Un guide pour les PME afin de comprendre les menaces du Dark Web

Votre guide pour comprendre le dark web, pourquoi il constitue une menace pour votre entreprise et comment réduire les risques.

Contenu

Introduction

Naviguer sur le Dark Web

Dans le monde d'aujourd'hui axé sur le numérique, les entreprises, en particulier les petites et moyennes entreprises (PME), dépendent plus que jamais de la technologie. Si cette connectivité apporte de nombreux avantages, elle expose également les entreprises à un nombre toujours croissant de cybermenaces.

L'un de ces périls est le Dark Web, où les informations d'identification des utilisateurs volées peuvent devenir des armes puissantes entre les mains des cybercriminels. Ce guide complet est conçu pour les responsables informatiques et les cadres supérieurs des PME. Il aborde le sujet crucial de la raison pour laquelle les informations d'identification des utilisateurs volées sur le dark web constituent une menace importante pour votre entreprise.

À propos de ce guide

Nous explorerons ce qu'est le dark web, comment il fonctionne et comment les cybercriminels l'exploitent à des fins malveillantes. En outre, nous étudierons les types de données commerciales qui peuvent être exposées et pourquoi cette exposition représente une menace importante.

Des exemples concrets de brèches de données causées par des informations d'identification exposées seront examinés, ainsi que des stratégies permettant d'atténuer les risques et l'efficacité de la surveillance du Dark Web en tant que solution.

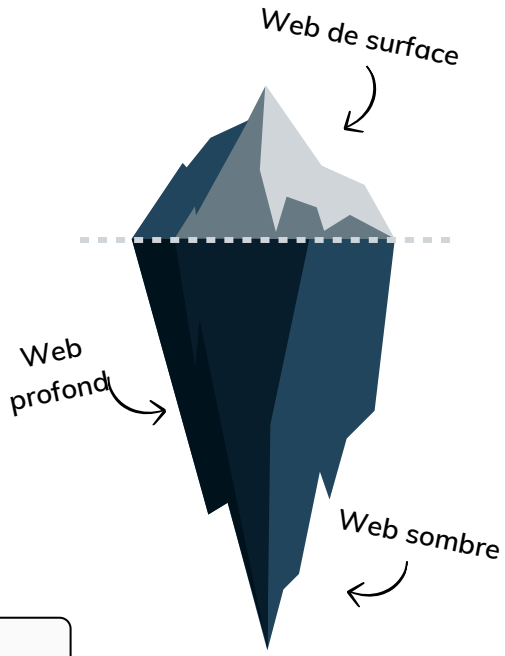
Comprendre le Dark Web

Qu’est-ce que le dark web ?

Le dark web est une partie cachée d’Internet qui n’est pas indexée par les moteurs de recherche conventionnels. Il opère au sein du Web profond, intentionnellement conçu pour rester caché à la vue du public. Pour accéder au dark web, les individus utilisent des logiciels spécifiques, comme Tor (The Onion Router), qui leur permettent de naviguer de manière anonyme. Cet anonymat inhérent en fait une plaque tournante attractive pour diverses activités illégales.

Le dark web est un terrain fertile pour les activités frauduleuses

Le dark web opère au sein du deep web, intentionnellement conçu pour rester caché à la vue du public. Pour accéder au dark web, les individus utilisent des logiciels spécifiques, comme Tor (The Onion Router), qui leur permettent de naviguer de manière anonyme. Cet anonymat inhérent en fait une plaque tournante attractive pour diverses activités illégales.



Le rapport Threat Horizons 2023 de Google Cloud révèle que 86 % des violations impliquent le vol d'identifiants.

Un rapport de Digital Shadow révèle que 24 milliards de noms d’utilisateur et de mots de passe sont disponibles sur le dark web, soit une augmentation de 65 % en seulement deux ans.

Exploitation cybercriminelle

Comment les cybercriminels exploitent le dark web à des fins criminelles

Les cybercriminels exploitent l'anonymat et les ressources fournies par le dark web pour cibler les entreprises, en particulier les PME, de multiples manières.

