LIVRE BLANC

Meilleures pratiques pour lutter contre le phishing et les ransomwares

Un livre blanc publié par Osterman Research

en septembre 2016

Sponsorisé par

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010–1058 • USA
Tel.: +1 (0)206 683 56 83 • Fax: +1 (0)253 458 09 34 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

RÉSUMÉ ANALYTIQUE

Le phishing et les ransomwares posent de sérieux problèmes, car ils peuvent voler ou désactiver l'accès à la situation financière personnelle ou de l'entreprise, aux données sensibles sur les employés, aux données du patient, à la propriété intellectuelle, aux dossiers des employés et aux autres contenus précieux. Les attaques d'hameçonnage et de ransomwares et leurs variantes (telles que le harponnage et l'arnaque au président/arnaque BEC (« Business Email Compromise ») sont de plus en plus courantes et ont des effets dévastateurs sur les entreprises de toutes tailles. L'impact financier de la cybercriminalité en général, et du phishing et du ransomware en particulier, est difficile à évaluer pour diverses raisons, mais le FBI estime que les ransomwares ont coûté à eux seuls aux organisations 209 millions de dollars au cours des trois premiers mois de 2016i.[i]

Le phishing, qui peut être considéré comme le mécanisme de prestation de choix pour les différents types de logiciels malveillants et pour les tentatives de cybercriminalité, et le ransomware, qui est une forme spécialisée de logiciels malveillants conçus dans le seul but d'extorquer de l'argent aux victimes, sont des problèmes graves que chaque organisation doit résoudre par divers moyens : la prise de conscience des utilisateurs, des solutions de sécurité, l'analyse de la vulnérabilité, des renseignements concernant les menaces, des procédures adaptées de sauvegarde et même avec du bon sens. La bonne nouvelle est que les organisations peuvent faire beaucoup de choses pour se protéger et protéger leurs données, leurs employés et leurs clients.

CE QU'IL FAUT RETENIR

- Le phishing et le crypto-ransomware[ii] augmentent au rythme de plusieurs centaines de pour cent par trimestre, une tendance qui, selon Osterman Research, se poursuivra pendant au moins les 18 à 24 prochains mois.
- La grande majorité des organisations ont été victimes d'hameçonnages, de ransomwares et d'une multitude d'attaques ciblant la sécurité au cours des 12 derniers mois. En fait, le phishing et les ransomwares sont parmi les quatre principales préoccupations des décideurs en matière de sécurité, comme l'a découvert Osterman Research lors de l'enquête menée pour ce livre blanc.
- Les dépenses en matière de sécurité vont augmenter de manière significative en 2017 puisque les organisations se rendent compte qu'elles ont besoin de se protéger contre le phishing, les ransomwares et le nombre croissant d'autres menaces auxquels elles sont confrontées.
- La plupart des organisations n'observent pas d'améliorations dans les solutions de sécurité qu'elles ont déployées et dans les pratiques de sécurité qu'elles suivent. Bien que beaucoup de ces solutions sont efficaces, la plupart ne s'améliorent pas avec le temps, dans de nombreux cas parce que le personnel interne ne dispose pas des compétences nécessaires pour améliorer la performance de ces solutions au fil du temps. Dans l'ensemble, seulement deux de ces solutions et pratiques sur cinq sont considérées comme « excellentes ».
- La formation de sensibilisation à la sécurité est un domaine essentiel pour l'amélioration de la protection des organisations contre le phishing et les ransomwares. En effet, notre recherche a révélé que les organisations avec des employés bien formés sont moins susceptibles d'être infectées.
- Il existe de nombreuses bonnes pratiques que les organisations devraient suivre afin de minimiser le risque de devenir des victimes d'hameçonnage et de ransomwares. Parmi ces bonnes pratiques, on trouve : la mise en place de programme de sensibilisation à la sécurité, le déploiement de systèmes qui permettent de détecter et d'éliminer les tentatives d'hameçonnage et de rançonnage, la recherche et la correction des vulnérabilités de sécurité dans les systèmes d'entreprise, le maintien de bonnes sauvegardes et l'utilisation efficace des renseignements concernant les menaces.

Le phishing et le crypto-ransomware augmentent au rythme de plusieurs centaines de pour cent par trimestre, une tendance qui selon Osterman Research se poursuivra pendant au moins les 18 à 24 prochains mois.

À PROPOS DE CE LIVRE BLANC

Ce livre blanc est sponsorisé par Barracuda (vous trouverez des informations sur cette société à la fin de ce livre).

PRÉOCCUPATIONS MAJEURES DE SÉCURITÉ

QUELLE EST LA GRAVITÉ DU PROBLÈME ?

Le nombre d'hameçonnages, de ransomwares et d'autres types de menaces empire considérablement au fil du temps. Par exemple :

- Le groupe APWG (Anti-Phishing Working Group) a observé une augmentation de 250 % du nombre de sites Web hameçonnés entre le quatrième trimestre de 2015 et le premier trimestre de 2016.[iii]
- McAfee Labs a découvert près de 1,2 million d'attaques par des ransomwares au cours du premier trimestre de 2016, une augmentation de 24% par rapport au quatrième trimestre de 2015.[iv]
- Une étude Kaspersky menée au cours des années 2014 et 2015 a révélé que le total des attaques de ransomwares pendant la période d'analyse a augmenté de 17,7%, mais que les variantes de cryptologiciels ont augmenté de 448% au cours de cette période.[v]
- Un document inter-institutions du gouvernement américain publié par le Département de la Justice des États-Unis en 2016 a indiqué que plus de 4 000 attaques de ransomwares se sont produites chaque jour depuis le début de l'année, une augmentation de 300 % par rapport à 2015.[vi]
- Selon le rapport 2015 de Trustwave Global Security, les attaquants reçoivent un retour sur investissement d'environ 1 425% pour les kits d'exploitation de vulnérabilités et les systèmes de ransomwares (84 100 $ du revenu net pour chaque tranche d'investissement de 5 900 $).

Le phishing, et en particulier les formes d'hameçonnage extrêmement ciblées comme le harponnage et l'arnaque au président/arnaque BEC, ainsi que les ransomwares, sont l'évolution logique de la cybercriminalité. Il y a une surabondance de ces informations sur le marché, car il y a eu de nombreuses violations de données au cours des dernières années ayant entraîné le vol de centaines de millions d'enregistrements. Il en résulte, comme dans toute autre entreprise motivée par la loi de l'offre et de la demande, que les prix pour les enregistrements volés sont en chute libre : une grande entreprise de sécurité estime que le prix d'un enregistrement de carte de paiement volée est passé de 25 $ en 2011 à seulement 6 $ en 2016.

