

Les utilisateurs de PayPal, cibles d'attaques de phishing

G DATA a détecté une nouvelle attaque qui cible une fois de plus les utilisateurs de PayPal, le service de transaction financière associé entre autre à eBay. Et ce sont cette fois-ci des cyber-criminels chinois qui sont à l'origine de cette extorsion de données (phishing). Les cyber-criminels chinois ont fait preuve de minutie et de nombreux efforts pour être convaincants. Une véritable passion du détail avec un faux site Web PayPal très ressemblant (voir PJ), un nom de domaine déposé spécifiquement (paypal-xxxxxxx-xxxxxxx.com) via une fausse entreprise chinoise dont le serveur est hébergé en Australie...

L'arnaque

Les victimes ont reçu un mail précisant que leur compte PayPal avait été suspendu en raison de transactions non autorisées. Pour résoudre le problème, le message demande aux internautes de s'identifier à nouveau. Au final, les victimes s'identifient sur le faux site Paypal.

Particulièrement malicieux

Ceux qui ne se font pas piéger par l'attaque de phishing courent le risque d'infecter leur système par le biais d'un Drive-by-download. Le logiciel malveillant qui s'installe ici à l'insu de l'internaute fait partie de la catégorie des Chevaux de Troie (Trojan-Downloader.HTML.Agent.ij) qui télécharge d'autres logiciels malveillants. Une fois de plus, les criminels en ligne opèrent avec une double stratégie :

- 1/ la collecte des informations de connexion des comptes existants pour les utiliser à des fins criminelles.
- 2/ l'infection du système afin de prendre le contrôle de celui-ci, voler des données à caractère personnel et rattacher le PC à un réseau de botnet.

Les recommandations G DATA :

Le système d'exploitation ainsi que le logiciel antivirus doivent être maintenus à jour pour se protéger contre de telles attaques. Les utilisateurs des solutions G DATA peuvent être soulagés : l'actuelle version de la signature détecte la menace.