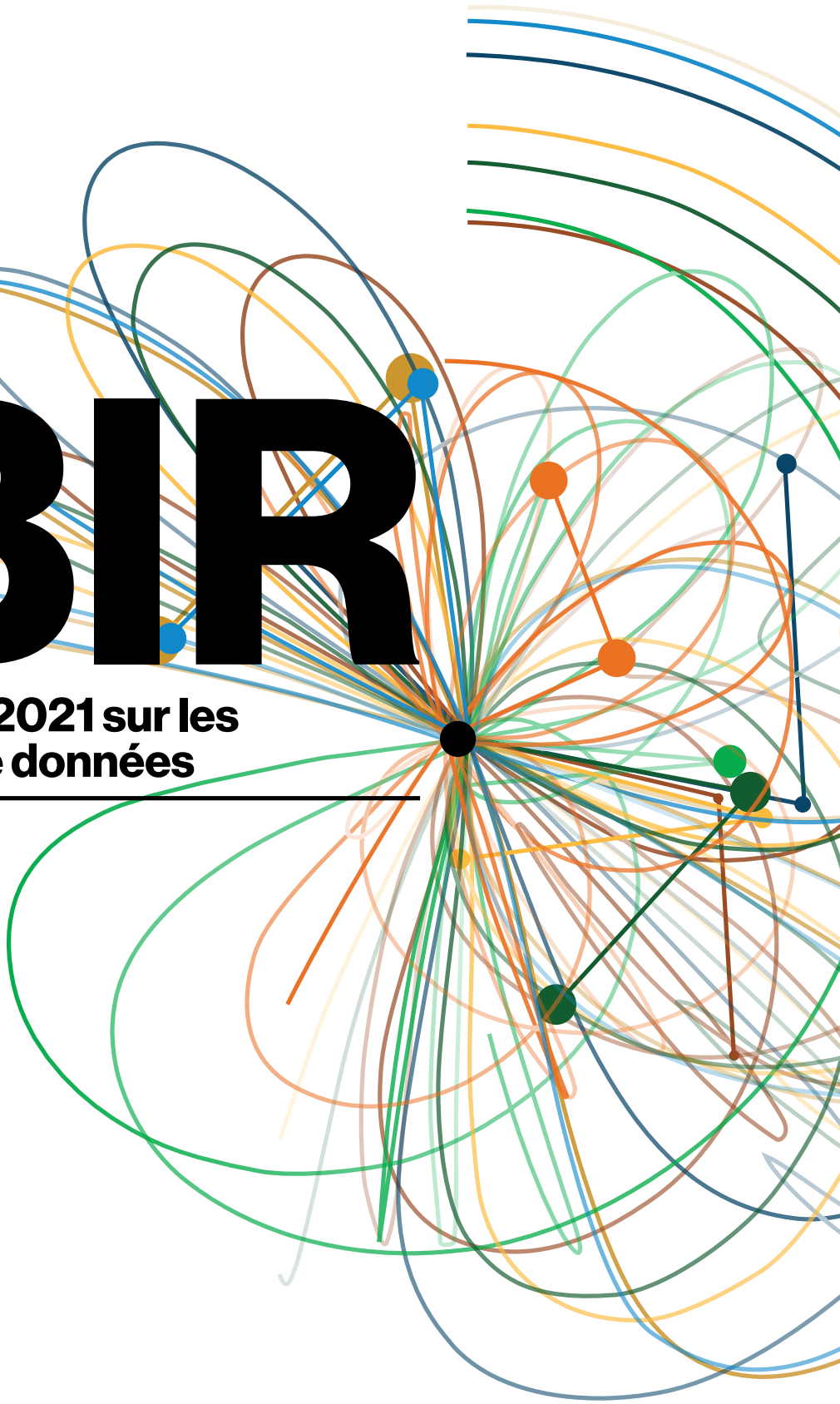
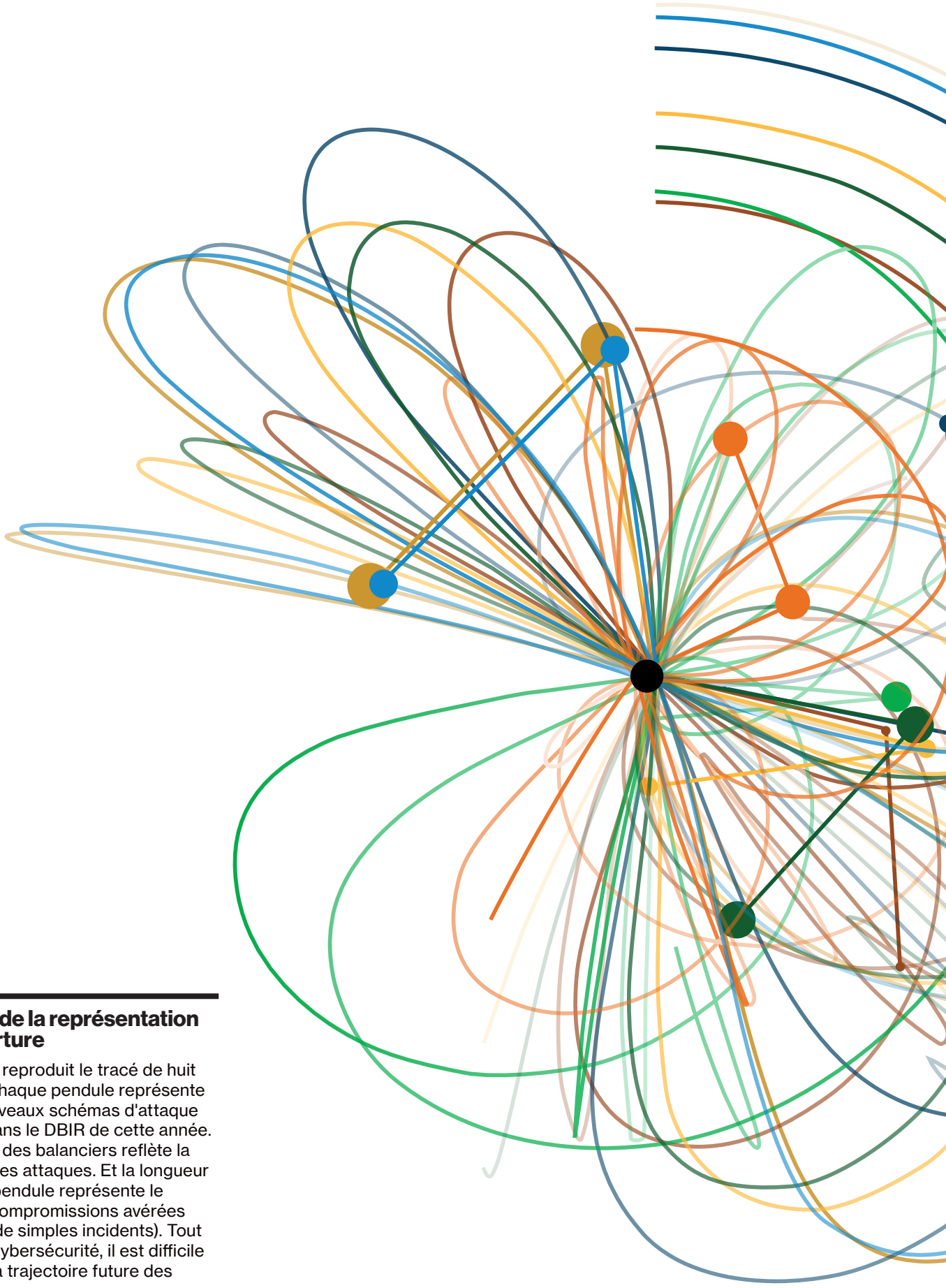
DBIR

