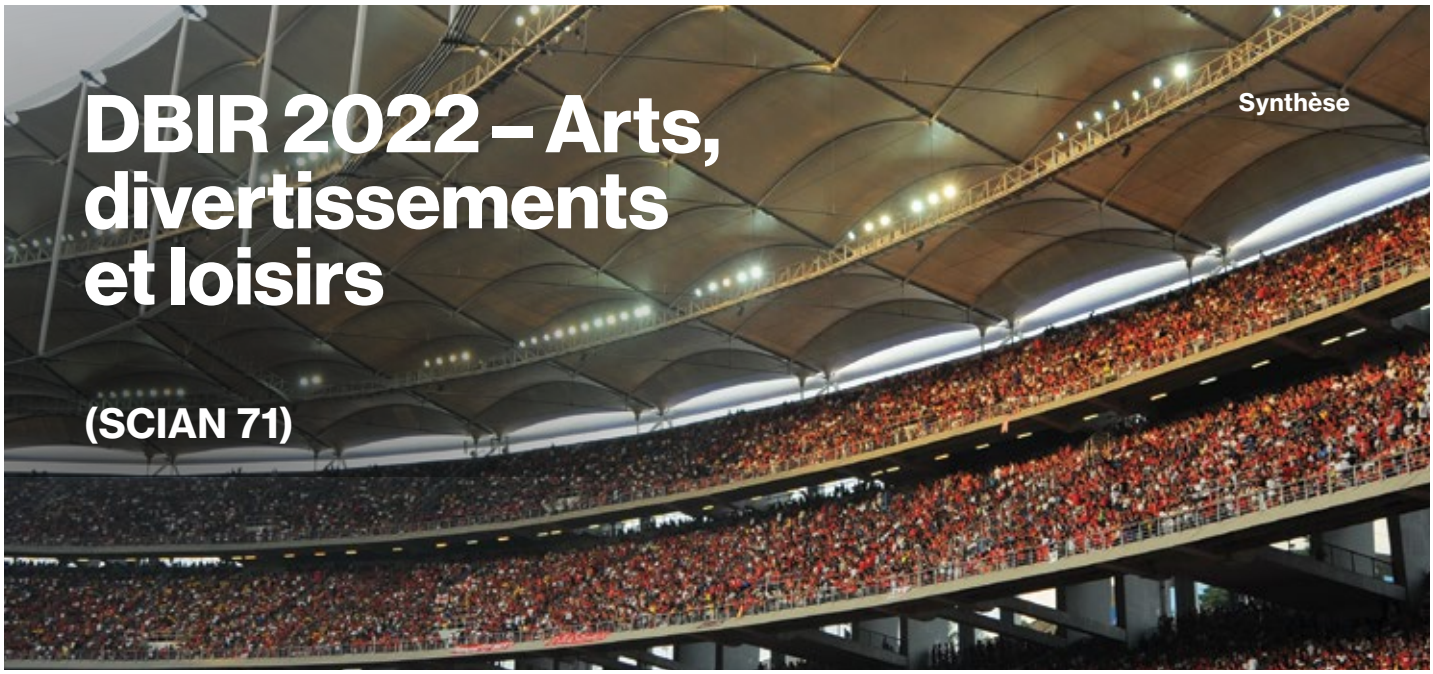

DBIR 2022 – Arts, divertissements et loisirs

Synthèse

(SCIAN 71)

Verizon Data Breach Investigations Report (DBIR) 15e édition : gros plan sur les arts, divertissements et loisirs. Quinze ans déjà depuis la parution de notre tout premier rapport.

Le DBIR dresse un état des lieux des cyberattaques les plus courantes et propose aux entreprises des recommandations pour s'en prémunir. Cette année, notre étude porte sur un total de 23 896 incidents. Le secteur des arts, divertissements et loisirs en recense 215, dont 96 compromissions de données confirmées. Les statistiques proviennent de compromissions et d'incidents sur lesquels le Verizon Threat Research Advisory Center (VTRAC) a enquêté mais aussi de nos 87 contributeurs à travers le monde.

