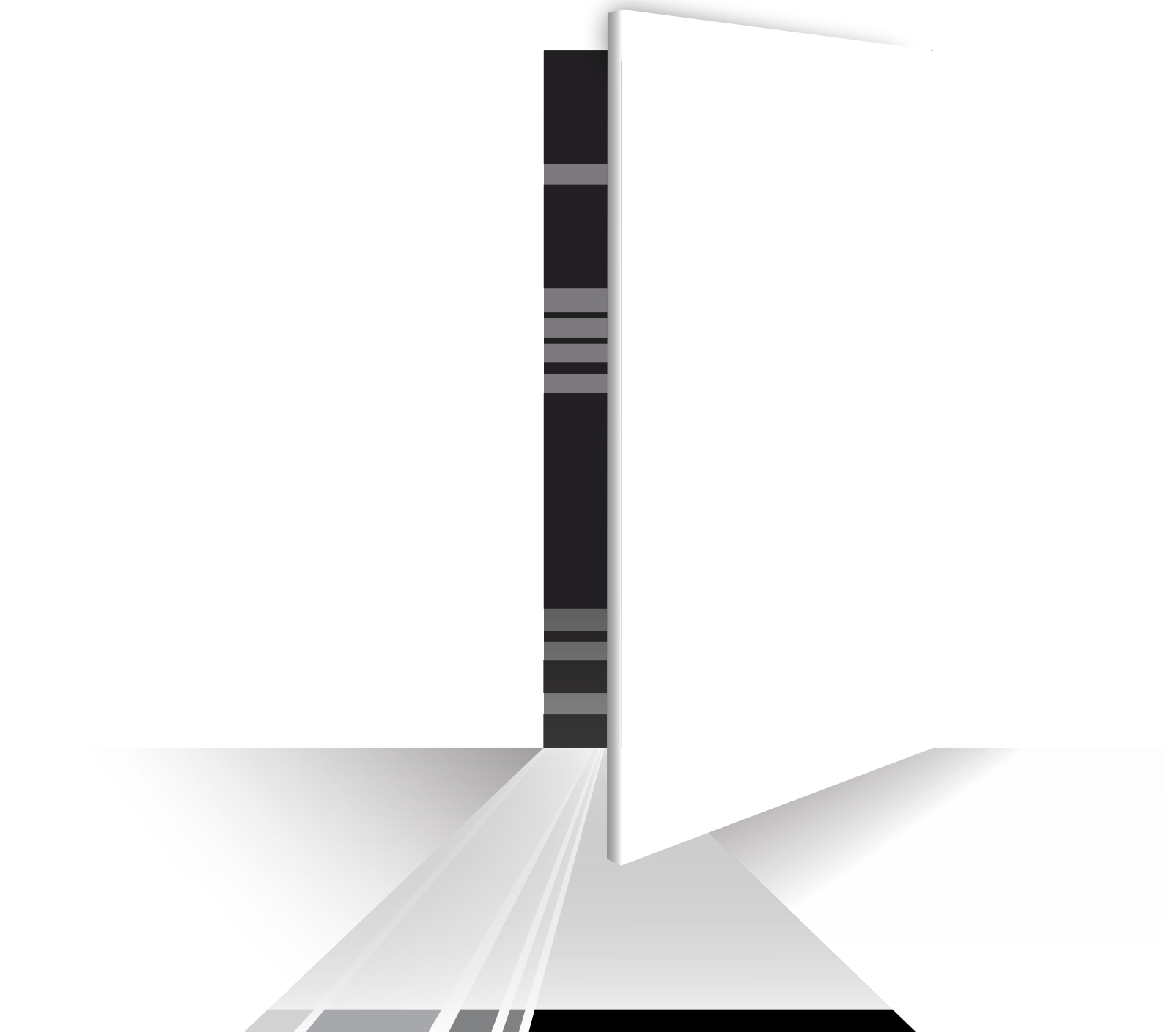
Rapport Data Breach Investigations Report – DBIR – 2024

