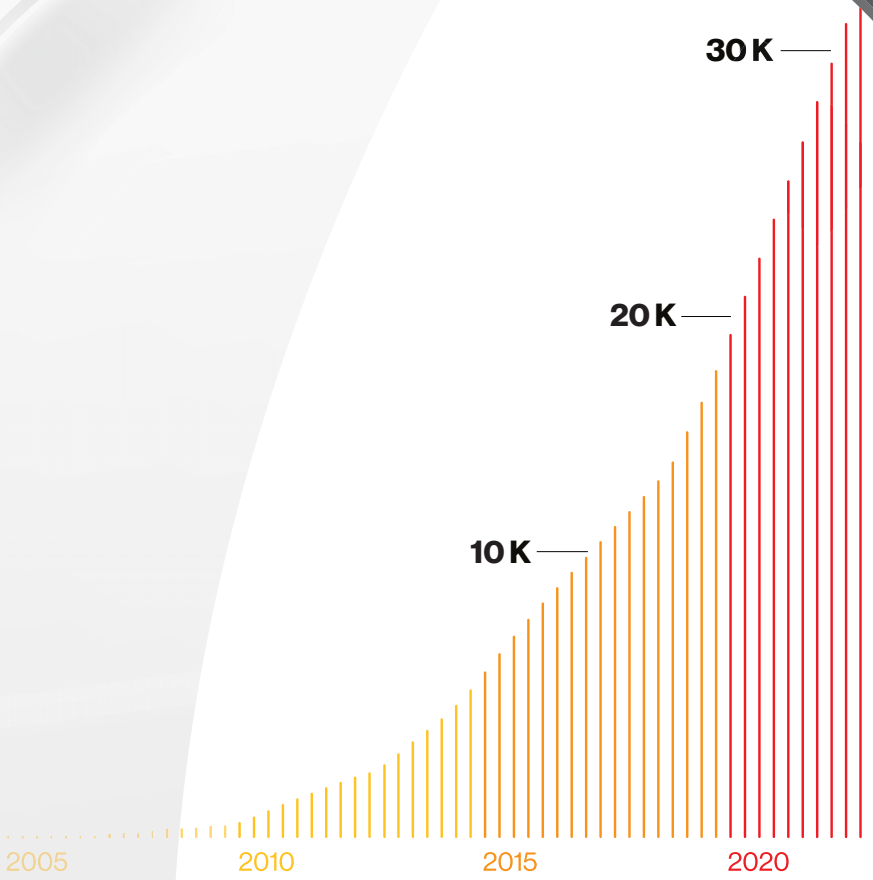
DBIR

Data Breach Investigations Report 2023

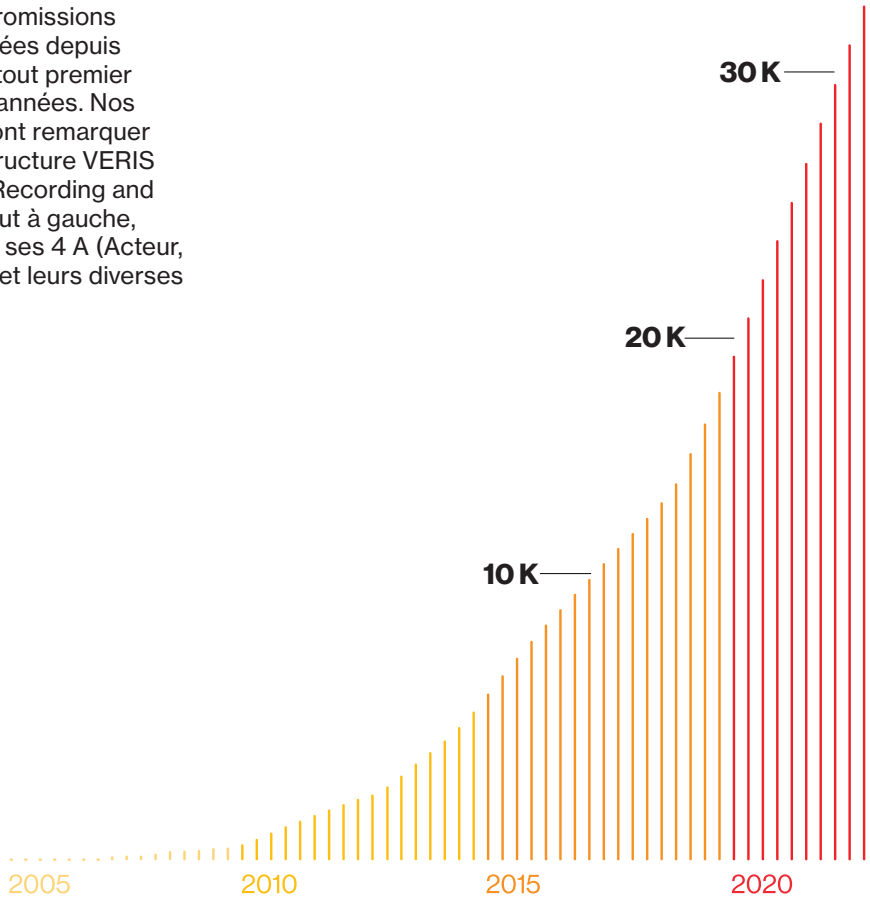
Document de synthèse



verizon

À propos de la représentation en couverture

La loupe située au centre de la couverture rappelle les efforts déployés par l'équipe pour recentrer ses ressources et son énergie sur son principal jeu de données de compromissions. Le graphique agrandi par la loupe représente le total cumulé des compromissions que nous avons recensées depuis la publication de notre tout premier rapport il y a quelques années. Nos lecteurs assidus pourront remarquer le motif alvéolé de la structure VERIS (Vocabulary for Event Recording and Incident Sharing) en haut à gauche, ajouté ici pour rappeler ses 4 A (Acteur, Action, Asset, Attribut) et leurs diverses énumérations.



Sommaire

Introduction 4

À retenir 6

Gros plan par secteur 8

Hôtellerie et restauration 8

Enseignement 9

Finance et assurance 9

Santé 10

Information 10

Industrie 11

Exploitation minière, extraction de pétrole et de gaz, compagnies d'énergie 11

Services professionnels, scientifiques et techniques 12

Service public 12

Retail 13

Petites et moyennes entreprises 14

Résultats par région 15

S'informer, c'est se préparer 17

Introduction

Bienvenue dans la 16e édition annuelle du Data Breach Investigations Report (DBIR) de Verizon.