Ainsi, les cybercriminels ont de plus en plus recours à des moyens de vol plus directs. Par exemple, un ransomware va extorquer de l'argent directement aux victimes sans qu'il soit nécessaire de vendre des données volées sur le marché libre où elles sont soumises à des forces économiques qui peuvent réduire leur valeur. L'arnaque au président/arnaque BEC peut rapporter des centaines de milliers voire des millions de dollars en peu de temps en amenant les victimes à transférer directement des fonds.

INCIDENTS DE SÉCURITÉ AU COURS DES 12 DERNIERS MOIS

Les recherches réalisées pour ce livre blanc ont révélé qu'un grand nombre d'incidents de sécurité se sont produits au cours des 12 derniers mois parmi les organisations interrogées. Les incidents les plus courants impliquaient des attaques d'hameçonnage ayant réussi à infiltrer le réseau de l'entreprise, des attaques de ransomwares réussies et des infiltrations malveillantes via certaines sources inconnues, comme le montre la figure 1. Cependant, de nombreux incidents de sécurité ont eu lieu. D'ailleurs, seulement 27% des organisations interrogées ont déclaré ne pas avoir rencontré l'un des problèmes de sécurité indiqués dans la figure ci-dessous.

De plus, nos recherches ont démontré que les incidents de sécurité ne sont pas isolés et se produisent fréquemment.

- 51 % des organisations interrogées ont subi une à cinq infections par un ransomware, infiltrations par un pirate informatique, infections par un programme malveillant, et autres attaques, car un employé a cliqué sur un lien ou sur une pièce jointe d'hameçonnage. 13 % de plus ont subi entre six et dix attaques de ce genre, et 11 % plus de 10 attaques.

Le phishing, notamment les types d'hameçonnage très ciblés comme le harponnage et l'arnaque au président/arnaque BEC, ainsi que les ransomwares, constitue l'évolution logique de la cyber-criminalité.

- Bien que les attaques avec arnaque au président ou arnaque BEC soient moins courantes que le phishing ou les ransomwares, 27 % des organisations ont fait face à ce type d'attaques lors des 12 derniers mois : 24 % des organisations ont subi jusqu'à cinq attaques de ce genre au cours de l'année dernière, tandis que 2 % ont subi entre six et dix attaques et 2 % plus de dix attaques.

Figure 1
Incidents de sécurité ayant eu lieu lors des 12 derniers mois

Problème	% des organisations atteintes
Une attaque d'hameçonnage par e-mail a réussi à infiltrer notre réseau.	34
Un ou plusieurs de nos points de terminaison contenaient des fichiers chiffrés suite à l'attaque d'un ransomware.	30
Un logiciel malveillant a infiltré notre réseau, mais nous ne sommes pas certains du canal utilisé.	29
Des informations sensibles/confidentielles ont été dévoilées de façon accidentelle ou malveillante par e-mail.	17
Une attaque de harponnage par e-mail a réussi à infecter un ou plusieurs de nos cadres supérieurs.	14
Notre réseau a été infiltré par une attaque « drive-by » (dissimulée derrière un site Web) suite à la navigation sur le Web d'un employé.	12
Un e-mail dans le cadre d'une attaque avec arnaque au président ou arnaque BEC a réussi à tromper un employé de notre organisation.	11
Des informations sensibles/confidentielles ont été dévoilées de façon accidentelle ou malveillante par l'intermédiaire d'un outil sur le Cloud, tel que Dropbox.	5
Des informations sensibles/confidentielles ont été dévoilées de façon accidentelle ou malveillante par l'intermédiaire d'une application de média social.	3
Des informations sensibles/confidentielles ont été dévoilées de façon accidentelle ou malveillante, mais la méthode reste inconnue.	1
Aucun de ces incidents n'a eu lieu	27

Source : Osterman Research, Inc.

EXEMPLES DE HAMEÇONNAGE, DE RANSOMWARES ET D'ARNAQUE AU PRÉSIDENT OU ARNAQUE BEC

Voici quelques exemples d'hameçonnage, de ransomwares et d'autres attaques associées qui ont eu lieu lors des derniers mois :

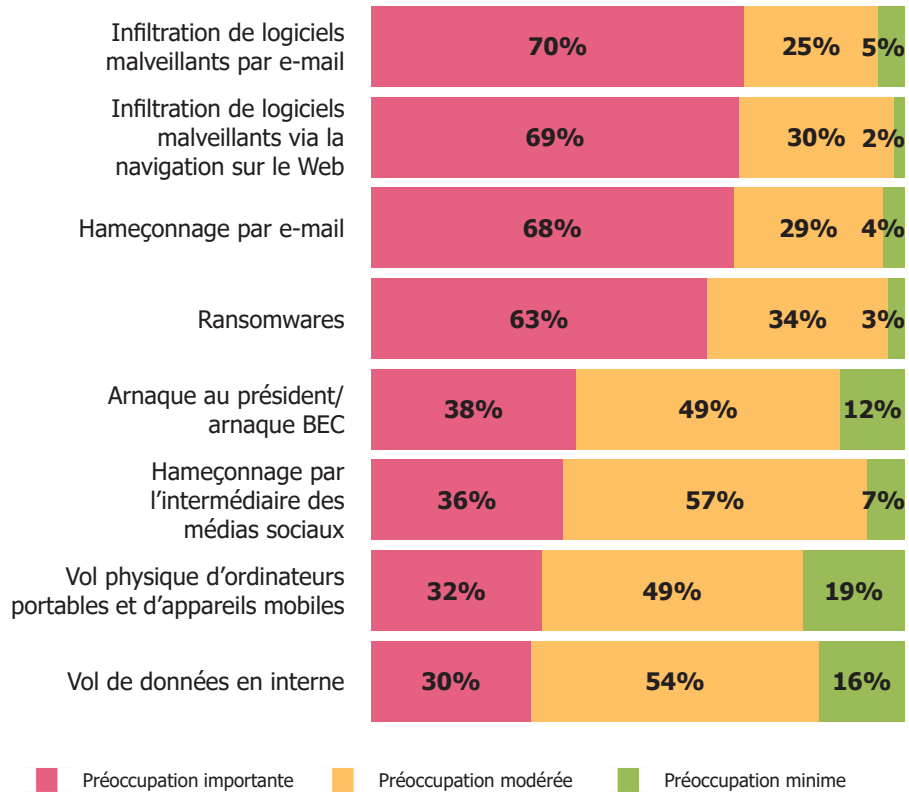
- En août 2016, la Bournemouth University a découvert qu'elle avait été infectée 21 fois lors des 12 mois précédents par un ransomware, soit une infection tous les 17 jours.[vii]
- Leoni AG, un important fabricant allemand de fibre optique, de câbles et de produits connexes a dévoilé en août 2016 qu'il avait été victime d'une attaque avec arnaque au président/arnaque BEC. Les cyber-criminels responsables de l'extorsion de 44 millions de dollars avaient apparemment étudié les processus de paiement de la société, probablement grâce à de précédentes attaques d'hameçonnage leur ayant permis de s'infiltrer dans le réseau de l'entreprise, et ont ainsi pu convaincre la directrice financière de l'usine située à Bistrita (en Roumanie) de la société que l'e-mail frauduleux qu'elle avait reçu était véritablement envoyé par un des cadres de la société en Allemagne.[viii]
- En avril 2016, MedStar Health, un réseau de 10 hôpitaux situés dans le Maryland, a été infecté par le ransomware SamSam (Samas), qui a neutralisé leurs systèmes. Une source a identifié qu'une vulnérabilité dans le serveur de l'application Web JBoss a été utilisée par les cyber-criminels pour mener leur attaque à bienix.[ix]

