Rapport d'enquête 2016 sur les compromissions de données

Résumé

La cybersécurité ne concerne pas seulement les experts sécurité. Le guide pour les Directeurs avec tout ce que vous devez savoir.

verizon

Avez-vous déjà été vicitime d'une compromission ?

Dans 93 % des cas, il a suffi de quelques minutes ou moins aux attaquants pour compromettre les systèmes. Les entreprises, quant à elles, ont mis des semaines voire plus à simplement découvrir qu'une compromission avait eu lieu et ce sont généralement des clients ou les autorités qui ont donné l'alerte, et non pas leurs propres mesures de sécurité.

Plus de 100 000 incidents de sécurité. Analyse de 2 260 compromissions de données. 82 pays. 67 services de police et organisations de sécurité informatique ont fourni leurs données.

Le Rapport d'Enquête de Verizon sur les Compromissions de Données (DBIR) est considéré par les experts sécurité comme une source inégalée d'analyse et notre neuvième édition est la plus complète à ce jour. Mais DSI, Directeur Marketing ou PDG, vous devez également comprendre les risques, et ce rapport vous concerne.

La sécurité devrait être un élément moteur et non une considération a posteriori.

Les données sont les forces motrices de l'innovation. Cela accélère les chaînes logistiques et redéfinie l'expérience client. Mais les entreprises et les consommateurs sont préoccupés par la sécurité. Il est essentiel que vous gériez le risque, tant pour rassurer vos clients que pour vous donner toute la confiance nécessaire pour complètement adopter l'accélération numérique.

D'une manière ou d'une autre, chaque entreprise compte sur le numérique pour communiquer, négocier, maintenir sa compétitivité. Aujourd'hui, obtenir un avantage concurrentiel, c'est être en mesure de le faire numériquement - et mieux. Mais pour ce faire, vous avez besoin de systèmes fiables et sécurisés. Et cela signifie que la sécurité des données doit être au cœur de nos préoccupations.

Les compromissions de données génèrent des coûts importants. Il ne s'agit pas simplement de dédommagement ou d'amendes ; les frais liés aux services juridiques et la restauration des services peuvent aussi être considérables. Les compromissions peuvent aussi vous coûter cher en termes de réputation et d'image de marque. Cela s'avère particulièrement crucial, car avoir la confiance de vos clients et partenaires n'a jamais été plus importante.

Une compromission ne touchera probablement pas immédiatement votre business mais pourra sérieusement lui nuire ultérieurement.

Imaginez que vous soyez un magasin de bricolage. Les clients pourraient toujours acheter dans votre magasin, bien qu'étant probablement plus enclins à payer en espèces, mais vont-ils télécharger votre nouvelle application ou acheter votre nouvelle solution de domotique connectée ?

La plupart des compromissions sont motivées par l'appât du gain

Oubliez les films hollywoodiens. La plupart des cyberattaques sont aveugles et motivées par la cupidité, et non pas par la vengeance ou pour rendre un service public. La plupart des attaquants agissent afin de voler vos données pour leur valeur, qui que vous soyez. Tout ce qui peut être converti en argent les intéresse. Étant donné que la valeur des informations des cartes de paiement chute, les banques améliorant la détection des fraudes, les attaquants se tournent de plus en plus vers d'autres cibles comme la propriété intellectuelle et des informations sensibles de santé.

Les attaquants prennent la voie la plus facile

Ce serait une erreur de penser que le plus grand risque auquel vous faites face provient des vulnérabilités récemment découvertes. La plupart des attaques exploitent des vulnérabilités connues, pour lesquelles un patch est souvent déjà disponible depuis des mois, voire des années.

63 % des compromissions de données confirmées ont impliqué l'exploitation de mots de passe faibles, par défaut ou volés.

Souvent, les criminels ont pu pénétrer les systèmes aussi rapidement car ils avaient déjà la clé. L'efficacité de l'ingénierie sociale est très inquiétante - « cliquez ici pour réinitialiser votre mot de passe bancaire ». Nous avons constaté que près d'un tiers (30 %) des messages de phishing étaient ouverts – jusqu'à 23 % en 2014. Et 12 % des cibles continuaient à ouvrir la pièce jointe malveillante ou cliquaient sur le lien - presque identique à 2014 (11 %).