Informations d'identification volées

Les cybercriminels acquièrent souvent les identifiants de connexion des comptes professionnels via des brèches de données, des campagnes de phishing ou des attaques de logiciels malveillants. Les informations d'identification sont ensuite vendues sur le dark web, offrant ainsi un accès non autorisé aux systèmes d'entreprise et aux données sensibles.

Attaques de force brut d'informations d'identification

Les attaquants utilisent des combinaisons de nom d'utilisateur et de mot de passe volées pour obtenir un accès non autorisé à plusieurs comptes sur divers services en ligne. Les PME peuvent utiliser des mots de passe partagés ou des mesures de sécurité faibles, ce qui les rend vulnérables à de telles attaques.

Rançongiciel

Les cybercriminels sur le dark web vendent des ransomwares en tant que service, permettant à des criminels moins compétents techniquement de lancer des attaques de ransomware contre les entreprises. Les PME, disposant de ressources limitées en matière de cybersécurité, peuvent être des cibles attractives.

Campagnes de phishing

Les criminels du dark web proposent des kits et des services de phishing qui leur permettent de créer des e-mails et des sites Web de phishing convaincants. Les employés des PME peuvent être victimes par inadvertance de ces escroqueries, entraînant des brèches de données ou des pertes financières.

Activités frauduleuses

Le dark web offre une plate-forme permettant aux cybercriminels de se livrer à diverses activités frauduleuses, telles que le vol d'identité, la fraude à la carte de crédit et les escroqueries au remboursement d'impôts, qui peuvent toutes cibler les PME et leurs employés.

Vente et échange de données

Les données commerciales volées, notamment les informations sur les clients, les dossiers des employés et les données exclusives, sont souvent échangées ou vendues sur le dark web. Ces données peuvent être exploitées à des fins financières ou utilisées dans d'autres attaques.

Quelles données d’entreprise peuvent être exposées ?

Les entreprises stockent une multitude d’informations sensibles qui peuvent être ciblées par les cybercriminels via des informations d’identification volées. Ces données peuvent inclure :

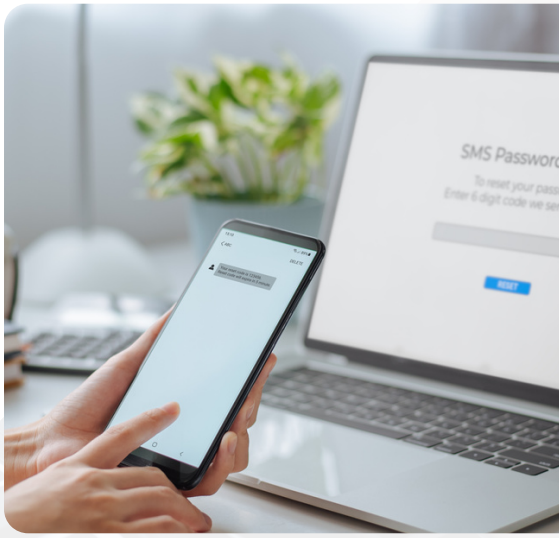
- Identifiants utilisateur : informations d'identification de connexion volées, telles que les noms d'utilisateur et les mots de passe
- Informations client : données personnelles et financières des clients
- Dossiers financiers : données financières de l'entreprise, y compris les détails du compte bancaire
- Propriété intellectuelle : secrets commerciaux, brevets et informations exclusives
- Données des employés : dossiers RH et informations personnelles des employés (informations personnellement identifiables)
- Correspondance par courrier électronique : les comptes de messagerie professionnels sont une cible précieuse
- Données opérationnelles : informations relatives aux opérations commerciales et aux chaînes d'approvisionnement
- Jetons d'authentification : clés API, jetons d'accès et informations d'authentification
- Données financières : données financières d'entreprise, y compris les budgets et les prévisions financières
- Documents juridiques : Contrats, accords juridiques et rapports de conformité
- Informations sur les fournisseurs et les partenaires : informations relatives aux fournisseurs et aux partenaires

65%

Les combinaisons nom d’utilisateur et mot de passe proposées à la vente sur le dark web ont augmenté de 65 % depuis 2020.

