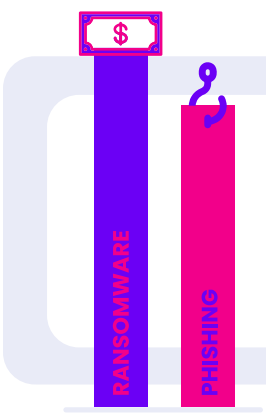
Ransomwares : 4 raisons pour lesquelles l'email est le principal vecteur

En 2020, les ransomwares ont généré près de 20 milliards de dollars de dégâts dans le monde entier.[1] S'il existe de nombreuses façons de lancer une attaque par ransomware, la plupart sont complexes, chronophages et coûteuses. Il existe pourtant un moyen rapide et économique de parvenir à ses fins : l'email, qui se trouve aussi être l'outil de communication le plus utilisé au monde.

1. Les emails de phishing sont faciles à créer

Pas besoin d'avoir fait de grandes études pour créer un email de phishing. Pour donner à leurs emails l'apparence de l'authenticité, les hackers imitent la charte graphique des marques en reprenant leurs images et logos directement depuis leur site Web ou sur Google.



67%
des infections par ransomware trouvent leur origine dans un email de phishing/spam. [2]

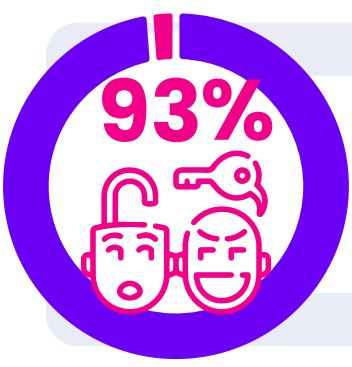
2. Les kits de ransomwares sont bon marché

Pour environ $66, les hackers peuvent acquérir un kit de ransomware en ligne. Des abonnements mensuels sont proposés pour le double de ce prix. Le travail du hacker est ainsi simplifié et l'attaque peut être lancée plus facilement par email.[3]

$66
c'est le coût moyen d'un kit de ransomware.

3. L'ingénierie sociale aide les hackers à créer l'email parfait

L'ingénierie sociale consiste à pousser des victimes à divulguer des informations sensibles ou à leur faire accomplir une action donnée. Les hackers n'ont aucun mal à retrouver des informations sur les employés, en particulier sur les réseaux sociaux, pour créer l'email de ransomware parfait.



93%
des violations réussies sont liées à l'ingénierie sociale. [4]

4. La charge utile se cache dans les pièces jointes et les fichiers partagés

Des liens cachés dans les pièces jointes téléchargent le malware au moment du clic. Dans d'autres cas, le ransomware commence à être téléchargé dès l'ouverture de la pièce jointe, souvent par l'intermédiaire de macros de fichiers Word ou PDF ou de scripts malveillants zippés.

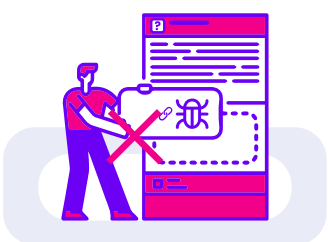
40%
des malwares sont déployés par des pièces jointes. [5]

Protégez votre entreprise des ransomwares :

Lorsqu'un ransomware frappera à la porte de votre entreprise, il prendra certainement la forme d'un email. Suivez les conseils ci-dessous pour protéger votre entreprise :

Réfléchissez avant de cliquer :

Etudiez de près les adresses des emails pour y repérer les caractères et extensions inhabituels et passez le curseur sur les liens pour afficher la véritable destination des URL.



N'ouvrez jamais les pièces jointes provenant d'expéditeurs inconnus :

La règle précédente est aussi valable pour les pièces jointes. Si l'expéditeur vous paraît suspect, n'ouvrez pas la pièce jointe.

Formez vos utilisateurs :

Sensibilisez-les en continu et proposez-leur une formation après chaque incident.

Ajoutez un niveau supplémentaire de sécurité de l'email :

Optez pour une solution qui explore les URL, les pièces jointes, les fichiers partagés, les images et les pages Web.

[1] Barrons. https://www.barrons.com/articles/2020-was-a-bad-year-for-ransomware-2021-will-be-worse-51610124513

[2] Statista. https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/

[3] AtlasVPN. https://atlasvpn.com/blog/most-damaging-cybercrime-services-cost-less-than-500-on-the-dark-web

[4] Verizon. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

[5] Ibid.

Pour découvrir comment Vade for M365 peut protéger votre entreprise des ransomwares, contactez Vade.

À propos de Vade :

- 1 milliard de boites mails protégées
- 100 milliards d'emails analysés par jour
- + 1400 partenaires dans le monde
- Renouvellement annuel de 95 %
- 17 brevets internationnaux actifs

En savoir plus :

www.vadesecure.com

@vadesecure

Contact :

Service commercial

sales@vadesecure.com