Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

SÉCURISER SON EXPOSITION SUR INTERNET

QU'EST-CE QUE L'EXPOSITION SUR INTERNET ?

L'exposition sur internet concerne toutes les données et les traces laissées par les systèmes connectés et disponibles sur internet. Ces informations peuvent être directement issues du système d'information (SI) (de manière volontaire ou non), ou peuvent être relayées par des serveurs tiers.

EN QUOI CONSISTE LA SECURISATION DE L'EXPOSITION SUR INTERNET ?

La sécurisation de l'exposition sur internet vise à maitriser la diffusion d'information sur les systèmes connectés à Internet. Les bonnes pratiques mises en œuvre permettent de réduire la surface d'attaque et les tentatives de compromission du SI.

GOOGLE DORKS

Le moteur de recherche Google peut être utilisé à des fins malveillantes via ce que l'on appelle les *Google Dorks*. Il s'agit de requêtes spéciales réalisées via l'utilisation de certains mots-clés spécifiques et permettant de trouver des fuites d'informations sensibles ou des serveurs vulnérables.

Des sites diffusent des exemples de requêtes (ex : https://www.webrankinfo.com/commandes/google) et certains proposent même des listes de mots-clés permettant de faciliter la recherche de données sensibles (ex : Exploit-DB https://www.exploit-db.com/google-hacking-database/).

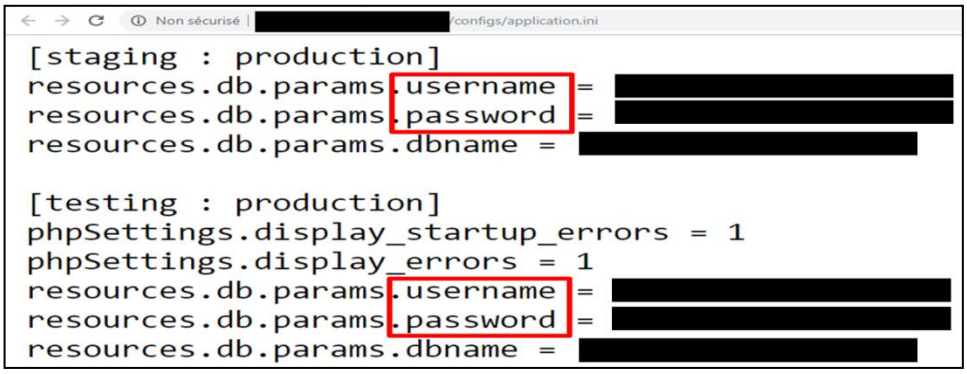

Figure 1 : Exemple de résultat de Google Dork permettant de trouver des identifiants

Afin de limiter son exposition web via les moteurs de recherches, il est recommandé de :

- Durcir la configuration de ses serveurs web exposés (suppression des fichiers installés par défaut, masquage des bannières logicielles, etc). Suivre les guides de durcissement dont celui de l'ANSSI: https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-securisation-des-sites-web/.
- Maintenir ses services à jour et appliquer les correctifs de sécurité dès que possible : https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiches_reflexes-Patch_Management-v1.2.pdf.
- Réaliser régulièrement des scans de vulnérabilité des systèmes exposés sur Internet afin de détecter d'éventuelles erreurs de configuration, fuites de données sensibles, etc.
- Utiliser les mêmes outils que les attaquants afin de détecter d'éventuelles vulnérabilités sur ses serveurs. Attention, il est à noter qu'une version d'un fichier indexé sur Google peut être retrouvée même après sa suppression (visionnage du cache Google).

SHODAN / CENSYS / ZOOMEYE

A la différence de Google ou de Bing qui référencent les sites web, il existe d'autres moteurs de recherche pouvant présenter un risque pour la sécurité de son SI. Il s'agit de *Shodan*, *Censys* et *ZoomEye*. Ces moteurs de recherche répertorient et identifient les équipements connectés à Internet. Certains équipements et logiciels sensibles de son infrastructure (logiciels d'administration, base de données, routeurs, caméras IP, TV connectée, système de gestion de centrales électriques, etc.) peuvent se retrouver indexés et consultables par quiconque. Les attaquants utilisent souvent ces services pour trouver des équipements et logiciels vulnérables.

