Un 'trojan' exploite les liens sponsorisés de Google

Les problèmes de sécurité dans les produits Google s'accumulent depuis quelques jours. Après la toolbar piégée, c'est au tour des liens sponsorisés d'afficher une menace. Pour l'instant, le niveau de propagation de ce maudit canasson nommé Qhost.WU est jugé faible par l'éditeur, le risque qu'il représente est, lui, qualifié de « moyen ». Sa première détection par Balazs remonte au 17 décembre 2007. L'objectif de ce cheval de Troie: pirater les liens sponsorisés de Google pour les remplacer par d'autres provenant de divers autres sources.

Plusieurs symptômes permettent aux webmasters de détecter la présence de ce '*trojan*'. D'abord, l'espace qui contient les liens sponsorisés Google peut s'arrêter de diffuser des messages publicitaires, ensuite les publicités qui s'affichent sur l'URL proviennent d'autres sources que Google.

Les fichiers hébergés utilisés pour associer un nom de domaine et un lieu de stockage des fichiers contiennent la ligne suivante: « page2.googlesyndication.com ».

Rappelons que Google Adsense est un service de la firme de Moutain View qui permet de placer des liens sponsorisés sur des pages Web. Ces annonces sont ciblées, c'est à dire qu'elles doivent normalement être en adéquation avec le thème général du site.

Cela reste bien sûr du domaine théorique, car dans les faits, les publicités n'ont souvent rien à voir avec le sujet du site. Il suffit de se balader sur la Toile pour s'en rendre compte.

Les revenus générés par chaque clic sont partagés entre Google et le groupe propriétaire de la page Web.

Ces publicités sont placées sur le site Web par le biais d'un petit morceau de code HTML/JavaScript (ndlr: un code propriété de Google).

Ce code a ensuite pour mission de se mettre en relation avec les serveurs Adsense du géant de la recherche qui délivrent alors des liens sponsorisés et « contextuels ».

Le code malveillant découvert par Bit Defender utilise les documents hébergés dans le dossier « %WINDIR%System32driversetc » pour rediriger la requête authentique vers **un attaquant** qui peut alors placer ce qu'il veut dans les liens.

Ce problème est nuisible tant pour Google que pour les sites Web. Google ne récupère plus d'argent et les webmasters également.

Comment vérifier si l'on est concerné par ce 'trojan'?

L'éditeur indique en marge de sa publication une méthode afin de détecter comment les webmasters peuvent vérifier qu'ils ne sont pas infectés.

À partir de la ligne de commandes «exécuter», envoyer la requête suivante: ping -t

pagead2.googlesyndication.com

La réponse normale doit être la suivante : envoi d’une requête ping sur pagead2… avec 32 octets de données. Ce lien doit pointer normalement vers une adresse IP de la forme [6x.xxx.xxx.xxx], x, représente une suite de chiffres, par contre si le cheval de Troie est déjà à l’œuvre le premier chiffre sera un 9.