Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 02 mai 2016
N° CERTFR-2016-ACT-018

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-018

1 - Etude sur les limites des adresses raccourcies

Une étude publiée par deux chercheurs américains met en évidence un défaut jusqu'alors ignoré dans le mécanisme de génération des adresses raccourcies ou *TinyURL*.

Ces adresses permettent de réduire de manière conséquente la taille d'une adresse WEB et de faciliter ainsi sa transmission sur des supports pour lequel les ressources sont réduites, le service Twitter en est un excellent exemple.

Cette réduction est assurée par un service tiers qui associera à l'adresse WEB une clef unique générée selon différents mécanismes qui, tous, visent à fournir une clef de taille très réduite. Le service sera ainsi à même de retourner l'adresse originale lors de la présentation de l'adresse raccourcie.

L'adresse de la page CERT-FR référençant l'avis de sécurité 143 publié en 2016 (http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-143/index.html) pourrait être réduite en l'adresse http://bit.ly/1SJqwst par le service bitly.

Citons parmi les services les connus: *t.co* opéré par la société Twitter (anciennement bit.ly), *goo.gl* opéré par la société Google ou encore *1drv.ms* de la société Microsoft.

L'objectif du fournisseur de service est bien évidemment de minimiser les collisions - la réduction d'au moins deux adresses WEB génère la même clef - tout en réduisant au maximum la taille de l'URL raccourcie. Un compromis est assez aisé à atteindre en s'appuyant sur les 26 lettres et 10 chiffres disponibles, voire en imposant une durée de vie à l'adresse raccourcie. L'encodage utilisé par le service *bitly* permet ainsi de disposer de plus de 58 milliards de combinaisons pour une longueur de clef de 6 caractères.

Ce mécanisme de réduction peut aussi profiter à l'internaute curieux qui pourrait avoir l'idée de parcourir tout ou partie de cet espace de noms à la recherche de pages ou de documents qui pourraient ne pas être autrement accessibles, car non indexés ou encore stockés dans un Cloud par exemple.

Dans leur rapport de recherche, Martin Georgiev et Vitaly Shmatikov montrent que l'espace de nommage offert par certains services de réduction d'adresses peut-être facilement échantillonné à la recherche de documents intéressants. Il pourrait même être intégralement parcouru en temps raisonnable - 3 années tout de même - en utilisant les interfaces de requêtes proposées par la plupart de ces services et la puissance de calcul offerte par les plate-formes réparties mais aussi par un botnet.

Les chercheurs se sont plus particulièrement intéressés au service de stockage dans le Cloud *OneDrive* géré par Microsoft et à l'utilisation d'adresses raccourcies pour partager l'accès aux répertoires et fichiers stockés via ce service. L'analyse de quelques 42 millions d'adresses raccourcies sur 6 caractères par le service *bitly* leur a permis d'identifier plus de 3000 adresses référençant un répertoire ou un fichier dans le domaine *onedrive.live.com* et plus de 16000 adresses liées au domaine *skydrive.live.com*. Ce sont ainsi, et en moyenne, 43 documents stockés dans l'un ou l'autre de ces domaines qui ont été découverts quotidiennement lors du test. Les chercheurs estiment qu'un botnet pourrait énumérer tous documents ainsi référencés et stockés sous ces domaines en moins d'une journée.

La transmission anticipée de ces résultats aux sociétés Microsoft et Google a conduit ces dernières à mettre en place des mécanismes rendant impossible un parcours exhaustif en temps raisonnable. On retiendra de cette

étude que l'utilisation de services de réduction d'adresses devra être proscrite pour toute adresse référençant une ressource privée ou non indexable par les moteurs de recherche - page, document, répertoire partagé dans le cloud - quand bien même ces adresses facilitent le partage et l'échange d'information dans une communauté d'usagers.

Rappelons par ailleurs que ces adresses raccourcies peuvent être utilisées à des fins de dissimulation de l'adresse WEB vers laquelle l'usager sera réellement dirigé. La généralisation de ces adresses raccourcies a hélas pour effet de rendre les usagers moins méfiants.

Documentation

- Gone in Six Characters: Short URLs Considered Harmful for Cloud Services :
  http://arxiv.org/pdf/1604.02734v1.pdf
- Réduction d'URL :
  https://fr.wikipedia.org/wiki/R%C3%A9duction_d'URL

2 - Rappel des avis émis

Dans la période du 25 avril au 01 mai 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-143 : Multiples vulnérabilités dans Wireshark
- CERTFR-2016-AVI-144 : Multiples vulnérabilités dans Juniper Junos Space
- CERTFR-2016-AVI-145 : Multiples vulnérabilités dans Veritas NetBackup
- CERTFR-2016-AVI-146 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-147 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2016-AVI-148 : Multiples vulnérabilités dans les produits Juniper

Gestion détaillée du document

02 mai 2016 version initiale.