Rapport d'enquête 2021 sur les compromissions de données

Document de synthèse



verizon



À propos de la représentation en couverture

Cette figure reproduit le tracé de huit pendules. Chaque pendule représente l'un des nouveaux schémas d'attaque explicités dans le DBIR de cette année. Le diamètre des balanciers reflète la fréquence des attaques. Et la longueur de chaque pendule représente le volume de compromissions avérées (plutôt que de simples incidents). Tout comme en cybersécurité, il est difficile de prédire la trajectoire future des pendules.

Sommaire

Rester vigilant dans un monde en pleine mutation

Les changements arrivent souvent sans prévenir, obligeant les entreprises à réagir dans l'urgence et à remettre à plat toute leur stratégie de sécurité. Mais pour faire les bons choix, mieux vaut être bien informé. Si nul ne peut prédire à la lettre comment les menaces évolueront au cours des douze prochains mois, les entreprises peuvent néanmoins discerner les grandes tendances et établir des probabilités pour mieux s'y préparer. C'est dans cet esprit que nous publions chaque année notre rapport d'enquête sur les compromissions de données (DBIR, Data Breach Investigations Report). Pour sa 14ème édition, ce document rassemble les contributions d'un nombre record de 83 organisations. Le rapport 2021 est le fruit d'une analyse de 29 207 incidents de sécurité, dont 5 258 compromissions de données confirmées.

Cette année, une méthode de clustering par machine learning a permis de mettre à jour les schémas d'attaque décrits dans le DBIR. Désormais au nombre de sept, ces schémas comprennent deux nouvelles catégories : ingénierie sociale et intrusion de système. Le schéma « attaques d'applications web » a fait l'objet d'une refonte complète pour devenir « attaques d'applications web de base », tandis que les catégories « attaque DoS », « vol ou perte de ressources », « erreurs diverses », « abus de privilèges » et « autres » ont elles aussi été recalibrées. Une fois encore, nous nous sommes penchés sur différentes parties du globe pour fournir une analyse régionale des tendances de compromissions. Douze secteurs sont passés à la loupe et nous dressons par ailleurs un comparatif de l'exposition des entreprises par taille (PME/ETI vs. grandes entreprises).

Découvrez sans plus attendre les principales conclusions du DBIR 2021, envoyez cette synthèse à vos collègues et téléchargez le rapport complet sur verizon.com/fr/dbir pour disposer d'une vision plus approfondie sur les menaces qui devraient dominer l'actualité de la cybersécurité en 2021.