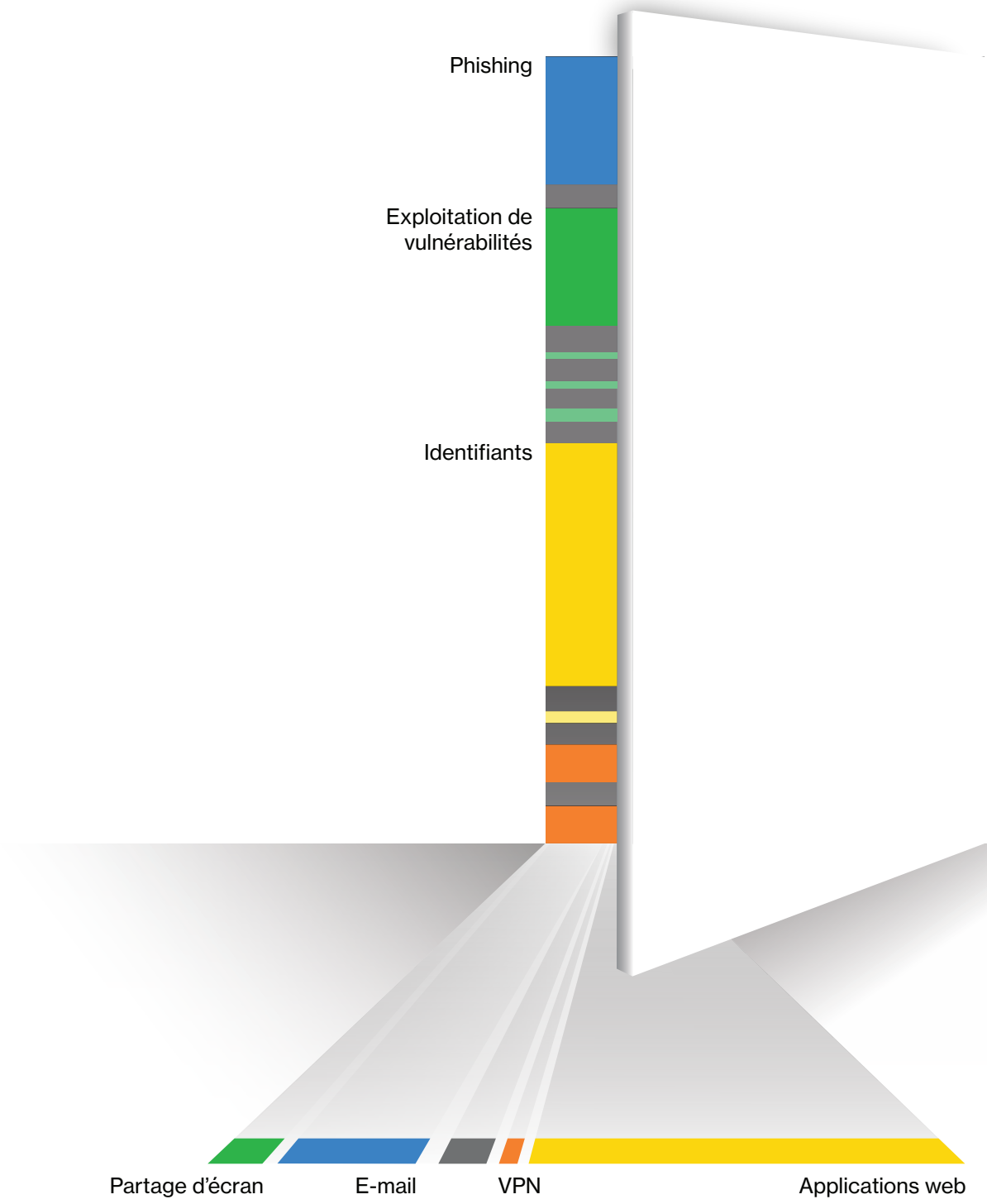
Document de synthèse



verizon business

À propos de la représentation en couverture

Cette année, notre rapport va encore plus loin dans son analyse pour mettre en relation les actions et vecteurs à l'origine de compromissions, et ainsi dresser un état des lieux complet de la menace actuelle. La porte entrouverte en couverture représente les différentes brèches que les attaquants peuvent utiliser pour s'introduire dans un environnement. À l'intérieur, la bande gris foncé matérialise les vecteurs de compromission et leurs proportions, délimitées par les traits gris clair (la figure 7 du rapport complet reprend ces mêmes données dans un schéma plus classique). La bande de lumière projetée au sol montre quant à elle les actions à l'origine de ces compromissions, là aussi en fonction de leur part dans la totalité des incidents analysés. Le schéma en page 3 ajoute de la couleur pour plus de clarté. Voilà pour la partie art contemporain !


