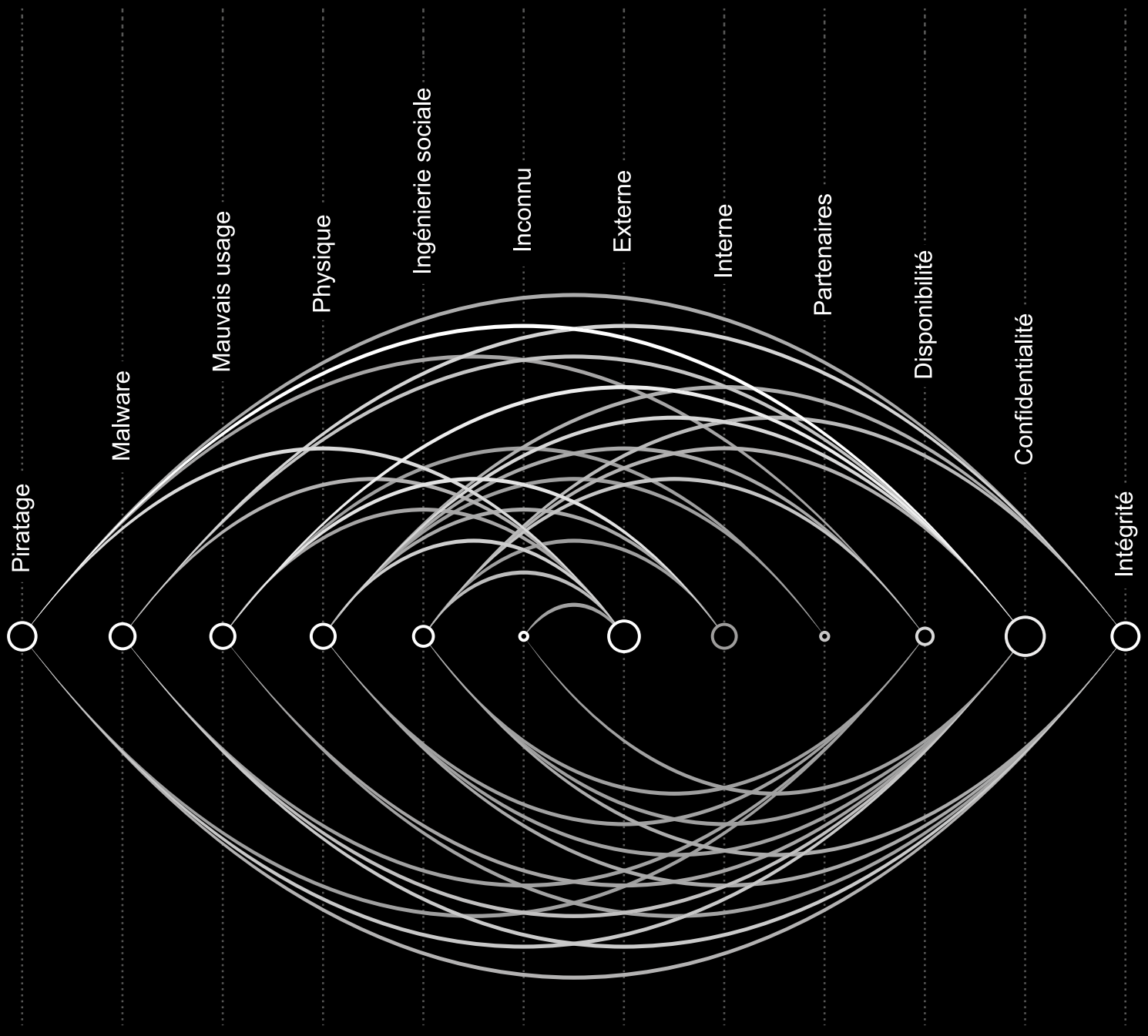
DBIR 2018

Document de synthèse

Rapport d'enquête sur les compromissions de données



verizon

verizon

La sécurité de votre entreprise est entre vos mains.

Les compromissions de données ne concernent pas seulement les équipes de sécurité. Et pour cause, leurs répercussions se font sentir à tous les niveaux : des salariés, privés de leurs outils, jusqu'aux juristes d'entreprise chargés de rendre des comptes devant les tribunaux. Désormais, tous les acteurs de l'entreprise doivent s'impliquer dans la gestion du risque. Mais encore faut-il bien cerner la nature des menaces.

