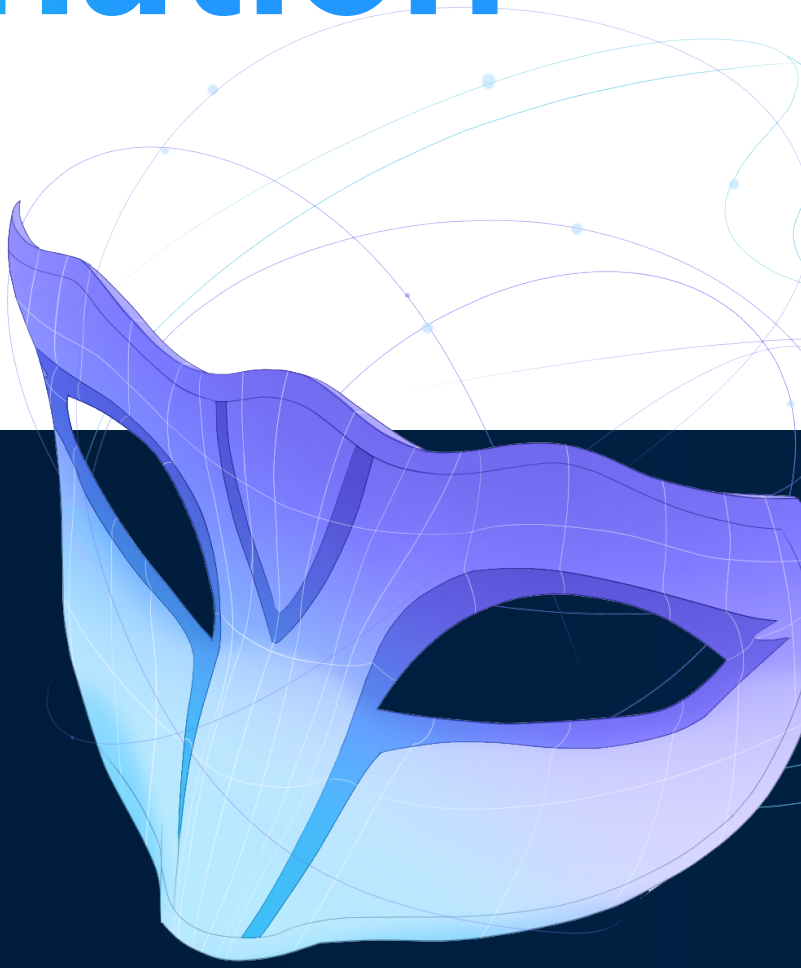
bfore.ai

Guide définitif de l'usurpation d'identité de Marque

Online Brand Impersonation



Try it now - sales@bfore.ai

Introduction

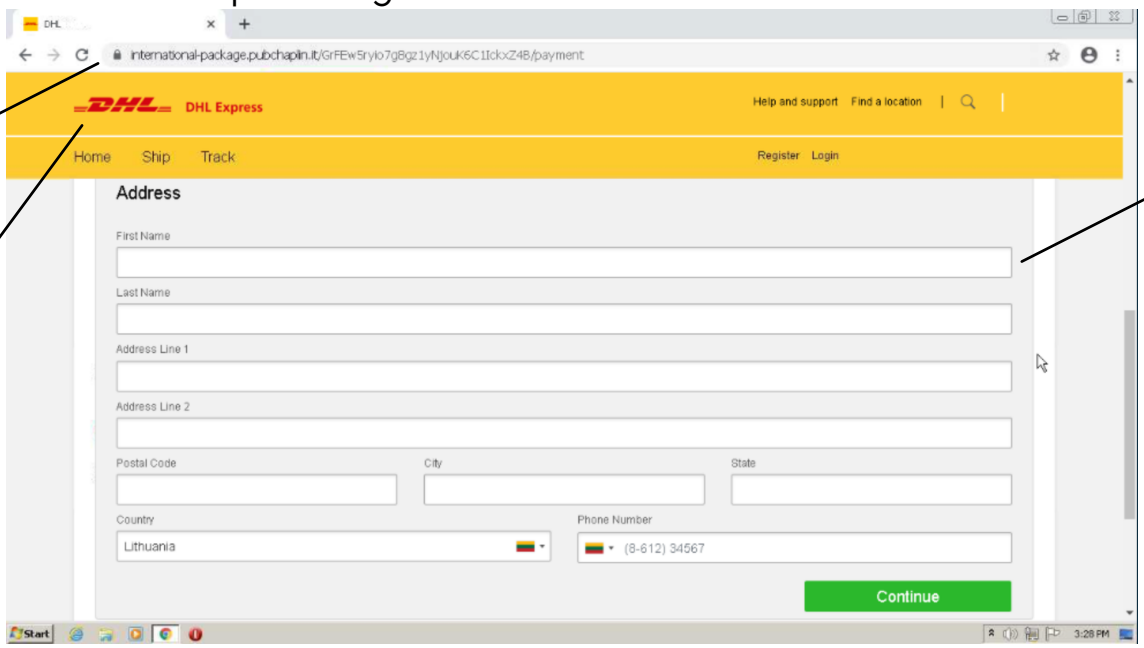
Dans les affaires d'aujourd'hui, la réputation est primordiale. Les visiteurs renforcent la confiance dans une marque et attendent des niveaux de fiabilité et de sécurité pour tout ce qui lui est associé. Les attaquants mènent intelligemment des attaques d'usurpation d'identité pour saper la confiance soigneusement construite en se faisant passer pour des sites légitimes pour diffuser des informations erronées, installer des logiciels malveillants et effectuer des ventes frauduleuses.

