Windows 7 et IE9 vulnérables au DLL hijacking

Windows, toutes versions desktop confondues de XP à 7, ainsi que le tout récent Internet Explorer 9 restent hautement faillibles aux attaques externes. C'est ce que compte démontrer **Mitja Kolsek**, directeur technique de ACROS Security, à l'occasion de la conférence Hack in the box (HitBSecConf, du 17 au 20 mai à Amsterdam). Le chercheur en sécurité devrait montrer comment il est possible de prendre le contrôle d'un système, localement ou à distance, **en remplaçant quelques fichiers DLL**, une attaque connue depuis une décennie sous les noms de 'DLL hijacking', 'DLL preloading' ou 'Untrusted library loading', voire 'binary planting' par Acros.

Le principe est simple : remplacer un fichier DLL (bibliothèque de liaisons dynamiques ou de routines) légitime par un fichier vérolé du même nom qui permettra au pirate d'exécuter du code malicieux par l'intermédiaire du logiciel qui l'exploitera. L'une des caractéristiques du fonctionnement de Windows est en effet qu'il exploite les DLL du répertoire de travail courant. Ce qui permet notamment d'**exploiter des DLL infectieuses en ligne sur Internet**. Mitja Kolsek entend démontrer la faisabilité de l'exploitation de la faille à travers des documents Office Word 2010 et PowerPoint 2010 ainsi que depuis IE9.

Bien que bénéficiant d'un système de bac à sable censé isoler les actions effectuées dans le navigateur du reste du système, le chercheur en sécurité démontrera également que **IE9 sous Windows 7 (ou Vista) est aussi faillible que IE8 sous Windows XP** dépourvu, lui, de ce mécanisme de sécurisation. *« Nous montrerons comment cette technique peut être exploitée pour lancer une attaque de type 'binary planting' contre Internet Explorers 8 sur Windows XP ainsi que contre Internet Explorer 9 en mode protégé sur Windows 7 – sans passer par un double-clic suspect ou des avertissements de sécurité »*, annonce Mitja Kolsek sur son blog.

Le problème du 'DLL hijacking' est connu depuis une décennie et **Microsoft déclare avoir corrigé les 13 failles DLL** trouvées depuis novembre 2009 à aujourd'hui. Mais selon Acros, il en existe bien d'autres. Sur sa page de présentation de la conférence, les chercheur en sécurité recensent plus de **520 vulnérabilités** exploitables à distance à travers 200 applications propres au DLL hijacking'. De plus, l'alerte de sécurité sur la question ouverte par Microsoft en août 2010 reste active, sa dernière mise à jour remontant au 12 avril 2011.

Il n'en reste pas moins que ce type d'attaque est **rarement exploité**. Pour la simple raison qu'il est difficile d'amener la victime à se rendre dans un dossier dédié et activer un fichier DLL infectieux, que ce soit par Internet, e-mail ou depuis une clé USB vérolée. Une chance pour les clients de Microsoft. L'éditeur a annoncé qu'il se pencherait néanmoins sur la question. Laquelle risque d'être des plus brûlante après le 19 mai, date de la démonstration de l'exploit au Hack in the box par Mitja Kolsek. Ou pas.