Injecteurs de publicités : Google fait le point sur le fléau n°1 du web

Début avril, Google prenait des mesures afin de protéger son butineur Chrome des **injecteurs de publicités**, des outils insérant des annonces (supplémentaires) au sein des pages web visitées par les internautes. Voir à ce propos notre article « Google vaccine Chrome contre l'injection d'adwares ».

Nous apprenions à cette occasion que 5 % des personnes visitant les sites de Google étaient infectées par un injecteur de publicités. La firme de Mountain View a mené plus précisément l'enquête et dévoile aujourd'hui que ce taux est de 5,5 %. **Soit 1 PC sur 18.**

Tout commence par l'installation d'un logiciel infecté, intégrant l'injecteur de publicités. Plus de **50 000 extensions** pour navigateurs web et plus de **34 000 applications** ont été recensées par Google. La firme précise que 30 % de ces logiciels en profitent pour voler des données d'identification, modifier les résultats de recherche et transmettre des données de navigation à des tiers.

Du marketing mafieux…

Mais qui distribuent ces outils ? Plus de **1000 sociétés**, explique Google. Le vecteur de choix de diffusion des injecteurs de publicités reste une installation en parallèle à celle d'un logiciel légitime. Ces outils marketing indésirables sont ainsi souvent insérés en direct dans les systèmes d'installation de certains portails de logiciels. Un des tristes exemples de cette pratique est **Sourceforge**, plate-forme d'hébergement de logiciels Open Source, qui intègre maintenant de multiples malwares dans les installeurs des applications qu'elle diffuse.

Au besoin, des campagnes marketing, en particulier sur les réseaux sociaux, permettent de faire la promotion de ces installeurs piégés.

… des intermédiaires peu scrupuleux…

Les diffuseurs d'applications piégées emploient des librairies clés en main permettant d'assurer l'injection de publicités au sein des navigateurs web. Environ 25 offres sont disponibles, dont les plus utilisées sont celles de **Superfish** (3,9 % des navigateurs infectés) et de **Jollywallet** (2,4 %). Ce sont ces sociétés qui décident quelles publicités seront diffusées, de façon parfois illégitime, et qui vont exploiter (traduction ; revendre) les données de navigation collectées et d'autres informations personnelles.

Superfish a récemment été mis en lumière, car intégré par **Lenovo** dans ses ordinateurs portables grand public.

… et des annonceurs lésés

Bien évidemment, pour chaque clic, les diffuseurs d'applications piégées touchent un pourcentage sur l'argent généré. Trois réseaux publicitaires sont utilisés par 77 % des injecteurs de publicités : **dealtime.com, pricegrabber.com et bizrate.com**. Et ceux-ci ne sont guère plus exemplaires que les autres maillons de la chaîne. Google explique ainsi que les publicités sont souvent détournées de leur usage d'origine (être présentes au sein de sites web) pour être insérées dans les cadres des injecteurs, sans que les annonceurs en soient avertis.

Plus de 3000 annonceurs seraient victimes de cette pratique, dont de grands acteurs, comme **eBay**.

À lire aussi :
Sécurité : 12 autres logiciels sur la trace de Superfish
Adware Superfish : Lenovo veut devenir exemplaire
Le phishing a explosé en France en 2014