RSA constate l'essor des failles de navigateur et des « Man in the browser »

A l'appui de son rapport de sécurité, RSA constate l'explosion des attaques de type « homme dans le navigateur Internet » (« Man-in-the-browser »). Cette catégorie d'attaques est principalement élaborée pour **intercepter et manipuler des données** lorsqu'elles transitent par des communications sécurisées entre un utilisateur et une application en ligne.

A la loupe, l'éditeur de sécurité explique le fonctionnement d'une telle infection : « *Un **Trojan infecte le navigateur Internet** qui peut être programmé pour se déclencher quand l'utilisateur accède à des sites spécifiques en ligne, comme son service bancaire.*» Il est alors facile pour un hacker de se procurer des données personnelles permettant ensuite de pirater simultanément le compte.

Un type d'attaque qui a donc pour objectif de transférer une somme d'argent de manière quasi invisible. De fait, **l'utilisateur ne va pas remarquer de mouvement anormal durant la transaction**. De même, la banque peut considérer la transaction comme légitime puisque c'est bien l'adresse IP de l'utilisateur qui sera enregistrée en tant qu'auteur du transfert.

L'éditeur RSA classifie ces attaques comme des trojan MITB et constate que le **nombre d'attaque a augmenté d'un facteur de 10 au cours des 12 derniers**

mois. Comme exemple, l'éditeur donne le cas de la page de fan de Paul McCartney sur Facebook : « *Le site a été hacké pendant 2 jours et tous les visiteurs du site ont été infectés par une forme dangereuse de malware financier*. »

Dès lors, RSA recommande de posséder une bonne connaissance des procédés utilisés et de pouvoir utiliser les parades en temps réel pour anticiper la fraude et sécuriser les données.