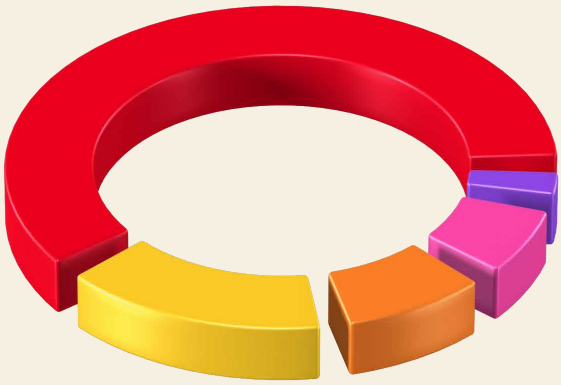
Rapport Data Breach Investigations Report – DBIR – 2026

Document de synthèse

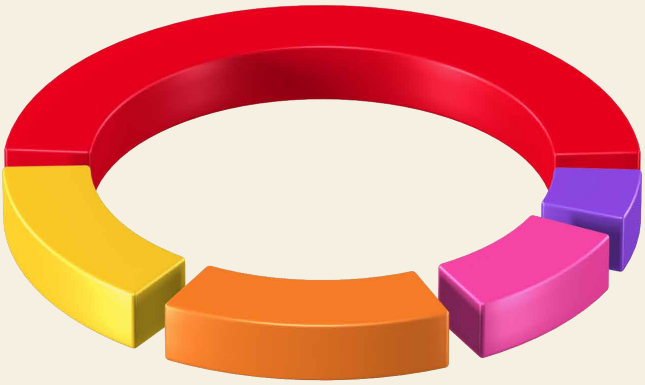
verizon business

2026



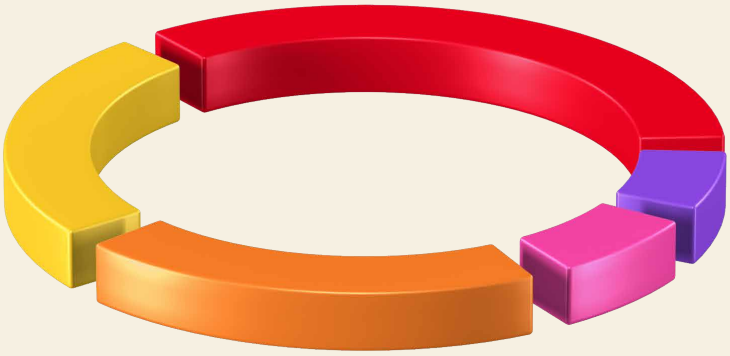
- **61 %** Intrusion système
- **17 %** Ingénierie sociale
- **10 %** Attaques d'applications web de base
- **8 %** Erreurs diverses
- **3 %** Abus de privilèges

2025



- **53 %** Intrusion système
- **18 %** Attaques d'applications web de base
- **17 %** Ingénierie sociale
- **12 %** Erreurs diverses
- **7 %** Abus de privilèges

2024



- **36 %** Intrusion système
- **25 %** Erreurs diverses
- **22 %** Ingénierie sociale
- **9 %** Attaques d'applications web de base
- **8 %** Abus de privilèges

À propos de l’image en couverture

« La seule constante est le changement », aurait affirmé le philosophe grec Héraclite. Même si aucun élément historique n’indique qu’il se soit essayé à la cybersécurité, nous sommes persuadés que sa façon de penser l’aurait prédestiné à une carrière dans notre domaine. Baromètre annuel du paysage des menaces en constante mutation, l’édition 2026 du Data Breach Investigations Report (DBIR) invite à affronter le changement permanent en se recentrant sur les fondamentaux de la cybersécurité. Du cyber-stoïcisme, en quelque sorte.

Les cercles concentriques en couverture représentent chacun une année de données se déposant en couches successives sur le socle de notre expertise en cybersécurité. Segmentés par schémas d’incident observés au cours des quatre dernières années, ils enrichissent notre compréhension et complètent nos stratégies défensives.

Le cercle supérieur représente l’édition 2026, suivi des années 2025, 2024 et enfin 2023, déjà intégrée au socle.

Parmi les grandes tendances observées cette année, les attaques zero day et les vulnérabilités critiques gagnent du terrain, les malwares augmentés par IA générative (GenAI) se généralisent et les formes complexes d’ingénierie sociale gagnent en efficacité comme vecteur d’intrusion initiale. Les attaquants sont certes plus rapides et leur force de frappe a de quoi inquiéter, mais les équipes de sécurité sont depuis longtemps confrontées à cette réalité. Nous vivons dans un nouveau monde qui demande davantage d’agilité et de focus, mais rien n’indique qu’un big-bang ne soit nécessaire. L’évolution, pas la révolution. Nous serons prêts à affronter l’avenir si nous continuons d’œuvrer ensemble pour un monde meilleur.

Et oui, nous avons opté pour des diagrammes en forme d’anneaux, malgré leur relative impopularité. Promis, ils resteront lisibles. Bonne lecture !

Sommaire

Introduction 5

Mode d'emploi du rapport 6

Thématiques et faits marquants 9

Gros plan par secteur 13

Enseignement 13
Finance et assurance 14
Santé 14
Industrie 15
Service public 15
Retail 16
PME et ETI 16

Tour d'horizon d'autres secteurs 17

Résultats par région 19

S'informer, c'est se préparer. 21

Introduction

Bienvenue dans le DBIR 2026 de Verizon, en particulier à nos nouveaux lecteurs, et bien sûr à celles et ceux qui nous font le plaisir de nous suivre depuis des années. C'est toujours un honneur et un plaisir de vous compter parmi nous.

Dans cette 19e édition du Verizon DBIR, nous décortiquons plus de 31 000 incidents de sécurité réels survenus dans des entreprises réparties dans 145 pays, dont au moins 22 000 compromissions de données avérées. Jamais nous n'en avions examiné autant dans un seul rapport ! Certes, c'est peu ou prou ce que nous répétons tous les ans, mais que voulez-vous ? Tant que le nombre de cas étudiés poursuivra son augmentation d'année en année, nous continuerons de battre nos records. Faut-il s'en réjouir ? À vous de juger. Les entreprises victimes ne le voient certainement pas d'un très bon œil, mais leurs expériences nous permettent de mettre en lumière les menaces qui pèsent sur vos activités pour mieux vous en protéger. Un mal pour un bien, en somme.