L'objectif de ce rapport est de fournir aux professionnels de la sécurité un bilan détaillé des actes cybercriminels perpétrés durant l'année écoulée. Fruit d'une analyse pointue de données réelles, cette étude dresse également un tableau par secteur, taille d'entreprise et zone géographique. Nous espérons qu'elle vous apportera des éclairages sur les menaces qui pèsent sur votre entreprise et vous aidera à vous y préparer de la meilleure des manières.

Comme lors des éditions précédentes, nous décortiquerons nos données sur les cyberattaquants et sur leurs outils de prédilection. Cette année, notre étude porte sur 16 312 incidents de sécurité, dont 5 199 compromissions avérées. Ces données proviennent de compromissions et d'incidents sur lesquels a enquêté le Verizon Threat Research Advisory Center (VTRAC) – qui célèbre ses 20 ans cette année – mais aussi de l'un de nos généreux contributeurs sans qui ce rapport n'aurait jamais pu exister. Nous espérons que le DBIR vous éclairera sur les tactiques les plus utilisées contre les entreprises en général et votre secteur en particulier, mais aussi sur les moyens de protection à votre disposition. Dans les pages qui suivent, vous découvrirez les principales conclusions du DBIR 2023. 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 vous concernent.

Évolution chronologique des incidents et des compromissions

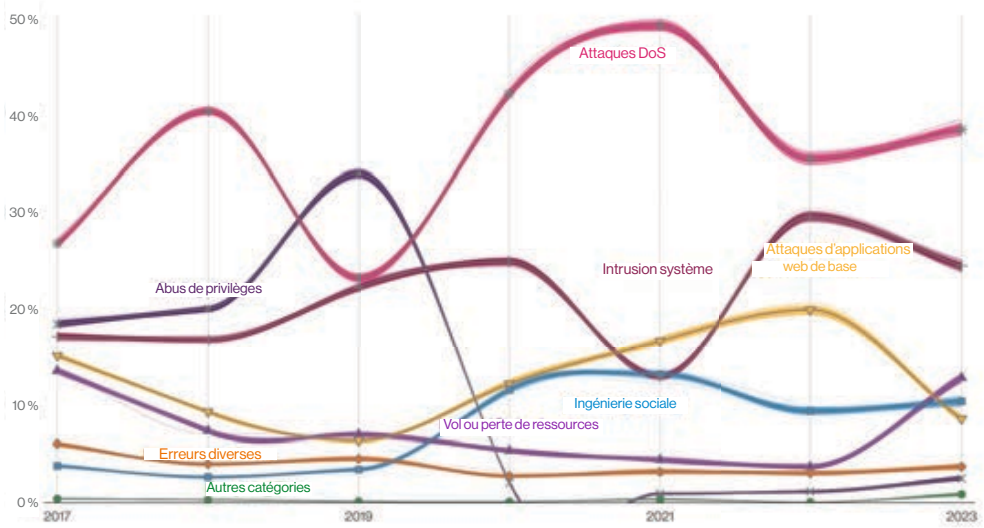


Figure 1. Évolution chronologique des incidents

Pour observer l'évolution des incidents au fil des ans, nous les avons classés en différentes catégories. Dans la Figure 1, le déni de service constitue clairement le premier type d'incident, comme c'est le cas depuis plusieurs années déjà.