24,6 milliards

Quelque 24,6 milliards d’ensembles complets de noms d’utilisateur et de mots de passe sont en circulation sur les marchés



Source : Recherche sur les photons des ombres numériques

Pourquoi les données exposées constituent-elles une menace pour les entreprises ?

Les données des utilisateurs exposées sur le dark web posent un problème important aux entreprises, car elles peuvent entraîner de graves failles de sécurité et des vols d'identité. Cette exposition met non seulement en danger les informations personnelles et financières des clients et des employés, mais porte également atteinte à la réputation et à la confiance de l'entreprise. Cela peut également entraîner des conséquences juridiques et des pertes financières dues à des fraudes et à des brèches de conformité.

Voici quelques-uns des risques auxquels les entreprises sont confrontées si elles ne s'attaquent pas aux menaces du Dark Web.

Pertes financières
Causé par des amendes, des frais juridiques et des transactions non autorisées.

Dommages à la réputation
Une brèche de données peut éroder la confiance entre les clients et les parties prenantes.

Répercussions juridiques
Causé par des poursuites judiciaires, des amendes réglementaires et des brèches de conformité.

Perturbation opérationnelle
La restauration des opérations normales après une brèche prend beaucoup de temps.

> L'impact moyen d'une brèche de données sur les organisations de moins de 500 employés est de 3,31 millions de dollars.

Rapport IBM 2023 sur le coût d'une brèche de données

Exemples de brèches de données réelles

Les brèches de données importantes constituent une menace importante pour les entreprises, en grande partie en raison de la pratique courante de réutilisation des mots de passe sur les comptes personnels et professionnels. Lorsqu'un compte est compromis, cela peut conduire à un accès non autorisé à d'autres, mettant ainsi en danger les informations commerciales sensibles et la confiance. Nous explorons ici certaines des plus grandes brèches de données de ces derniers temps et l'ampleur des données compromises.

Date
Août 2013
Impact
3 milliards de comptes

Yahoo

La brèche massive de données de Yahoo, signalée pour la première fois en 2016 mais survenue en 2013. Initialement estimée à plus d'un milliard de comptes d'utilisateurs concernés, Yahoo a ensuite révisé ce chiffre à 3 milliards. La brèche a compromis les informations du compte, telles que les questions de sécurité, mais n'incluait pas les mots de passe en clair ni les données financières.

Date
juin 2021
Impact
700 millions d'utilisateurs

LinkedIn

Un pirate informatique a publié les données de 700 millions d'utilisateurs de LinkedIn sur le dark web après avoir exploité l'API du site. LinkedIn a classé cela comme une brèche des conditions de service, et non comme une brèche de données, car cela n'incluait pas de données personnelles sensibles. Cependant, les données exposées contenaient des adresses e-mail, des numéros de téléphone et d'autres détails, soulevant des inquiétudes quant à d'éventuelles attaques d'ingénierie sociale.

Date
avril 2019
Impact
533 millions d'utilisateurs

Facebook

En avril 2019, il a été découvert que les données des applications Facebook, notamment les numéros de téléphone, les noms de compte et les identifiants Facebook de plus de 530 millions d'utilisateurs, avaient été exposées publiquement. En avril 2021, ces données sont apparues gratuitement sur le dark web, suggérant une intention criminelle.

Lutter contre les menaces du Dark Web

Comment protéger votre entreprise contre le dark web

Réduire les risques associés aux données utilisateur exposées sur le dark web est un aspect essentiel de la cybersécurité moderne. Voici quelques moyens essentiels par lesquels les entreprises peuvent renforcer leurs défenses et protéger les informations sensibles des utilisateurs.

Surveillance et audits réguliers des données

Effectuez un suivi et des audits réguliers de vos données. Utilisez des outils qui analysent le dark web à la recherche de données volées pour alerter l'entreprise si ses informations sont compromises.

Formation complète des utilisateurs

Mettez en œuvre des programmes de formation continue des utilisateurs pour les employés afin de les informer sur les meilleures pratiques en matière de cybersécurité, les escroqueries par phishing et l'importance d'une gestion sécurisée des mots de passe, avec du matériel de formation régulièrement mis à jour.