Pour exploiter tout le potentiel de l'innovation digitale, votre entreprise doit pouvoir compter sur une sécurité fiable. C'est pourquoi nous publions chaque année un Rapport d'enquête sur les compromissions de données (DBIR), dont la 11e édition vient de paraître. Comme ses prédécesseurs, ce nouveau rapport se base sur l'analyse de milliers de cas réels, soit plus de 53.000 incidents et 2 216 compromissions avérées pour être exact.

53 308 incidents, 2 216 compromissions, 67 contributeurs, 65 pays.

Cette année encore, les cybercriminels n'ont eu qu'à répéter les bonnes vieilles méthodes car les victimes ont répété les mêmes erreurs.

Pour vous guider sur la voie d'une sécurité renforcée, nous avons dépeint les différents profils des attaquants, de leurs motivations et des tactiques mises en œuvre. Suivez le guide.

Un jour, ce sera votre tour

La plupart des cybercriminels sont attirés par l'appât du gain. Vol de données de cartes bancaires, données personnelles, propriété intellectuelle… s'il y a de l'argent à gagner, soyez sûr qu'ils tenteront leur chance.

Et ils frappent sans discernement. Oubliez cette idée reçue qui voudrait que seules les plus grandes firmes internationales sont visées. En réalité, la plupart des attaques sont opportunistes et visent les entreprises les moins bien préparées – et non les plus riches ou les plus connues.

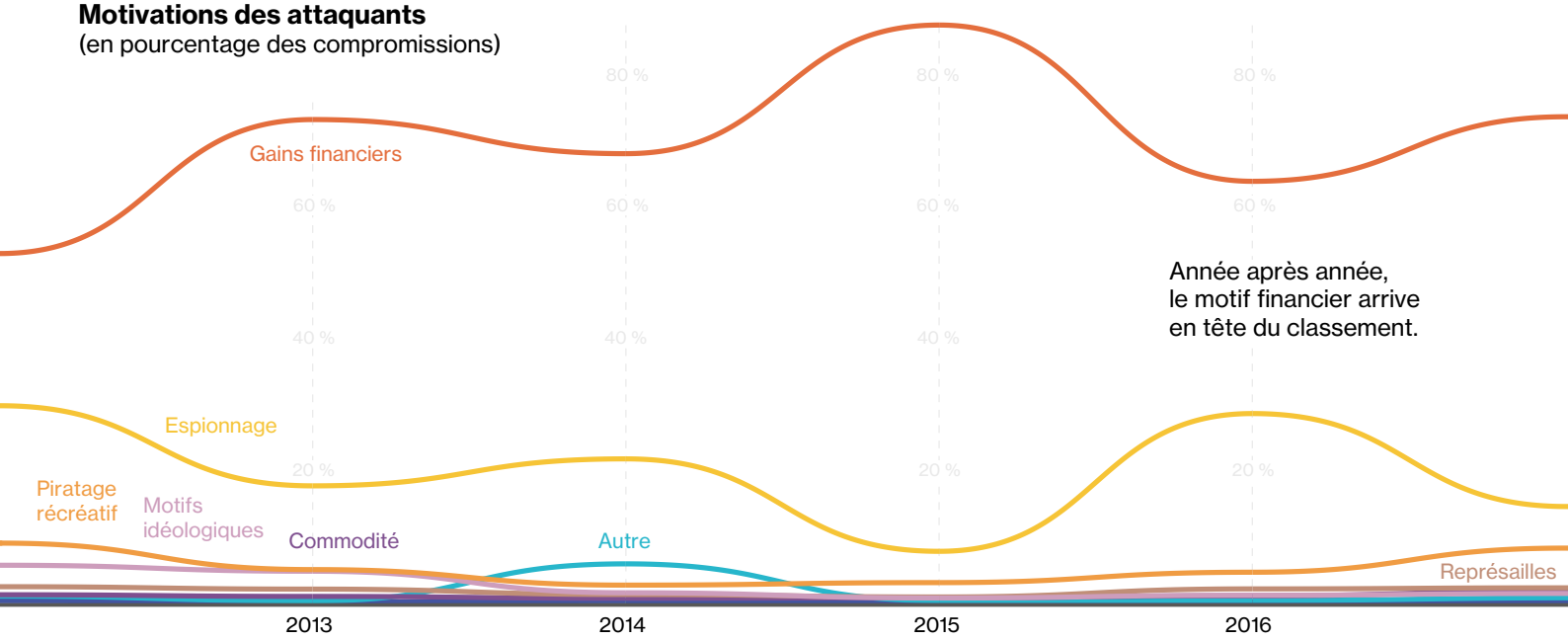
76 % des compromissions étaient motivées par l'appât du gain.

