Le greffon Flash d'Adobe au cœur d'une attaque d'envergure

Une attaque sans précédent est en cours sur Internet. Les pirates combinent ici plusieurs fonctionnalités avancées du web et du greffon Adobe Flash pour **voler les informations de connexion** des utilisateurs. Cette attaque permet de récupérer des données sensibles depuis un site web piégé : clés de session d'une précédente connexion, cookies fixés par un site tiers, etc.

Il ne s'agit pas à proprement parler d'une faille du greffon Flash, mais de l'utilisation d'une combinaison de fonctionnalités proposées par Flash, par les navigateurs web modernes et par les sites web de dernière génération.

Exfiltration de données via JSONP

Le principe est relativement simple. Il met en œuvre **une requête JSONP**, laquelle permet à un site de demander des données à un autre. Un outil, Rosetta Flash, permet de convertir un module Flash en texte. Ce texte est inséré dans la requête JSONP, où il sera vu comme des données, mais exécuté comme un module Flash par le navigateur.

À partir de là, tout s'enchaîne. Le site web pirate effectue une requête sur un site légitime. Les données de la requête comprennent en fait le composant Flash piégé, lequel s'exécute. Ce dernier peut alors lire des données sensibles sur le site légitime visé, par exemple des informations liées à une connexion en cours (qui peuvent être celles relatives à une page web que vous venez de quitter).

Ces données sont renvoyées au site d'origine par le composant Flash. Ce dernier peut ainsi **exfiltrer des données d'un site 'normal' vers un site 'pirate'**. Un système qui s'active tout simplement en visitant le site du pirate.

Des sites majeurs sont concernés

Tous les sites utilisant le JSONP peuvent être visés par cette attaque. Et ils sont nombreux. Les services de Google (y compris YouTube) ont été modifiés pour filtrer ces requêtes JSONP piégées. Idem chez Twitter et Tumblr. De nombreux autres sites d'envergure restent toutefois sensibles à cette faille, dont Instagram et eBay.

Adobe a également réagi, en proposant **la version 14.0.0.145 du greffon Flash** (11.2.202.394 sous Linux et 13.0.0.231 sur certains anciens OS), laquelle intègre des systèmes de protection détectant et interdisant un tel usage de Flash. Les utilisateurs du navigateur web Google Chrome disposeront automatiquement de cette mise à jour. Il en va de même pour ceux qui emploient Internet Explorer 10 ou 11 sous Windows 8 et Windows 8.1 (mais également sous Windows Server 2012 et Windows Server 2012 R2).

Pour les autres, il conviendra de mettre à jour le greffon Flash manuellement, et rapidement. Pas

question donc d'attendre que l'outil de mise à jour d'Adobe se décide à réagir. Le mieux est de vérifier sur cette page web si vous disposez de la dernière version du greffon. Si ce n'est pas le cas, un tour sur cette autre page permettra de la télécharger, puis de l'installer.

Notez que cette nouvelle mouture de Flash corrige trois vulnérabilités, dont certaines permettent à un attaquant de prendre le contrôle d'une machine à distance, indique Adobe. Mise à jour obligatoire donc.

Sur le même thème

Une campagne de piratage touche les utilisateurs d'AOL mail
Orange tente de minimiser l'impact du piratage des données de ses abonnés
La NSA aurait mené de nombreuses opérations de piratage