Rapport d'enquête 2020 de Verizon sur les compromissions de données – Guide de référence à destination des RSSI

mai 27, 2020
by SentinelOne

Pour la 13e année consécutive, Verizon a publié son rapport d'enquête sur les compromissions de données (*Data Breach Investigations Report*), lequel constitue une source détaillée d'informations précieuses et directement exploitables par les RSSI et DSI. L'édition 2020 s'appuie sur les données fournies par 81 entreprises, parmi lesquelles des sociétés spécialisées en cybersécurité, des autorités policières, des centres ISAC (*Information Sharing and Analysis Center*), des groupes CERT (*Computer Emergency Response Teams*), des cabinets de conseil et des organismes publics. Ce nouveau rapport couvre 157 525 incidents signalés et 108 069 compromissions de données. Avec ses 119 pages, c'est un document relativement dense. Nous allons ici aborder en détail les principales conclusions du rapport et proposer des recommandations qui vous aideront à renforcer vos opérations de sécurité.

Qui se cache derrière la plupart des cyberattaques ?

Bien qu'on ne puisse nier l'existence d'attaques d'origine interne (pas moins de 30 % des attaques) et que leur nombre soit même en augmentation, la grande majorité des menaces qui pèsent sur votre entreprise sont le fait d'intervenants externes. Les données recueillies au cours de l'année passée montrent en effet que 70 % des compromissions sont dues à ces intervenants externes. Seul 1 % des attaques impliquaient plusieurs parties ; 1 % impliquaient l'intervention de partenaires. Comme l'indique le rapport :

> « Beaucoup considèrent que les plus grandes menaces pour la sécurité d'une entreprise viennent de l'intérieur, mais nous pensons que cette hypothèse est erronée. »

Une mise en garde s'impose toutefois : il ne faut pas confondre le nombre de menaces d'une origine particulière et l'ampleur du risque qu'elles représentent. Suivant la nature de l'incident, une seule attaque d'origine interne est capable de provoquer dix fois plus de dégâts qu'une attaque externe. Cela dit, même si les équipes de sécurité doivent gérer des attaques indépendamment de leur origine, les données disponibles montrent clairement que les cybercriminels externes à l'entreprise se bousculent au portillon pour mettre à mal vos systèmes de défense.

Mais qui sont ces « intervenants externes » ? Autrement dit, qui ne font pas partie de vos effectifs ? Environ 55 % sont classés dans la catégorie du « crime organisé », ce qui correspond pour les chercheurs à des « criminels suivant un processus défini », sans faire pour autant référence à la mafia. Pour être plus clair, il s'agit d'attaques venant de criminels dont on peut observer qu'ils ont un objectif clair et une méthodologie identifiable. Nous aborderons ces objectifs dans la section suivante, mais soulignons simplement pour le moment que le terme « criminel » exclut ici tout acteur agissant pour le compte d'un État et que l'expression « processus défini » exclut les attaques opportunistes, les attaques de cyberactivistes et les attaques dont la motivation n'a pas pu être déterminée.

Que cherchent les cybercriminels ?

Vous aurez sûrement deviné la réponse à cette question : de l'argent. C'est du moins le moteur principal dans la grande majorité des cas. D'après le rapport, environ 86 % des compromissions sont motivées par l'appât du gain. Cela ne devrait pas étonner les spécialistes en sécurité, mais pour de nombreuses parties prenantes au sein de votre entreprise qui entendent souvent parler d'attaques commanditées par des États et de menaces APT, cela peut être une véritable révélation.

