Mai 2021 • Vol. 8 n° 5

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies

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

« Une simulation d'hameçonnage très près de la réalité.

J'ai mis en place une stratégie de simulation d'hameçonnage en collaboration avec ARS et cet exercice a été très révélateur pour notre organisation. **ARS a su créer une simulation très près de la réalité qui a suscité des réactions surprenantes et une belle dynamique.** J'aime beaucoup la régularité de leurs envois de capsules informatives sur l'hameçonnage. On les intègre à notre infolettre interne pour que les employés en prennent connaissance. Pour moi, c'est important de sensibiliser les employés en continu.

C'est définitivement une formule que je veux garder en place. »

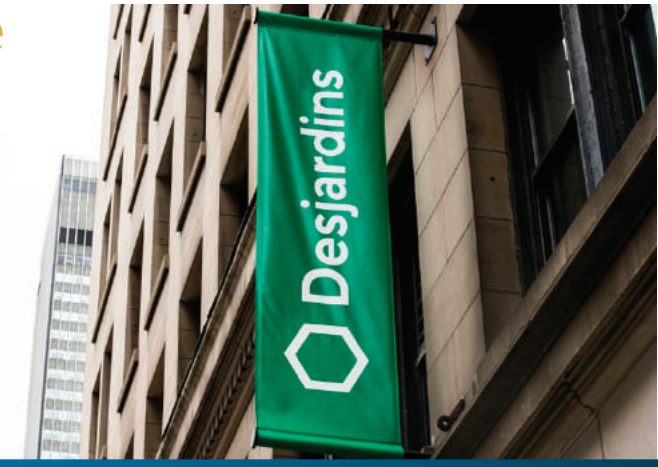
Stéphane Lapierre
Directeur de l'informatique et du développement logiciel
Signalisation Ver-Mac

Suivez-nous

Sécurité des données

Victime de fraude suite à la fuite de données Desjardins : je vous présente les conséquences et la marche à suivre

TEMPS DE LECTURE 3:50



Crédit photo : OLIVIER PONTBRIAND

«Je me suis fait frauder pour un total de 8 000 $ en demandes de PCU en 2020 et les informations utilisées par le fraudeur pour effectuer les demandes étaient les mêmes que celles volées chez Desjardins.»

En avril dernier, j'ai reçu mon avis de cotisation pour l'année d'imposition 2020 sur lequel il était inscrit qu'on avait modifié le montant de mes prestations d'assurance-emploi et autres prestations pour qu'il soit le même que mon T4E. **Le montant révisé était de 8 000 $ suite à plusieurs demandes de prestation canadienne d'urgence (PCU) que je n'avais pourtant jamais effectuées.** Inutile de vous mentionner que le montant dû sur mes avis de cotisation fédéral et provincial était très élevé alors que j'étais plutôt censée recevoir un remboursement dans les deux cas. C'est à ce moment que j'ai su que quelque chose clochait. J'ai donc contacté immédiatement Service Canada qui m'ont appris que je m'étais fait frauder en vérifiant que mes informations ne concordaient pas avec celles qui ont été utilisées pour les demandes de PCU à mon dossier. Ils m'ont également informée qu'il y avait **30 000 cas de fraude similaires** au mien cette année.

Même si rien ne prouve hors de tout doute que l'incident soit lié au vol de données de Desjardins, je soupçonne que cette fraude vient de la fuite qui a exposé les données de 6,2 millions de membres, car le fraudeur a utilisé les **mêmes identifiants que ceux volés chez Desjardins, comme mon nom complet, ma date de naissance et mon numéro d'assurance sociale.** Il est important de savoir comment réagir rapidement à ce genre de situations avant que les dommages ne deviennent incontrôlables.

