Isolation des liens contenus dans les e-mails

Isolez les liens contenus dans les e-mails pour réduire la surface d'attaque et simplifier les opérations

Réduisez les risques de phishing en appliquant des protections et des contrôles d'isolation du navigateur

Défi : phishing multi-canaux sophistiqué

Le phishing multi-canaux repose sur des méthodes de distribution d'e-mails et de contenus web conçues pour échapper avec agilité aux règles de filtrage. En voici quelques types courants :

- **Phishing en différé** : un lien initialement bénin inclus dans un e-mail est modifié avec une intention malveillante après la distribution.
- **Phishing de service cloud :** des liens HTTPS dangereux ressemblent fortement à des services de cloud courants (par ex. Google Drive, Box)

Pour arrêter ce type de menaces, une solution moderne de protection des e-mails doit être en mesure d'appliquer à tous les liens un examen fondé sur l'approche Zero Trust (« ne jamais faire confiance, toujours vérifier »).

Solution : l'isolation des liens contenus dans les e-mails

L'intégration de fonctionnalités d'isolation à distance du navigateur (RBI) à une solution de sécurité des e-mails dans le cloud (CES) applique ce niveau d'examen afin de renforcer la protection contre le phishing. Les clients utilisateurs de Cloudflare Area 1 peuvent activer l'isolation du navigateur Cloudflare pour neutraliser ces menaces multi-canaux.

Les administrateurs peuvent contrôler les interactions des utilisateurs avec des pages web isolées (restriction de la saisie au clavier et des transferts de fichiers, par exemple) afin de prévenir les conséquences des attaques par phishing, telles que la collecte d'informations d'identification ou le vol de données confidentielles.

En outre, l'ouverture des liens présents dans les e-mails dans un navigateur isolé permet de neutraliser les logiciels malveillants en exécutant l'ensemble du code dans le cloud, à l'écart des appareils locaux.

Voici ce que disent les analystes :

« Les URL incluses dans des e-mails qui se résolvent sur des sites externes sont souvent utilisées pour hameçonner des employés. L'isolation de ces liens peut permettre de réduire le nombre d'attaques par phishing concluantes. »

« La plupart des attaques sont lancées depuis l'Internet public, soit pendant la navigation web, soit par le biais de liens contenus dans des e-mails qui incitent l'utilisateur à se rendre sur des sites malveillants. Retirer (ou, mesure plus efficace, isoler) le navigateur du poste de travail de l'utilisateur améliore considérablement le niveau de sécurité de l'entreprise, notamment sa protection contre les attaques par rançongiciels. »

« Évaluez et pilotez une solution d'isolation du navigateur pour des utilisateurs spécifiques (par ex., les équipes financières) ou des scénarios d'utilisation à haut risque (par ex., le rendu d'URL incluses dans les e-mails), en particulier si votre organisation est réticente au risque. » [1]

Gartner

En savoir plus

Avantages opérationnels de l'intégration de solutions CES et RBI

Renforcement de la protection contre le phishing

L'isolation des e-mails empêche non seulement l'exécution locale du code malveillant contenu dans un lien de phishing, mais applique également des contrôles de protection des données permettant d'éviter que des informations sensibles ne tombent dans de mauvaises mains.

Libérer la productivité des services informatique et de sécurité

Activez l'isolation des e-mails pour n'importe quel site web en quelques clics.

Les équipes informatiques et de sécurité évitent la configuration fastidieuse de stratégies de filtrage risquant d'entraîner des blocages excessifs (qui grèveraient la productivité des utilisateurs) ou insuffisants (qui laisseraient passer les menaces).

Exemple de scénario d'utilisation : prévention du phishing en différé

Problème : le phishing différé échappe à la détection

Portées par des tactiques efficaces et la motivation, les campagnes de phishing différé peuvent échapper aux solutions de protection traditionnelles.

Configuration de la campagne : les acteurs malveillants peuvent commencer par envoyer un e-mail en apparence authentique depuis un domaine nouvellement créé, à l'aide d'une authentification d'e-mail appropriée (SPF, DKIM, DMAR) et d'une page web bénigne.