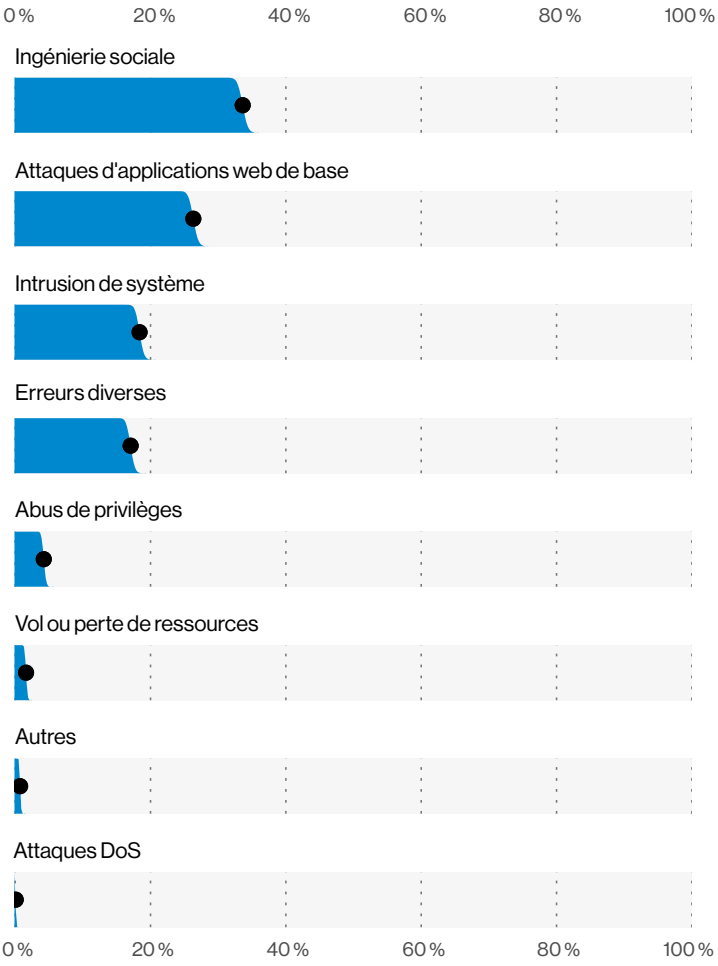
29 207

incidents de sécurité analysés, dont 5 258 compromissions de données confirmées

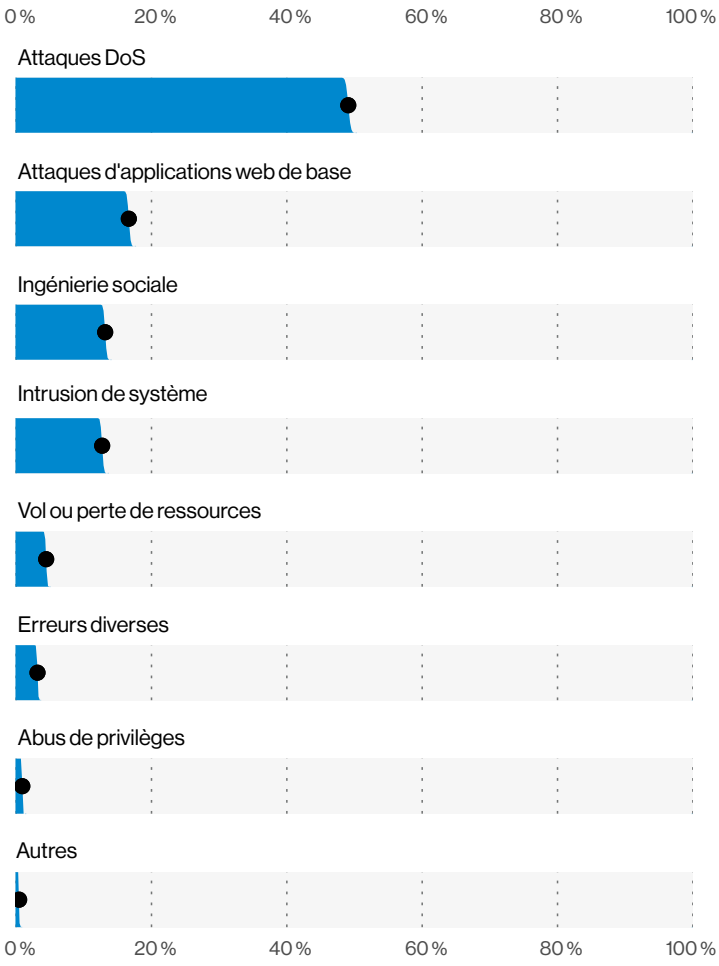
Des améliorations continues

L'équipe de rédaction du DBIR 2021 s'appuie sur la structure VERIS (Vocabulary for Event Recording and Incident Sharing), enrichie et simplifiée, pour classifier et analyser les incidents et compromissions. Nous avons également développé un nouveau mapping avec la toute dernière version des contrôles du CIS (Center for Internet Security), publiés en début d'année. Certains de ces contrôles sont recommandés pour chaque secteur étudié dans le DBIR afin de leur fournir des conseils et recommandations propres aux spécificités de leurs métiers respectifs. Ces nouveaux points de référence nous ont permis d'optimiser nos analyses et de les mettre à la disposition de toute la communauté de la sécurité.

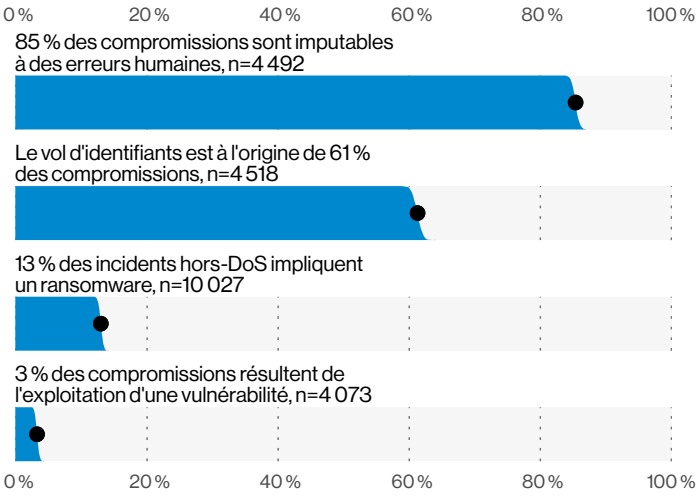
Synthèse des résultats



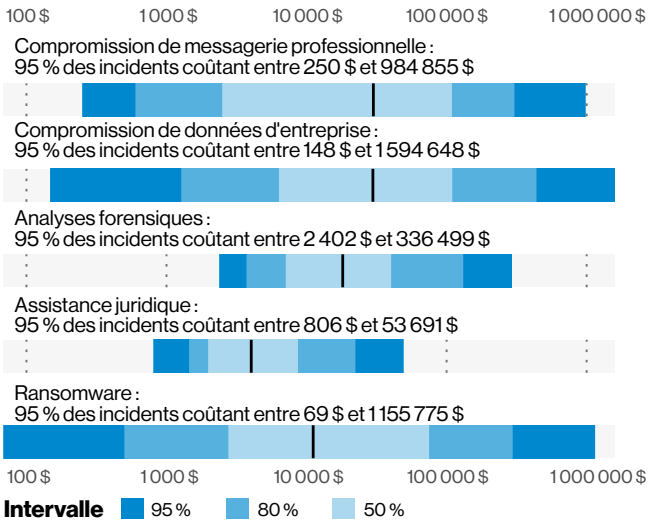
Schémas d'attaque pour les incidents (n = 5 275)



Schémas d'attaque pour les compromissions (n=29 206)



Principaux types d'actions (n=4 073)



Principaux impacts des incidents

À retenir

Les ransomwares continuent de proliférer.

