DÉTOURNEMENT DE SOUS-DOMAINE

RAPPORT DE VULNÉRABILITÉ

RÉSUMÉ

Les entreprises du monde entier utilisent internet pour l'ensemble de leurs opérations : sites web, messagerie, authentification, communications VoIP, et plus encore. Faisant parti de l'angle d'attaque externe d'une entreprise, Internet doit donc, à ce titre, faire l'objet d'une surveillance continue pour contrer les attaques des cybercriminels et la fraude. Le DNS (système de noms de domaine) est essentiellement « l'annuaire » d'Internet. Or, actuellement la maintenance des enregistrements DNS est l'une des tâches les plus négligées. Ce manque de rigueur est dû à 20 ans d'accumulation de différents propriétaires, politiques et fournisseurs autour des DNS, et bien sûr, à la crainte inhérente des administrateurs de supprimer quoi que ce soit pour lequel ils ne sont pas sûrs à 100 %. Recenser tous leurs actifs numériques et différencier ceux qui sont critiques, fonctionnels ou redondants (et donc inutiles) est un défi de taille pour les entreprises. Il est encore plus terrible de s'apercevoir qu'en passant en revue les milliers de portefeuilles de noms de domaine gérés par CSC, on constate qu'un enregistrement DNS sur cinq est vulnérable au détournement de sous-domaine.

QUELQUES CHIFFRES CLÉS

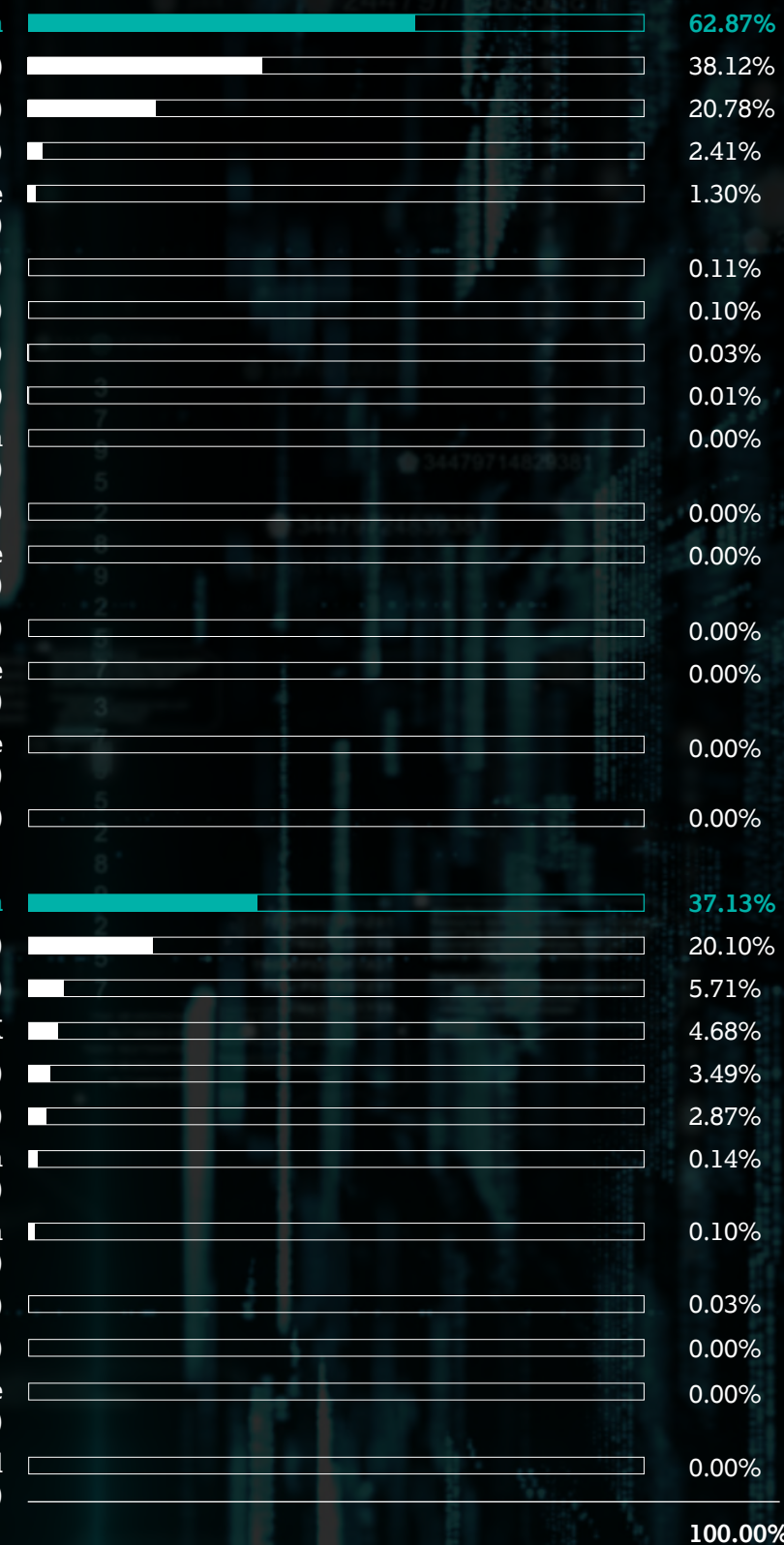
CSC a analysé plus de 6 millions d'enregistrements DNS de notre base de données. Nous avons ensuite isolé les enregistrements de type A et les enregistrements CNAME pointant vers une infrastructure Cloud, ce qui nous a donné un peu plus de 440 000 enregistrements DNS qui pourraient être potentiellement compromis par un détournement de sous-domaine. Cette analyse nous a permis de comprendre l'état actuel de la gestion des sous-domaines des entreprises. À partir de ces 440 000 enregistrements DNS, nous avons démontré que de nombreuses entreprises étaient susceptibles d'être victimes d'un détournement de sous-domaine.

