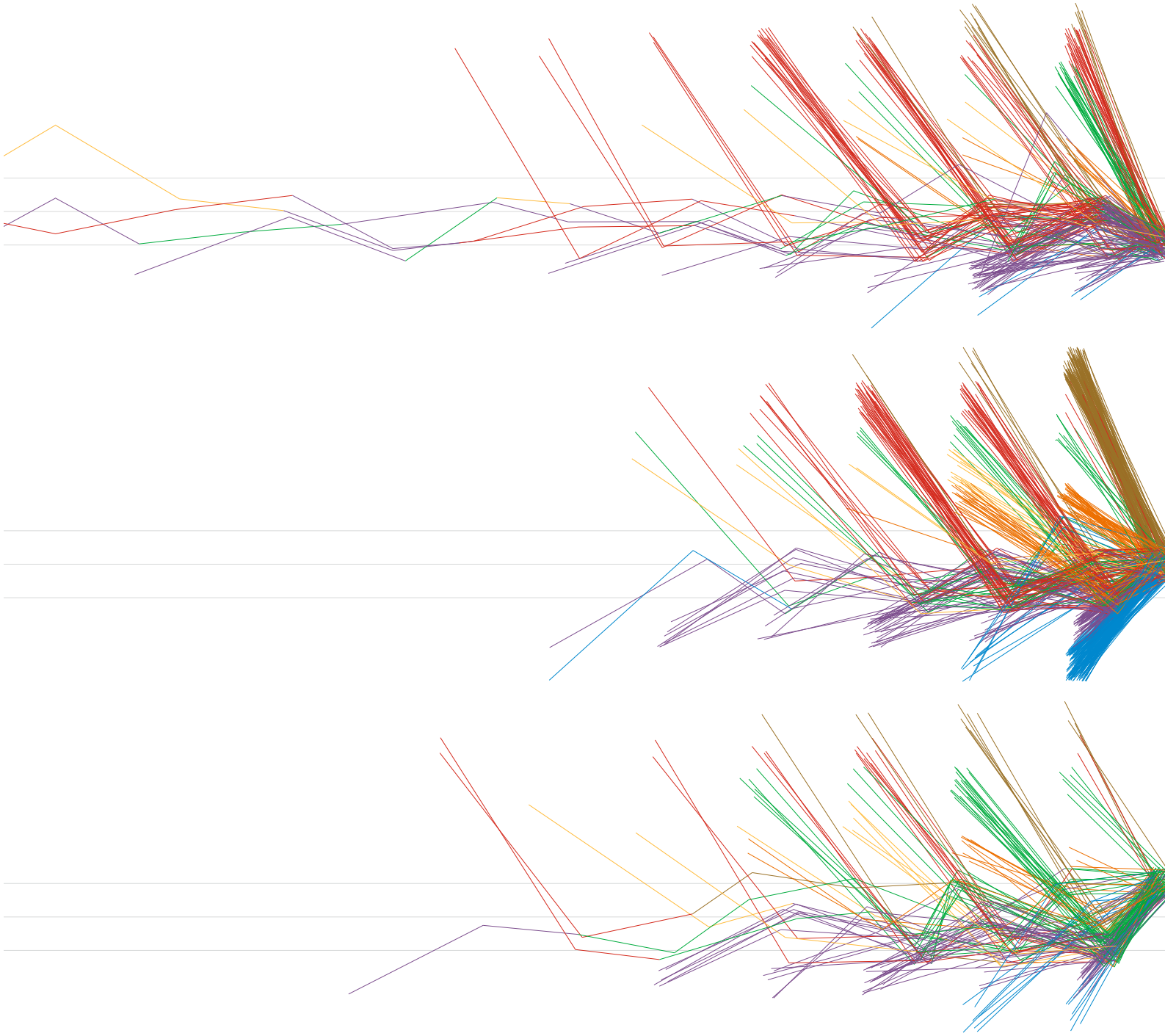
Synthèse

Rapport d'enquête 2019 sur les compromissions de données



verizon

Le rapport d'enquête 2019 sur les compromissions de données (DBIR) de Verizon vous offre une vision stratégique des menaces auxquelles les organisations comme la vôtre doivent faire face. La 12ème édition du rapport DBIR s'appuie sur les données réelles de 41 686 incidents de sécurité et 2 013 compromissions de données émanant de 73 sources des secteurs publics et privés et couvrant 86 pays différents.