Phishing
Exploitation de vulnérabilités
Identifiants
Partage d’écran
E-mail
VPN
Applications web

Sommaire

Introduction

Bienvenue dans le DBIR 2024 de Verizon.

Cette année marque la 17e édition de notre rapport consacré aux compromissions des données. Que vous soyez lecteur de la première heure ou que vous découvriez notre rapport pour la première fois, vous trouverez dans cette étude de précieux éclairages sur le profil des attaquants, leurs modes opératoires et leurs cibles privilégiées. Nous en profitons pour saluer le talent, la générosité et le dévouement de nos contributeurs du monde entier qui, année après année, nous livrent leurs perspectives et leurs données. Nous remercions également les membres de l'équipe VTRAC (Verizon Threat Research Advisory Center), dont nous ne louerons jamais assez l'action. Chacun de ces deux groupes nous aide à examiner et à analyser les tendances phares de la cybersécurité qui impactent les entreprises de tous horizons.

Chaque année, nous voyons apparaître des attaques complètement inédites, en même temps que de nouvelles variantes de techniques qui ont maintes fois fait leurs preuves. De l'exploitation de vulnérabilités zero-day (comme celle qui a frappé le logiciel de transfert de fichiers MOVEit) au classique mais redoutable ransomware, en passant par le vol d'identifiants et les attaques par déni de service (DoS), les cybercriminels ne reculent devant rien pour donner tort à tous ceux qui pensent encore que le crime ne paie pas.

Difficile de suivre le rythme face à ces menaces en constante évolution. Et cette année a été particulièrement prolifique pour les acteurs malveillants. Nous avons passé au crible pas moins de 30 458 incidents réels (un chiffre record !) dans 94 pays, dont 10 626 compromissions de données avérées. Vous trouverez dans ces pages les points les plus saillants de notre rapport. Nous espérons qu'ils vous apporteront des éclairages utiles sur un danger qui vous concerne au premier degré.

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

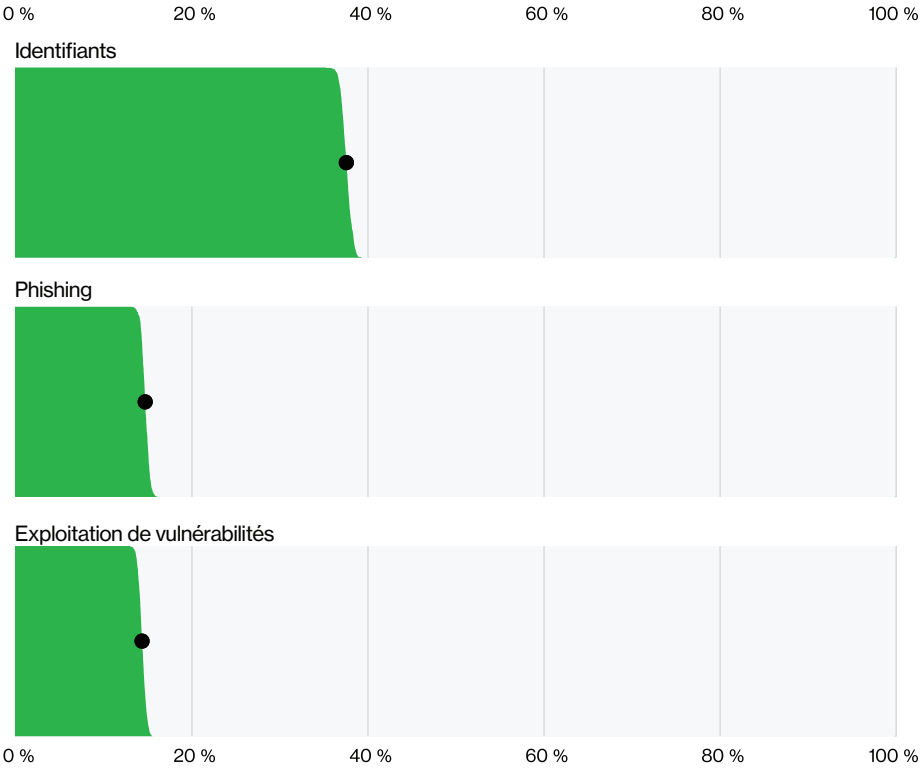


Figure 1. Part des trois grands vecteurs dans les compromissions hors erreurs et abus de privilèges (n = 6 963)

Le nombre d'attaques utilisant l'exploitation des vulnérabilités comme principal vecteur d'intrusion et de compromission a presque triplé en 12 mois (+180 %). Cette prolifération s'explique par la multiplication des vulnérabilités zero-day (comme celle dans l'incident MOVEit), exploitées principalement par les groupes de ransomware et autres spécialistes de l'extorsion qui font des applications web leur point d'entrée initial.

