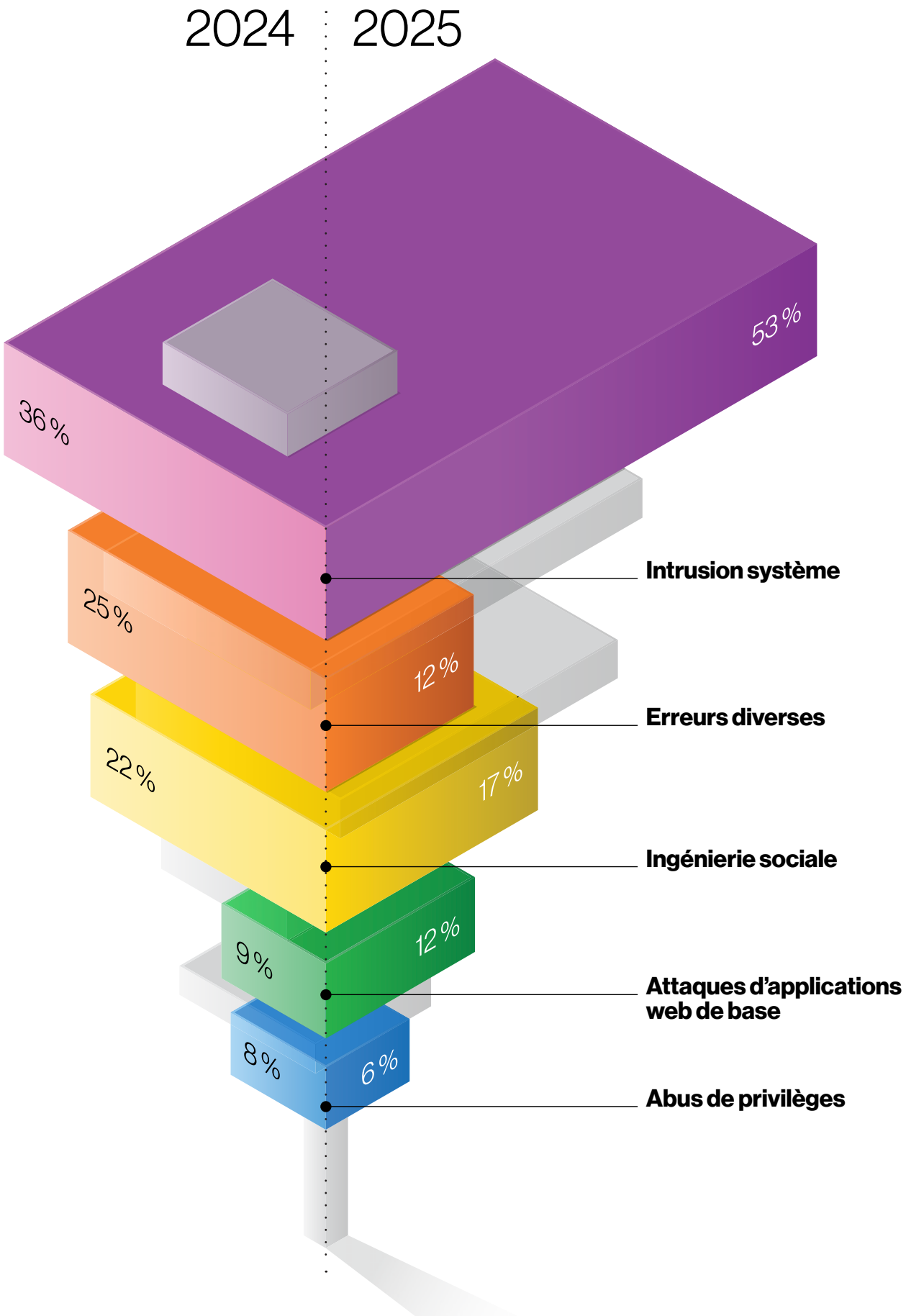
Data Breach Investigations Report – DBIR – 2025

Document de synthèse

verizon business


2024
2025
36 %
53 %
25 %
12 %
22 %
17 %
9 %
12 %
8 %
6 %
Intrusion système
Erreurs diverses
Ingénierie sociale
Attaques d'applications web de base
Abus de privilèges

À propos de l'image en couverture

Les incidents de l'année dernière se distinguent par l'implication constante de tiers dans les compromissions. Le rôle de ces acteurs externes varie. Ils peuvent être dépositaires de données clients, tout comme ils peuvent constituer l'un des piliers opérationnels de l'entreprise.