Si une thématique globale ressort de ce rapport, c'est certainement l'importance de conserver des appuis solides face aux changements. Or, par bien des aspects, une succession rapide de transformations profondes est en train de bouleverser nos vies. Peu de personnes nous contrediront sur ce point. À travers les analyses contenues dans ce rapport, nous voulons aider les entreprises à affronter le mieux possible les évolutions cyber en cours. Pour cette édition, notre corpus de données s'étend d'octobre 2024 à novembre 2025. Néanmoins, Verizon en général, et l'équipe DBIR en particulier, sont tout à fait conscients des développements à l'œuvre dans le domaine de l'IA générative en 2026, tant pour la détection de vulnérabilités que pour la conception d'exploits, selon les premiers chiffres et tendances observés au moment de la publication. Nous tenterons donc de proposer quelques commentaires prospectifs à ce sujet, le cas échéant.

Nous avons remarqué que, dans certains domaines, la cybercriminalité a connu une profonde mutation depuis la publication de notre rapport 2025. Dans d'autres, ce sont avant tout la vitesse et le périmètre d'action qui changent d'échelle, plus que la nature même des menaces. L'exploitation de vulnérabilités, qui revient dans plusieurs parties du rapport, émerge désormais comme le vecteur d'accès initial privilégié des attaquants. D'où l'importance de maîtriser les fondamentaux de la sécurité. En outre, comme les oracles des temps anciens[1] l'avaient prédit, les acteurs de menace intègrent de plus en plus la GenAI pour gagner en efficacité à différents stades de l'attaque : choix des cibles, implantation dans l'environnement de la victime, recherche de vulnérabilités et développement de malwares, entre autres. En parallèle, l'ingénierie sociale – depuis longtemps une valeur sûre pour les attaquants – s'adapte également aux nouveaux usages. Ainsi, les hackers exploitent de plus en plus des appels vocaux ou autres techniques « mobile-first » pour prendre leurs victimes de court en pleine journée de travail.

Dans les pages qui suivent, vous découvrirez les principales conclusions du rapport DBIR, en particulier les derniers chiffres sur les compromissions par secteur et par région. N'hésitez pas à partager avec vos collègues et à télécharger le rapport complet pour une vue plus détaillée des menaces qui pèsent sur votre activité.

1. Par « temps anciens », nous voulons parler des deux derniers rapports DBIR, que nous mentionnons quelques paragraphes plus haut.

Grille de lecture du rapport

Nouveaux lecteurs :

Avant d'entamer votre exploration du rapport DBIR 2026, nous vous invitons à consulter cette grille de lecture. Depuis le temps que nous publions ces analyses, nous savons combien notre vocabulaire peut parfois sembler difficile à appréhender pour nos lecteurs. Cette apparente complexité tient à notre exigence de précision : les conventions de nommage, la terminologie et les définitions sont toutes mûrement réfléchies, et nous veillons à les respecter assidûment tout au long du rapport. Nous espérons que cette entrée en matière les rendra plus accessibles. Si vous nous lisez depuis longtemps (merci à vous) et détenez déjà les clés de lecture du DBIR, nous vous invitons à passer directement à la partie suivante.

Périmètre et objectifs du rapport

Le Data Breach Investigations Report (DBIR) se concentre avant tout sur l'analyse de données anonymisées relatives aux incidents de sécurité, recueillies chaque année par Verizon auprès d'une centaine de contributeurs. Celles-ci sont normalisées selon le framework VERIS (Vocabulary for Event Recording and Incident Sharing), dont nous parlons plus en détail à la page suivante. Ce référentiel établit un schéma solide pour l'analyse statistique de ce type de données. Compte tenu de la culture du secret qui entoure les incidents de sécurité, sans parler de la difficulté à y répondre, nous disposons rarement de détails très spécifiques sur un incident donné.

Ce qui nous démarque ? Le large éventail de données collectées. Lorsque le rapport d'un fournisseur ne couvre que les cas sur lesquels il est lui-même intervenu, il peut en effet proposer une analyse détaillée des incidents, fondée sur une connaissance approfondie des scénarios en question. Chez Verizon, nous cherchons à concilier plusieurs perspectives et types de contributeurs : grands acteurs de la réponse à incident, cabinets spécialisés dans l'analyse forensique, pouvoirs judiciaires à l'échelle locale ou nationale, courtiers en cyberassurance, réassureurs, etc. Notre objectif : dresser le tableau le plus fidèle possible du paysage actuel des menaces.

Nomenclature VERIS

Vous rencontrerez souvent les termes « actions de menace », « acteur de menace » et « variétés », empruntés au VERIS, un référentiel conçu pour uniformiser la collecte d'informations sur les incidents de sécurité, et ainsi dissiper toute ambiguïté. Ils doivent être compris selon les définitions suivantes :

Acteur de menace : qui est à l'origine de l'événement ? Il peut s'agir d'un acteur malveillant externe, par exemple à l'origine d'une campagne de phishing, mais aussi d'un collaborateur étourdi oubliant des documents sensibles dans la poche de siège d'un avion.

Action de menace : quelles tactiques (actions) ont été employées ? VERIS classe les attaques en sept catégories principales : Malware, Hacking, Ingénierie sociale, Abus, Effraction physique, Erreur et Environnemental. Elles peuvent prendre la forme d'un serveur piraté, d'un malware installé sur un poste de travail ou d'un comportement anormal influencé par l'ingénierie sociale.

Variété : les dénominations spécifiques au sein des catégories générales. Il s'agit, par exemple, de classifier l'acteur malveillant externe comme appartenant au crime organisé ou d'identifier un hacking comme une injection SQL ou une attaque par force brute.

En savoir plus :

- github.com/vz-risk/veris — Vous y trouverez le schéma JSON du référentiel avec des mises à jour, des scripts d'utilitaires, des listes de dénomination, des correspondances avec les Critical Security Controls (CSC) du CIS et MITRE ATT&CK, ainsi qu'un guide de style VERIS
- verisframework.org — Site légèrement plus convivial offrant des informations sur le référentiel, avec des exemples et des listes de dénominations

Incident ou compromission ?

Lorsque nous parlons d'incidents et de compromissions, nous les entendons aux sens suivants :

Incident : événement de sécurité qui compromet l'intégrité, la confidentialité ou la disponibilité d'une ressource informatique.

Compromission : incident qui entraîne la divulgation avérée, et pas uniquement l'exposition potentielle, de données à une entité non autorisée. Une attaque par déni de service distribué (DDoS), par exemple, relève plus souvent de l'incident que de la compromission, car des données sont rarement exfiltrées. Non pas qu'elle soit inoffensive, bien au contraire.

Intitulés de secteurs

Notre classification sectorielle repose sur les codes du Système de classification des industries de l'Amérique du Nord (SCIAN). Ce système utilise des codes de deux à six chiffres pour catégoriser les entreprises. Notre analyse porte généralement sur le niveau à deux chiffres, et nous indiquons le code SCIAN pour chaque intitulé de secteur. Ainsi, dans l'intitulé « Finance (52) », le nombre 52 ne correspond pas à une valeur, mais au code défini pour ce secteur. Dans les graphiques, l'intitulé général de « Finance » est employé par souci de concision. De plus amples détails sur les codes et le système de classification sont disponibles ici : census.gov/naics.

