HISCOX

Rapport Hiscox 2022 sur la gestion des cyber-risques

RANSOMWARE – ACTUALISATION

Cover illustration
www.johnholcroft.com

La lutte contre les ransomwares

Les données montrent que seules 59% des entreprises ayant versé une rançon ont réellement récupéré toutes leurs données.

Gareth Wharton
Cyber CEO, Hiscox

C'est une bien triste réalité: les cybercriminels et les entreprises qui se défendent sont engagés depuis dix ans dans un jeu du chat et de la souris à la fois coûteux et risqué. En 2019, nous avons toutefois assisté à un changement important en faveur des cybercriminels. Les attaques par ransomware ont progressé de façon rapide et plusieurs groupes, comme REvil, LockBit et d'autres, sont passés au premier plan. Les attaques contre Norsk Hydro[1] et la ville de Baltimore[2] sont parmi les attaques qui ont fait couler le plus d'encre. Au cours de l'année 2020, les cyber-assureurs ont commencé à fixer de plus en plus d'exigences en matière de cybersécurité à leurs clients. À ce stade, les ransomwares ne concernaient que le chiffrement des données, les assureurs ont donc préconisé des sauvegardes de données hors site afin de minimiser le risque de chiffrement de leurs données critiques par les cybercriminels. Cette tendance a rebattu les cartes dans une certaine mesure, en forçant les gangs de ransomwares à modifier leurs techniques.

Depuis 2020, deux tendances majeures ont évolué. D'abord, les cybercriminels ont commencé à utiliser des techniques dites de double extorsion, consistant d'une part à chiffrer les données et d'autre part à les exfiltrer (voler). En quoi cela a-t-il changé la donne? Même si les clients avaient régulièrement effectué des sauvegardes de leurs données hors site, les cybercriminels pouvaient toujours les contraindre à payer en les menaçant de divulguer les données sensibles volées. Ensuite, la prolifération des offres de ransomware as a service (RaaS) a ouvert des possibilités même aux cybercriminels dotés de peu de moyens. Tout comme le 'software as a service' (SaaS), par lequel les clients souscrivent à un ensemble de services comme des serveurs d'email ou des serveurs collaboratifs, les RaaS permettent aux cybercriminels sans connaissance dans le domaine de la cybercriminalité, de lancer des campagnes de ransomware pour un coût mensuel modique.

Ces deux facteurs ont conduit les assureurs à exiger des contrôles de sécurité informatique nouveaux et plus efficaces. Ainsi, les compagnies d'assurance ont par exemple demandé à leurs clients de ne pas mettre en place de services d'accès à distance non sécurisés, de veiller à ce que les services à distance soient correctement protégés par une authentification à plusieurs facteurs (MFA) et de déployer dans toute l'entreprise les correctifs des services critiques dans un certain délai après leur publication par le fournisseur. Désormais, les entreprises doivent non seulement remplir des formulaires de contrats de cyber-assurance plus complets, mais pour obtenir un devis, elles doivent également souvent améliorer leurs contrôles et procédures de sécurité. Tout cela a pour but de faire en sorte que l'entreprise soit une cible plus difficile à atteindre pour les gangs de ransomware.

Ces contrôles de sécurité ne sont bien entendu pas les seuls outils disponibles pour lutter contre les ransomwares. Les fournisseurs de premier plan et les gouvernements ont un intérêt à lutter contre la menace des ransomwares. Par exemple, l'une des techniques les plus courantes des gangs de ransomware consiste à envoyer des emails de phishing avec des documents Microsoft Office en pièce jointe qui contiennent des macros dans le but de télécharger les premiers éléments d'une attaque par ransomware. Cette année, Microsoft a annoncé qu'elle bloquerait les macros Office par défaut. Bien que cela constitue une avancée positive, les gangs de ransomware se tournent déjà vers des types de fichiers différents comme les .lnk ou .iso. Cela montre la rapidité à laquelle évolue ce jeu du chat et de la souris.