Nous espérons que le DBIR vous éclairera sur les tactiques les plus utilisées contre le secteur des arts, divertissements et loisirs et qu'il aidera votre entreprise à mieux se préparer.

Dans les pages qui suivent, vous découvrirez les principales conclusions du rapport pour ce domaine d'activité. N'hésitez pas à partager cette synthèse avec vos collègues et à télécharger le rapport intégral sur verizon.com/dbir pour un tour d'horizon complet des menaces en 2022.

Notre classification sectorielle pour le rapport DBIR repose sur les codes du Système de classification des industries de l'Amérique du Nord (SCIAN). Ce système utilise des codes de deux à six chiffres pour catégoriser les entreprises. Notre analyse porte généralement sur le niveau à deux chiffres, et nous indiquons le code SCIAN pour chaque intitulé de secteur. De plus amples détails sur les codes et le système de classification sont disponibles ici : census.gov/naics/?58967?yearbck=2012

Classification des incidents

C'est en 2014 que le DBIR a commencé à classer les incidents en différentes catégories afin de refléter les scénarios d'attaque les plus courants. L'année dernière, en raison de l'évolution des types d'attaques et du champ des menaces en général, nous avons modifié et affiné la classification de ces schémas d'attaque, en choisissant de n'en retenir que huit au lieu de neuf.

Ces nouvelles catégories ont été définies au terme d'un processus sophistiqué de clustering par machine learning. 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.

Ingénierie sociale

Manipulation psychologique d'une personne pour l'inciter à agir d'une certaine façon ou à enfreindre des règles de confidentialité.

Le facteur humain reste impliqué dans 82 % des compromissions et l'ingénierie sociale compte pour une grande part d'entre elles. À cela s'ajoutent les malwares et le vol d'identifiants qui constituent généralement la deuxième phase de ce type d'attaques, une fois que l'attaquant s'est engouffré dans la brèche. D'où l'importance d'un solide programme de sensibilisation à la cybersécurité.

- 59 % des attaques par ingénierie sociale s'appuient sur des identifiants compromis et 31 % sur des identifiants volés. Notons que la compromission des identifiants est trois fois supérieure dans les compromissions par ingénierie sociale que dans les autres catégories
- Les actes de phishing sont plus de deux fois plus nombreux que ceux de pretexting
- Les attaques par ingénierie sont huit fois plus souvent motivées par l'appât du gain que par l'espionnage

Attaques d'applications web de base

Attaques d'applications web simples qui ne comportent que quelques étapes ou actions supplémentaires après la compromission initiale.

Ce schéma continue d'être largement dominé par des attaquants utilisant des identifiants volés pour accéder aux infrastructures Internet d'une entreprise, comme les serveurs web ou de messagerie.

- Quatre attaques d'applications web sur cinq impliquent des identifiants volés, un constat qui souligne l'importance de protéger les mots de passe
- L'espionnage est quatre fois plus souvent à l'origine des attaques d'applications web de base (BWAA) que dans les autres schémas. Ce taux élevé prouve que les acteurs étatiques n'ont pas besoin de faire compliqué quand des vecteurs plus simples et plus efficaces leur permettent d'atteindre leurs objectifs
- Dans les compromissions BWAA, l'utilisation d'identifiants volés est six fois plus courante que les exploitations de vulnérabilités

Intrusion système

Cette catégorie renvoie à des attaques complexes qui s'appuient sur des malwares et/ou actes de hacking pour parvenir à leurs fins, y compris le déploiement de ransomwares.

Les intrusions système sont des compromissions et des attaques plus complexes qui combinent plusieurs actions (ingénierie sociale, hacking, malwares, etc.). Les compromissions de la supply chain et les ransomwares, en plein essor cette année, relèvent de cette catégorie.

- 92 % des intrusions système sont motivées par l'appât du gain
- Dans les compromissions de ce type, l'utilisation d'identifiants volés est quatre fois plus courante que l'exploitation de vulnérabilités

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 ».