Il est intéressant de noter que cette recherche de rentabilité explique également pourquoi les cybercriminels ne mettent principalement en œuvre que des attaques impliquant deux à trois étapes maximum. Tout processus plus complexe est soit abandonné, soit le fait de cybercriminels persistants. Cela s'explique très simplement : si vous êtes un cybercriminel attiré uniquement par la recherche de profit, vous chercherez à automatiser vos attaques au maximum, et vous optenez de préférence pour des proies faciles plutôt que de consacrer beaucoup de temps et d'efforts à percer les défenses de cibles plus coriaces. Agir rapidement et à grande échelle à l'aide d'outils automatisés de ciblage et d'exploitation offre un excellent retour sur investissement. S'il y a donc un enseignement à retenir, c'est que si vous mettez en place une protection efficace et étendue et que vous donnez du fil à retordre aux cybercriminels, la grande majorité d'entre eux ne perdront pas leur temps à vous attaquer.

Cela dit, même si l'argent est la motivation ultime des cybercriminels, ce n'est souvent pas la seule chose qu'ils parviennent à dérober lors de leurs incursions. Ainsi, 58 % des attaques ont entraîné la compromission de données personnelles et 37 % se sont soldées par l'exploitation ou le vol d'identifiants d'utilisateurs. Comme nous le verrons plus loin, les identifiants d'utilisateurs représentent en effet un butin de choix pour les cybercriminels. Notez par ailleurs que votre entreprise peut également faire l'objet d'une attaque car elle permet au cybercriminel un moyen d'accéder à une autre cible, d'une valeur plus grande aux yeux des cybercriminels. Un cybercriminel peut même s'intéresser à l'un de vos serveurs dont la protection n'est pas suffisante, uniquement dans le but de l'enrôler au sein d'un botnet utilisé dans une attaque DDoS contre une autre cible. Peut-être faites-vous également partie de la chaîne logistique d'une victime plus prometteuse, à moins que vous ne soyez un prestataire d'infogérance dont la valeur pour les cybercriminels réside dans votre base de clients plutôt que dans votre entreprise en soi.

Comment les pirates déjouent-ils vos défenses ?

Sur cette question, les données disponibles sont claires : les identifiants volés, récupérés par phishing ou obtenus via des attaques par force brute sont le principal moyen utilisé par les cybercriminels pour s'introduire dans les réseaux. Une fois dans la place, l'un de leurs principaux objectifs consiste alors à récupérer d'autres identifiants afin de conserver leur accès ou de les revendre. Plus de 80 % des compromissions liées à un piratage s'appuient sur une forme d'attaque par force brute ou sur l'emploi d'identifiants d'utilisateurs perdus ou volés. Ces chiffres sont loin de nous étonner. On estime à plusieurs dizaines de millions de fois par jour le recours aux pratiques de credential stuffing, reposant sur la réutilisation d'une liste de combinaisons nom d'utilisateur / mot de passe (souvent divulguées dans le cadre d'autres compromissions) pour tenter d'accéder à des comptes.

Cette tendance est étroitement liée au fait que de nombreuses entreprises ont basculé une grande partie de leurs données et services vers le cloud, où il est plus difficile de déployer des malwares. Les cybercriminels se tournent alors vers une solution beaucoup plus simple et flexible : ils assaillent le service cible de requêtes de connexion à l'aide des identifiants qu'ils ont dérobés ou obtenus par l'acquisition de grands volumes de données. Par ailleurs, dans la mesure où les attaques par ransomware les plus agressives exfiltrent désormais les données avant de les chiffrer, il est fort probable que ces données soient revendues ou réutilisées par les mêmes cybercriminels pour tenter d'accéder à nouveau aux comptes des entreprises ciblées, à un stade ultérieur, par le biais de la technique du credential stuffing. Selon le rapport :

> « Cela s'apparente à un processus constant qui se déroule à un rythme plus ou moins régulier : infiltration, récupération d'identifiants, mise à jour du dictionnaire, exécution d'attaques par force brute, et on recommence. »

Étant l'intérêt des cybercriminels pour le vol d'identifiants, que ce soit à des fins de persistance ou de nouvelles compromissions, il est essentiel que les entreprises prennent les mesures nécessaires pour les sécuriser.

