; title withheld. https://blog.report-uri.com/ (URL de l'article retirée) · vérifié le 2026-11-22.

S54: French-language monitor, closing-period claims and follow-ups; article URLs withheld. https://frenchbreaches.com/ (URL de l'article retirée) · vérifié le 2026-11-22.

S55: CNIL, private-hospital sanction for an earlier incident, 3 September 2026; title withheld. https://www.cnil.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S56: Cybermalveillance.gouv.fr, false contest-vote messaging campaign; published 27 October 2026; updated 3 November 2026. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/vigilance-faux-vote-whatsapp · Vérifié le 23 novembre 2026.

S57: Energy supplier, commercial-partner incident, 27 October 2026; title withheld. https://www.bleepingcomputer.com/ (URL de l'article retirée) · vérifié le 2026-11-22.

S58: Vocational-training agency, external accommodation-tool incident, 21 September 2026; title withheld. https://www.01net.com/ (URL de l'article retirée) · vérifié le 2026-11-22.

S59: Education press, public agronomy institution disruption notice quoted, January 2026; title withheld. https://etudiant.lefigaro.fr/ (URL de l'article retirée) · contenu vérifié le 2026-11-22 ; disponibilité de la référence variable.

S60: Cybersecurity press, public agronomy school internship-record extraction notice quoted; title withheld. https://www.cyberattaque.org/ (URL de l'article retirée) · contenu vérifié le 2026-11-22.

S61: French legislative records, amended resilience and cybersecurity bill, first reading 17 November 2026. https://www.assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731#AN1 ; https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000050349138/ · vérifié le 2026-11-22.

S62: Cato CTRL, Operation Poisson, 16 June 2026. https://www.catonetworks.com/blog/cato-ctrl-operation-poisson-analyzing-a-cybercriminals-entire-operation/ · vérifié le 2026-11-22.

S63: Regional public broadcaster, alumni-platform disclosure, April 2026; title withheld. https://france3-regions.franceinfo.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S64: Local press, university web-shop script incident, September 2026; title withheld. https://www.toutmontbeliard.com/ (URL de l'article retirée) · vérifié le 2026-11-22.

S65: Technology press, research institute exposure statement quoted, August 2026; title withheld. https://next.ink/ (URL de l'article retirée) · contenu vérifié le 2026-11-22.

S66: Business-software provider, original multi-instance statement; title withheld. https://fr.linkedin.com/ (URL de l'article retirée) · vérifié le 2026-11-22.

S67: Technology press, external-operator disclosure, January 2026; title withheld. https://www.01net.com/ (URL de l'article retirée) · vérifié le 2026-11-22.

S68: Cybersecurity press, hospital imaging-supplier notice quoted, November 2026; title withheld. https://www.cyberattaque.org/ (URL de l'article retirée) · contenu vérifié le 2026-11-22.

S69: Technology press, student-support appointment-platform notice quoted, March 2026; title withheld. https://www.01net.com/ (URL de l'article retirée) · contenu vérifié le 2026-11-22.

S70: News-agency reporting, regulated-owner records disclosure, March 2026; title withheld. https://www.tf1info.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S71: News-agency reporting, health-prevention document-platform disclosure, August 2026; title withheld. https://www.tf1info.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S72: Technology press, primary-school administration notice quoted, March 2026; title withheld. https://next.ink/ (URL de l'article retirée) · contenu vérifié le 2026-11-22.

S73: Higher-education authority, admissions-module notice, 23 April 2026; title withheld. https://www.enseignementsup-recherche.gouv.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S74: Technology press, school-sport historical extraction notice quoted, March 2026; title withheld. https://www.01net.com/ (URL de l'article retirée) · contenu vérifié le 2026-11-22.

S75: Public broadcaster, health-ministry population statement, 27 February 2026; title withheld. https://www.franceinfo.fr/ (URL de l'article retirée) · vérifié le 2026-11-22.

S76: Tourism trade press, provider CEO interview and recovery update, 20–21 November 2026; title withheld. https://www.lechotouristique.com/ (URL de l'article retirée) · vérifié le 2026-11-22.

S77: Credential-security research, combolist definition and historical-data repetition. https://spycloud.com/blog/plot-twist-combolists-are-still-a-threat/ · vérifié le 2026-11-22.

S78: Crédit Mutuel Arkéa, Amendement n° 2 au Document d'enregistrement universel 2025, 18 novembre 2026. https://www.cm-arkea.com/arkea/banque/upload/docs/application/pdf/2026-11/cma_amendement_semestriel_2025_fr_n2_20261118.pdf · Vérifié le 23 novembre 2026.

S79: ANSSI et CERT-FR, Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002), 11 mars 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf · Vérifié le 23 novembre 2026.

S80: ANSSI, Présentation du Panorama de la cybermenace 2025, 11 mars 2026. https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2025/ · Vérifié le 23 novembre 2026.

Annexe D. Glossaire

Terme	Définition simple
C4	Centre de Coordination des Crises Cyber, instance interministérielle française d'analyse de la menace informatique [S10].
Credential	Secret d'authentification ou information de compte associée. Sa présence n'établit pas sa validité actuelle.
Liste combinée (combolist)	Liste compilée d'identifiants de compte et de mots de passe pouvant réunir ou répéter des données anciennes. Sa présence n'établit pas sa validité actuelle [S77].
Session	Interaction authentifiée pouvant se poursuivre après la connexion initiale.
MFA	Authentification utilisant plusieurs facteurs. Sa solidité dépend aussi de la récupération et des validations.
Object-level authorisation	Vérification du droit de consulter le dossier précis demandé, au-delà de la connexion.
Infostealer	Logiciel malveillant collectant notamment des secrets de connexion et des données de session.
Ransomware listing	Revendication publique liée à l'extorsion ; elle ne confirme pas seule chiffrement ou vol.
Controller	Partie déterminant les finalités et les moyens du traitement de données personnelles.
Processor	Partie traitant des données personnelles pour un responsable de traitement, dans ce périmètre.
DMARC	Préférence publiée du domaine pour le traitement des messages selon leur authentification et pour les rapports.
SPF	Déclaration publiée des infrastructures autorisées à envoyer pour une identité de messagerie.
DKIM	DomainKeys Identified Mail utilise des signatures cryptographiques pour associer un domaine signataire à un courriel [S27].
HSTS	HTTP Strict Transport Security est une politique de site demandant aux navigateurs d'utiliser des connexions sécurisées vers ce site [S27].
DNSSEC	Extensions du DNS permettant de valider des informations DNS signées.
TLS	Protocole protégeant les communications en transit ; un résultat de certificat n'évalue pas l'application.

Terme	Définition simple
DORA	Cadre européen de résilience opérationnelle numérique du secteur financier, dans son périmètre.
ReCyF	Référentiel français de cybersécurité présenté par l'ANSSI comme document de travail à la clôture.

Les définitions suivent les sources techniques, de recherche et juridiques citées dans les chapitres concernés [S9] [S10][S18][S19][S20][S27][S77].

À propos de ce rapport

Odin by Brandefense a préparé cette édition pour les responsables de sécurité et les équipes opérationnelles. Elle aide à valider les éléments, préparer la continuité et décider face à un incident. Elle n'authentifie pas les offres criminelles, n'estime pas la prévalence nationale et ne remplace pas une enquête interne.

L'édition française est traduite du document maître anglais. En cas de divergence de sens, l'anglais fait foi. La publication et toute mise à jour exigent le processus de revue et de diffusion applicable.

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