IE 8 trop peu protégé contre le clickjacking

Microsoft vient de fournir de plus amples informations sur le fonctionnement de son **outil anti-*clickjacking*** contenu dans **Internet Explorer 8**.

Cette méthode de piratage consiste à**utiliser les propriétés HTML d'une page Web afin de manipuler son affichage**. Principalement utilisé pour gonfler le trafic d'un site (souvent publicitaire) il a pour conséquence de faire effectuer au visiteur des actions différentes de celles qu'il visualise lorsqu'il clique sur un lien.

Responsable de la programmation chez le géant de Redmond, Eric Lawrence a donc fourni des informations techniques sur le blog IE officiel traitant de la version d'IE8 actuellement en version Release Candidate (IE8 RC1). Selon lui, la **protection mise en place empêche de se faire piéger.**

Insuffisant rétorque notamment Robert Hansen, p-dg de SecTheory LLC, société spécialisée dans le conseil en sécurité : « *la technique utilisée pour IE8 n'est* ***pas exactement la meilleure pour protéger les utilisateurs***« . Pour illustrer son propos, il explique que l'**outil HTTPOnly** de Microsoft n'est utile que pour empêcher les codes malveillants d'infiltrer les cookies.

Par ailleurs, cet outil nécessite l'insertion par les webmasters de balises spéciales dans le code leurs pages. A eux donc de prendre les choses en main afin de contourner la faille présente dans les navigateurs Web. *« Cette solution prendra des années »*, ajoute Hansen. Surtout, les internautes utilisant IE8 penseront être protégés alors qu'il n'en sera rien si le code du site visité n'a pas été modifié.

Pour rappel, la version test du navigateur Internet Explorer 8 est disponible depuis le début de la semaine. Avec ce nouvel opus, Microsoft a mis l'accent sur les fonctionnalités : *web slices*, navigation en mode privé, accélérateur…

Côté sécurité, la compagnie a choisi de mettre l'accent sur les attaques par injection de code malicieux (*cross site scripting*) à la source. Un bon point sachant que la **majorité des failles découvertes dans les navigateurs web exploitent cette technique de diffusion**.

A lire : notre test de la bêta RC1 de IE8