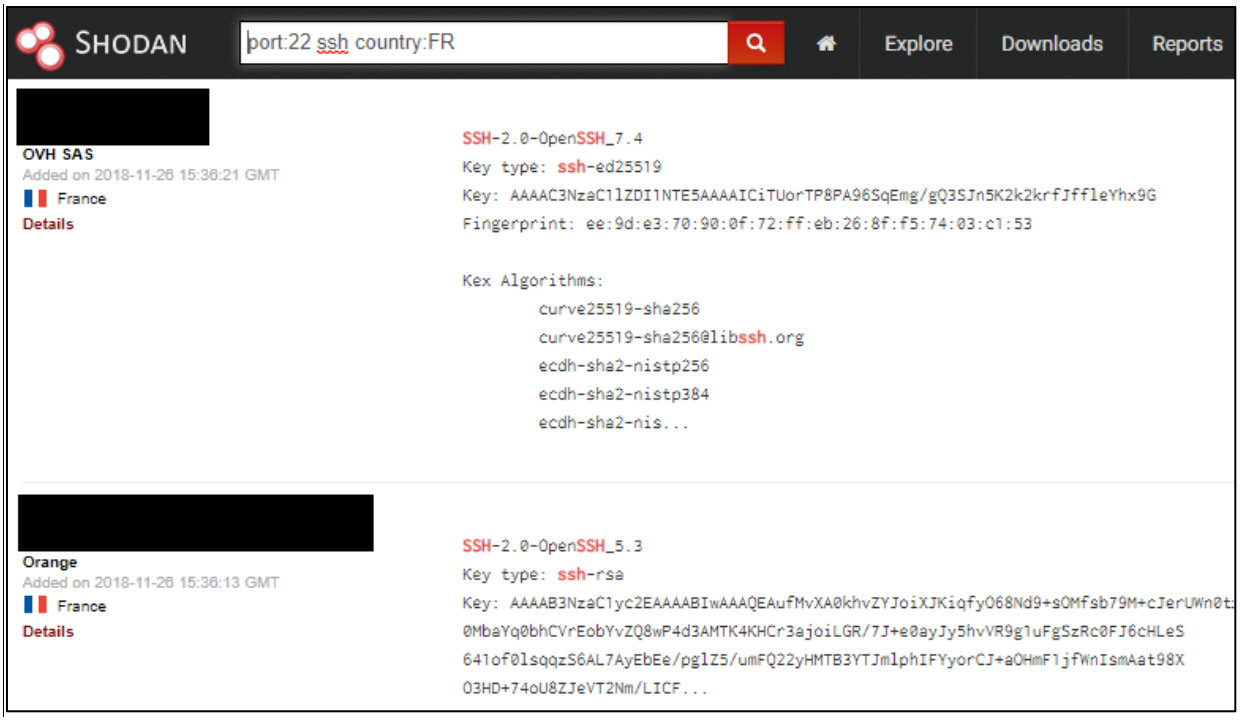

Figure 2 - Exemple de résultats de Shodan listant les adresses IP localisées en France avec le port 22 ouvert

Pour limiter son exposition aux services de type Shodan, Censys et ZoomEye (et les autres outils disponibles sur le marché), il est recommandé de :

- Ne rendre accessible sur Internet que les serveurs et les ports pour lesquels cela est nécessaire (accès public, service à distance, etc.) et restreindre, si possible, aux ports 80 et 443, correspondants aux services HTTP et HTTPS. Les interfaces d'administration (SSH, RDP, etc) doivent être filtrées et uniquement accessibles depuis les réseaux internes et aux personnels dûment habilités.
- Effectuer régulièrement des recherches à partir de ces services afin de vérifier son exposition. A noter que les résultats publiés par ces outils ne sont pas toujours à jour.
- Il est aussi possible de bloquer l'indexation de ses équipements par la mise en place d'un filtrage :
  - Censys utilise les plages IP 141.212.121.0/24 et 141.212.122.0/24.
  - Shodan ne fournit pas les IP qu'il utilise pour ses scans mais il est possible de trouver des listes sur Internet (https://www.evdoinfo.com/content/view/5221/64). Il existe des scripts permettant de créer de manière dynamique une liste noire d'IP lors de tentatives de scan par ce service (https://github.com/romcheckfail/shodan-ip-block-list).
  - ZoomEye ne fournit pas d'adresse IP à bannir non plus. Cependant, le service met à disposition deux mécanismes permettant d'empêcher les scans (un pour les services web, et un autre pour tous les autres appareils) : https://www.zoomeye.org/about.