Compliquez-leur la vie

Le système impénétrable n'existe pas mais souvent même une défense à moitié décente dissuadera bon nombre de cybercriminels ; ils passeront leur chemin et rechercheront une cible plus facile. Malheureusement, de nombreuses entreprises ne parviennent même pas à atteindre cette modeste ambition.

95 % des brèches peuvent être décrites en neuf modèles.

Cette année, le DBIR se concentre à nouveau sur les neuf modèles d'incidents que nous avons identifiés en 2014. Leur compréhension vous aidera à concentrer vos efforts de sécurité là où c'est le plus nécessaire.

Dépenser plus intelligemment.

Les malfrats ne cessent de s'améliorer et votre infrastructure évolue plus vite que jamais. Comment pouvez-vous garder le dessus sans casser la tirelire ?

La pression sur les entreprises pour devenir plus « Numériques » s'accroît chaque jour. Il y a davantage d'appareils à protéger, davantage de personnes ayant accès aux données et davantage de partenaires à intégrer.

Les nouvelles technologies, comme le mobile et l'Internet des Objets (IoT), peuvent donner de nouvelles opportunités aux attaquants.

Nous n'avons pas encore vu de volume significatif d'incidents impliquant des terminaux mobiles ou IoT. Mais la menace est certainement réelle. Des démonstrations de faisabilité ont été faites et ce n'est qu'une question de temps avant de voir une compromission à grande échelle.

Neuf modèles décrivent plus de 80 % des incidents

Incidents
Compromissions

Changer la vue

Et les malfrats placent la barre toujours plus haut. Ils n'ont pas le choix car la valeur marchande de certains types de données chute, en particulier les informations liées aux cartes de paiement. Pour maintenir leurs revenus, les attaquants doivent voler davantage de données ou trouver de nouvelles formes d'information plus lucratives, comme des informations sensibles liées à la santé et à la propriété intellectuelle.

Vous devez les frapper là où ça fait mal : au portefeuille. Mais vous ne disposez pas d'un budget illimité. Cela signifie que vous devez dépenser plus intelligemment. La classification des incidents à neuf modèles que nous avons publiée pour la première fois en 2014 couvre la grande majorité des incidents et des compromissions confirmées, comme indiqué à la Figure 1. Et lorsque vous isolez et examinez un secteur de l'industrie en particulier, la majorité des menaces se retrouvent dans seulement trois modèles - voir la Figure 2. L'étude de ces modèles vous aidera à comprendre la meilleure façon de déployer vos effectifs et votre budget, tous deux limités, afin d'atteindre les meilleurs résultats.

95 % des compromissions et 86 % des incidents sont couverts par seulement neuf modèles.

