Statistiques de cybersécurité pour 2023 que vous devez savoir où, qui et quoi est ciblé

Nicole Kolesnikov ⁝

La cybersécurité est devenue indispensable à nos vies numériques dans notre monde interconnecté.
Alors que la technologie progresse et que les organisations s'appuient de plus en plus sur les systèmes numériques, la protection des données sensibles, la préservation de la confiance des clients et la garantie d'opérations ininterrompues sont devenues des objectifs critiques.

Du nombre croissant de violations de données aux pertes financières subies par les entreprises et à la sophistication croissante des pirates informatiques, notre liste organisée de statistiques sur la cybersécurité souligne l'urgence de mesures de cybersécurité robustes.
Cet article se penchera sur des données révélatrices sur la cybersécurité, mettant en lumière nos défis et soulignant l'importance de protéger nos actifs numériques.

Statistiques clés sur la cybersécurité

- En 2022, 493,33 millions d'attaques de ransomware ont été détectées par des organisations du monde entier.
- L'hameçonnage reste la cyberattaque la plus courante, avec environ 3,4 milliards de spams quotidiens.
- Le coût moyen mondial des violations de données était de 4,35 millions de dollars en 2022.
- En 2022, le coût moyen des atteintes résultant de justificatifs d'identité volés ou compromis s'élevait à 4,50 millions de dollars.
- Le secteur de la santé a été le plus coûteux en matière de violations pendant 12 années consécutives, avec un coût moyen des violations de données atteignant 10,10 millions de dollars en 2022.

Statistiques de cybersécurité par type d'attaque

Dans le paysage en constante évolution de la cybersécurité, il est crucial de rester informé des diverses cyberattaques qui menacent les individus et les organisations. L'impact de ces attaques est considérable, tant en termes de pertes financières que de réputation.

Le rapport du FBI sur la criminalité sur Internet pour 2022 a révélé que le public avait signalé un total de 800 944 plaintes en matière de cybercriminalité.

Les attaques d'hameçonnage **étaient le type de crime numéro un, avec 300 497 plaintes signalées.**
Les pertes totales dues aux attaques de phishing ont dépassé 10,3 milliards de dollars.

2022 CRIME TYPES

By Victim Count

Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

*Descriptors**			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

Données d'attaque de phishing

Les attaques de phishing restent la cyberattaque la plus courante, avec environ 3,4 milliards de spams quotidiens.
Ils englobent diverses techniques trompeuses pour inciter les individus à révéler des informations sensibles ou à se livrer à des activités malveillantes par le biais de courriels ou de sites Web déguisés.

Les attaques de phishing sont responsables de 90% des violations de données.
En effet, les hameçonneurs supposent souvent l'identité d'une entité fiable et crédible dans les communications électroniques.

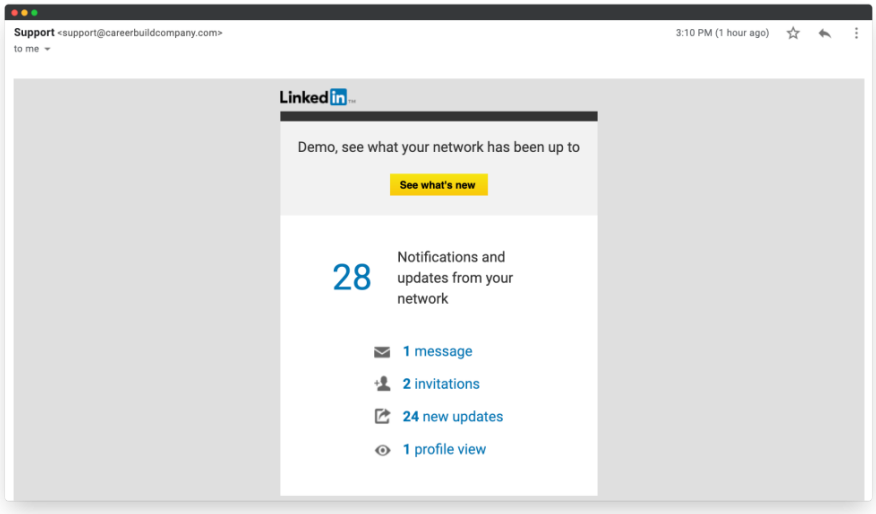
Type d'hameçonnage	Détails	But
Hameçonnage par courriel	Les attaquants usurpent l'identité d'entités de confiance et créent des courriels convaincants qui semblent souvent urgents ou importants.	• Obtenez un accès non autorisé aux données sensibles. • Effectuer un vol d'identité. • Mener d'autres activités malveillantes.
Spear phishing	Les attaquants personnalisent leurs techniques d'attaque pour faire paraître les courriels ou les messages frauduleux hautement légitimes et dignes de confiance.	• Rassemblez des informations sur les cibles pour créer des e-mails personnalisés. • Voler les identifiants de connexion.
Cloner le phishing	Implique la création d'une copie frauduleuse, ou clone, d'un courriel ou d'un site Web légitime.	• Commettre des fraudes financières. • Exploitez pour le vol d'identité.
Chasse à la baleine	Cible les cadres supérieurs ou les personnes occupant des postes d'autorité au sein d'une organisation.	• Gain financier. • Accès aux données d'entreprise et aux secrets commerciaux.
Pop-up	Se produit par l'utilisation de fenêtres contextuelles décevantes ou de boîtes de dialogue.	• Persuadez les utilisateurs d'entrer leurs informations personnelles.

Selon les statistiques de Norton, environ 88% des organisations rencontrent des attaques de spear phishing dans l'année.
Ces données indiquent que les entreprises sont ciblées presque quotidiennement.

Un rapport du 1er trimestre 2022 publié par Check Point Research a révélé une liste des meilleures marques classées en fonction de leur apparence globale dans les tentatives de phishing de marque.

1. LinkedIn (concernant 52 % de toutes les attaques de phishing dans le monde)
2. DHL (14%)
3. Google (7 %)
4. Microsoft (6 %)
5. FedEx (6 %)
6. WhatsApp (4 %)
7. Amazon (2 %)
8. Maersk (1%)
9. AliExpress (0,8 %)
10. Apple (0,8 %)

LinkedIn était lié à 52% des attaques liées au phishing dans le monde.
Ce chiffre significatif représente la première fois qu'une plateforme de médias sociaux revendique la première place du classement, ce qui indique la gravité du problème.
Voici un exemple d'un courriel de phishing LinkedIn typique :



Au 4e trimestre 2022, Yahoo a connu une hausse notable de **23 positions à 20% en raison d'une campagne de phishing efficace au trimestre précédent.**
LinkedIn est tombé au cinquième rang de la liste avec une apparition globale de 5,7% dans les tentatives de phishing de marque.

Avec l'essor du travail à distance, il y a eu une augmentation des escroqueries de **compromission des e-mails professionnels (BEC).**
Ces escrocs emploient des tactiques d'hameçonnage par courriel pour tromper les individus en leur permettant de divulguer des informations confidentielles sur l'entreprise ou d'effectuer des transferts d'argent non autorisés.

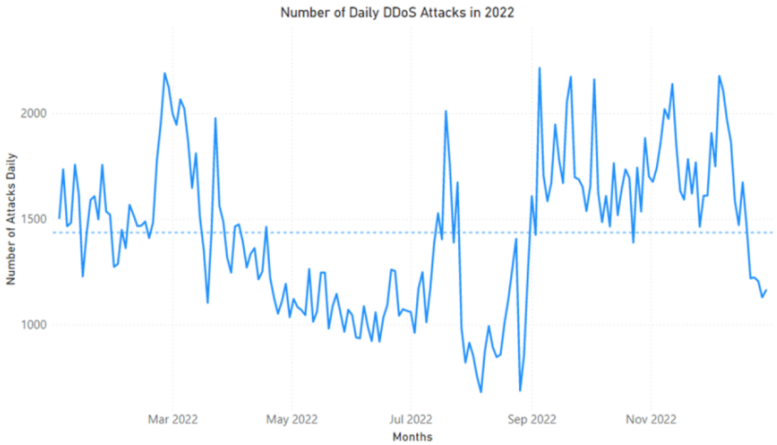
En 2022, **IC3 a enregistré 21 832 plaintes liées à BEC, ce qui a entraîné des pertes ajustées de plus de 2,7 milliards de dollars.**

Données par déni de service distribué (DDoS)

Une attaque par déni de service distribué (DDoS) **est une tentative malveillante de perturber le fonctionnement normal d'un réseau, d'un service ou d'un site Web en le submergeant d'un flot de trafic Internet.**
Une attaque DDoS vise à perturber ou à neutraliser les ressources et l'infrastructure de la cible, entraînant des temps d'arrêt de service et des pertes financières potentielles.

En 2022, Microsoft a atténué en moyenne 1 435 attaques DDoS par jour.