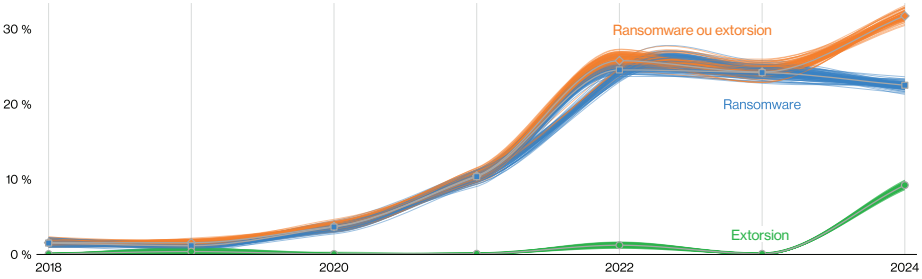


Figure 2. Évolution chronologique de la proportion des compromissions liées aux ransomwares et à l'extorsion

Près d'un tiers des compromissions impliquaient un ransomware ou d'autres techniques d'extorsion. L'extorsion pure est en hausse par rapport à l'année dernière. Elle représente désormais 9 % de toutes les compromissions et prend peu à peu la place des ransomwares classiques, en recul à 23 %. Néanmoins, ces techniques représentent à elles deux 32 % des compromissions. Quant au ransomware, il reste l'ennemi n° 1 dans 92 % des secteurs.

Figure 3. Part des principaux vecteurs de compromission

Nous avons recalculé l'incidence du facteur humain pour exclure les abus de privilèges et montrer plus clairement l'impact du niveau de sensibilisation aux enjeux de sécurité. Mais cette année encore, ce facteur humain intervient dans 68 % des compromissions, un chiffre relativement similaire à celui présenté dans notre DBIR 2023.

Nous avons également revu et élargi le concept de compromission imputable à un tiers, qui englobe désormais les incidents sur les infrastructures de partenaires et les problèmes (directs et indirects) sur la supply chain logicielle, y compris les cas où une entreprise est impactée par une vulnérabilité sur un logiciel tiers. En clair, il s'agit d'incidents que les organisations peuvent éviter en tentant de sélectionner des fournisseurs justifiant d'un parcours irréprochable en matière de sécurité. Ce type de compromissions représente 15 % du chiffre total, soit une augmentation de 68 % par rapport à l'année précédente. Un boom qui s'explique principalement par l'exploitation des vulnérabilités zero-day dans les attaques de ransomware et d'extorsion.

Notre analyse montre également une hausse des compromissions dues à des erreurs, aujourd'hui à 28 %. Cette augmentation s'explique notamment par le fait que notre groupe de contributeurs s'est étoffé de plusieurs entités concernées par l'obligation de signalement des compromissions. Ce chiffre vient confirmer notre théorie : les erreurs sont bien plus prévalentes que ce que laissent entendre les médias ou les équipes de réponse à incident.

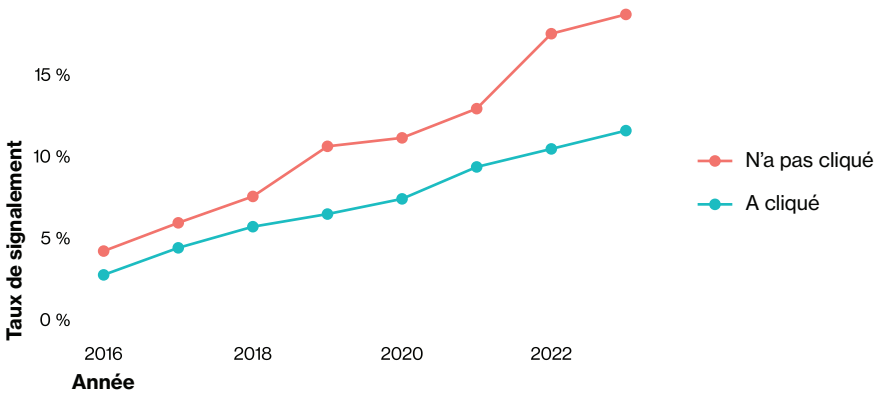


Figure 4. Taux de signalement des e-mails de phishing en fonction de la réaction du destinataire