Les gouvernements jouent également un rôle central dans la lutte contre les ransomwares, grâce à des opérations plus offensives. Au cours des 18 derniers mois, les États-Unis et l'Union européenne ont ciblé les gangs de ransomware. À titre d'exemple, l'action d'Interpol contre Clop[3], l'action des États-Unis contre le gang Darkside[4] et la neutralisation par Interpol du célère botnet Emotet[5]. Par ailleurs, les gouvernements essaient de limiter la possibilité pour les cybercriminels d'encaisser des cryptomonnaies. Cela contraint les gangs de ransomware à mener d'autres types d'attaques ou à viser d'autres cibles que les entreprises américaines ou européennes. Enfin, les agences gouvernementales, telles que la CISA aux États-Unis et la NCSC au Royaume-Uni, ont été beaucoup plus proactives en alertant sur de potentielles attaques comme la vulnérabilité Log4j au mois de décembre 2021.

Ainsi, au vu de l'évolution des ransomwares au cours des dernières années, quel tableau dresser aujourd'hui des ransomwares? En regardant les données du Rapport Hiscox 2022 sur la gestion des cyber-risques, nous pouvons mieux comprendre ce à quoi les clients sont réellement confrontés. Le rapport se base sur les conclusions d'une enquête menée auprès de plus de 5,000 entreprises de tailles et secteurs différents, issues de huit pays.

[1] https://www.bbc.co.uk/news/business-48661152

[2] https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack

[3] https://www.bleepingcomputer.com/news/security/operation-cyclone-deals-blow-to-clop-ransomware-operation/

[4] https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-operation-shuts-down/

[5] https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

La lutte contre les ransomwares
Suite

Les données montrent que seules 59% des entreprises ayant versé une rançon ont réellement récupéré leurs données. Il est important de comprendre que payer pour obtenir une clé de déchiffrement ne signifie pas que vous récupérerez toutes vos données. Dans presque tous les cas que nous avons observés, les cybercriminels fournissent effectivement une clé de déchiffrement, étant donné qu'il s'agit pour eux d'une opération commerciale. Deux choses peuvent néanmoins limiter l'efficacité d'une clé de déchiffrement fonctionnelle. La première est la vitesse car il faut généralement des semaines pour déchiffrer totalement les données. Deuxièmement, lorsque la routine de chiffrement malveillante est lancée, elle s'exécute sur des systèmes transactionnels en cours de fonctionnement. Cela équivaut à débrancher le cordon d'alimentation d'un serveur de base de données en fonctionnement, et il est vraisemblable que le ransomware portera atteinte à l'intégrité des données. En d'autres termes, le fait que le ransomware se soit exécuté, même si l'on obtient une clé de déchiffrement, implique que les données ne pourront pas être totalement récupérées et qu'elles devront être reconstruites. Quarante-trois pour cent des participants de l'étude qui ont versé une rançon ont indiqué avoir reçu la clé de récupération, mais ont néanmoins été contraints de reconstruire leurs systèmes. De façon toute aussi alarmante, 36% des entreprises qui ont versé une rançon ont subi une autre attaque.

Les secteurs les mieux et les moins bien préparés (%)

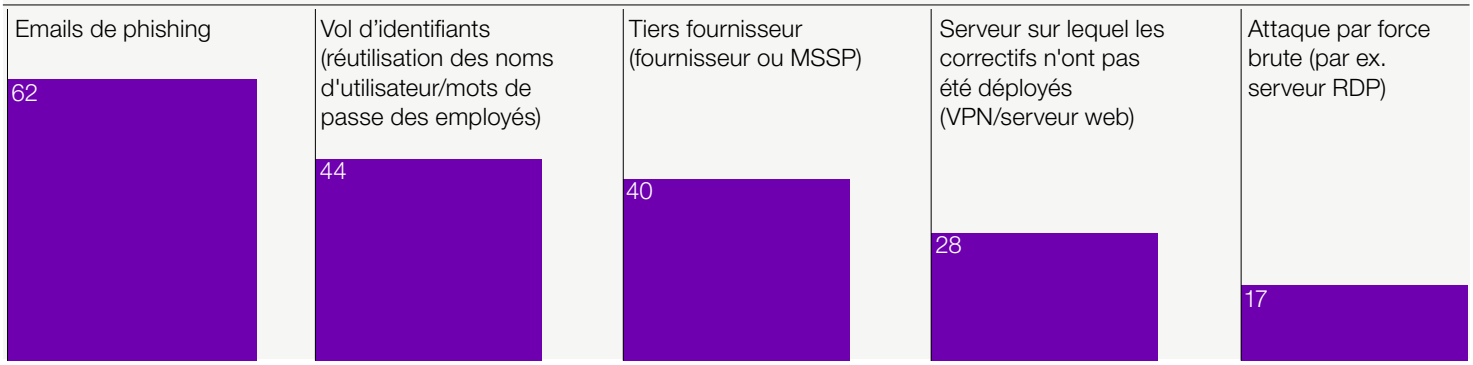
La plupart des journaux se font l'écho des rançons versées lorsqu'il s'agit d'une entreprise connue ou lorsque la demande de rançon est importante (par ex. plusieurs millions de dollars). Toutefois, notre recherche montre que la rançon médiane versée était inférieure à $10 000. Cela montre que les ransomwares ne sont pas uniquement des attaques complexes de grande ampleur menées sur des grandes entreprises par des gangs connus, mais qu'il s'agit désormais d'un mode d'attaque basique utilisé par des pirates dotés de moindres moyens. L'enseignement essentiel est que les petites et moyennes entreprises ne sont absolument pas épargnées par ce type d'attaques.