Nos graphistes avaient pour défi de représenter cette dépendance croissante aux tiers et l'exercice d'équilibriste qu'elle représente pour les équipes de sécurité. Pari tenu ! Si vous vous demandez comment un tel assemblage peut tenir debout, vous commencerez alors à mieux comprendre le véritable casse-tête que doivent résoudre les responsables de la sécurité des systèmes d'information (RSSI) au quotidien.

Autour de l'axe central s'articulent les vecteurs de compromission les plus répandus dans nos données de recherche. À titre comparatif, les données 2024 sont orientées vers la gauche, et celles de 2025 vers la droite. Le schéma en deuxième de couverture ajoute de la couleur et des chiffres pour plus de clarté.

Que cet échafaudage précaire continue de tenir debout est en soi un miracle qui doit tout à la persévérance et à la collaboration des équipes de cybersécurité. Un savant mélange de coopération, d'organisation et de partage d'information devrait nous permettre de renforcer encore la sécurité et, qui sait, de retrouver un sommeil réparateur.

Sommaire

Introduction

Bienvenue dans le DBIR 2025 de Verizon.

Cette année marque la 18e édition de notre rapport annuel consacré aux compromissions des données. Que vous soyez nouveau lecteur ou fidèle de la première heure, vous trouverez dans cette étude un état des lieux étayé de la cybercriminalité, assorti de précieux éclairages sur les menaces spécifiques à votre entreprise, le profil des attaquants et les mesures de protection à adopter.

Cette année, l'équipe DBIR de Verizon a passé au crible 22 052 incidents de sécurité, dont un record de 12 195 compromissions de données avérées ! Les entreprises victimes sont de toutes tailles et de tous horizons. Les données étudiées proviennent des missions d'intervention de l'équipe VTRAC (Verizon Threat Research Advisory Center), de nos contributeurs dévoués du monde entier et d'incidents déclarés dont les détails sont disponibles dans le domaine public. Au total, quelque 139 pays sont concernés par ces attaques.

Même si la physionomie des menaces tend à différer selon certaines variables (taille de l'entreprise, secteur, région, etc.), quelques thématiques phares semblent néanmoins toujours prédominer. Et le cru 2025 ne fait pas exception. La plus notoire d'entre elles, sans aucun doute, concerne le rôle des tiers, à la fois dans l'origine et le déroulé des compromissions.

Certes, les éditeurs de logiciels jouent depuis longtemps, et bien malgré eux, un rôle avéré dans l'expansion de la surface d'attaque. Toutefois, au cours des deux ou trois dernières années, des cas jusque-là dispersés (et d'importance mineure à modérée) se sont généralisés en un problème plus insidieux aux effets potentiellement, voire effectivement, dévastateurs pour les entreprises. L'ampleur de ce phénomène est telle qu'il illustre la couverture de l'édition 2025 et réapparaît en fil rouge tout au long de cette synthèse.

Dans les pages qui suivent, vous découvrirez les principales conclusions du rapport DBIR, en particulier les dernières données sur les compromissions par secteur et par région. N'hésitez pas à envoyer cette synthèse à vos collègues et à télécharger le rapport complet (en anglais) pour une vue plus détaillée des menaces qui pèsent sur votre activité.

Points clés/Synthèse des résultats

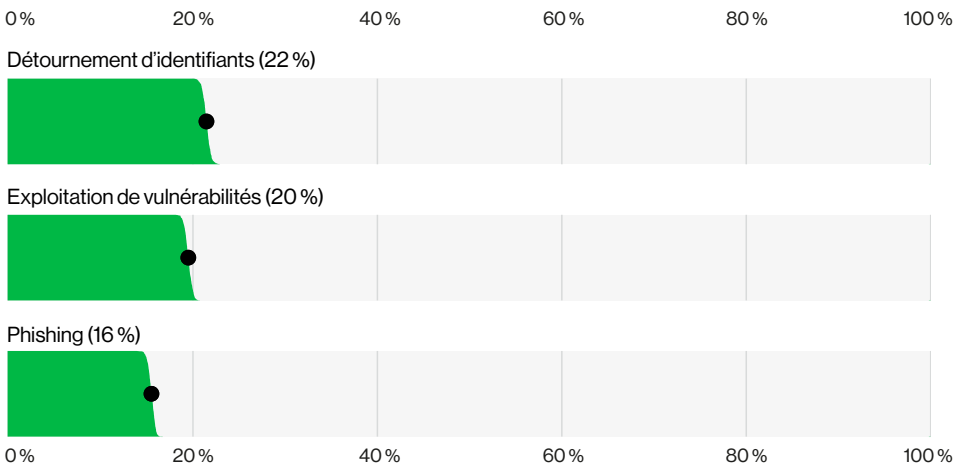


Figure 1. Part des trois grands vecteurs d'accès initial dans les compromissions hors erreurs et abus de privilèges (n=9,891)