Mesures de cybersécurité strictes

Adoptez des protocoles de cybersécurité robustes tels que des pare-feu, des systèmes de détection d'intrusion et assurez des mises à jour régulières des logiciels de sécurité. Cela crée une formidable première ligne de défense contre les cybermenaces.

Cryptage des données

Chiffrez les données sensibles, en transit comme au repos. Le cryptage agit comme une barrière critique, rendant difficile l'utilisation des données par des personnes non autorisées, même si elles parviennent à y accéder.

Protocoles de contrôle d'accès et d'authentification

Mettez en œuvre des mesures strictes de contrôle d'accès avec des méthodes d'authentification fortes telles que l'authentification à deux ou plusieurs facteurs. Cela garantit que seul le personnel autorisé a accès aux données sensibles.

Surveillance du Dark Web

Surveillance du Dark Web : une couche de sécurité essentielle

La surveillance du Dark Web est une approche proactive pour détecter et atténuer les risques associés aux informations d'identification des utilisateurs exposées. Cela implique l'utilisation d'outils et de services spécialisés pour analyser en permanence le dark web à la recherche de signes de données compromises, y compris les identifiants de connexion.

Voici quelques raisons pour lesquelles la surveillance du dark web est une solution efficace :

La détection préventive

La surveillance du Dark Web peut identifier les informations d'identification compromises dès le début de la chaîne d'approvisionnement des cybercriminels, donnant ainsi aux entreprises une longueur d'avance pour atténuer les risques.

Réponse rapide

Grâce à des informations instantanées, les entreprises peuvent prendre des mesures rapides, comme réinitialiser les mots de passe ou informer les parties concernées, pour minimiser les dommages.

Avantages de la surveillance du Dark Web

Protection proactive

En recherchant activement les données exposées, les entreprises peuvent se protéger avant que les cybercriminels n'aient la possibilité de les exploiter.

Couverture complète

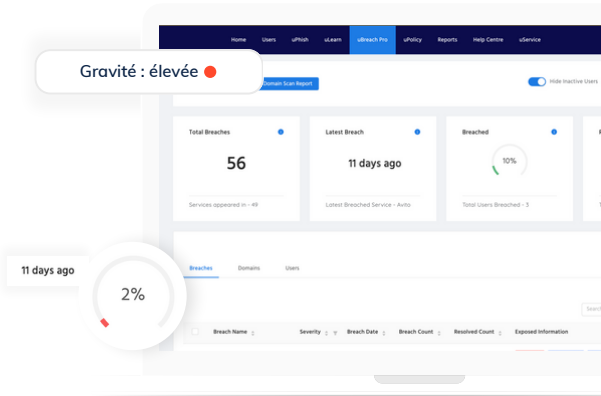
Les outils de surveillance du Dark Web peuvent analyser plusieurs couches du Dark Web, offrant ainsi une couverture complète et réduisant les angles morts.

Entrer en contact

Votre entreprise dispose-t-elle de données sensibles exposées sur le dark web ? Découvrons-le...

Obtenez un rapport gratuit sur les brèches du Dark Web pour votre entreprise

Franchissez une étape cruciale vers la protection de votre entreprise contre les cybermenaces en demandant votre analyse gratuite de domaine en cas de brèche du Dark Web.



Comment ça fonctionne

Votre analyse de domaine gratuite évaluera si les informations professionnelles de vos utilisateurs finaux, y compris les mots de passe des comptes de messagerie, sont exposées sur le dark web.

Que doit fournir mon entreprise ?

Fournissez-nous simplement le nom de domaine de votre entreprise et, si disponible, une liste d'adresses e-mail spécifiques que vous souhaitez que nous analysions (facultatif).

Une fois terminé, vous recevrez un rapport PDF détaillant l'exposition de votre entreprise sur le dark web et les mesures d'atténuation que vous devez prendre.

Contactez-nous dès maintenant et ayez l'esprit tranquille grâce à notre analyse experte des brèches.