SUITE À LA PAGE 2 ▼

Voici 6 choses à faire si vous découvrez que vous avez été fraudé lors de la réception de votre avis de cotisation d'impôts 2020 :

1. Contacter Service Canada pour les aviser

Vous devez les appeler pour les informer que des demandes de PCU à votre T4E ne proviennent pas de vous. Ils vous demanderont de confirmer votre numéro d'institution financière ainsi que votre adresse postale et si les informations ne concordent pas avec celles des demandes de PCU, ils vont ouvrir une enquête de fraude et faire bloquer le compte utilisé pour les demandes. Suite à l'enquête, qui peut durer plus de 12 mois, votre cotisation d'impôts sera ajustée avec les demandes de PCU frauduleuses en moins.

2. Porter plainte à la police municipale de votre secteur

Obtenez le numéro de votre dossier, le nom du policier et son numéro de téléphone. Assurez-vous que le rapport indique votre nom et votre NAS et demandez une copie de cette plainte. Rendez-vous dans un Centre Service Canada pour leur fournir le rapport de police. Cette étape risque de jouer en votre faveur lors de l'enquête exigée par Service Canada et faire en sorte qu'elle soit complétée plus rapidement.

3. Communiquer avec Equifax/Transunion, Desjardins et Postes Canada pour vérifier s'il y a eu des changements à votre dossier

Vérifiez bien qu'aucune demande de crédit n'a été autorisée sans votre consentement et demandez à ce qu'on vous appelle en cas de demande ou modification à votre dossier comme un changement d'adresse.

4. Changer d'identifiants dans "Mon dossier Service Canada"

Vous devez écraser le compte que le fraudeur a utilisé pour effectuer les demandes de PCU à votre nom en vous créant un compte ou en modifiant votre nom d'utilisateur ainsi que votre mot de passe à l'aide de votre NAS et autres identifiants personnels en plus de l'authentification à deux facteurs comme l'envoi d'un code par texto à votre numéro de cellulaire.

5. Protéger votre numéro d'assurance sociale (NAS)

Service Canada propose sur son site Web plusieurs manières de protéger votre NAS telles que le ranger dans un endroit sûr au lieu de le traîner avec vous, ne pas l'utiliser comme pièce d'identité, l'utiliser au téléphone seulement si c'est vous qui avez appelé et que vous savez que la loi l'exige, ne jamais répondre aux courriels dans lesquels on vous demande votre NAS, déchiqueter les dossiers papier contenant votre NAS dès que vous n'en avez plus besoin, etc.

6. Communiquer avec l'Agence du revenu du Canada et l'Agence du revenu du Québec.

Il est important de les informer que vous avez été fraudé afin qu'ils l'inscrivent à votre dossier et qu'ils mettent vos informations à jour, notamment pour que votre prochain chèque de remboursement d'impôts soit livré à votre adresse et non à celle du fraudeur. Assurez-vous également auprès d'eux qu'ils ne vous chargeront pas d'intérêt sur le montant que vous devez actuellement dans le cas où l'enquête dépasse votre délai maximal de paiement dû.

Somme toute, cette mésaventure m'aura procuré son lot de stress. J'ai dû mettre un total de **20 heures pour passer à travers les étapes ci-dessus.** Heureusement, il s'agit de la seule fraude effectuée à mon nom et je n'ai rien eu à débourser pour le moment, mais il sera important pour moi de **bien vérifier que les pénalités de retard reliées au paiement du solde d'impôt à payer ont bien été annulées lorsque l'enquête sera terminée** dans le cas où elle dépasserait le 30 avril 2022, soit la date limite pour payer la somme due de notre avis de cotisation pour l'année d'imposition 2020.

L'ensemble des entreprises se doivent de prendre toutes les mesures préventives pour protéger les données de leurs clients et employés. **Le vol d'identifiants personnels numériques, comme votre nom, prénom, date de naissance, numéro d'assurance sociale, n'est pourtant pas quelque chose de nouveau.** Les compagnies continuent tout de même d'attendre que ça leur arrive avant d'agir. **La cybercriminalité est une réalité bien présente à laquelle on doit faire face en mettant en place les protections adéquates avant d'en devenir victime,** car une cyberattaque peut rapidement se transformer en cauchemar pour la personne ou l'entreprise qui la vit et son personnel.