L'exploitation des vulnérabilités comme vecteur initial d'accès poursuit son irrésistible ascension pour représenter 20 % des compromissions, talonnant au passage le détournement d'identifiants, qui demeure en tête à 22 %. Cette progression du rôle des vulnérabilités marque une augmentation de 34 % par rapport à l'édition 2024, sous-tendue en partie par les exploits zero-day ciblant les équipements en périphérie (edge) et les réseaux privés virtuels (VPN). Le pourcentage d'équipements edge et de VPN visés par l'exploitation de vulnérabilités a été multiplié quasiment par 8 en un an, passant de 3 % à 22 %. Malgré les efforts des entreprises pour patcher leur parc en périphérie, seulement 54 % des vulnérabilités ont fait l'objet d'une remédiation complète au cours de l'année écoulée, dans un délai médian de 32 jours.

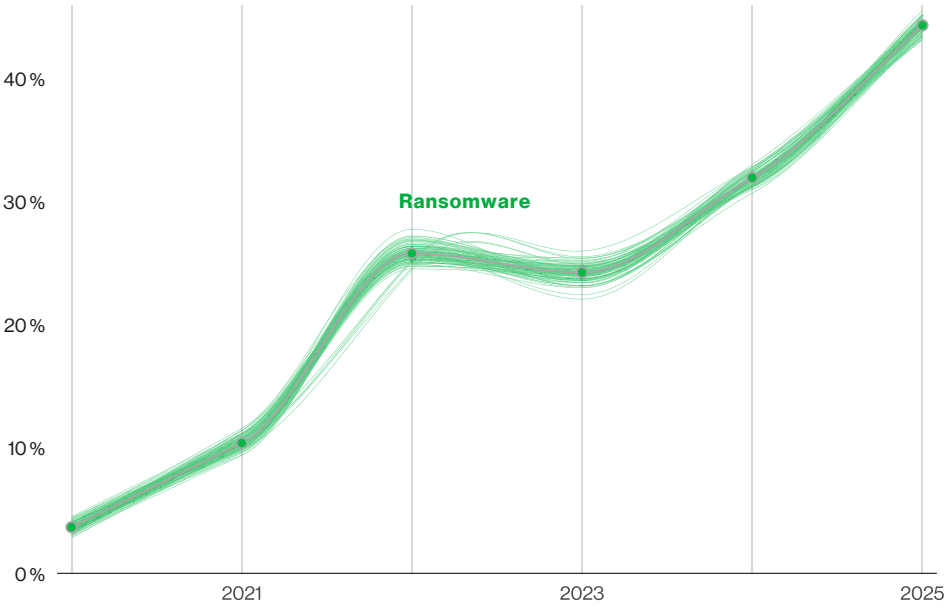


Figure 2. Évolution chronologique de la part des ransomwares dans les compromissions (n=10 747 dans le corpus de données analysées 2025)

Quant aux ransomwares (avec ou sans chiffrement), ils gagnent du terrain dans notre dataset, avec une augmentation de 37 % par rapport à l'édition 2024. De même, ils étaient présents dans 44 % de toutes les compromissions de données recensées, soit une hausse de 32 %. La bonne nouvelle toutefois, c'est le recul du montant moyen de la rançon versée aux gangs de ransomware, qui s'élève désormais à 115 000 $ (contre 150 000 $ l'année dernière). D'après nos chiffres, 64 % des entreprises victimes ont refusé de payer la rançon, soit deux fois plus qu'en 2023. Ce refus expliquerait en partie la baisse des sommes versées.

Autre constat, les ransomwares visent de manière disproportionnée les PME et ETI. La preuve, ils comptent pour 88 % des compromissions dans ces dernières, contre 39 % dans les entreprises de plus grande taille.