Qui sont vos adversaires ?

Cette année, 73 % des cyberattaques ont été perpétrées par des individus externes à l'entreprise. Parmi l'ensemble des compromissions, la moitié étaient le fait de groupes criminels organisés. Les acteurs en lien avec des États étaient quant à eux impliqués dans 12 % d'entre elles.

Pourtant, la menace n'est pas seulement externe puisque dans 28 % des cas, elle vient de l'intérieur. Une menace d'autant plus insidieuse qu'il est extrêmement difficile d'identifier les abus de privilèges commis par les utilisateurs.

Motivations des attaquants
(en pourcentage des compromissions)



verizon

L'erreur est humaine

En interne, la menace ne vient pas seulement de vos salariés les moins scrupuleux. Règles de confidentialité non respectées, envois d'e-mails aux mauvais destinataires, serveurs mal configurés… l'erreur humaine est en fait à l'origine de 17 % des compromissions. Mais son caractère accidentel ne modifie en rien leur impact financier.

Campagnes de phishing : 4 % des utilisateurs piégés

Voilà maintenant trois ans que nous soulignons l'ampleur des dommages occasionnés par le phishing. Malheureusement, force est de constater que ces campagnes fonctionnent toujours aussi bien. Sur l'ensemble de l'année, 78 % des salariés n'ont cliqué sur aucun lien malveillant. C'est bien, mais 4 % des utilisateurs continuent de se faire piéger à la première campagne venue. Fait plus inquiétant encore : plus un individu a tendance à cliquer, plus il est susceptible de répéter son erreur à l'avenir.

Vous avez 16 minutes avant qu'une campagne de phishing ne fasse une première victime. Quant aux utilisateurs les plus perspicaces, ils ne donneront pas l'alerte avant 28 minutes.

Gare au chantage

Pour s'enrichir, les cybercriminels n'ont pas forcément besoin d'exfiltrer des données. Ils peuvent tout simplement vous empêcher de les utiliser. Dans l'édition 2013 du DBIR, nous documentions pour la première fois les ravages des rançongiciels, ou ransomwares. Cette année, ils représentent la catégorie prédominante des malwares connus.

Avec 39 % de part totale, les ransomwares représentent la première catégorie de malwares identifiés.

Les ransomwares doivent leur essor fulgurant à deux grands facteurs : leur efficacité et leur simplicité de déploiement. Dorénavant, même un pirate en herbe peut se procurer des kits d'attaques prêts à l'emploi pour créer et déployer des ransomwares en à peine quelques minutes. Outre un coût et un risque minimes, le retour sur investissement est immédiat, contrairement au vol de données dont la revente donne lieu à des tractations.