Nous observons également une disparité, à savoir que certains secteurs sont davantage ciblés par les demandes de rançon. Lorsqu'on observe le pourcentage de participants ayant versé une rançon par secteur, cela donne une indication sur les secteurs dans lesquels les entreprises sont le mieux et le moins bien préparées.

Ces observations corroborent en grande partie notre expérience. Les entreprises des secteurs des services professionnels et des services financiers ont souvent les liquidités pour mettre en place des programmes de sécurité plus rigoureux, ils sont donc mieux protégés et disposent de la capacité de répondre à une éventuelle attaque. En outre, les secteurs les moins bien préparés sont ceux dont les pans de la chaine logistique sont parmi les plus étroits et au sein desquels la réglementation est moins contraignante. Si une attaque se produit, ces entreprises ne peuvent se permettre de sortir du jeu trop longtemps, et verser la rançon semble souvent la seule option.

Lorsque nous observons les données relatives au mode d'intrusion des cyber-pirates dans les systèmes des participants de notre étude, le constat est malheureusement très classique. Il existe 5 modes d'intrusion principales, et au vu de nos données, toutes ces méthodes sont mises en œuvre. Bien que ces techniques d'attaque soient testées et éprouvées par les gangs de ransomware, il n'est pas impossible de s'en prémunir.

Modes d'intrusion les plus communs (%)



La lutte contre les ransomwares
Suite

Cet été, Hiscox a mené une analyse complémentaire sur la menace du phishing. Selon un test récent mené auprès de cinq entreprises, nous avons observé qu'un test de phishing générique n'est pas suffisant pour stopper un ransomware.

Nous avons réalisé deux tests auprès de ces cinq entreprises. La première simulation consistait à utiliser un prestataire de tests de phishing bien connu et des leurres standards (colis Amazon, alerte LinkedIn, etc.). Le taux de clics global suite à l'envoi d'emails en masse dans cette première simulation était de 9%. À titre d'observation intéressante, le plus efficace des 5 leurres était un email Office 365 concernant la réinitialisation d'un mot de passe. Bien que cela ne soit pas surprenant compte tenu du déploiement massif d'Office 365, le fait que les personnes piégées aient cliqué quatre fois plus souvent sur ce leurre que sur les autres est édifiant.

Dans la deuxième simulation, nous avons utilisé un email ciblé conçu uniquement et spécifiquement pour chaque entreprise, mais avec un effort d'ingénierie social minimal. Nous avons par ailleurs ciblé des membres de la direction plutôt qu'une population de salariés plus générale. Dans ce scénario, le taux de clics a été multiplié par quatre pour atteindre 36%. Cela montre que si la formation contre le phishing est un élément essentiel des besoins de sécurité d'une entreprise, il convient également de mettre en œuvre une formation ciblée pour les dirigeants.

Dans la mesure où il n'y a pas de solution miracle une fois que l'entreprise a été attaquée par un ransomware, il est donc nécessaire de limiter le risque autant que possible.