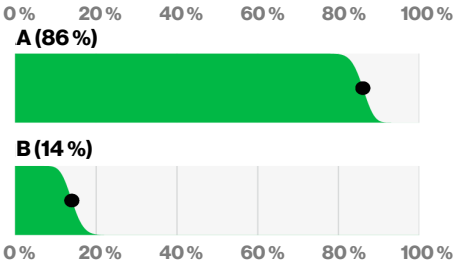


Figure 2. Exemple de diagramme en barres à extrémité inclinée (n=230)

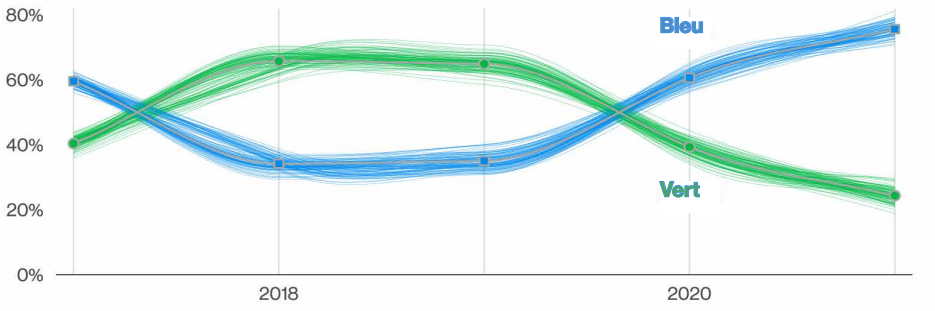


Figure 1. Exemple de diagramme spaghetti

Des données dignes de confiance

Depuis 2019, le DBIR adopte les graphiques en barres à extrémité oblique pour démontrer qu'en matière de sécurité des systèmes d'information, la seule certitude est que rien n'est certain. Malgré toutes les données à notre disposition, nous ne serons jamais sûrs à 100 %. Mais loin de nous l'envie de baisser les bras ou, pire, d'inventer des chiffres de toutes pièces, même devant la difficulté de mesurer quoi que ce soit dans un monde cyber en carence de données. À la place, nous nous sommes simplement mis au travail. Cette année encore, vous verrez cette part d'incertitude représentée dans l'ensemble du rapport.

Les exemples des Figures 1, 2 et 3 illustrent diverses réalités, toutes potentiellement vraies dans cette marge de confiance. Que ce soit à travers l'inclinaison de l'extrémité des barres, les fils, les points ou les couleurs choisis, tous nos diagrammes expriment à leur manière l'incertitude ambiante dans le secteur de la cybersécurité.

Les habitués de ce rapport connaissent bien notre diagramme en barres à extrémité oblique. Le degré d'inclinaison représente le degré d'incertitude du point de données à un niveau de confiance de 95 % (typique dans le domaine des statistiques). Pour faire simple, si les parties inclinées de deux barres (ou plus) se recoupent, on ne peut pas dire que l'une est plus grande que l'autre sans courroucer les dieux des mathématiques.

De la même manière, le diagramme spaghetti représente lui aussi les valeurs possibles qui existent dans l'intervalle de confiance. À la seule différence qu'il intègre aussi le facteur temps, ce qui le rend légèrement plus complexe. Les fils correspondent chacun à un échantillon des connexions possibles entre les points situés dans l'intervalle de confiance de chaque cas étudié. Comme vous pouvez le voir, certains sont plus relâchés que d'autres, signe d'un intervalle de confiance plus large pour un échantillon moindre.

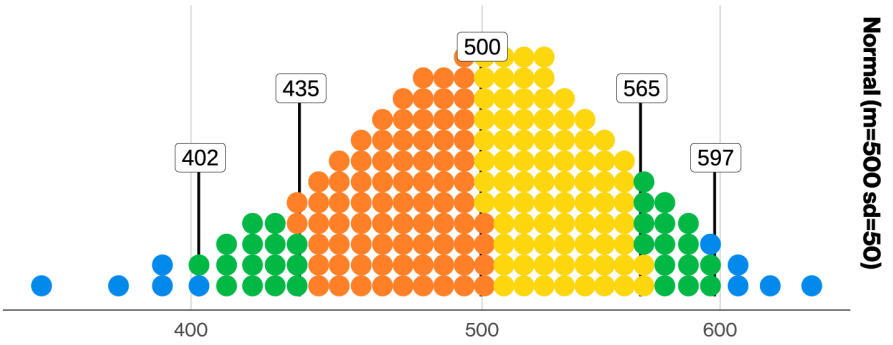


Figure 3. Exemple de diagramme à points (n=10 000, chaque point représente un événement)
Orange : moitié inférieure des 80 % ; jaune : moitié supérieure des 80 % ; vert : 80–95 % ; bleu : cas particuliers ; 95 % des événements : 402–597 ; 80 % des événements : 435–565 ; médiane : 500

Le diagramme à points est un autre classique. Pour le comprendre, il faut garder à l'esprit qu'un seul point équivaut à un nombre précis d'événements, indiqué dans la légende. Ce format permet d'exprimer clairement la distribution d'un phénomène dans l'ensemble des entreprises, tout en fournissant bien plus d'informations qu'une simple moyenne ou médiane. Dans un souci didactique, nous avons ajouté aux diagrammes des couleurs et des légendes. En termes statistiques, il s'agit simplement d'un diagramme de densité quantifiée. Et d'un point de vue plus profane, qui n'aime pas un joli dessin avec des pois colorés ?

Thématiques et faits marquants

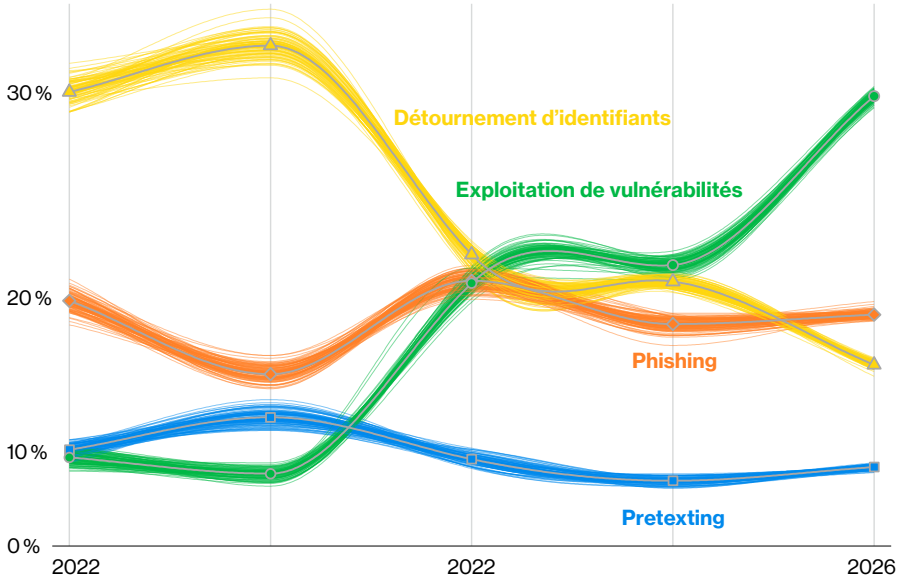


Figure 4. Évolution des principaux vecteurs d'accès initial dans les compromissions hors erreurs et abus de privilèges au fil des ans (pour les données de l'étude 2026, n=19 905)

Hausse de l'exploitation de vulnérabilités

L'exploitation de vulnérabilités constitue désormais le principal vecteur d'accès initial pour les compromissions recensées. Elle représente 31 % des données étudiées cette année, tandis que le détournement d'identifiants, autrefois n°1, est tombé à 13 %.

