CookieMonster, l'outil qui croque les HTTPS

Les sites Web protégés le sont-ils vraiment ? **CookieMonster** apporte un début de réponse. Son créateur, **Mike Perry**, explique l'utilité de son outil qui démontre la possibilité de rassembler des données pas suffisamment sécurisées sur le fichier cookies du navigateur (Firefox par exemple).

Par principe, les **données HTTPS (issues des sites sécurisés comme les banques) sont censées être sécurisées** et garantir, la sécurité d'un paiement ou un enregistrement en ligne (voire la consultation de compte bancaire).

Pourtant certains sites qui exploitent ce type de données n'ont pas, à proprement parler, de sécurité du type « *Encrypted Sessions Only* » garantissant une bonne **protection des 'cookies'**. Des pirates peuvant alors tenter de se procurer les mots de passe et autres codes secrets par ce biais.

Mike Perry propose néanmoins un test simple pour savoir si les sites que vous utilisez sont vulnérables : « *Allez dans l'**onglet vie privée** et cliquez sur '*Afficher les cookies*'. Pour un site donné, inspectez le cookie du nom du site et de chaque sous-domaine. Si vous voyez le message « Send For: Encrypted connections only" vous devez l'effacer. Retournez ensuite sur le site, si vous y parvenez, cela voudra dire que le site n'est pas sécurisé***« .**

Le spécialiste affirme que son outil a démontré la vulnérabilité à ce genre d'attaques de sites très populaires comme United, Expedia, US Airways, Bank of America, Discover Card, les Apple Store en ligne, eBay, Google Search et Blogger.

Sur son blog, le créateur explique plus en détail qu'il compte laisser sa **création à disposition d'un cercle limité** de chercheurs en sécurité ainsi qu'à un public restreint.