

# DBIR 2022 – Finance et assurance

Synthèse

(SCIAN 52)

## Verizon Data Breach Investigations Report (DBIR) 15<sup>e</sup> édition : gros plan sur la finance et les assurances. 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 financier en recense 2 527, dont 690 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 les services financiers 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](https://www.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](https://www.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.

## Finance et assurance

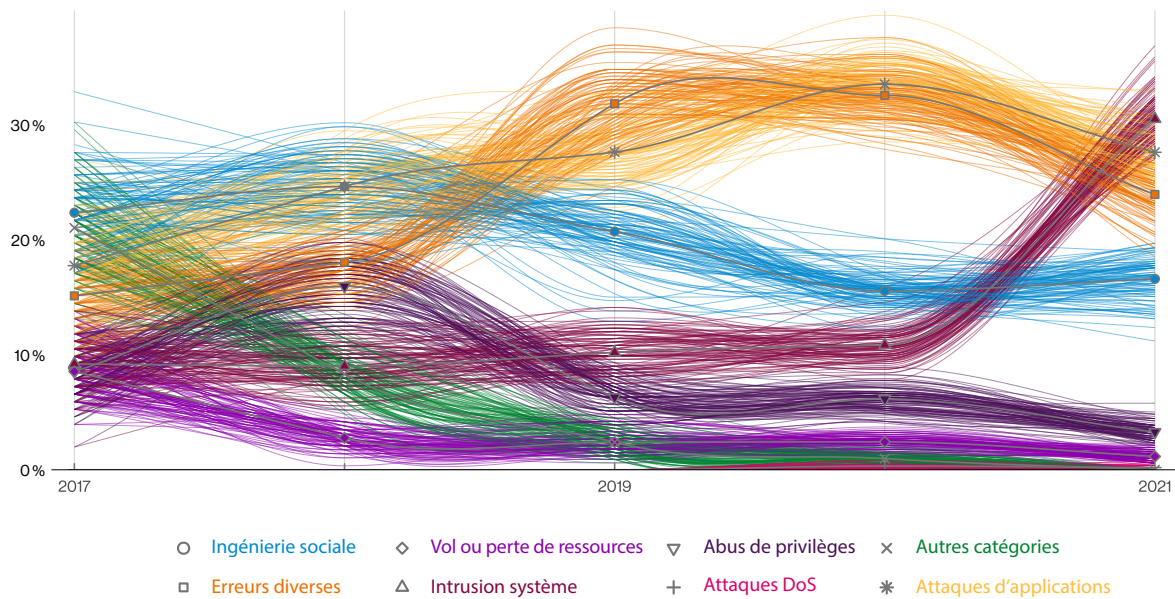
Les établissements financiers et les compagnies d'assurance continuent de subir les assauts du crime organisé, attiré par la manne qu'ils représentent. Ses armes de prédilection : l'ingénierie sociale (phishing), le hacking (utilisation d'identifiants volés) et les malwares (ransomwares). Par ailleurs, les erreurs diverses (souvent des erreurs d'adressage) sont très courantes depuis trois ans.

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

En 2016, les serveurs étaient impliqués dans 50 % des compromissions de ce secteur, contre 90 % actuellement. Cependant, nous observons un bond dans la sous-catégorie « Serveur – applications web », qui est passée de 12 % à 51 % sur le même laps de temps. D'où la présence des attaques d'applications web de base (BWAA) dans le trio de tête des schémas d'attaque. Ce type de compromissions repose très souvent sur l'utilisation d'identifiants volés, qui constitue d'ailleurs le vecteur n°1 dans ce secteur. S'il existe de nombreuses tactiques pour obtenir ces identifiants, les attaques par force brute et le « credential stuffing » sont les coupables les plus probables. Une chose est sûre, identifiants volés et applications web font très bon ménage.

<b>Volume</b>	2 527 incidents, dont 690 compromissions de données confirmées
<b>Principaux schémas</b>	Les attaques d'applications web de base, l'intrusion système et les erreurs diverses représentent 79 % des compromissions.
<b>Attaquants</b>	Externes (73 %), internes (27 %) (compromissions)
<b>Motivations</b>	Financières (95 %), espionnage (5 %) (compromissions)
<b>Données compromises</b>	Données personnelles (71 %), identifiants (40 %), autres (27 %), bancaires (22 %) (compromissions)
<b>Principaux contrôles de sécurité IG1</b>	Programme de sensibilisation et de formation à la sécurité (CSC 14), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4), Protection des données (CSC 3)
<b>Ce qui n'a pas changé</b>	Comme l'année dernière, les erreurs diverses et les attaques d'applications web de base restent une source majeure de compromission dans ce secteur.





**Figure 1.** Évolution chronologique des schémas d'attaque à l'origine de compromissions dans le secteur de la finance et des assurances

### Des erreurs qui coûtent cher

Les « erreurs d'adressage » (16 %) arrivent en deuxième position des actes les plus susceptibles de provoquer une compromission dans ce secteur. Comme le nom le laisse entendre, des informations à caractère personnel ou autres données sensibles sont envoyées par inadvertance aux mauvais destinataires. On s'attendrait plutôt à trouver ce genre de méprises dans le secteur public ou la santé, où le volume de correspondance est très important du fait de la nature même de leurs activités. Or, selon nos données, ces erreurs d'adressage s'avèrent environ trois fois plus nombreuses dans les services financiers que dans les autres secteurs. Un constat pour le moins surprenant et inquiétant, compte tenu de la nature très sensible des données financières.

### Les temps changent

Les intrusions système ont doublé depuis 2016, passant de 14 % à 30 % cette année. La part de responsabilité du crime organisé dans ces compromissions atteint 79 % cette année, contre seulement 49 % en 2018. Les conséquences des compromissions sur la disponibilité s'élèvent à 14 % aujourd'hui, contre seulement 6 % en 2016. Quant au mode de détection « divulgation par l'attaquant », elle atteint aujourd'hui 58 % par rapport aux 5 % de 2016. Il va sans dire que cette évolution est principalement due à l'explosion des attaques pas ransomware.

Tant que ce filon restera lucratif et peu risqué, les cybercriminels continueront de l'exploiter.

Enfin, nous aurions tort de passer sous silence les attaques DoS qui demeurent un véritable fléau. Elles constituent 58 % des incidents de sécurité dans ce secteur, soit près du double des attaques DoS recensées dans d'autres domaines d'activité.

### 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 financier, 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/](https://www.verizon.com/dbir/)**