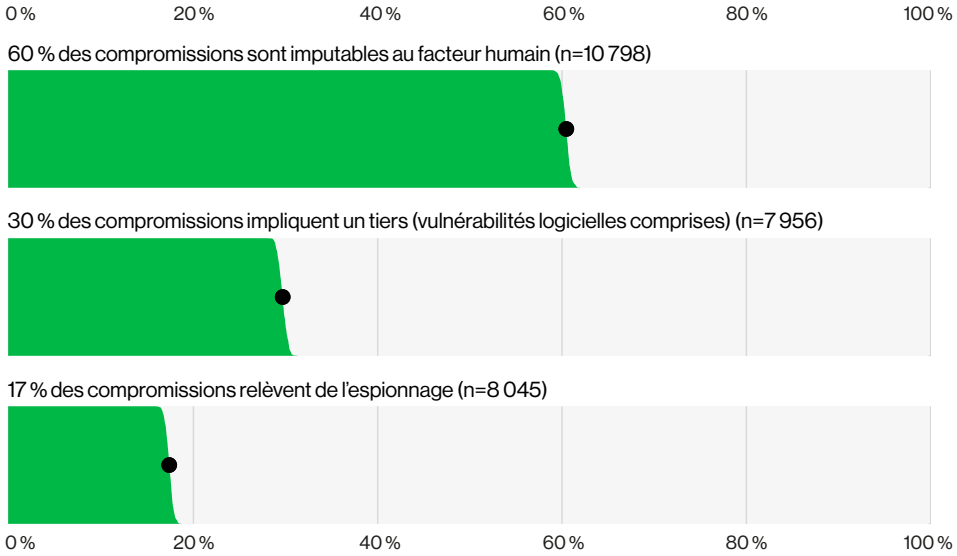


Figure 3. Part des principaux vecteurs de compromission

Si l'implication du facteur humain dans les compromissions reste plus ou moins le même que l'an dernier, aux alentours des 60 %, le pourcentage de compromissions imputables à un tiers a doublé, passant de 15 à 30 %.

Symbole de cette progression, cette année a été marquée par plusieurs cas d'incidents liés à la réutilisation d'identifiants dans l'environnement d'un tiers. Par ailleurs, notre étude estime à 94 jours le délai moyen pour remédier à la fuite de secrets dans un dépôt de code GitHub.

L'espionnage a également augmenté, représentant à lui seul 17 % des incidents analysés. Cet accroissement s'explique en partie par un changement dans notre cohorte de contributeurs. Dans 70 % des cas, ces compromissions s'appuient sur l'exploitation des vulnérabilités comme vecteur d'accès initial, démontrant une fois de plus le risque d'opérer des services en retard de correctifs. Toutefois, il ressort de notre étude que l'espionnage n'est pas la seule motivation des groupes étatiques. L'appât du gain représente 28 % des incidents les impliquant. Selon certains médias, ce double jeu leur permettrait de se constituer un pécule en prenant leur part du magot.

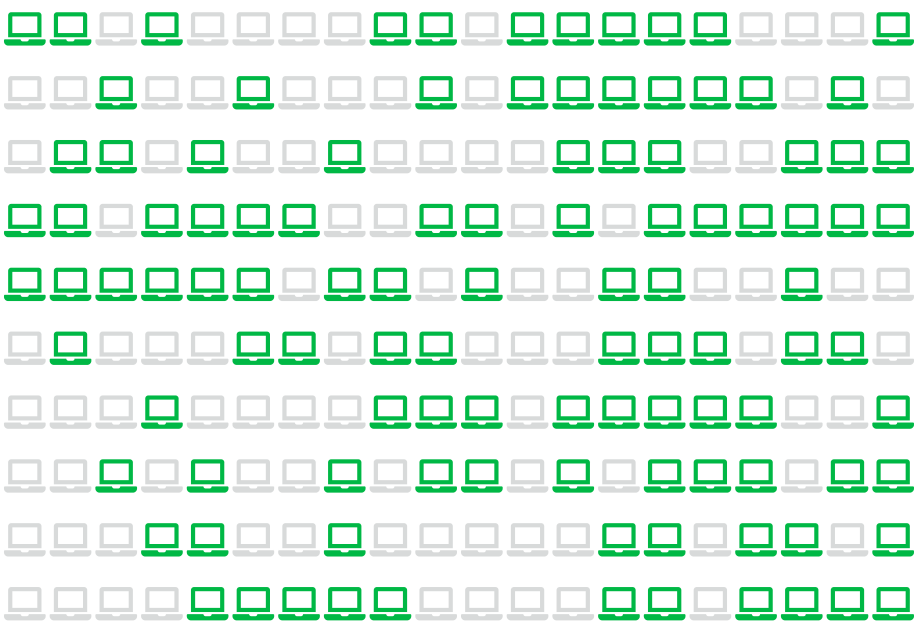


Figure 4. Pourcentage d'appareils non gérés dotés d'identifiants d'entreprise retrouvés dans les journaux d'infostealers (chaque glyphe représente 0,5 %)

Côté vol d'identifiants, l'analyse des journaux d'identifiants de malwares voleurs d'informations (ou infostealers) a révélé que 30 % des systèmes compromis étaient des équipements d'entreprise. Le problème, c'est que 46 % de ceux comptant des identifiants d'entreprise parmi les données compromises étaient non gérés et renfermaient une myriade d'identifiants, aussi bien personnels que professionnels. Il s'agissait probablement d'appareils relevant d'un programme BYOD (Bring Your Own Device) ou d'équipements appartenant à l'entreprise et enfreignant les politiques d'usage autorisé.