- En février 2016, le service de paie de Snapchat a été victime d'une attaque d'hameçonnage qui a entraîné la divulgation d'informations sensibles sur l'entreprise à un tiers non autorisé. Ces informations comprenaient le nom des victimes, leur numéro de sécurité sociale, leurs salaires de 2015, leur État de résidence, l'État de leur lieu de travail, leurs cotisations d'employé pour leur compte de retraite, l'impôt retenu, ainsi que d'autres données sensibles.[x]
- En février 2016 également, le Hollywood Presbyterian Medical Center a été victime du ransomware Locky, qui a perturbé son fonctionnement pendant environ deux semaines avant que l'administration de l'hôpital ne paie 40 Bitcoin (environ 17 000 dollars) pour récupérer ses fichiers.[xi]
- En juin 2015, des employés d'Ubiquiti Networks ont été victimes de plusieurs attaques avec arnaque au président/arnaque BEC qui ont provoqué le transfert de 46,7 millions de dollars aux cyber-criminels. Ces attaques de harponnage, qui ciblaient des employés du service financier d'Ubiquiti, ont utilisé une simple méthode d'usurpation d'adresse e-mail.[xii]

PROBLÈMES QUI INQUIÈTENT LE PLUS LES DÉCIDEURS

Les DSI, les responsables informatiques, les directeurs informatiques, les officiers principaux de la sécurité de l'information ainsi que les autres décideurs liés à la sécurité redoutent un large éventail de problèmes de sécurité. Cependant, tel qu'indiqué dans la figure 2, ils s'inquiètent surtout des infiltrations de logiciels malveillants par e-mail et par l'intermédiaire de la navigation sur le Web, du hameçonnage par e-mail et des ransomwares. Ils se préoccupent également des arnaques au président ou arnaques BEC, du hameçonnage sur les médias sociaux ainsi que des méthodes plus classiques de pertes de données, tels que le vol physique d'appareil et les activités malveillantes des employés.

Figure 2
Problèmes qui préoccupent les décideurs liés aux domaines de l'informatique et de la sécurité



Remarque : les totaux peuvent ne pas correspondre à 100 % en raison d'erreurs d'arrondis.
Source : Osterman Research, Inc.

De nombreuses attaques utilisent les e-mails, et les liens et pièces jointes qu'ils contiennent, comme principale méthode d'infiltration. Beaucoup d'utilisateurs sont en « surdose d'informations » en ce qui concerne leurs e-mails.

QU'EST-CE QUI REND LE PHISHING ET LES RANSOMWARES AUSSI EFFICACES ?

Le succès des tentatives d'hameçonnage et d'infiltration par des ransomwares dépend d'un certain nombre de facteurs, notamment : la naïveté ou le manque de méfiance des victimes lorsqu'elles reçoivent des e-mails où font face à d'autres pièges tendus par des cyber-criminels, la quantité et la qualité de la formation qu'elles ont suivie, la qualité de l'infrastructure de sécurité de leur organisation et la quantité d'informations qu'elles peuvent rassembler pour lutter contre les attaques potentielles.

Cependant, certains critères font que le phishing et les ransomwares sont particulièrement efficaces de nos jours :

- De nombreuses attaques utilisent les e-mails, et les liens et pièces jointes qu'ils contiennent, comme principale méthode d'infiltration. Beaucoup d'utilisateurs sont en « surdose d'informations » en ce qui concerne leurs e-mails, ce qui fait qu'ils sont moins susceptibles de vérifier prudemment les tentatives d'hameçonnage, d'arnaque au président ou arnaque BEC ou toute autre tentative. Une enquête de Osterman Research datant de juillet 2016 sur les utilisateurs finaux[xiii] a révélé que 94 % des utilisateurs éprouve un certain niveau d'overdose d'informations par e-mail, et 32 % indiquent qu'ils souffrent « considérablement » de cet amas d'informations.
- Les cyber-criminels créent du contenu de plus en plus pertinent afin de tromper les utilisateurs et de passer outre les technologies de détection. L'utilisation de logos, le ton professionnel des messages ainsi que la personnalisation du contenu rendent les tentatives d'hameçonnage plus convaincantes. Ainsi, les victimes potentielles sont plus susceptibles de cliquer sur les liens et les pièces jointes contenues dans les e-mails. L'amélioration des méthodes des cyber-criminels s'explique notamment par le fait qu'ils ont tendance à travailler pour des organisations criminelles très bien financées, qui disposent des ressources financières et techniques nécessaires pour améliorer leurs techniques.
- Les cybercriminels mettent au point de nouvelles formes de ransomwares plus efficaces, ainsi que des méthodes améliorées de communication aux systèmes infectés. En partant des ransomwares plus classiques de verrouillage de données qui constituaient la norme il y a quelques années, des variantes basées sur le chiffrement ont émergé, comme CryptoWall (2014), CTB-Locker (2014), TeslaCrypt (2015), Samas (2016), Locky (2016) et Zepto (2016). De plus, le ransomware en tant que service devient plus courant ; par exemple, le service Cerber avait infecté 150 000 points de terminaison en juillet 2016 et engrangé des bénéfices de près de 200 000 $ par mois.[xiv]
- De nombreux utilisateurs partagent trop d'informations sur les réseaux sociaux, et donnent ainsi des renseignements que les cybercriminels peuvent utiliser pour créer des messages courriels personnalisés et plus crédibles, donc plus difficiles à détecter.
- Certaines solutions anti-hameçonnage et anti-ransomwares ne sont pas soutenues par une base de données suffisamment solide d'intelligence de messagerie en temps réel, et ne peuvent donc pas détecter les dernières techniques utilisées par les spécialistes de le phishing et des ransomwares.
- De nombreux utilisateurs sont formés de façon inadaptée sur le phishing et les ransomwares, ainsi que sur les meilleures pratiques de gestion des menaces inconnues. Cela s'explique par le fait que beaucoup d'utilisateurs ne sont tout simplement pas suffisamment sceptiques lorsqu'ils reçoivent des demandes pour effectuer des actions comme virer des fonds, ouvrir des pièces jointes ou transmettre des informations sensibles.
- Des exploit kits, comme ceux utilisés pour infecter des victimes avec des ransomwares, peuvent être utilisés par des cybercriminels qui n'ont que des connaissances limitées. Ces kits, qui exploitent les vulnérabilités d'une large gamme de logiciels disponibles sur le marché, comportent plusieurs options, comme l'utilisation de ses propres logiciels malveillants pour le cybercriminel ou l'utilisation des chaînes de distribution offertes par l'organisation criminelle qui vend ou loue l'exploit kit. S'il peut être coûteux d'acheter directement ces exploit kits, ils peuvent être loués pour seulement 500 $ par mois.[xv]

Les cybercriminels mettent au point de nouvelles formes de ransomwares plus efficaces, ainsi que des méthodes améliorées de communication aux systèmes infectés.

