



Article de Frédéric Guérin, CISA
Conseiller principal en sécurité
ESI Technologies

Détournements de navigateur : comment les prévenir

Les détournements de navigateur - browser hijacking en anglais - sont provoqués par des programmes malicieux qui, depuis le Web, s'introduisent dans les ordinateurs par l'entremise du navigateur.

Bien que les dommages potentiels de ce type d'attaque peuvent être très élevés, le plus souvent ce sont les paramètres du navigateur qui sont changés. Par exemple, la page de démarrage et les pages de recherche sont modifiées. Certains de ces programmes affichent aussi des fenêtres en incrustation (pop up), ajoutent des sites à la liste des favoris ou redirigent l'utilisateur vers un site particulier lorsqu'il entre une adresse incorrectement. L'objectif premier des auteurs de ces méfaits est de gonfler artificiellement les statistiques de fréquentation de leurs sites afin de faire monter les enchères publicitaires.

Un détournement de navigateur peut s'avérer extrêmement nuisible et il est souvent difficile de s'en débarrasser. Non seulement affecte-il la productivité des utilisateurs, mais il peut même leur causer un tort particulièrement injuste. Par exemple, en accédant contre leur gré à des sites indésirables – très souvent pornographiques – ces programmes malicieux placent potentiellement leurs victimes dans la délicate situation d'avoir à justifier, aux yeux de leur employeur (ou de toute autre personne), la consultation de pareil matériel. Or, il est difficile de dire, à partir des traces laissées sur le disque dur d'un ordinateur, si les sites consultés l'ont été avec ou sans le consentement de l'utilisateur.

Il existe heureusement des moyens de se prémunir contre cette peste. Le premier d'entre eux est d'installer la toute dernière version de son navigateur, de même que l'ensemble des rustines qui y sont associées. Le système d'exploitation doit également être mis à jour sur une base régulière. À cet effet, Microsoft met à la disposition de ses clients un site (<http://windowsupdate.microsoft.com>) permettant de télécharger toutes les mises à niveau diffusées par la multinationale.

D'ailleurs, les systèmes d'exploitation et les navigateurs choisis par une très vaste majorité d'utilisateurs à l'échelle de la planète étant des produits de Microsoft - Windows et Internet Explorer (IE) - les pirates du Web exploitent les failles de ces programmes en tout premier lieu. Par conséquent, on peut réduire le risque auquel on s'expose en se servant d'un autre navigateur. D'autant plus que la sécurité de produits concurrents comme Mozilla, Firefox et Opera est plus étanche.

Comme il est très difficile, voire impossible, de remplacer complètement IE, il faut envisager d'autres mesures également. Dans un premier temps, on peut substituer la machine virtuelle Java de Sun à celle de Microsoft (téléchargement à partir de <http://www.java.com>), car de nombreux pirates profitent de failles présentes dans cette dernière.

Autre consigne à suivre, les paramètres de sécurité des options Internet, auxquelles on a accès par le Panneau de configuration de Windows, doivent être correctement configurées.

Précaution supplémentaire, certains logiciels peuvent sécuriser davantage IE, en neutralisant un très grand nombre de sites indésirables ou certains programmes ActiveX, ou encore en exerçant une surveillance des changements qui surviennent aux pages d'accueil et de recherche choisies par l'utilisateur. IE-SPYADS, SpywareBlaster et Browser Hijack Blaster sont des exemples de tels programmes.

Pareillement, il est préférable de désactiver le volet de visualisation (preview pane) des applications Outlook et Outlook Express, afin d'empêcher le visionnement d'un site Web à partir d'un courriel provenant d'un pirate.

Assurez-vous aussi que votre antivirus est à jour et en mesure de détecter la présence de code malicieux à l'intérieur de pages Web, afin de prévenir les attaques.

En dernier lieu, les entreprises peuvent également choisir d'installer un serveur mandataire (proxy) comprenant des fonctions qui permettent de détecter les détournements de navigateur, comme c'est le cas avec Aladdin eSafe et McAfee WebShield.