Devolutions

# Les plus grandes violations de données de 2020

## LES PIRATES, EUX, NE SONT PAS PASSÉS EN « MODE CONFINEMENT »

Il va sans dire que la plus grande histoire de 2020 – ou du 21e siècle tout court – était la pandémie de coronavirus. Alors que cette crise faisait rage, les pirates, eux, ne sont pas passés en « mode confinement » pour autant. Ils ont plutôt accéléré le rythme de leurs attaques.

Ci-dessous, nous mettons en évidence certaines des plus grandes violations de données de 2020. Notez que les dates suivantes ne sont pas toujours celles où les violations se sont produites initialement, mais plutôt quand elles ont été découvertes et révélées publiquement pour la première fois.

## Janvier

- Le bureau de change londonien Travelex a été déconnecté en raison d'un logiciel malveillant.
- Un district scolaire du Texas a été escroqué de 2,3 millions de dollars en raison d'une attaque par hameçonnage.
- Une brèche de données généralisée dans la chaîne de magasins de proximité américaine Wawa a révélé les informations sensibles de millions de clients.
- Une faille sur la plateforme éducative en ligne Unacademy a révélé plus de 20 millions de comptes d'utilisateurs.

## Février

- Une brèche de données chez Estée Lauder a révélé plus de 440 millions de dossiers.
- Twitter a suspendu un vaste réseau de faux comptes utilisés pour associer les numéros de téléphone aux utilisateurs.
- L'agence de défense des systèmes d'information des États-Unis a été victime d'une violation de données qui a révélé les détails personnels d'environ 200 000 personnes.
- La liste complète des clients de Clearview AI a été volée lors d'une violation de données.
- General Electric a averti ses employés qu'une personne non autorisée pouvait accéder à leurs informations sensibles en raison de défaillances de sécurité avec un fournisseur.
- MGM Resorts a révélé que les données personnelles de plus de 142 millions de clients qui ont séjourné dans les propriétés de la société en 2019 avaient été publiées sur le dark web. Le nombre de clients concernés était initialement de 10,6 millions, mais il a depuis été révisé.

## Mars

- Une faille chez le fournisseur de télécommunications T-Mobile a permis aux pirates d'accéder aux données des employés et des clients. Note : début janvier 2021, T-Mobile a révélé une autre faille qui exposait potentiellement les numéros de téléphone et les enregistrements d'appels des clients.
- La chaîne d'hôtels Marriott a subi une cyberattaque qui a touché 5,2 millions de clients. En 2019, des pirates ont volé les données personnelles de plus de 383 millions de clients Marriott après avoir infiltré le système de réservation de l'hôtel.

- L'application de partage de secrets anonyme Whisper a été piratée, exposant les profils privés de millions d'utilisateurs.
- Le réseau social Weibo a été piraté et les données personnelles de plus de 538 millions d'utilisateurs ont été volées puis mises en vente sur le ***dark web***.
- Une faille chez Virgin Media a révélé les données de 900 000 utilisateurs, dont les informations privées sont restées non sécurisées et accessibles en ligne pendant 10 mois.
- Le site pour adultes CAM4.com a laissé son serveur de production sans protection, ce qui a exposé 10,88 milliards de dossiers.
- Advanced Info Service, un opérateur de réseau mobile basé en Thaïlande, a laissé sa base de données exposée et accessible au public, ce qui a entraîné la fuite de 8 milliards de dossiers.
- Antheus Tecnologia, une société de biométrie basée au Brésil, a laissé des informations sensibles exposées sur un serveur non sécurisé, dont 76 000 enregistrements d'empreintes digitales uniques.

## Avril

- La U.S. Small Business Association a révélé que jusqu'à 8 000 demandeurs de prêts d'urgence peuvent avoir vu leurs renseignements personnels exposés.
- 300 000 utilisateurs ont été touchés par une campagne de piratage massif de comptes chez Nintendo.
- Une faille chez le fournisseur de messagerie Email.it a conduit à la mise en vente des données de 600 000 utilisateurs sur le ***dark web***.
- Plus de 500 000 comptes Zoom ont été piratés puis offerts sur le ***dark web***.
- Magellan Health a été victime d'une attaque de rançongiciel au cours de laquelle plus de 365 000 dossiers de patients ont été compromis.

