

# McAfee automatise le 'Google Hacking'

Le détournement des fonctionnalités de recherche de Google peut permettre de récupérer des documents Word, des numéros de carte de crédits, des liens vers des Webcams personnelles ou des même des vulnérabilités sur des applicatifs en ligne pourvu que la requête soit correctement formulée. Récemment Google a même été utilisée dans le mécanisme de propagation d'un Worm. McAfee, au travers de l'acquisition de Foundstone, a récupéré la solution SiteDigger et lance la deuxième version du produit au travers d'une application Win32 gratuite. Son ambition est d'aider les administrateurs à découvrir des erreurs de configuration ou des informations sensibles qui pourraient être diffusées largement au travers du portail Web. La technologie repose sur Microsoft .Net et exploite l'API de Google dans le cadre de la recherche d'informations. L'outil permet ainsi de récupérer de multiples informations au travers d'une dizaine de catégories que sont les fichiers de backup, les consoles d'administration distantes, les fichiers de configurations, les messages d'erreurs, les données confidentielles, les vulnérabilités ou encore les profils d'application. Selon le responsable des services de Foundstone, la proposition de valeur de la solution repose sur un constat simple : « l'erreur est humaine ». La solution est disponible gratuitement au travers de ce

[lien](#). Elle nécessite cependant Microsoft .Net (qui peut être installé au travers de Microsoft Windows Update) ainsi qu'une licence valide pour l'utilisation de l'API Google. (\*) **pour Vulnerabilite.com**