Mars 2022 • Vol. 9 n° 3

# PASSION AFFAIRES et technologies

**Présentés ce mois-ci :**



Entreprise TI classée #1 à Québec en 2021 par **ThreeBest Rated®**

## « ARS Solutions est une compagnie proactive en matière de cybersécurité…

La veille technologique mise en place par leur équipe me permet de **demeurer informée des plus récentes tendances en matière de cybermenaces** via l'infolettre mensuelle ainsi que les courriels hebdomadaires partagés par madame Marie-Josée Galarneau.

L'équipe d'ARS possède une connaissance approfondie des cybermenaces et des meilleures tactiques défensives pour les atténuer. **Leurs solutions de cybersécurité proactives me permettent donc d'avoir l'esprit tranquille** et de rester concentrée sur les enjeux spécifiques à mon domaine. »

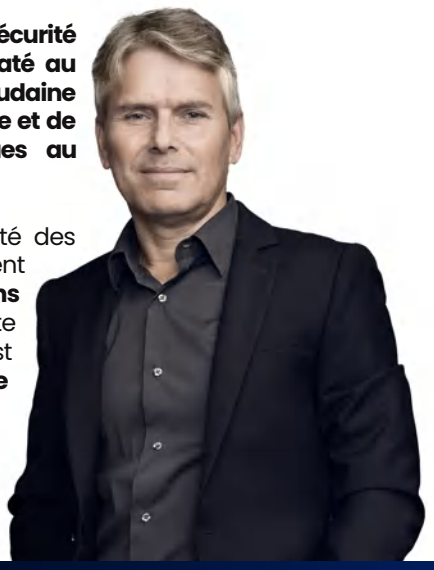
Christine Vézina
**Vice-présidente,**
**Chef de la direction financière**
**Medicart**

# Augmentation de 800 % des attaques d'hameçonnage dues au conflit en Russie

**La société Avanan, spécialisée dans la cybersécurité des courriels, a déclaré qu'elle avait constaté au début du mois de mars une augmentation soudaine et significative des attaques d'hameçonnage et de collecte d'informations d'identification dues au conflit en Russie.**

L'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) a lancé un avertissement le 16 février au sujet d'une campagne de **2 ans en cours menée par la Russie.** La forte augmentation a commencé le 27 février et est environ **8 fois plus importante que le volume normalement observé.**

SUITE PAGE 2



Le PDG d'Avanan, Gil Freidrich, a déclaré que son entreprise traite généralement environ 100 millions de courriels de clients par jour. Pour chaque tranche de 100 000 courriels traités, l'entreprise trouve habituellement entre 30 et 50 attaques d'hameçonnage et, normalement, seule une infime partie de cette activité (environ 1 %) correspond à des attaques de collecte d'informations d'identification. Cependant, les attaques de type russe ont augmenté de façon spectaculaire, passant de 50 à 400 par jour depuis le 27 février. Donc si vous recevez plus de courriels étranges depuis les dernières semaines, il se peut fort bien que ce soit relié.

L'activité observée jusqu'à présent **ne semble pas suivre la même stratégie de masse que celle que l'on observe habituellement** dans les attaques d'hameçonnage. **Les cibles sont des clients des secteurs de la fabrication, de l'expédition internationale et du transport. L'augmentation de ces attaques coïnciderait avec les premiers jours d'une invasion de l'Ukraine par la Russie,** qui a entraîné de sévères sanctions économiques contre le pays et son économie. Ce scénario potentiel a suscité l'alarme des experts en cybersécurité quant à la possibilité de cyberattaques, mais Avanan n'attribue pas les attaques au gouvernement russe et ne confirme pas qu'elles sont liées aux tensions actuelles.

Les appâts utilisés dans ces courriels ne diffèrent pas de ceux que l'on voit habituellement dans le domaine de l'hameçonnage, comme **l'usurpation de l'identité d'un PDG ou d'un employé interne qui envoie des documents "urgents"** ou des courriels Microsoft 365 usurpés vous demandant de cliquer sur un lien pour que votre compte reste actif. La principale différence qu'Avanan constate dans les données est "l'ampleur, et non les méthodes" de ces attaques.