Qui se cache derrière ces attaques ?

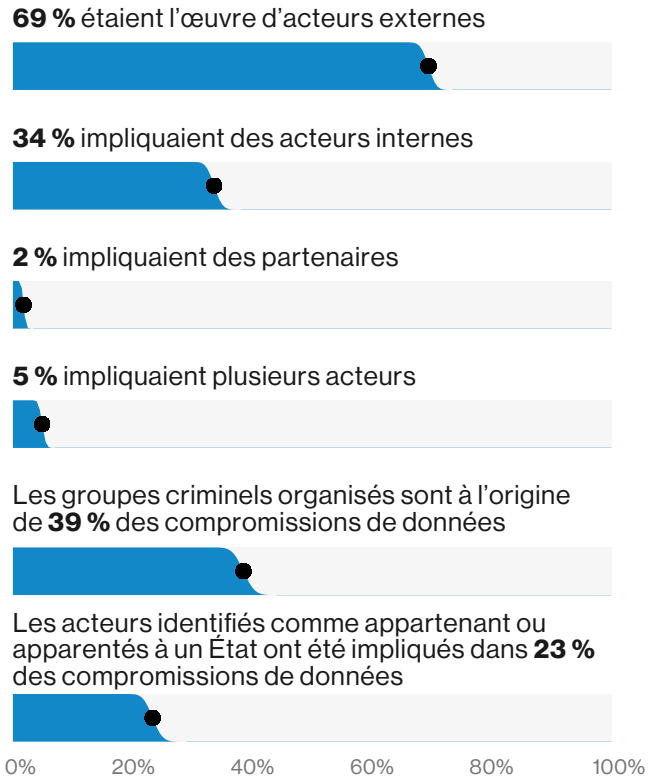


Figure 4. Qui sont les auteurs des compromissions de données ?

Quelles sont les tactiques utilisées ?

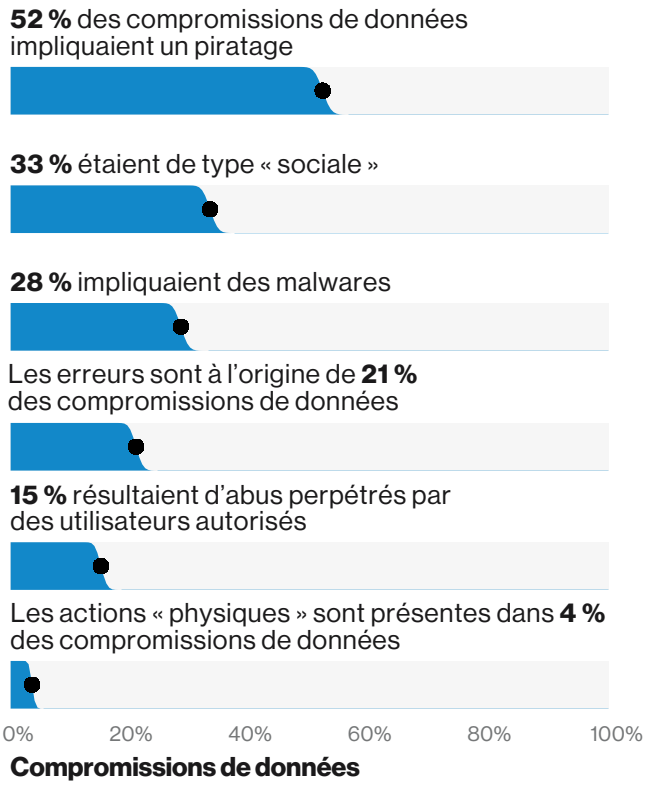


Figure 3. Quelles sont les tactiques employées ?

Qui sont les victimes des compromissions de données ?

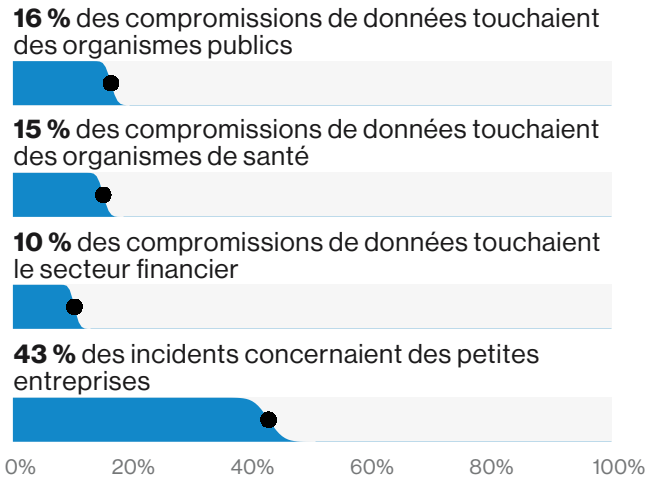


Figure 2. Qui sont les victimes ?