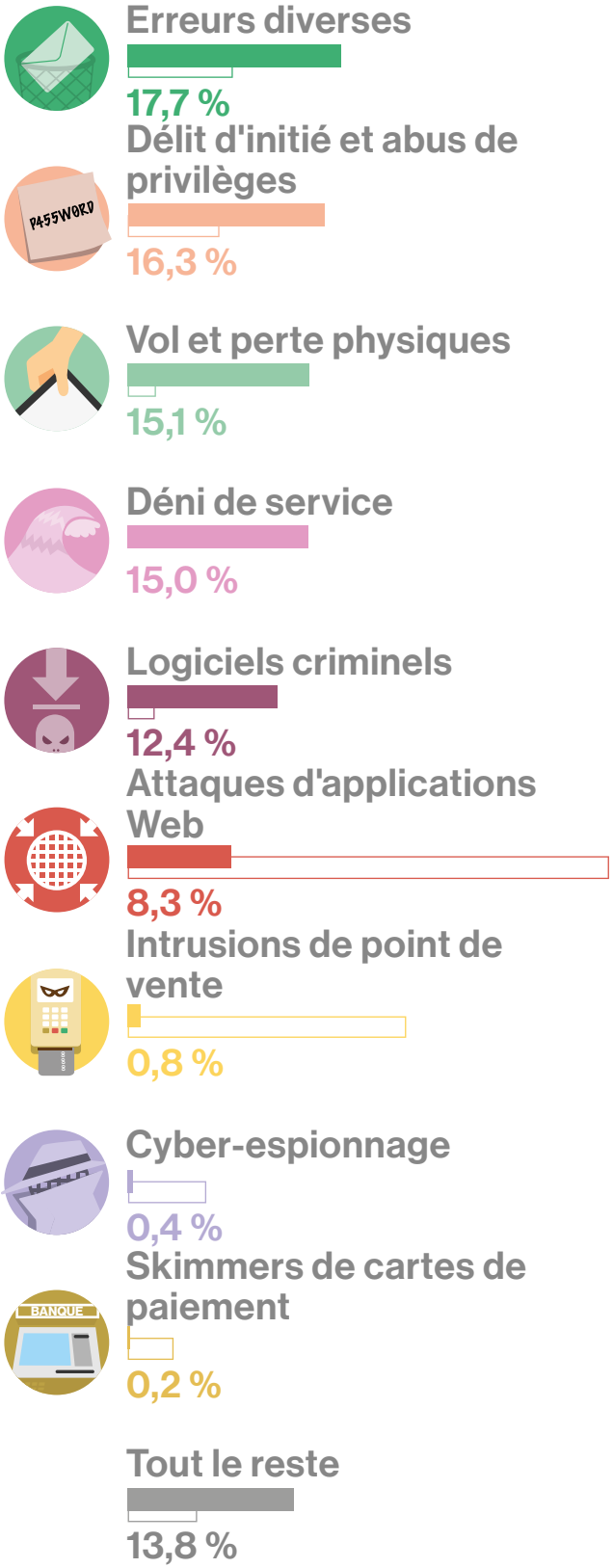


Figure 1 : Incidents / brèches par modèle de classification, toutes industries

Dans la plupart des industries, les trois quarts des incidents et des brèches sont couverts par seulement trois modèles.

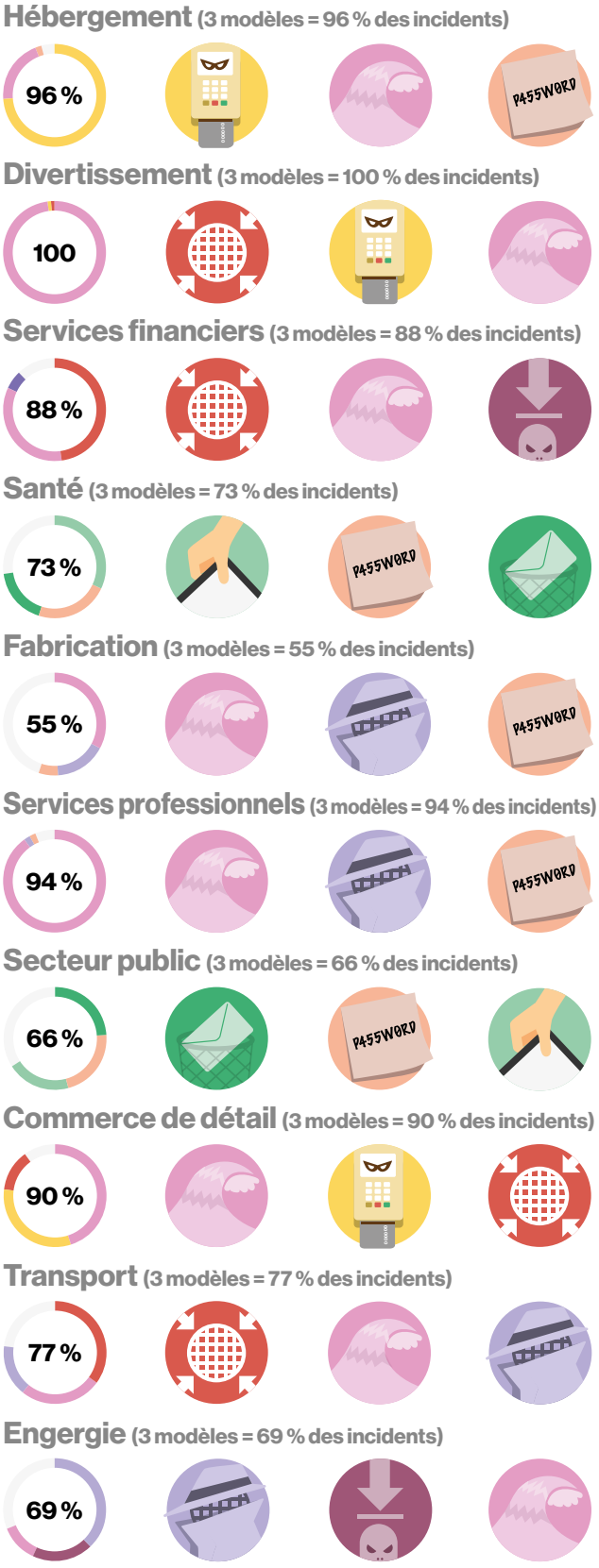


Figure 2 : Le top 3 des incidents / compromissions par industrie

Erreurs diverses

Toute action non intentionnelle ou erreur compromettant la sécurité, à l'exclusion de la perte d'actifs.