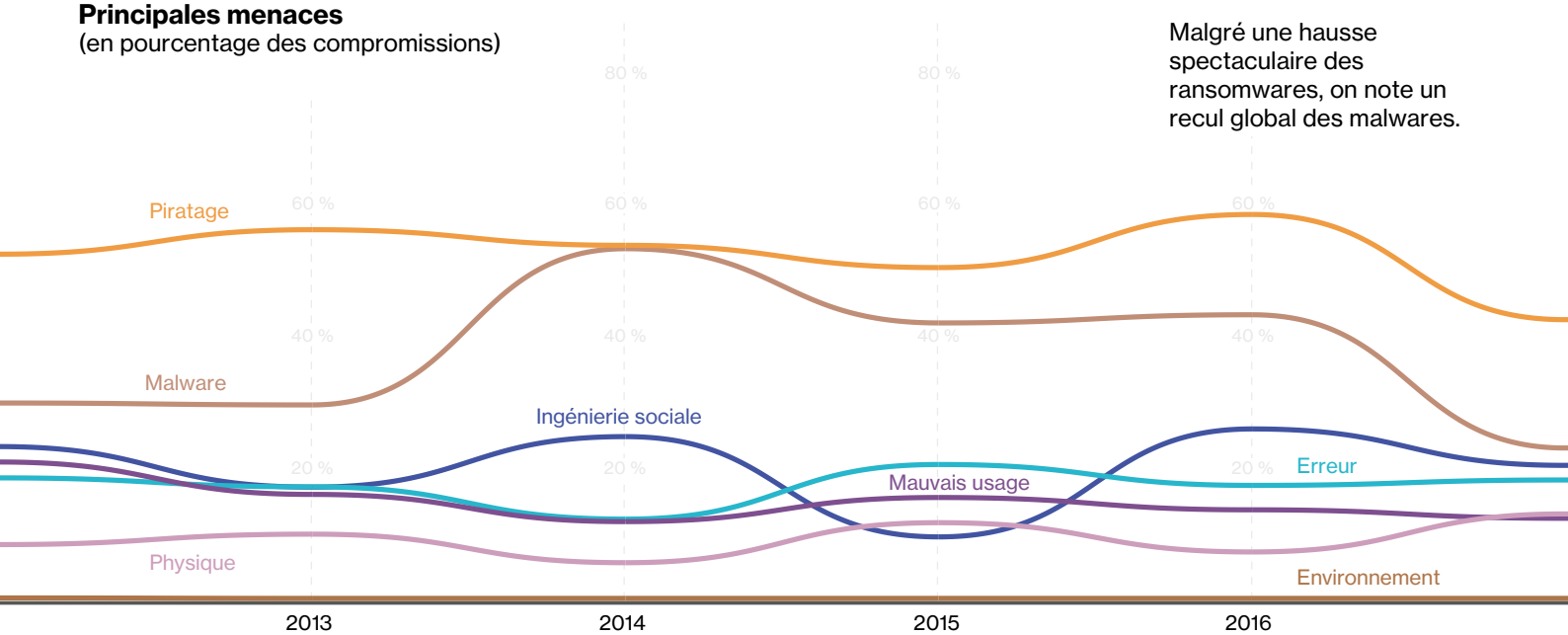
Les cybercriminels s'intéressent de moins en moins aux terminaux d'utilisateurs individuels. Ils savent en effet qu'ils ont beaucoup plus à gagner du cryptage d'un serveur de fichiers ou d'une base de données. Sans un système de sauvegarde efficace, votre entreprise pourrait vite se retrouver paralysée.

Ce que vous pouvez faire

Découvrez les principales menaces pour votre secteur.

Principales menaces
(en pourcentage des compromissions)

Malgré une hausse spectaculaire des ransomwares, on note un recul global des malwares.



verizon

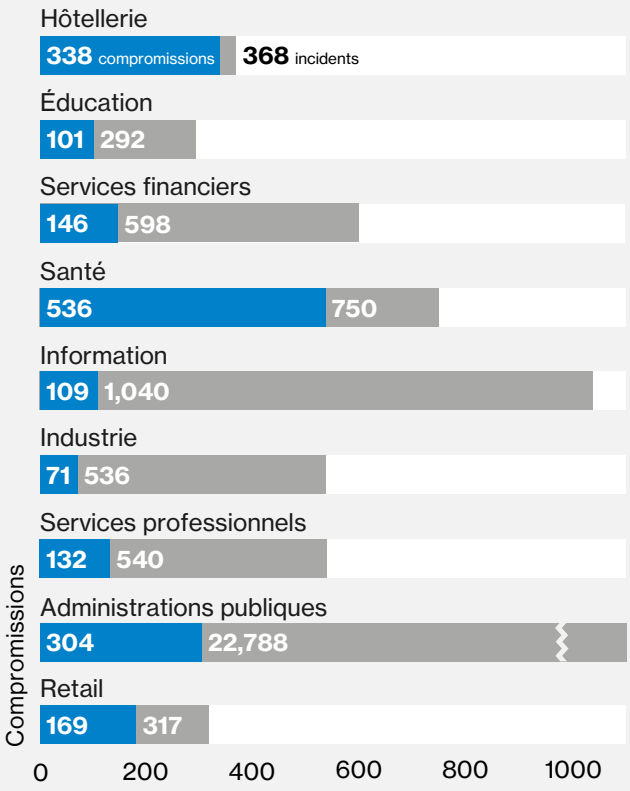
Quel est le risque n° 1 pour votre entreprise ?