- Les ransomwares ont évolué en passant de technologies de blocage/verrouillage qui empêchaient les utilisateurs d'accéder à leurs fichiers, à des technologies de chiffrement qui cryptent des fichiers. Les anciens ransomwares sont plus faciles à déjouer, en comparaison, grâce à la disponibilité d'outils qui permettent de déverrouiller les ordinateurs infectés. Les nouveaux ransomwares, en revanche, sont presque impossibles à éradiquer après infection, car la cryptographie ne peut normalement pas être déchiffrée et les victimes de ransomwares n'ont généralement qu'un court laps de temps pour payer la rançon.

Il faut ajouter à cela le fait que les spécialistes en hameçonnage et en ransomwares ne cessent de se perfectionner dans le vol de données financières ou autres. Par exemple :

- Certaines menaces peuvent rester inactives sur une période prolongée et sont moins susceptibles d'être détectées par de nombreuses solutions habituelles anti-hameçonnage et anti-ransomwares.
- Certains types de logiciels malveillants peuvent détecter s'ils ont été placés dans un bac à sable et ils ne s'exécuteront qu'une fois qu'ils n'y seront plus.
- Certains cybercriminels coordonnent leurs attaques sur plusieurs lieux de diffusion notamment les e-mails, les réseaux sociaux, les navigateurs Web, les fichiers, etc.
- Un logiciel malveillant peut en diriger un autre qui semble inoffensif.
- Certains logiciels malveillants nécessitent une interaction avec l'utilisateur (par exemple, cliquer sur un bouton d'une boîte de dialogue) avant de s'activer et ne se sera pas dupe si l'utilisateur clique sur le bouton dans un bac à sable.

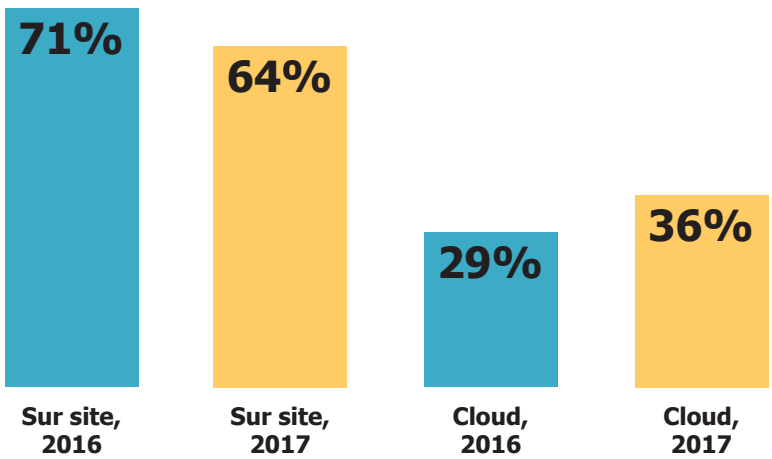
DÉPENSES DE SÉCURITÉ EN 2016 ET 2017

Les décideurs ont conscience de la menace d'hameçonnage, de ransomwares et d'autres risques en matière de sécurité et consacrent des dépenses significatives à les combattre. Notre recherche a montré que le budget total de la sécurité dans les organisations interrogées sera en moyenne de 425 $ par employé en 2016 et augmentera de 10,1 % en 2017 pour atteindre 468 $. De plus, notre recherche indique que les plus petites organisations (jusqu'à 999 employés) dépenseront, pour les frais liés à la sécurité, 51 % de plus par employé que les organisations plus grandes (de 1 000 employés ou plus). Cela met en relief les économies d'échelle dont profitent les grandes entreprises dans le cadre des dépenses informatiques en général, et dans les dépenses de sécurité en particulier.

Notre recherche a également révélé que les capacités en matière de sécurité sont en train de passer au Cloud. Comme le montre la figure 3, 71 % du budget lié à la sécurité est destiné à des solutions sur site en 2016, tandis que 29 % est destiné aux solutions basées sur le Cloud. Cependant, en 2017, les décideurs prévoient que la partie sur site du budget lié à la sécurité sera réduite à 64 % tandis que la proportion consacrée au Cloud atteindra 36 %. Notre recherche met en lumière l'importance croissante du Cloud dans le contexte de la sécurité et montre qu'en 2016, seulement 12 % des organisations disposaient d'un budget pour la sécurité basée sur le Cloud supérieur aux dépenses pour des solutions sur site, tandis que ce chiffre devrait atteindre 18,5 % en 2017.

Notre recherche montre que, pour de nombreuses organisations, les solutions de sécurité essentielles ne s'améliorent pas au fil du temps ou voient leurs performances se dégrader.

Figure 3
Répartition du budget lié à la sécurité consacré aux solutions sur site et sur le Cloud en 2016 et 2017



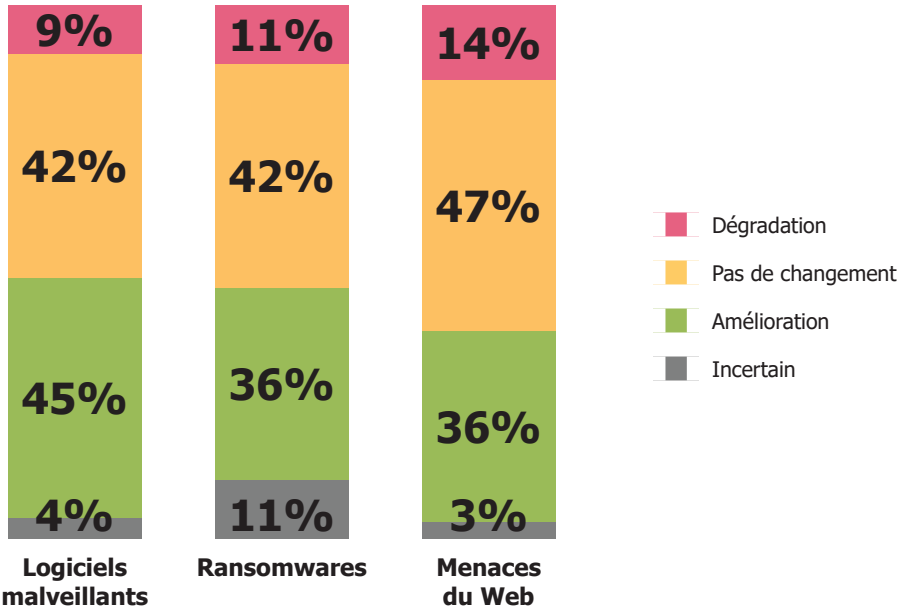
Source : Osterman Research, Inc.