- Le nombre maximum d'attaques quotidiennes était de 2 215 le 22 septembre 2022.
- Le nombre minimum d'attaques quotidiennes était de 680 le 22 août 2022.
- Le nombre total d'attaques uniques atténuées en 2022 était supérieur à 520 000.



Selon un rapport publié par Cloudflare, les **attaques DDoS contre rançon ont connu une augmentation de 67% en glissement annuel et une augmentation trimestrielle de 24%.**

Les industries en ligne ont connu une augmentation significative des attaques DDoS de la couche applicative, avec une augmentation trimestrielle de 131% et une augmentation de 300% en glissement annuel.

En septembre 2017, une attaque DDoS record a ciblé les services Google, atteignant une taille énorme de 2,54 Tbps.
Google Cloud a révélé cet incident en octobre 2020.

L'attaque a été attribuée à la Chine et a été trouvée pour provenir du réseau de quatre fournisseurs de services Internet chinois.
Les pirates ont envoyé des paquets usurpés à 180 000 serveurs Web, qui ont envoyé des réponses à Google.

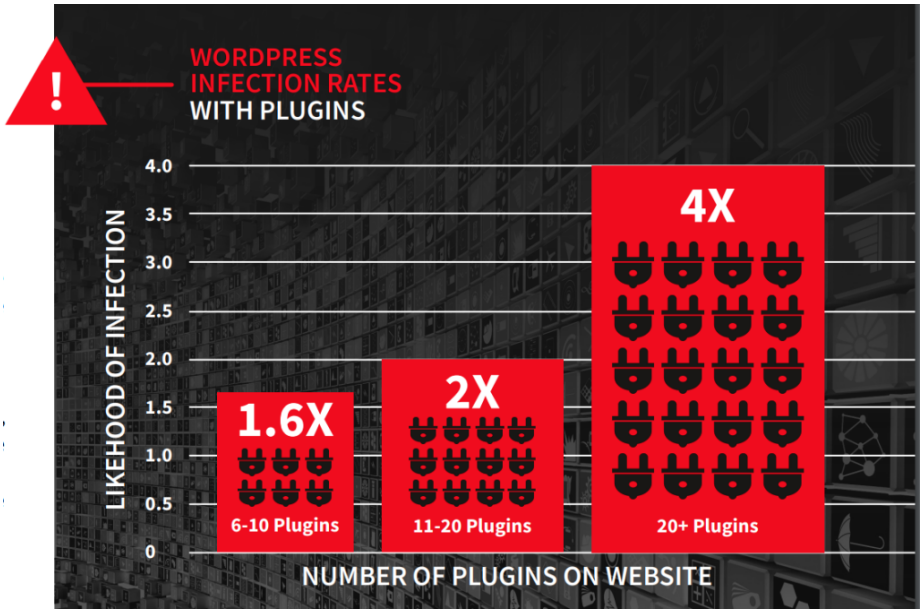
L'une des attaques DDoS les plus importantes a eu lieu en mars 2023.
Le site de l'Assemblée nationale française a connu une panne temporaire en raison d'une attaque DDoS orchestrée par des pirates russes. Dans un post Telegram, les pirates ont attribué l'attaque au soutien du gouvernement français à l'Ukraine.

Données sur les logiciels malveillants

En 2023, **300 000 nouvelles instances de logiciels malveillants sont générées quotidiennement, dont 92% sont distribuées par courriel, avec une moyenne de 49 jours pour être détectés.**
Les logiciels malveillants sont utilisés pour obtenir un accès non autorisé aux systèmes informatiques, voler des données, perturber les services système ou endommager les réseaux informatiques.

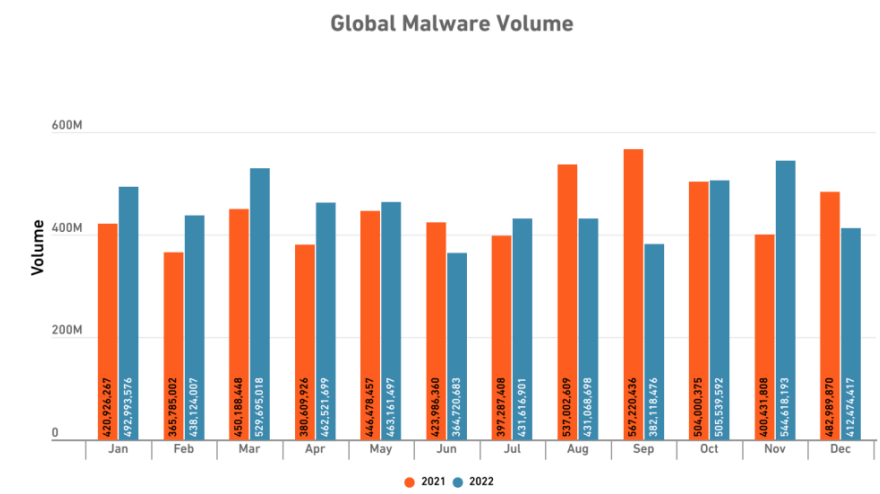
4,1 millions de sites Web sont infectés par des logiciels malveillants.
Et 18% des sites Web contiennent des menaces critiques pour la cybersécurité.

De plus, 97% **de toutes les failles de sécurité sur les sites Web exploitent les plugins WordPress.**
Sur les 47 337 plugins malveillants installés de 2012 à 2021, 94% étaient actifs sur 24 931 sites WordPress différents, chacun hébergeant deux plugins malveillants ou plus.



Selon le rapport 2023 sur les cybermenaces de **SonicWall**, **les logiciels malveillants ont connu leur première augmentation depuis 2018, atteignant 5,5 milliards d'attaques, soit une augmentation de 2 % d'une année sur l'autre.**
Bien que la légère augmentation, la montée en flèche des taux de cryptojacking et de logiciels malveillants IoT a largement entraîné la hausse substantielle.

En 2022, le cryptojacking a connu une augmentation de 43%, tandis que les logiciels malveillants IoT ont connu une augmentation stupéfiante de 87%.
Les gains combinés dans le cryptojacking et les logiciels malveillants IoT ont compensé la baisse du volume mondial de ransomwares, entraînant un changement positif dans les tendances globales des logiciels malveillants pour la première fois depuis 2018.

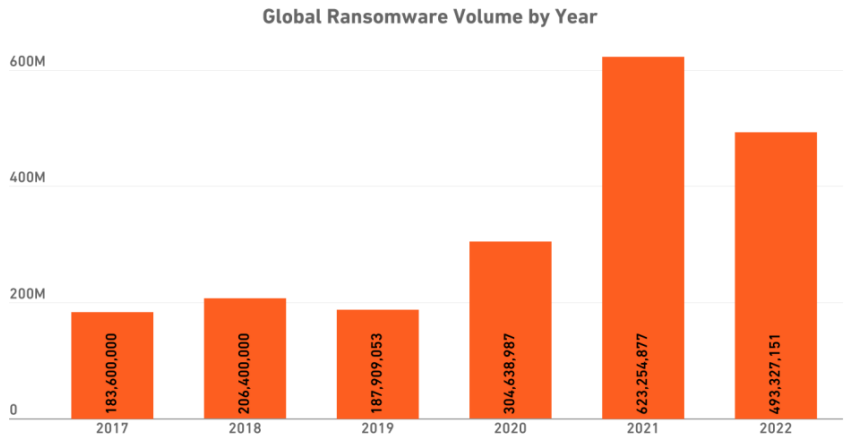


Données de ransomware

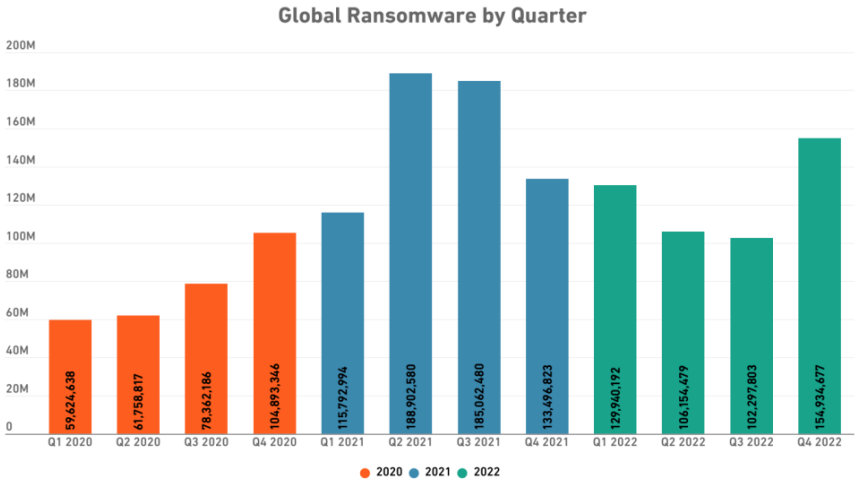
Dans le domaine des logiciels malveillants, les rançongiciels se distinguent comme un type spécifique qui tient en otage les données ou les systèmes ciblés jusqu'à ce que la victime fasse une rançon.