Les chiffres de cette année montrent à quel point le facteur humain est central, les erreurs d'adressage et de configuration occupant respectivement les deux premières positions. Les erreurs de configuration sont souvent détectées par des chercheurs en sécurité.

- L'exposition accidentelle de serveurs mal configurés sur Internet et l'envoi d'e-mails aux mauvais destinataires (erreur d'adressage) représentent 13 % de l'ensemble des compromissions
- Depuis l'année dernière, les compromissions dues à des erreurs diverses ont diminué de 83 % dans les ressources cloud externes, une baisse qui peut s'expliquer par une migration vers des technologies sécurisées par défaut
- 85 % des compromissions dues à des erreurs diverses impliquent des serveurs

Abus de privilèges

Incidents dus principalement à l'utilisation non autorisée ou malveillante de privilèges légitimes.

La majorité de ces incidents se soldent par des compromissions de données. L'appât du gain demeure la principale motivation des attaquants. Leur cible privilégiée ? Les données personnelles, faciles à monnayer.

- Les documents sont trois fois plus souvent impliqués dans des abus de privilèges que dans les autres schémas

Vol ou perte de ressources

Tout incident impliquant la perte accidentelle ou le vol d'une ressource informatique.

La prévalence des vols s'explique en grande partie par les motivations financières des attaquants, à l'affût du profit immédiat que leur rapporte la revente du matériel volé.

- Le type de données concernées ne varie (quasiment) pas de l'année dernière. Généralement, les vols sont imputables aux acteurs externes, et les pertes de ressources à des collaborateurs internes
- Les attaquants sans aucune affiliation sont quatorze fois plus impliqués dans les vols ou pertes de ressources que dans les autres schémas

Attaques DoS

Attaques ayant pour but de compromettre la disponibilité des réseaux et systèmes. Se rapporte aux attaques des couches réseau et applicative.

Les grandes entreprises sont deux fois plus représentées dans les incidents DoS que dans d'autres types de schémas. Si ce fléau impacte un large éventail de structures, certaines sont ciblées très régulièrement, ce qui peut nuire à leur fonctionnement.

Autres

Cette dernière catégorie rassemble tous les incidents qui ne correspondent pas aux critères des autres schémas.

Arts, divertissements et loisirs

Si les intrusions système et les attaques d'applications web de base ont échangé leur place dans le top 3 des schémas d'attaque ciblant les arts, divertissements et loisirs, les erreurs diverses continuent d'occuper la dernière marche de ce triste podium. Côté incidents, les attaques par déni de service demeurent un problème pour le secteur, surtout sur le marché des jeux d'argent.

Évolution sur la durée	Évolution en cinq ans	Évolution en trois ans	Évolution par rapport aux autres secteurs
Attaques d'applications web de base	statu quo	statu quo	statu quo
Intrusion système	statu quo	statu quo	baisse
Erreurs diverses	statu quo	statu quo	hausse

Volume	215 incidents, dont 96 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web de base, l'intrusion système et les erreurs diverses représentent 80 % des compromissions.
Attaquants	Externes (74 %), internes (26 %) (compromissions)
Motivations	Financières (97 %), représailles (3 %) (compromissions)
Données compromises	Données personnelles (66 %), identifiants (49 %), autres (23 %), données médicales (15 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4), Gestion du contrôle des accès (CSC 6)
Ce qui n'a pas changé	Les catégories restent les mêmes. Seul l'ordre change. La compromission des données médicales demeure un risque majeur dans ce secteur.