Seuls 26 % des vulnérabilités critiques, telles que définies par le catalogue CISA KEV (Cybersecurity Infrastructure and Security Agency Known Exploited Vulnerabilities), ont fait l'objet d'une résolution complète – un chiffre en forte baisse par rapport à l'an dernier (38 %).

Le délai médian de résolution complète s'est élevé à 43 jours, soit quasiment deux semaines de plus qu'en 2024 (32 jours). Dans le cas médian, les entreprises ont dû corriger 50 % de vulnérabilités critiques de plus que l'année précédente.

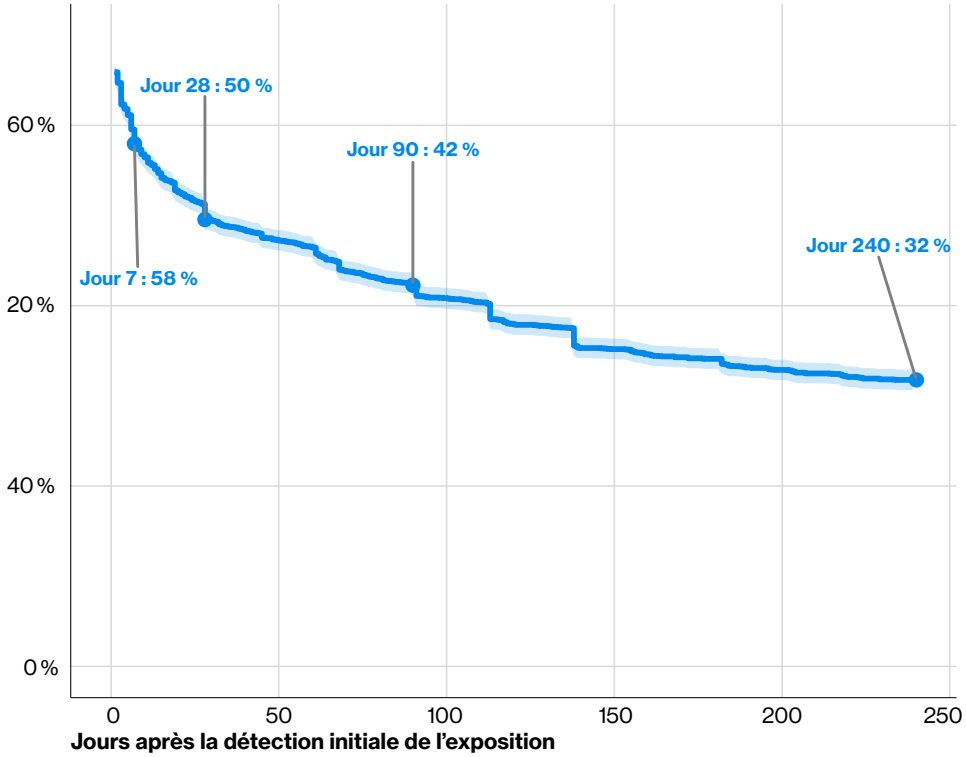


Figure 5. Analyse de survie lors d'expositions de la MFA des entités cloud tierces (n=7 513)

Les compromissions par ransomware continuent d'augmenter

La part des ransomwares dans les vecteurs de compromission ne cesse de croître, passant de 44 % l'an dernier à 48 % cette année. Avec une bonne nouvelle, toutefois : le paiement des rançons perd encore du terrain, avec 69 % des victimes ayant choisi de ne pas payer. Le montant médian de la rançon poursuit aussi sa baisse globale, s'élevant aujourd'hui à 139 875 US$ selon nos données, contre 150 000 US$ l'an passé.

Les entreprises se tournent de plus en plus vers des services et logiciels tiers, ce qui les expose à davantage de risques cyber. En témoigne la hausse de 60 % des incidents imputables à un tiers, comptant pour 48 % des compromissions.

Si l'on se penche sur les attaques visant le cloud en particulier, seuls 23 % des prestataires externes ont entièrement corrigé les mauvaises configurations, voire l'absence totale, d'authentification multifacteur (MFA) de leurs comptes cloud. Par ailleurs, 50 % des détections ont été résolues en l'espace d'un mois.

Côté mots de passe faibles et erreurs de configuration des autorisations, la moitié des cas observés ont été plus lents à résoudre, atteignant huit mois en moyenne.

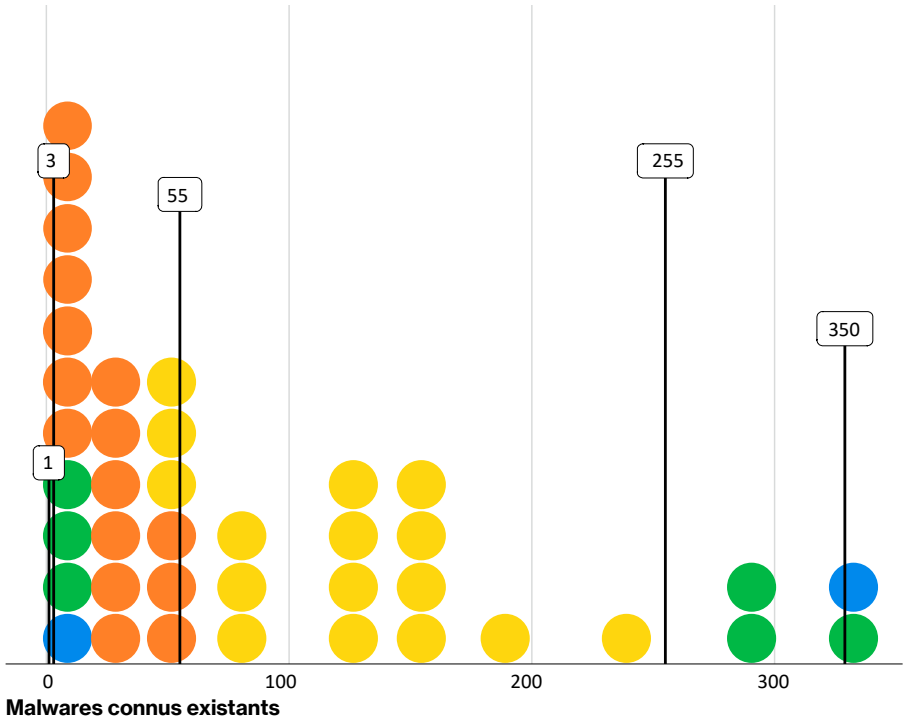


Figure 6. Répartition des malwares connus par technique ATT&CK observée (n=9 897, chaque point correspond à 247,43 observations)