**« Je soupçonne que nous allons commencer à voir peut-être de nouvelles méthodes pour contourner les protections d'Office 365, a déclaré Freidrich. Je ne serais pas surpris que les cybercriminels aient gardé certaines de leurs méthodes de dissimulation les plus sophistiquées pour un événement comme celui-ci. »**

Donc en cas de doute, **ne cliquez sur rien et avisez rapidement votre fournisseur TI pour vérifier la légitimité d'un courriel et éviter sa propagation**. N'hésitez pas à nous contacter pour obtenir de l'aide.

*Source : Derek B. Johnson*

## Conseils anti-hammeçonnage

Continuez de lutter contre la cybercriminalité! Inscrivez-vous pour recevoir nos **NOUVEAUX "conseils anti-hameçonnage" SANS FRAIS** et gardez vos employés alertes. **Vous recevrez ensuite un conseil à tous les mois par courriel.**


**Pour vous inscrire :**
www.ars-solutions.ca/conseils-anti-hameconnage-phase-2/
info@ars-solutions.ca • 418 872-4744 #233

# 6 mois pour se remettre d'une cyberattaque en entreprise

**Six mois après avoir subi une attaque par rançongiciel, Morley Companies a commencé à informer les personnes touchées par l'événement. Des experts indépendants en cybersécurité ont aidé à la récupération.**

Morley Companies, un fournisseur de services aux entreprises de Saginaw, dans le Michigan, a révélé avoir été victime d'une **attaque par rançongiciel le 1er août 2021, qui a permis aux cybercriminels de voler des données appartenant à des employés actuels, d'anciens employés et certains clients.** La vénérable entreprise, fondée en 1863, propose des services commerciaux à des clients du Fortune 500 et du Global 100. M. Morley soupçonne que **des noms, des adresses, des numéros d'assurance sociale, des dates de naissance, des numéros d'identification de clients, des informations sur les diagnostics et les traitements médicaux, ainsi que des informations sur l'assurance maladie** ont été dérobés lors de l'attaque.

## Les fournisseurs de services de sécurité gérés (MSSP) impliqués pour la réponse au cyberincident

**La société a déclaré avoir engagé des "experts indépendants en cybersécurité"**, ce qui semble être une référence aux fournisseurs de services de sécurité gérés et aux analystes de cybercriminalité. Cependant, Morley n'a pas révélé quels fournisseurs TI elle avait engagés. En outre, Morley a déclaré qu'après avoir appris que son infrastructure avait été compromise, elle a pris des "mesures en réponse à cet incident" pour verrouiller son environnement. À la suite d'une enquête, Morley a déterminé que les acteurs de la menace ont volé les informations personnelles de plus de **520 000 personnes, y compris des données appartenant aux employés, aux entrepreneurs et aux clients de Morley,** rapporte BleepingComputer.

À ce stade, Morley a déclaré n'avoir vu aucune preuve indiquant l'utilisation abusive d'informations potentiellement impliquées dans cet incident. Morley a déclaré avoir informé les personnes potentiellement touchées par le cyberévénement et leur avoir fourni un certain nombre de ressources pour les aider, notamment des mesures pour protéger leurs informations personnelles, informer leurs institutions financières et prendre d'autres mesures de protection du crédit. À partir du 1er février 2022, soit six mois après le cyberincident, Morley a commencé à notifier les personnes touchées par l'événement, en leur fournissant des informations sur l'incident et sur les mesures que les personnes potentiellement touchées peuvent prendre pour protéger leurs informations.


## Divulgation tardive d'un cyberincident

Morley s'est attiré quelques critiques pour ce qui semble être une **longue période avant que les personnes potentiellement touchées ne soient informées** de la violation. « Six mois. Six mois entre le moment où la violation a été détectée et celui où les parties concernées ont été informées. », a déclaré Chris Clements, vice-président de Cerberus Sentinel. **« Il est fort probable que les attaquants aient eu accès aux données de Morley pendant des semaines, voire des mois, avant d'exécuter leur rançongiciel qui a bloqué l'accès de Morley et de ses clients à leurs données.** Pendant ce laps de temps, les personnes exposées à un risque de fraude ou d'usurpation d'identité ont pu être activement ciblées tout en étant inconscientes de ce risque », a-t-il déclaré.

**Une cyberattaque peut paralyser une organisation de façon permanente** et les chances de fermer sont malheureusement plus importantes que de s'en sortir. Même si vous vous rétablissez, **vous risquez un arrêt de vos opérations de plusieurs semaines, de perdre des clients et de mettre votre réputation en péril**. Il est moins coûteux d'investir dans des protections proactives. Et comme **la plupart des cyberattaques se produisent dans les entreprises de moins de 1 000 employés**, vous n'êtes pas trop petit pour être une cible. Il ne s'agit plus de savoir si une violation se produira, mais quand elle se produira.