Selon SonicWall, il y a eu 493,3 millions de tentatives de ransomware en 2022, ce qui démontre une baisse notable de 21% observée d'une année sur l'autre.
En 2020, il y a eu une augmentation de 62 % et une augmentation supplémentaire de 105 % en 2021.

Cependant, ces types de cyberattaques représentaient encore 12% des atteintes aux infrastructures critiques **en 2022,** ce qui les rend responsables de plus d'un quart des atteintes dans les industries des infrastructures critiques.



Malgré une légère baisse d'un peu plus d'un cinquième, 2022 reste la deuxième année la plus élevée jamais enregistrée pour les attaques mondiales de ransomware.



En outre, les chiffres pour 2022 sont beaucoup plus proches des niveaux extraordinairement élevés observés en 2021 qu'ils ne le sont des années précédentes.
Ils ont dépassé les volumes observés en 2017 (+155%), 2018 (+127%), 2019 (+150%) et 2020 (+54%) par des marges significatives.

Comparitech a rapporté les principales conclusions suivantes en matière de cybersécurité dans son étude de 2022 :

Année	**2022**	**2021**
Nombre d'attaques	795	1,365
Demande moyenne de rançon	7,2 millions de dollars	8,2 millions de dollars
Nombre moyen d'enregistrements touchés	115,8 millions	49,8 millions
Nombre moyen d'enregistrements affectés par attaque	559,695	119,114

Le nombre d'attaques et le montant des rançons ont diminué de 2021 à 2022.
Cependant, l'augmentation du nombre moyen d'enregistrements impactés indique que lorsque des attaques se produisent, elles ont un impact plus significatif sur le nombre d'enregistrements compromis.

Types d'attaques de ransomware dans les statistiques de cybersécurité

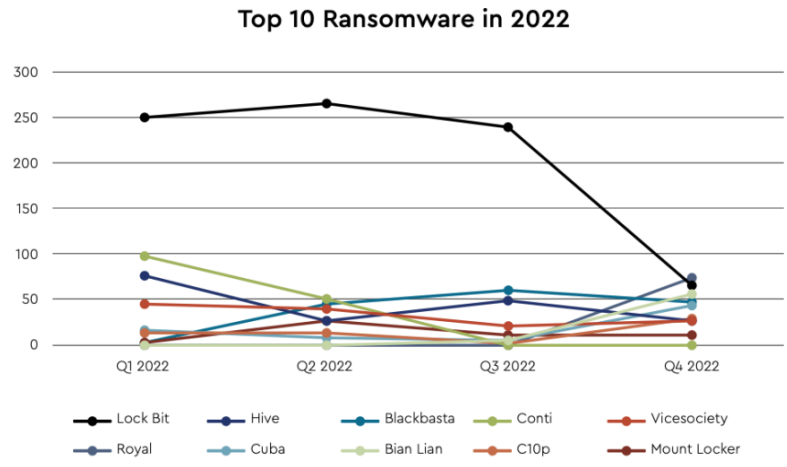
IC3 a reçu 2 385 plaintes de rançongiciels en 2022, ce qui a entraîné des pertes ajustées dépassant 34,3 millions de dollars.
Les attaquants de ransomware utilisent souvent des techniques d'ingénierie sociale pour accéder à l'environnement d'une victime.

Selon le même rapport, les principales causes d'incidents de ransomware étaient l'hameçonnage, l'exploitation du protocole RDP (Remote Desktop Protocol) **et les vulnérabilités logicielles**.

Le tableau ci-dessous répertorie les types de ransomware les plus courants responsables de cyberattaques graves.

Type de rançongiciel	Détails
Crypto / Crypteurs	• Une variante très dommageable du ransomware. • Se concentre sur le chiffrement des fichiers et des données au sein d'un système. • Le contenu chiffré devient inaccessible sans la clé de déchiffrement appropriée.
Casiers	• Verrouille complètement les utilisateurs hors de leur système, rendant leurs fichiers et applications inaccessibles. • Un écran de verrouillage affiche la demande de rançon et peut inclure un compte à rebours.
Scareware	• Un faux logiciel qui prétend avoir détecté un virus. • Contraint les utilisateurs à acheter des logiciels ou des services faux ou inutiles pour résoudre des problèmes fabriqués. • Verrouille l'ordinateur ou inonde l'écran de fenêtres contextuelles.
Leakware (Doxware)	• Menace de divulguer ou de vendre publiquement des informations confidentielles à moins qu'une rançon ne soit payée. • Cible les données des victimes et menace leur exposition.
RaaS (Ransomware en tant que service)	• Une plateforme prête à l'emploi avec des outils pour mener des campagnes de ransomware. • Les cybercriminels louent/vendent des RaaS à d'autres individus ou groupes, qui mènent ensuite les attaques.

LockBit, ALPHV/Blackcoats et Hive étaient les trois principales variantes de rançongiciels signalées à l'IC3 qui ciblaient les membres des secteurs des infrastructures essentielles.

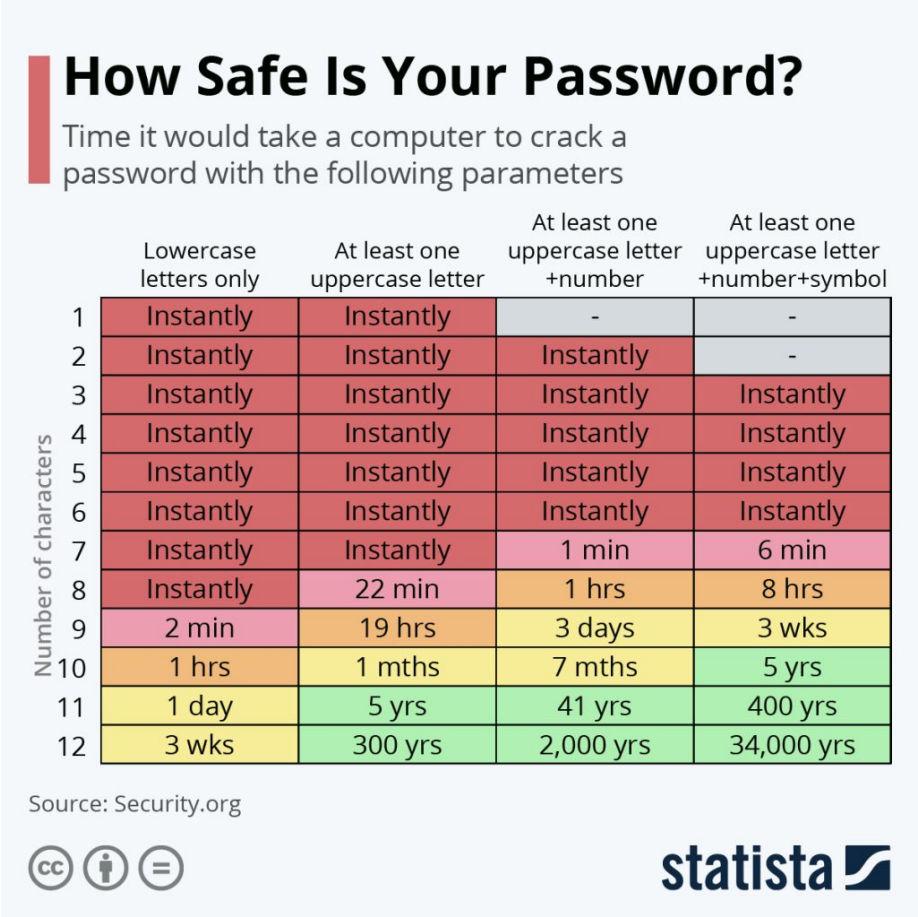


Données d'attaque de craquage de mot de passe

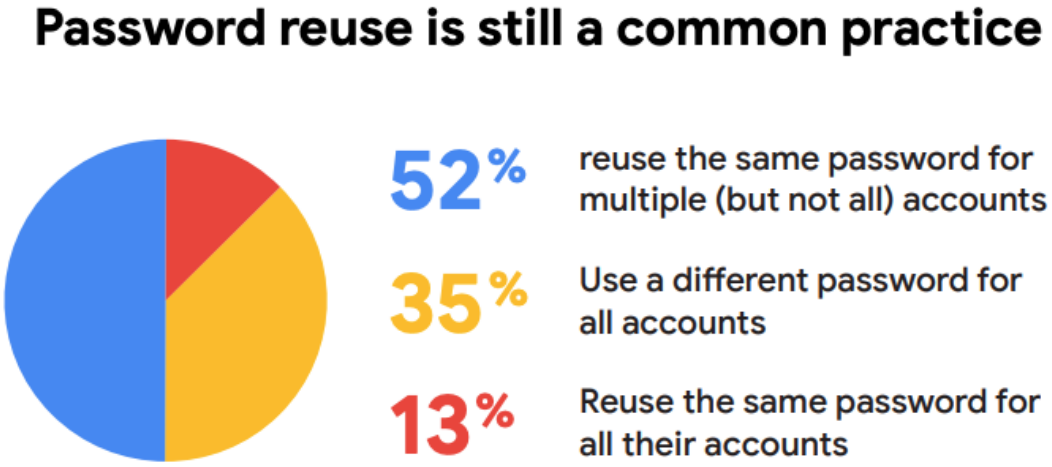
En 2019, **80 % de toutes les violations de données ont été attribuées à des mots de passe compromis, ce qui a entraîné des pertes financières importantes pour les entreprises et les consommateurs.**
49% des utilisateurs ne changeront qu'une lettre ou un chiffre dans l'un de leurs mots de passe préférés lorsque cela sera nécessaire pour créer un nouveau mot de passe.