Le taux de signalement des e-mails de phishing a augmenté ces dernières années. Selon les résultats des campagnes de sensibilisation transmis par nos contributeurs en 2023, 20 % des utilisateurs ciblés lors d'une simulation ont lancé l'alerte. Autre chiffre intéressant, 11 % des utilisateurs qui ont ouvert l'e-mail ont aussi signalé l'incident. C'est une bonne nouvelle, surtout lorsque l'on sait qu'une fois l'e-mail ouvert, la victime met environ 21 secondes pour cliquer sur le lien malveillant et 28 secondes supplémentaires pour entrer ses données. Bref, si l'on fait le calcul, un utilisateur mord à l'hameçon du phishing en moins de 60 secondes (délai médian).

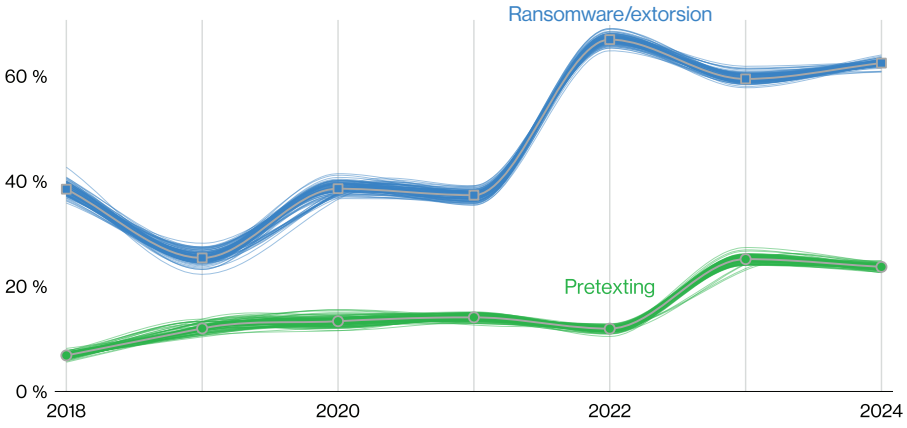


Figure 5. Évolution chronologique des principales actions à l'origine d'attaques à motivations financières

Les acteurs à motivations financières s'arrêteront logiquement sur les techniques qui leur offrent le meilleur retour sur investissement.

Au cours des trois dernières années, les ransomwares et autres extorsions combinés ont représenté près de deux tiers des compromissions (fluctuant entre 59 % et 66 %). Selon les plaintes enregistrées par la cellule IC3 (Internet Crime Complaint Center) du FBI, les pertes médianes associées à la combinaison ransomwares et extorsions s'élèvent à 46 000 $ pour 95 % des cas, allant de 3 $ pour le montant le plus faible à 1 141 467 $ pour le plus élevé. Nous avons également passé en revue les données de nos contributeurs sur les négociations avec les gangs de ransomware. Les rançons exigées par les attaquants comptent généralement pour 1,34 % du chiffre d'affaires de la victime (pourcentage médian), mais ce ratio varie entre 0,13 % et 8,3 % dans 4 cas sur 5.

Enfin, ces deux dernières années ont été marquées par plusieurs incidents impliquant le pretexting. Cette technique d'ingénierie sociale a été employée dans un quart des attaques motivées par l'appât du gain (entre 24 % et 25 %). Elle s'est soldée dans la majorité des cas par une compromission de messagerie professionnelle (BEC). Les pertes médianes causées par les BEC se sont élevées à environ 50 000 $.

Gros plan par secteur

Comme nous l'avons déjà mentionné dans nos rapports précédents, les préoccupations varient grandement d'un secteur à l'autre. Tout dépend de la surface d'attaque de l'entreprise, autrement dit le terrain de jeu des attaquants. La cybersécurité est un domaine extrêmement complexe. Profil des attaquants, infrastructures technologiques spécifiques à chaque secteur, types de données traitées et stockées par l'entreprise, méthodes d'accès et d'utilisation des informations… toutes ces variables viennent compliquer l'équation.

