Octobre 2021 • Vol. 8 n° 9

ARS solutions affaires et technologies

PASSION AFFAIRES et technologies

NOUS AIDONS LES ENTREPRISES À TRANSFORMER LEURS TECHNOLOGIES EN LEVIER D'AFFAIRES

« On pense trop souvent que les Ransomwares, c'est pour les autres.

Nous avons été victimes d'une cyberattaque de type Cryptolocker qui a paralysé l'ensemble de nos opérations pendant 8 jours.

On n'a pas l'expertise à l'interne pour répondre à ce genre d'attaque. J'ai donc décidé de contacter ARS pour avoir une firme expérimentée et compétente chez nous dans le but de nous aider à nous remonter plus facilement et plus rapidement.

J'aurais aimé être plus conscient de mes données critiques et de comment elles étaient protégées. On s'est rendu compte que nos copies de sécurité n'étaient pas suffisantes, même si on s'en occupait à l'interne.

Si c'était à refaire, on s'informerait plus sur les types d'attaques, comment elles fonctionnent et comment on peut se protéger et faire de la prévention. »

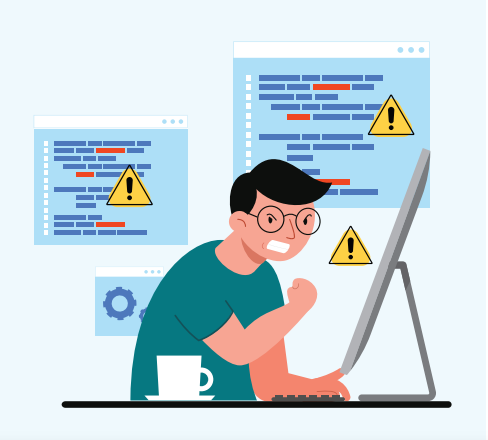
François-Xavier Bonneville
Directeur général
Lepage Milwork

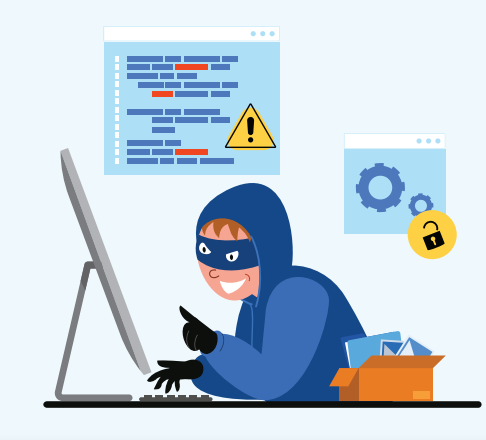
Suivez-nous

Affaires-TI

Le coût faramineux des rançongiciels en 2021 par pays

TEMPS DE LECTURE 2:30





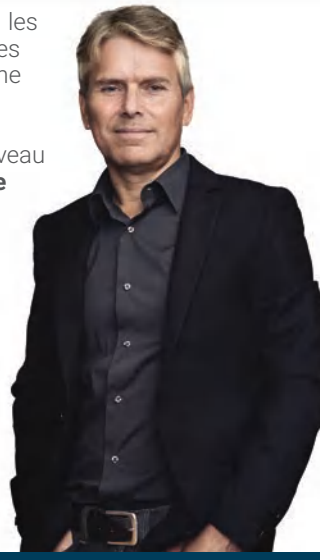
Les rançongiciels ont causé des centaines de milliards de dollars de dommages économiques en 2020.

Alors que le monde s'efforçait de relever les défis de la pandémie, les cybercriminels ont prospéré, l'adoption accrue de l'exfiltration des données ayant contribué à créer une année lucrative pour eux et une année coûteuse et extrêmement perturbante pour les victimes.

La demande de rançon moyenne a augmenté de plus de 80 %. Au niveau mondial, **les rançons versées se sont élevées à 18 milliards de dollars au minimum,** tandis que le coût des temps d'arrêt dans les secteurs privé et public a ajouté des milliards de dollars supplémentaires.

Les statistiques à la page suivante montrent le bilan économique dévastateur des rançongiciels sur un certain nombre de marchés clés. Les données comprennent les demandes de rançon, le coût des temps d'arrêt et le coût global des rançongiciels, ainsi que des statistiques distinctes pour les secteurs public et privé.