Les attaques par ransomware représentent 10 % de toutes les compromissions, soit plus du double de l'année dernière. Cette forte recrudescence s'explique notamment par de nouveaux modes opératoires , avec le vol de données qui vient s'ajouter au chiffrement des resources. Le ransomware se hisse ainsi à la troisième place du classement des actions provoquant des compromissions.

Les salariés pris au piège.

85 % des compromissions impliquent le facteur humain. Le phishing se retrouve dans 36 % des compromissions observées, un taux en forte progression par rapport aux 25 % de l'an dernier. La compromission d'adresses e-mail professionnelles constitue la deuxième forme la plus courante d'ingénierie sociale, traduisant une explosion des impostures et autres usurpations d'identité, 15 fois plus nombreuses que l'an passé.

Les erreurs posent (un peu) moins problème.

Au cours des douze derniers mois, la part des compromissions imputables à des erreurs a baissé (de 22 à 17 %), bien que leur nombre ait augmenté de 883 à 905 en valeur absolue. Cette diminution est la première après trois ans de hausse ou de stagnation.

Les attaquants ont toujours un faible pour les applications web.

Les attaques d'applications web restent nombreuses. Avec plus de 80 % des compromissions, elles constituent de loin le principal vecteur d'attaque parmi les actes de hacking, le partage de bureau (RDP) se hissant au deuxième rang cette année.

Le cloud n'est pas épargné.

Les compromissions de ressources cloud externes ont dépassé celles des ressources sur site, à la fois en termes d'incidents et de compromissions. On observe en revanche un recul du nombre de terminaux utilisateurs compromis (PC fixes et portables). Cette tendance est somme toute logique dans la mesure où les attaquants se tournent de plus en plus vers l'ingénierie sociale et les applications web pour faire main basse sur des identifiants et infiltrer des messageries cloud.

C'est quoi le mot de passe ?

On ne change pas les vieilles habitudes : comme toujours, les compromissions sont principalement le fait d'attaquants externes motivés par l'appât du gain. Et le vol d'identifiants est à l'origine de 61 % d'entre elles.

Une année qu'on n'est pas près d'oublier.

En août 2020, nous prédisions que la pandémie de COVID-19 entraînerait une intensification de certains schémas : phishing, ransomware, erreurs humaines et utilisation d'identifiants volés sur les applications web. D'après le rapport DBIR 2021, nous avons vu juste pour certaines de ces prévisions : le phishing a en effet augmenté de 11 % et le ransomware de 6 %. En revanche, l'utilisation d'identifiants volés et les erreurs de publication sont restées sensiblement au même niveau que l'an dernier (+1 % et -0,5 % respectivement), tandis que la part des erreurs de configuration et d'envoi a diminué (-2 % et -6 % respectivement).

Les compromissions coûtent cher, très cher.

Cette année, nous avons tenté d'approfondir notre analyse des impacts des compromissions sur les entreprises. En nous appuyant sur différentes données (pertes de données, frais d'assurance et cours de l'action en Bourse), nous avons pu modéliser l'échelle des pertes imputables aux incidents de sécurité.

La bonne nouvelle ? 14 % des compromissions simulées n'ont eu aucun impact. Mais ne vous réjouissez pas trop vite. Le coût médian des incidents avec impact s'élevait à 21 659 $, avec 95 % des incidents provoquant des pertes allant de 826 $ à 653 587 $.

Classification des incidents

C'est en 2014 que le DBIR a commencé à classer les incidents en différentes catégories afin de refléter les scénarios les plus courants pour les entreprises. Depuis, le champ des menaces a évolué et c'est pourquoi la présente édition propose une refonte des schémas de classification DBIR.

Ces nouvelles catégories sont issues d'un processus sophistiqué de clustering par machine learning. Par rapport aux anciens schémas, elles illustrent mieux la complexité des règles d'interaction et sont davantage axées sur le déroulement complet d'une compromission. Cette refonte apporte également une plus grande précision dans les recommandations de contrôles.

Les schémas actualisés couvrent 95,8 % des compromissions analysées et 99,7 % des incidents analysés sur toute la durée concernée.

Découvrez nos principales observations pour chaque schéma d'attaque.

Ingénierie sociale	Manipulation psychologique d'une personne pour l'inciter à agir d'une certaine façon ou à enfreindre les règles de confidentialité	Les attaques par ingénierie sociale sont en plein essor depuis 2017, le nombre de compromissions de messageries professionnelles ayant encore doublé au cours des douze derniers mois. Les messageries web constituent une cible de choix. • Plus de 80 % des compromissions sont détectées par des acteurs externes • Les campagnes de phishing génèrent des taux de clics très variés, allant de 0 à plus de 50 % • Sur un échantillon de 1148 personnes ayant reçu un e-mail de phishing réel et un autre simulé, aucune n'a cliqué sur le faux contenu de phishing mais 2,5 % ont cliqué sur la menace réelle
Attaques d'applications web de base	Attaques d'applications web simples qui ne comportent que quelques étapes ou actions supplémentaires après la compromission initiale	Nous avons redéfini les contours de ce schéma afin d'y inclure les actes se cachant derrière des erreurs sur des applications web, des attaques par ingénierie sociale et des intrusions de système. Les attaques ciblent pour la plupart des serveurs cloud piratés par le biais d'identifiants volés ou des attaques par force brute. • 95 % des entreprises victimes de « credential stuffing » ont subi entre 637 et 3,3 milliards de tentatives de connexion malveillantes au cours de l'année passée • Cette année, la finance cède sa place de cible n°1 des botnets au secteur de l'information

