Depuis le début de l'année 2015, les entreprises françaises sont la cible d'une large campagne de spam en français. Sous prétexte de relance de facture, les attaquants poussent les employés à ouvrir des fichiers bureautiques infectés.

Les codes malveillants derrière ces attaques sont des trojans bancaires, capables de manipuler un transfert bancaire légitime réalisé par le service comptabilité de l'entreprise, en modifiant son montant et son destinataire.

Les trojans bancaires sont des programmes malveillants avancés. Grâce à des extensions appelées Webinjects, il s'adaptent à une multitude de portails bancaires en ligne. Ces extensions attaquent les navigateurs Web et manipulent la communication entre le PC et le serveur de la banque. La communication chiffrée est detournée et l'ensemble des données envoyées est modifié avant le chiffrement au niveau du navigateur. C'est l'attaque dite Man-in-the-Browser.

Un exemple de signalement par le gouvernement : http://cert.ssi.gouv.fr/site/CERTFR-2015-ALE-012/index.html (trojan Dridex)

N'hésitez pas à nous contacter pour effectuer un audit de vos protections.