21 % des enregistrements DNS pointent vers du contenu qui n'est plus actif et donc qui ne répondent pas ; cela rend les entreprises particulièrement vulnérables à un détournement de sous-domaine.

63 % affichent des erreurs correspondant à des codes tels que « 404 not found » (page non trouvée) ou « 502 bad gateway » (mauvaise passerelle). De nombreux noms de domaine, dont les enregistrements DNS sont configurés, renvoient une mauvaise réponse.

Un pourcentage considérable de 38 % affichent l'erreur « internal server error » (erreur de serveur interne), ce qui montre que les entreprises doivent améliorer leurs procédures de nettoyage du DNS et de « cyber-hygiène ».

ENREGISTREMENTS DNS ANALYSÉS



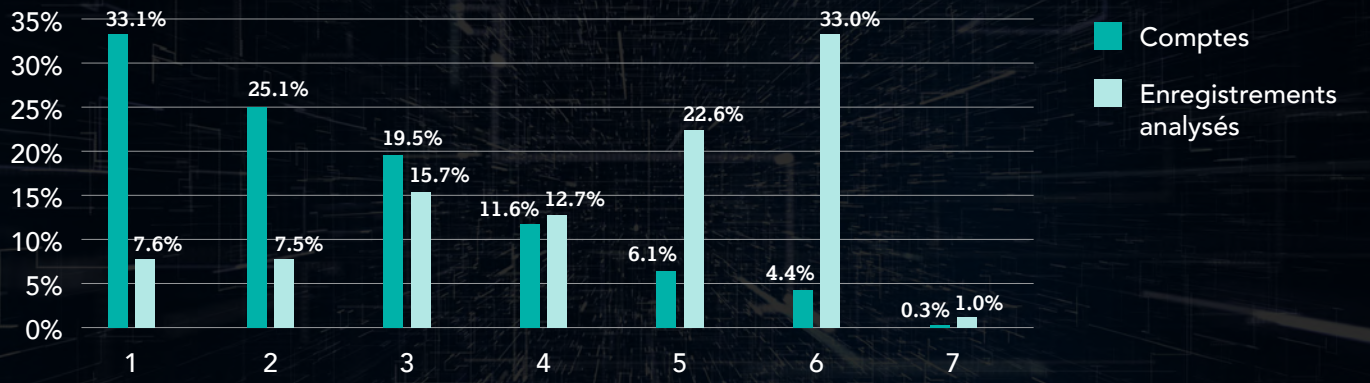
FACTEURS DE RISQUE : FORTE UTILISATION DE FOURNISSEURS CLOUD

Parmi tous les enregistrements analysés, **plus de 82 %** sont hébergés par des fournisseurs de services cloud

Ce pourcentage reflète une tendance selon laquelle, ces dernières années, les entreprises ont externalisé leur infrastructure auprès de fournisseurs de services cloud plutôt que d'utiliser des centres de données internes classiques. Faire appel à des fournisseurs de services cloud permet aux entreprises d'accéder à de nouvelles technologies, et leur permet d'être plus agiles et dynamiques, et de réduire leurs coûts. Néanmoins, cette externalisation comporte des risques supplémentaires pour les entreprises, qui doivent désormais gérer plus d'enregistrements DNS qu'auparavant.

FACTEURS DE RISQUE : DÉCENTRALISATION DES FOURNISSEURS POUR LES ENTREPRISES POSSEDANT D'IMPORTANTS PORTEFEUILLES

NOMBRE DE FOURNISSEURS UTILISÉS



58 % des entreprises analysées semblent parvenir à regrouper leurs sous-domaines auprès d'un ou deux fournisseurs de services cloud, mais elles possèdent généralement des portefeuilles plus petits et plus faciles à gérer.

À l'inverse, 11 % des entreprises analysées dans le cadre de cette étude ont fait appel à au moins cinq fournisseurs de services cloud. Ces entreprises comptent pour plus de la moitié de tous les enregistrements DNS analysés et certaines détiennent de vastes portefeuilles incluant des milliers d'enregistrements. Cela montre que les entreprises possédant de grands portefeuilles peuvent ne pas avoir une gestion centralisée de leurs fournisseurs de services cloud, ce qui les empêche d'avoir une bonne vue d'ensemble de leurs enregistrements DNS.