SUITE À LA PAGE 2 ▼



Répartition par pays - Utilisateurs privés inclus

Pays	Soumissions totales	Coût minimum (USD)	Coûts estimés (USD)
États-Unis	23,661	$920,353,010	$3,682,228,067
Italie	9,226	$346,729,130	$1,387,389,097
Espagne	8,475	$298,254,459	$1,193,709,500
France	7,824	$283,816,080	$1,135,795,109
Allemagne	7,138	$252,609,210	$1,011,001,498
U.K.	4,788	$169,182,845	$677,113,461
Canada	4,257	$164,772,274	$659,246,267
Australie	2,775	$105,978,531	$424,034,780
Autriche	1,254	$46,643,868	$186,645,857
Nouvelle-Zélande	399	$14,230,333	$56,951,495
Total (tous les pays)	**506,185**	**$18,658,009,233**	**$74,632,036,933**

Secteurs privé et public - Utilisateurs privés exclus

Pays	Soumissions totales	Coût minimum (USD)	Coûts estimés (USD)
États-Unis	15,672	$596,436	$2,385,747,238
Italie	4,476	$159,738,887	$638,955,546
Espagne	4,088	$151,309,229	$605,236,914
France	3,835	$147,376,932	$589,507,727
Allemagne	3,747	$132,558,050	$530,232,201
U.K.	3,236	$123,697,351	$494,789,403
Canada	2,718	$93,475,142	$373,900,568
Australie	2,072	$79,951,174	$319,804,685
Autriche	819	$32,252,920	$129,011,681
Nouvelle-Zélande	265	$9,906,552	$39,626,209

Conclusion

Bien que tous ces chiffres soient basés sur les meilleures informations actuellement disponibles, il est impossible de faire des projections vraiment précises en raison des ensembles de données limités, des restrictions en matière de partage d'informations, de l'absence d'obligation de divulgation des incidents, etc.

Par conséquent, ce rapport ne prétend pas être une estimation précise du coût mondial réel des rançongiciels. Nous souhaitons plutôt souligner l'ampleur du problème. En attirant l'attention sur l'énorme impact économique des rançongiciels, on veut encourager les entreprises, les organismes d'application de la loi et les législateurs à être plus proactifs dans la protection contre l'une des plus grandes menaces de cybersécurité au monde.

Méthodes de calcul et hypothèses

• Le nombre d'incidents est tiré des soumissions au service d'identification des rançongiciels ID Ransomware. Chaque soumission à ce service représente un incident confirmé et il y a eu un total de **506 185 soumissions en 2020**.

• Seulement 25 % des organisations des secteurs public et privé touchées par les rançongiciels utilisent ID Ransomware. Par conséquent, on a fourni deux estimations : un coût minimum basé sur le nombre réel de soumissions et un coût estimé basé sur ce nombre multiplié par 4.

• Le paiement moyen de la rançon est de 154 108 $.

• 27 % des organisations touchées paient la demande de rançon.

• Le coût total moyen des temps d'arrêt par incident est de 274 200 dollars.

Source : Emsisoft Malware Lab

Gmail a trouvé une astuce

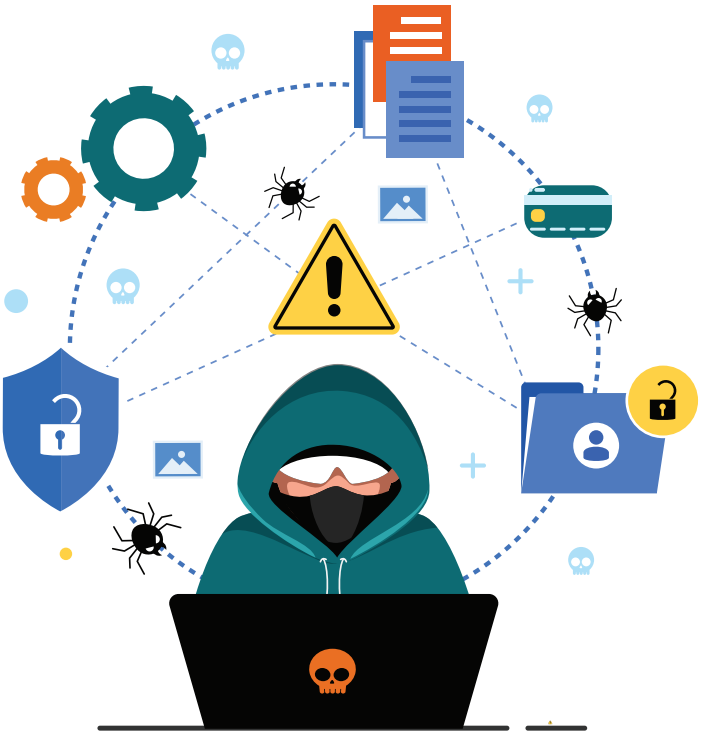
toute simple pour distinguer les courriels légitimes de l'hameçonnage