Mesures pour prévenir une attaque par ransomware:

Mode d'attaque	Mesure de prévention
Email de phishing	Formation générale et spécialisée du personnel, sécurité forte des emails
Vol d'identifiants (réutilisation des noms d'utilisateur/ mots de passe des employés)	Formation du personnel concernant l'utilisation de mots de passe uniques, MFA
Third party (supplier or MSSP)	Compréhension des chaines logistiques, audits réguliers
Serveur sur lequel les correctifs n'ont pas été déployés (VPN/serveur web)	Inventaire des logiciels (SBoM) pour savoir de quoi est composé votre parc, déploiement régulier des correctifs
Attaque par force brute (par ex. serveur RDP)	Formation du personnel à l'utilisation de mots de passe uniques, MFA, contrôles 'juste-à-temps' des ports ouverts sur Internet

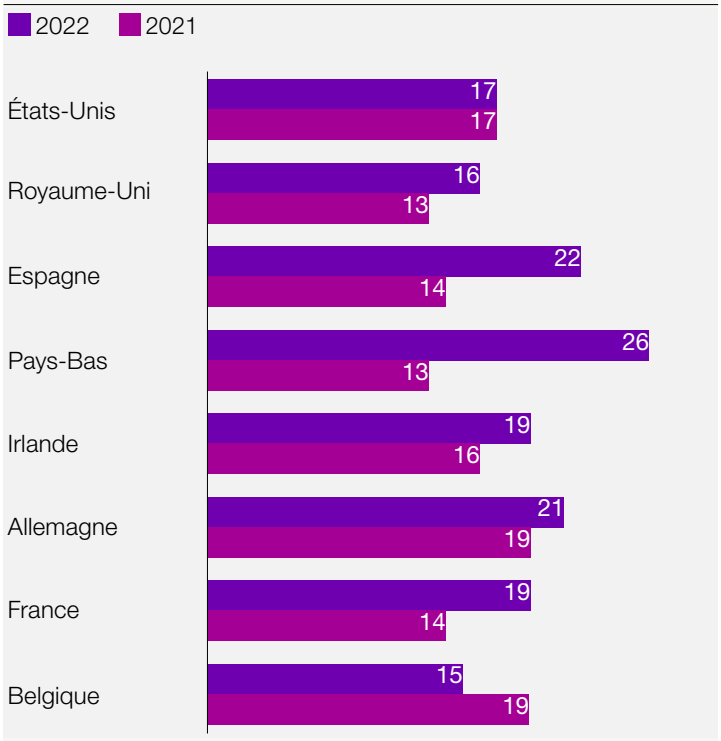
Si le pire se produit, comment atténuez-vous les conséquences d'une attaque par ransomware?

- Assurez-vous de réaliser des sauvegardes hors ligne fiables, fréquentes et testées. Pour les petites entreprises, cela peut simplement consister à emporter des disques durs chez soi ou à les stocker hors ligne.
- Préparez-vous au pire: assurez-vous de disposer d'un plan de réponse en cas d'attaque par ransomware et de le tester fréquemment. Qui appelleriez-vous, comment communiqueriez-vous avec le personnel, les clients, les parties prenantes, les médias etc.?
- Obtenez de l'aide auprès de votre fournisseur informatique, avez-vous besoin des services d'un prestataire de réponse aux incidents de sécurité (PRIS)?
- Cyber-assurance – bénéficiez des services d'un prestataire de réponse aux incidents de sécurité par l'intermédiaire de votre assureur pour gérer l'incident et remettre votre entreprise en ordre de marche.
- Ne paniquez pas, prenez le temps d'évaluer la situation et les options dont vous disposez avant de prendre des mesures.

