CF-Scavenger

FONCTIONNALITÉS CLÉS

- Détection des fuites d'information pouvant impacter la sécurité de votre système d'information

BÉNÉFICES CLÉS

- Pas d'installation sur vos systèmes : une simple liste d'emails ou de TLD nous suffit
- S'intègre à votre SIEM si vous le souhaitez

Pourquoi choisir CF-Scavenger ?

Dans l'environnement complexe de travail actuel, les employés, ainsi que les serveurs, les réseaux et de nombreux autres appareils, utilisent et détiennent des informations d'identification. Ces identifiants, comprenant les noms d'utilisateur et les mots de passe, sont l'épine dorsale de toute bonne stratégie de sécurité.

Le « Credential Stuffing » est un type de cyberattaque où des identifiants extraits illégalement d'un matériel ou d'un service, sont réutilisés par le biais de demandes de connexion automatisée à grande échelle pour obtenir des accès non autorisés à d'autres matériels ou services. La prolifération des fuites de données, combinée aux progrès des outils utilisés par les cybers attaquants pour contourner les protections traditionnelles a fait du Credential Stuffing un vecteur d'attaque populaire.

La principale raison de l'efficacité de ce type d'attaques tient à la réutilisation des mots de passe par les utilisateurs. Des études récentes suggèrent que la majorité des utilisateurs (selon certaines estimations cela peut aller jusqu'à 85%) réutilisent les mêmes identifiants pour accéder à plusieurs services.

CF-Scavenger parcours inlassablement le Web, le Deep Web et le Dark Web pour collecter des fuites de données et vous prévenir quand des identifiants liés à vos domaines ou à vos salariés sont découverts sur internet.

PREUVE DE CONCEPT

Si vous souhaitez réaliser un PoC, contactez-nous à poc@computablefacts.com

SITE WEB

Pour plus d'informations, consultez notre site web : https://computablefacts.com

DISPONIBLE EN BETA !

Comment fonctionne CF-Scavenger ?

CF-Scavenger recherche les informations sensibles accessibles en dehors de votre réseau.

CF-Scavenger surveille, collecte et analyse les données provenant de :

- Forums, sites de « Pastes » et « Google Dorks » pour identifier les bases de données fuitées et en extraire des noms d'utilisateurs et des mots de passes ;
- Répertoires Git/Github/Gitlab accessibles en ligne pour en extraire des secrets ou clefs d'API ;
- Compartiments AWS S3 (Amazon), Azure Storage (Microsoft) et Cloud Storage (Google) pour en exfiltrer des données d'intérêt.

Une fuite de données est détectée. Et après ?

En cas de découverte d'une fuite de données, nous vous alertons aussitôt :

- Via un email si vous le souhaitez ;
- Via une alerte s'intégrant à votre SIEM.

Chaque alerte contient les informations nécessaires et suffisantes pour :

- Prioriser la prise en charge de l'alerte ;
- S'assurer de l'existence de la fuite.

Prix

- 1 euro HT par mois et par email

- 10 000 euros HT par an et par domaine de premier niveau