Les attaquants utilisent des noms de domaine frauduleux pour détourner le trafic légitime, incitant les utilisateurs à accéder à leurs informations. Les noms de domaine frauduleux apparaissent proches du nom de domaine réel, déroutant les utilisateurs. Selon une étude de Proofpoint, près de 96 % des entreprises ont des noms DNS identiques mais des domaines de premier niveau différents tels que .net au lieu de .com. Avec plus de 30 000 domaines malveillants détectés chaque jour, le contrôle des noms de domaine et le blocage de l'utilisation frauduleuse sont cruciaux pour les organisations afin d'éviter de nuire aux ventes et à la réputation. Beaucoup de ces domaines ne publient aucun contenu Web et restent inactifs pendant plusieurs mois avant que l'acteur malveillant ne lance une attaque qui peut entraîner une violation de données coûtant finalement en moyenne 4,35 millions USD.

Cet ebook couvre les concepts de base des concepts d'attaque par usurpation d'identité, les tactiques et ce que les organisations peuvent faire pour arrêter les attaques avant qu'elles ne puissent endommager leur organisation.

Qu'est-ce que l'usurpation d'identité ?

Les attaques par usurpation d'identité jouent sur la réputation et la confiance d'une entreprise pour tromper les victimes. Les attaquants créent des sites imposteurs qui imitent le contenu légitime pour créer l'illusion que leur contenu est légitime. Ils trompent les utilisateurs avec des e-mails de phishing, des liens vers les réseaux sociaux et l'usurpation de domaine pour attraper les visiteurs imprudents. Une fois que les visiteurs arrivent sur le site, ils peuvent être soumis à un code malveillant pour installer des rançongiciels et des rootkits, des informations erronées sur la marque ou un faux commerce pour voler les informations de carte de paiement. L'usurpation d'identité crée une confusion entre la vraie marque et les faux sites, amenant les visiteurs à associer une activité malveillante à la marque d'origine.

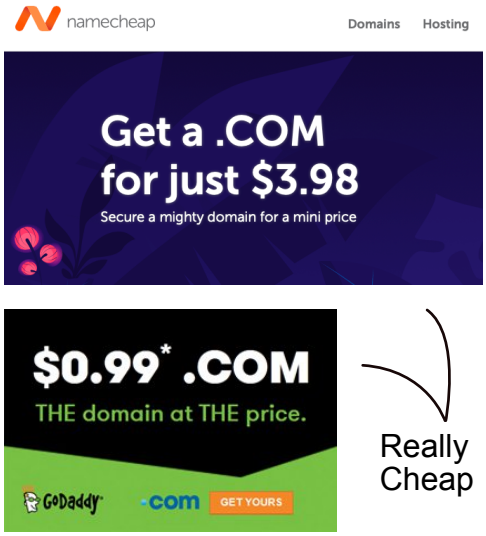


Les attaques par usurpation d'identité se multiplient

Les attaques d'usurpation d'identité de marque sont si efficaces que leur utilisation a augmenté de 171 % entre 2019 et 2021. L'un des principaux vecteurs d'attaques d'usurpation d'identité est le nom de domaine. L'utilisation de variantes d'un nom de domaine établi donne l'impression que le lien est légitimement associé à l'entreprise sans éveiller les soupçons des victimes potentielles.

Pourquoi les attaquants abusent-ils des domaines Web ?