Concerts, théâtre, sports… le direct représente le principal dénominateur commun d'un domaine très varié où tout est en live, et donc sans filet. Les jeux d'argent constituent l'autre volet. Autant dire qu'avec une telle diversité d'entreprises, le SCIAN 71 se distingue par la pluralité de ses surfaces d'attaque. Aussi différentes soient-elles, nombre de ces organisations partagent néanmoins une caractéristique : la dépendance d'une partie plus ou moins importante de leur infrastructure à Internet pour réaliser des opérations essentielles du type billetterie, prise de commandes, et même de paris en ligne selon les cas. Pour tous les acteurs du secteur, une chose est sûre : les attaques DoS tombent toujours mal. Et elles tombent d'autant plus mal qu'elles sont très fréquentes, avec plus de 20 % des incidents recensés dans ce secteur, les entreprises de jeux d'argent de la région Asie-Pacifique étant particulièrement touchées.

Par ailleurs, la forte présence des attaques d'applications web de base est inquiétante vu leur caractère plutôt élémentaire. À l'inverse, celles par intrusion système requièrent bien plus d'efforts et d'habileté de la part des attaquants. Dans cette catégorie, le ransomware reste l'outil de prédilection. Comme nous l'avons vu par le passé, les identifiants ont toujours la cote auprès des cybercriminels. Ce précieux sésame leur permet de se faire passer pour des collaborateurs légitimes, opérant ainsi à couvert pendant tout le temps nécessaire pour faire main basse sur l'objet de leur convoitise.

