Les scams seront les principales attaques lors de l'Euros 2012 et les JO
Internet
PostÃ© par : JPilo
PubliÃ©e le : 14/6/2012 13:30:00

La seconde moitiÃ© de lâ□□annÃ©e 2012 sera une pÃ©riode trÃ¨s mÃ©diatique, avec deÂ grands Ã©vÃ©nements sportifs et politiques tels que lâ□□Euro 2012, les JeuxÂ Olympiques ou encore les Ã©lections prÃ©sidentielles aux Etats-Unis. De telsÂ Ã©vÃ©nements garantissent une forte activitÃ© Internet et, avec, un dÃ©ferlementÂ dâ□□attaques de logiciels malveillants ! **Les scams seront certainement les principales attaques dont il faudra se mÃ©fier.**

Avec plus de 2 milliards de personnes connectÃ©es, lâ□□Internet est devenu le terrain de jeu favori des scammers. Il existe des milliers de scams en circulation aujourdâ□□hui et il serait difficile de tous les lister. Mais ils ont clairement le mÃªme objectif : extorquer de lâ□□argent Ã leurs victimes en tirant profit de leur crÃ©dulitÃ©, nous confie **Karine de Ponteves**, analyste anti-virus de lâ□□Ã©quipe FortiGuard chez Fortinet.

Avec les grands Ã©vÃ©nements mÃ©diatiques Ã venir Ã travers le monde, il est probable que les scammers susciteront la curiositÃ© des Internautes dans les prochains jours en commenÃ§ant par des â□□fausses lotteriesâ□□. Ce sont des spams envoyÃ©s par email aux utilisateurs indiquant quâ□□ils sont les heureux gagnants dâ□□une importante somme dâ□□argent ou dâ□□un lot Ã forte valeur. Pour percevoir leurs gains, il est demandÃ© aux utilisateurs de payer dâ□□abord les taxes. Bien sÃ»r, quâ□□ils paient ou non, ils ne recevront jamais leurs prix. Cette pratique est la plus populaire lors de grands Ã©vÃ©nements tels que lâ□□Euro, les Jeux Olympiquesâ□¦

Un autre type de scam, appelÃ© â□□achat frauduleuxâ□□ , promettant des billets Ã prix rÃ©duits pour de grands Ã©vÃ©nements, fleuriront Ã©galement sur la Toile. En surfant sur des sites de petites annonces tels quâ□□eBay, Leboncoin ou autres, les utilisateurs trouveront des billets Ã bas prix, mais la mÃ©fiance est essentielle en cette pÃ©riode dâ□□Ã©vÃ©nements, car les bonnes affaires sont souvent de pures fraudes.

Un troisiÃ¨me type de scams que lâ□□on pourrait observer est le â□□faux anti-virusâ□□. En pÃ©riode de grands Ã©vÃ©nements politiques ou sportifs, de nombreux Internautes surfent sur Internet pour connaitre les scores, rÃ©sultats et autres actualitÃ©s. Dâ□□une simple recherche sur leur moteur de recherche prÃ©fÃ©rÃ©, il est tout Ã fait possible pour les utilisateurs de cliquer sur un lien vers un site Internet malveillant - ou sur un site Internet lÃ©gitime qui a Ã©tÃ© piratÃ© - qui affiche un pop-up sur leur Ã©cran indiquant que leur ordinateur est infectÃ© (mÃªme sâ□□ils ont dÃ©jÃ un antivirus) et offrant de le nettoyer. Ce faux message incite typiquement les

utilisateurs Ã cliquer sur le pop-up, permettant lâ□□installation dâ□□un faux anti-virus Ã leur insu et, ensuite, lâ□□installation de chevaux de Troie pour collecter les donnÃ©es clÃ©s des utilisateurs tels que les mots de passe, coordonnÃ©es bancaires...