En corrélant les journaux d'infostealers avec les annonces de marketplaces du Dark Web où les acteurs du ransomware avaient publié les domaines Internet des victimes, nous avons fait deux constats. Primo, les domaines de 54 % de ces victimes ont été révélés lors de ce dumping d'identifiants (ex. : des URL auxquels les identifiants volés étaient supposés donner accès). Secundo, 40 % des victimes de compromissions d'identifiants comptaient des adresses e-mail professionnelles parmi les identifiants compromis. Cela laisse à penser que ces identifiants auraient pu être exploités dans le cadre de compromissions par ransomware, pointant ainsi l'implication potentielle d'un broker comme source de vecteurs d'accès initial.

Figure 5. Répartition en pourcentage des types de comptes d'accès au service GenAI (chaque glyphe représente 0,5 %)

Début 2025, l'intelligence artificielle générative (GenAI) n'avait toujours pas provoqué le déferlement d'attaques annoncé, même si son utilisation par des acteurs cyber est confirmée par les plateformes d'IA elles-mêmes. Par ailleurs, d'après les données fournies par l'un de nos partenaires, le volume de texte généré synthétiquement dans les e-mails malveillants a doublé au cours des deux dernières années.

Cependant, le nouveau risque de fuite de données sensibles d'entreprise sur les plateformes de GenAI semble beaucoup plus réel, au vu des 15 % de collaborateurs qui accèdent régulièrement à des systèmes GenAI depuis leurs équipements professionnels (au moins une fois tous les 15 jours). Plus inquiétant encore, nombre de ces collaborateurs recourent à une adresse e-mail non professionnelle pour se connecter à leur compte (72 %), voire utilisent leur adresse professionnelle sans système d'authentification intégré (17 %), très probablement contraire à la politique d'entreprise.

Gros plan par secteur

Comme nous l'évoquions en introduction, Verizon a analysé 22 052 incidents cette année, parmi lesquels 12 195 compromissions avérées. Cette partie vise à disséquer et analyser ces incidents et compromissions sous un angle sectoriel, car la nature de la menace varie grandement d'un domaine d'activité à l'autre. C'est évident. Et le plus souvent, ces différences dépendent de la surface d'attaque de l'entreprise.

Ainsi, une grande banque internationale sera confrontée à des menaces tout autres que celles qui planent sur une entreprise régionale de logistique. Néanmoins, il arrive que certains recoupements se produisent contre toute attente. En d'autres termes, il semblerait que les acteurs cyber actuels se préoccupent moins de la taille de l'entreprise, de son secteur d'activité ou de sa zone géographique qu'on pourrait le penser. C'est leur côté pragmatique et opportuniste : l'occasion fait le larron. Par ailleurs, d'autres variables entrent en jeu dans cette partie, comme les différences d'obligations de déclaration d'incidents entre les secteurs, les contrôles draconiens dont certains font l'objet, la taille de l'échantillon dont nous disposons pour un secteur en particulier, et bien d'autres encore. Il est donc important de bien garder ces facteurs à l'esprit avant de juger de la posture de sécurité d'un domaine d'activité en particulier. Dernier point, nous rappelons que notre classification sectorielle repose sur les codes du Système de classification des industries de l'Amérique du Nord (SCIAN).

Enseignement (SCIAN 61)

Volume	1 075 incidents, dont 851 compromissions de données confirmées
Principaux schémas	L'intrusion système, les erreurs diverses et l'ingénierie sociale représentent 80 % des compromissions.
Attaquants	Externes (62 %), internes (38 %) (compromissions)
Motivations	Financières (88 %), espionnage (18 %) (compromissions)
Données compromises	Données personnelles (58 %), internes (49 %), autres (35 %), identifiants (12 %) (compromissions)
Ce qui n'a pas changé	L'intrusion système, les erreurs diverses et l'ingénierie sociale trustent les trois premières marches du podium, comme les deux dernières années précédentes.
En bref	Même si l'on constate une baisse du nombre d'incidents et de compromissions dans le secteur de l'enseignement, les attaques examinées demeurent semblables à celles observées par le passé. L'intrusion système s'impose comme le principal schéma d'attaque, impulsé largement par des acteurs externes à visées financières.