L'abus de domaine est facile à commettre pour les attaquants car il ne faut que peu de temps et d'argent pour enregistrer un faux domaine. Ils utilisent des noms de domaine similaires à des domaines légitimes tels que "www.youbusinessname.com" au lieu de "www.yourbusinessname.com" où la seule différence est qu'il manque un "r" dans "yourbusiness". Des attaques comme celle-ci s'attaquent à l'incapacité de l'utilisateur à différencier parfaitement les fautes d'orthographe et les légères différences en un coup d'œil.



Un piège attend sa victime

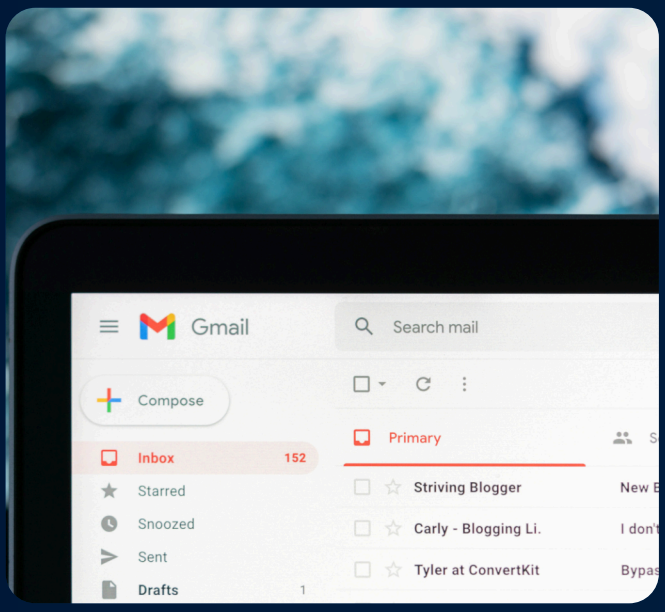
Les domaines malveillants sont des artefacts dangereux affectant non seulement ceux qui ont mal saisi le domaine, mais aussi ceux qui suivent des liens sur des sites Web, des e-mails ou des réseaux sociaux. Des noms de domaine similaires éloignent les utilisateurs des sites légitimes et les dirigent vers des emplacements contrôlés par des attaquants. La portée réelle de l'abus est beaucoup plus large, car les attaquants abusent des domaines pour nuire à la réputation d'une entreprise, diffuser des logiciels malveillants, mener des attaques de phishing ou commettre des fraudes.

Il n'y a aucun contrôle sur les domaines nouvellement enregistrés

Les URL malveillantes sont devenues un pilier des attaques de phishing pour attirer les victimes vers des sites Web usurpés, apparaissant 3 à 4 fois plus que les pièces jointes malveillantes. La cause la plus courante d'une violation de données concerne les informations d'identification volées ou compromises, les attaques de phishing venant en deuxième position. En termes d'usurpation de site Web, l'objectif est généralement d'amener les utilisateurs à se connecter à ce qu'ils pensent être leur compte personnel, permettant aux attaquants d'enregistrer leurs informations personnelles et de les utiliser sur le site Web légitime et/ou de vendre les informations d'identification volées sur le dark web.

Risque pour les Entreprises

Les employés sont une cible de choix pour les attaquants qui cherchent à mener des attaques plus importantes contre l'organisation. La même psychologie
ce qui rend difficile pour les consommateurs
remarquer un domaine frauduleux s'applique tout aussi bien aux salariés de l'entreprise.



Les fournisseurs peuvent être une porte dérobée

Les e-mails de phishing provenant de domaines similaires au domaine de l'entreprise ou de fournisseurs et de partenaires ne sont pas toujours signalés comme un risque aux employés. Au lieu de cela, ils semblent être légitimes et les informations ou demandes contenues dans l'e-mail sont supposées être valides. Cette attaque est si efficace que 94 % des organisations ont observé des domaines frauduleux utilisés dans les e-mails pour une attaque.

Prise de contrôle de compte

L'usurpation d'identité est l'une des principales voies vers une attaque de prise de contrôle de compte réussie. Arrêter les attaques d'usurpation d'identité avant qu'elles ne deviennent actives est le meilleur moyen de protéger vos employés et vos actifs.