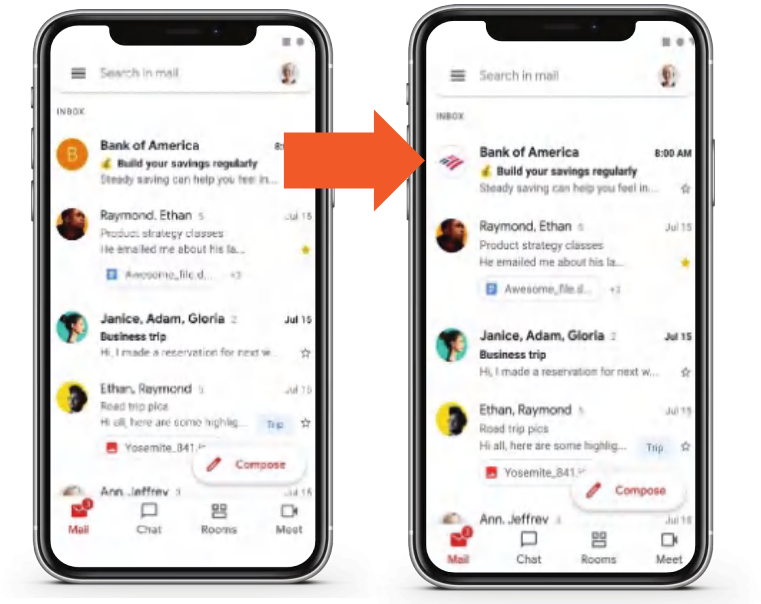
TEMPS DE LECTURE 1:30

Après une phase d'expérimentation, Google annonce que Gmail gère la spécification d'authentification BIMI, qui garantit l'authenticité d'un courriel en provenance d'une entreprise.

Comment savoir si le courrier électronique que l'on a reçu de la part d'une entreprise est légitime?

En utilisant un logo officiel selon Google. C'est l'objet d'une nouvelle spécification d'authentification, baptisée BIMI (Brand Indicators for Message Identification).





Grâce à ce procédé, une entreprise ou une marque peut ainsi **remplacer l'avatar générique utilisé dans Gmail par son propre logo.** L'image ci-dessus montre un exemple avant/après avec la Bank of America, qui fait partie des partenaires de Google pour le lancement de cette nouvelle fonction.

Pour ce faire, l'entreprise doit utiliser le protocole d'authentification DMARC (Domain-based Message Authentication, Reporting and Conformance) qui protège les propriétaires de noms de domaines d'éventuelles usurpations.

De plus, le logo doit être validé par une autorité compétente, telle que Entrust Datacard ou DigiCert. Cette autorité fournit alors un **certificat d'authenticité, appelé Verified Mark Certificate (VMC).**

Enfin, le service de courrier électronique doit être compatible avec la spécification BIMI. C'est le cas actuellement de MailChimp, SendGrid, Valimail, Fastmail, Proofpoint, Verizon Media. **L'arrivée de Google va sans doute donner un coup d'accélérateur à ce procédé d'authentification et compliquer davantage le travail des malfaiteurs et experts du phishing.**

Source : 01net.com

10 entreprises connues qui passent au télétravail à long terme

TEMPS DE LECTURE 2:30

Pendant la pandémie, la transition vers le télétravail a été rapide et brutale pour beaucoup d'organisations. Mais de nombreuses entreprises ont compris que le travail à distance permanent est l'avenir du travail, pandémie ou pas.

