CybercriminalitÃ© : Mondial de football 2014 : A quoi devons-nous nous attendre ?
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 10/6/2014 15:00:00

Alors que des milliers dâ□□ouvriers brÃ©siliens tentent dâ□□achever en temps et en heure le stade pour le match dâ□□ouverture, les cybercriminels brÃ©siliens sont, quant Ã eux, dâ□□ores et dÃ©jÃ prÃªts.
Avec une population dâ□□environ 201 millions dâ□□habitants en 2013, le BrÃ©sil est le 5Ã¨me pays le plus peuplÃ© et a lâ□□une des plus importantes communautÃ©s cybercriminelles au monde. Jusquâ□□en 2003, les hackers brÃ©siliens ciblaient les sites Internet, sans sâ□□en prendre Ã leurs utilisateurs. Au cours des annÃ©es qui ont suivi, ils se sont professionnalisÃ©s en sâ□□attaquant aux sites Internet des banques locales, cible de choix car trois quart des BrÃ©siliens effectuent leurs transactions financiÃ¨res en ligne.

Ainsi, dâ□□aprÃ¨s une enquÃªte menÃ©e par la FÃ©dÃ©ration BrÃ©silienne des banques (FEBRABAN) en 2011, le secteur bancaire au BrÃ©sil a enregistrÃ© R$1.5 milliards de pertes dues au phishing, vol des donnÃ©es, vol dâ□□identitÃ©, scams et fraudes Ã la carte bancaire en ligne. Mais la banque est la cible dâ□□une partie seulement des menaces Internet Ã travers le pays.

En effet, les fraudeurs appliquent ce quâ□□ils ont appris au cours des 10 derniÃ¨res annÃ©es, Ã travers les attaques visant les banques, pour monnayer leurs expertises dans le piratage dâ□□autres domaines tels que les factures de consommation dâ□□Ã©lectricitÃ©, les programmes de fidÃ©lisation des compagnies aÃ©riennes, les personnes fortunÃ©es â□¦

Au-delÃ des seuls cybercriminels BrÃ©siliens, Ã J-2 avant le coup dâ□□envoi du match dâ□□ouverture de la coupe du monde de football 2014, on peut sâ□□attendre Ã de nombreuses arnaques sur la Toile de la part de la communautÃ© globale des cybercriminels dans les prochains jours et semaines. Il est donc important de rappeler quelques conseils aux fans du ballon rond pour leur Ã©viter de mauvaises surprises :

- Emails non sollicitÃ©s : ce sont des spams envoyÃ©s par email aux Internautes indiquant quâ□□ils sont les heureux gagnants dâ□□une loterie avec Ã la clÃ© 2 billets pour la finale de la coupe du monde, ou bien quâ□□ils peuvent accÃ©der Ã des sites Internet de retransmission des matchs en temps rÃ©elâ□¦.

Â

Alors quâ□□il est trÃ¨s tentant pour un supporter de cliquer sur le lien dâ□□un email annonÃ§ant : â□□Vous avez gagnÃ© 2 places pour la Finale de la Coupe du Mondeâ□□, soyez prudent! En cliquant sur ce lien, vous pourriez Ãªtre dirigÃ© vers un site Internet qui tÃ©lÃ©charge des logiciels malveillants sur votre ordinateur.

Ce logiciel malveillant peut Ãªtre ensuite utilisÃ© comme enregistreur de frappe de votre ordinateur pour rÃ©cupÃ©rer toutes vos informations personnelles tels que vos mots de passes, numÃ©ro de comptes bancairesâ□¦. ou pour tÃ©lÃ©charger dâ□□autres malwares, tels que les faux logiciels dâ□□antivirus, ou encore transformer votre ordinateur en gÃ©nÃ©rateur de spams.

Les spammers et les escrocs aiment ce genre dâ□□Ã©vÃ©nements car ils savent que pendant toute la durÃ©e de la Coupe du Monde, les fans de football surfent sur le Web Ã la recherche dâ□□offres attractives.

- Marchands de vente en ligne proposant des billets Ã prix rÃ©duits: Si vous dÃ©couvrez une boutique en ligne avec dâ□□incroyables promotions pour des billets, renseignez-vous quâ□□il sâ□□agisse dâ□□un magasin lÃ©gitime et non dâ□□une fausse faÃ§ade qui disparaitra prochainement avec les informations de votre carte de crÃ©dit. Et mÃªme sâ□□il est lÃ©gitime, vous devez vous assurer que son site nâ□□a pas Ã©tÃ©, sans le savoir, exploitÃ© par une injection SQL ou dâ□□autres attaques de type serveur.

Les sites Internet exploitÃ©s ne vous dirigent pas toujours vers un site malveillant, mais souvent utiliseront la technique du phishing ou essayeront dâ□□installer furtivement dâ□□autres formes de malwares sur votre ordinateur, tels que des Chevaux de Troie (Trojans), des bots, des enregistreurs de frappe (keyloggers) et des outils de dissimulation dâ□□activitÃ© (rootkits), qui sont conÃ§us pour porter atteinte aux ordinateurs et voler les informations personnelles.

De la mÃªme faÃ§on, Ã©viter de croire les sites des petites annonces tels quâ□□eBay, Leboncoin ou autres, vous faisant miroiter des billets Ã prix cassÃ©s pour lâ□□Ã©vÃ©nement. La mÃ©fiance est essentielle en cette pÃ©riode dâ□□Ã©vÃ©nements car les bonnes affaires sont souvent de pures fraudes.

- Le phishing et vol dâ□□identitÃ© : Les utilisateurs reÃ§oivent un email de leur banque et / ou de Paypal indiquant quâ□□un paiement pour lâ□□achat de deux places de football est en cours alors que lâ□□Internaute nâ□□a en rÃ©alitÃ© procÃ©dÃ© Ã aucun achat. Pour annuler la transaction, lâ□□Internaute devra cliquer sur un lien oÃ¹ il lui sera demandÃ© de remplir un formulaire avec ses informations bancaires.

Les 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.

- Points dâ□□accÃ¨s (hotspot) Wi-Fi non sÃ©curisÃ©s au BrÃ©sil: Alors que le gouvernement BrÃ©silien renforce les dispositifs de sÃ©curitÃ© pour le Mondial, les 17 000 supporters des Bleus qui se dÃ©placeront au BrÃ©sil devront rester vigilants. Les supporters qui nâ□□auront pas la chance de suivre les matchs au stade, surferont sur Internet pour connaÃ®tre les rÃ©sultats en temps rÃ©el, en se connectant aux points dâ□□accÃ¨s Wifi des hÃ´tels, bars...

Attention Ã ne pas vous connecter Ã un point dâ□□accÃ¨s inconnu non sÃ©curisÃ©. Un point dâ□□accÃ¨s non sÃ©curisÃ© permet aux cybercriminels de capturer toutes les donnÃ©es qui circulent Ã partir du hotspot afin dâ□□intercepter les logins et mots de passe, emails, les documents en piÃ¨ce jointe et autres informations personnelles et confidentielles.

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 de Guillaume Lovet, expert en cybercriminalitÃ© chez Fortinet 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 sÃ»rement le casâ□□.
- Si vous nâ□□avez pas participÃ© Ã une loterie, vous ne pouvez pas avoir gagnÃ© !
- En se connectant mÃªme sur des points dâ□□accÃ¨s sÃ©curisÃ©s, vÃ©rifiez que les connexions Ã vos sites favoris soient bien en connexion sÃ©curisÃ© https.