Panoptinet

Gardez un oeil sur votre réseau

Qu’est ce que le pharming ?

admin · Wednesday, October 19th, 2011

Amis internautes, méfiez-vous du pharming : ce piège consiste à remplacer un site officiel par un faux, dans le but de soutirer aux visiteurs trompés des informations personnelles ou bancaires. Un peu comme le phishing ? Non, c'est encore plus vicieux...

Les tentatives de phishing (ou hameçonnage) utilisent des e-mails frauduleux comme leurres : ils se font passer pour des mails officiels (exemples : Hadopi, EDF, SFR, Paypal, CAF, Visa/Mastercard, etc.), et proposent un lien vers un faux site, reprenant les traits exacts du site officiel imité. Il suffit en général de regarder l'**adresse du site** (URL) pour se rendre compte qu'elle est complètement loufoque : les internautes avertis ne se font plus piéger. Le **pharming** (ou **dévoiement** en bon français) est beaucoup plus insidieux : même **si vous tapez la bonne adresse dans votre navigateur internet, vous serez redirigé vers le site d'un hacker**, sans vous en rendre compte.

Comment le pharming fonctionne ?

Le pharming est souvent décrit comme étant du "phishing sans leurre". C'est plus complexe que cela : il s'agit d'une **méthode de piratage** informatique qui exploite les **failles du système DNS**. Le DNS est ce qui fait le **lien entre une adresse IP** (en général celle d'un serveur où est hébergé un site web) **et un nom de domaine** (ex : cocolasticot.com). Le pirate pharmeur va réussir à **modifier ces requêtes DNS**, en faisant correspondre un nom de domaine courant (ex : hadopi.fr) avec une adresse IP frauduleuse qui lui appartient : ainsi, en tapant dans le navigateur internet une adresse de site habituelle, on arrive sur un **site malveillant**, qui reprend bien sûr la **même apparence** que le site remplacé.

Concrètement, cela signifie que le visiteur piégé n'a **aucun moyen de se douter** de la supercherie, et qu'il risque de **donner ses informations personnelles et/ou bancaires** aux hackers. C'est justement l'objectif des sites de pharming.

D'autres types de pharming utilisent aussi des vers ou des chevaux de Troie pour attaquer plus indirectement la barre d'adresse du navigateur internet, et ainsi rediriger l'internaute vers un site frauduleux, tout en continuant d'afficher l'adresse URL initiale.

Une menace non négligeable

Selon *PC Mag*, suite à une attaque en mars 2010, l'étude de serveurs web infectés a permis de constater que **900 adresses** de sites internet (URL) et quelques **75 000 e-mails** avaient ainsi été redirigés vers des pirates pharmeurs.

Comment se protéger du pharming ?

Hélas, même la vigilance de l'internaute peut ne pas suffire dans les cas de pharming. Certains sites web sont néanmoins immunisés contre ce genre de hack (sites **PhC**, pour *pharming-conscious*), et certains logiciels de sécurité peuvent aussi **alerter l'utilisateur** à temps : ces solutions détectent une **incohérence** entre le certificat du site demandé et le site réellement affiché. Si votre navigateur ou votre solution de sécurité affiche un message d'alerte pharming, passez votre chemin !

Source : bullguard.com

This entry was posted on Wednesday, October 19th, 2011 at 5:57 pm and is filed under Actualités pratiques
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.