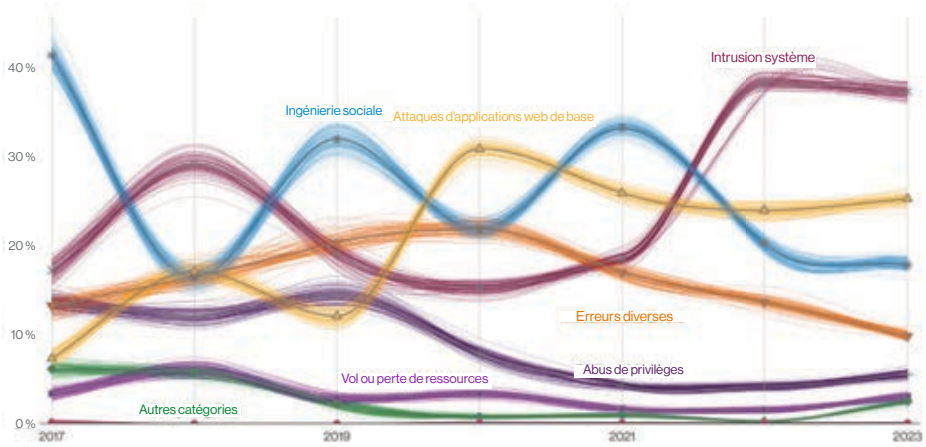
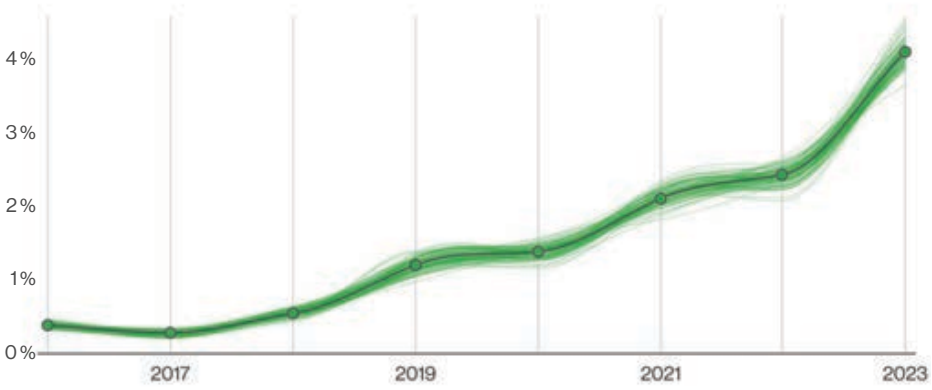


Figure 2. Évolution chronologique des compromissions

La Figure 2 montre à quel point le constat diffère lorsque le curseur est placé sur les incidents avec perte de données avérée.

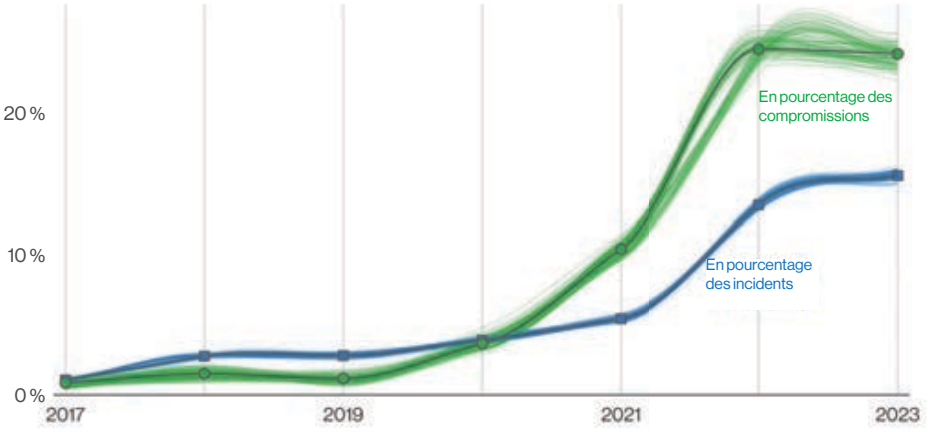
Plus complexe, l'intrusion système gagne du terrain et est souvent l'aboutissement d'attaques multi-étapes, y compris au moyen de ransomwares. Mais avant d'aller plus loin, faisons le point sur les faits marquants de cette édition.