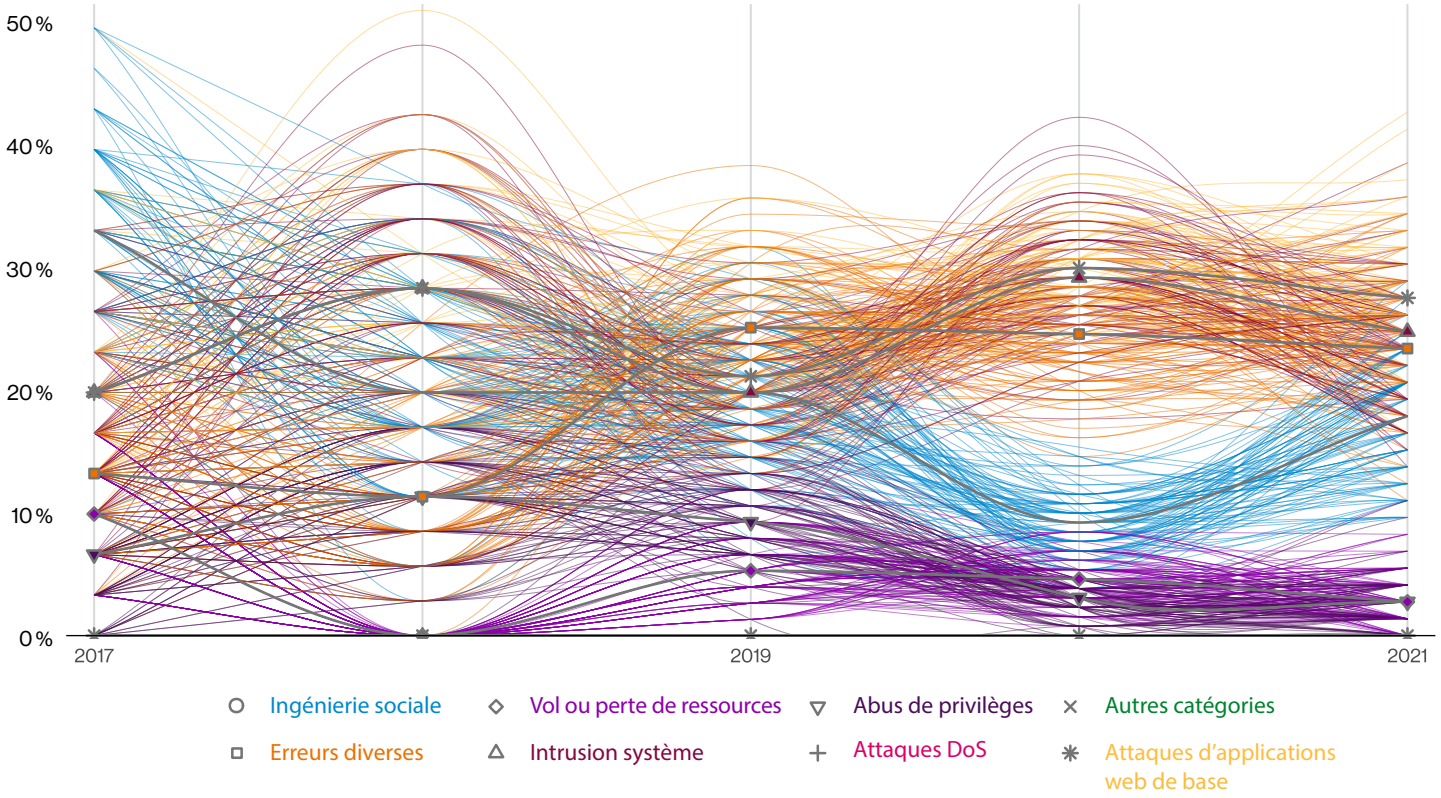

Figure 1. Évolution chronologique des schémas d'attaque à l'origine de compromissions dans les arts, divertissements et loisirs

Au rang des données les plus convoitées figurent les informations à caractère personnel (même si en baisse par rapport à leur record de 83 % l'année dernière) et les identifiants. Étrangement, les attaquants continuent de faire main basse sur les données médicales, et ce dans 15 % des compromissions de ce secteur. Même si c'était déjà le cas l'année dernière (avec un taux de 26 %), ce type de données demeure pour le moins déconcertant dans un domaine d'activité sans aucun lien avec le milieu médical. À cela, on pourrait avancer deux hypothèses. Soit les informations dérobées proviennent d'entreprises qui s'auto-assurent pour les besoins médicaux de leurs salariés, et ont donc besoin de conserver ce type de renseignements sur leurs systèmes. Soit elles sont issues des dossiers RH (à la suite d'accidents du travail). Autre piste éventuelle : les dossiers médicaux subtilisés pourraient provenir d'équipes sportives qui rentrent dans ce secteur d'activité. Quoi qu'il en soit, ces observations sont pour le moins surprenantes.

Cette année encore, les erreurs diverses se classent dans le trio de tête des schémas d'attaque (25 %). Dans cette catégorie, les erreurs de configuration sont les plus courantes et représentent environ 15 % des cas de compromission. Il semblerait que ce secteur se soit contenté d'échanger un problème contre un autre, puisque les erreurs d'adressage (en première position l'an passé) ont fortement chuté.

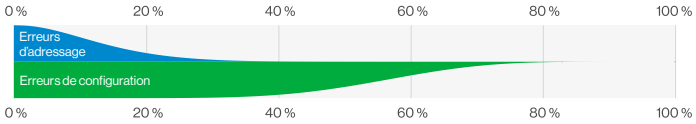

Figure 2. Proportion des erreurs d'adressage vs. erreurs de configuration dans les compromissions liées à des erreurs dans le secteur des arts et divertissements (n=16)

Des données dignes de confiance

Depuis 2019, le DBIR adopte les graphiques à barres obliques pour démontrer qu'en matière de sécurité de l'information, la seule certitude c'est que rien n'est certain.

Le degré d'inclinaison représente le degré d'incertitude du point de données à un niveau de confiance de 95 % (typique dans le domaine des statistiques).

Dans la même veine, les diagrammes spaghetti, et plus récemment les graphiques à pictogrammes, tentent de rendre compte de cette part d'incertitude, même s'ils conviennent mieux à une proportion unique.

S'informer, c'est se préparer

Pour faire face aux cybermenaces qui pèsent actuellement sur le secteur des arts, divertissements et loisirs, vous devez pouvoir compter sur une information fiable. Le rapport DBIR vous présente des données réelles sur les acteurs, tendances et modes opératoires pour vous aider à mieux vous protéger et sensibiliser vos salariés.

Lisez le rapport DBIR 2022 complet sur verizon.com/dbir/