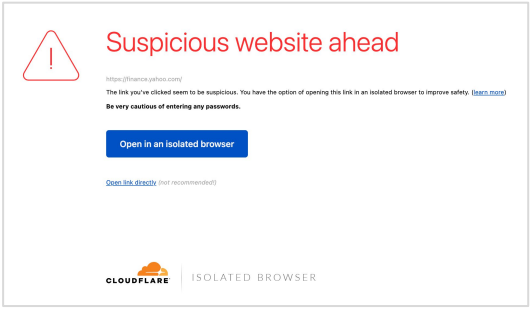
Distribution dans les boîtes de réception : ces e-mails peuvent échapper à la détection par les passerelles d'e-mail sécurisées, les filtres basés sur l'authentification ou d'autres services utilisant des signaux de réputation et d'autres techniques déterministes.

Réorientation vers un lien malveillant : une fois l'e-mail distribué, l'acteur malveillant peut réorienter le lien afin qu'il renvoie vers une destination malveillante, en modifiant la page web qu'il contrôle. Par exemple, une réorientation fréquente consiste à proposer une fausse page de connexion utilisée pour collecter des informations d'identification.

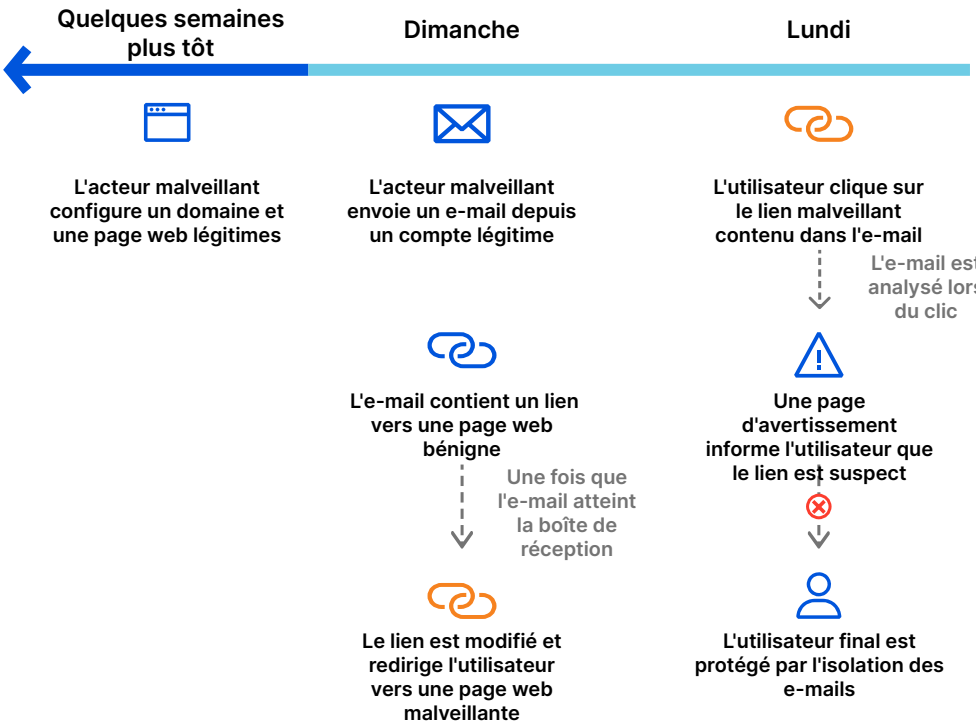
Solution : isoler les liens suspects après la distribution

L'isolation des liens des e-mails offre une couche essentielle de protection après la distribution. Cloudflare analyse tous les liens contenus dans un e-mail lorsque l'utilisateur clique dessus. Si un lien est considéré comme suspect ou dangereux, Cloudflare affiche une page d'avertissement *(voir ci-dessous)*, puis isole la page web, si l'utilisateur décide d'y accéder.

Les administrateurs empêchent l'exécution du code malveillant sur les appareils locaux et peuvent appliquer des contrôles de protection des données, tels que la restriction des transferts et téléchargements de fichiers, l'interdiction de la saisie au clavier ou l'ouverture de pages en lecture seule.



Chronologie d'une campagne de phishing différé



Cloudflare analyse chaque lien au moment du clic

Lien sûr : les utilisateurs sont redirigés vers ce site en toute transparence.

Lien malveillant : la navigation des utilisateurs est bloquée.