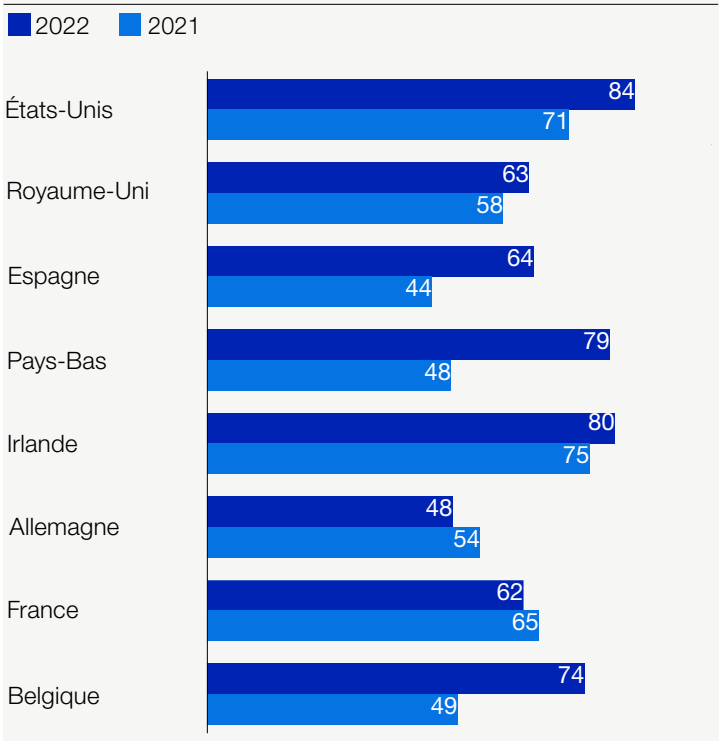
Les ransomwares constituent une menace pour toutes les entreprises, quels que soient leur taille, leur secteur ou leur localisation. Cette menace doit être prise très au sérieux par tous les acteurs, clients, assureurs et gouvernements. L'action coordonnée s'est révélée efficace, mais il existe bien d'autre mesures à prendre. C'est une menace contre laquelle vous pouvez et vous devez vous défendre, dans la mesure où, comme nous l'avons expliqué, une fois que vous avez été attaqué, il n'est jamais simple de reprendre ses activités normalement. La plupart des entreprises sont la cible des ransomwares de base, et non d'acteurs étatiques de premier ordre, elles doivent donc s'efforcer de se prémunir au maximum contre les attaques. Quoi qu'il en soit, il est tout aussi important de disposer d'un plan au cas où le pire se produirait, un plan testé et de bonnes sauvegardes. Nous vous recommandons d'utiliser l'outil en ligne **'Exercise in a box'** de la NCSC, qui permet aux entreprises de tester leur réponse en cas de cyber-attaque, c'est un bon point de départ. **(https://www.ncsc.gov.uk/information/exercise-in-a-box).**

Quels pays sont attaqués ? lesquels paient ?

Entreprises ayant subi un ransomware (%)



Entreprises ayant subi un ransomware et versé une rançon (%)



Pourquoi les entreprises ont-elles payé une rançon ?

Dans de nombreuses attaques, les gangs de rançongiciels ciblent délibérément les sauvegardes, il y a ainsi une vraie nécessité d'effectuer des sauvegardes séparées pour être à nouveau opérationnel.

Les entreprises se doivent de protéger les données clients lorsque la fuite de données se produit et qu'il y a menace de publication des données.

Raisons pour lesquelles les entreprises ont versé une rançon (%)

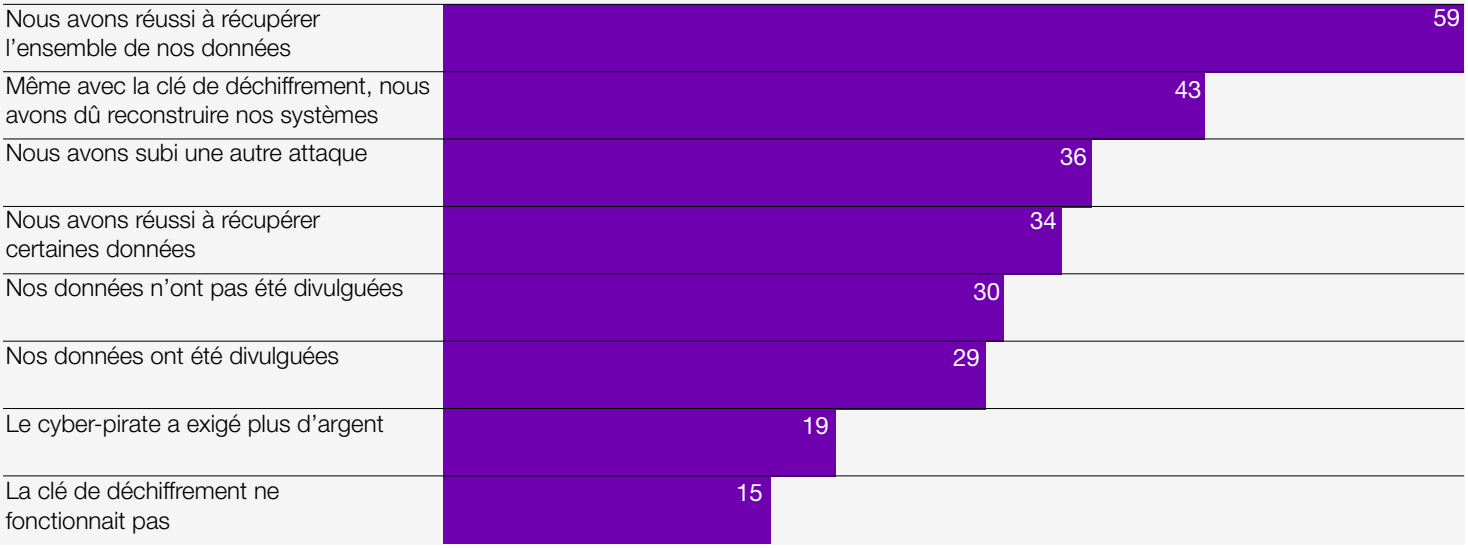
Le paiement des rançons a-t-il fonctionné ?