Un pirate peut tenter 2,18 billions de combinaisons de mots de passe et de noms d'utilisateur en 22 secondes.
L'introduction d'une seule lettre majuscule dans un mot de passe transforme considérablement son potentiel.

Et un crack de mot de passe de huit caractères pourrait initialement être cassé en une seconde.
Mais ce temps peut augmenter à 22 minutes en ajoutant une lettre majuscule.



En 2019, une enquête Google a rapporté que l'habitude de réutiliser les mots de passe sur plusieurs comptes est notamment présente.



59% des personnes interrogées pensent que leurs comptes sont plus protégés contre les menaces en ligne que la personne moyenne.
69% se donnent une note A ou B lorsqu'il s'agit de protéger leurs comptes.

Selon le SANS Software Security Institute, les vulnérabilités les plus courantes sont

- Compromission des e-mails professionnels
- Protocoles hérités
- Réutilisation des mots de passe

Compte tenu de ces données critiques, que pensent les gens de la sécurité en ligne et des violations de mot de passe?

Le rapport LastPass Psychology of Passwords présente des résultats remarquables concernant les émotions et les comportements des répondants en matière de sécurité en ligne.

- 45% des répondants à l'enquête n'avaient pas changé de mot de passe au cours de la dernière année, même après une violation de la sécurité.
- 79 % sont d'accord pour dire que les mots de passe compromis sont préoccupants.
- 51% comptent sur leur mémoire pour garder une trace des mots de passe.
- 65% utilisent toujours ou presque toujours le même mot de passe ou une variante.

Sur les 3 750 professionnels interrogés dans sept pays, seulement 8% ont déclaré qu'un mot de passe fort ne devrait pas avoir de liens avec des informations personnelles.
La plupart des utilisateurs créent des mots de passe qui reposent sur des informations personnelles liées à des données publiques potentiellement accessibles, telles qu'une adresse de date ou de domicile.

Les méthodes les plus utilisées dans les attaques par mot de passe incluent:

Type d'attaque par mot de passe	Détails
Brute Force	• Essayer systématiquement toutes les combinaisons possibles de mots de passe jusqu'à ce que le bon soit trouvé.
Dictionnaire	• Une liste de mots de passe couramment utilisés ou de mots d'un dictionnaire est utilisée pour tenter l'authentification.
Hybride	• Combine des éléments d'attaques par force brute et par dictionnaire. • Essayer systématiquement diverses combinaisons de mots du dictionnaire, de substitutions courantes et de modifications.
Credential Stuffing	• Repose sur l'utilisation de grands ensembles de noms d'utilisateur et de mots de passe volés. • Comptes cibles dont le mot de passe n'a jamais été modifié après un cambriolage de compte. • Les pirates essaient des combinaisons d'anciens noms d'utilisateur et mots de passe.

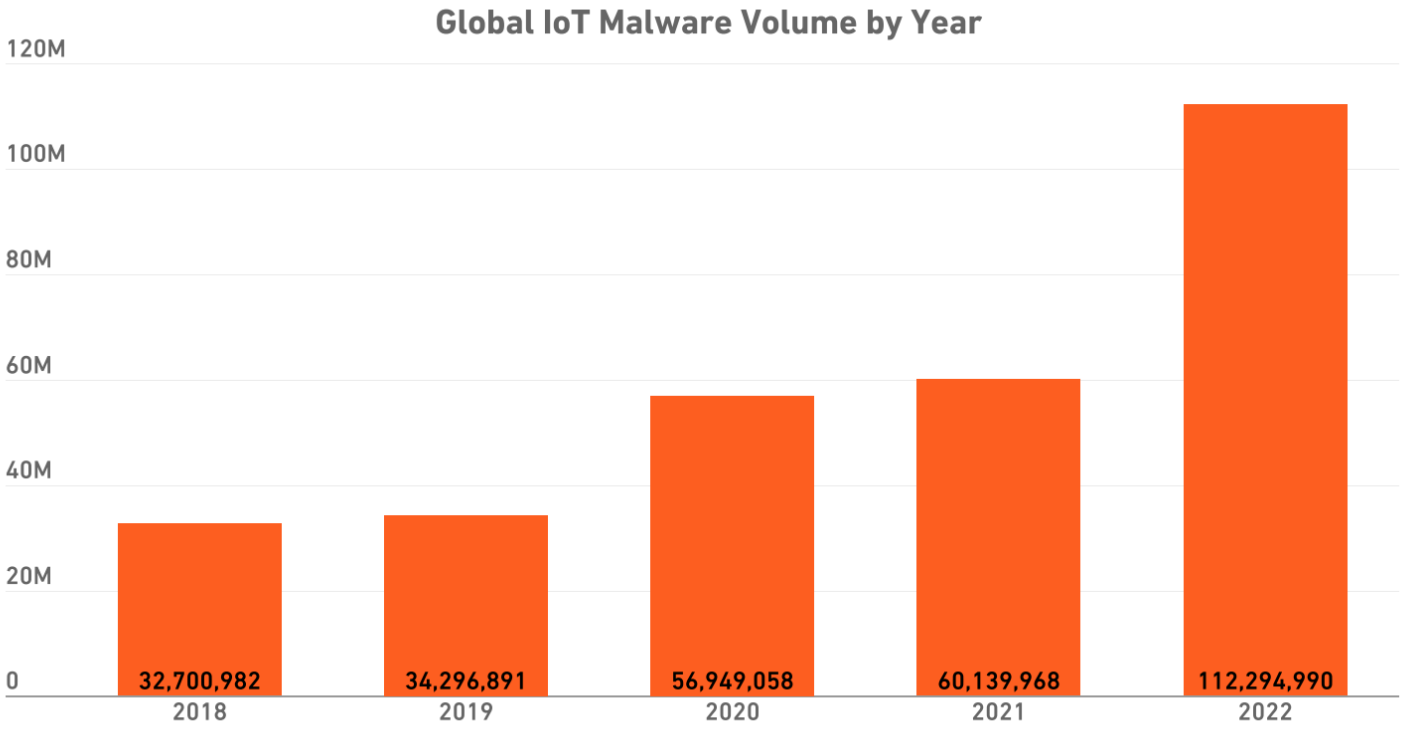
En décembre 2016, Yahoo a révélé que plus d'un milliard de comptes avaient été compromis lors de la violation notoire de 2013.
Au cours de cette violation, les pirates ont obtenu un accès non autorisé aux systèmes de Yahoo, compromettant les informations personnelles identifiables (PII).
Cela incluait les noms d'utilisateur, les adresses courriel, les numéros de téléphone et les mots de passe hachés.
Il est considéré comme l'une des plus grandes violations de données de l'histoire de la cybersécurité.

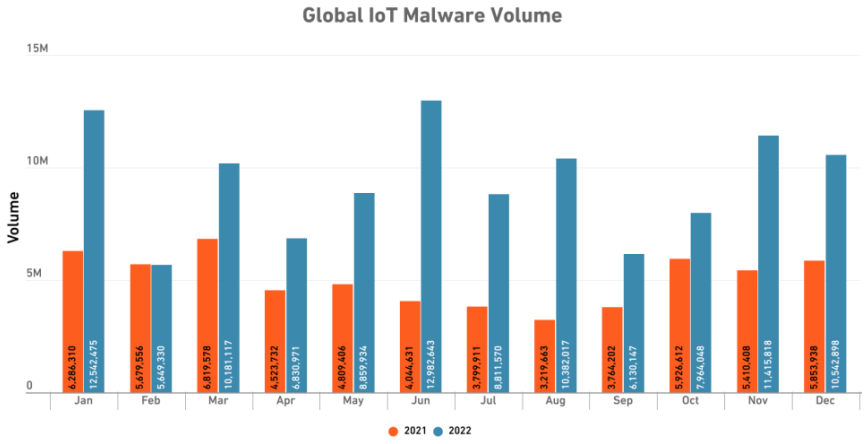
Internet des objets (IoT) Pirater les données

L'Internet des objets (IoT) fait référence à un réseau d'appareils physiques ou d'objets interconnectés.
Contrairement au piratage traditionnel des serveurs et des systèmes, l'IoT cible les appareils connectés à Internet.