Une erreur stupide peut coûter des millions

Dans les attaques de type ATO, les perpétuateurs avec des informations d'identification volées peuvent se faire passer pour de véritables utilisateurs, accédant aux mêmes ressources que l'utilisateur pourrait le faire. Les programmes exécutés peuvent installer des rançongiciels qui créent des revenus directs pour les attaquants ou lancer un rootkit sur le terminal, permettant aux attaquants d'accéder au réseau interne. Avec un rootkit, les attaquants peuvent organiser des attaques plus complexes et persistantes qui peuvent compromettre de grandes quantités de données au fil du temps avec peu de risque d'être pris.

$150,000

coût d'une attaque de phishing réussie

$170,000

coût d'une violation de données réussie

$330,000

coût d'un incident de sécurité réussi

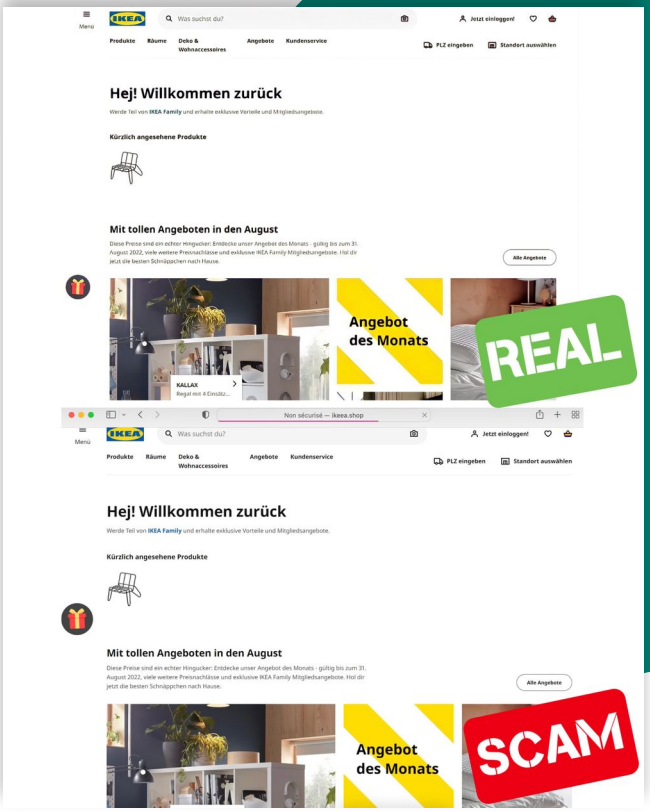
Ne faîtes confiance a personne

Les attaques peuvent être aussi simples que de demander aux utilisateurs de remplir un formulaire pour mettre à jour leur mot de passe, comme la violation de Twilio en août 2022 où les employés ont été invités à mettre à jour leurs mots de passe de connexion via un domaine malveillant qui a recréé leur page de gestion des services informatiques d'Okta, leur fournisseur d'identification. Dans cette brèche, au moins un employé est tombé dans le piège de l'escroquerie qui a permis à l'auteur de la menace d'accéder aux informations sensibles des clients et aux données de l'entreprise.

Protéger les clients et les parties prenantes

Le consommateur est une autre cible de nombreuses attaques de domaine frauduleuses. Les consommateurs naviguant sur un domaine frauduleux se voient souvent présenter un site qui est une copie apparente du domaine auquel ils s'attendaient, ce qui ajoute au défi de différencier la fraude. Toute information donnée est interprétée comme provenant de l'organisation réelle, et les vitrines fournies semblent tout aussi fonctionnelles que l'original.

La réputation de la marque peut être durement touchée

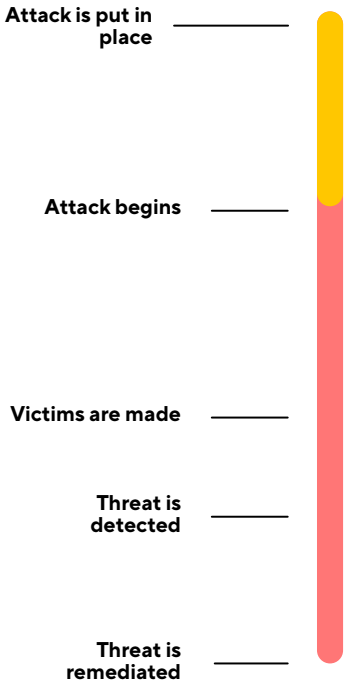


Les utilisateurs trompés achètent des produits sur le site qui ne seront jamais livrés et transmettent volontairement leurs informations de carte de crédit aux attaquants, comme dans l'arnaque ciblant IKEA, détectée par Bfore.Ai en août 2022. Dans cette arnaque, les acteurs de la menace ont créé un site Web sous le domaine ikeea[.]shop et dupliqué le site d'origine (ikea.com) rendant presque impossible la distinction entre le vrai et le faux. Une fois qu'un achat est effectué sur le site malveillant, les utilisateurs sont déçus lorsque leurs achats n'arrivent jamais et exaspérés lorsque leurs cartes sont utilisées illégalement.