Les compromissions de données font toujours les gros titres du monde entier. Quels que soient les stratagèmes de défense déployés par les professionnels de la sécurité, les hackers semblent toujours trouver une parade pour les contourner. Aucune entreprise, quels que soient sa taille ou son secteur d'activité, n'est à l'abri d'une attaque. Peu importe le type ou la quantité des données de votre entreprise, elles représentent une cible. Une meilleure compréhension des menaces auxquelles vous et vos pairs faites face, de leur évolution au fil du temps et des tactiques les plus susceptibles d'être utilisées peut vous préparer à gérer plus efficacement ces risques.

Points clés à retenir

Les dirigeants en ligne de mire
Les cadres supérieurs étaient douze fois plus susceptibles d'être la cible d'incidents d'ingénierie sociale et neuf fois plus susceptibles d'être la cible de compromissions de données sociales qu'auparavant. Les chiffres de ce rapport illustrent parfaitement la croissance des attaques d'ingénierie sociale avec intérêt financier : les incidents de sécurité et les compromissions de données impliquant des dirigeants sont passés de quelques cas à plusieurs dizaines.

Le cloud n'est pas épargné
Les entreprises se tournent de plus en plus vers le cloud par souci de rentabilité entraînant une migration de leurs e-mails et autres données précieuses vers le cloud. Les criminels ne font que changer de cible et adapter leurs stratégies pour localiser et voler les données les plus utiles à leurs yeux. On constate donc une augmentation proportionnelle du nombre de piratages de serveurs e-mail cloud à l'aide d'identifiants usurpés. Pour autant, cela ne signifie pas que les services cloud sont moins sûrs. Il apparaît simplement que les attaques de phishing, les vols d'identifiants et les erreurs de configuration sont des effets de bord inhérents à ce processus.

Le piège des applications web
En matière de paiement par carte, les compromissions concernant les applications web sont en voie de dépasser celles des terminaux physiques. D'après les données de l'un de nos contributeurs, la National Cyber-Forensics and Training Alliance (NCFTA), cette mutation a déjà eu lieu et l'ensemble de nos données confirme cette tendance.

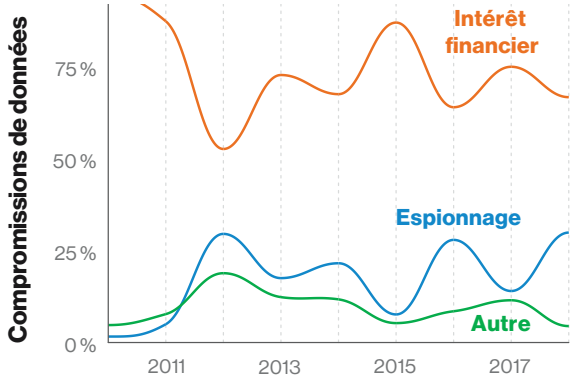


Figure 7. Évolution des motivations des auteurs de compromissions de données

Lorsqu'un mobile est connu ou valable, l'appât du gain est le moteur le plus courant des compromissions de données dans 71 % des cas. Pour sa part, l'espionnage motive 25 % des compromissions de données.

Le ransomware toujours vaillant
Le ransomware continue de faire des ravages et représente près de 24 % des incidents impliquant des malwares. Il s'est tellement répandu qu'il fait moins souvent la une des médias spécialisés, sauf si une cible prestigieuse est visée. Pourtant, cette menace reste sérieuse pour tous les secteurs. En revanche, d'autres menaces, comme le « cryptomining » (2 % des malwares), font fréquemment les gros titres alors qu'elles n'apparaissent que très peu dans nos données.

Puce et PIN : l'arme fatale ?
En matière d'infractions liées aux cartes de paiement, le nombre de compromissions de terminaux physiques est en baisse par rapport à celles des applications web. Ce déclin pourrait en partie s'expliquer par les premiers effets de la mise en œuvre technologique de paiements par carte à puce avec code PIN.