Intrusion de système	Cette catégorie renvoie à des attaques complexes qui s'appuient sur des malwares et/ou du hacking pour parvenir à leurs fins, y compris le déploiement de ransomwares	La création de ce schéma et son classement au troisième rang des compromissions (à égalité avec les erreurs diverses et juste derrière l'ingénierie sociale et les attaques d'applications web de base) permettent de guider les entreprises dans leurs investissements en prévention des menaces avancées. • Plus de 70 % des cas dans cette catégorie impliquaient des malwares et 40 % du hacking • 99 % des cas de ransomware relevaient de cette catégorie
Erreurs diverses	Incidents dans lesquels des actes accidentels compromettent directement la sécurité d'une ressource informatique. Ce schéma ne comprend pas les pertes d'appareils, qui appartiennent à la catégorie « vol ou perte de ressources ».	En pourcentage de toutes les compromissions, la proportion des erreurs diverses a diminué, non pas parce que le nombre d'erreurs a baissé, mais en raison de l'augmentation d'autres types de compromissions. • Les erreurs de configuration constituaient de loin la forme d'erreur la plus courante (environ 52 %) • Dans la grande majorité des cas analysés, ces compromissions ont été détectées par des chercheurs en sécurité (80 %) • Les données les plus exposées dans cette catégorie sont des données personnelles
Abus de privilèges	Incidents dus principalement à l'utilisation non autorisée ou malveillante de privilèges légitimes	En pourcentage des compromissions, l'abus de privilèges continue de baisser, ce qui reflète une incidence plus faible des menaces internes par rapport à d'autres schémas. • 70 % des compromissions dans cette catégorie sont dues à un abus de privilège • Plus de 30 % de ces incidents sont découverts au bout de plusieurs mois, voire plusieurs années
Vol ou perte de ressources	Tout incident impliquant la perte accidentelle ou le vol d'une ressource informatique	Les pertes de ressources s'avèrent plus fréquentes que les vols, par ailleurs, ce type d'incident est la plupart du temps identifié par les salariés eux-mêmes. De plus en plus, les utilisateurs égarent leurs équipements plutôt que des documents ou d'autres supports.
Attaques DoS	Attaques ayant pour but de compromettre la disponibilité des réseaux et systèmes. Se rapporte aux attaques des couches réseau et applicative.	Les attaques DDoS sont distribuées de manière très inégale (distribution en pics), ce qui les rend difficiles à anticiper. Les entreprises n'ont donc pas d'autres choix que de simplement prévoir le taux d'attaques DDoS qu'elles souhaitent pouvoir contrer (50 %, 80 %, 95 % ou plus).
Autres	Cette dernière catégorie rassemble tous les incidents qui ne correspondent pas aux critères des autres schémas.	C'est ainsi que l'ancien schéma d'attaque par skimming a atterri dans ce groupement. Seuls 20 incidents de skimming (compromissions avérées) ont en effet été observés cette année. • Trois des rares compromissions attribuées à des causes environnementales ont été relevées cette année et ajoutées à cette catégorie, étant donné leur relative rareté • La refonte des schémas nous a permis de classer 18 % de compromissions en plus qui, à défaut, seraient entrées dans cette catégorie

Gros plan par secteur

Quelle que soit sa taille ou son activité, nulle entreprise n'est à l'abri d'une cyberattaque. Ce qui varie en revanche, c'est le type de menaces qui pèsent sur elle selon son secteur d'activité. Pour renforcer vos défenses et optimiser votre budget de sécurité, vous devez avoir une vision sectorielle des menaces qui vous concernent. Notre classification sectorielle repose sur les codes du Système de classification des industries de l'Amérique du Nord (SCIAN).

Hôtellerie et restauration (SCIAN 72)

Le secteur de l'hôtellerie et de la restauration est la cible d'attaques par hacking, ingénierie sociale et malware, dans sensiblement la même proportion.

Volume	69 incidents, dont 40 compromissions de données confirmées
Principaux schémas	L'intrusion de système, l'ingénierie sociale et les attaques d'applications web de base représentent 85 % des compromissions
Attaquants	Externes (90 %), internes (10 %) (compromissions)
Motivations	Financières (86 %-100 %), espionnage (0 %-14 %) (compromissions)
Données compromises	Données personnelles (51 %), identifiants (49 %), données de paiement (33 %), autres (15 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Gestion du contrôle des accès (6), Configuration sécurisée des ressources et logiciels d'entreprise (4)

Arts, divertissements et loisirs (SCIAN 71)

L'utilisation d'identifiants volés, le phishing et le ransomware restent particulièrement présents dans ces secteurs. La compromission d'informations médicales (issues d'applications de sport) a atteint un niveau exceptionnellement élevé.

Volume	7 065 incidents, dont 109 compromissions de données confirmées
Principaux schémas	L'intrusion de système, les attaques d'applications web de base et les erreurs diverses représentent 83 % des compromissions
Attaquants	Externes (70 %), internes (31 %), multiples (1 %) (compromissions)
Motivations	Financières (100 %) (compromissions)
Données compromises	Données personnelles (83 %), identifiants (32 %), médicales (26 %), autres (18 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Configuration sécurisée des ressources et logiciels d'entreprise (4), Gestion du contrôle des accès (6)

Enseignement (SCIAN 61)

Le secteur de l'enseignement doit faire face à un nombre particulièrement élevé d'attaques par ingénierie sociale, avec le Pretexting comme principal mode opératoire. Ces attaques ont généralement comme objectif le transfert frauduleux de fonds. Les erreurs diverses et intrusion de systèmes viennent compléter ce triste podium.

Volume	1332 incidents, dont 344 compromissions de données confirmées
Principaux schémas	L'ingénierie sociale, les erreurs diverses et l'intrusion de système représentent 86 % des compromissions
Attaquants	Externes (80 %), internes (20 %), multiples (1 %) (compromissions)
Motivations	Financières (96 %), espionnage (3 %), piratage récréatif (1 %), commodité (1 %), représailles (1 %) (compromissions)
Données compromises	Données personnelles (61 %), identifiants (51 %), autres (12 %), médicales (7 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Gestion du contrôle des accès (6), Configuration sécurisée des ressources et logiciels d'entreprise (4)

Finance et assurance (SCIAN 52)

Les erreurs d'envoi représentent 55 % des erreurs dans le secteur financier, qui subit par ailleurs un feu nourri de ransomwares et de vols d'identifiants de la part d'acteurs externes.