La menace change de visage avec la GenAI

Les acteurs de menace exploitent la puissance offensive de la GenAI à plusieurs stades de l'attaque, du choix de la cible à l'obtention de l'accès initial, en passant par le développement de malwares ou d'autres outils. Ainsi, l'acteur type s'est servi de l'IA pour effectuer des recherches ou pour développer 15 techniques documentées différentes, avec des pics à 40 voire 50 dans certains cas.

La plupart des outils malveillants développés avec l'aide de l'IA étaient associés à des méthodes d'attaque bien connues. Nous avons relevé une médiane de 55 malwares connus remplissant les mêmes fonctions, tandis que moins de 2,5 % des attaques assistées par IA observées ont employé des techniques plus inhabituelles, avec un malware connu ou moins.

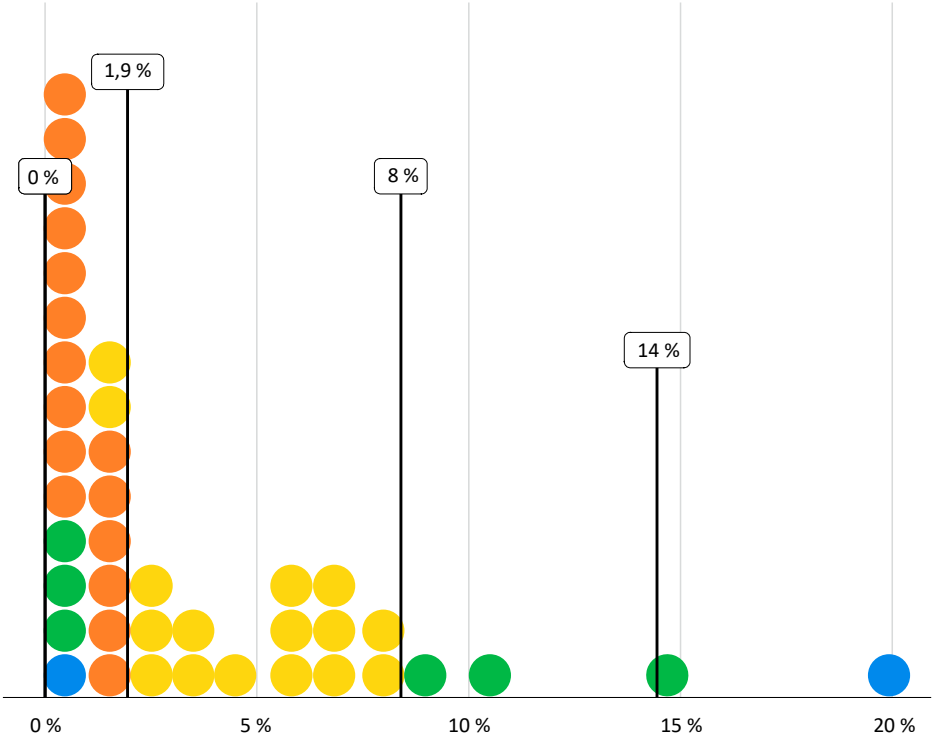


Figure 7. Répartition des taux de réussite des campagnes d'attaque par ingénierie sociale simulées hors e-mail (n=35, chaque point correspond à 0,88 campagne)

L'ingénierie sociale se recentre sur le mobile

Le facteur humain se retrouve dans 62 % des compromissions, une légère augmentation depuis l'année dernière (60 %). Troisième schéma de compromission le plus courant, l'ingénierie sociale représente 16 % de tous les incidents.

Dans les simulations de phishing, les vecteurs mobiles (appels vocaux et SMS) affichent un taux de clic médian 40 % supérieur aux e-mails.

Le pretexting se développe en tant que vecteur d'accès initial pour les ransomwares et l'extorsion, comptant désormais pour 6 % des compromissions, alors que le phishing stagne à 16 %. Cette technique s'appuie sur des scénarios soigneusement orchestrés pour instaurer la confiance et amener l'utilisateur à agir, à son insu, au détriment de son entreprise. L'appel vocal est le mode opératoire le plus courant, même si le pretexting par e-mail ou SMS a aussi été observé.

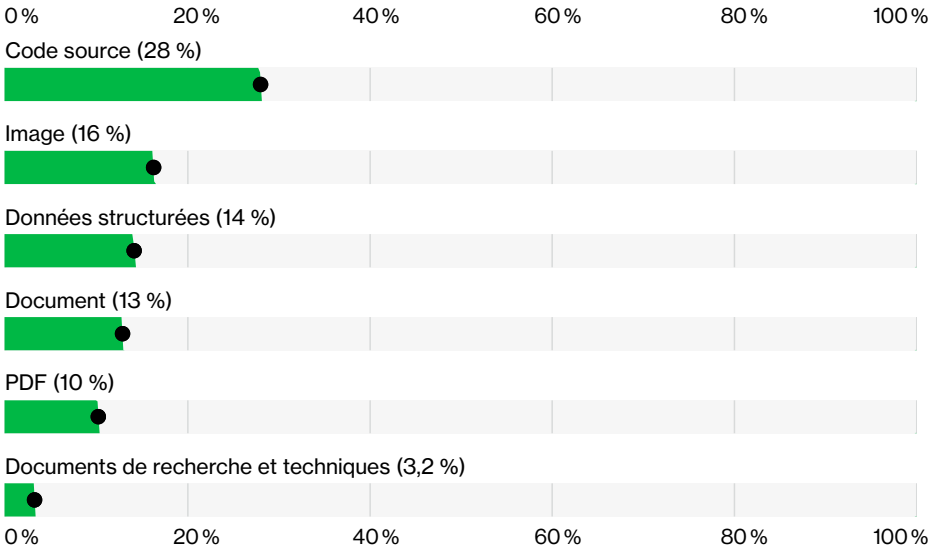


Figure 8. Sélection des types de données impliqués dans les événements DLP non fiables contre les outils d'IA générative (n=858 440)

Infractions aux politiques de Shadow AI et menaces internes

Côté services de GenAI non autorisés (« Shadow AI »), 67 % des utilisateurs y accèdent avec des comptes personnels depuis leurs équipements professionnels, une proportion en légère baisse depuis l'an dernier. Toutefois, 45 % des collaborateurs utilisent désormais régulièrement l'IA (autorisée ou non) sur les appareils d'entreprise, soit 15 % de plus que l'année dernière.