L'ingénierie sociale reste la principale méthode utilisée pour dérober de nouveaux identifiants, obtenir l'accès aux réseaux des entreprises et/ou détourner leur argent. Environ 96 % des attaques par phishing reposent sur la diffusion d'e-mails ou de courriers indésirables malveillants. Pour ce qui est des types de fichiers utilisés, le choix des cybercriminels se porte très majoritairement sur les documents et les applications Windows. Parmi les autres types de fichiers qui ont pu être utilisés dans une moindre mesure, citons notamment les scripts shell, les archives, les fichiers Java et Flash, les PDF, les DLL ou encore les applications macOS, Linux et Android.

De quelles ressources les cybercriminels tirent-ils le plus parti ?

Bien que les attaques ciblant les ressources sur site continuent de dominer le paysage des menaces (à hauteur d'environ 70 % des compromissions), les ressources dans le cloud ont fait l'objet de 24 % des compromissions au cours de l'année passée. Sur cette part, les serveurs d'applications Web ou de messagerie étaient impliqués dans 73 % des cas, avec vol d'identifiants dans 77 % de ces intrusions particulières. Il semble clair que les cybercriminels ont intégré que les entreprises conservent désormais leurs informations sensibles dans des applications ou infrastructures cloud, et adaptent leur approche à cette nouvelle évolution afin de récupérer et monétiser ces informations.

Les serveurs d'applications Web sont ciblés davantage que n'importe quelle autre ressource (y compris le personnel, via l'ingénierie sociale). De manière générale, cela passe soit par l'utilisation d'identifiants volés (comme indiqué précédemment), soit par l'exploitation de vulnérabilités non corrigées.

Les équipes de sécurité doivent donc se montrer particulièrement attentives à ce point d'accès aux données, car seulement la moitié de toutes les vulnérabilités signalées sont effectivement corrigées dans les trois mois qui suivent leur découverte. Nous sommes donc ici face à deux failles majeures en termes de sécurité. D'une part, les cybercriminels réagissent souvent rapidement pour devancer le cycle de correction, en utilisant notamment des services comme Shodan pour analyser l'ensemble du réseau à la recherche d'équipements vulnérables. D'autre part, et c'est un point qui est peut-être sous-estimé, les équipes informatiques qui ne corrigent pas une vulnérabilité dans les trois mois après sa découverte risquent de ne jamais la corriger. Les vulnérabilités auxquelles s'intéressent le plus les cybercriminels sont celles qui ont trait aux injections SQL, PHP ou de fichiers locaux, notamment contre des cibles appartenant au secteur de la vente au détail.

De mauvaises pratiques de sécurité sont-elles un facteur d'échec ?

L'erreur est humaine, on le sait. Mais toute entreprise est pilotée par des processus, et c'est justement l'application et le contrôle rigoureux de ces processus qui permettent de réduire la risque d'erreurs humaines. Dans le cas qui nous occupe, les erreurs humaines entraînant une mauvaise configuration du stockage connaissent une augmentation dans les compromissions signalées. D'après les données disponibles, ces erreurs ont une incidence directe sur 22 % des compromissions confirmées. Pour mettre ce chiffre en perspective, il s'agit du même pourcentage que celui attribué à l'ingénierie sociale sur le même ensemble de données.

La bonne nouvelle est qu'une partie, peut-être non négligeable, des compromissions relevant d'une mauvaise configuration du stockage sont signalées par les chercheurs spécialistes en sécurité plutôt que découvertes par les cybercriminels. La mauvaise nouvelle est que les problèmes de ce type ont tendance à faire la une des médias et portent atteinte à la réputation de l'entreprise concernée — avec un impact difficile à quantifier, mais qui pourrait être l'équivalent d'un vol de données par des cyberpirates.

Quels types de malwares sont privilégiés par les cybercriminels ?

Environ 17 % des compromissions confirmées impliquent une forme ou une autre de malware. Dans le lot, 27 % sont imputables à des ransomwares, ce qui ne devrait étonner personne compte tenu du volume important d'incidents fortement médiatisés au cours de l'année passée.