RÉPARTITION DES FOURNISSEURS DE SERVICES CLOUD UTILISÉS

- GoDaddy (34.2%)
- Microsoft (16%)
- Cloudflare (17.4%)
- Akami (12.7%)
- AWS (16.3%)
- Others (3.4%)

Plus de 96 % de tous les enregistrements DNS analysés sont répartis parmi cinq des plus grands fournisseurs de services cloud : GoDaddy®, Cloudflare®, AWS, Microsoft® et Akamai.

ATTÉNUER LES MENACES CYBER PAR LA SURVEILLANCE DES SOUS-DOMAINES

Les grandes entreprises qui possèdent des portefeuilles de marques diversifiés et sont actives dans plusieurs pays n'ont souvent pas conscience de l'ampleur de leur empreinte numérique. Les enregistrements numériques se multiplient au fil du temps, et transforment la cyber-hygiène en véritable casse-tête.

Sans une supervision appropriée des tâches d'administration et des enregistrements numériques, les entreprises accumulent les éléments inutiles qui compliquent les opérations simples de cyber-hygiène et de nettoyage, et laissent la porte ouverte aux abus des cybercriminels. Cette accumulation de zones inactives qui ne pointent vers aucun contenu est connue sous le nom de « dangling DNS » et présente un risque de détournement de sous-domaine. Ce détournement ouvre la voie à d'autres cyberattaques, telles que le phishing, les logiciels malveillants et les rançongiciels, qui pourraient nuire à la réputation de l'entreprise, entamer la confiance des consommateurs et entraîner des violations plus graves des données et de la sécurité. Les administrateurs qui ne connaissent pas forcément l'historique de chaque nom de domaine hésitent à supprimer ces enregistrements anciens, de peur qu'ils ne soient liés à l'infrastructure critique, ce qui pourrait, par inadvertance, entraîner une interruption des services.

Recenser tous leurs actifs numériques et différencier ceux qui sont critiques, fonctionnels ou redondants (et donc inutiles) est un véritable défi pour les entreprises. Le nettoyage des enregistrements DNS est l'une des tâches les plus négligées par les entreprises, du fait de l'accumulation, depuis plus de 20 ans, des titulaires, des politiques et des fournisseurs autour du DNS, et bien sûr, de la crainte inhérente des administrateurs de supprimer quoi que ce soit pour lequel ils ne sont pas 100 % certains.

En outre, le détournement de sous-domaine n'est que l'une des nombreuses menaces pesant aujourd'hui sur la sécurité des noms de domaine, parmi lesquelles on retrouve le détournement de nom de domaine et de DNS, la technique du domain-shadowing et l'empoisonnement du cache. Ces menaces servent souvent de véhicule à des attaques de phishing et par rançongiciels plus sévères, ainsi qu'aux attaques BEC (Business Email Compromise), au spoofing par e-mail, voire à des violations de données.

Nous recommandons, à toutes les entreprises, d'adopter une solution de surveillance des sous-domaines qui, non seulement, vous alerte en cas de modification de vos enregistrements DNS, mais qui vous fournit également les données nécessaires pour que vous puissiez prendre les décisions et les mesures qui s'imposent afin d'empêcher un détournement de sous-domaine.

En savoir plus sur la solution de surveillance des sous-domaines de CSC.

CSC est le partenaire de confiance des entreprises du Forbes Global 2000 et des 100 Best Global Brands® en matière de gestion des noms de domaine, de services DNS et de certificats numériques, et propose des solutions de protection des marques en ligne contre la fraude. Alors que les entreprises du monde entier investissent massivement dans leur stratégie de sécurité, CSC peut les aider à identifier leurs failles de cyber-sécurité et à sécuriser leurs actifs numériques et leurs marques en ligne. En s'appuyant sur la technologie propriétaire de CSC, les entreprises peuvent consolider leur stratégie de sécurité pour se protéger contre les vecteurs de cybermenaces qui pèsent sur leur patrimoine numérique, et éviter les pertes de revenus, les atteintes à la réputation de leur marque ou les pénalités financières pouvant résulter d'une non-conformité aux réglementations de type Règlement général sur la protection des données (RGPD). Nous fournissons également des services de protection des marques en ligne, qui combinent la surveillance de marque et des actions ciblées. Nous proposons une approche holistique de la cyber-sécurité et des services de protection contre la fraude pour contrer les tentatives de phishing. Basée à Wilmington (Delaware) aux États-Unis depuis 1899, CSC possède des bureaux sur tout le territoire des États-Unis, mais également au Canada, en Europe et dans la région Asie-Pacifique. CSC est une entreprise d'envergure mondiale, ce qui nous permet d'intervenir là où sont nos clients en mettant à leur disposition nos équipes d'experts dans chacune de nos activités. Consultez notre site à l'adresse suivante : cscdbs.com/fr.

DBS04052023