Riposte des RH
Il est intéressant de noter que les attaques contre le personnel des ressources humaines ont diminué par rapport à l'an dernier. Nos données indiquent en effet que ces effectifs a été 6 fois moins touché cette année que l'an dernier. Cette constatation est liée à la disparition quasi totale des escroqueries aux formulaires fiscaux W-2 aux Etats-Unis des données du DBIR.

Je clique donc je suis
Le taux de clics enregistré durant les campagnes de phishing simulé de nos partenaires est passé de 24 % à 3 % au cours des sept dernières années. Toutefois, 18 % des personnes ayant cliqué sur les liens de test de phishing l'ont fait sur des appareils mobiles. Les études montrent en effet que les utilisateurs de smartphones sont plus vulnérables au phishing, probablement en raison de leurs interfaces utilisateur et d'autres facteurs. Il en va de même pour les e-mails de harponnage ou « spear phishing » et les attaques sur les médias sociaux.

Quelles menaces pèsent sur votre secteur ?
Tous les types d'organisations sont des victimes potentielles. Certains secteurs sont toutefois plus exposés à certains types d'attaques. Cela est dû à une multitude de facteurs comme leur modèle économique, le type de données transmises et stockées, la clientèle et même les différentes technologies nécessaires à la sécurité de leur environnement. Être en mesure de localiser les points d'attaque les plus probables permet d'optimiser ses ressources et d'orienter l'allocation de son budget. Beaucoup de lecteurs du DBIR consultent directement les rubriques de leur secteur d'activité pour comprendre les menaces auxquelles eux-mêmes et leurs pairs sont confrontés. Toutefois, un tour d'horizon des autres secteurs peut également être très instructif.

Notre rapport DBIR 2019 présente une étude approfondie des différents secteurs d'activité et de la spécificité des menaces, motivations et adversaires auxquels ils ont à faire face.