Comme SentinelLabs le souligne depuis un certain temps, les tactiques d'utilisation des ransomwares ont évolué ces derniers mois et incluent désormais souvent une part d'extorsion : en exfiltrant les données avant de les chiffrer, les groupes cybercriminels spécialisés en ransomwares peuvent menacer leurs victimes de dévoiler des données clients sensibles ou des éléments de propriété intellectuelle si elles refusent de payer. Cette tendance est réellement apparue après la fin de la collecte de données réalisée dans le cadre du rapport Verizon. Nous devrions donc pouvoir l'observer plus concrètement dans le rapport de l'année prochaine. Toutefois, avant octobre 2019 (échéance maximale pour l'inclusion des données au rapport 2020), on peut noter une nette progression des ransomwares sur la première partie de l'année. Les ransomwares sont ainsi considérés comme étant :

> « (…) le troisième type de compromission par malware le plus courant et le deuxième type d'attaque par malware le plus courant. »

Sur les différents secteurs d'activité couverts par le rapport, les secteurs public et de l'enseignement ont été des cibles privilégiées des opérateurs de ransomwares au cours de l'année passée.

Dans la mesure où les données montrent que le vol d'identifiants a été la priorité numéro 1 des cybercriminels, il est peu étonnant que le type de malware le plus utilisé ait été les outils de collecte de mots de passe. Viennent ensuite les téléchargeurs (type Emotet et TrickBot, par exemple), puis les chevaux de Troie, qui sont surtout associés aux cybercriminels spécialisés visant une persistance à long terme par le biais de backdoors et de la fonctionnalité C2. Fait intéressant, on a pu constater une baisse notable du nombre de malwares de cryptojacking après un pic de popularité en 2017 et surtout en 2018.

Recommandations de SentinelOne

Avec ses 119 pages, ce rapport contient encore beaucoup d'autres informations, mais nous espérons qu'il vous en présenter fidèlement les grandes lignes. Dans cette section, nous souhaitons vous proposer différentes recommandations fondées sur notre analyse du rapport dans son ensemble et sur les propres données télémétriques de SentinelOne.

Contrairement à ce que l'on observe avec les attaques APT, la majorité des cybercriminels ne cherchent pas à mettre en place des stratégies particulièrement compliquées et organisées en plusieurs phrases. Autrement dit, intercepter une attaque à *n'importe quelle étape* (plutôt qu'à chaque étape) de son cycle de vie, également appelé la « chaîne de frappe », augmentera considérablement vos chances d'éviter une compromission. Par ailleurs, plus tôt vous y parviendrez, meilleures seront vos chances de repousser les cybercriminels qui, se retrouvant bredouilles, iront tenter leur chance ailleurs sans insister. Comme l'ont montré les résultats de la récente évaluation MITRE ATT&CK, SentinelOne se distingue dans la neutralisation des attaques à toutes les étapes de la chaîne de frappe, mais plus particulièrement dans le blocage des attaques avant même qu'elles ne s'établissent. Notre première recommandation, et sûrement la plus évidente : assurez-vous de vous appuyer sur une plateforme d'intelligence artificielle de nouvelle génération éprouvée, fiable et capable de protéger vos équipements.

Comme nous l'expliquions précédemment, les cybercriminels automatisent leurs attaques afin de se faciliter la tâche. Compliquez-leur les choses en veillant à ne pas laisser de ports ouverts inutilement et à limiter le nombre de ports exposés. Autorisez uniquement l'accès à Internet aux services essentiels et réduisez autant que possible le nombre de personnes autorisées à utiliser ces services. Les protocoles SSH et Telnet (par défaut respectivement affectés aux ports 22 et 23) sont des cibles privilégiées dans les tentatives de connexion malveillantes. Qui dans votre entreprise en a réellement besoin ? Identifiez les intervenants concernés et bloquez l'accès à tous les autres.