Un géant de la tech gérant un vaste parc d'appareils mobiles et d'applications en tout genre ne s'exposera pas aux mêmes risques qu'une boutique indépendante ou qu'une plateforme d'e-commerce. En d'autres termes, la nature de la menace dépend du secteur, de la taille de l'entreprise, et de bien d'autres facteurs. Il faut aussi noter que les différentes branches d'activité ne sont pas toutes soumises aux mêmes obligations de déclaration des incidents. Certains secteurs particulièrement sensibles font en effet l'objet d'un contrôle beaucoup plus draconien de la part des autorités compétentes. Ce chapitre brosse un tour d'horizon des résultats dans les neuf secteurs couverts par notre étude. Nous rappelons au passage que notre classification sectorielle repose sur les codes du Système de classification des industries de l'Amérique du Nord (SCIAN).

Hôtellerie et restauration
(SCIAN 72)

Volume	220 incidents, dont 106 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 92 % des compromissions
Attaquants	Externes (92 %), internes (9 %), multiples (1 %) (compromissions)
Motivations	Financières (100 %) (compromissions)
Données compromises	Identifiants (50 %), données personnelles (28 %), données de paiement (19 %), données système (19 %), autres (16 %) (compromissions)
Ce qui n'a pas changé	Les ransomwares et l'ingénierie sociale continuent de poser problème dans ce secteur, où ils représentent 35 % des incidents.
En bref	Le nombre d'attaques par ingénierie sociale est en forte hausse et compte désormais pour 25 % des compromissions dans le secteur. Les cas de pretexting ont plus que doublé par rapport à l'année précédente (20 % des incidents).

Enseignement
(SCIAN 61)

Volume	1 780 incidents, dont 1 537 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les erreurs diverses représentent 90 % des compromissions.
Attaquants	Externes (68 %), internes (32 %) (compromissions)
Motivations	Financières (98 %), espionnage (2 %) (compromissions)
Données compromises	Données personnelles (83 %), internes (20 %), autres (18 %), identifiants (9 %) (compromissions)
Ce qui n'a pas changé	On retrouve en tête les trois mêmes schémas que l'année précédente. La majorité des compromissions implique le vol de données personnelles par des acteurs externes.
En bref	La principale menace dans ce secteur reste les erreurs commises par des acteurs internes et l'extorsion par des acteurs externes.

Finance et assurance
(SCIAN 52)

Volume	3 348 incidents, dont 1 115 compromissions de données confirmées
Principaux schémas	L'intrusion système, les erreurs diverses et l'ingénierie sociale représentent 78 % des compromissions
Attaquants	Externes (69 %), internes (31 %) (compromissions)
Motivations	Financières (95 %), espionnage (5 %) (compromissions)
Données compromises	Données personnelles (75 %), autres (30 %), données bancaires (27 %), identifiants (22 %) (compromissions)
Ce qui n'a pas changé	Les erreurs diverses continuent de poser problème dans ce secteur, en particulier les erreurs d'adressage.
En bref	L'intrusion système se hisse en tête du classement des menaces dans le secteur de la finance et de l'assurance, doublant au passage les erreurs diverses et les attaques d'applications web de base. Une tendance qui témoigne de la complexification des attaques. L'ingénierie sociale est aussi en hausse. Nous bénéficions cette année de plus de visibilité sur la région EMEA (Europe, Moyen-Orient et Afrique). Ces nouvelles données montrent que dans ces pays, les attaques par ransomware continuent de faire des ravages.

Santé
(SCIAN 62)

Volume	1 378 incidents, dont 1 220 compromissions de données confirmées
Principaux schémas	Les erreurs diverses, l'abus de privilèges et l'intrusion système représentent 83 % des compromissions
Attaquants	Internes (70 %), externes (30 %) (compromissions)
Motivations	Financières (98 %), espionnage (1 %) (compromissions)
Données compromises	Données personnelles (75 %), internes (51 %), autres (25 %), identifiants (13 %) (compromissions)
Ce qui n'a pas changé	L'intrusion système reste en tête des trois principaux schémas d'attaque dans ce secteur.
En bref	L'analyse des données provenant du secteur de la santé montre une évolution marquante par rapport aux années précédentes. En léger recul depuis 2018, les compromissions délibérées causées par des acteurs internes refont surface et se hissent à la seconde place. Fait intéressant, les attaquants délaissent les données médicales au profit des données personnelles.