Les industries les plus touchées :
Secteur public, Santé, Information

40 % des incidents de ce modèle sont causés par un manque de capacité serveur pour lesquels des surcharges, pourtant non malveillantes, dans le trafic Web submergent les systèmes et provoquent le crash d'applications clés. Mais c'est souvent une simple erreur de l'un de vos employés qui déclenche un incident.

26 % des erreurs diverses impliquaient l'envoi d'informations sensibles à la mauvaise personne.

Quelles actions mener ?

- **Apprenez de vos erreurs :** Tenez un registre des erreurs courantes qui se sont produites dans le passé. Vous pouvez l'utiliser pour améliorer la formation de sensibilisation à la sécurité et mesurer l'efficacité de vos contrôles.
- **Renforcez les contrôles :** Pensez à utiliser un logiciel de prévention de perte de données (DLP) qui peut limiter les informations sensibles partagées en dehors de la société.
- **Mettez en œuvre des procédures sécurisées de suppression des données :** Assurez-vous que vos actifs soient exempts de données sensibles avant qu'ils ne soient vendus. Cela semble évident, mais nous avons vu beaucoup d'exemples où cela ne s'est pas passé.

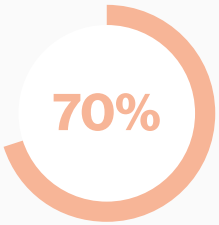
Délit d'initié et abus de privilèges

Cela se compose principalement d'incidents impliquant une utilisation abusive par du personnel interne. Mais des tiers externes (cas de collusion) et des partenaires bénéficiant d'un accès privilégié à des systèmes apparaissent également.

Les industries les plus touchées :
Santé, secteur public, administration

Contrairement à ce que pensent certaines personnes, ce sont rarement les administrateurs systèmes ou les développeurs avec des privilèges élevés qui sont les victimes. Les comptes des utilisateurs finaux représentent un tiers des abus pour du personnel interne. Les attaques sont généralement motivées par l'argent : 34 % des compromissions impliquant un abus étaient motivées par un gain financier, même si un quart (25 %) peut être lié à de l'espionnage, tel qu'un vol de propriété intellectuelle.

70 % des compromissions impliquant un abus de personnels internes ont pris des mois voire des années à être découverte.



Quelles actions mener ?

- **Connaissez vos données :** Vous devez savoir évaluer quelles sont vos données sensibles, pouvoir les localiser et connaitre qui y a accès. La Gouvernance doit veiller à ce que l'accès soit limité à ceux qui en ont vraiment besoin et l'accès effectif est vérifié par rapport à cette liste.
- **Surveillez le comportement des utilisateurs :** Suivez l'utilisation du système, en particulier l'accès à des données qui peuvent être utilisées pour un gain financier, et retirez immédiatement les droits d'accès lorsque les employés quittent l'entreprise.
- **Suivez l'utilisation de l'USB :** Ne vous mettez pas dans une situation où vous ne pourrez que constater qu'un employé a subtilisé des données après son départ.

Vol et perte physique

La perte ou le vol d'ordinateurs portables, de clés USB, de documents imprimés et d'autres actifs d'information.

Les industries les plus touchées :
Santé, secteur public

Un incident de sécurité est généralement déclenché par la perte d'un ordinateur portable ou d'un mobile par un employé. Mais la plus grande menace de brèche de données arrive avec des documents perdus ou volés qui ne peuvent pas être chiffrés.

39 % des vols ont eu lieu sur les espaces de travail des victimes et 34 % dans le véhicule personnel des employés.

Quelles actions mener ?

- **Chiffrez vos données :** Si les terminaux volés sont chiffrés, il est beaucoup plus difficile pour les agresseurs d'accéder aux données.
- **Formez votre personnel :** Il est essentiel de développer une sensibilisation à la sécurité au sein de votre entreprise. Travaillez avec les RH pour intégrer une formation à la sécurité physique des actifs dans le cadre de la formation continue des employés.
- **Réduisez l'usage du papier :** Réduisez l'usage de l'impression de documents. Établissez des règles de classification des données et créez une politique d'entreprise portant sur l'impression et le transport de données sensibles.