L'utilisation d'un **SIEM (Security Information and Event Management),** qui sert à détecter les anomalies et comportements douteux, est un outil indispensable aujourd'hui. À partir d'une console centralisant les informations, le SIEM apporte une vue globale sur l'ensemble du réseau, autant pour les activités que les permissions : **qui fait quoi et quand sur les serveurs, qui accède à quoi sur le réseau et particulièrement sur les serveurs, qui a modifié les configurations, les permissions des usagers telles que l'accès aux répertoires de l'entreprise, etc.**

La meilleure option est de vous préparer et de commencer par mettre en place une cybersurveillance. N'hésitez pas à contacter ARS Solutions pour obtenir plus d'informations.

Par : Alyson Lemieux

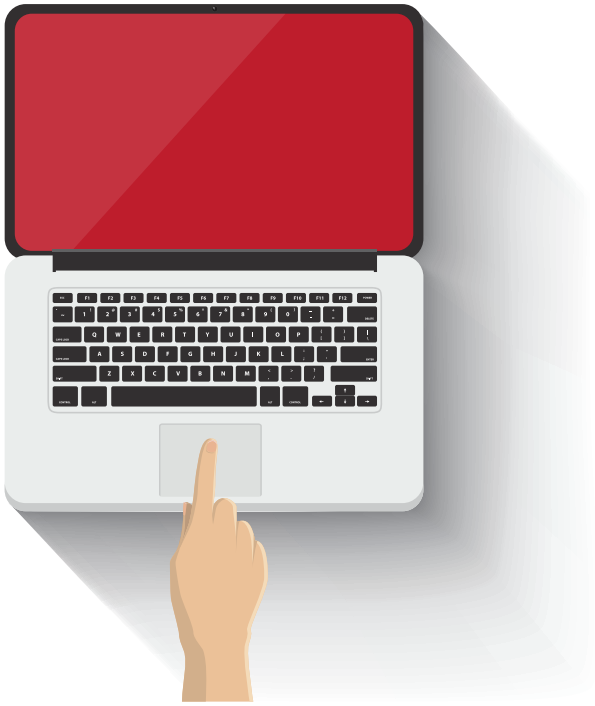
Rapport Cybersécurité 2021

Nous sommes en train de mettre à jour notre rapport Cybersécurité version 2021 qui sera bientôt disponible. **Inscrivez-vous maintenant pour réserver votre version électronique qui vous sera envoyée lors de sa sortie!**

→ **https://www.ars-solutions.ca/services-geres/ - info@ars-solutions.ca - 418-872-4744 #233**

CYBERATTAQUE : Une rançon de 50 millions pour les schémas du MacBook!

TEMPS DE LECTURE 1:50



L'un des secrets les mieux gardés d'Apple, les plans complets nécessaires à la fabrication de sa gamme de MacBooks, a été volé par un groupe de cybercriminels appelé REvil, selon un nouveau rapport de The Record.

REvil affirme avoir pénétré dans Quanta Computer, une société taïwanaise qui fabrique de nombreux ordinateurs portables dans le monde, et affirme qu'il les publiera tous les jours à moins qu'Apple ne lui verse 50 millions de dollars. REvil aurait publié un message sur un forum du Dark Web indiquant que Quanta avait refusé catégoriquement de payer et de récupérer les données volées, raison pour laquelle le groupe vise désormais le plus gros client de Quanta, Apple, à la place. Le groupe a déjà publié 21 captures d'écran de schémas qu'il prétend être officiels.

Pire encore, le groupe affirme être en pourparlers avec "plusieurs grandes marques" pour vendre de grandes quantités de dessins et des "gigaoctets de données personnelles" collectées lors du piratage. Ces informations pourraient être constituées de données provenant de n'importe quel client important de Quanta, comme HP, Dell, Microsoft, Toshiba, LG et Lenovo.

Une question importante demeure : REvil dit-il la vérité?

Apple est vraiment le seul acteur dans cette affaire qui peut confirmer ou infirmer la véracité des affirmations de REvil. Pour l'instant, cependant, le géant de la technologie garde les yeux ouverts et la bouche fermée.