*Source : D. Howard Kass*

# La cyberassurance comme outil de protection des entreprises québécoises?

**Actuellement, les principales cybermenaces sont l'hameçonnage et les mises à jour.** La fréquence des cyberattaques ne cesse d'augmenter, les attaques sont de plus en plus sophistiquées et les cybercriminels de plus en plus audacieux. Le mode de fonctionnement des cyberassurances va donc évoluer. **Il est inévitable que les assureurs ne proposeront pas de police d'assurance aux organisations qui accordent peu d'attention à leur cybersécurité.** De plus, quand on a recours à une cyberassurance suivant une attaque, c'est qu'il est déjà trop tard. Il est donc primordial de mettre en place des mesures de protection dès maintenant.

### Un service encore peu répandu

Avoir une couverture pour les cybermenaces n'est pas encore très courant chez les propriétaires d'entreprise canadienne, révèle un sondage mené par la Fédération canadienne de l'entreprise indépendante (FCEI) auprès de 2 778 de ses membres. 60 % d'entre eux ne détiennent pas de cyberassurance. D'ailleurs, la pandémie n'a pas vraiment accéléré l'acquisition d'une cyberassurance, car seulement 2 % des entrepreneurs répondants disent en avoir acquis une depuis le début de la crise mondiale. Cependant, 13 % des répondants mentionnent avoir un intérêt à s'en procurer une au cours des prochains mois.

### Les cyberrisques sont pourtant bien présents

La FCEI affirme que plus de la moitié des dirigeants s'inquiètent concernant le risque des cyberattaques potentielles. Près de 25 % des PME affirment avoir subi une cyberattaque depuis mars 2020, dont 5 % qui ont été victimes de dommages collatéraux. Aussi, **plus de 80 % des entreprises victimes de cyberattaques ont subi des tentatives d'hameçonnage par courriel**. De plus, 50 % d'entre elles ont été la cible de logiciels malveillants. Selon la FCEI, les entreprises les plus vulnérables sont :

1. Celles qui œuvrent dans les **secteurs manufacturiers et des services professionnels**;
2. Celles qui comptent **20 employés ou plus**;
3. Celles qui ont permis le **télétravail** ou ont pris un tournant numérique durant la pandémie.

« **Lorsqu'une petite entreprise subit une cyberattaque, les effets peuvent être très lourds.** On parle de stress généré par la situation, de pertes financières causées par le vol de renseignements personnels et bancaires et même de dégradation des relations avec les clients. », souligne l'analyste principale à la FCEI, Andreea Bourgeois.

### L'importance de se protéger en amont

Malgré ces constats, 67 % des répondants disent n'avoir fait aucun investissement supplémentaire en cybersécurité depuis le mois de mars. De plus, **60 % d'entre eux affirment n'avoir ni le temps, ni les connaissances ou les ressources nécessaires pour bien protéger leur organisation**. Pourtant, les impacts sont tangibles pour les PME ayant subi une cyberattaque, et ce, autant sur les opérations que sur la santé mentale de ses dirigeants.

Au Québec, toutes les entreprises sont responsables de protéger les renseignements personnels qu'elles détiennent sur leurs employés, leur clientèle et leurs fournisseurs. Malheureusement, **les organisations québécoises sont de plus en plus victimes de cyberattaques de tous types**. C'est pourquoi plusieurs d'entre elles s'interrogent sur la pertinence d'une cyberassurance comme moyen de protection. Mais celle-ci ne garantit pas que vos données seront retrouvées et ne les empêchera pas de se retrouver sur le Dark Web... **La meilleure option est de vous préparer et de commencer par mettre en place les 3 incontournables suivants : une stratégie de sauvegardes adaptée aux rançongiciels, la cybersurveillance et un programme de formation et de simulations d'hameçonnage auprès des employés.** N'hésitez pas à nous contacter pour obtenir de l'aide.

*Source : Hubert Roy, Promutuel et Aviva Canada*


6655, boul. Pierre-Bertrand, bureau 301, Québec, QC G2K 1M1
www.ars-solutions.ca I info@ars-solutions.ca I 418 872-4744