Par exemple, les appareils ménagers intelligents tels que les téléviseurs, les haut-parleurs, les caméras de sécurité et les appareils médicaux font l'objet d'attaques.

Alors que le nombre d'appareils connectés continue de croître, la fréquence des logiciels malveillants IoT a grimpé en flèche de 87% en 2022 par rapport à l'année précédente, atteignant un niveau record de **112,3 millions** de **cas.**





Le graphique ci-dessus montre que le volume mondial de logiciels malveillants IoT a connu une augmentation notable, entraînant plusieurs incidents alarmants.

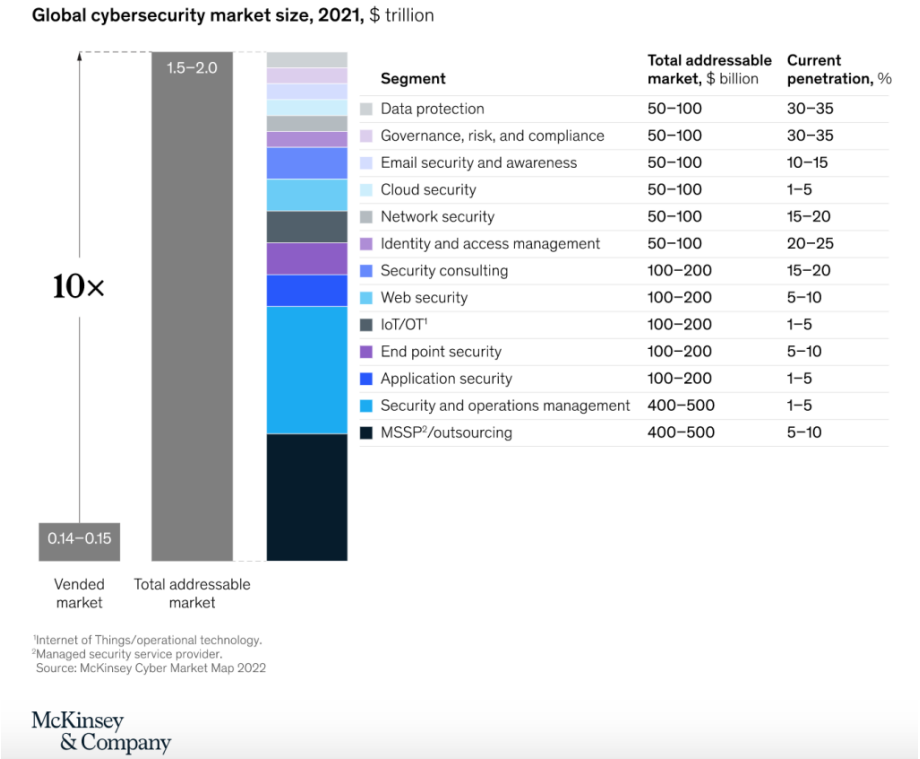
Par exemple, en janvier 2022, un **chercheur de 19 ans**, **David Colombo, a révélé qu'il pouvait exploiter un bogue dans le tableau de bord TeslaMate pour contrôler plus de 25 véhicules dans 13 pays différents.**
Colombo a obtenu un accès à distance à diverses fonctionnalités de Tesla, telles que le déverrouillage des portes, l'ouverture des fenêtres, le lancement de la conduite sans clé, le contrôle de la chaîne stéréo, le klaxon et la vérification de l'emplacement de la voiture et de la présence du conducteur.
Cependant, Colombo a déclaré qu'il n'était pas possible de déplacer le véhicule à distance.

Dans un autre cas, l'aspirateur robot **iRobot Roomba série J7 a capturé et transmis des images d'une femme portant un T-shirt lavande tout en utilisant les toilettes.** Ces images ont ensuite été envoyées à Scale AI, une start-up qui embauche des travailleurs du monde entier pour étiqueter les données audio, photo et vidéo à des fins de formation à l'IA.

Coûts des données de cybersécurité

Valeur des statistiques sur la cybersécurité

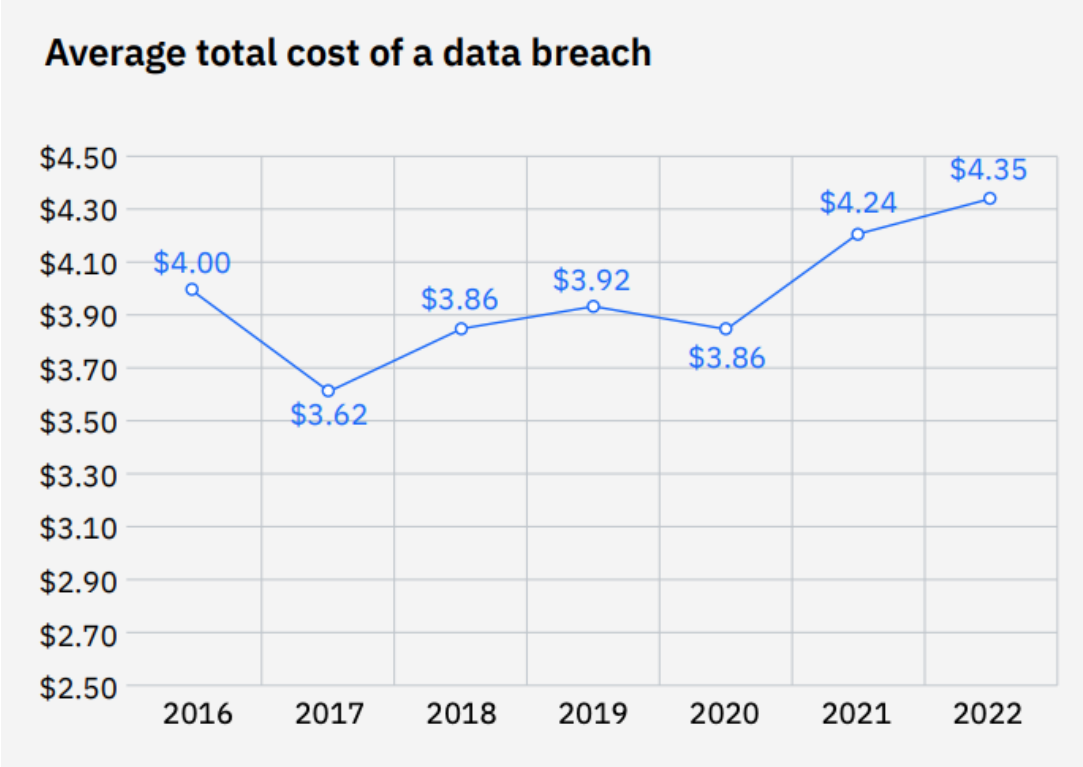
Il existe une opportunité de marché importante pour les fournisseurs de technologies et de services de cybersécurité, dont la valeur est estimée à **2 billions de dollars.**
Le tableau de taille du marché mondial de la cybersécurité de McKinsey & Company met l'accent sur le potentiel des fournisseurs à offrir des solutions et des services innovants en réponse à l'évolution des cybermenaces.
Cela présente des perspectives financières prometteuses et souligne le rôle crucial de ces fournisseurs dans le renforcement des défenses numériques et la protection des entreprises contre les cyber-risques persistants.



Segment	Total addressable market, $ billion	Current penetration, %
Data protection	50–100	30–35
Governance, risk, and compliance	50–100	30–35
Email security and awareness	50–100	10–15
Cloud security	50–100	1–5
Network security	50–100	15–20
Identity and access management	50–100	20–25
Security consulting	100–200	15–20
Web security	100–200	5–10
IoT/OT[1]	100–200	1–5
End point security	100–200	5–10
Application security	100–200	1–5
Security and operations management	400–500	1–5
MSSP[2]/outsourcing	400–500	5–10

Prix des violations de données de cybersécurité

Selon le rapport d'IBM sur le coût **d'une** violation de données, **le coût moyen mondial d'une violation de données est passé de 4,24 millions de dollars en 2021 à 4,35 millions de dollars en 2022.**
Le phishing représentait 16% des principaux vecteurs d'attaque dans la cybercriminalité, avec un coût moyen de violation de 4,91 millions de dollars.
De plus, les atteintes à la sécurité causées par des justificatifs d'identité volés ou compromis se sont élevées à 4,50 millions de dollars.