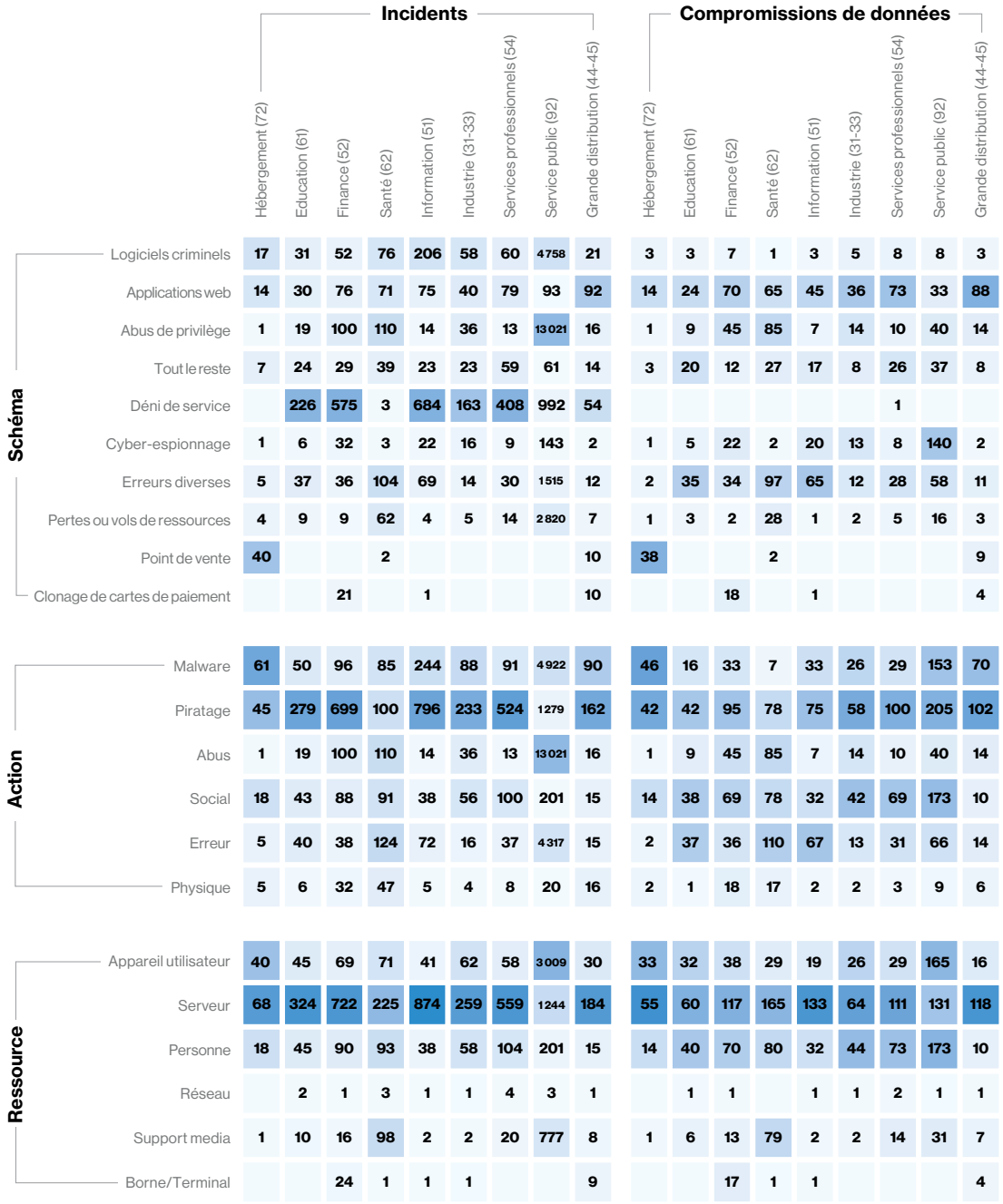


Figure 39. Comparaison sectorielle
(à gauche : tous les incidents de sécurité,
à droite : compromissions de données uniquement)

Hébergement et restauration

Nos données révèlent une baisse du nombre total de compromissions par rapport à l'an dernier ; ce phénomène serait principalement dû à l'absence d'incident au niveau des fournisseurs de POS ayant pu autrefois compromettre nombre d'organisations suite au vol d'identifiants de partenaires.

Fréquence	87 incidents, dont 61 avec divulgation confirmée des données
Top 3 des schémas	Intrusions sur les points de vente, applications web et logiciels criminels sont à l'origine de 93 % de toutes les compromissions de données du secteur de l'hébergement.
Acteurs concernés	Externes (95 %), internes (5 %) (compromissions de données)
Motivations	Intérêt financier (100 %) (compromissions de données)
Données compromises	Paiement (77 %), identifiants (25 %), internes (19 %) (compromissions de données)

Education

L'éducation continue d'être la proie d'erreurs, de l'ingénierie sociale et d'une mauvaise sécurisation des identifiants d'accès aux e-mails. Les attaques DoS représentent en effet plus de la moitié de tous les incidents frappant ce secteur.

Fréquence	382 incidents, dont 99 avec divulgation confirmée des données
Top 3 des schémas	Erreurs diverses, attaques des applications web et tout le reste sont à l'origine de 80 % des compromissions de données
Acteurs concernés	Externes (57 %), internes (45 %), multiples (2 %) (compromissions de données)
Motivations	Intérêt financier (80 %), espionnage (11 %), divertissement (4 %), représailles (2 %), idéologie (2 %) (compromissions de données)
Données compromises	À caractère personnel (55 %), identifiants (53 %) et internes (35 %) (compromissions de données)

Banque et assurance

Le déni de service et l'utilisation d'identifiants usurpés restent monnaie courante avec les applications bancaires. Les comptes e-mail compromis sont facilement identifiables une fois que les personnes attaquées sont filtrées. Le nombre de piratages de distributeurs automatiques (skimming) poursuit son déclin.

Fréquence	927 incidents, dont 207 avec divulgation confirmée des données
Top 3 des schémas	Applications web, abus de privilèges et erreurs diverses sont à l'origine de 72 % des compromissions de données
Acteurs concernés	Externes (72 %), internes (36 %), multiples (10 %), partenaires (2 %) (compromissions de données)
Motivations	Intérêt financier (88 %), espionnage (10 %) (compromissions de données)
Données compromises	À caractère personnel (43 %), identifiants (38 %), internes (38 %) (compromissions de données)

Santé

Le secteur de la santé est un cas à part : la majorité des compromissions de données est en effet liée à des acteurs internes. Si les attaques par déni de service sont rares, la disponibilité des services est mise à mal par des ransomwares.