Information
(SCIAN 51)

Volume	1 367 incidents, dont 602 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 79 % des compromissions
Attaquants	Externes (79 %), internes (21 %), multiples (1 %) (compromissions)
Motivations	Financières (87 %), espionnage (14 %) (compromissions)
Données compromises	Autres (46 %), données personnelles (45 %), identifiants (27 %), internes (22 %) (compromissions)
Ce qui n'a pas changé	Étonnamment, l'ordre et la nature des trois principaux schémas d'attaque restent exactement les mêmes, malgré une explosion du nombre de compromissions par rapport à l'année précédente.
En bref	Si l'échantillon global de compromissions analysées est plus important que celui de l'année précédente, le nombre d'incidents a en revanche diminué dans le secteur. Les ransomwares et le vol d'identifiants dominent toujours le schéma intrusion système. Le phishing recule, à l'inverse du pretexting et de l'ingénierie sociale, qui sont tous les deux en hausse. Nous avons également observé une légère augmentation des attaques d'espionnage (y compris étatique) dans le secteur, soulignant l'importance d'une détection renforcée.

Industrie
(SCIAN 31–33)

Volume	2 305 incidents, dont 849 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les erreurs diverses représentent 83 % des compromissions.
Attaquants	Externes (73 %), internes (27 %) (compromissions)
Motivations	Financières (97 %), espionnage (3 %) (compromissions)
Données compromises	Données personnelles (58 %), autres (40 %), identifiants (28 %), internes (25 %) (compromissions)
Ce qui n'a pas changé	Deux schémas persistent depuis l'année dernière. La plupart des attaques restent motivées par l'appât du gain.
En bref	L'industrie fait face à un nombre croissant de compromissions dues à des erreurs. L'installation de malwares, après connexion au moyen d'identifiants légitimes volés, est également très courante.

Services professionnels, scientifiques et techniques
(SCIAN 54)

Volume	2 599 incidents, dont 1 314 compromissions de données confirmées
Principaux schémas	L'ingénierie sociale, l'intrusion système et les erreurs diverses représentent 85 % des compromissions.
Attaquants	Externes (75 %), internes (25 %) (compromissions)
Motivations	Financières (95 %), espionnage (6 %) (compromissions)
Données compromises	Données personnelles (40 %), identifiants (38 %), autres (33 %), internes (23 %) (compromissions)
Ce qui n'a pas changé	Les données personnelles et les identifiants restent les cibles privilégiées des attaquants dans le secteur.
En bref	L'ingénierie sociale est l'une des principales menaces qui pèsent sur le secteur. Elle représente 40 % des compromissions. Le pretexting ne compte quant à lui que pour 20 % des compromissions. On observe également une augmentation du nombre d'erreurs, en particulier des erreurs d'adressage.

Service public
(SCIAN 92)

Volume	12 217 incidents, dont 1 085 compromissions de données confirmées
Principaux schémas	Les erreurs diverses, l'intrusion système et l'ingénierie sociale représentent 78 % des compromissions
Attaquants	Internes (59 %), externes (41 %) (compromissions)
Motivations	Financières (71 %), espionnage (29 %) (compromissions)
Données compromises	Données personnelles (72 %), internes (37 %), autres (31 %), identifiants (17 %) (compromissions)
Ce qui n'a pas changé	L'intrusion système et l'ingénierie sociale restent les deux principaux schémas observés dans le secteur.
En bref	Par manque de vigilance, les erreurs diverses, en particulier les erreurs d'adressage, se multiplient au point de se retrouver à la première place du classement, suivies par l'intrusion système et l'ingénierie sociale. On note donc à quel point les acteurs internes jouent un rôle prépondérant dans les compromissions recensées.