Le Shadow AI constitue la troisième menace interne non malveillante la plus courante observée dans notre jeu de données DLP en 2025, représentant un pourcentage quatre fois supérieur à 2024.

Le code source arrive en tête des données injectées dans des GenAI externes, suivi par les images et d'autres types de données structurées. Dans 3,2 % des infractions aux politiques DLP, des travaux de recherche et documents techniques ont été importés dans des systèmes IA non autorisés, ce qui présente des risques pour la propriété intellectuelle de l'organisation.

Gros plan par secteur

Comme nous l'évoquions en introduction, nous avons analysé plus de 22 000 compromissions de données avérées cette année, un chiffre qui bat tous les records établis par nos précédents rapports. Cette partie vise à disséquer et analyser ces incidents sous un angle sectoriel. Chaque secteur est confronté à des menaces qui lui sont propres, car les surfaces d'attaque varient d'une branche à l'autre.

Avant de vous présenter les résultats, quelques clarifications s'imposent. Les variations sectorielles peuvent s'expliquer par les obligations réglementaires, les exigences de reporting et les différences de contrôle externe qui en découlent, ainsi que par la taille de l'échantillon disponible. Tous ces facteurs influencent les résultats présentés dans le rapport : n'oubliez pas d'en tenir compte lorsque vous comparez deux secteurs.

Nos lecteurs se tournent souvent vers cette section en quête d'analyses « sur mesure », spécifiques à leur propre branche. Vous y trouverez en effet les principaux schémas d'attaque dans votre domaine d'activité. Pour un tableau plus détaillé d'un secteur ou d'un schéma en particulier, nous vous invitons à consulter le rapport complet. Il vous aidera à mieux comprendre et mieux vous défendre face aux menaces qui pèsent sur vos opérations.

Enseignement

(SCIAN 61)

Le secteur de l'enseignement doit principalement faire face à des menaces externes à motivation financière, les modes opératoires les plus courants étant le ransomware, l'exploitation de vulnérabilités et le vol d'identifiants.

Volume	1 302 incidents, dont 1 252 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les erreurs diverses représentent 83 % des compromissions
Acteurs de menace	Externes (78 %), internes (22 %) (compromissions)
Motivations	Financières (78 %), espionnage (21 %), idéologiques (2 %) (compromissions)
Données compromises	Données internes (64 %), personnelles (41 %), autres (26 %), secrets (19 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (34 %), phishing (22 %), détournement d'identifiants (8 %) (compromissions)
Autres indicateurs	Facteur humain (68 %), entité tierce (40 %)
Ce qui n'a pas changé	L'intrusion système, l'ingénierie sociale et les erreurs diverses trustent les trois premières marches du podium, comme les deux dernières années.

Finance et assurance

(SCIAN 52)

Ce secteur continue de subir un pilonnage incessant d'attaquants externes motivés par l'appât du gain, dont les principales méthodes sont les intrusions par ransomware, le phishing, l'exploitation de vulnérabilités et le vol d'identifiants. Notons que l'erreur humaine et les risques tiers contribuent encore largement aux compromissions.

Volume	3 809 incidents, dont 1 300 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et la catégorie « autres » représentent 81 % des compromissions
Acteurs de menace	Externes (88 %), internes (12 %) (compromissions)
Motivations	Financières (98 %), espionnage (3 %) (compromissions)
Données compromises	Données internes (53 %), personnelles (43 %), autres (28 %), identifiants (26 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (22 %), phishing (20 %), détournement d'identifiants (15 %) (compromissions)
Autres indicateurs	Facteur humain (65 %), entité tierce (34 %)
Ce qui n'a pas changé	L'intrusion système demeure le principal schéma d'attaque depuis 2022. Les motivations des attaquants restent essentiellement financières.

Santé

(SCIAN 62)

Les acteurs de la santé sont confrontés à un mélange de vulnérabilités et d'erreurs humaines récurrentes, lesquelles permettent à des attaquants aux motivations financières de s'introduire par exploits, phishing et vols d'identifiants pour déployer des ransomwares. Les erreurs des collaborateurs et les mauvaises configurations demeurent des sources de compromission constantes.

Volume	1 492 incidents, dont 1 438 compromissions de données confirmées
Principaux schémas	L'intrusion système, les erreurs diverses et l'ingénierie sociale représentent 81 % des compromissions
Acteurs de menace	Externes (81 %), internes (19 %) (compromissions)
Motivations	Financières (99 %), espionnage (2 %) (compromissions)
Données compromises	Données internes (65 %), personnelles (37 %), identifiants (25 %), autres (19 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (20 %), phishing (14 %), détournement d'identifiants (11 %) (compromissions)
Autres indicateurs	Facteur humain (54 %), entité tierce (32 %)
Ce qui n'a pas changé	Les erreurs diverses figurent parmi les principaux schémas dans ce secteur depuis que nous avons commencé à l'étudier. L'intrusion système demeure en haut du podium pour la deuxième année consécutive.

Industrie

(SCIAN 31-33)

Dans ce secteur d'activité, le nombre de compromissions continue de croître, principalement sous l'influence des ransomwares.

Volume	3 627 incidents, dont 2 713 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 91 % des compromissions
Acteurs de menace	Externes (95 %), internes (5 %) (compromissions)
Motivations	Financières (87 %), espionnage (15 %) (compromissions)
Données compromises	Données internes (81 %), identifiants (26 %), autres (22 %), personnelles (17 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (38 %), phishing (13 %), détournement d'identifiants (11 %) (compromissions)
Autres indicateurs	Entité tierce (61 %), facteur humain (56 %) (compromissions)
Ce qui n'a pas changé	Les principaux schémas d'attaque dans l'industrie restent les mêmes, la majorité des cybercriminels ayant des visées financières.

Service public

(SCIAN 92)

Qu'ils soient motivés par l'argent ou membres de groupes étatiques, les cybercriminels exploitent les vulnérabilités ou déploient des ransomwares pour s'introduire dans les systèmes des acteurs publics. Outre la récurrence fréquente de ces types d'incidents, le rapport relève un taux anormalement élevé d'incidents internes dus 1) à des erreurs diverses, en particulier des erreurs d'adressage imputables au très grand volume d'e-mails, et 2) à une manipulation volontairement malveillante des données.