DES AMÉLIORATIONS SIGNIFICATIVES DE LA SÉCURITÉ SONT NÉCESSAIRES

LES AMÉLIORATIONS SONT MODESTES

Notre recherche montre que, pour de nombreuses organisations, les solutions de sécurité essentielles ne s'améliorent pas au fil du temps ou voient leurs performances se dégrader. Par exemple, comme le montre la figure 4, 42 % des organisations déclarent que leurs solutions destinées à bloquer les logiciels malveillants ne s'améliorent pas au fil du temps, tandis que 9 % déclarent que ces solutions vont même en empirant. Le problème des performances statiques ou qui se dégradent est encore plus prononcé pour les solutions destinées à bloquer les ransomwares et les menaces du Web.

Figure 4
Changements perçus dans les performances des solutions clés



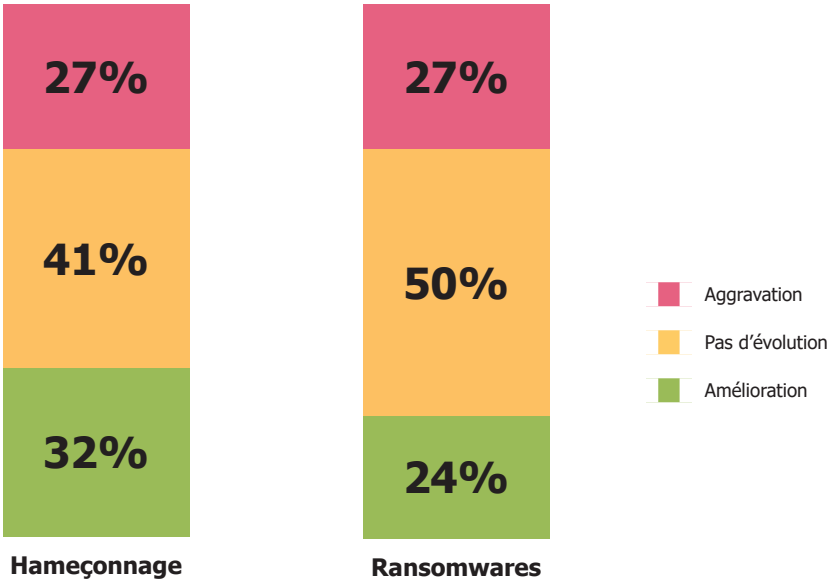
Source : Osterman Research, Inc.

… au cours des 12 derniers mois, les problèmes d'hameçonnage et de ransomwares auxquels la plupart des organisations ont été confrontées se sont aggravés ou ne se sont pas améliorés.

LES PROBLÈMES D'HAMEÇONNAGE ET DE RANSOMWARES S'AGGRAVENT

Nous avons également découvert que, au cours de 12 derniers mois, les problèmes d'hameçonnage et de ransomwares auxquels la plupart des organisations ont été confrontées se sont aggravés ou ne se sont pas améliorés. Comme le montre la figure 5, plus d'une organisation sur quatre déclare que les problèmes d'hameçonnage et de ransomwares s'aggravent, tandis que le phishing et les ransomwares sont aussi graves que l'année précédente pour respectivement 41 % et 50 % des organisations.

Figure 5
Évolution des problèmes d'hameçonnage et de ransomwares au cours de 12 derniers mois



Remarque : les totaux peuvent ne pas correspondre à 100 % en raison d'erreurs d'arrondis.
Source : Osterman Research, Inc.

…un tiers des organisations, ou moins, considèrent que leurs pratiques de formation des utilisateurs finaux concernant les ransomwares, la navigation sur Internet et les arnaques au président, ou arnaques BEC, sont « excellentes ».

QUELLE EST L'EFFICACITÉ DES SOLUTIONS ACTUELLES ?

Notre recherche visait également à étudier les capacités et les solutions actuelles en matière de sécurité et déterminer leur efficacité pour protéger les organisations du nombre croissant de menaces auxquelles elles sont confrontées. Comme le montre la figure 6, un tiers des organisations, ou moins, considèrent que leurs pratiques de formation des utilisateurs finaux concernant les ransomwares, la navigation sur Internet et les arnaques au président, ou arnaques BEC, sont « excellentes ». Les seuls domaines dans lesquels une majorité des décideurs informatiques considèrent qu'ils font un excellent travail sont l'élimination des logiciels malveillants et des courriers indésirables avant que ceux-ci ne parviennent aux utilisateurs finaux.

Figure 6
Efficacité perçue des capacités actuelles en matière de sécurité

Capacité	Excellente	Moyenne	Médiocre
Formation des utilisateurs finaux sur la détection et la gestion des ransomwares	27%	61%	13%
Formation des utilisateurs finaux sur les meilleures pratiques à adopter en naviguant sur Internet	28%	63%	9%
Formation des utilisateurs finaux sur la détection et la gestion des arnaques au président ou arnaques BEC	33%	58%	9%
Éviter la perte de données par e-mail ou sur Internet	36%	57%	8%
Formation des utilisateurs finaux sur la détection et la gestion des menaces d'hameçonnage	37%	55%	9%
Empêcher les appareils mobiles personnels des utilisateurs d'introduire des logiciels malveillants dans le réseau de l'entreprise	43%	48%	9%
Éliminer les ransomwares avant qu'ils ne parviennent aux utilisateurs finaux	50%	49%	9%
Éliminer les logiciels malveillants avant qu'ils ne parviennent aux utilisateurs finaux	56%	44%	0%
Éliminer les courriers indésirables avant qu'ils ne parviennent aux utilisateurs finaux	58%	43%	0%
MOYENNE	**41%**	**53%**	**6%**

Remarque : les totaux peuvent ne pas correspondre à 100 % en raison d'erreurs d'arrondis.
Source : Osterman Research, Inc.