Volume	721 incidents, dont 467 compromissions de données confirmées
Principaux schémas	Les erreurs diverses, attaques d'applications web de base et l'ingénierie sociale représentent 81 % des compromissions
Attaquants	Externes (56 %), internes (44 %), multiples (1 %), partenaires (1 %) (compromissions)
Motivations	Financières (96 %), espionnage (3 %), représailles (2 %), piratage récréatif (1 %), idéologiques (1 %) (compromissions)
Données compromises	Données personnelles (83 %), bancaires (33 %), identifiants (32 %), autres (21 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Configuration sécurisée des ressources et logiciels d'entreprise (4), Gestion du contrôle des accès (6)

Santé (SCIAN 62)

Dans la continuité de ce que nous avons observé depuis déjà plusieurs années, les erreurs humaines de base restent la plaie de ce secteur. La plus fréquente étant l'erreur d'envoi (36 %) de messages électroniques ou de documents papier. En revanche, les actes de malveillance internes restent en dehors du trio de tête des compromissions, et ce pour la deuxième année consécutive. Les groupes criminels motivés par l'appât du gain en ont fait un de leurs terrains de chasse favoris, avec le déploiement de ransomwares comme mode opératoire privilégié.

Volume	655 incidents, dont 472 compromissions de données confirmées
Principaux schémas	Les erreurs diverses, attaques d'applications web de base et l'intrusion de système représentent 86 % des compromissions
Attaquants	Externes (61 %), internes (39 %) (compromissions)
Motivations	Financières (91 %), piratage récréatif (5 %), espionnage (4 %), représailles (1 %) (compromissions)
Données compromises	Données personnelles (66 %), médicales (55 %), identifiants (32 %), autres (20 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Configuration sécurisée des ressources et logiciels d'entreprise (4), Gestion du contrôle des accès (6)

Information (SCIAN 51)

Le secteur rencontre d'importants problèmes d'erreurs, notamment de configuration. Côté incidents, les attaques DoS se taillent la part du lion. Pour la première fois, la finance cède sa place de cible n°1 des botnets à l'information.

Volume	2 935 incidents, dont 381 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web de base, erreurs diverses et intrusion de systèmes représentent 83 % des compromissions
Attaquants	Externes (66 %), internes (37 %), multiples (4 %), partenaires (1 %) (compromissions)
Motivations	Financières (88 %), espionnage (9 %), représailles (2 %), commodité (1 %), piratage récréatif (1 %) (compromissions)
Données compromises	Données personnelles (70 %), identifiants (32 %), autres (27 %), internes (12 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Configuration sécurisée des ressources et logiciels d'entreprise (4), Gestion du contrôle des accès (6)

Industrie (SCIAN 31-33)

Comme dans beaucoup d'autres secteurs, les attaques par ingénierie sociale sévissent fortement dans l'industrie, marquée également par une forte hausse des compromissions par ransomware.

Volume	585 incidents, dont 270 compromissions de données confirmées
Principaux schémas	L'intrusion de système, l'ingénierie sociale et les attaques d'applications web de base représentent 82 % des compromissions
Attaquants	Externes (82 %), internes (19 %), multiples (1 %) (compromissions)
Motivations	Financières (92 %), espionnage (6 %), commodité (1 %), représailles (1 %), secondaires (1 %) (compromissions)
Données compromises	Données personnelles (66 %), identifiants (42 %), autres (36 %), de paiement (19 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Gestion du contrôle des accès (6), Configuration sécurisée des ressources et logiciels d'entreprise (4)

Exploitation minière, extraction de pétrole et de gaz (SCIAN 21), compagnies d'énergie (SCIAN 22)

Cette année, les deux secteurs ont été frappés par des attaques d'ingénierie sociale. Parmi les types de données les plus fréquemment convoités : les identifiants, données personnelles et internes. Le ransomware représente également une menace majeure pour ces branches d'industrie.

Volume	546 incidents, dont 355 compromissions de données confirmées
Principaux schémas	L'ingénierie sociale, l'intrusion de système et les attaques d'applications web de base représentent 98 % des compromissions
Attaquants	Externes (98 %), internes (2 %) (compromissions)
Motivations	Financières (78 %-100 %), espionnage (0 %-33 %) (compromissions)
Données compromises	Identifiants (94 %), données personnelles (7 %), internes (3 %), autres (3 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Gestion du contrôle des accès (6), Gestion des comptes (5)

Services professionnels, scientifiques et techniques (SCIAN 54)

L'infiltration de système et l'ingénierie sociale représentent la majorité des schémas d'attaque observés dans ce secteur. L'utilisation d'identifiants volés est monnaie courante et les salariés semblent tomber plus souvent dans le piège de l'ingénierie sociale.

Volume	1 892 incidents, dont 630 compromissions de données confirmées
Principaux schémas	L'intrusion de système, l'ingénierie sociale et les attaques d'applications web de base représentent 81 % des compromissions
Attaquants	Externes (74 %), internes (26 %) (compromissions)
Motivations	Financières (97 %), espionnage (2 %), représailles (1 %) (compromissions)
Données compromises	Identifiants (63 %), données personnelles (49 %), autres (21 %), bancaires (9 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Gestion du contrôle des accès (6), Configuration sécurisée des ressources et logiciels d'entreprise (4)

Service public (SCIAN 92)

L'ingénierie sociale constitue de loin la menace la plus importante. Dans ce secteur, les attaquants capables de créer un e-mail de phishing crédible s'emparent d'identifiants à une vitesse alarmante.

Volume	3 236 incidents, dont 885 compromissions de données confirmées
Principaux schémas	L'ingénierie sociale, les erreurs diverses et l'intrusion de système représentent 92 % des compromissions
Attaquants	Externes (83 %), internes (17 %) (compromissions)
Motivations	Financières (96 %), espionnage (4 %) (compromissions)
Données compromises	Identifiants (80 %), données personnelles (18 %), autres (6 %), médicales (4 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Gestion du contrôle des accès (6), Gestion des comptes (5)

Retail (SCIAN 44-45)

Le retail reste la cible d'attaquants à visées financières qui cherchent à tirer profit des données de paiement et informations personnelles dont les acteurs de ce secteur sont les dépositaires. Les tactiques d'ingénierie sociale comprennent des actes de pretexting et de phishing, la première catégorie se soldant généralement par des transferts d'argent frauduleux.