Seules **59%** des entreprises récupèrent entièrement leurs données. En effet dans de nombreux cas, l'ensemble des données n'a pas pu être récupéré même après le paiement.

Pour les gangs de ransomwares, il n'y a aucun avantage à ne pas donner les clés de déchiffrement. Toutefois cela ne veut pas dire qu'il sera aisé de reprendre ses activités immédiatement avec la clé.

En plus, pour 36% de ceux qui ont payé une rançon, le ransomware initial a tout de même conduit à de nouvelles attaques par la suite.

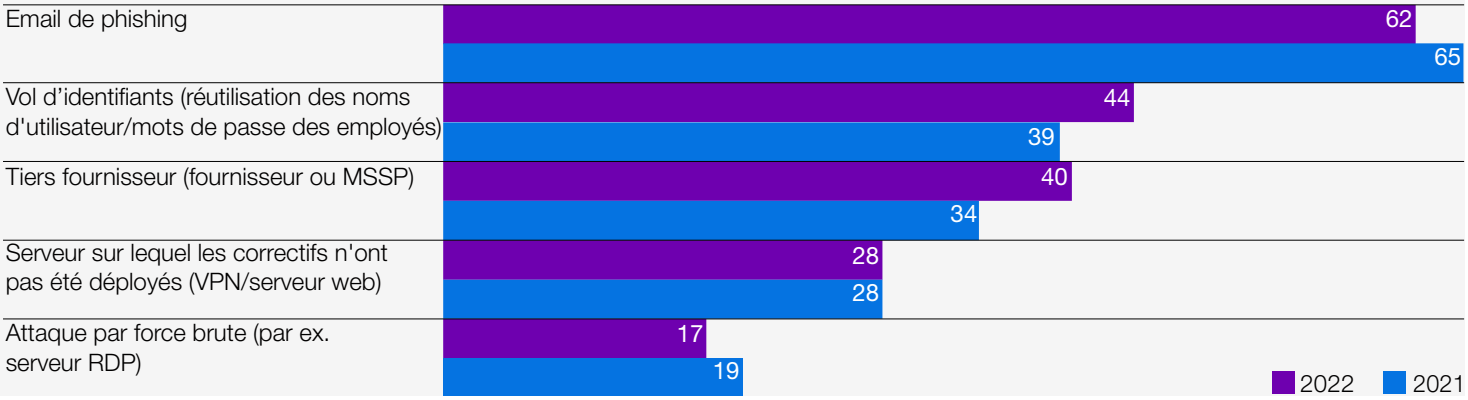
Conséquences du paiement de la rançon (%)



Comment les cyber-criminels entrent-ils ?

Cinq méthodes d'entrée sont utilisées. Cinq méthodes d'entrée sont utilisées. Chacune est essayée et testée par des gangs de Ransomware, il n'est donc pas impossible de se défendre.

Modes d'intrusion (%)



D'après un récent test réalisé par Hiscox auprès de cinq entreprises, un test de phishing générique n'est pas suffisant pour arrêter les ransomwares. Selon Beauceron Security, le taux de clics moyen varie de 3,4% à 12%. En effet, le taux de clics global suite à l'envoi d'emails en masse dans le test d'hameçonnage générique était de 9%. Mais sur la cible des cadres supérieurs, ce taux grimpait à 36%, soit plus du double de la moyenne. Une formation ciblée pour les cadres supérieurs est donc particulièrement important.

Hiscox Ltd

Chesney House
96 Pitts Bay Road
Pembroke HM 08
Bermuda

+1 441 278 8300
enquiries@hiscox.com
hiscoxgroup.com/cyber-readiness

22161 11/22