URL courte : mini taille mais maxi risques de sécurité

Ils sont utilisés quotidiennement par millions, les hyperliens courts font maintenant partie du paysage du web. Mais ils ne sont pas exempts de soucis de sécurité. Martin Georgiev et Vitaly Shmatikov, chercheur à l'Université Cornell Tech, ont découvert que les URL raccourcies sont élaborés sur une syntaxe prévisible qui peut être recherchée et identifiée pour tenter un vol de données personnelles. Les liens courts sont une combinaison de noms de domaine et un mélange de jeton de 5 à 7 caractères. Une faiblesse congénitale selon les deux experts.

Dans leurs travaux (« Gone in Six Characters: Short URLs Considered Harmful for Cloud Services »), les universitaires ont étudié les réducteurs d'URL, notamment Google (avec le nom de domaine Goo.gl), le service Bit.ly et Microsoft OneDrive (1drv.ms) et Bing Maps (Binged.it). Ils se sont aperçus que des attaquants pouvaient accéder à des documents personnels ou pousser des malwares en générant facilement des adresses pré-existantes. Et que des cybercriminels motivés pouvaient trouver l'ensemble des liens courts émis par les éditeurs. A noter que deux services, Google Maps avec le domaine Goo.gl et Microsoft OneDrive qui comprend aussi un réducteur de lien intégré, ont poussé des correctifs pour sécuriser les liens courts. Cependant les anciens liens restent vulnérables.

La force brute pour révéler des informations personnelles

Concrètement les universitaires ont utilisé la technique de la force brute pour parvenir à leurs fins. « *Les URL courtes créées par bit.ly, goo.gl et autres services similaires peuvent être balayées par force brute*, explique Vitaly Shmatikov, *notre analyse a mis à jour un grand nombre de comptes OneDrive avec des documents personnels. Or beaucoup de ces comptes ne sont pas verrouillés et s'exposent à l'injection de malwares qui seront ensuite téléchargés sur le terminal de l'utilisateur.* » Pour OneDrive, ils ont mené un scan sur 100 millions de liens courts et ont eu accès à 1,1 million de données. Pour Google Maps, les chiffres sont aussi étonnants. Les chercheurs ont examiné près de 24 millions de liens dont 10% contenaient des itinéraires « sensibles », comme des établissements de santé (toxicomanie, avortement, cancer, etc.), des prisons ou des clubs de strip-tease.

Au final les universitaires veulent alerter les utilisateurs sur les risques encourus avec ces outils de réducteur de lien. *« Les entreprises et les personnes pensent qu'il s'agit simplement de partager un document avec un collaborateur, mais si vous partagez un lien court avec 6 caractères, vous le partagez avec le monde entier »*, conclut Vitaly Shmatikov.

A lire aussi :

Amazon Web Services renforce la sécurité de ses services Cloud

Google Chrome plus strict avec la sécurité des pages web