## Mai

- Une brèche chez la compagnie aérienne à bas prix EasyJet a révélé les données de 9 millions de clients, y compris certains dossiers financiers.
- Une attaque par rançongiciel contre le fournisseur de services infonuagiques Blackbaud a pu avoir un impact sur des centaines d'organisations à but non lucratif (et qui a par la suite conduit à 23 propositions de recours collectifs auprès des consommateurs).
- Des pirates ont volé 220 gigaoctets de données lors d'une attaque de rançongiciel contre le groupe de transport australien Toll Group.

- Une violation de l'application de vote et sondage Wishbone a conduit à la mise en vente des données de 40 millions d'utilisateurs sur le ***dark web***.

## Juin

- L'entreprise de marketing spécialisée en médias sociaux Preen.Me a révélé que les données personnelles d'environ 100 000 influenceurs avaient été divulguées. La même violation a également mené à la publication des données de 250 000 utilisateurs de médias sociaux sur un forum de piratage du ***dark web***.
- Amtrak a révélé que des pirates informatiques avaient enfreint le système de récompenses Amtrak Guest Rewards et accédé aux données des clients.
- L'Université de Californie à San Francisco a versé 1,14 million de dollars à des pirates informatiques lors d'une attaque par rançongiciel.
- Des employés malhonnêtes de la banque sud-africaine Postbank ont volé les données personnelles de millions de titulaires de comptes.
- Une campagne de clonage de cartes dans la société d'accessoires Claire's a permis à des pirates de récupérer des informations sensibles sur les clients.
- Wattpad a subi une violation de données qui a exposé près de 271 millions de dossiers.

## Juillet

- L'Université d'York a révélé une violation de données qui a conduit au vol des dossiers du personnel et des étudiants. L'université a blâmé son fournisseur de plateforme infonuagique Blackbaud, mentionné ci-dessus.
- Une brèche dans la célèbre agence de casting en ligne MyCastingFile a révélé les données personnelles de plus de 260 000 utilisateurs.
- Une brèche dans l'entreprise de fitness V Shred a révélé les données personnelles de près de 100 000 utilisateurs.
- Le fournisseur d'énergie EDP a révélé que plus de 10 To de documents commerciaux avaient été volés en raison d'un incident de rançongiciel.
- Les comptes Twitter de certaines des personnalités les plus connues au monde ont été compromis par des pirates informatiques qui ont utilisé des attaques de harponnage pour générer du trafic vers des escroqueries Bitcoin.

## Août

- Une base de données de près de 235 millions de profils de réseaux sociaux connectés à Instagram, TikTok et YouTube a été exposée et non protégée par des mots de passe ou tout autre type d'authentification.
- Un ingénieur en sécurité de Cisco a piraté son employeur, ce qui a coûté 2,4 millions de dollars à l'entreprise. Le vilain a ensuite été condamné à deux ans de prison.
- YouTube a supprimé 2 millions de chaînes et 51 millions de vidéos à la suite d'escroqueries.
- Canon a révélé qu'il avait été victime d'une attaque de rançongiciel et que des pirates avaient volé des données sur le serveur de l'entreprise.
- Le même groupe de pirates (Maze) qui a attaqué Canon avec un rançongiciel a aussi frappé LG et Xerox.
- 20 Go de données sensibles d'entreprises – y compris des documents et enregistrements marqués comme confidentiels et secrets appartenant à Intel – ont été publiés en ligne.
- Une brèche à l'hôtel de luxe The Ritz London a permis à des pirates de mener des attaques d'hameçonnage convaincantes contre des clients.
- Une violation de données de l'application de photos gratuites Freepik a révélé les données de 8,3 millions d'utilisateurs.
- Une attaque de rançongiciel à l'Université de l'Utah a contraint l'institution à payer plus de 450 000 dollars pour empêcher les pirates de publier des informations sur les étudiants.
- La succursale d'Experian en Afrique du Sud a révélé une violation de données impliquant 24 millions d'utilisateurs.
- L'opérateur de croisière Carnival a été victime d'une attaque de rançongiciel qui a affecté les clients de trois compagnies de croisière différentes (Carnival Cruise Line, Holland America Line et Seabourn).