Volume	725 incidents, dont 165 compromissions de données confirmées
Principaux schémas	L'intrusion de système, l'ingénierie sociale et les attaques d'applications web de base représentent 77 % des compromissions
Attaquants	Externes (84 %), internes (17 %), multiples (2 %), partenaires (1 %) (compromissions)
Motivations	Financières (99 %), espionnage (1 %) (compromissions)
Données compromises	Données de paiement (42 %), personnelles (41 %), identifiants (33 %), autres (16 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (14), Configuration sécurisée des ressources et logiciels d'entreprise (4), Gestion du contrôle des accès (6)

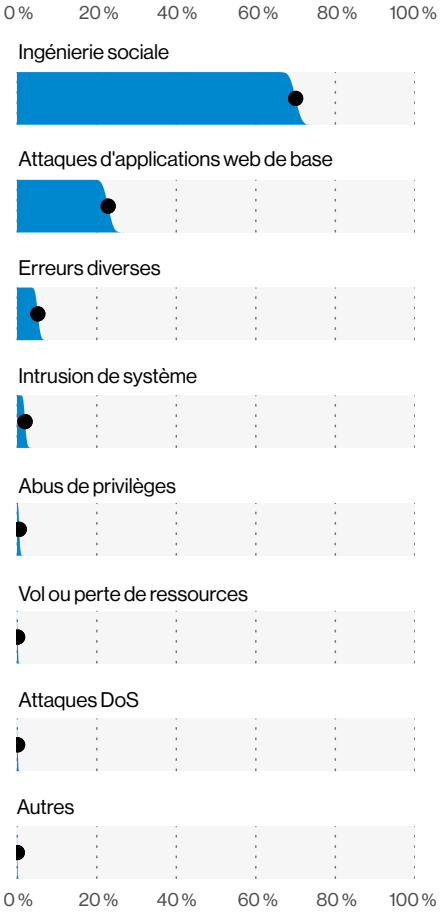
Zoom sur les PME/ETI

Cette année, l'écart s'est largement rétréci entre PME/ETI et grandes entreprises en termes de nombre de compromissions subies. On observe également un nivellement du côté des principaux schémas d'attaque. Pour la première fois depuis que nous évaluons les compromissions et incidents au regard de la taille des entreprises, nous nous trouvons face à un tableau relativement homogène. Petite ou grande, aucune entreprise n'est épargnée par le crime organisé et ses visées financières.

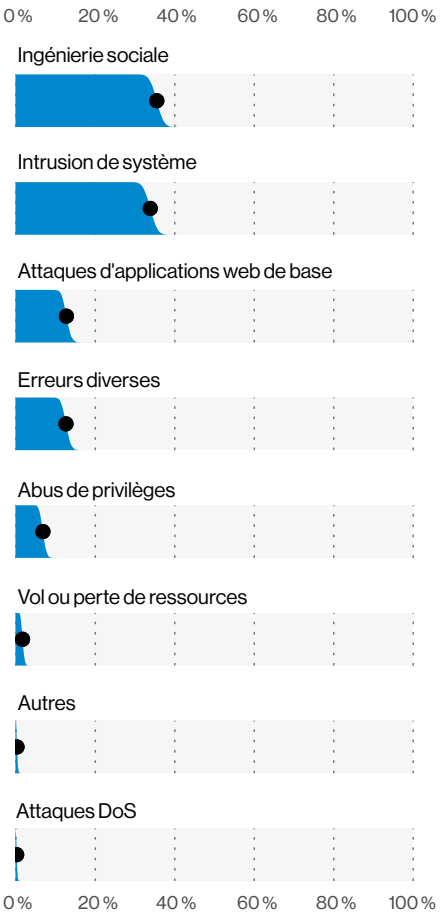
Dans notre précédente édition, les PME/ETI semblaient détecter les compromissions plus rapidement. Mais les données de cette année montrent que les grandes entreprises ont fait mieux que rattraper leur retard : elles sont parvenues à détecter les compromissions en quelques jours voire moins dans plus de la moitié des cas (55 %), contre 47 % pour les PME.

	Petite et moyenne (moins de 1 000 salariés)	Grande (plus de 1 000 salariés)
Volume	1 037 incidents, dont 263 compromissions de données confirmées	819 incidents, dont 307 compromissions de données confirmées
Principaux schémas	L'intrusion de système, les erreurs diverses et les attaques d'applications web de base représentent 80 % des compromissions	L'intrusion de système, les erreurs diverses et les attaques d'applications web de base représentent 74 % des compromissions
Attaquants	Externes (57 %), internes (44 %), multiples (1 %), partenaires (0 %) (compromissions)	Externes (64 %), internes (36 %), partenaires (1 %), multiples (1 %) (compromissions)
Motivations	Financières (93 %), espionnage (3 %), piratage récréatif (2 %), commodité (1 %), représailles (1 %), autres (1 %) (compromissions)	Financières (87 %), piratage récréatif (7 %), espionnage (5 %), commodité (2 %), représailles (2 %), secondaires (1 %) (compromissions)
Données compromises	Identifiants (44 %), données personnelles (39 %), autres (34 %), médicales (17 %) (compromissions)	Identifiants (42 %), données personnelles (38 %), autres (34 %), internes (17 %) (compromissions)

Analyse par région



Schémas de compromissions en région APAC (n=1 495)