Finance et assurance

(SCIAN 52)

Volume	3 336 incidents, dont 927 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base comptent pour 74 % des compromissions.
Attaquants	Externes (78 %), internes (22 %), partenaires (1 %) (compromissions)
Motivations	Financières (90 %), espionnage (12 %) (compromissions)
Données compromises	Données personnelles (54 %), autres (44 %), données internes (35 %), identifiants (22 %) (compromissions)
Ce qui n'a pas changé	L'intrusion système demeure cette année le principal schéma d'attaque, en raison de la prépondérance d'attaques plus complexes. Serait-ce un signe que ces dernières demandent plus d'efforts aux attaquants ? Nous n'osons l'espérer.
En bref	Si le secteur de la finance et de l'assurance reste dominé par des acteurs malveillants à l'affût de tout type de données monétisables, l'espionnage enregistre une augmentation par rapport à l'année dernière.

Santé

(SCIAN 62)

Volume	1 710 incidents, dont 1 542 compromissions de données confirmées
Principaux schémas	L'intrusion système, la catégorie « autres » et les erreurs diverses constituent 74 % des compromissions.
Attaquants	Externes (67 %), internes (30 %), partenaires (4 %), multiples (1 %) (compromissions)
Motivations	Financières (90 %), espionnage (16 %) (compromissions)
Données compromises	Données médicales (45 %), données personnelles (40 %), données internes (32 %), autres (24 %) (compromissions)
Ce qui n'a pas changé	Les schémas d'attaques restent identiques, même si leurs positions respectives ont changé.
En bref	Le secteur de la santé demeure une cible de choix pour les cyberattaquants, comme le prouve la légère augmentation du nombre d'incidents et de compromissions observée cette année. L'intrusion système (y compris les ransomwares) se hisse en tête du classement des principales causes de compromission, doublant au passage les erreurs diverses. Fait inquiétant, la montée de l'espionnage au rang des motivations des attaquants.

Industrie

(SCIAN 31-33)

Volume	3 837 incidents, dont 1 607 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 85 % des compromissions.
Attaquants	Externes (86 %), internes (14 %) (compromissions)
Motivations	Financières (87 %), espionnage (20 %) (compromissions)
Données compromises	Données internes (64 %), autres (37 %), données personnelles (33 %), identifiants (22 %) (compromissions)
Ce qui n'a pas changé	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base occupent toujours les trois premières places du podium, dominées très largement par des acteurs externes motivés par l'appât du gain.
En bref	Cette année, 20 % des compromissions relevaient de cas d'espionnage, contre seulement 3 % l'année dernière. Les données internes (plans, rapports, e-mails sensibles) s'imposent comme le principal type d'informations dérobées. Autre fait notoire, plus de 90 % des entreprises victimes de compromissions étaient des PME et ETI de moins de 1 000 salariés.

Retail

(SCIAN 44-45)

Volume	837 incidents, dont 419 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base comptent pour 93 % des compromissions.
Attaquants	Externes (96 %), internes (3 %), partenaires (1 %) (compromissions)
Motivations	Financières (100 %), espionnage (9 %) (compromissions)
Données compromises	Données internes (65 %), autres (30 %), identifiants (26 %), données de paiement (12 %) (compromissions)
Ce qui n'a pas changé	Aucun changement à noter, tant au niveau des 3 principaux schémas d'attaques que de leur position au classement ou du profil des attaquants.
En bref	Le nombre de cyberincidents dans le retail est en hausse. Les attaquants jettent de plus en plus leur dévolu sur d'autres types de données que celles de paiement, plus faciles d'accès. Les cas d'espionnage ont nettement augmenté par rapport à l'année dernière. Un avertissement pour les équipes de sécurité qui devraient être conscientes du risque de menaces plus sophistiquées et plus difficiles à déceler.

Secteur public

(SCIAN 92)

Volume	1 422 incidents, dont 946 compromissions de données confirmées
Principaux schémas	L'intrusion système, les erreurs diverses et les attaques d'applications web de base représentent 78 % des compromissions.
Attaquants	Externes (67 %), internes (33 %), partenaires (1 %) (compromissions)
Motivations	Financières (76 %), espionnage (29 %), idéologiques (2 %) (compromissions)
Données compromises	Données personnelles (47 %), internes (44 %), autres (41 %), secrets (17 %) (compromissions)
Ce qui n'a pas changé	Les acteurs publics continuent de subir les assauts sophistiqués d'attaquants cherchant à mettre la main sur la mine de données personnelles dont les administrations sont dépositaires. Bien que la majorité des attaques soient le fait d'acteurs externes, un nombre non négligeable d'entre elles sont dues à de simples erreurs en interne.
En bref	Si le nombre d'incidents signalés a chuté, en raison d'un changement dans la composition de nos contributeurs, le volume de compromissions confirmées reste néanmoins stable. Les attaques contre les pouvoirs publics ne faiblissent donc pas. En tête des principales menaces, le ransomware est à l'origine de 30 % des compromissions, et ce dans toutes les strates des administrations et collectivités. Les erreurs demeurent un problème de taille, en particulier les erreurs d'adressage.