Chaque secteur doit affronter une multiplicité de menaces qui lui sont propres. Mieux connaître ces dangers, c'est mieux orienter vos dépenses de sécurité et, in fine, mieux maîtriser les risques.

Cette section vous livre une synthèse des principales menaces rencontrées dans neuf secteurs. Si le vôtre n'apparaît pas, ne vous réjouissez pas trop vite. Cela signifie simplement que notre échantillon de données était trop restreint pour servir de base à une analyse fiable.

Le rapport DBIR 2018 vous offre une image plus détaillée des menaces secteur par secteur, ainsi que des conseils indispensables à une meilleure gestion des risques.

Nombre d'incidents et de compromissions par secteur



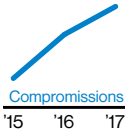
Hôtellerie

Qui	externe (99 %), interne (1 %)
Quoi	données de paiement (93 %), données personnelles (5 %), identifiants (2 %)
Comment	hacking (93 %), malware (91 %)

On distingue très clairement les zones d'action à prioriser. Sur la totalité des compromissions, 90 % impliquaient des terminaux de paiement. Vous avez en fait 100 fois plus de chances d'essuyer une attaque de ce type que la moyenne de tous les secteurs réunis.

Éducation

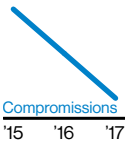
Qui	externe (81 %), interne (19 %)
Quoi	données personnelles (72 %), capital intellectuel (14 %), médical (11 %)
Comment	hacking (46 %), ingénierie sociale (41 %)



Les attaquants manient avec brio l'art de l'ingénierie sociale pour faire main basse sur les données personnelles de vos salariés et usurper leur identité. Mais avec 20 % des attaques perpétrées à des fins de cyber-espionnage, vos projets de recherche sont eux aussi clairement menacés. Notons que le gain financier n'est pas l'unique motif des attaques, puisque 11 % d'entre elles relèvent d'un piratage « récréatif ».

Services financiers

Qui	externe (79 %), interne (19 %)
Quoi	données personnelles (36 %), de paiement (34 %), bancaires (13 %)
Comment	hacking (34 %), physique (34 %)



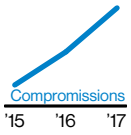
Vous devez rester vigilant face au risque de skimming, une pratique qui consiste à cloner les cartes de vos clients par le biais de systèmes installés sur les DAB. Avec le Jackpotting, les attaquants les plus habiles vont même jusqu'à transformer ces distributeurs en véritables machines à cash. De leur côté, les attaques DoS constituent une autre menace susceptible de perturber vos opérations.

Santé

Qui externe (43 %), interne (56 %)

Quoi données médicales (79 %), données personnelles (37 %), de paiement (4 %)

Comment erreurs (35 %), mauvais usage (24 %)



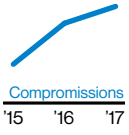
Voici le seul secteur où la menace provient majoritairement de l'intérieur. Au premier rang des accusés, on retrouve l'erreur humaine. Nombre de salariés usent en effet de leurs droits d'accès aux systèmes et données à mauvais escient, même si 13 % des cas sont motivés par l'amusement ou la curiosité (quelle célébrité a récemment été traitée, dans quel établissement, etc.).

Services professionnels

Qui externe (70 %), interne (31 %)

Quoi données personnelles (56 %), identifiants (28 %), internes (16 %)

Comment hacking (50 %), ingénierie sociale (21 %)



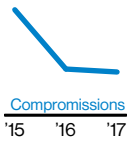
Les attaques ont généralement des visées financières et reposent le plus souvent sur le phishing ou l'utilisation d'identifiants volés. Les erreurs d'employés représentent également un danger bien réel. Alors que la compromission des données ne prend souvent que quelques heures voire moins, la détection de l'incident peut elle prendre des jours entiers. Bien souvent, l'alerte est même donnée par une entité externe.