Même si le propriétaire du domaine existant n'héberge pas de faux domaines, les consommateurs estiment toujours que l'existence d'un tel site est un signe de faiblesse dans la sécurité de l'organisation. Toute désinformation fournie ou mauvais traitement subi par le client est directement imputé non pas au fraudeur mais au propriétaire du domaine. Les entreprises qui ne connaissent pas les faux domaines continueront de subir les effets néfastes de leur existence jusqu'à ce qu'elles soient au courant du domaine et prennent les mesures appropriées pour le supprimer.

Comment sont menées les attaques d'usurpation d'identité en ligne ?

Les attaques d'usurpation d'identité en ligne ne se limitent pas à la création et au chargement d'un site Web frauduleux avec un contenu trompeur ou malveillant. L'utilisation efficace des attaques d'usurpation d'identité nécessite de diriger les autres vers le contenu. Ceci est accompli en intégrant des liens dans les médias sociaux, les e-mails, les SMS et d'autres canaux de communication courants. Les utilisateurs sont incités à cliquer sur ces liens soit par le biais de messages qui créent un sentiment d'urgence, soit en faisant apparaître le lien comme faisant partie intégrante d'un flux de travail tel que la facturation.



L'attaquant veut que les personnes qui voient les liens croient qu'il s'agit d'un site Web légitime, et non d'un faux, de sorte que le style et la mise en page exacts seront souvent copiés. Lorsque les visiteurs entrent sur le site, le thème cohérent aidera à les rassurer sur le fait que tout va bien, à renforcer la confiance et, espérons-le, à encourager le visiteur à rester.

94 % des organisations ont observé des domaines frauduleux utilisés dans les e-mails pour une attaque

Se défendre contre l'usurpation d'identité en ligne

Les organisations ne sont pas sans recours pour se protéger contre les domaines frauduleux. Créer du contenu pour peupler des sites frauduleux et semer de faux liens ne se fait pas instantanément. Les entreprises qui surveillent les enregistrements pour des domaines similaires et émettent rapidement des ordres de retrait permettent aux entreprises d'arrêter les attaques avant qu'elles n'aient le temps de s'intensifier

Formez votre équipe

Sensibiliser les employés et le personnel aux attaques par usurpation d'identité est un élément de la protection de votre organisation. Les membres de l'équipe conscients de ces attaques et de leur impact potentiel servent de couches de détection supplémentaires, aidant à identifier et alerter lorsqu'elles sont vues. En plus de soutenir les efforts d'identification de l'organisation, la sensibilisation les aide à ne pas devenir des cibles d'attaques, les empêchant d'aller sur des sites usurpés où ils pourraient devenir victimes d'hameçonnage ou de logiciels malveillants.

Les humains peuvent toujours être trompés

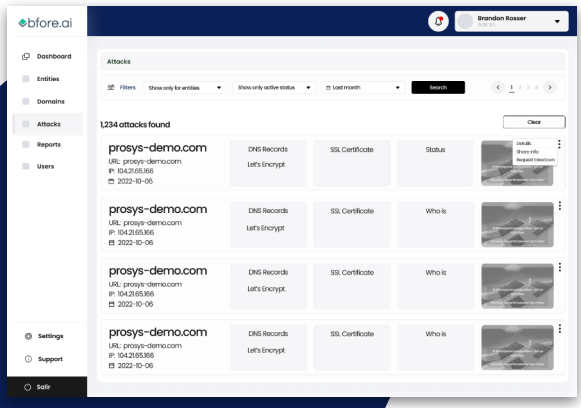
Bien que la sensibilisation soit une couche importante, elle ne remplace pas suffisamment une solution automatisée pour détecter et se défendre de manière proactive contre l'usurpation d'identité. Comme les individus ne sont pas des identificateurs parfaits, il suffit d'un seul faux pas dans la détection pour qu'un employé soit victime de tels sites, entraînant des divulgations de données ou des infections par des logiciels malveillants. Les solutions technologiques qui défendent l'organisation sont beaucoup plus précises et appliquent systématiquement la couche de protection dans toute l'organisation, améliorant ainsi son efficacité globale.

bfore.ai

Automatisez pour gagner

Traquer les squatters n'est pas une tâche accomplie une fois, et vous pouvez reprendre vos activités habituelles. Les squatters reviendront à plusieurs reprises avec de nouveaux sites usurpés et de faux domaines, tentant d'attirer les sans méfiance. La gestion de ce défi nécessite une surveillance continue pour détecter leur retour et les éliminer le plus rapidement possible.