À retenir



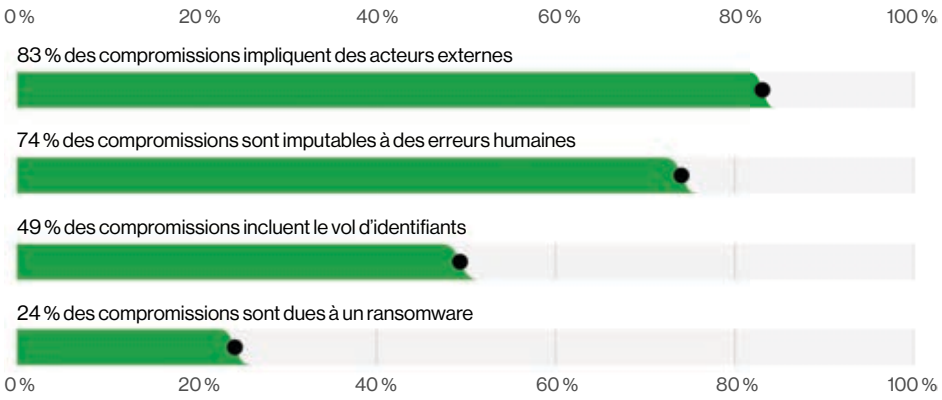
D'une efficacité souvent redoutable, l'ingénierie sociale constitue une activité extrêmement lucrative pour les cybercriminels. C'est peut-être la raison pour laquelle les cas de compromission de messagerie professionnelle (qui sont des actes de pretexting par essence) ont presque doublé dans les données d'incidents analysées, comme le montre la Figure 3. Cette catégorie représente plus de 50 % des incidents recourant à l'ingénierie sociale.

Figure 3. Évolution des incidents de pretexting dans le temps



S'il n'a pas augmenté depuis l'an dernier, le ransomware reste malgré tout l'une des principales causes de compromission avec un taux stable de 24 %. Et toutes les entreprises sont concernées, peu importe la taille ou le secteur.

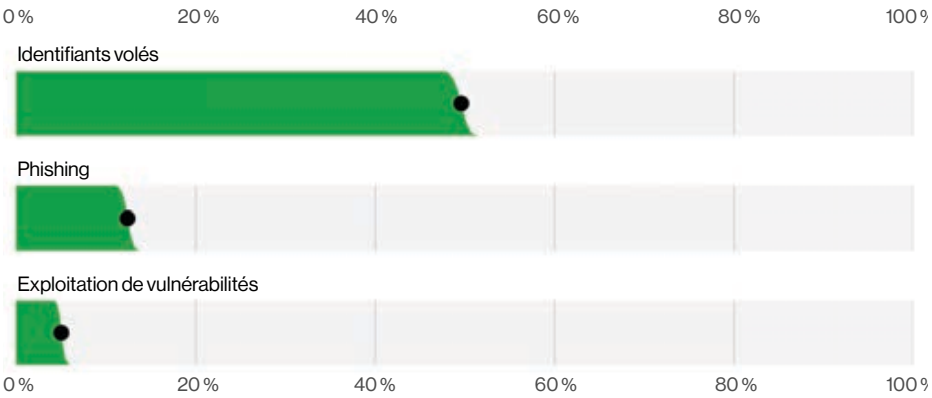
Figure 4. Comparaison des actes de ransomware dans le temps



74 % des compromissions incluent le facteur humain, avec des individus plus ou moins directement impliqués de différentes manières : erreurs accidentelles, abus de privilèges, vols d'identifiants ou ingénierie sociale.

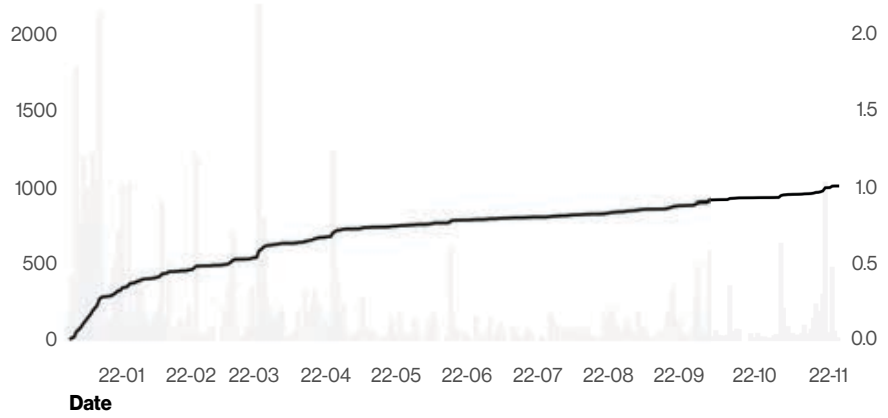
Des acteurs externes sont mis en cause dans 83 % des compromissions et le principal motif des attaques reste majoritairement l'appât du gain, avec 95 % des compromissions concernées.

