
A la Une

# Cyber-news pour journalistes: Le retour du trojan (virus) visant les clients de banques

*8 mai 2019*

**Situation :**
Retefe est un malware bancaire qui cible les institutions et clients suisses. Son but est d'infecter des ordinateurs de personne utilisant de l'ebanking pour ensuite voler des accès bancaires et faire des transferts. Après près d'un an sans activité majeur, nous voyons ce Trojan réapparaitre avec des nouvelles techniques d'infection et d'attaque.

**Analyse :**
Les victimes sont autant les utilisateurs Mac que PC lorsqu'ils installent des applications légitimes qui ont été modifiées par les hackeur (notamment l'application « Convert PDF to Word Plus 1.0 » et Adobe). Une fois l'infection de l'ordinateur réussi, l'internaute sera redirigé vers un faux site web pour son ebanking qui permettra au hackeur de récupérer ces accès.

La liste des banques se trouve en bas de l'email

**Avis personnel :**
Retefe est l'un des pires malwares bancaires que nous ayons vus, il est très efficace, très discret et très difficile à détecter. Dans la majorité des cas, l'infection n'est pas due à une erreur humaine, mais plutôt à du matériel de cyber-sécurité qui n'est pas à la hauteur (ce qui est généralement le cas pour les personnes privées et les PME). Pour se protéger correctement il faut vraiment appliquer le principe de sécurité en profondeur (plusieurs couches de protection pour bloquer une attaque à différent stade de son exécution).

Les banques aussi se doivent de réagir en avisant leurs clients du risque accru et en mettant en place des contrôles/notifications supplémentaires.

**Steven Meyer**
**Partner & CEO**
Ing. EPFL, CISSP

**ZENData Sarl**