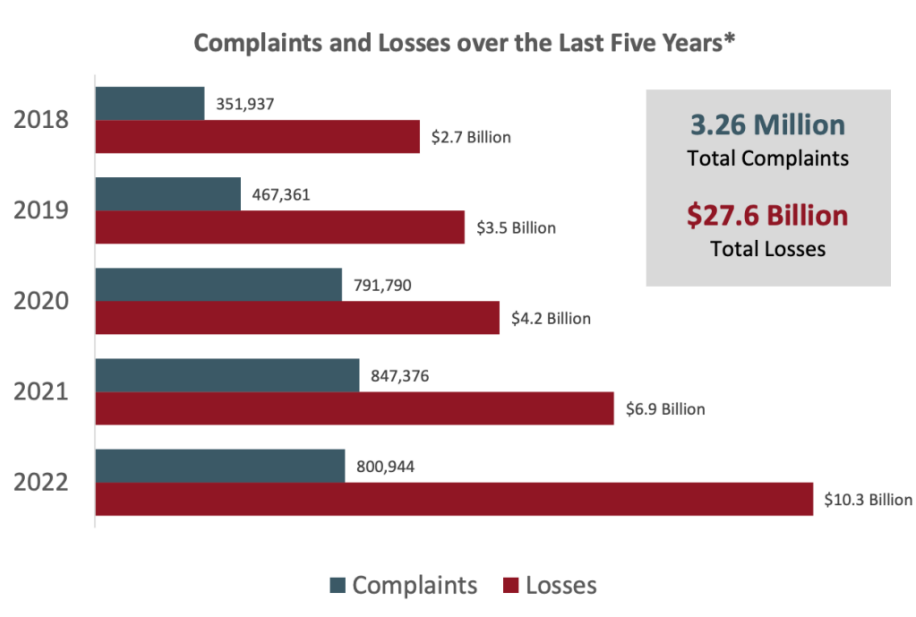


En 2022, le prix moyen par enregistrement compromis dans une violation de données à l'échelle mondiale était de 164 $, ce qui représente une augmentation de 1,9 % par rapport à 161 $ en 2021.
Cette augmentation est encore plus importante par rapport au coût moyen de 146 $ par enregistrement en 2020, affichant une hausse de 12,3 %.

Les attaques de ransomware ont représenté 11% des violations analysées, ce qui indique un taux de croissance de 41% par rapport aux 7,8% de violations de ransomware de l'année précédente.
Le coût moyen des attaques de ransomware a légèrement diminué, passant de 4,62 millions de dollars en 2021 à 4,54 millions de dollars en 2022.
Toutefois, ce coût est demeuré légèrement supérieur au coût total moyen de l'atteinte à la protection des données de 4,35 millions de dollars.

L'étude d'IBM sur le coût des violations de données montre également que les violations liées au travail à distance coûtent environ 1 million de dollars de plus, en moyenne, que les violations sans travail à distance.
Le coût moyen des atteintes au travail à distance était de 4,99 millions de dollars, tandis que les atteintes non influencées par le travail à distance s'élevaient en moyenne à 4,02 millions de dollars.
Ces violations liées au travail à distance coûtent environ 600 000 $ de plus que la moyenne mondiale.

Au cours des cinq dernières années, l'IC3 (Internet Crime Complaint Center) du FBI a reçu en moyenne 652 000 plaintes par an.
Depuis 2018, il y a eu 3,26 millions de plaintes et 27,6 milliards de dollars de pertes.



Statistiques sur la cybersécurité Coût pour les entreprises

Le coût de la cybersécurité pour les entreprises peut varier considérablement en fonction de divers facteurs en raison de la vaste gamme de services et de produits.
Par exemple, la taille et la nature de l'organisation, le niveau des mesures de sécurité mises en œuvre et l'étendue des menaces potentielles influent tous sur les coûts.

Selon une enquête de **Deloitte Insights**, **les organisations consacrent environ 10,9 % de leur budget informatique à la cybersécurité.**
Les entreprises consacrent environ 0,48 % de leur chiffre d'affaires aux dépenses de cybersécurité.
En ce qui concerne les dépenses par employé, les répondants ont déclaré un investissement moyen d'environ 2 700 $ par employé à temps plein pour les mesures de cybersécurité.

Cependant, selon **l'étude d'IBM** sur le coût d'une violation de données, ces investissements en valent la peine.

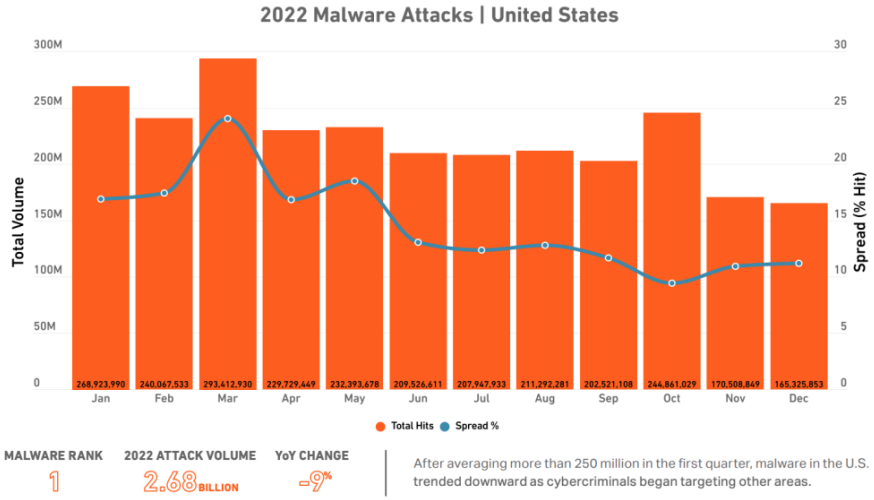
Les organisations disposant d'une **IA et d'une automatisation de sécurité entièrement déployées ont connu des violations 3,05 millions de dollars moins chères que les organisations sans tels déploiements.**
Cette différence significative de 65,2 % dans le coût moyen des atteintes à la vie privée a mis en évidence des économies substantielles, les organisations entièrement déployées s'élevant en moyenne à 3,15 millions de dollars, tandis que les organisations non déployées ont dû faire face à un prix moyen de 6,20 millions de dollars.

En outre, les entreprises dotées d'une IA et d'une automatisation de sécurité entièrement déployées ont connu une réduction de 74 jours de l'identification et du confinement des violations par rapport à celles qui n'en ont pas.
Les organisations entièrement déployées avaient un cycle de vie moyen de 249 jours, tandis que les organisations non déployées prenaient 323 jours.

Statistiques sur la cybersécurité par pays

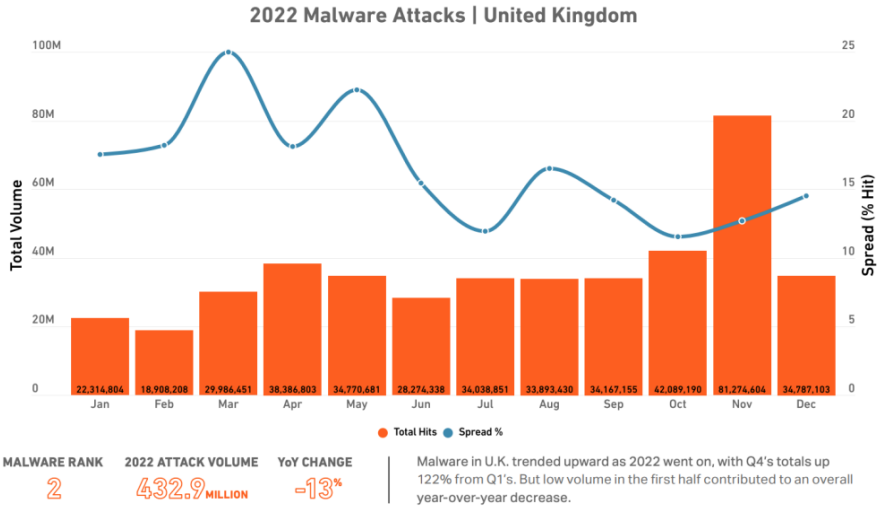
Volume de logiciels malveillants par pays

Selon le **rapport 2023 sur les cybermenaces de Sonic Wall**, **les États-Unis occupent la première place de la liste avec le plus grand volume d'attaques de logiciels malveillants, totalisant 2,68 milliards.**
Cependant, une diminution significative de -9% d'une année sur l'autre des instances de logiciels malveillants indique un changement dans l'attention des cybercriminels vers le ciblage d'autres pays.



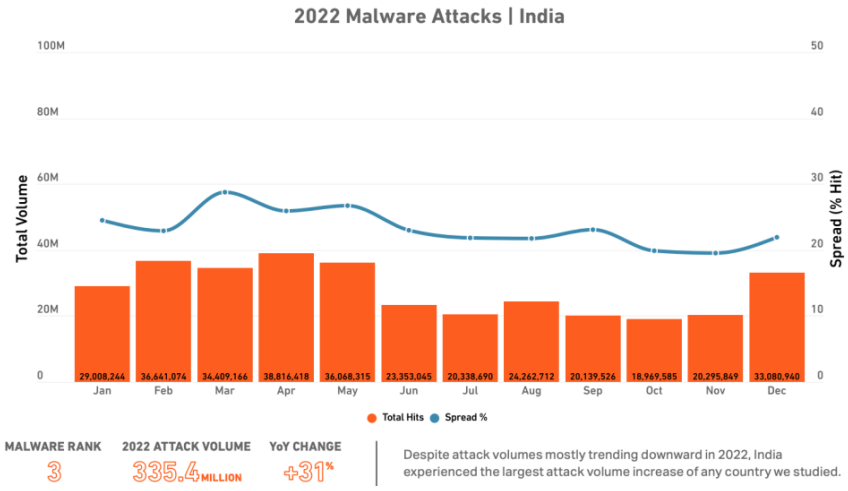
Le Royaume-Uni occupe la deuxième position pour le plus grand volume d'attaques de logiciels malveillants, avec 432,9 millions d'attaques en 2022.

