

### **G-Data : Les chevaux de Troie bancaires optent pour le Cloud**

Sécurité

Posté par : JerryG

Publié le : 12/9/2013 14:00:00

**Les experts du G Data SecurityLabs** ont découvert un nouveau fonctionnement dans les chevaux de Troie bancaires.

Alors que précédemment les URL des pages Internet bancaires ou des formulaires en ligne étaient contenus dans le code malveillant, ces adresses sont maintenant stockées sur des serveurs distants. Une évolution technologique qui rend l'analyse des cibles potentielles plus difficile.

**Certains chevaux de Troie sont spécialisés dans le vol** de données personnelles ou le détournement de virements bancaires. Pour réussir ces actions, ces programmes détectent les liens affichés dans le navigateur Internet de la victime et modifient les pages pour capter les informations saisies. Pour cela, ces codes utilisent traditionnellement des fichiers de configuration stockés sur l'ordinateur attaqué. Ces fichiers contiennent les adresses des sites Web compromis et le code, appelé WebInject, qu'ils cherchent à ajouter à ces sites via les chevaux de Troie bancaires.



Ce code est alors chargé de voler des données d'accès et des informations personnelles par exemple.

### **Le Cloud pour plus de réactivité et de furtivité**

Dans leurs nouvelles versions, différentes parties de la configuration des logiciels malveillants

sont désormais placés sur des serveurs distants. Grâce à cette procédure, leurs auteurs rendent les programmes plus flexibles et plus hermétiques aux analyses.

Des Javascripts complémentaires sont par exemple chargés en fonction de la page visitée afin d'optimiser l'attaque, un fonctionnement constaté par les analystes de G Data dans une nouvelle variante de Zeus.

**Les URL peuvent aussi être stockés sur des serveurs distants.** C'est par exemple un fonctionnement constaté par G Data dans le nouveau cheval de Troie Ciavax. Les URL n'étant pas stockés dans le programme en lui-même, y accéder par analyse du code est impossible. Quant à l'attaque du serveur (par brute force) pour obtenir accès aux URL, il est facilement repérable par le cybercriminel qui peut alors prendre les contre-mesures adéquates.

L'autre avantage de l'utilisation de serveurs distants pour les cybercriminels est la grande évolutivité que cela confère à leur code. Ces chevaux de Troie remontant toutes les URL consultées par la victime, il peut ainsi définir de nouveaux scénarios d'attaque en complétant sa liste d'adresses et en développant de nouveaux Webinjects.

### Les utilisateurs de solutions G Data protégés

En bloquant la source de l'attaque sur l'ordinateur, autrement dit en protégeant le navigateur Internet de toute injection de code et de capture de données, les protections BankGuard et CloseGap permettent aux utilisateurs des solutions G Data de ne pas être impactés par ces nouveaux chevaux de Troie bancaire.

**Les solutions G-Data sont disponibles chez GS2i.**

[Visitez le site de GS2i](#)