Pour les cybercriminels, les identifiants représentent une source de profits inespérée. Assurez-vous que tous vos systèmes Windows ont abandonné les protocoles LM et NTLMv1 hérités, et appliquez nos recommandations pour garantir que vos identifiants Windows sont bien protégés.

Vos données constituent la force vitale de votre entreprise. Contrôlez l'accès à ces données, maintenez à jour l'inventaire de vos fichiers sensibles et confidentiels et, surtout, adoptez le chiffrement par défaut.

Après les serveurs insuffisamment protégés, les personnes sont l'une des principales « ressources » que les cybercriminels cherchent à exploiter, que ce soit par l'ingénierie sociale ou des attaques par phishing. Mettez en place et pérennisez des programmes de sensibilisation des utilisateurs afin de donner à votre personnel les connaissances nécessaires pour qu'il puisse mieux se protéger contre les attaques par phishing. Équipez vos utilisateurs de logiciels automatisés de protection des endpoints qui détectent les malwares même s'ils font l'erreur de cliquer sur un lien malveillant ou subissent un téléchargement automatique (drive-by). Compliquez la tâche des cybercriminels en déployant l'authentification à deux facteurs et l'authentification multifacteur pour l'ensemble des comptes d'utilisateurs.

Les erreurs de configuration ou les mauvaises configurations sont des backdoors involontaires qui ouvrent la porte à une éventuelle compromission. Réalisez une analyse approfondie des autorisations actives sur vos systèmes de stockage et mettez en place des procédures de révision adaptées, capables de prévenir et d'identifier les problèmes de configuration. Combien d'utilisateurs sont autorisés à exploiter des référentiels sans quelque sorte de contrôle ou de validation ? La réponse à cette question devrait être « zéro ».

Enfin, et c'est un refrain connu : appliquez les correctifs disponibles le plus vite possible et le plus souvent possible. Le nombre d'entreprises qui n'appliquent pas les correctifs dans les trois mois suivant la découverte d'une vulnérabilité est suffisamment inquiétant pour que vous ne veniez pas gonfler ces chiffres, et vous avez tout intérêt à ne pas offrir aux cybercriminels un accès aussi facile à vos systèmes.

Conclusion

Ce ne sera un scoop pour personne, mais il est important de le rappeler : la plupart des cybercriminels sont motivés par l'argent. Et comme l'on pouvait s'y attendre, les cybercriminels ont suivi les entreprises dans leur transition vers le cloud. Alors que le modèle de sécurité Zero Trust, sans périmètre défini, se répand dans les entreprises à travers le monde, les cybercriminels continueront de plus que jamais à obtenir des identifiants de connexion. Et comme les entreprises continuent de s'appuyer sur les e-mails et les liens qu'ils peuvent contenir pour permettre à leurs collaborateurs de mener à bien leurs tâches, les cybercriminels continueront de diffuser des liens de phishing pour tirer parti de ces failles.

Les données les plus récentes en matière de compromissions ne font que refléter les pratiques qui ont actuellement cours dans les entreprises. Quelle que soit la direction qu'elles emprunteront, les cybercriminels suivront. Une lutte efficace contre les compromissions passe par la reconnaissance de ce rapport symbiotique, par l'anticipation des risques et par la mise en place de solutions de sécurité, de bonnes pratiques et de processus organisationnels qui font grimper le coût des attaques au-delà de ce que les cybercriminels sont prêts à payer.

Si vous souhaitez découvrir comment SentinelOne peut vous aider à protéger votre entreprise contre les compromissions, contactez-nous dès maintenant ou demandez une démonstration gratuite.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- eBook – Traque des menaces et intervention sur incident sous macOS | Présentation d'Alex Burinskiy
- Faire entrer l'identité dans l'ère du XDR
- Six idées reçues dont devont se méfier les conseils d'administration des entreprises