Information

Qui externe (74 %), interne (23 %)

Quoi données personnelles (56 %), identifiants (41 %), internes (9 %)

Comment hacking (57 %), erreur (26 %)



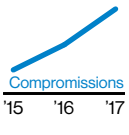
Ce secteur est particulièrement exposé aux attaques via applications web, généralement perpétrées au moyen d'identifiants volés. Ici comme ailleurs, l'erreur humaine est un problème. Elle prend le plus souvent la forme d'erreurs de publication ou de configuration des bases de données. Le plus grand danger vient néanmoins des attaques DoS qui comptent pour 56 % du total des incidents recensés en 2017.

Administrations publiques

Qui externe (67 %), interne (34 %)

Quoi données personnelles (41 %), secrets industriels (24 %), médical (14 %)

Comment hacking (52 %), ingénierie sociale (32 %)



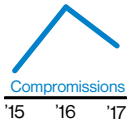
Le cyber-espionnage demeure un fléau puisqu'il représente 44 % des compromissions. Les attaques passent généralement par des campagnes de phishing, l'installation et l'utilisation de backdoors ou canaux de commande et contrôle (C2). Ne croyez pas que les attaquants ne ciblent que les secrets d'État : les données personnelles de vos salariés et administrés sont aussi dans leur collimateur.

Industrie

Qui externe (89 %), interne (13 %)

Quoi données personnelles (32 %), secrets industriels (30 %), identifiant (24 %)

Comment hacking (66 %), malware (34 %)



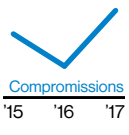
Avec 86 % d'attaques ciblées, l'industrie se distingue clairement des autres secteurs, où la majorité des attaques ont un caractère opportuniste. Ici, les pirates visent souvent les opérations de planification, recherche et développement. Parmi l'ensemble des compromissions, 47 % visaient la propriété intellectuelle pour obtenir un avantage concurrentiel.

Retail

Qui externe (91 %), interne (10 %)

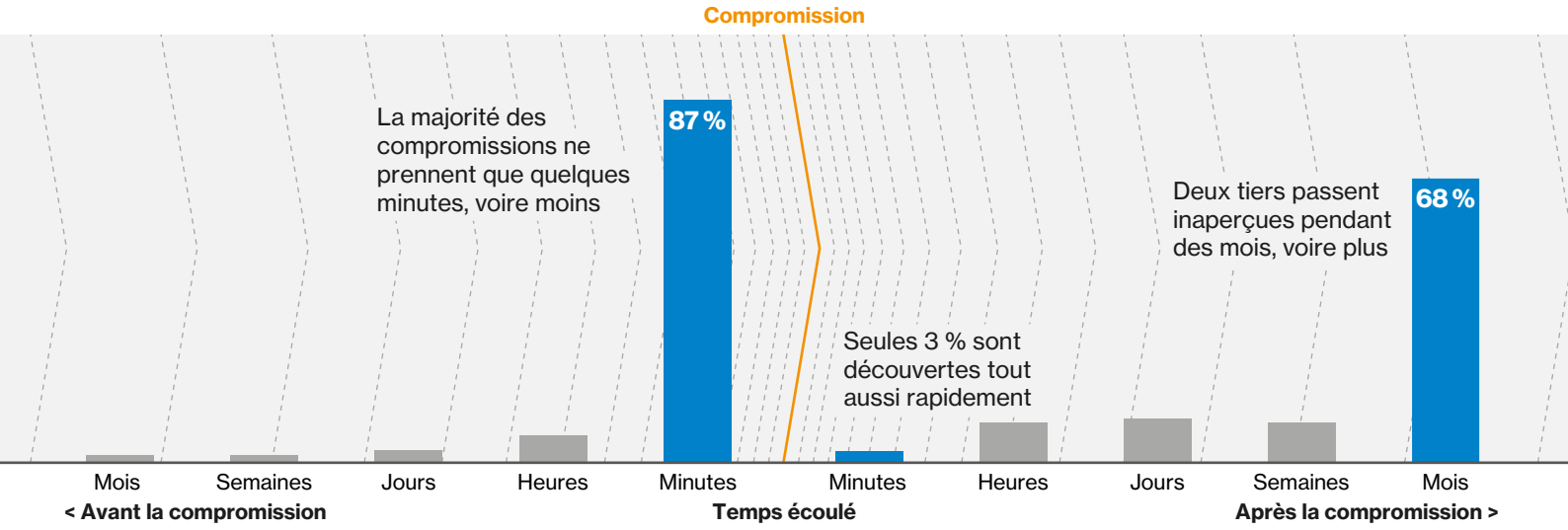
Quoi données de paiement (73 %), données personnelles (16 %), identifiants (8 %)

Comment hacking (46 %), physique (40 %)



Le vol de données est d'abord imputable aux attaques via applications web profitant d'identifiants volés ou d'un mauvais contrôle des saisies. Mais d'autres menaces planent également sur le secteur. Du blocage des transactions au ralentissement des sites web et systèmes en magasin, les attaques DoS ont elles aussi de lourdes répercussions.