Figure 5. Part des principaux actes entraînant une compromission



Pour accéder à l'environnement d'une entreprise, les attaquants ont principalement recours à trois modes opératoires : le vol d'identifiants, le phishing et l'exploitation de vulnérabilités.

Figure 6. Part des trois grands vecteurs dans les compromissions hors erreurs et abus de privilèges (n = 4 291)



Plus de 32 % des scans Log4j au cours de l'année ont eu lieu dans les 30 jours qui ont suivi la publication de la CVE (le pic ayant été atteint au bout de 17 jours).

Figure 7. Pourcentage de scans Log4j pour 2022

La vulnérabilité Log4j est une préoccupation majeure pour les équipes de réponse à incident de nos contributeurs. De fait, 90 % des incidents avec pour mode opératoire l'exploitation d'une vulnérabilité mentionnaient « Log4j » ou « CVE-2021-44228 » en note. Cependant, seuls 20,6 % des incidents comportaient une note.

Figure 8. Pourcentage des exploitations de vulnérabilités identifiées comme Log4j (n = 394).Chaque glyphe représente un incident.

Gros plan par secteur

Quels que soient votre secteur et la taille de votre entreprise, la cybercriminalité constitue un risque à ne pas prendre à la légère. Toutefois, le type et la fréquence des attaques peuvent varier en fonction de la taille, de la fonction et de l'implantation géographique de votre organisation. Pour mettre en place un système de défense efficace, vous devez non seulement examiner le champ des menaces dans son ensemble, mais aussi celles qui vous concernent le plus. Cette année encore, nous proposons un état des lieux de 10 grands secteurs.

Intitulés de secteurs

Notre classification sectorielle pour le rapport DBIR 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 « Service public (SCIAN 92) », le nombre 92 ne correspond pas à une valeur, mais au code défini pour ce secteur. De plus amples détails sur les codes et le système de classification sont disponibles ici : https://www.census.gov/naics/?58967?yearbck=2012

Hôtellerie et restauration

(SCIAN 72)

Volume	254 incidents, dont 68 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 90 % des compromissions.
Attaquants	Externes (93 %), internes (9 %), multiples (1 %) (compromissions)
Motivations	Financières (100 %) (compromissions)
Données compromises	Données de paiement (41 %), identifiants (38 %), personnelles (34 %), autres (26 %) (compromissions)
Ce qui n'a pas changé	Comme l'an dernier, ce secteur subit les trois mêmes types d'attaques. Seul l'ordre a changé. Les acteurs externes continuent de cibler ce secteur en raison des données lucratives qu'il renferme.
Conclusion	Sans surprise, les données de paiement demeurent le principal type de données compromises dans ce secteur. Les *RAM scrapers* restent l'outil favori des assaillants qui s'en prennent inlassablement à ce secteur dans le but de s'enrichir.

Enseignement

(SCIAN 61)

Volume	497 incidents, dont 238 compromissions de données confirmées
Principaux schémas	L'intrusion système, les erreurs diverses et l'ingénierie sociale représentent 76 % des compromissions
Attaquants	Externes (72 %), internes (29 %), multiples (1 %), partenaires (1 %) (compromissions)
Motivations	Financières (92 %), espionnage (8 %), commodité (1 %), piratage récréatif (1 %) (compromissions)
Données compromises	Données personnelles (56 %), identifiants (40 %), autres (25 %), internes (20 %) (compromissions)
Ce qui n'a pas changé	Cette année encore, l'intrusion système et les erreurs diverses constituent deux des trois principaux schémas visant ce secteur. Le rapport entre acteurs externes et internes reste quasiment identique à celui de l'an dernier.
Conclusion	Les attaques d'applications web de base ne font plus partie des trois principaux schémas et cèdent leur place à l'ingénierie sociale sur ce triste podium. Le ransomware reste particulièrement présent dans ce secteur.

Finance et assurance

(SCIAN 52)

Volume	1 832 incidents, dont 480 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web de base, les erreurs diverses et l'intrusion système représentent 77 % des compromissions
Attaquants	Externes (66 %), internes (34 %), multiples (1 %) (compromissions)
Motivations	Financières (97 %), espionnage (3 %), commodité (1 %), idéologiques (1 %) (compromissions)
Données compromises	Données personnelles (74 %), identifiants (38 %), autres (30 %), bancaires (21 %) (compromissions)
Ce qui n'a pas changé	Les trois principaux schémas restent les mêmes. Seul l'ordre change. Particulièrement utiles aux fraudes, les données personnelles continuent d'être visées dans la majorité des attaques.
Conclusion	Étant donné la prédominance des attaques d'applications web de base, il est évident que les assaillants parviennent à s'infiltrer dans les environnements sans trop de difficultés. Le grand nombre d'erreurs d'adressage indique également que de meilleurs contrôles permettraient de réduire une bonne part des attaques visant ce secteur.