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 1 brosse un schéma d'ensemble de ces autres domaines d'activité.

Secteur d'activités (SCIAN)	Volume	Principaux schémas	Attaquants	Motivations	Données compromises
Agriculture (11)	80 incidents, dont 55 compromissions de données confirmées	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale constituent 96 % des compromissions	Externes (96 %), internes (4 %) (compromissions)	Financières (98 %), espionnage (33 %), idéologiques (2 %) (compromissions)	Données internes (67 %), autres (39 %), secrets (35 %) (compromissions)
Services administratifs (56)	153 incidents, dont 145 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les erreurs diverses comptent pour 97 % des compromissions	Externes (95 %), internes (3 %), partenaires (2 %) (compromissions)	Financières (100 %) (compromissions)	Données internes (83 %), identifiants (31 %), données personnelles (10 %), autres (8 %) (compromissions)
BTP (23)	307 incidents, dont 252 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 96 % des compromissions	Externes (97 %), internes (3 %) (compromissions)	Financières (77 %), espionnage (23 %) (compromissions)	Données internes (77 %), identifiants (31 %), autres (23 %), secrets (21 %) (compromissions)
Divertissements (71)	493 incidents, dont 293 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les erreurs diverses constituent 76 % des compromissions	Externes (71 %), internes (29 %) (compromissions)	Financières (97 %), espionnage (18 %), idéologiques (3 %), piratage récréatif (1 %) (compromissions)	Données personnelles (58 %), autres (39 %), données internes (32 %), identifiants (18 %) (compromissions)
Information (51)	1 589 incidents, dont 784 compromissions de données confirmées	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale comptent pour 82 % des compromissions	Externes (83 %), internes (17 %), partenaires (1 %) (compromissions)	Financières (78 %), espionnage (36 %), idéologiques (1 %) (compromissions)	Autres (62 %), données internes (51 %), données personnelles (37 %), secrets (27 %) (compromissions)

Tableau 1. Tableau récapitulatif d'autres secteurs victimes sans section dédiée

Secteur d'activités (SCIAN)	Volume	Principaux schémas	Attaquants	Motivations	Données compromises
Gestion (55)	113 incidents, dont 107 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les abus de privilèges représentent 99 % des compromissions	Externes (97 %), partenaires (2 %), internes (1 %) (compromissions)	Financières (99 %), espionnage (1 %) (compromissions)	Données internes (95 %), identifiants (33 %), données médicales (1 %), données personnelles (1 %), données système (1 %) (compromissions)
Exploitation minière (21)	64 incidents, dont 52 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base constituent 96 % des compromissions	Externes (98 %), internes (6 %), multiples (4 %) (compromissions)	Financières (100 %), espionnage (3 %), représailles (3 %) (compromissions)	Données internes (59 %), identifiants (43 %), données système (20 %), autres (18 %) (compromissions)
Autres services (81)	683 incidents, dont 583 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les erreurs diverses comptent pour 79 % des compromissions	Externes (68 %), internes (33 %) (compromissions)	Financières (69 %), espionnage (31 %) (compromissions)	Données personnelles (57 %), internes (48 %), autres (44 %), secrets (18 %) (compromissions)
Services professionnels (54)	2 549 incidents, dont 1 147 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 91 % des compromissions	Externes (93 %), internes (7 %), partenaires (1 %) (compromissions)	Financières (88 %), espionnage (17 %) (compromissions)	Données internes (70 %), autres (25 %), identifiants (24 %), données personnelles (24 %) (compromissions)
Immobilier (53)	339 incidents, dont 320 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les erreurs diverses représentent 84 % des compromissions	Externes (64 %), internes (36 %) (compromissions)	Financières (100 %) (compromissions)	Données personnelles (70 %), internes (40 %), autres (27 %), données bancaires (17 %) (compromissions)
Transports (48-49)	361 incidents, dont 248 compromissions de données confirmées	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale constituent 91 % des compromissions	Externes (94 %), internes (7 %), multiples (2 %), partenaires (1 %) (compromissions)	Financières (98 %), espionnage (16 %), idéologiques (1 %) (compromissions)	Données internes (67 %), autres (25 %), identifiants (22 %), données personnelles (20 %) (compromissions)
Énergie (22)	358 incidents, dont 213 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base comptent pour 92 % des compromissions	Externes (92 %), internes (8 %), multiples (1 %) (compromissions)	Financières (70 %), espionnage (66 %), représailles (1 %) (compromissions)	Données internes (80 %), secrets (61 %), autres (42 %) (compromissions)
Commerce de gros (42)	330 incidents, dont 319 compromissions de données confirmées	L'intrusion système, l'ingénierie sociale et les abus de privilèges représentent 98 % des compromissions	Externes (97 %), internes (3 %) (compromissions)	Financières (100 %) (compromissions)	Données internes (93 %), identifiants (24 %), autres (3 %), données personnelles (3 %), données système (3 %) (compromissions)