Fréquence	466 incidents, dont 304 avec divulgation confirmée des données
Top 3 des schémas	Erreurs diverses, abus de privilèges et applications web sont à l'origine de 81 % des compromissions de données
Acteurs concernés	Internes (59 %), externes (42 %), partenaires (4 %) et responsabilité multiple (3 %) (compromissions de données)
Motivations	Intérêt financier (83 %), divertissement (6 %), commodité (3 %), représailles (3 %) et espionnage (2 %) (compromissions de données)
Données compromises	Médicales (72 %), à caractère personnel (34 %), identifiants (25 %) (compromissions de données)

Information

Les applications web sont la cible d'attaques visant leur disponibilité et constituent une voie d'accès aux comptes e-mail cloud des entreprises.

Fréquence	1094 incidents dont 155 avec divulgation confirmée des données
Top 3 des schémas	Erreurs diverses, applications web et cyber-espionnage sont à l'origine de 83 % des compromissions de données dans le domaine de l'information
Acteurs concernés	Externes (56 %), internes (44 %), partenaires (2 %) (compromissions de données)
Motivations	Intérêt financier (67 %), espionnage (29 %) (compromissions de données)
Données compromises	À caractère personnel (47 %), identifiants (34 %), secrets (22 %) (compromissions de données)

Industrie

Le secteur industriel a enregistré une augmentation du nombre de compromissions de données motivées par des raisons financières au cours des deux dernières années, mais l'espionnage reste un motif prédominant. La plupart des compromissions de données passent par du phishing et le vol d'identifiants.

Fréquence	352 incidents dont 87 avec divulgation confirmée des données
Top 3 des schémas	Applications web, abus de privilèges et cyber-espionnage sont à l'origine de 71 % des compromissions de données
Acteurs concernés	Externes (75 %), internes (30 %), multiples (6 %), partenaires (1 %) (compromissions de données)
Motivations	Intérêt financier (68 %), espionnage (27 %), représailles (3 %), divertissement (2 %) (compromissions de données)
Données compromises	Identifiants (49 %), internes (41 %), secrets (36 %) (compromissions de données)

Services professionnels, scientifiques et techniques

Le phishing et le vol d'identifiants liés aux comptes e-mail cloud tiennent désormais le haut du pavé.

Fréquence	670 incidents dont 157 avec divulgation confirmée des données
Top 3 de schémas	Applications web, tout le reste et erreurs diverses sont à l'origine de 81 % des compromissions de données du secteur des services professionnels
Acteurs concernés	Externes (77 %), internes (21 %), partenaires (5 %), multiples (3 %) (compromissions de données)
Motivations	Intérêt financier (88 %), espionnage (14 %), commodité (2 %) (compromissions de données)
Données compromises	Identifiants (50 %), internes (50 %), à caractère personnel (46 %) (compromissions de données)

Administration publique

Le cyber-espionnage est un mal endémique du secteur public : les acteurs apparentés à des États sont en effet responsables de 79 % de toutes les compromissions de données impliquant des acteurs externes. Les abus de privilèges et les erreurs internes constituent 30 % des compromissions de données.

Fréquence	23 399 incidents dont 330 avec divulgation confirmée des données
Top 3 des schémas	Cyber-espionnage, erreurs diverses et abus de privilèges sont à l'origine de 72 % des compromissions de données
Acteurs concernés	Externes (75 %), internes (30 %), partenaires (1 %), multiples (6 %) (compromissions de données)
Motivations	Espionnage (66 %), intérêt financier (29 %), autres (2 %) (compromissions de données)
Données compromises	Internes (68 %), à caractère personnel (22 %), identifiants (12 %) (compromissions de données)

Grande distribution

Le nombre d'infractions sur présentation de cartes aux points de vente ou de piratages de pompes à essence continue de diminuer. Les attaques sur les applications de paiement en ligne aiguisent en effet les appétits financiers des acteurs de ce secteur.

Fréquence	234 incidents dont 139 avec divulgation confirmée des données
Top 3 des schémas	Applications web, abus de privilèges et erreurs diverses sont à l'origine de 81 % des compromissions de données
Acteurs concernés	Externes (81 %), internes (19 %) (compromissions de données)
Motivations	Intérêt financier (97 %), divertissement (2 %), espionnage (2 %) (compromissions de données)
Données compromises	Paiement (64 %), identifiants (20 %), à caractère personnel (16 %) (compromissions de données)

Renforcez votre sécurité en misant sur des informations concrètes et exploitables

Face à l'évolution constante des menaces de sécurité et des hackers, les professionnels de la sécurité de l'information peuvent se sentir dépassés par l'ampleur de la tâche. Mais les professionnels de la sécurité et les dirigeants d'entreprise ont à leur disposition de puissants outils pour lutter efficacement contre les acteurs malveillants.