## Septembre

- Une école du Nevada a refusé de céder aux demandes de rançongiciel et, en représailles, des pirates ont publié en ligne des données sur les élèves.
- Un hôpital en Allemagne a été victime d'une attaque de rançongiciel. Initialement, il a été annoncé que cette attaque avait entraîné la mort d'un patient, mais une enquête a conclu que la patiente en question était en si mauvaise santé que sa mort n'était probablement pas attribuable à l'attaque. Néanmoins, la police affirme que ce n'est qu'une question de temps avant que le rançongiciel n'entraîne la perte de vies.

- La banque chilienne BancoEstado a été contrainte de fermer temporairement toutes ses succursales en raison d'une attaque de rançongiciel.
- La société de marketing par courriel Mailfire a été frappée par une cyberattaque qui a révélé plus de 320 millions de dossiers provenant de plus de 70 sites Web.

## Octobre

- Une attaque par rançongiciel contre le libraire Barnes & Noble a révélé l'historique des transactions des clients et leurs adresses courriel.
- L'Organisation maritime internationale des Nations Unies a été frappée par ce qu'elle a appelé une « cyberattaque sophistiquée » contre ses systèmes informatiques.
- Le fournisseur de services de télécommunications Boom! Mobile a été victime d'une attaque de clonage de cartes.
- La chaîne de restaurants américaine Dickey a révélé qu'entre juillet 2019 et août 2020, plus de trois millions de ses clients ont vu les détails de leur carte affichés en ligne.
- Le groupe de rançongiciel Egregor a frappé Ubisoft et Crytek et a publié des informations sensibles de ces entreprises en ligne.

## Novembre

- La société de technologie d'assurance Vertaforce a révélé une violation de données entre mars 2020 et août 2020 qui a potentiellement exposé les informations sensibles de 27,7 millions de clients.
- La société de boissons Campari a été temporairement mise hors ligne après une attaque par rançongiciel. La société a révélé qu'une violation de données avait potentiellement touché environ 6 000 anciens et actuels employés, ainsi que plus de 10 000 clients et fournisseurs.
- Le groupe de pirates ShinyHunters a divulgué la base de données appartenant à Mashable.com, exposant plus de 5,2 Go de données.
- Le fabricant de jeux vidéo Capcom a été touché par une attaque par rançongiciel qui a potentiellement compromis les données de près de 400 000 utilisateurs.
- L'entreprise aérospatiale brésilienne Embraer a été victime d'une cyberattaque qui a entraîné un vol de données.

## Decembre

- Flight Center a révélé qu'un hackathon en 2017 était responsable d'une fuite impliquant les données de cartes de crédit et les numéros de passeport de près de 7 000 clients.
- Une attaque par rançongiciel à Vancouver TransLink a perturbé les transactions et la billetterie pendant deux jours.
- Un employé malhonnête de la banque sud-africaine Absa a vendu les informations personnelles de 200 000 clients à des tiers.
- Le bureau des impôts britannique HMRC a été accusé d'être « incompétent » à la suite de 11 violations de données graves qui ont touché près de 24 000 personnes.
- Leonardo SpA, le plus grand entrepreneur de défense au monde, a été touché par une attaque de logiciel malveillant qui a exfiltré jusqu'à 10 Go de données.
- Des pirates ont inséré du code malveillant dans une mise à jour du logiciel SolarWinds, appelé Orion. Ce piratage s'appelle une attaque de la chaîne d'approvisionnement, parce qu'il infecte le logiciel lors de son assemblage. SolarWinds a déclaré qu'environ 18 000 clients ont installé la mise à jour contaminée sur leurs systèmes. Ces attaques doivent être prises au sérieux et sont très puissantes. Cette attaque a eu (et a toujours) un impact énorme, alors qu'on découvre encore de nouvelles informations au fil du temps.

## Et cette année...

Les pirates ont volé ou exposé des milliards de données l'année passée. Cette année, l'attaque se poursuivra – en particulier contre les PME. Heureusement, les PME peuvent faire quelque chose pour protéger leurs données et leur réputation.