Toutefois, il a également connu une baisse notable d'une année à l'autre de -13 %.



L'Inde arrive en troisième position sur la liste, totalisant 335,4 millions, affichant une augmentation notable de +31% d'une année sur l'autre.

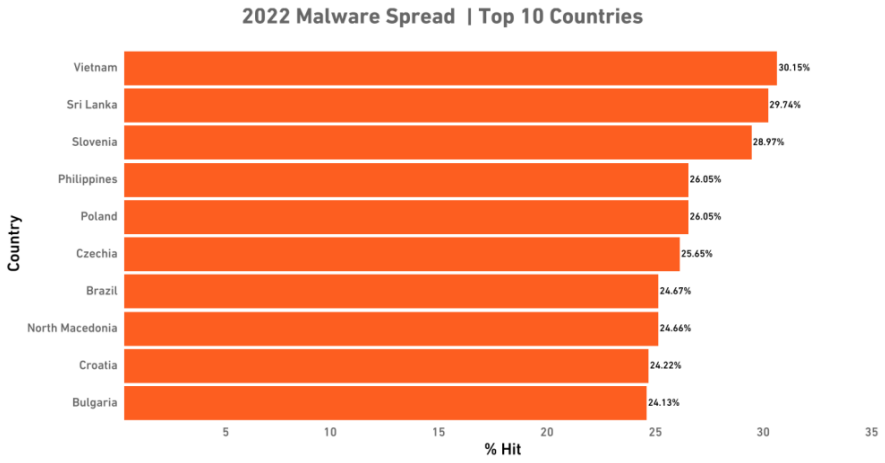
Alors que les volumes d'attaques ont généralement diminué en 2022, l'Inde s'est distinguée comme le pays avec la plus forte croissance du volume d'attaques parmi ceux inclus dans l'étude.



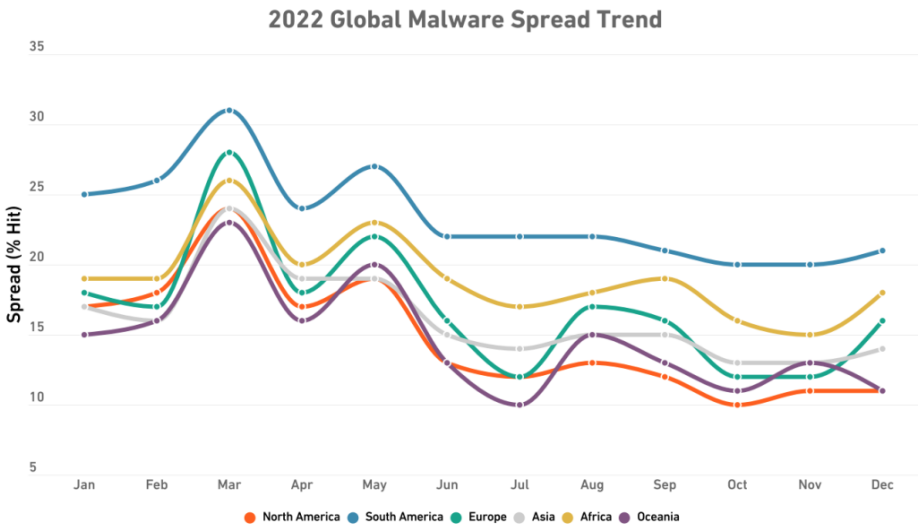
Propagation des logiciels malveillants par pays et région

Le pourcentage de propagation des logiciels malveillants de Sonic Wall représente le calcul des capteurs qui ont détecté une attaque de logiciel malveillant, indiquant l'étendue de la portée du logiciel malveillant dans cette région particulière.

Le Vietnam était le premier pays ciblé par les logiciels malveillants avec 30,15%.
Cependant, l'observation la plus significative est la montée de l'Europe en tant que point chaud de la cybercriminalité, le nombre de pays européens figurant sur la liste ayant doublé depuis 2021, constituant la majorité dans le top 10.



Selon le même rapport, l'Europe, l'Amérique latine et l'Asie ont connu des augmentations significatives à deux chiffres en 2022, avec des taux de croissance respectifs de 10%, 17% et 38%.



Fait intéressant, le volume de logiciels malveillants en Amérique du Nord a connu une baisse significative de 10 % d'une année sur l'autre, ce qui a donné un total de 2,75 milliards d'instances.
Ce chiffre représente le volume le plus bas enregistré depuis 2017, soulignant une baisse notable de l'activité des logiciels malveillants dans la région.

En outre, en décembre, les tentatives de logiciels malveillants en Amérique du Nord ont atteint un niveau record de 158,9 millions, soit le volume mensuel le plus bas depuis 2018.
Ces développements indiquent un changement potentiel parmi les cybercriminels qui ne ciblent pas l'Amérique du Nord et d'autres centres de cybercriminalité importants pour se concentrer sur d'autres régions du monde.

Données de cyberguerre – Russie et Chine vs États-Unis

La Chine et la Russie émergent comme les acteurs dominants dans le paysage de la cybersécurité, représentant près de 35% des attaques mondiales, combinées.
Avec 79 attaques confirmées en provenance de Chine et 75 en provenance de Russie, ces deux pays ont largement ciblé les gouvernements nationaux.

L'Agence américaine de cyberdéfense met fréquemment à jour ses avis, alertes et rapports d'analyse des logiciels malveillants (MAR) sur les cyberactivités malveillantes russes.
« Le gouvernement russe se livre à des cyberactivités malveillantes pour permettre le cyberespionnage à grande échelle, pour supprimer certaines activités sociales et politiques, pour voler de la propriété intellectuelle et pour nuire à des adversaires régionaux et internationaux. »

En février 2022, la BBC a rapporté que 74% des revenus des ransomwares allaient aux pirates informatiques liés à la Russie.
Les chercheurs ont identifié que plus de 400 millions de dollars de paiements en crypto-monnaie étaient dirigés vers des groupes fortement soupçonnés d'avoir des affiliations avec la Russie.

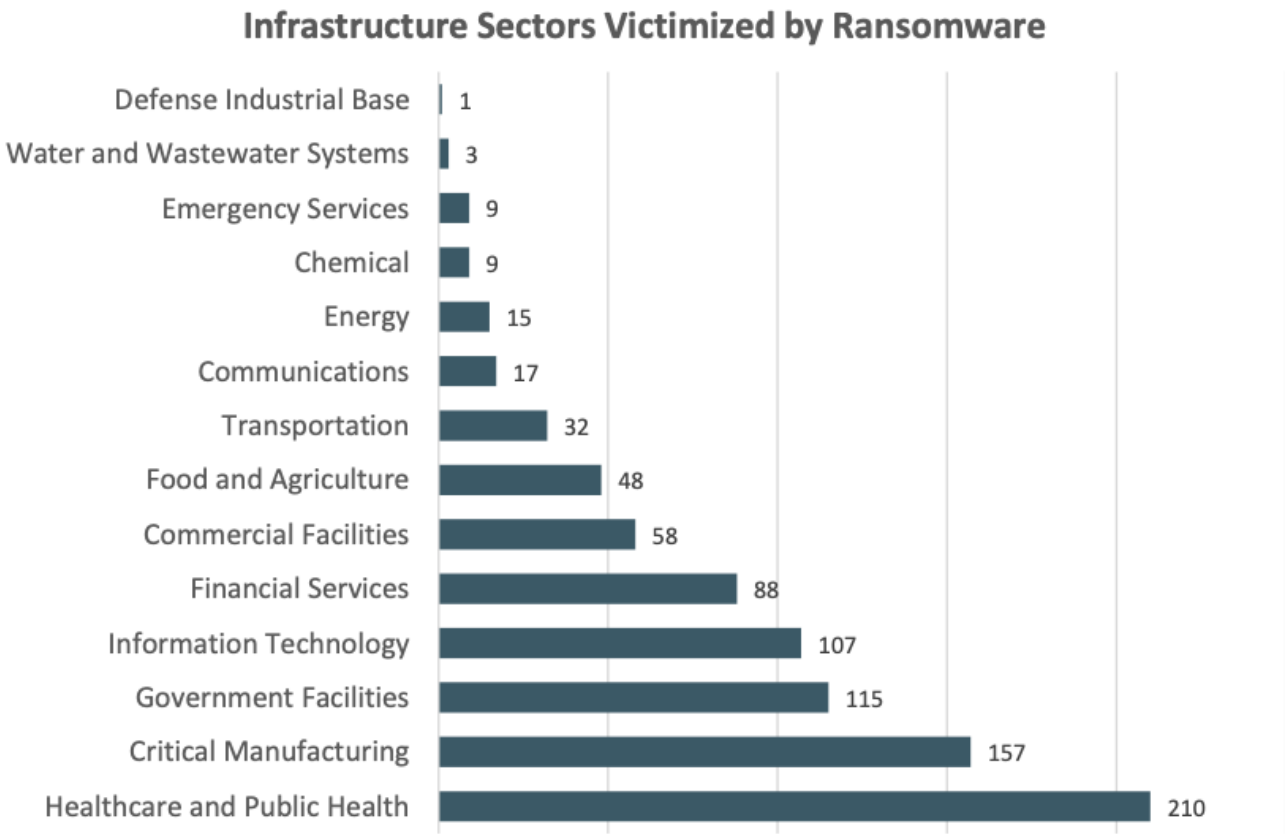
La Maison Blanche a publié une déclaration en juillet 2021 dénonçant le comportement irresponsable de la République populaire de Chine (RPC) dans le cyberespace.
« Comme détaillé dans les documents d'accusation publics dévoilés en octobre 2018 et en juillet et septembre 2020, des pirates informatiques ayant travaillé pour le ministère de la Sécurité d'État (MSS) de la RPC se sont livrés à des attaques de ransomware, à l'extorsion cybernétique, au crypto-jacking et au vol de rang de victimes du monde entier, le tout à des fins financières. »