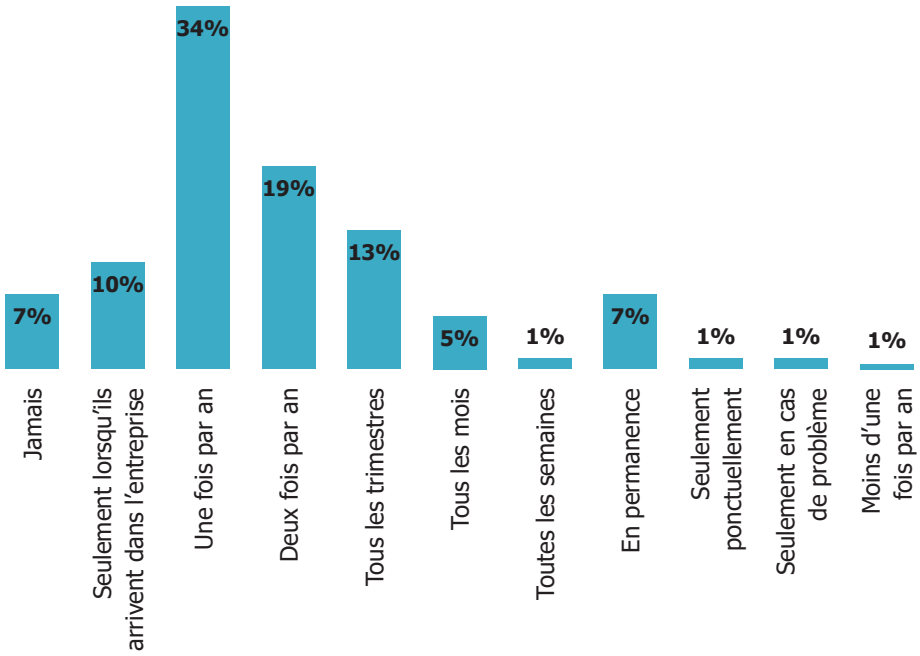
LA FORMATION DOIT ÊTRE AMÉLIORÉE

Notre recherche étudiait en détail la confiance que les organisations ont (ou n'ont pas) dans le degré de formation de leurs employés pour gérer des attaques d'hameçonnage et de ransomwares. En demandant aux décideurs d'évaluer leur organisation sur une échelle de 1 (pas confiant) à 100 (très confiant), nous nous sommes aperçus que 13,6 % des organisations seulement obtenaient 90 ou plus concernant la préparation à la formation en hameçonnage, tandis que seulement 11,1 % obtenaient autant concernant la préparation à la formation aux ransomwares. De plus, nous avons observé que 17,6 % des organisations se disent « pas très confiantes » ou « pas confiantes du tout » quant à leur capacité à neutraliser les attaques d'hameçonnage, tandis que 23,8 % déclarent la même chose concernant les attaques de ransomwares.

Les scores relativement bas pour la préparation à la formation sont liés au faible nombre de formations de sensibilisation à la sécurité dont bénéficient les employés. Par exemple, comme le montre la figure 7, 52 % des employés bénéficient d'une formation de sensibilisation à la sécurité (lorsqu'une formation existe) au maximum une fois par an.

…52 % des employés bénéficient d'une formation de sensibilisation à la sécurité (lorsqu'une formation existe) au maximum une fois par an.

Figure 7
Fréquence de formation des employés à la sensibilisation à la sécurité



Source : Osterman Research, Inc.

Cette auto-évaluation révèle trois points importants :

- Sans surprise, nous constatons une relation entre le nombre d'attaques subies par les organisations au cours des 12 derniers mois et leurs scores d'auto-évaluation concernant la sécurité : les organisations qui ont déclaré n'avoir été confrontées à aucun ransomware, logiciel malveillant, piratage ou autre problème de sécurité au cours des 12 derniers mois se sont attribuées un score d'efficacité perçue des capacités en matière de sécurité 7 % plus élevé que les organisations ayant subi au moins un problème de sécurité.
- Avec 41 % de mention « excellente » au total, les organisations ont manifestement encore beaucoup de progrès à faire pour protéger leurs utilisateurs, leurs réseaux et leurs données contre le phishing, les ransomwares, d'autres formes d'infiltration malveillante, la perte de données et d'autres menaces liées à la sécurité. Même dans les domaines où les décideurs attribuent des scores relativement élevés à leur organisation, les données révèlent que des améliorations significatives doivent être apportées afin de fournir une protection plus adaptée.
- Des améliorations de la protection contre le phishing et les ransomwares sont nécessaires dans tous les domaines, et une formation accrue de sensibilisation à la sécurité s'impose pour réduire le taux d'infection des attaques d'hameçonnage et de ransomwares. Si la formation ne constitue qu'une partie d'une stratégie fructueuse pour gérer le phishing et les ransomwares, elle peut s'avérer efficace: notre enquête montre que les organisations où les utilisateurs bénéficient d'une formation de sensibilisation à la sécurité seulement une fois par an au maximum subissent en moyenne 18,5 attaques contre la sécurité par an. En revanche, dans les organisations dont les employés sont formés plus d'une fois par an, le nombre moyen d'attaques est de 4,3.

QUELLES SONT LES TENDANCES À VENIR ?

Osterman Research prévoit que les attaques d'hameçonnage et de ransomwares continueront d'augmenter, comme cela est le cas depuis plusieurs années. Plus précisément, nous prévoyons que :

- Le nombre d'e-mails d'hameçonnage contenant des liens ou des pièces jointes destinés à diffuser des ransomwares ou d'autres types de logiciels malveillants augmentera à un rythme important au cours du reste de l'année 2016 et en 2017. Une étude Symantec a mis en lumière le rythme rapide du développement des ransomwares en montrant qu'entre 2005 et 2014, environ 16 familles de ransomwares ont été trouvées en circulation. Cependant, 27 ont été découvertes seulement en 2015 et 15 autres au cours du premier trimestre de 2016.[xvi]
- Une part croissante des tentatives d'hameçonnage visera à installer des ransomwares sur les ordinateurs des « victimes ». Une entreprise de sécurité a déterminé que 93 % des e-mails d'hameçonnage du milieu d'année 2016 visent à diffuser des ransomwares.[xvii]
- Si le problème général des courriers indésirables est en déclin depuis plusieurs années, les courriers indésirables constituent encore un moyen efficace de diffuser de logiciels malveillants, dont des ransomwares. Par exemple, Trustwave a constaté, sur une période de sept jours en mars 2016, que 18 % du volume total de courriers indésirables détectés contenaient des logiciels malveillants ou des liens vers ce type de logiciels[xviii]. Nous prévoyons que les courriers indésirables continueront d'être utilisés en tant que moyen secondaire pour diffuser des ransomwares et d'autres formes de logiciels malveillants.
- De plus, nous pensons qu'il est possible que le marché des ransomwares et d'autres formes de logiciels malveillants puisse se scinder dans une certaine mesure. Étant donné la facilité avec laquelle les cybercriminels non initiés peuvent pénétrer le marché, nous nous attendons à une tendance croissante vers deux domaines distincts pour les criminels utilisant les ransomwares : a) des ransomwares « bas de gamme » qui demandent une rançon de quelques centaines de dollars et sont envoyés par des amateurs et d'autres petits criminels en utilisant des techniques classiques d'hameçonnage, et b) des ransomwares « haut de gamme » envoyés par des cybercriminels plus sophistiqués et qui visent des cibles à grande valeur dans les soins de santé, les services financiers, les assurances et d'autres secteurs qui sont plus susceptibles de payer des sommes importantes pour récupérer leurs données chiffrées. Nous pensons que ces derniers auront recours à des techniques de harponnage plus sophistiquées lors de leurs tentatives d'infection de cibles de grande valeur.
- Le phishing et plus particulièrement les ransomwares prennent de plus en plus pour cible les entreprises et délaissent les particuliers. Étant donné qu'elles détiennent, en général, des données critiques qui doivent être récupérées et qu'elles peuvent payer la rançon en Bitcoin ou d'autres monnaies numériques, même si le montant de la demande de rançon est élevé, les entreprises sont devenues des cibles de choix pour les cybercriminels.