Il est temps d'agir.



En règle générale, la compromission d'un système ne prend que quelques minutes, voire moins. L'incident n'étant détecté qu'au bout de plusieurs semaines ou plusieurs mois, les attaquants ont plus de temps qu'il n'en faut pour exfiltrer des données critiques.

68 % des compromissions passent inaperçues pendant des mois, voire plus

Bien souvent, c'est même une entité externe à l'entreprise qui donne l'alerte. Il peut s'agir de partenaires, de pouvoirs publics ou, pire encore, des clients eux-mêmes. Inutile d'insister sur les ravages d'une telle découverte pour votre image de marque.

Pour défendre votre réputation, vous devez articuler votre action autour de deux grands axes : la protection et la réponse à incident. En fait, vous devez ériger un rempart tel que les cybercriminels se mettront en quête de proies plus faciles. Rappelez-vous cependant qu'aucune protection n'est efficace à 100 %. Si un attaquant parvient à s'infiltrer, vous devrez être prêt à répondre rapidement et efficacement.

Les solutions à votre disposition

Restez sur vos gardes
N'attendez pas qu'un client ou la police vous signale une compromission. Comptez plutôt sur vos logs et vos systèmes de gestion du changement pour vous alerter rapidement.

Faites de vos collaborateurs votre premier rempart
Vos salariés saisissent-ils l'importance de la cybersécurité pour votre image de marque et, plus largement, pour votre santé financière ? Intégrez-les à votre système de défense en leur apprenant à identifier une attaque et à réagir efficacement.

Autorisez l'accès aux seules données nécessaires (principe du "need to know")
Savez-vous quels collaborateurs ont accès à vos systèmes et données critiques ? Accordez uniquement des droits d'accès en rapport avec leurs missions. Appliquez également des processus rigoureux de révocation des droits en cas de départ ou de changement de poste.

Appliquez rapidement les correctifs
Les cybercriminels continuent d'exploiter à loisir des failles pourtant bien connues. Vérifiez que vos anti-virus sont à jour : ils vous protégeront contre beaucoup de menaces.

Chiffrez vos données sensibles
En dépit de tous vos efforts, une attaque finira toujours par aboutir un jour ou l'autre. En chiffrant vos données, vous les rendrez inutilisables par les attaquants si elles venaient à être volées.

Utilisez l'authentification à deux facteurs
Les campagnes de phishing restent d'une redoutable efficacité. Et votre entreprise n'est pas non plus immunisée contre l'erreur humaine. L'authentification à deux facteurs vous permet de limiter les dégâts en cas de vol ou de perte d'identifiants.

N'oubliez pas la sécurité physique
Le web n'est pas le seul champ de bataille de la sécurité. Loin s'en faut. Avec des dispositifs de sécurité physique (caméras de surveillance, sas de sécurité…), vous pourrez empêcher vos adversaires de manipuler vos systèmes ou de subtiliser des données sensibles.

Capitalisez sur notre expertise.

Les attaquants élaborent constamment de nouvelles tactiques pour accéder plus facilement à vos données et à vos systèmes. Mais comme le montre notre rapport, trop d'entreprises continuent de leur simplifier la tâche. Pour certaines, même les mesures de sécurité les plus élémentaires laissent à désirer (mise à jour de l'antivirus, formation des collaborateurs à la détection d'une attaque, etc.).

