Firefox, Arsène Lupin des mots de passe?

Les chercheurs de l'éditeur de sécurité **BitDefender** ont découvert une nouvelle manière de **dérober des mots de passe.** A l'origine, se trouve une application de détournement de mot de passe, masquée en '*plug in*' pour **Firefox**. **Elle filtre les informations de connexion des utilisateurs.**

La menace porte la marque d'un cheval de Troie, baptisé **Trojan.PWS.ChromeInject.A**.

BitDefender rend ainsi compte de la nature de la menace : « *Chargé sur un ordinateur par l'intermédiaire d'un autre malware, le '*trojan*' se place dans un* ***dossier de 'plug in' du navigateur Mozilla Firefox***« .

La suite est alors presque aussi simple qu'un cambriolage digne d'un cambrioleur masqué puisque le **code malveillant s'exécute à chaque fois que Firefox est lancé**. Il s'agit donc d'une faille qui, sans mesure appropriée, peut tout à fait s'insinuer dans un poste et y rester fermement ancré, volant ainsi vos informations personnelles.

Selon des recherches approfondies des mêmes spécialistes, il apparaît que ce malware est capable de **filtrer les données que l'utilisateur infecté envoie vers une centaine de sites bancaires**. Et non des moindres. Par exemple, *bankofamerica.com*, ou *chase.com*, ou encore *halifax-online.co.uk*, ou même *paypal.com* et *e-gold.com* – tous ces établissements bancaires sont potentiellement touchés par le 'malware'.

Dès lors, ces identifiants et mots de passe sont détournés vers une **adresse en .ru (nom de domaine russe)**. On découvre ensuite que le serveur hôte est aussi basé en Russie. Une piste qui se vérifie. Déjà, Fabien Lang, commissaire de police adjoint au chef de l' OCLCTIC, à la direction centrale de la police judiciaire, confiait à notre rédaction : « *Le 'carding',* ***le piratage et le trafic des données est une menace.*** *Ce phénomène reste très difficile à chiffrer, car très international. Il consiste tout d'abord à récupérer des données de cartes bancaires, principalement par le* ***piratage de bases de données*** *et par des attaques en direct auprès de particuliers, via des attaques de 'phishing 'ou à l'aide de* ***chevaux de Troie***« . Cet expert explique alors que ces données sont revendues sur Internet, sur des forums spécialisés, **souvent hébergés en Russie…**

En résumé, une attention toute particulière doit être adoptée en ces temps de **fêtes de fin d'année.** Les menaces sur les sites de paiement risquant d'être plus prégnantes dans les jours à venir. Prudence reste donc mère de sûreté.