...d'importantes améliorations doivent être apportées pour assurer une protection plus appropriée.

MEILLEURES PRATIQUES RECOMMANDÉES

Osterman Research recommande aux décideurs d'adopter une série de mesures visant à lutter plus efficacement contre les attaques de hameçonnage et de ransomwares.

COMPRENDRE LES RISQUES ENCOURUS

Bien qu'émettre une simple recommandation sur la compréhension des risques encourus par votre entreprise puisse sembler banal, nous ne saurions que trop souligner son importance. Les décideurs doivent comprendre que les menaces auxquels ils font face sont non seulement dues à des attaques de hameçonnage et de ransomwares, mais également à un nombre croissant de menaces dans l'ensemble de leurs systèmes de communication et de collaboration, des dispositifs personnels que leurs utilisateurs emploient et même des utilisateurs eux-mêmes. La cybercriminalité est une industrie bénéficiant de solides compétences techniques, d'un financement important et d'un environnement cible riche.

ÉLABORER DES POLITIQUES APPROPRIÉES

De nombreuses entreprises n'ont pas encore élaboré ou publié de politiques détaillées et approfondies propres à chaque type de courriel, site Internet, collaboration, médias sociaux et d'autres outils déployés par leurs services informatiques ou dont l'utilisation est permise par ces dernières dans le cadre des services informatiques fantômes ou « shadow IT ». En conséquence, nous recommandons aux entreprises d'adopter en tant que première mesure l'élaboration de politiques détaillées et approfondies axées sur tous les outils qui sont ou seront probablement utilisés dans un avenir prévisible. Ces politiques doivent se focaliser sur les obligations légales, réglementaires et autres visant à chiffrer des courriels et autres contenus si ceux-ci contiennent des données sensibles ou confidentielles ; à rechercher des logiciels malveillants sur tous les messages publiés sur les blogs, les médias sociaux et d'autres sites ; et à contrôler l'utilisation de dispositifs personnels ayant accès aux systèmes internes.

La mise en œuvre de politiques solides ne fournit aucune protection en matière de sécurité en soi. En revanche, elle peut être utile pour limiter le nombre d'outils utilisés par les employés au moment d'accéder aux ressources d'entreprise. À leur tour, ces limitations peuvent aider à réduire le nombre de points d'entrée pour les ransomwares, d'autres formes de logiciels malveillants, les tentatives d'hameçonnage et d'autres contenus qui pourraient poser un risque de sécurité.

MAINTENIR LES SYSTÈMES À JOUR

Les vulnérabilités de l'application, du système d'exploitation et du système peuvent permettre aux cybercriminels d'infiltrer avec succès les défenses de l'entreprise. Chaque application et système doit être soumis à un contrôle de vulnérabilité et mis à jour à l'aide des derniers correctifs des fournisseurs.

VEILLER À AVOIR DES SAUVEGARDES RÉCENTES ET FIABLES

La restauration à partir d'un point de sauvegarde connu, fiable et créé si possible juste avant l'infection est une méthode utile de récupération à la suite d'une attaque de ransomware, ainsi que d'autres types d'infections de logiciels malveillants. En utilisant une sauvegarde récente, il est possible de réinitialiser un point d'extrémité et de remettre en état ses données avec le moins de perte de données possible. Bien que cette stratégie puisse comprendre un certain niveau de perte de données, en raison normalement d'un écart entre la sauvegarde la plus récente et la réinitialisation, les sauvegardes récentes permettent de minimiser la perte de données, faute d'autres recours.

DÉPLOYER DES SOLUTIONS ANTI-HAMEÇONNAGE ET ANTI-RANSOMWARES

Des solutions adaptées et pouvant être déployées sur site ou sur le Cloud sont proposées afin de détecter les tentatives de hameçonnage, de rançonnage et une variété d'autres menaces. Il est recommandé que chaque entreprise mette en œuvre des solutions adaptées à ses exigences en matière d'infrastructure de sécurité, tout en mettant l'accent sur sa capacité à détecter, isoler et corriger les menaces liées au hameçonnage et aux ransomwares.

METTRE EN ŒUVRE LES MEILLEURES PRATIQUES RELATIVES AU COMPORTEMENT DE L'UTILISATEUR

Par la suite, une variété de meilleures pratiques visant à résoudre les failles de sécurité pouvant exister dans l'entreprise est mise en œuvre. Par exemple :

- Les employés doivent utiliser des mots de passe qui correspondent à la sensibilité et aux risques associés aux ressources de données d'entreprise auxquelles ils ont accès. Ces mots de passe doivent être changés selon un calendrier précis sous la direction des services informatiques.
- Mettre en œuvre un programme de formation solide de sensibilisation à la sécurité visant à aider les utilisateurs à prendre de meilleures décisions sur le contenu de leur messagerie, sur ce qu'ils voient ou les liens sur lesquels ils cliquent sur les médias sociaux, sur leur type de connexion, etc. L'objectif de la formation de sensibilisation à la sécurité est tout simplement d'aider les utilisateurs à être plus prudents quant à ce qu'ils voient, ce qu'ils ouvrent et les liens sur lesquels ils cliquent. Bien que la formation de sensibilisation à la sécurité ne résout pas en soi complètement les problèmes liés à la sécurité d'une entreprise, elle permet

Bien qu'en général, les courriels indésirables sont de moins en moins problématiques depuis plusieurs années, ils sont toujours efficaces pour distribuer des logiciels malveillants, y compris des ransomwares.

de renforcer la capacité des utilisateurs, la première ligne de défense dans une infrastructure de sécurité, à être plus sensibles aux questions de sécurité et plus à même de réduire les tentatives de hameçonnage et de rançonnage. Investir suffisamment dans la formation des employés afin de mettre en place à titre de « pare-feu humain » une première ligne appropriée de défense contre des tentatives d'hameçonnage et d'autres attaques d'ingénierie sociale de plus en plus sophistiquées est essentiel.