Déni de service (DoS)

L'utilisation de botnets, une armée d'ordinateurs « zombies », généralement enrôlés sans la permission du propriétaire, pour submerger une entreprise de trafic malveillant. Des attaques de DoS peuvent stopper vos opérations courantes, provoquant le chaos.

Les industries les plus touchées :
Divertissements, professionnel, éducation

Ne sous-estimez pas l'impact qu'une attaque DoS pourrait avoir sur votre entreprise. Il s'agit du quatrième modèle le plus courant dans nos données concernant tous les incidents de sécurité. Et une attaque à grande échelle pourrait mettre votre site Web ou des systèmes critiques hors service pendant des semaines.

Le trafic médian d'une attaque DoS est de 1,89 million de paquets par seconde, l'équivalent de plus de 113 millions de personnes tentant d'accéder à votre serveur chaque minute.

1,89 Mpps

Quelles actions mener ?

- **Isolez les serveurs clés :** Séparez les systèmes primaires pour les protéger des attaques.
- **Choisissez vos prestataires avec soin :** Assurez-vous que vos prestataires de services cloud aient des solutions en place pour protéger la disponibilité de leurs services et de leur infrastructure.
- **Testez votre service anti-DoS :** Il ne suffit pas de l'installer puis de l'oublier. Assurez-vous que vous ayez une bonne compréhension de vos accords de niveau de service (SLA) pour la mitigation du DoS.

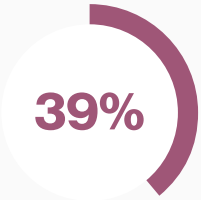
Logiciels criminels

Cette partie couvre toute utilisation de logiciels malveillants qui n'entre pas dans un modèle plus spécifique. Le crimeware affecte souvent les consommateurs.

Les industries les plus touchées :
Secteur public, fabrication, information

Les attaques sont généralement opportunistes et motivées par un gain financier. Le malware se met sur votre système lorsque quelqu'un clique sur le lien d'un e-mail malveillant ou visite un site infecté. Le ransomware (demande de rançon) est de plus en plus répandu. Il implique le chiffrement du contenu d'un terminal par les attaquants, le rendant ainsi inutilisable. Ils demandent alors une rançon pour déverrouiller les données.

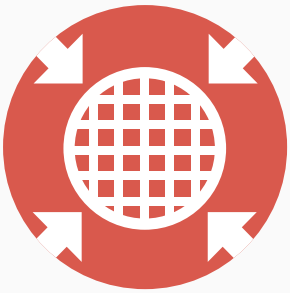
39 % des incidents de crimewares en 2015 ont impliqué une demande de rançon.



Quelles actions mener ?

- **Patchez rapidement :** Les cybercriminels exploitent avec succès des vulnérabilités connues ; patcher à temps permet de bloquer de nombreuses attaques.
- **Mettez en œuvre un suivi du changement de configuration :** De nombreuses méthodes d'attaque peuvent être facilement détectées en observant des indicateurs clés.
- **Faites des sauvegardes régulières de vos systèmes :** Cela permettra de garder votre entreprise en bonne marche si des systèmes venaient à tomber sous le coup d'un ransomware.
- **Capturez des données durant les attaques :** Examinez les différents types de malwares qui vous ont attaqués et, si possible, le point d'entrée. Cela vous donnera des renseignements sur les zones où concentrer vos efforts.

Attaques d'applications Web

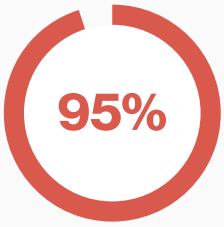


Si une application Web, comme un système de gestion de contenu (Content Management System - CMS) ou une plate-forme d'e-commerce, a été utilisée comme moyen d'entrée.

Les industries les plus touchées :
Services financiers, vente de détail, information

De nombreuses attaques d'applications Web frappent sans distinction. Les attaquants trouvent une cible fragile avec une vulnérabilité qu'ils ont pu compromettre ; ou bien ils se sont infiltrés via une campagne de phishing. Les cybercriminels ont eu beaucoup de succès en utilisant des plugins CMS pour déployer des logiciels malveillants. Une fois à l'intérieur, de nombreuses attaques ont défiguré le site Web de la cible. Nous avons pu également constater que pour près de 20 000 incidents, les sites Web compromis avaient étéutilisés comme vecteurs d'attaques de déni de service distribué (DDoS) ou réutilisés comme sites de phishing.

