La menace est dans le courriel

L'hameçonnage et les autres menaces transmises par courriel demeurent les principales menaces pour la cybersécurité

L'IMPACT DES MENACES

$2.4B

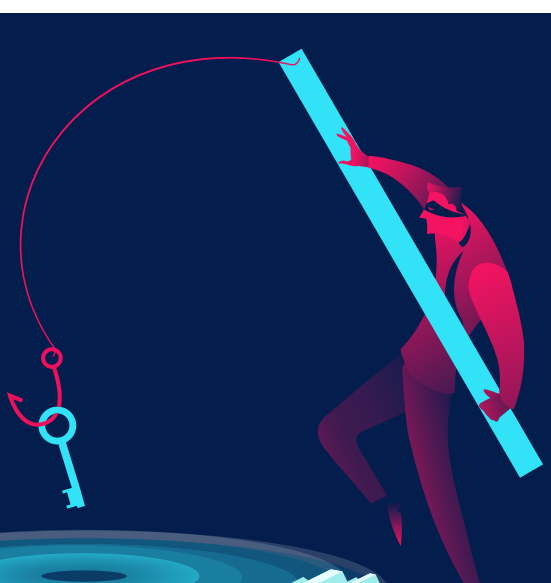
Quel est le coût de l'inaction?

Le FBI a signalé que la compromission des courriels d'affaires à elle seule a entraîné des pertes de 2,4 milliards de dollars en 2021. Plus de 320 000 attaques par hameçonnage/courriel ont été signalées au FBI l'an dernier.

90%

Presque toutes les attaques commencent par un courriel

Plus de la MOITIÉ de toutes les petites et moyennes entreprises (PME) ont été victimes d'une cyberattaque, dont 90 % ont commencé par un courriel d'hameçonnage (2020 Verizon DBIR).



150%

Un an à vivre dangereusement

Les attaques de logiciels malveillants par courriel ont bondi de plus de 150% entre 2020 et 2021

200+

Ralentissement de la détection

Ralentissement de la détection Le délai moyen pour repérer une brèche est

À mesure que le coût et l'impact des menaces continuent de croître, les organisations de toutes tailles doivent trouver de nouvelles façons de les arrêter avant qu'elles ne passent de la nuisance à la responsabilité

LES PROBLÈMES QUE NOUS AVONS DÉCOUVERT

82 SECONDS

Le temps est un facteur essentiel:

Le temps moyen de clic sur un courriel d'hameçonnage n'est que de 82 secondes à partir du moment où il est reçu.

Le manque d'automatisation pèse sur les équipes informatiques

Près du trois quarts des organisations utilisent UNIQUEMENT des processus manuels pour examiner les cas de phishing signalés par les utilisateurs, ce qui limite la capacité de l'informatique à se concentrer sur les initiatives stratégiques.

60%

Les violations de données sont des menaces existentielles

60 % des entreprises ferment leurs portes dans les six mois suivant une violation de données ou une cyberattaque.

Les passerelles sécurisées ne suffisent pas

Chaque année, des millions de messages malveillants contournent les défenses traditionnelles du courrier électronique telles que les solutions de Sécurité de la boite de messagerie.

24%

Le temps des employés est bien utilisé?

Dans leur semaine de travail typique de 40 heures, les analystes de la sécurité consacrent à l'enquête, à la détection ou à la correction des courriels d'hameçonnages.

La pénurie de compétences en matière de sécurité entraine des répercussions

La plupart des analystes ne peuvent traiter plus de quatre menaces d'hameçonnages par jour.

$8900

Impact réel des attaques

Le coût mensuel de la gestion des attaques d'hameçonnages pour une organisation comptant 5000 utilisateurs.

Qu'est-ce qui tient la direction éveillée la nuit?

L'hameçonnage est la principale préoccupation des décideurs.

Les menaces par courriel étant de plus en plus sophistiquées, aucun outil ne suffit à lui seul à prévenir l'infection et la diffusion de charges utiles. Les entreprises doivent adopter une approche à plusieurs dimensions pour prévenir la perte ou l'exfiltration de données.

LA SOLUTION!

Comment fonctionne la détection et la réponse des boîtes de messagerie GoSecure Titan®?

1. **L'employé remarque un courriel suspect et clique sur le bouton IDR de GoSecure Titan pour commencer le processus de soumission.**
2. **Le courriel est automatiquement mis en quarantaine et acheminé par le centre de réponse active de GoSecure.**
3. **Les moteurs d'apprentissages automatique GoSecure enquêtent sur le courriel suspect.**
4. **Les experts en sécurité humaine effectuent un examen plus approfondi des messages non concluants au moyen d'une analyse multidimensionnelle.**
5. **En quelques minutes, un message d'état est renvoyé, soit le message est vérifié, soit il est supprimé.**
6. **Les rapports en temps réel donnent à l'équipe de sécurité interne une visibilité claire sur l'incident et sa résolution.**

Obtenez le livre numérique complet : Arrêter les attaques par courriel avec la sécurité multiniveaux à https://fr.gosecure.net

GoSecure est un leader reconnu en matière de cybersécurité, qui propose des solutions de sécurité gérées innovantes et des services de conseil spécialisés. Les solutions de sécurité gérées par GoSecure Titan® offrent une protection multivectorielle pour contrer les cybermenaces modernes grâce à une gamme complète d'offres qui étendent les capacités des équipes internes de nos clients. Le service de détection et réponse gérées Titan de GoSecure (MDR) offre le meilleur délai de réponse de sa catégorie, avec une couverture complète des réseaux, des terminaux et des boîtes de réception des clients. Depuis plus de 10 ans, GoSecure aide ses clients à mieux comprendre leurs lacunes en matière de sécurité, à améliorer le risque organisationnel et à renforcer la posture de sécurité grâce à des services de conseil fournis par l'une des équipes les plus fiables et les plus compétentes du secteur. Pour en savoir plus, veuillez visiter : https://fr.gosecure.net.

GoSecure fr.gosecure.net | 855-893-5428