Lorsqu'on lui a demandé de commenter l'affaire, Apple a répondu à The Record qu'elle "examine l'incident" et n'a "rien à partager pour le moment". C'est généralement la manière de procéder d'Apple dans ces cas-là; nous n'entendrons probablement plus parler de l'entreprise jusqu'à ce que l'affaire soit réglée.

Mais les fichiers sont-ils réels?

Les attaques par ransomware sont particulièrement dommageables, car elles tentent d'extorquer des ressources aux entreprises et aux particuliers sans aucune preuve réelle de leurs menaces. Ces menaces sont lourdes, quelle que soit leur véracité.

Dans ce cas, par exemple, on ne sait pas exactement combien de données REvil a réellement recueillies auprès de Quanta. Et si ces données représentent plusieurs gigaoctets d'informations, il est possible qu'une grande partie d'entre elles soient obsolètes ou non pertinentes. L'un des schémas divulgués que REvil utilise comme "preuve" semble être celui du ThinkPad Z60m, un ordinateur portable sorti en 2005.

En ce qui concerne les fichiers d'Apple, les schémas divulgués jusqu'à présent ne représentent que les informations d'assemblage et les spécifications techniques les plus basiques. Rien de sensible, en d'autres termes, sauf si vous craigniez que les malfaiteurs réparent leurs MacBooks.

À moins que REvil, Apple ou Quanta ne nous tiennent informés, il est probable que nous ne connaîtrons jamais l'étendue des documents divulgués. **En mars, REvil a également demandé 50 millions de dollars à Acer, mais aucune des parties n'a encore donné suite à cette demande.**

Source : Matt Wille

Voici pourquoi 65 % des travailleurs à distance ne veulent pas retourner au bureau

2:00 TEMPS DE LECTURE

58%

58 % des personnes interrogées ont déclaré qu'elles chercheraient un nouvel emploi si elles devaient retourner au bureau.

65%

Une enquête réalisée par Flexjobs montre que 65 % des travailleurs à distance pendant la pandémie souhaitent continuer ainsi.

$$$

L'absence de trajet et les économies réalisées sont les principaux avantages du travail à domicile.

Bien que le travail de la maison soit largement préféré, l'enquête a également mis en évidence certains inconvénients tels que la surcharge de travail et les problèmes techniques.

Dans une enquête réalisée par le site d'offres d'emploi Flexjobs, 65 % des télétravailleurs durant la pandémie ont déclaré vouloir continuer à travailler à domicile et 58 % ont même affirmé qu'ils chercheraient un nouvel emploi s'ils devaient retourner au bureau. **Seuls 2 % ont déclaré qu'ils préféreraient y retourner, tandis que 11 % ont affirmé que le travail à distance n'était pas essentiel pour eux.** Avec un tiers des personnes interrogées qui l'ont désigné comme leur mode de travail favoris, le modèle hybride qui combine le travail au bureau et à distance est également populaire.

Les personnes interrogées sont à peu près d'accord sur les principaux avantages du travail à domicile : l'absence de trafic et les économies d'essence réalisées ont été citées par 84 % et 75 % des travailleurs à distance, respectivement. Les raisons qui s'opposent au travail à distance sont plus diverses et comprennent **le surmenage et la possibilité de se débrancher** (35 % des répondants), les distractions à la maison et les problèmes techniques (28 % chacun), ainsi que la difficulté de trouver un réseau Wi-Fi fiable (26 %) et la fatigue des réunions vidéo (24 %).

L'enquête a également révélé que seuls **24 % des télétravailleurs pandémiques disposent d'un bureau à domicile, tandis que 34 % ont créé un espace de travail temporaire.** Le souhait de déménager dans une autre région - un tiers environ a déclaré qu'il le ferait, tandis qu'un autre tiers a envisagé l'idée - pourrait permettre à certains de disposer de plus d'espace de travail. **47 % des personnes interrogées souhaitent déménager pour vivre à moindre coût, mais la recherche d'une meilleure qualité de vie (58 %) est plus importante.**

Source : Katharina Buchholz avec la collaboration de Statista

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