95 % des attaques d'application Web dans lesquelles des criminels ont volé des données étaient motivées par l'argent.



Quelles actions mener ?

- **Utilisez une authentification à deux facteurs :** Et verrouillez les comptes après des échecs répétés de tentatives de connexion. Pensez également à utiliser la biométrie.
- **Patchez rapidement :** Mettez en place un processus solide pour patcher les plates-formes CMS, y compris les plugins tiers et les systèmes de commerce électronique. Voir la section : « Un patching efficace peut les arrêter » à la page 10.
- **Surveillez toutes entrées :** Passez en revue tous vos journaux de logs pour aider à identifier les activités malveillantes.

Intrusions de point de vente

Lorsque des attaquants compromettent les ordinateurs et serveurs qui exécutent des applications de point de vente, dans le but de récupérer des données de paiement.

Les industries les plus touchées :
Hôtellerie, vente de détail

En 2015, les chaînes hôtelières ont fait la une des journaux pour des brèches liées aux cartes de paiement à distance. En 2014, c'était la grande distribution. Les compromissions réussies arrivaient souvent par l'intermédiaire d'un prestataire du point de vente plutôt qu'à la suite d'une configuration défaillante de terminaux de PdV connectés à Internet.

95 % des brèches confirmées dans le secteur de l'hôtellerie ont impliqué des intrusions de PdV.

Quelles actions mener ?

- **Patchez les serveurs rapidement :** Et ne donnez accès qu'à des gens qui en ont absolument besoin.
- **Choisissez vos prestataires avec soin :** Assurez-vous que vos prestataires de services cloud aient des solutions en place pour protéger vos systèmes.
- **Réservez les systèmes de point de vente aux activités de PdV :** Ne laissez pas le personnel les utiliser pour naviguer sur le Web, consulter leurs e-mails ou jouer à des jeux.
- **Utilisez une authentification à deux facteurs :** Votre prestataire de PdV doit également utiliser une authentification à deux facteurs.

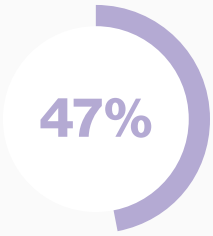
Cyber-espionnage

Attaques motivées par l'espionnage menées par des acteurs affiliés à des États, souvent à la recherche de propriété intellectuelle.

Les industries les plus touchées :
Fabrication, information, professionnel

Ces attaques commencent généralement avec les mêmes outils et techniques utilisés ailleurs avec succès, avant de passer à des méthodes plus sophistiquées. Cela signifie que les mesures de sécurité de base sont étonnamment efficaces dans la protection contre le cyber-espionnage et ne doivent pas être oubliées en faveur d'une protection plus spécifique.

47 % de toutes les brèches confirmées dans le secteur de la fabrication peuvent être classés comme du cyber-espionnage.



Quelles actions mener ?

- **Patchez rapidement :** Les cybercriminels exploitent avec succès des vulnérabilités connues ; patcher à temps peut bloquer de nombreuses attaques.
- **Mettez en œuvre un suivi du changement de configuration :** De nombreuses méthodes d'attaque peuvent être facilement détectées en observant des indicateurs clés.
- **Isolez les systèmes :** Assurez-vous qu'un ordinateur compromis ne soit pas une porte ouverte vers des systèmes et des données plus critiques.

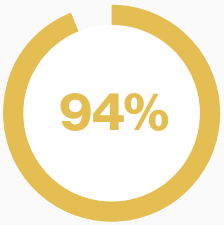
Skimmers de cartes de paiement

Incidents impliquant l'installation physique d'un dispositif sur un distributeur automatique, une pompe à essence ou un terminal de PdV qui interceptent des données de cartes.

Les industries les plus touchées :
Services financiers, commerce, hôtellerie

La plupart de ces attaques se produisent aux distributeurs automatiques, mais les pompes à essence et autres terminaux sont aussi concernés. Les skimmers peuvent être presque impossibles à détecter, même pour l'œil exercé.