Tableau 1. Tableau récapitulatif d'autres secteurs victimes sans section dédiée

Résultats par région

On nous demande souvent si la nature du cybercrime varie ou non d'une région à l'autre. Pour y apporter des éléments de réponse, le DBIR propose cette année encore une analyse des incidents et compromissions par zone géographique. Toutefois, notre visibilité sur une région donnée dépend de multiples facteurs : la présence de contributeurs, les obligations locales de notification d'incidents, notre propre jeu de données, etc. Nous espérons que nos lecteurs trouveront dans cette perspective globale des éclairages utiles et instructifs.

Si vous souhaitez fournir des données pour votre zone géographique, n'hésitez pas à nous contacter pour devenir contributeur et encouragez vos clients et partenaires à en faire de même.

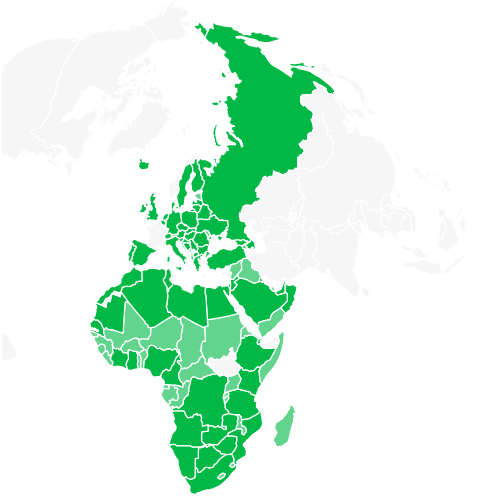
Pays pour lesquels des données existent

Pays pour lesquels aucune donnée n'existe

Asie-Pacifique (APAC)

Volume	2 687 incidents, dont 1 374 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base constituent 97 % des compromissions.
Attaquants	Externes (99 %), internes (1 %) (compromissions)
Motivations	Financières (83 %), espionnage (34 %) (compromissions)
Données compromises	Données internes (78 %), autres (41 %), secrets (33 %) (compromissions)

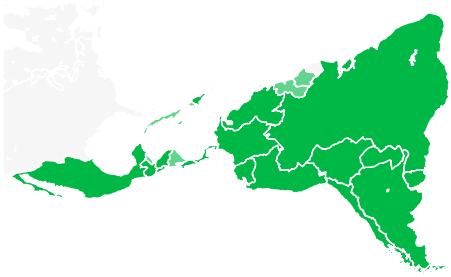
Europe, Moyen-Orient et Afrique (EMEA)



Volume	9 062 incidents, dont 5 321 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les erreurs diverses représentent 89 % des compromissions.
Attaquants	Externes (71 %), internes (29 %) (compromissions)
Motivations	Financières (87 %), espionnage (18 %) (compromissions)
Données compromises	Données internes (62 %), données personnelles (49 %), autres (37 %), secrets (13 %) (compromissions)

Pays pour lesquels des données existent Pays pour lesquels aucune donnée n'existe

Amérique latine et Caraïbes (LAC)



Volume	657 incidents, dont 413 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 99 % des compromissions.
Attaquants	Externes (100 %), partenaires (1 %), multiples (2 %) (compromissions)
Motivations	Financières (84 %), espionnage (27 %) (compromissions)
Données compromises	Données internes (97 %), secrets (27 %), autres (24 %) (compromissions)

Amérique du Nord (NA)

Volume	6 361 incidents, dont 2 867 compromissions de données confirmées
Principaux schémas	L'intrusion système, la catégorie « autres » et l'ingénierie sociale comptent pour 90 % des compromissions.
Attaquants	Externes (91 %), internes (5 %), partenaires (5 %), multiples (1 %) (compromissions)
Motivations	Financières (95 %), espionnage (9 %) (compromissions)
Données compromises	Données internes (49 %), médicales (35 %), identifiants (23 %), autres (17 %) (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 2025 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 de Verizon, rien de plus simple : écrivez à dbircontributor@verizon.com.

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/veriss.