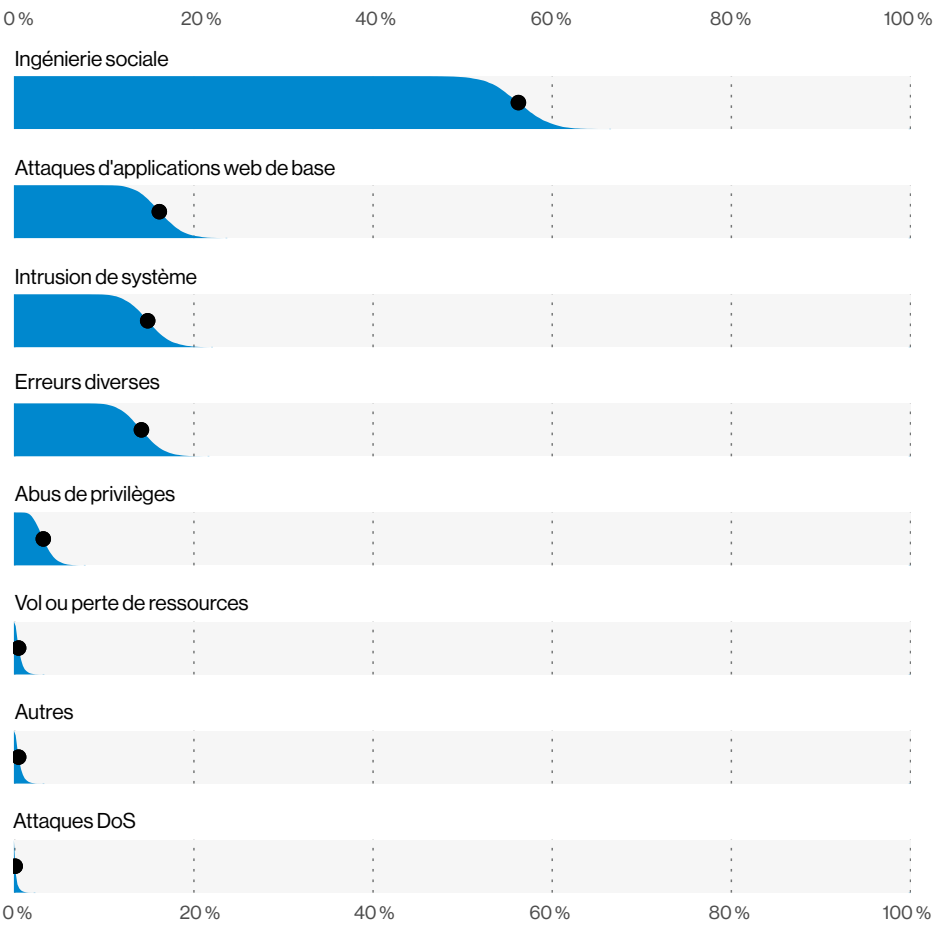


Schémas de compromissions en Amérique du Nord (n=1 080)

Attaques à visées financières en Amérique du Nord et en région APAC

Un grand nombre des compromissions relevées en Asie-Pacifique (APAC) sont perpétrées par des cybercriminels dans un but purement financier. Leurs méthodes : piéger les salariés par un e-mail de phishing pour obtenir leurs identifiants, puis accéder aux comptes de messagerie et serveurs d'applications web.

L'Amérique du Nord est également en proie aux attaquants motivés par l'appât du gain ou en quête de données faciles à revendre. Leurs outils de prédilection restent le hacking, les malwares et l'ingénierie sociale.



Schémas de compromissions en région EMEA (n=293)

Les habitués de l'EMEA presque au complet

Comme à l'accoutumée, les attaques d'applications web de base, par intrusion de systèmes et par ingénierie sociale continuent d'assaillir l'Europe, le Moyen-Orient et l'Afrique (EMEA).

Bonnes pratiques

Cette année, nous avons aligné notre nouvelle classification des schémas d'attaques sur les contrôles actualisés du CIS, l'idée étant d'aider les entreprises à identifier plus facilement les principaux contrôles à implémenter, peu importe leur taille et leur budget.

Contrôle 4 : Configuration sécurisée des ressources et logiciels d'entreprise

Outre son titre relativement long, ce contrôle comprend de nombreuses mesures qui proposent des solutions de sécurité à intégrer dès le départ et non à ajouter après coup. L'implémentation de ce contrôle permet d'activer la fonction d'effacement à distance sur les équipements mobiles afin de réduire les compromissions dues à des erreurs, notamment de configuration, et à des pertes d'appareils.

Contrôle 5 : Gestion des comptes

Techniquement parlant, ce contrôle de la nouvelle version 8 du CIS est nouveau mais il devrait vous être familiers car ses sous-contrôles regroupent les précédentes pratiques de gestion des comptes préconisées dans les anciens contrôles (tels que « Protection périmétrique » et « Surveillance et contrôle des comptes »). Ce contrôle a pour principal objectif d'aider les entreprises à gérer les accès aux comptes et s'avère efficace contre les attaques par force brute et de « credential stuffing ».

Contrôle 6 : Contrôle des accès

Ce contrôle est directement lié au contrôle 5. Au lieu de simplement gérer les accès aux comptes utilisateurs, vous en configurez également les droits et privilèges. Cela passe notamment par l'implémentation de l'authentification multifacteur pour l'accès à des zones sensibles de l'environnement, une arme essentielle contre l'utilisation d'identifiants volés.

Contrôle 14 : Programme de sensibilisation et de formation à la sécurité

Ce contrôle est un grand classique et son intitulé suffit à le décrire. Étant donnée la prédominance des erreurs et attaques par ingénierie sociale, il semble judicieux d'investir dans la sensibilisation et la formation technique des équipes pour les aider à évoluer dans un environnement semé d'embûches.

S'informer, c'est se préparer.

Pour faire face aux cybermenaces actuelles, vous devez pouvoir compter sur une information fiable. Le rapport DBIR vous présente des données réelles sur les acteurs, tendances et modes opératoires qui pèsent sur votre activité pour vous aider à mieux vous protéger et sensibiliser vos salariés. Bénéficiez de tous les éclairages concrets dont vous avez besoin pour sécuriser votre entreprise.

Lisez le rapport DBIR 2021

Vous aussi, vous voulez œuvrer pour un monde digital plus sûr ?

Le DBIR s'appuie sur la contribution de dizaines d'entreprises. Pourquoi ne pas apporter votre pierre à l'édifice ? Apportez votre contribution au rapport 2022 ou faites-nous part de vos commentaires afin de nous aider à améliorer la prochaine édition. Écrivez-nous à dbir@verizon.com, contactez-nous par twitter à @VZDBIR et consultez la page VERIS GitHub : https://github.com/vz-risk/veris.

verizon