94 % des brèches impliquant des skimmers de cartes de paiement ont eu lieu sur un distributeur automatique.



Quelles actions mener ?

- **Utilisez des terminaux inviolables :** Certains terminaux sont plus sensibles à la falsification que d'autres. Choisissez-en un qui a été conçu pour dissuader les criminels.
- **Surveillez la falsification :** Mettez en place une procédure pour vérifier régulièrement l'intégrité des lecteurs de cartes des distributeurs automatiques et des pompes à essence. Formez vos employés à repérer les skimmers et facilitez-leur le signalement de toute activité suspecte.
- **Utilisez des contrôles inviolables :** Cela pourrait être aussi simple que de mettre un scellé sur la porte d'une pompe à essence.

Les malfrats sont plus rapides

Les cybercriminels peuvent pénétrer des systèmes puis voler (exfiltrer) des données en quelques minutes. Dans 93 % des cas où des données ont été volées, les systèmes ont été compromis en quelques minutes, voire moins. Et l'exfiltration a eu lieu en quelques minutes dans 28 % des cas. Mais même quand l'exfiltration a pris des jours, les criminels n'ont pas eu à s'inquiéter. Dans 83 % des cas, les victimes n'ont pas su qu'elles avaient été compromises après plusieurs semaines voire plus.

Plus vous prenez de temps à découvrir une compromission, plus les criminels auront de temps pour trouver les données précieuses qu'ils recherchent et perturber votre entreprise. C'est la raison pour laquelle la protection ne suffit pas. Vous devez avoir des systèmes et des procédés efficaces de détection et de remédiation pour déjouer les attaques et réduire les dommages possibles.

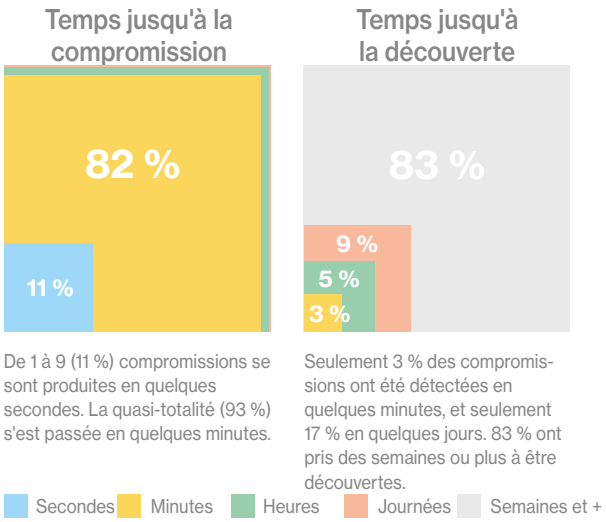


Figure 3 : Chronologie d'une brèche

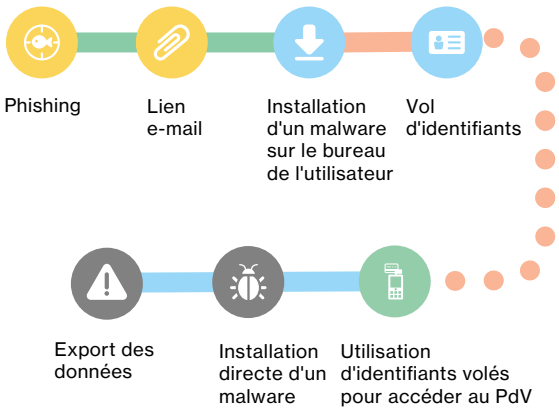


Figure 4 : Naissance et renaissance d'une compromission de données

Comment ils frappent

La compréhension des éléments constitutifs d'une attaque doit vous aider à bâtir des défenses solides et à détecter rapidement une compromission le cas échéant.

Même les attaques sophistiquées partagent l'ADN des plus simples. Mais les différentes parties d'une attaque n'ont pas toujours lieu dans le même ordre. Et en général, vous ne subissez pas juste une attaque à la fois. Des graphiques d'attaques peuvent vous aider à mettre en évidence votre zone d'attaque tout entière, pas seulement les voies visibles.

Un patching efficace peut les arrêter

Le Top 10 des vulnérabilités [Common Vulnerabilities and Exposures, ou CVE] représentait 85 % du trafic d'exploit réussi. Les 15 % restants comprennent plus de 900 CVEs.