Retail
(SCIAN 44–45)

Volume	725 incidents, dont 369 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 92 % des compromissions
Attaquants	Externes (96 %), internes (4 %) (compromissions)
Motivations	Financières (99 %), espionnage (1 %) (compromissions)
Données compromises	Identifiants (38 %), autres (31 %), données de paiement (25 %), systèmes (20 %) (compromissions)
Ce qui n'a pas changé	On retrouve, dans le même ordre, les trois principaux schémas d'attaque de l'année précédente. Les attaques à motivations financières continuent de faire rage dans le secteur.
En bref	Les attaquants ciblant ce secteur visaient autrefois les données de paiement. Aujourd'hui, ils jettent leur dévolu sur les identifiants. Le phishing est en recul, mais le pretexting se fait plus fréquent. Les attaques DoS restent un vrai problème pour les entreprises du retail. En paralysant leurs systèmes, elles les empêchent de servir leurs clients et impactent leur chiffre d'affaires.

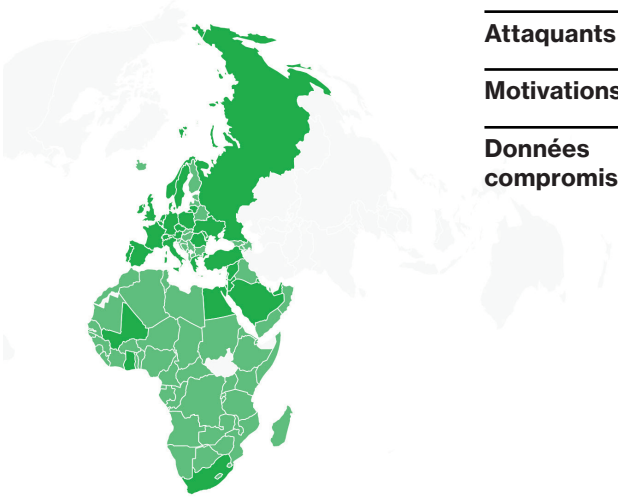
Résultats par région

Cette année encore, le DBIR fournit une analyse géographique des incidents et compromissions pour donner à nos lecteurs un aperçu de l'évolution – ou non – des tendances en matière de cybercrime, région par région. Comme nous l'avons mentionné par le passé, notre visibilité sur une région donnée dépend de multiples facteurs : la présence de contributeurs, les obligations de notification régionales, nos propres investigations, etc. Nous espérons que nos lecteurs trouveront dans cette perspective globale des informations utiles et instructives.

Asie-Pacifique (APAC)

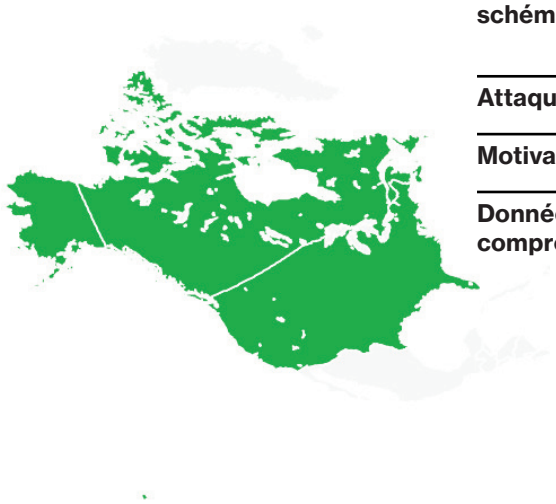
Volume	2 130 incidents, dont 523 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 95 % des compromissions
Attaquants	Externes (98 %), internes (2 %) (compromissions)
Motivations	Financières (75 %), espionnage (25 %) (compromissions)
Données compromises	Identifiants (69 %), internes (37 %), secrets (24 %), autres (17 %) (compromissions)

Europe, Moyen-Orient et Afrique (EMEA)



Volume	8 302 incidents, dont 6 005 compromissions de données confirmées
Principaux schémas	Les erreurs diverses, l'intrusion système et l'ingénierie sociale représentent 87 % des compromissions
Attaquants	Externes (51 %), internes (49 %) (compromissions)
Motivations	Financières (94 %), espionnage (6 %) (compromissions)
Données compromises	Données personnelles (64 %), autres (36 %), données internes (33 %), identifiants (20 %) (compromissions)

Amérique du Nord (NA)



Volume	16 619 incidents, dont 1 877 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 91 % des compromissions
Attaquants	Externes (93 %), internes (8 %) (compromissions)
Motivations	Financières (97 %), espionnage (4 %) (compromissions)
Données compromises	Données personnelles (50 %), identifiants (26 %), données internes (19 %), autres (16 %) (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 2024 complet 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 sur X à @VZDBIR et consultez la page VERIS GitHub : https://github.com/vz-risk/veris.