FireEye

UN E-MAIL PARMI DES MILLIONS

Attaques par e-mail : les origines du mal

269 milliards d'e-mails sont envoyés chaque jour.[1]

Avec 150 millions d'e-mails de phishing envoyés chaque jour, les cyberattaquants ne ménagent pas leurs efforts. Imprimés et mis bout à bout, ces messages malveillants s'étaleraient sur près de 42 000 kilomètres, soit plus que la circonférence de la Terre !

Cibles principales

Le plus souvent, les hackers tentent de faire main basse sur des informations financières, de la propriété intellectuelle et des données personnelles à exploiter ou à revendre. Leurs proies de choix : les cadres et les dirigeants d'entreprises ou organismes publics.

Dans la ligne de mire des attaquants : les coordonnées personnelles, les informations clients et les équipements.

2/3
Près de 2 e-mails sur 3 sont des SPAMS.[2]

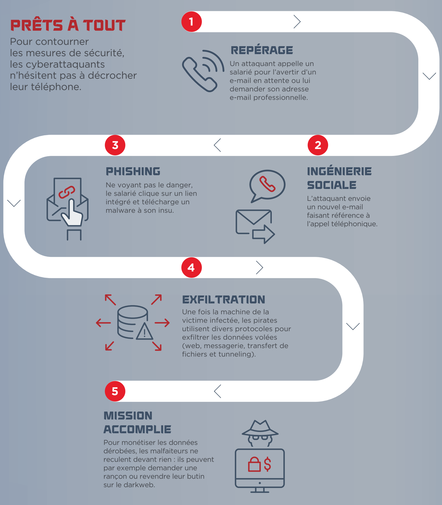
91 %
Quasiment toutes les cyberattaques commencent par un e-mail.[3]

84 %
La plupart des organisations ont déjà été victimes de spear-phishing.[4]

Méthodologie

PRÊTS À TOUT

Pour contourner les mesures de sécurité, les cyberattaquants n'hésitent pas à décrocher leur téléphone.



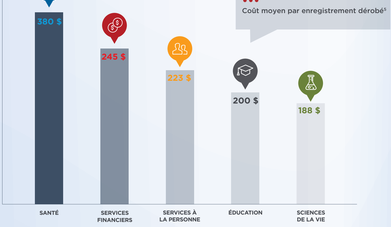
95 % des compromissions par phishing s'accompagnent de l'installation de logiciels malveillants.[4]

Une compromission par e-mail peut coûter très cher

COÛT FINANCIER	DÉLAI DE REMÉDIATION	TAUX DE RÉCURRENCE
3,62 M$	**66 jours**	**27,7 %**
Coût moyen d'une compromission par e-mail	Délai moyen pour confiner la menace	Probabilité de subir une nouvelle violation de données dans les 24 mois[5]

SECTEURS LES PLUS TOUCHÉS

À l'échelle internationale, le coût moyen d'un enregistrement volé s'élève à 141 $. Certains secteurs, comme la santé et les services financiers, sont beaucoup plus touchés que d'autres.



En misant sur des équipes de réponse à incident réactives et en généralisant le chiffrement des données, les entreprises peuvent espérer **ramener le coût d'une attaque à moins de 19 $ par enregistrement compromis.[4]**

Optimisez votre protection avec FireEye Email Security

Protégez les ressources de votre organisation contre le phishing et les ransomwares

Optez pour une protection automatisée et en temps réel contre le spear-phishing et les autres attaques d'ingénierie sociale

Garantissez la sécurité de votre messagerie sur site, dans le cloud ou dans un environnement hybride

Bénéficiez d'une protection toujours à jour, sans avoir à mettre constamment vos systèmes à niveau

Misez sur une Threat Intelligence contextuelle et détaillée pour réagir plus efficacement aux menaces

Protégez votre organisation contre les attaques multi-vecteurs et multiflux, difficiles à détecter

Protégez vos collaborateurs, vos données et vos ressources avec FireEye Email Security. Pour tout savoir, rendez-vous sur **https://www.fireeye.fr/solutions/ex-email-security-products.html**

- Réduction des risques liés aux accès non autorisés
- Baisse des coûts d'exploitation
- Déploiement en quelques minutes, sans infrastructure physique

1. Radicati Group (février 2017). Email Statistics Report, 2017-2021
2 Shcherbakova, Vergelis et Demidova (13 mai 2015). Spam and Phishing in the First Quarter of 2015
3 PhishMe (2016). Enterprise Phishing Susceptibility and Resiliency Report
4 Verson Bourne. « The Impact of Spear Phishing ». 2016
5 Ponemon Institute LLC (juin 2017). « 2017 Cost of Data Breach Study: Global Analysis »

© 2018 FireEye, Inc. Tous droits réservés. FireEye est une marque déposée de FireEye, Inc. Tous les autres noms de marques, de produits ou de services sont ou peuvent être des marques commerciales ou des marques de service de leurs propriétaires respectifs. E-EXT-IG-FR-FR-000070-01.PDF

FireEye