Santé

(SCIAN 62)

Volume	525 incidents, dont 436 compromissions de données confirmées
Principaux schémas	L'intrusion de système, les attaques d'applications web de base et les erreurs diverses représentent 68 % des compromissions
Attaquants	Externes (66 %), internes (35 %), multiples (2 %) (compromissions)
Motivations	Financières (98 %), espionnage (2 %), piratage récréatif (1 %), idéologiques (1 %) (compromissions)
Données compromises	Données personnelles (67 %), médicales (54 %), identifiants (36 %), autres (17 %) (compromissions)
Ce qui n'a pas changé	Les trois principaux schémas restent les mêmes. Seul l'ordre change. Les erreurs commises par des acteurs internes continuent de nuire à ce secteur.
Conclusion	Ce secteur reste la proie des auteurs de ransomware, entraînant de fait un nombre croissant de compromissions de données avérées. Les erreurs (d'adressage en particulier) sont fréquentes et les menaces internes gagnent du terrain.

Information

(SCIAN 51)

Volume	2 110 incidents, dont 384 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 77 % des compromissions
Attaquants	Externes (81 %), internes (20 %), multiples (2 %), partenaires (1 %) (compromissions)
Motivations	Financières (92 %), espionnage (8 %) (compromissions)
Données compromises	Données personnelles (51 %), identifiants (37 %), autres (35 %), internes (19 %) (compromissions)
Ce qui n'a pas changé	L'intrusion système reste le principal schéma d'attaque dans ce secteur, encore dominé par des acteurs externes à visées financières.
Conclusion	Comme c'est le cas depuis plusieurs années, les erreurs perdent du terrain et cèdent leur place à l'ingénierie sociale dans le top 3. Les attaques par déni de service représentent 70 % des incidents classés pour ce secteur d'activité.

Industrie

(SCIAN 31-33)

Volume	1 817 incidents, dont 262 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 83 % des compromissions
Attaquants	Externes (90 %), internes (11 %), multiples (2 %), partenaires (1 %) (compromissions)
Motivations	Financières (96 %), espionnage (4 %), commodité (1 %) (compromissions)
Données compromises	Données personnelles (60 %), identifiants (38 %), autres (37 %), internes (18 %) (compromissions)
Ce qui n'a pas changé	Les trois principaux schémas restent les mêmes. Seul l'ordre change légèrement. Les acteurs externes motivés par l'appât du gain continuent de causer de sérieux dégâts dans ce secteur.
Conclusion	Les malwares et actes de hacking trustent les deux premières places au coude à coude. Si les attaques par ingénierie sociale sont toujours aussi tenaces, elles restent néanmoins loin derrière au troisième rang. Concernant les incidents, les attaques par déni de service contre l'infrastructure des entreprises industrielles restent préoccupantes, car elles impactent directement les délais de production.

Exploitation minière, extraction de pétrole et de gaz + compagnies d'énergie

(SCIAN 21 + 22)

Volume	143 incidents, dont 47 compromissions de données confirmées
Principaux schémas	L'intrusion de système, les attaques d'applications web de base et les erreurs diverses représentent 81 % des compromissions
Attaquants	Externes (80 %), internes (20 %) (compromissions)
Motivations	Financières (63 à 93 %), espionnage (4 à 32 %), représailles (1 à 21 %), idéologiques (0 à 15 %), commodité/intimidation/piratage récréatif/autres/secondaires (0 à 7 % chacun) (compromissions)
Données compromises	Données personnelles (50 %), internes (33 %), autres (26 %), identifiants (24 %) (compromissions)
Ce qui n'a pas changé	L'intrusion système et les attaques d'applications web de base restent une source d'inquiétude majeure pour ce secteur.
Conclusion	Le ransomware est responsable de près d'une compromission sur trois dans ce secteur. Et malgré une hausse globale, l'ingénierie sociale semble en recul dans ces entreprises.

Services professionnels, scientifiques et techniques

(SCIAN 54)

Volume	1 398 incidents, dont 423 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 90 % des compromissions
Attaquants	Externes (92 %), internes (9 %), multiples (3 %), partenaires (2 %) (compromissions)
Motivations	Financières (96 %), espionnage (4 %), commodité (1 %) (compromissions)
Données compromises	Données personnelles (57 %), identifiants (53 %), autres (25 %), internes (16 %) (compromissions)
Ce qui n'a pas changé	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale restent des menaces majeures pour les entreprises et organisations de ce secteur.
Conclusion	Si les principaux schémas restent les mêmes, ce secteur fait face à une montée des ransomwares depuis l'an dernier. Quant aux incidents, ils sont causés par les mêmes vecteurs principaux que lors des 12 mois précédents.