A prÃ©sent, voici dâ□□autres types de scams, qui sont Ã©galement trÃ¨s actifs :

- Les canulars vidÃ©o et rÃ©seaux sociaux

Dans ce cas, les utilisateurs reÃ§oivent un message dâ□□un ami Facebook qui prÃ©tend possÃ©der des images "exclusives" ou des vidÃ©os "rares", surtout aprÃ¨s un Ã©vÃ©nement majeur â□□ comme la mort de Michael Jackson, le tsunami au Japon en Mars 2011 ou encore lâ□□exÃ©cution dâ□□Oussama Ben Laden â□□ qui fait lâ□□actualitÃ©. Ces images ou vidÃ©os sont souvent fausses. En cliquant sur le lien, les utilisateurs sont dirigÃ©s vers une page Facebook qui semble Ãªtre lÃ©gitime et sont invitÃ©s Ã copier et coller un lien dans leur navigateur, qui installera un logiciel malveillant sur lâ□□ordinateur et propagera automatiquement le scam Ã leurs listes de contacts.

- Le phishing et vol dâ□□identitÃ©

Les utilisateurs reÃ§oivent un email de leur banque et / ou de Paypal indiquant que leur compte est bloquÃ© et, pour remÃ©dier Ã la situation il leur est demandÃ© de remplir un formulaire avec leurs informations bancaires. Ces utilisateurs ne devraient pas rÃ©pondre et garder en mÃ©moire que leur banque ne leur demandera jamais leurs identifiants bancaires par email. Sâ□□ils donnent leurs coordonnÃ©es bancaires, leurs comptes pourraient Ãªtre complÃ¨tement vidÃ©s par les scammers. Cette technique, appelÃ©e phishing, est Ã©galement utilisÃ©e pour obtenir dâ□□autres informations sensibles comme les numÃ©ros de sÃ©curitÃ© sociale. Ce scam peut rapidement devenir un problÃ¨me majeur qui touche bien plus de personnes que la victime elle-mÃªme : les dÃ©gÃ¢ts peuvent avoir un effet boule de neige lorsque les coordonnÃ©es volÃ©es sont utilisÃ©es dans une seconde phase dâ□□attaques.

- La fraude NigÃ©rienne sur les frais avancÃ©s

Ce scam existe sous diffÃ©rentes formes depuis des siÃ¨cles. Le concept est simple: convaincre les victimes quâ□□elles vont recevoir une Ã©norme somme dâ□□argent en Ã©change dâ□□un peu ou dâ□□aucun effort de leur part. AprÃ¨s avoir pris contact avec la victime, le scammer demande des frais fictifs pour dÃ©bloquer de lâ□□argent. De plus en plus dâ□□argent peut Ãªtre demandÃ© par la suite. Ce type de fraude peut parfois conduire Ã de graves problÃ¨mes financiers pour la victime.

- Les escroqueries amoureuses

Les auteurs dÃ©veloppent une relation longue distance avec des victimes dÃ©signÃ©es. Dans la plupart des cas, les cybercriminels se font passer pour de riches hommes dâ□□affaires travaillant Ã lâ□□Ã©tranger, ou de charmantes femmes cherchant quelquâ□□un pour sâ□□occuper dâ□□eux/elles. Lorsque le contact est Ã©tabli, il ne faut pas attendre longtemps avant que lâ□□auteur commence Ã demander de lâ□□argent.

Tous ces types de scams fleurissent sur le Web et mÃªme les Internautes avertis peuvent se faire piÃ©ger.

Voici donc quelques conseils de base importants pour Ã©viter de perdre ses informations personnels ou son argent :

- Les demandes de mots de passe et informations de cartes de crÃ©dit devraient vous mettre la puce Ã lâ□□oreille, vÃ©rifiez Ã deux fois avant dâ□□obtempÃ©rer

- MÃ©fiez-vous des liens qui vous dirigent soit vers des applications soit vers des sites Internet externes

- Croyez le vieux dicton : â□□Si câ□□est trop beau pour Ãªtre vrai, câ□□est que câ□□est sÃ»rement le casâ□□.

- Ne pas envoyer dâ□□argent Ã quelquâ□□un que vous nâ□□avez jamais rencontrÃ© en personne.

- Si vous nâ□□avez pas participÃ© Ã une loterie, vous ne pouvez pas avoir gagner !