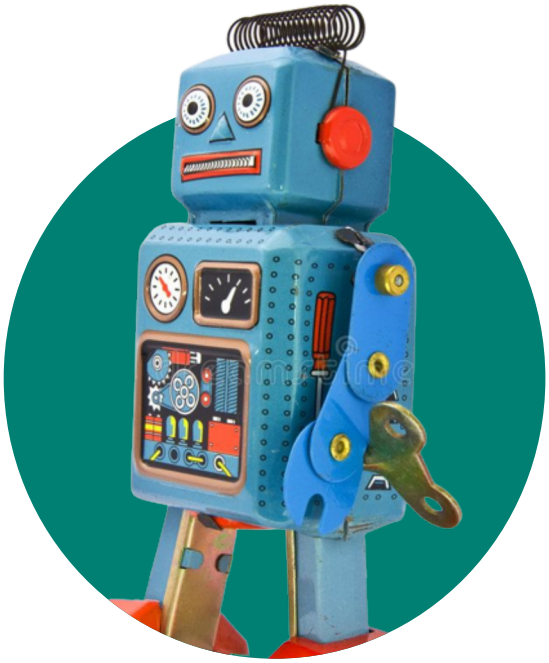
La surveillance ressemble à un processus simple, car tous les enregistrements de domaine sont essentiellement publics, donc surveiller l'apparition de noms de domaine similaires sur la liste devrait être trivial. Cependant, en réalité, le nombre de permutations que les attaquants peuvent apporter à un domaine existant est assez important lorsque l'on tient compte des combinaisons de substitutions, d'omissions et de transpositions de lettres que les attaquants pourraient utiliser pour imiter un seul domaine.



Des solutions existent

Des outils comme Bfore.Ai conçus pour automatiser l'identification préventive des vecteurs malveillants aident à faire le travail. Avec plus de 5 millions de nouveaux domaines enregistrés par mois (plus de 180 000 par jour) et compte tenu du nombre de permutations possibles de noms de domaine similaires, les efforts manuels pour surveiller les nouveaux enregistrements prennent du temps et ne sont pas extrêmement efficaces. ... Bfore.Ai détecte plus de 120 000 domaines malveillants par mois...

Constituez votre boîte à outils



L'automatisation est essentielle pour se protéger contre les nouvelles menaces. Un seul acteur malveillant pourrait enregistrer des centaines de domaines pour usurper l'identité de votre marque. Si vous ne surveillez pas activement vos noms de domaine, vous ne le saurez jamais. Une protection efficace de la marque repose sur l'automatisation pour suivre toutes les attaques potentielles

Surveillance des domaines Web

La surveillance continue des modifications DNS de domaine malveillantes et des nouveaux enregistrements est inefficace avec les processus manuels. Avec le volume de changements de domaine quotidiens dans le monde, les nouveaux enregistrements sont facilement manqués. Un investissement massif en main-d'œuvre est nécessaire pour identifier les menaces potentielles et analyser leur contenu à des fins de vérification.

L'automatisation est cruciale pour éviter les menaces corrélées à votre domaine et à ceux des fournisseurs. Avec l'automatisation, l'identification et l'analyse fastidieuses sont confiées à des machines qui excellent dans ces tâches plutôt qu'à des humains, qui s'ennuient et ont d'autres tâches à gérer. La réduction de cette charge permet au personnel de valider plus efficacement les menaces identifiées et de tirer parti des capacités de retrait intégrées au service, rationalisant ainsi l'ensemble du processus.

Surveillance des médias sociaux

Les médias sociaux sont utilisés non seulement par l'organisation seule, mais aussi par les cadres dont la messagerie est considérée comme une voix alternative de l'entreprise. Prendre le contrôle de comptes de réseaux sociaux ou se faire passer pour des comptes légitimes offre aux attaquants un canal réceptif pour diffuser des messages malveillants, tels que des URL toxiques ou des informations erronées.

Le leadership est en jeu

La surveillance de la marque de l'entreprise et des profils des dirigeants doit être gérée 24 heures sur 24, 7 jours sur 7, car tout manquement peut rapidement entraîner des problèmes. Les solutions optimales disposent d'une automatisation pour surveiller en permanence et détecter efficacement les problèmes avant que les attaquants ne puissent les exploiter. Les capacités de retrait intégrées sont essentielles pour une solution efficace, résolvant rapidement le problème une fois détecté.