Un patching rapide est important, mais avec tant de nouvelles vulnérabilités découvertes, il est difficile de savoir par où commencer. Le rapport DBIR de cette année fournit des informations précieuses pour vous aider à résoudre ce casse tête.

Les données fournies par Kenna Security suggèrent que les vulnérabilités dans les produits Adobe étaient exploitées le plus rapidement ; celles des produits Mozilla le plus lentement - Voir Figure 5. L'étude de ces informations vous aidera à éviter des « alertes » et à vous concentrer sur vos efforts de correction.

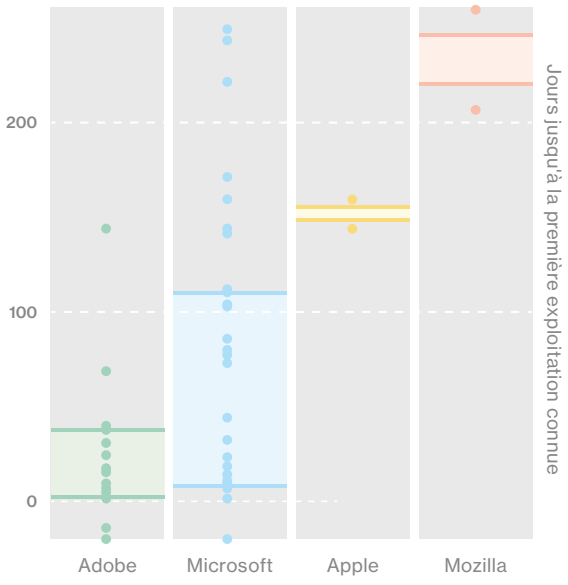


Figure 5 : Temps en jours jusqu'à la première exploitation connue de vulnérabilités

Utilisez l'intelligence, les escrocs le font !

Les cybercriminels ne se satisfont pas du statu quo. Étant donné que la valeur de certaines formes de données chute, ils jettent leurs filets de façon plus large et améliorent leurs tactiques.

Aucun système n'est sécurisé à 100 %, mais trop d'entreprises leur facilitent la tâche. Elles laissent ouvertes des vulnérabilités bien connues et les employés peuvent utiliser des mots de passe facile à deviner et même souvent les valeurs par défaut des systèmes.

Cela signifie que nombre des compromissions que nous avons constatées auraient pu être évitées si les entreprises avaient mis en place des mesures de sécurité de base. Nos sept conseils dans l'encadré à droite couvrent les erreurs simples que nous avons pu voir à maintes et maintes reprises.

Mais votre équipe SI doit avoir une compréhension approfondie des menaces auxquelles votre entreprise doit faire face. Les cybercriminels utilisent toutes les informations qu'ils peuvent se procurer pour dominer le jeu. Vous devez faire de même. Le Rapport d'Enquête 2016 de Verizon sur les compromissions de données est un document incontournable pour toute entreprise qui prend la cybersécurité au sérieux.

Quelques mesures simples et rapides

- **Soyez vigilants :** Les journaux de logs et systèmes de gestion des changements peuvent vous donner une alerte précoce d'une compromission.
- **Faites de vos employés votre première ligne de défense :** Formez le personnel à repérer les signes avant-coureurs.
- **Conservez les données conformément au principe « need to know » :** Limitez l'accès aux seuls systèmes dont les employés ont besoin pour leur travail.
- **Patchez rapidement :** Cela vous protégera contre de nombreuses attaques.
- **Chiffrez les données sensibles :** Rendez vos données presque inutiles si elles sont volées.
- **Utilisez une authentification à deux facteurs :** Cela limitera les dommages possibles avec des identifiants perdus ou volés.
- **N'oubliez pas la sécurité physique :** Tous les vols de données ne se produisent pas en ligne.

Téléchargez le Rapport d'Enquête Verizon 2016 sur les compromissions de données

Le DBIR est notre principale publication annuelle sur la sécurité, et l'une des sources les plus respectées de l'industrie de l'information. En plus du rapport complet et de ce résumé, nous publions également un certain nombre d'autres ressources pour vous aider à comprendre les menaces et améliorer vos défenses. N'hésitez pas à les consulter.

Recevez notre DBIR 2016 complet et d'autres ressources utiles.

Lire la suite ›

Votre cybersécurité est-elle mauvaise ? Consultez notre SlideShare.

SlideShare ›

VerizonEnterprise.com/fr