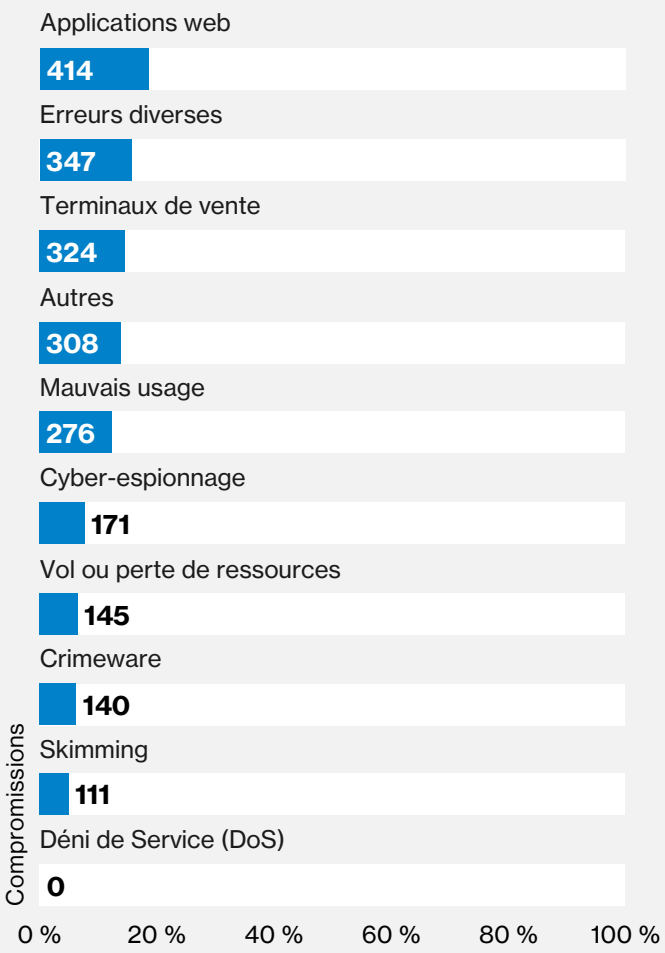
Sur le front de la sécurité, savoir c'est pouvoir. D'où l'importance de lire le rapport DBIR. En 2014, nous avions identifié neuf grands schémas d'attaque couvrant la majorité des menaces. Aujourd'hui, cette classification reste plus que jamais d'actualité.

94 % des incidents de sécurité et 90 % des compromissions avérées entrent dans l'une de ces neuf catégories.

Ces catégories vous aideront à mieux cerner les principales menaces qui pèsent sur votre entreprise. Que vous planifiez la mise à jour de systèmes ou le lancement d'une nouvelle application, vous saurez quels facteurs de sécurité intégrer en amont. Quant aux professionnels de la sécurité, ils disposeront d'un outil efficace pour mieux prioriser leurs dépenses.

Pour en savoir plus sur ces schémas d'attaque et la menace qu'ils représentent pour votre secteur en particulier, consultez dès maintenant l'édition 2018 du DBIR.

Répartition des compromissions par catégorie

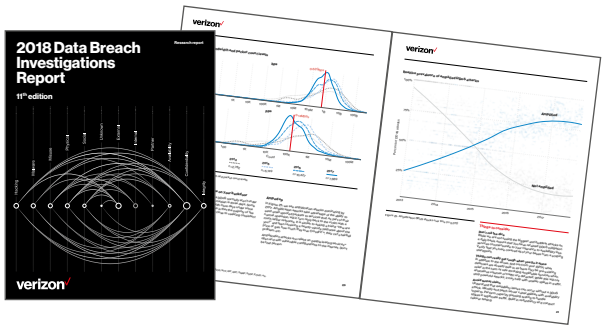


Le Rapport d'enquête Verizon sur les compromissions de données vous aide à comprendre les dangers qui vous menacent et les moyens d'y faire face.

Le DBIR 2018 se fonde sur l'analyse de plus de 53 000 incidents et 2 216 compromissions avérées. Déjà dans sa 11e édition, notre rapport est aujourd'hui reconnu comme une référence incontournable dans le monde de la sécurité.

Téléchargez le rapport complet ici :

verizonenterprise.com/DBIR2018



À propos de la couverture

Le diagramme en arcs placé en première de couverture est extrait de l'Annexe C du rapport principal. Dans ce diagramme, les nœuds représentent des acteurs, des actions et des attributs. Les arcs qui les relient reflètent leur ordre de survenue dans le déroulement d'une attaque. La taille des nœuds est proportionnelle au nombre d'occurrences recensées sur chaque chemin d'attaque. Enfin, la teinte des arcs correspond à la fréquence de passage d'une attaque entre les deux nœuds reliés.

verizonenterprise.com/fr