Les menaces sur les réseaux sociaux continuent d'augmenter avec une croissance de 47 % du premier au deuxième trimestre 2022

Remédier à une attaque

Ce n'est pas parce que le processus d'enregistrement a une validation minimale pour les nouveaux domaines qu'il n'y a pas de règles concernant les enregistrements appropriés. Les noms de domaine qui enfreignent les noms commerciaux existants, les marques de commerce ou qui existent pour fraude peuvent être supprimés par le biais d'un processus de retrait. L'identification et la demande de retrait incombent au titulaire du domaine existant, ce qui plaide auprès des bureaux d'enregistrement autorisés pour la suppression du domaine.

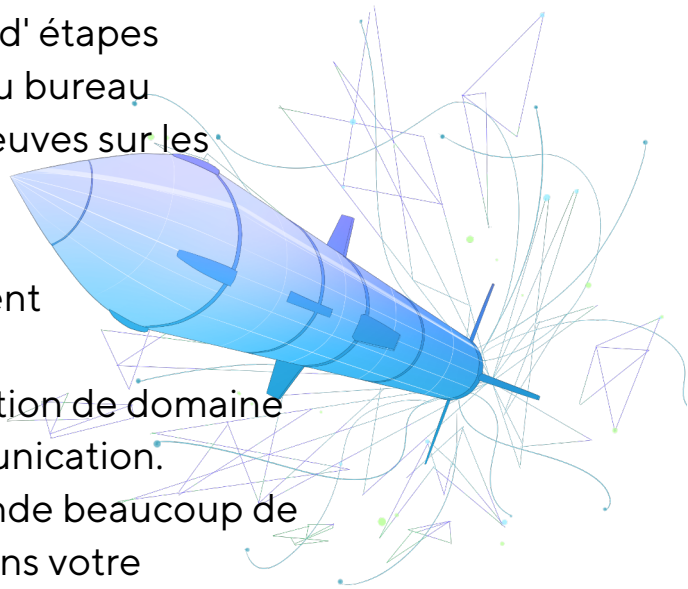
Constituez vos preuves

Les entreprises doivent expliquer pourquoi elles pensent qu'un domaine a été enregistré de mauvaise foi. Trouver un domaine similaire ne garantit pas qu'il s'agit d'un motif suffisant pour un retrait immédiat. De nombreuses entreprises ont des noms identiques et les utilisent dans le cadre de leur enregistrement.

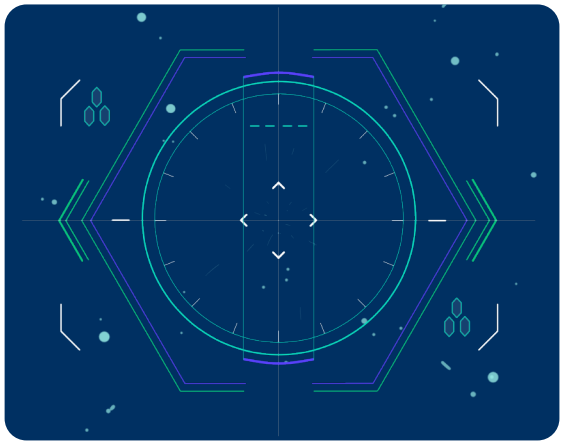
La ressemblance de domaine n'est pas tout

Cela a été vu dans le cas des moteurs Nissan contre Uzi Nissan qui a persisté pendant des années et a nécessité un tribunal pour décider de la propriété du domaine.

Comment neutraliser une attaque ?



Le processus de retrait est généralement plein d' étapes manuelles à gérer. Contacter l'équipe d'abus du bureau d'enregistrement de domaine, recueillir des preuves sur les raisons pour lesquelles le domaine agit de manière malveillante, et un suivi continu, en collaboration avec le bureau d'enregistrement jusqu'à ce que le domaine soit supprimé.
Ce processus est répété pour chaque permutation de domaine suspecte, créant un ensemble de fils de communication.
Gérer ce processus sans automatisation demande beaucoup de temps et d'investissement en main-d'œuvre dans votre organisation.