Service public

(SCIAN 92)

Volume	3 273 incidents, dont 584 compromissions de données confirmées
Principaux schémas	L'intrusion système, le vol ou la perte de ressources et l'ingénierie sociale représentent 76 % des compromissions
Attaquants	Externes (85 %), internes (30 %), multiples (16 %) (compromissions)
Motivations	Financières (68 %), espionnage (30 %), idéologiques (2 %) (compromissions)
Données compromises	Données personnelles (38 %), autres (35 %), identifiants (33 %), internes (32 %) (compromissions)
Ce qui n'a pas changé	Ce secteur demeure la cible d'attaquants externes à visées financières, mais aussi de groupes d'espionnage à la solde d'États qui cherchent à se renseigner sur les activités de puissances adversaires ou concurrentes. Les informations personnelles restent le type de données le plus convoité.
Conclusion	Cette année encore, ce secteur détient le taux le plus élevé de compromissions liées à des activités d'espionnage. Les compromissions sont beaucoup le fait d'acteurs multiples. Et ce rapprochement d'acteurs externes, internes et partenaires unissant leurs forces pour faire main basse sur des données n'est certainement pas ce que nous souhaitons voir se développer à l'échelle mondiale.

Retail

(SCIAN 44-45)

Volume	406 incidents, dont 193 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 88 % des compromissions
Attaquants	Externes (94 %), internes (7 %), multiples (2 %), partenaires (2 %) (compromissions)
Motivations	Financières (100 %), espionnage (1 %) (compromissions)
Données compromises	Données de paiement (37 %), identifiants (35 %), autres (32 %), personnelles (23 %) (compromissions)
Ce qui n'a pas changé	Les enseignes du retail restent des cibles lucratives pour les cybercriminels qui convoitent les données de carte bancaire.
Conclusion	Si les mêmes trois grands schémas dominent ce secteur, comme pour beaucoup d'autres, le retail est aussi visé pour les données de carte bancaire en sa possession, en plus des menaces courantes comme le ransomware et les attaques d'applications web de base.

Petites et moyennes entreprises

Dans certains de nos rapports précédents, nous avons comparé les PME aux grandes entreprises pour savoir si la surface d'attaque différait sensiblement d'une catégorie à l'autre. Or, il s'avère que les infrastructures et services utilisés par les unes comme par les autres se recoupent de plus en plus. D'où des similarités sans précédent entre leurs surfaces d'attaques respectives et une convergence des profils d'attaque, peu importe la taille de l'entreprise. Ce qui diffère, en revanche, c'est la capacité des entreprises à répondre aux menaces en raison des disparités de ressources qu'elles sont à même de déployer en cas d'attaque.

C'est pourquoi nous nous sommes appuyés sur notre collaboration avec MITRE pour recadrer l'alignement de la structure VERIS sur le framework ATT&CK, et ainsi être davantage en prise avec le monde réel. Vous pouvez ainsi associer ces mappings aux contrôles du groupe d'implémentation du CIS (Center for Internet Security) selon la taille de votre entreprise.

Attaque des frameworks
L'équipe de rédaction du DBIR continue de s'appuyer sur la structure VERIS (Vocabulary for Event Recording and Incident Sharing) pour classifier et analyser les incidents et compromissions. Nous avons développé des mappings en collaboration avec le framework MITRE ATT&CK et le Center for Internet Security's Critical Security Controls (CIS CSC) afin d'aider les entreprises à élaborer et maintenir un programme de cybersécurité basé sur des données précises et actualisées.

La deuxième version du mapping VERIS/ATT&CK a été publiée le 6 avril 2023 et nous vous invitons à consulter la page https://center-for-threat-informed-defense.github.io/attack_to_veris/. Cette alliance renouvelée arrive à point nommé, dans un contexte de durcissement réglementaire qui impose de plus en plus de déclarer toute compromission de données, bien que la forme de ces déclarations ne soit pas encore clairement définie.