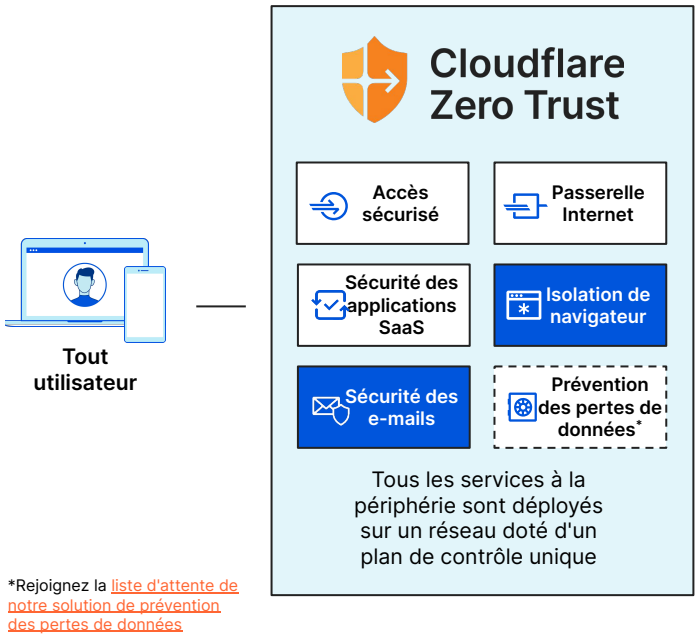
Lien suspect : la navigation des utilisateurs est fortement découragée, et une page d'avertissement les encourage à consulter le lien dans un navigateur isolé.

Intégrer la sécurité des e-mails dans le cloud avec Cloudflare Zero Trust

Une sécurité moderne avec Zero Trust

Cloudflare Zero Trust améliore la visibilité, élimine la complexité et réduit les risques liés aux connexions d'utilisateurs distants et sur site aux applications de l'entreprise et à l'Internet public.

Le 1er avril 2022, Cloudflare a terminé l'acquisition d'Area 1 Security avec l'intention d'étendre la protection offerte par notre plateforme Zero Trust contre les attaques par phishing lancées depuis les e-mails, le web et les environnements réseau. Lisez la suite ici.



*Rejoignez la liste d'attente de notre solution de prévention des pertes de données

Sécurité des e-mails : essentielle à l'approche Zero Trust

La solution de sécurité des e-mails Cloudflare Area 1 améliore l'approche Zero Trust en éliminant la confiance implicite envers les e-mails, afin de bloquer préventivement les attaques par phishing et la compromission des adresses e-mail professionnelles (BEC).

Ne faites confiance à aucun expéditeur, même interne. Assurez-vous que tout le trafic utilisateur, notamment les e-mails, est vérifié, filtré, inspecté et isolé des menaces d'Internet. La sécurité des e-mails sera intégrée aux services Zero Trust de Cloudflare, afin de créer une combinaison performante avec RBI, CASB, etc.

Remplacement du VPN
Simplifiez et sécurisez la connexion de n'importe quel utilisateur à n'importe quelle ressource

Protection Internet
Protégez vos données contre les menaces sur n'importe quels port et protocole

Simplifier la sécurité SaaS
Visibilité et contrôle des applications, dont les e-mails

Modernisation de la sécurité
Productivité améliorée, opérations plus simples, surface d'attaque réduite

Sécurité des e-mails dans le cloud (CES)

- Réduisez les temps de réaction en cas d'incident de 90 %.
- Identifiez à l'avance l'infrastructure et les mécanismes de diffusion des auteurs d'attaques, afin d'arrêter le phishing dès les premières étapes du cycle d'une attaque.
- Éliminez la confiance implicite dans les e-mails en analysant le contenu, le contexte et les graphiques de confiance des communications.
- Tirez profit des intégrations avec Microsoft, Google et d'autres environnements pour améliorer la sécurité intégrée.

Isolation de navigateur à distance

- Prévenez la compromission d'informations d'identification en ouvrant les sites dangereux en mode « lecture seule », en contrôlant les interactions des utilisateurs (par ex. saisie au clavier, copier/coller, transfert/téléchargement).
- Exécutez l'ensemble du code du navigateur sur le réseau de Cloudflare, en isolant les appareils locaux du code malveillant.
- Proposez une expérience utilisateur final rapide et fluide. Plutôt qu'un flux de pixels classique, nous créons une réplique exacte de la page depuis d'un navigateur distant, présente à moins de 50 ms de 95 % des utilisateurs d'Internet dans le monde entier.

Demandez dès aujourd'hui une évaluation des risques de phishing

Nous contacter

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : PMM-2022JUN

[1] *Gartner Hype Cycle for Network Security, 2021* | GARTNER et HYPE CYCLE sont des marques déposées et des marques de service de Gartner, Inc. ou de ses filiales aux États-Unis et dans le monde entier, et sont utilisées ici avec son accord. Tous droits réservés.