L'année suivante, les chefs du **FBI et du MI5** ont **fait une première apparition conjointe et ont lancé un avertissement sur la menace posée par la Chine :**
« Dans notre monde, nous appelons ce genre de comportement un indice... cela représenterait l'une des perturbations commerciales les plus horribles que le monde ait jamais vues », a déclaré le chef du FBI, Christopher Wray.

Statistiques sur la cybersécurité par industrie

L'IC3 a enregistré 870 plaintes en 2022, signalant des attaques de rançongiciels ciblant des organisations dans les secteurs des infrastructures critiques.
Parmi les 16 secteurs d'infrastructures essentielles, les rapports d'IC3 ont révélé qu'au moins un membre avait été victime d'une attaque de rançongiciel.

Les organisations d'infrastructures essentielles ont dû faire face à un coût moyen de violation de données de **4,82 millions de dollars, dépassant de 1 million de dollars la moyenne des autres industries.**
Parmi eux, 28% ont été confrontés à des attaques destructrices ou de ransomware, et 17% ont subi des violations dues à des partenaires commerciaux compromis.



Le secteur de la santé a été le plus coûteux pour les violations de ransomware pendant 12 années consécutives, avec un coût moyen de violation de données atteignant 10,10 millions de dollars.
Les données des patients sont extrêmement précieuses pour les cybercriminels, en particulier dans les dossiers de santé électroniques (DSE).
Ces dossiers englobent des informations sur les individus, y compris leurs noms, numéros de sécurité sociale, détails financiers, adresses passées et présentes et antécédents médicaux.

Pendant ce temps, l'industrie manufacturière a considérablement souffert des attaques d'extorsion en 2022, avec 447 victimes enregistrées sur différentes plateformes.
Le secteur des services professionnels et juridiques suivait de près, avec 343 victimes signalées.

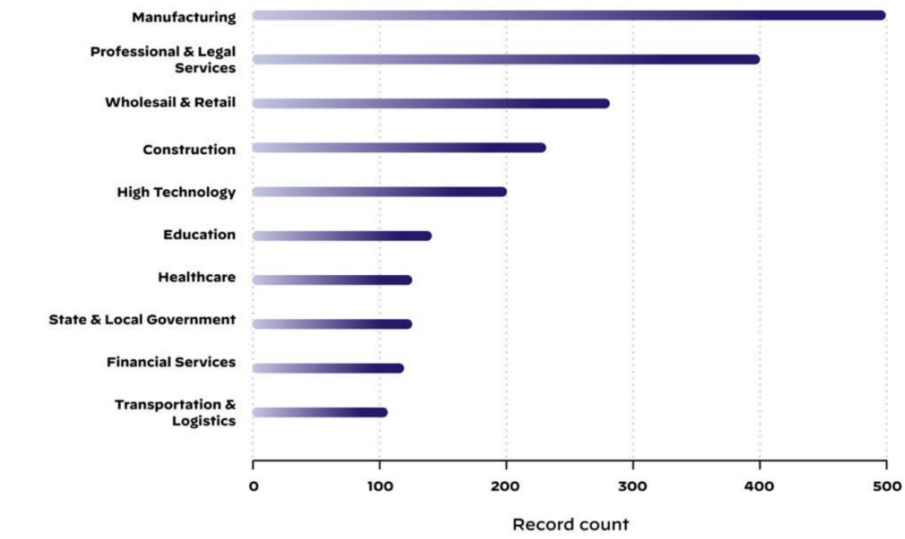


Figure 4. Industries most heavily impacted by extortion attacks (leak site data, 2022)

Principales industries Violations de données de cybersécurité

En 2022, le Costa Rica a déclaré une urgence nationale en réponse à une série d'attaques de ransomware ciblant des institutions critiques.
La première série d'attaques visait des organismes gouvernementaux et a été revendiquée par le gang Conti, un groupe influent de pirates informatiques basé en Russie.

Le site d'extorsion de Corti a revendiqué la publication de 50% des données volées du gouvernement costaricien, dont 850 gigaoctets de matériel du ministère des Finances.
Les attaquants ont exigé une rançon de 10 millions de dollars pour empêcher la fuite d'informations.

La deuxième série d'attaques a eu lieu le 31 mai 2022 par le groupe de rançongiciels HIVE.
La principale cible était la Caisse costa-ricienne de sécurité sociale, l'entité responsable de la gestion des services de santé du pays.
En outre, l'attaque a touché plus de 10 400 ordinateurs et la plupart des serveurs au Costa Rica.
Par conséquent, environ 34 677 rendez-vous ont été annulés cette semaine-là, ce qui représente 7 % de tous les rendez-vous prévus.

En mai 2021, Colonial Pipeline a subi une attaque de ransomware qui a complètement fermé son pipeline de distribution de carburant.
En l'espace de seulement deux heures, les cybercriminels appartenant au groupe connu sous le nom de DarkSide ont réussi à extraire près de 100 gigaoctets de données du réseau de la société basée à Alpharetta, en Géorgie.

Le pipeline colonial a versé environ 5 millions de dollars à des pirates informatiques russes pour faciliter la restauration du plus grand oléoduc du pays.

De même, en juin 2021, JBS, la plus grande entreprise de conditionnement de viande au monde, a été victime d'une importante attaque de ransomware par des pirates russes.
La violation a entraîné le paiement par JBS d'une rançon de 11 millions de dollars aux pirates informatiques qui ont obtenu un accès non autorisé à son système informatique.

L'importance de la cybersécurité

Avec l'augmentation des cyberattaques et la sophistication croissante des acteurs malveillants, les entreprises et les particuliers sont confrontés à des risques importants. Les statistiques sur la cybersécurité révèlent des tendances alarmantes, telles que l'escalade des coûts des violations de données, la prévalence des attaques de phishing et l'impact du travail à distance sur les dépenses de violation.

Cependant, il met également en lumière la valeur des investissements dans la cybersécurité, en mettant l'accent sur les économies de coûts et l'amélioration de la réponse aux incidents obtenues grâce à la mise en œuvre d'équipes d'IA de sécurité, d'automatisation et de réponse aux incidents.

Alors que les entreprises continuent de naviguer dans le paysage changeant des menaces, il est clair qu'il est essentiel de donner la priorité à des mesures de cybersécurité robustes pour protéger les données sensibles, préserver la continuité des activités et se protéger contre les dommages financiers et de réputation.

Sources:

- Statista
- CISCO
- IBM et le Ponemon Institute
- FBI IC3
- ConnectWise
- Norton
- Astra
- Point de contrôle
- SCRS
- Usenix
- AAG
- CNBC (en anglais seulement)
- Mur sonore
- Verrouillage du site
- Cloudflare
- Google Cloud
- Microsoft
- Kaspercé
- LastPass
- Google (en anglais)
- Yahoo
- Le SANS Software Security Institute
- Un seul login
- Deloitte Insights
- Technologie MIT
- Blog moyen
- McKinsey & Company
- Instinct profond
- Réseaux de Palo Alto
- CompariTech
- La Maison Blanche
- NBC
- Renseignements de sécurité
- Affaires relatives à la protection des renseignements personnels
- Nouvelles mondiales
- Bloomberg (en anglais seulement)

Découvrez plus d'informations sur la cybersécurité ici.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230719
"C'est ensemble qu'on avance"