Volume	3 634 incidents, dont 2 410 compromissions de données confirmées
Principaux schémas	L'intrusion système, les erreurs diverses et les abus de privilèges représentent 80 % des compromissions.
Acteurs de menace	Externes (56 %), internes (44 %) (compromissions)
Motivations	Financières (69 %), espionnage (33 %), idéologiques (2 %) (compromissions)
Données compromises	Données personnelles (50 %), internes (39 %), autres (37 %), secrets (30 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (40 %), phishing (20 %), détournement d'identifiants (8 %) (compromissions)
Autres indicateurs	Facteur humain (69 %), entité tierce (36 %)
Ce qui n'a pas changé	On retrouve en tête les deux mêmes schémas que l'an dernier, bien que les attaques d'applications web basiques aient cédé la place aux abus de privilèges cette fois-ci. La prévalence des menaces externes reste constante année après année.

Retail

(SCIAN 44-45)

Le retail vie sous la menace constante d'attaquants externes, lesquels exploitent des vulnérabilités, volent des identifiants et lancent des campagnes de phishing pour déployer des ransomwares et exfiltrer des données. En ce sens, les informations d'entreprise et de systèmes tiers constituent des cibles privilégiées.

Volume	997 incidents, dont 806 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 95 % des compromissions
Acteurs de menace	Externes (99 %), internes (1 %) (compromissions)
Motivations	Financières (85 %), espionnage (19 %) (compromissions)
Données compromises	Données internes (84 %), identifiants (26 %), secrets (20 %), autres (14 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (42 %), détournement d'identifiants (14 %), phishing (9 %) (compromissions)
Autres indicateurs	Facteur humain (68 %), entité tierce (58 %) (compromissions)
Ce qui n'a pas changé	Les trois principaux schémas restent identiques. Seul leur taux d'incidence change légèrement. Une tendance que l'on observe à l'échelle globale du secteur depuis de nombreuses années, tous schémas confondus.

PME et ETI

Les ransomwares visent de manière disproportionnée les PME et ETI, confrontées aux mêmes menaces que les autres entreprises, mais avec des ressources moindres pour les contrer.

Volume	7 256 incidents, dont 7 152 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 100 % des compromissions
Acteurs de menace	Externes (100 %) (compromissions)
Motivations	Financières (100 %) (compromissions)
Données compromises	Données internes (97 %), identifiants (31 %), données système (1 %), autres (1 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (26 %), détournement d'identifiants (13 %), phishing (9 %) (compromissions)
Autres indicateurs	Entité tierce (55 %), facteur humain (45 %) (compromissions)
Ce qui n'a pas changé	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale restent les principaux vecteurs de compromission pour les PME et ETI.

Tour d'horizon d'autres secteurs

Faute de place, de temps ou, dans certains cas, de données suffisantes, nous n'avons pu examiner en détail tous les secteurs. Le tableau ci-dessous brosse un schéma d'ensemble de ces autres domaines d'activité.

Secteur d'activités (SCIAN)	Volume	Principaux schémas	Acteurs de menace	Motivations	Données compromises
Agriculture (11)	223 incidents, dont 219 compromissions de données confirmées	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale constituent 91 % des compromissions.	Externes (100 %) (compromissions)	Financières (71 %), espionnage (29 %), idéologiques (1 %) (compromissions)	Données internes (70 %), autres (43 %), secrets (36 %) (compromissions)
Services administratifs (56)	422 incidents, dont 419 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 98 % des compromissions	Externes (99 %), internes (1 %) (compromissions)	Financières (100 %) (compromissions)	Données internes (96 %), identifiants (28 %), autres (2 %), données système (2 %) (compromissions)
BTP (23)	843 incidents, dont 828 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 95 % des compromissions	Externes (99 %), internes (1 %) (compromissions)	Financières (97 %), espionnage (5 %) (compromissions)	Données internes (86 %), identifiants (34 %), autres (13 %), secrets (6 %) (compromissions)
Divertissements (71)	587 incidents, dont 483 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et la catégorie « autres » représentent 82 % des compromissions	Externes (86 %), internes (14 %) (compromissions)	Financières (89 %), espionnage (20 %), idéologiques (1 %) (compromissions)	Données internes (54 %), personnelles (45 %), autres (31 %), secrets (20 %) (compromissions)
Information (51)	1 703 incidents, dont 1 099 compromissions de données confirmées	L'intrusion système, les attaques d'applications web de base et la catégorie « autres » représentent 79 % des compromissions	Externes (89 %), internes (11 %), multiples (1 %) (compromissions)	Financières (84 %), espionnage (16 %), idéologiques (2 %) (compromissions)	Données internes (52 %), personnelles (39 %), autres (31 %), identifiants (24 %) (compromissions)

Tableau 1. Tableau récapitulatif pour les autres secteurs victimes sans section dédiée

Secteur d'activités (SCIAN)	Volume	Principaux schémas	Acteurs de menace	Motivations	Données compromises
Gestion (55)	103 incidents, dont 101 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 98 % des compromissions	Externes (100 %) (compromissions)	Financières (100 %) (compromissions)	Données internes (96 %), identifiants (35 %), méthodes MFA (3 %), autres (2 %) (compromissions)
Exploitation minière (21)	72 incidents, dont 70 compromissions de données confirmées	L'intrusion système, la catégorie « autres » et les attaques d'applications web de base représentent 96 % des compromissions	Externes (100 %) (compromissions)	Financières (97 %), espionnage (1 %), idéologiques (1 %) (compromissions)	Données internes (74 %), identifiants (31 %), personnelles (17 %), autres (9 %) (compromissions)
Autres services (81)	900 incidents, dont 885 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les erreurs diverses représentent 85 % des compromissions	Externes (81 %), internes (19 %) (compromissions)	Financières (78 %), espionnage (23 %) (compromissions)	Données internes (66 %), personnelles (38 %), autres (28 %), secrets (20 %) (compromissions)
Services professionnels (54)	3 578 incidents, dont 2 558 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 91 % des compromissions	Externes (97 %), internes (3 %) (compromissions)	Financières (96 %), espionnage (5 %) (compromissions)	Données internes (80 %), identifiants (31 %), personnelles (14 %), autres (11 %) (compromissions)
Immobilier (53)	505 incidents, dont 499 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les erreurs diverses représentent 85 % des compromissions	Externes (79 %), internes (22 %) (compromissions)	Financières (100 %) (compromissions)	Données internes (63 %), personnelles (43 %), identifiants (24 %), autres (16 %) (compromissions)
Transports (48-49)	689 incidents, dont 652 compromissions de données confirmées	L'intrusion système, les attaques d'applications web de base et la catégorie « autres » représentent 89 % des compromissions	Externes (99 %), internes (1 %) (compromissions)	Financières (89 %), espionnage (15 %), idéologiques (1 %) (compromissions)	Internes (84 %), identifiants (27 %), secrets (16 %), autres (14 %) (compromissions)
Énergie (22)	638 incidents, dont 597 compromissions de données confirmées	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 94 % des compromissions	Externes (97 %), internes (3 %) (compromissions)	Espionnage (71 %), financières (36 %) (compromissions)	Données internes (85 %), secrets (68 %), autres (21 %) (compromissions)
Commerce de gros (42)	1 057 incidents, dont 1 048 compromissions de données confirmées	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 99 % des compromissions	Externes (100 %) (compromissions)	Financières (100 %) (compromissions)	Données internes (98 %), identifiants (29 %) (compromissions)

