# Les cybercriminels utilisent aussi les Sous-domaines abandonnés


## Les cybercriminels utilisent aussi les Sous-domaines abandonnés

**Si la plupart des hackeurs tentent de contourner les mesures de sécurité mises en place sur les serveurs d'une entreprise, il est parfois plus simple de scruter l'architecture d'un site au global et les sous-domaines, notamment.**

Spécialisée dans la sécurité, la société Detectify, propose un outil de scan en mode SaaS et annonce avoir mené une enquête concernant la vulnérabilité des sous-domaines. Ces derniers seraient largement laissés à l'abandon et constitueraient un vecteur d'attaques.
Un prestataire de services proposant de créer des comptes utilisateur en leur attribuant un sous-domaine peut lui-même créer son propre sous-domaine pour lancer un service ou une campagne promotionnelle pendant quelques semaines, voire quelques années. Par la suite, à la fin de cette campagne ou à la fermeture du service en question, Detectify explique que le prestataire n'efface pas systématiquement la redirection du sous-domaine pointant vers le service ou la campagne. Or, un internaute peut donc se créer un compte chez ce prestataire de service puis obtenir ce même sous-domaine et orchestrer une attaque de phishing, par exemple.
Cette manipulation est possible lorsque la société en question ne procède pas à la validation du détenteur de chaque sous-domaine. Et il en existerait un certain nombre parmi lesquels nous retrouvons Heroku, Github, Bitbucket, Squarespace, Shopify, Desk, Teamwork, Unbounce, Helpjuice, HelpScout, Pingdom, Tictail, Campaign Monitor, CargoCollective, StatusPage.io ou encore Tumblr.
« Nous avons également identifié 200 organisations qui s'en trouvent affectées. Dans beaucoup de cas, nous parlons de société listées au NASDAQ ou figurant dans le top 100 d'Alexa », ajoute Detectify.
Pour vérifier si une personne est bien le propriétaire d'un domaine ou d'un sous-domaine, quelques sociétés, comme Google demandent de transférer un ficher HTML via FTP ou d'ajouter une CNAME particulière dans le panneau de contrôle du nom de domaine.

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html?&xtc_mode=M&xtc_campaign=NL_ClubicPro_New_25/10/2014&partner=-&xtc_position=717264607&xtc_misc=-&crmID=639453874_717264607&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html