La connaissance est la meilleure des défenses. En améliorant la perspective, l'analyse et la compréhension des menaces qui pèsent sur elles, les entreprises peuvent prendre des mesures cruciales pour les maîtriser. Le rapport DBIR tient un rôle central dans l'actualisation des connaissances. Depuis 2014, nous avons identifié neuf schémas d'incidents couvrant la majorité des incidents et des compromissions de données. Les connaître peut vous aider à adapter vos mesures de sécurité et à utiliser votre budget pour faire face aux menaces probables.

> **98 % des incidents de sécurité et 88 % des compromissions de données s'inscrivent encore dans l'un des neuf schémas.**

Les enjeux sont de taille : les données, les clients, les informations confidentielles et les secrets commerciaux des entreprises sont exposés aux attaques. Les compromissions de données continuent de menacer la réputation et la santé financière des organisations. Mais les professionnels de la sécurité ont le pouvoir de répondre à ces défis.

Consultez le DBIR 2019 pour obtenir toutes les précisions utiles, y compris les schémas d'attaques par secteur d'industrie.

> **Mesurer les pertes**
>
> **Cette année, l'Internet Crime Compliant Center (IC3) du FBI a contribué au DBIR avec les rapports sur les Business Email Compromise (BEC) et les Computer Data Breach (CDB). Les pertes directes médianes occasionnées par les acteurs malveillants s'élèvent à environ 8 000 $ pour les Computer Data Breach (CDB) et 25 000 $ pour les Business Email Compromise (BEC).**
>
> **Ils travaillent dur mais c'est payant**
>
> **De plus, l'intervention de la Recovery Asset Team de l'IC3, en collaboration avec la banque destinataire, a permis à la moitié de toutes les victimes de BEC aux États-Unis de récupérer ou de bloquer 99 % des fonds dérobés, ne laissant que 9 % des victimes avec une perte totale.**

Quelques bonnes pratiques de prévention

Faites le ménage.
De nombreuses compromissions de données sont le résultat d'une mauvaise hygiène de sécurité et d'un manque d'attention accordée aux principes de sécurité. Supprimez les erreurs humaines autant que possible puis fixez un référentiel de sécurité portant sur les ressources en contact avec Internet comme les serveurs web et les services cloud.

Veillez sur l'intégrité.
Les compromissions touchant les applications web utilisent aujourd'hui des codes capables de capturer les données saisies dans les formulaires web. Pensez à la supervision de l'intégrité des fichiers pour les sites de paiement en plus des correctifs des systèmes d'exploitation et des applications de paiement.

Redoublez d'efforts.
2FA systématiquement. Faites appel à l'authentification forte pour les applications clientes, les accès à distance et les comptes e-mail cloud. Certes il y a des exemples de vulnérabilité du 2FA mais ils ne justifient en rien de ne pas le mettre en œuvre.

Méfiez-vous des menaces internes.
Surveillez les comportements internes en contrôlant et en consignant les accès aux données sensibles. Expliquez clairement au personnel votre grande capacité à identifier les transactions frauduleuses.