- Établir une communication « à canal de retour » pour les membres clés du personnel qui pourraient être appelés à traiter les finances de l'entreprise ou des informations sensibles. Par exemple, si un PDG en déplacement envoie à son directeur financier une demande de transfert de fonds à un fournisseur, ce dernier doit prévoir un moyen indépendant lui permettant de vérifier l'authenticité de la demande, comme envoyer un message au PDG ou l'appeler sur son smartphone.
- Les employés doivent être évalués périodiquement afin de mesurer l'efficacité de leur formation de sensibilisation à la sécurité.
- Il convient de rappeler en permanence aux employés les dangers du partage à outrance d'informations sur les médias sociaux. Bien que les publications des employés concernant leur dernier petit-déjeuner, leurs vacances ou la visite d'un restaurant sur les réseaux sociaux peuvent intéresser leurs amis, il s'agit pour les cybercriminels de sources d'informations utiles visant à élaborer un courriel de hameçonnage.
- Veiller à ce que chaque employé maintienne des défenses anti-programme malveillant solides sur leurs plates-formes gérées personnellement si ces appareils appartenant aux employés ont accès aux ressources de l'entreprise.
- Il convient de rappeler aux employés qu'ils sont tenus de maintenir les systèmes d'exploitation et les logiciels à jour afin de minimiser la possibilité que des logiciels malveillants n'exploitent une vulnérabilité connue en vue d'infecter un système.

UTILISER UNE SOLUTION THREAT INTELLIGENCE ÉPROUVÉE

Grâce à l'utilisation d'une solution Threat Intelligence en temps réel et de son historique, chaque entreprise parvient à minimiser les risques d'infection. Threat Intelligence en temps réel peut fournir une défense solide pour limiter tout accès à des domaines peu recommandés et, par conséquent, susceptibles d'être utilisés par les cybercriminels pour des attaques d'hameçonnage, de rançonnage et autres. Les analystes de la sécurité et d'autres individus peuvent également utiliser de manière proactive Threat Intelligence en vue d'enquêter sur les attaques récentes et de découvrir les sources de menaces inconnues jusqu'ici. En outre, l'historique de Threat Intelligence, par exemple, un enregistrement de données Whois comprenant le précédent propriétaire des domaines, peut être utile pour mener des enquêtes sur la cybercriminalité.

L'utilisation du Threat Intelligence par IP en temps réel et à partir de son historique est un complément important à toute infrastructure de sécurité, car celle-ci protège de plusieurs façons :

- Les entreprises peuvent continuer de se conformer aux différentes obligations réglementaires auxquelles elles sont confrontées pour protéger les données des employés, des clients et d'autres informations qu'elles possèdent ou gèrent.
- Un bon Threat Intelligence permet de suivre intentionnellement ou non l'utilisation de l'image d'entreprise, afin de garantir sa protection.
- Threat Intelligence fournit aux chercheurs inforensiques un aperçu approfondi sur la façon dont les attaques ont commencé, comment les cybercriminels ont mené leurs attaques et comment les attaques futures peuvent être détectées en amont ou stoppées avant d'endommager le système.

www.barracuda.com
@barracuda
info@barracuda.com

RÉSUMÉ

Le phishing et les ransomwares sont des menaces très graves pouvant porter atteintes aux finances d'une entreprise, ses ressources de données et sa réputation. Ils peuvent grandement perturber les employés ou le service informatique d'une entreprise, amener une entreprise à transgresser les réglementations du secteur et du gouvernement, se traduire par des poursuites judiciaires, et dans les cas extrêmes, mettre en faillite une entreprise. Cependant, des mesures peuvent être prises par toute entreprise aux fins de traiter les tentatives d'hameçonnage et de rançonnage de manière à réduire les risques d'infection et les conséquences qui en découlent.

COMMANDITAIRE DE CE LIVRE BLANC

Barracuda Networks, Inc. propose des solutions de pointe conçues pour résoudre des problèmes informatiques généraux, de manière efficace et rentable, tout en maintenant un niveau d'assistance client et de satisfaction irréprochable. Nos produits englobent trois marchés distincts, y compris : 1) la sécurité des contenus, 2) la mise en réseau et la mise à disposition d'applications, ainsi que 3) le stockage de données, la protection et la récupération d'urgence.

Forts de notre longue expérience dans le domaine des dispositifs de sécurité Web et de messagerie électronique, nos applications primées comprennent plus d'une douzaine de solutions conçues pour un usage spécifique prenant littéralement en charge chaque aspect du réseau, en proposant aux entreprises de toutes tailles une véritable protection de bout en bout qui peut être déployée sous un format matériel, virtuel, dans le Cloud et mixte.

Barracuda est une société cotée en bourse (NYSE : CUDA) qui fournit des solutions de sécurité et de stockage puissantes mais simples d'utilisation qui simplifient l'informatique. CitiBank, Coca-Cola, Delta Dental, FedEx, Harvard, IBM, L'Oréal, Liberty Tax Service, Mythbusters et les écoles publiques de Spokane font partie des plus de 150 000 entreprises et organismes dans plus de 100 pays qui protègent en toute confiance leurs utilisateurs, leurs applications et leurs données avec des solutions Barracuda. Avec son siège dans la Silicon Valley, dans le nord de la Californie, notre réseau est composé de bureaux dans 15 pays, plus de 1 000 employés et plus de 5 000 partenaires.

RÉFÉRENCES

i http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
ii Un ransomware chiffré est un type ransomware plus récent qui chiffre les fichiers des utilisateurs, contrairement au ransomware de blocage qui en empêche simplement l'accès. Cependant, l'objectif des deux types de ransomware est de prévenir tout accès à des fichiers contre le paiement d'une rançon par la victime.
iii Source: Phishing Activity Trends Report, APWG, 23 mai 2016
iv Source: McAfee Labs Threats Report, juin 2016
v http://www.securityweek.com/history-and-statistics-ransomware
vi https://www.justice.gov/criminal-ccips/file/872771/download
vii http://www.bbc.com/news/technology-37166545
viii https://www.leoni.com/en/press/releases/details/leoni-targeted-by-criminals/; https://blog.knowbe4.com/cyberheist-nets-44-million-in-single-ceo-fraud-attack
ix http://arstechnica.com/security/2016/04/maryland-hospital-group-denies-ignored-warnings- allowed-ransomware-attack/
x https://oag.ca.gov/system/files/Snapchat%20Inc%20updated%20Sample%20of%20Employee%20Notice%20of%20Data%20Breach_Redacted_0.pdf?
xi http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
xii http://resources.infosecinstitute.com/spear-phishing-real-life-examples/
xiii Results of an End User Survey About Communications Practices, Osterman Research, Inc.
xiv http://www.itworldcanada.com/article/largest-ransomware-as-service-scheme-pulls-in- us195000-a-month-report/385700
xv Source: Infosec Institute
xvi https://blog.malwarebytes.com/cybercrime/2016/06/ransomware-dominates-the threat-landscape/
xvii http://www.digitaltrends.com/computing/93-percent-phishing-emails-ransomware/
xviii https://www.trustwave.com/Resources/SpiderLabs-Blog/Massive-Volume-of-Ransomware- Downloaders-being-Spammed/