Tableau 1. Tableau récapitulatif pour les autres secteurs victimes sans section dédiée (suite)

Résultats par région

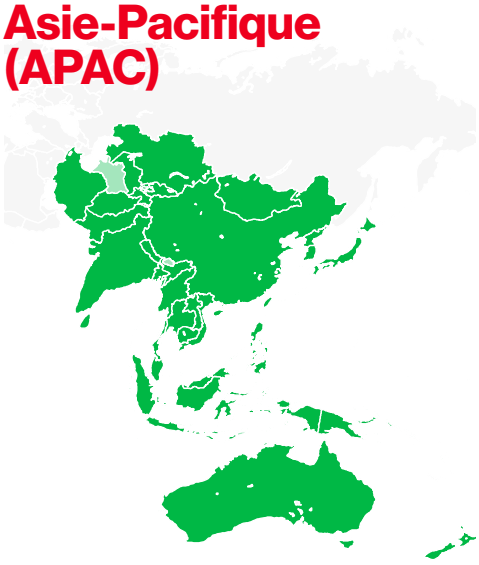
Dans cette partie, nous analysons les compromissions par zone géographique, l'objectif étant d'offrir un aperçu de l'évolution – ou non – des tendances cyber, région par région.

Toutefois, notre visibilité sur une zone donnée dépend de multiples facteurs : la présence de contributeurs, les obligations locales de notification d'incidents, notre propre jeu de données, etc. Si vous souhaitez améliorer la représentation de votre zone géographique dans les pages suivantes, n'hésitez pas à nous contacter pour devenir contributeur et encouragez d'autres entreprises de votre région à en faire de même.

Pays pour lesquels des données existent

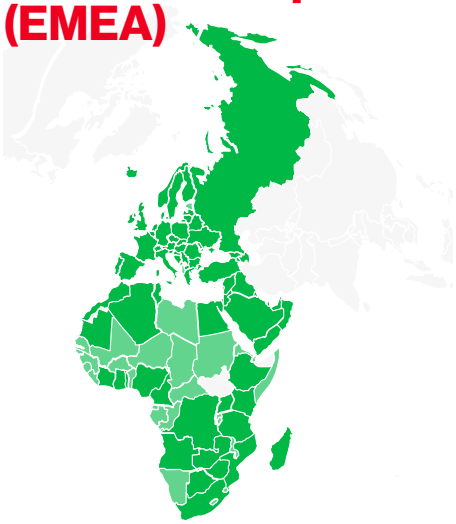
Pays pour lesquels aucune donnée n'existe

Asie-Pacifique (APAC)



Volume	5 229 incidents, dont 2 855 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 97 % des compromissions
Acteurs de menace	Externes (99 %), internes (1 %) (compromissions)
Motivations	Financières (70 %), espionnage (36 %) (compromissions)
Données compromises	Données internes (70 %), identifiants (36 %), autres (35 %), secrets (30 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (42 %), détournement d'identifiants (25 %), phishing (15 %) (compromissions)
Divers	Entité tierce (69 %), facteur humain (71 %) (compromissions)

Europe, Moyen-Orient et Afrique (EMEA)

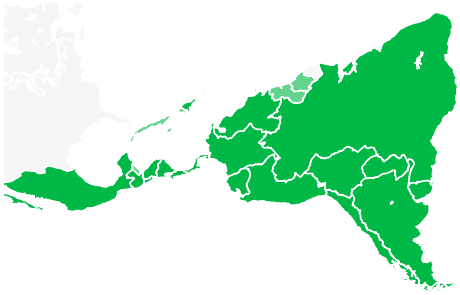


Volume	8 245 incidents, dont 6 060 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les erreurs diverses représentent 92 % des compromissions
Acteurs de menace	Externes (80 %), internes (20 %) (compromissions)
Motivations	Financières (76 %), espionnage (27 %) (compromissions)
Données compromises	Données internes (73 %), autres (49 %), personnelles (34 %), secrets (24 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (47 %), phishing (28 %), détournement d'identifiants (6 %) (compromissions)
Divers	Entité tierce (54 %), facteur humain (70 %) (compromissions)

Pays pour lesquels des données existent

Pays pour lesquels aucune donnée n'existe

Amérique latine et Caraïbes (LAC)



Volume	813 incidents, dont 718 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 98 % des compromissions
Acteurs de menace	Externes (99 %), internes (1 %) (compromissions)
Motivations	Financières (90 %), espionnage (11 %) (compromissions)
Données compromises	Données internes (93 %), identifiants (23 %), secrets (24 %), autres (3 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (44 %), phishing (20 %), détournement d'identifiants (5 %) (compromissions)
Divers	Entité tierce (74 %), facteur humain (57 %) (compromissions)

Amérique du Nord (NA)

Volume	12 371 incidents, dont 8 426 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 87 % des compromissions
Acteurs de menace	Externes (88 %), internes (12 %) (compromissions)
Motivations	Financières (98 %), espionnage (3 %) (compromissions)
Données compromises	Données internes (77 %), identifiants (36 %), personnelles (9 %), autres (8 %) (compromissions)
Vecteurs d'accès initiaux	Exploitation de vulnérabilités (30 %), détournement d'identifiants (20 %), phishing (12 %) (compromissions)
Divers	Entité tierce (43 %), facteur humain (59 %) (compromissions)

S’informer, c’est se préparer.

Pour faire face aux menaces actuelles, vous devez pouvoir compter sur une information fiable.

Le rapport DBIR vous présente les acteurs, tendances et modes opératoires qui pèsent sur votre activité pour vous aider à mieux vous protéger et sensibiliser vos utilisateurs. Bénéficiez de tous les éclairages concrets dont vous avez besoin pour sécuriser votre entreprise.

Lisez le rapport DBIR 2026 complet (en anglais) sur verizon.com/dbir/.

Envie d’œuvrer pour un monde digital plus sûr ?

Votre entreprise recueille des données de sécurité et des informations sur les incidents ? Pour contribuer au rapport annuel DBIR ou devenir partenaire de recherche de Verizon, rien de plus simple : écrivez à dbircontributor@verizon.com. Nous pourrons ainsi discuter des différentes formalités et vous intégrer à la communauté de recherche DBIR.

N’hésitez pas à nous faire part de vos commentaires afin de nous aider à améliorer la prochaine édition. Écrivez-nous à dbir@verizon.com, contactez-nous (Verizon Business ou l’un des auteurs) sur LinkedIn et consultez la page VERIS GitHub : https://github.com/vz-risk/veris.