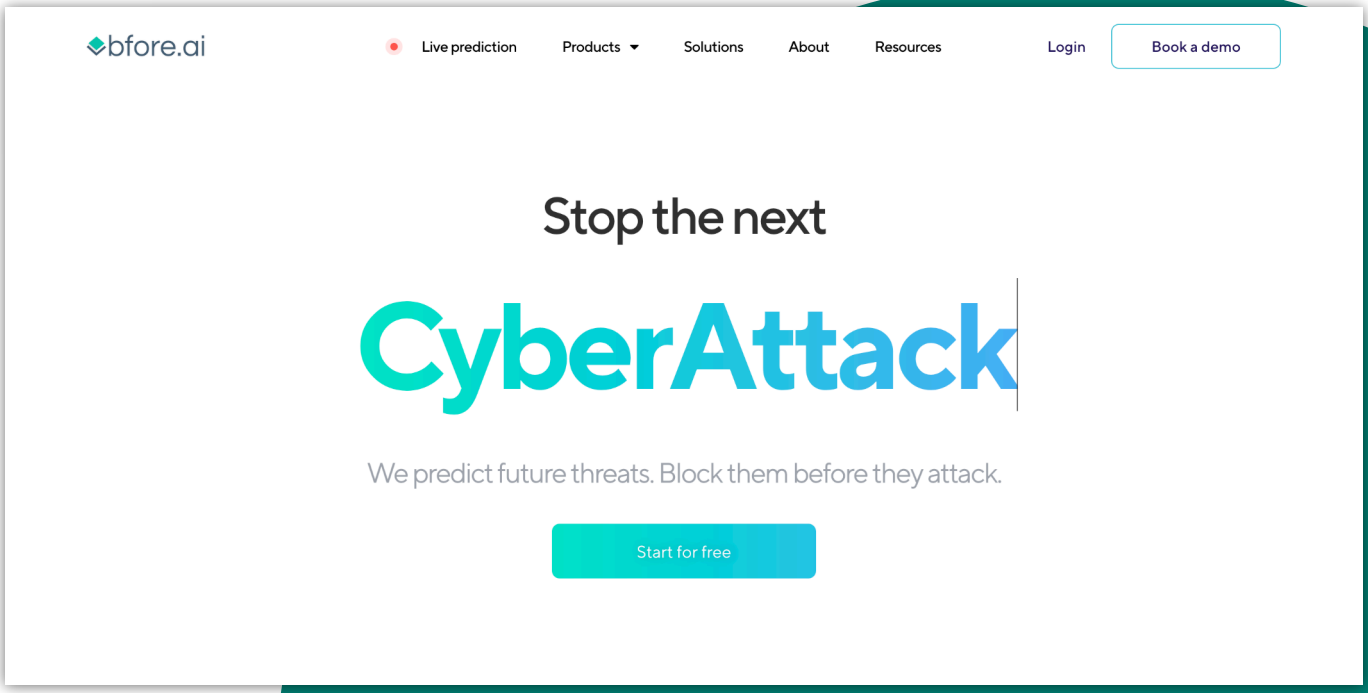


Faîtes le plus vite

Afin de le faire plus rapidement, de manière plus sûre et pour réussir un retrait, il est crucial de travailler avec un partenaire de sécurité autorisé. Les experts en démantèlement de sécurité sauront comment rassembler des preuves et pousser les bureaux d'enregistrement de domaine à réaliser des démantèlements, parfois même en moins de 10 minutes.
Une fois qu'un retrait a lieu, le bureau d'enregistrement public supprime l'enregistrement du domaine frauduleux. Même si les utilisateurs cliquent sur des liens contenant le nom, les serveurs DNS ne pourront pas le résoudre en une adresse IP, arrêtant ainsi son utilisation comme vecteur d'attaque.

Soyez prédictif, arrêtez de chasser

Arrêter l'utilisation frauduleuse d'un domaine rapidement après l'enregistrement est essentiel pour éliminer une attaque avant qu'elle ne nuise à une organisation. Cela nécessite une surveillance continue de tous les domaines nouveaux et existants pour l'existence d'activités frauduleuses. Bfore.ai permet aux organisations de surveiller et d'évaluer automatiquement les domaines enregistrés. Bfore.ai dispose d'un ensemble complet de solutions pour défendre votre organisation contre les activités frauduleuses, en déployant des contre-mesures pour limiter l'impact et en gérant le processus de retrait.



Learn more how prediction can help

Book a Demo

Visit Website

Distribué en France par :
AMC SOFT
1, Pl Paul Verlaine
92100 Boulogne - Billancourt FRANCE.
https://amcsoft.fr
contact@amcsoft.fr
Tel : +33680741316

bfore.ai