1. Adobe

Adobe est une société de logiciels qui fournit des solutions axées sur le client pour les applications Web et le développement de contenu. Société innovante proposant une large gamme de produits et de solutions, Adobe s'engage à créer un lieu de travail agréable pour son personnel. Plan de travail à distance : les employés auront la possibilité de travailler à domicile environ 50 % du temps et au bureau le reste du temps.

2. Amazon

Premier détaillant en ligne au monde, Amazon emploie près de 92 000 personnes dans le monde entier et propose des livres traditionnels et électroniques, des meubles, des articles ménagers, des vêtements, des appareils électroniques, de la musique, des films, etc. Plan de travail à distance : en juin 2021, Amazon a déclaré que les employés dont le poste leur permet de travailler à domicile peuvent le faire deux jours par semaine.

3. Capital One

Fondée en 1988, Capital One est l'une des 10 plus grandes banques du pays en termes de dépôts des clients et gère près de 45 millions de comptes. La société est un fournisseur réputé de services et de produits financiers pour les clients commerciaux, les petites entreprises et les consommateurs. Plan de travail à distance : Capital One adopte un modèle hybride flexible et n'obligera pas les employés à être présents au bureau un certain nombre de jours. Certains employés sont en mesure de travailler à domicile 100 % du temps.

4. Dropbox

Dropbox aide les personnes et les entreprises à synchroniser leurs fichiers et à partager et collaborer sur des projets à tout moment et en tout lieu. Plan de travail à distance : Dropbox permettra à tous les employés de travailler à domicile de façon permanente. Les bureaux existants deviendront des studios Dropbox, où les employés pourront choisir de se rendre pour travailler.

5. Facebook

Fondé en 2004, Facebook est le plus grand réseau de médias sociaux au monde, avec plus de 2,85 milliards d'utilisateurs actifs chaque mois. Plan de travail à distance : en juin 2021, Facebook a annoncé que les employés pourraient travailler à domicile de façon permanente.

6. Microsoft

Microsoft est une société multinationale de technologie qui développe, fabrique et commercialise des logiciels informatiques, des produits électroniques grand public et des ordinateurs personnels. Plan de travail à distance : les employés peuvent travailler à domicile pendant environ 50 % de leur semaine de travail. Les responsables ont la possibilité d'approuver le travail à distance à temps plein pour le personnel.

7. Spotify

Entreprise suédoise, Spotify propose des services de musique, de comédie, de podcast et de streaming. Les utilisateurs peuvent écouter de la musique directement depuis le cloud, au lieu de la télécharger sur leur appareil, et ont accès à plus de 30 millions de titres. Plan de travail à distance : Spotify a récemment annoncé que les employés peuvent choisir de travailler au bureau, à distance ou dans un espace de coworking payé par l'entreprise.

8. Twitter

Twitter est un réseau social en ligne et un service d'information qui permet aux gens de publier des messages et d'interagir instantanément avec d'autres personnes dans le monde entier en utilisant des messages courts. Plan de travail à distance : les employés de Twitter pourront travailler à domicile indéfiniment et se rendre au bureau quand ils le souhaitent.

9. VMware

Filiale de Dell Technologies, VMware est spécialisée dans les logiciels et services de cloud computing et de virtualisation. Ses produits et services comprennent l'infrastructure des centres de données et du cloud et sa gestion, la mise en réseau, la sécurité, le stockage, etc. Plan de travail à distance : VMware propose le travail à distance permanent à tous ses employés.

10. Zoom Video Communications

Zoom Video Communications a été fondée en 2011 pour révolutionner la façon dont les équipes communiquent. Zoom fournit des communications vidéo modernes en entreprise qui permettent la conférence audio et vidéo, la collaboration, le chat et les webinaires. Plan de travail à distance : Zoom Video Communications mélange stratégiquement le travail à distance et au bureau.

Compte tenu du succès du travail à distance au cours des deux dernières années, il est probable que le nombre d'entreprises qui optent pour le travail à domicile va continuer à augmenter, de même que le nombre d'emplois à domicile disponibles.

Source : Emily Courtney

ARSolutions
6655, boul. Pierre-Bertrand, bureau 301, Québec (Québec) G2K 1M1
www.ars-solutions.ca | info@ars-solutions.ca | 418 872-4744