

Yahoo, eBay et Paypal, un trio contre les hameçonneurs

Le service de mailing de Yahoo, baptisé Yahoo! Mail, va intégrer la technologie Domain Keys Identified Mail ou DKIM qui permet d'identifier et authentifier l'expéditeur d'un courriel ou d'un spam. A long terme, il serait pertinent de généraliser cette technologie qui a été normalisée par l'IETF (Internet Engineering Task Force).

Tous les internautes reçoivent des pourriels, des scams et autres messages dont le but est bien entendu de profiter de la naïveté de certains internautes qui ne connaissent pas les risques auxquels ils s'exposent en surfant sur la Toile et en ouvrant les pièces jointes de mails suspects.

Pour faire face à l'explosion du nombre de spams, selon une récente étude réalisée par l'éditeur de solutions de messageries Ipswitch 95 % des e-mails reçus peuvent être des « pourriels » ou « spam ».

Un pourcentage incroyable qui montre bien que les cybercriminels utilisent de plus en plus régulièrement ce vecteur pour lancer des attaques, récupérer des données confidentielles exploitables, ou bien encore installer sur des postes étrangers des Trojans ou autres codes malveillants.

Ebay et Paypal vont également intégrer cette technologie de surveillance des messages entrants et sortants au niveau du backbone des opérateurs.

Du coup, les chanceux utilisateurs de Yahoo! Mail ne devraient bientôt plus recevoir de spam de la part de pirates se faisant passer pour des officiels d'eBay ou de Paypal.

Reste que pour être réellement performante cette technologie doit être disponible d'un bout à l'autre de la chaîne tant chez le fournisseur de services que chez le fournisseur d'accès...

Dans les faits, DKIM fonctionne par signature cryptographique qui permet d'authentifier l'expéditeur d'un message. Il s'agit d'une approche radicalement différente de la précédente qui consistait en une simple analyse partielle du contenu du courrier électronique.

La majorité des spécialistes de la sécurité s'accordent à dire qu'il s'agit d'un événement important qui va permettre de limiter les risques pour les utilisateurs et porter un sérieux coup au moral des spammeurs et autres cyber malfaiteurs à l'affût des moindres opportunités. DKIM est une couche de sécurité en plus qui vient compléter les solutions déjà utilisées par les navigateurs Web comme Opéra, Firefox ou Internet Explorer.

Selon des analyses de Trend Micro eBay et son système de paiement Paypal sont deux des dix principales cibles des spammeurs. Et cela, depuis plusieurs mois. D'après l'analyse de MessageLabs, dans le monde sur 173 mails envoyés chaque jour au moins un contient un code permettant une attaque par phishing.

La première version de DKIM remonte à 2005 à la suite d'une longue collaboration entre les

industriels du secteur pour développer un standard ouvert permettant l'authentification des emails. Parmi les participants à ce projet, l'on peut citer Alt-N Technologies, AOL, Brandenburg InternetWorking, Cisco, EarthLink, IBM, Microsoft, PGP Corporation, Sendmail, StrongMail Systems, Tumbleweed, VeriSign et Yahoo!.

Plus d'informations sur la technologie DKIM sont disponibles sur [ce site officiel](#).