Lycos.fr infecte-t-il ses visiteurs? Entre ouï-dire et preuves

Des spywares profiteraient de l'incrédulité de certains internautes pour s'installer sur nos machines et espionner dans la plus grande discrétion nos données confidentielles tant convoitées par les spécialistes du marketing. Coup de projecteur sur ce qui s'annonce comme un scandale retentissant.

Suite à une visite sur le site *https://mulitmania.lycos.fr*, un internaute du nom de Sylla1337 a signalé au site *Zataz.com* qu'il avait tout à coup constaté qu'un programme, intitulé bla.exe, a tenté de se connecter à Internet. En menant une enquête plus approfondie, notre Sherlock en herbe, intrigué par le phénomène s'est livré à des petites expériences qui ont donné des résultats pour le moins surprenants. Lors d'une visite du site Lycos.fr, un PC sécurisé par le programme Bitdefenders pro 8 a signalé une tentative d'intrusion par un cheval de Troie : « BehavesLike :Trojan.Downloader ». Elémentaire mon cher… D'autres antivirus comme Norton ne signalent pas la présence du dit trojan. Conséquence il s'installe ni vu ni connu sur le disque système. Selon Sylla1337 : *« le téléchargement se fait à partir du script installé en bas de page de Lycos »*. Plus étonnant, dans le code source de ce script (V5.js) apparaît la signature d'un des partenaires de Lycos la société australienne RedSheriff l'un des principaux fournisseurs de données sur le recensement des visites sur les sites Web. Une étrange collusion. Alors, la conclusion la plus directe que l'on tire de ce piratage avéré est que RedSheriff utilise des méthodes illégales pour collecter des informations sur les visiteurs. D'autant que c'est l'ensemble des sites de Lycos en Europe qui est concerné. Et les soupçons se portent sur RedSheriff car le JavaScript (V5.js) est exécuté via un serveur (https://secure-uk.worlwide.com) de la firme californienne ce qui fait que ce code malicieux est appelé sur tous les serveurs Lycos dans le monde. Une fois le sympathique fichier exécuté, un second programme se lance : w.exe. Toujours selon le webzine *Zataz* qui a procédé à une manipulation pour remonter l'IP dévoilé dans la ligne terminale du code source de la page. L'IP du serveur incriminé qui permet la propagation des trojans est celui d'un site en construction de l'agence de publicité de DDB Worldwide. Tiens donc! Contacté par téléphone, le directeur technique de Lycos, Cédric Leroy, a confirmé l'information :*« Il semblerait qu'il y ait eu des modifications dans le script de la page Lycos sur une machine de RedSheriff, ce qui explique la présence de ce trojan. Pour le moment le problème est résolu, mais Lycos attend des explications de la part de RedSheriff dont la responsabilité est d'ores et déjà engagée. »* La présence de ce fichier espion n'est donc pas le fait d'une manipulation orchestrée par Lycos qui rejette fermement sur RedSheriff ces pratiques abusives. Ces nouvelles, démontrent bien que le v5.js a permis la diffusion massive de spyware sur l'ensemble des PC mal sécurisés qui ont utilisé des sites Lycos sur la planète. Un constat qui explique le chiffre exorbitant lancé par Symantec selon lequel 76% des ordinateurs de la planète sont infectés par un fichier-espion. Alors Lycos va chercher, d'accord? mais des spywares non merci! Une affaire à suivre?