	PME (moins de 1 000 salariés)	Grandes entreprises (plus de 1 000 salariés)
Volume	699 incidents, dont 381 compromissions de données confirmées	496 incidents, dont 227 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 92 % des compromissions	L'intrusion de système, l'ingénierie sociale et les attaques d'applications web de base représentent 85 % des compromissions
Attaquants	Externes (94 %), internes (7 %), multiples (2 %), partenaires (1 %) (compromissions)	Externes (89 %), internes (13 %), multiples (2 %), partenaires (2 %) (compromissions)
Motivations	Financières (98 %), espionnage (1 %), commodité (1 %), représailles (1 %) (compromissions)	Financières (97 %), espionnage (3 %), idéologiques (2 %), commodité (1 %), piratage récréatif (1 %) (compromissions)
Données compromises	Identifiants (54 %), données internes (37 %), autres (22 %), systèmes (11 %) (compromissions)	Données internes (41 %), identifiants (37 %), autres (30 %), systèmes (22 %) (compromissions)

Résultats par région

Cette édition du DBIR est la quatrième à vous proposer une analyse des cyberincidents par région du globe. Nous espérons que les résultats présentés vous apporteront des éclairages utiles. Comme nous l'avons déjà évoqué, notre visibilité sur une région en particulier dépend de nombreux facteurs, y compris nos contributeurs, les lois relatives à la divulgation d'informations dans chaque région et nos propres données. Si votre zone géographique n'est pas représentée 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. Cela nous permettra d'étendre et d'améliorer notre couverture géographique d'une année sur l'autre. Pour l'heure, si une région n'est pas répertoriée dans ce rapport, c'est parce que nous y avons recensé un nombre d'incidents insuffisant pour créer une section représentative et statistiquement pertinente.

Asie-Pacifique (APAC)

Volume	699 incidents, dont 164 compromissions de données confirmées
Principaux schémas	L'ingénierie sociale, l'intrusion système et les attaques d'applications web de base représentent 93 % des compromissions
Attaquants	Externes (92 %), internes (9 %), partenaires (2 %), multiples (2 %) (compromissions)
Motivations	Financières (61 %), espionnage (39 %), commodité (2 %), représailles (2 %), secondaires (1 %) (compromissions)
Données compromises	Données internes (56 %), secrets (42 %), autres (33 %), identifiants (29 %) (compromissions)

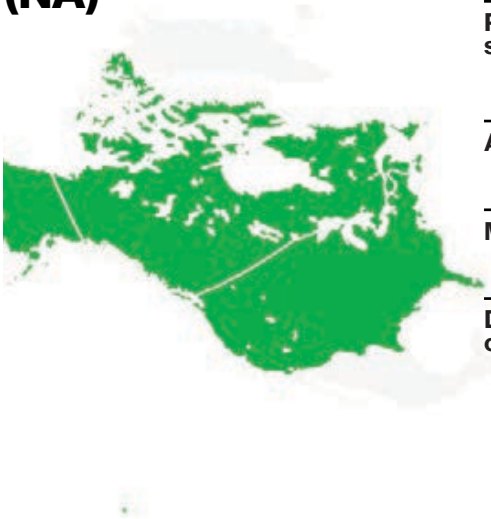
Europe, Moyen-Orient et Afrique (EMEA)

Volume	2 557 incidents, dont 637 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 97 % des compromissions
Attaquants	Externes (98 %), internes (2 %), multiples (1 %) (compromissions)
Motivations	Financières (91 %), espionnage (8 %), idéologiques (1 %), piratage récréatif (1 %) (compromissions)
Données compromises	Identifiants (53 %), données internes (37 %), systèmes (35 %), autres (15 %) (compromissions

Amérique latine et Caraïbes (LAC)

Volume	535 incidents, dont 65 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 94 % des compromissions
Attaquants	Externes (95 %), internes (5 %), partenaires (2 %), multiples (2 %) (compromissions)
Motivations	Financières (93 %), espionnage (11 %), idéologiques (2 %) (compromissions)
Données compromises	Données systèmes (55 %), internes (32 %), confidentielles (23 %), identifiants (23 %), autres (19 %) (compromissions)

Amérique du Nord (NA)



Volume	9 036 incidents, dont 1 924 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 85 % des compromissions
Attaquants	Externes (94 %), internes (12 %), multiples (9 %), partenaires (2 %) (compromissions)
Motivations	Financières (99 %), espionnage (1 %), représailles (1 %) (compromissions)
Données compromises	Identifiants (67 %), données internes (50 %), personnelles (38 %), autres (24 %) (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 votre organisation. Bénéficiez de tous les éclairages concrets dont vous avez besoin pour sécuriser votre entreprise.

Lisez le rapport DBIR 2023 complet sur verizon.com/dbir/.

Envie d’œuvrer pour un monde digital plus sûr ?

Le DBIR s’appuie sur les contributions de dizaines d’entreprises. Pourquoi ne pas apporter votre pierre à l’édifice ? Pour contribuer au rapport annuel de Verizon, rien de plus simple : écrivez-nous à dbircontributor@verizon.com ou contactez-nous par twitter à @VZDBIR pour nous faire part de vos commentaires afin de nous aider à améliorer la prochaine édition. Vous pouvez également consulter la page verisframework.org pour en savoir plus sur la structure VERIS.