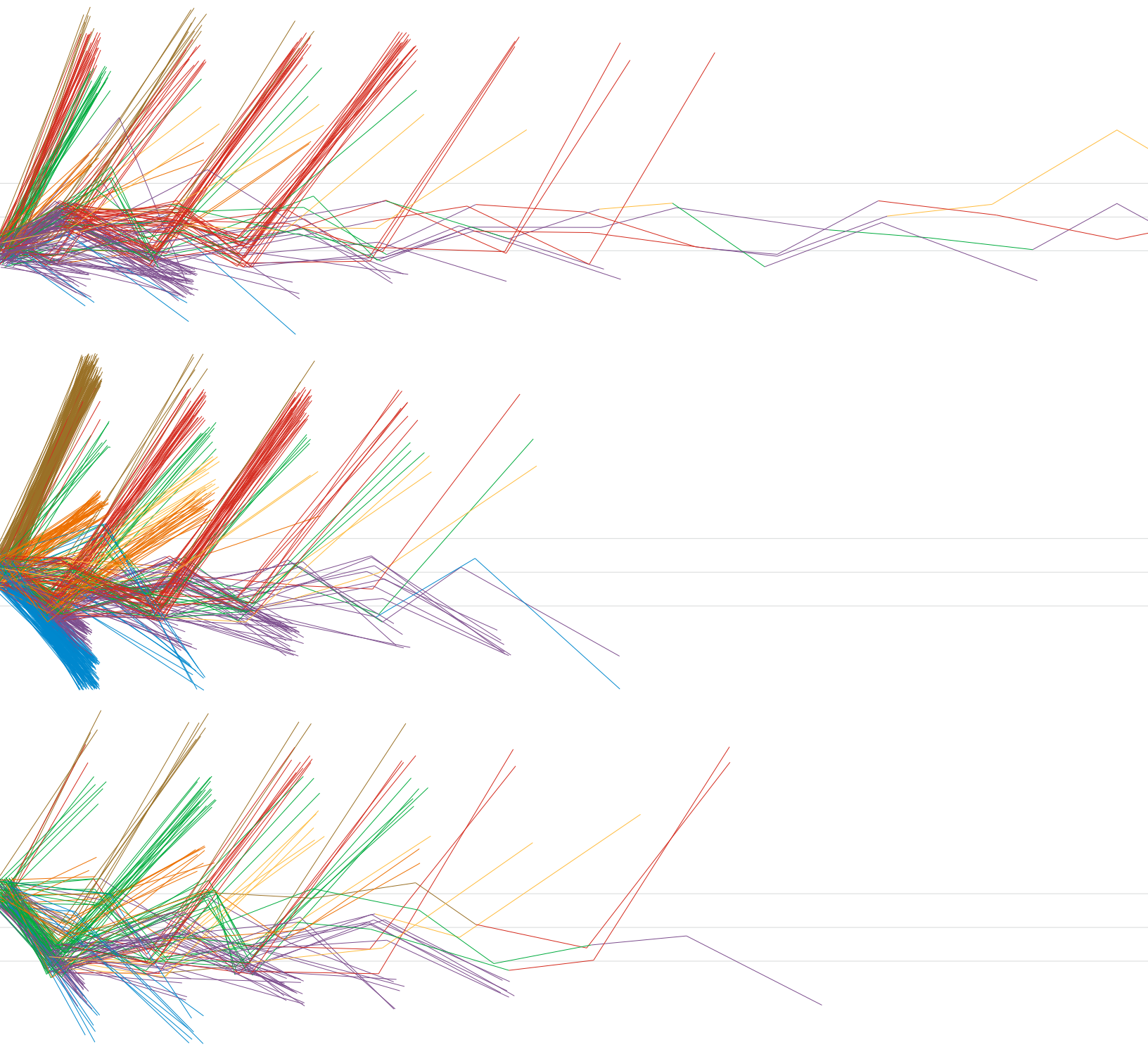
Filtrez les paquets de données.
La protection contre le déni de service distribué (DDoS) est indispensable dans de nombreux secteurs d'activité. Protégez-vous des interruptions intempestives grâce à un contrôle continu et au Capacity Planning qui permettent de gérer les pics de trafic.

Restez conscients « socialement ».
Les attaques d'ingénierie sociale sont très efficaces pour s'emparer d'identifiants. Contrôlez les e-mails contenant des liens et des exécutables. Donnez à vos équipes les moyens de signaler des tentatives de Phishing ou de Pretexting.

Le rapport d'enquête 2019 sur les compromissions de données de Verizon offre aux professionnels de la sécurité et aux dirigeants d'entreprise du monde entier un aperçu complet du paysage de la cybercriminalité. Il leur présente comment les menaces évoluent et les recommandations les plus récentes pour maîtriser ces risques.
Le rapport 2019 s'appuie sur une analyse précise de 41 686 incidents de sécurité, dont 2 013 compromissions de données confirmées. Présenté cette année dans sa 12e édition, le DBIR est reconnu comme l'une des sources d'informations et de données les plus respectées du secteur de la sécurité.

Téléchargez le rapport complet :
enterprise.verizon.com/DBIR2019/

Synthèse du rapport d'enquête 2019 sur les compromissions de données



verizon