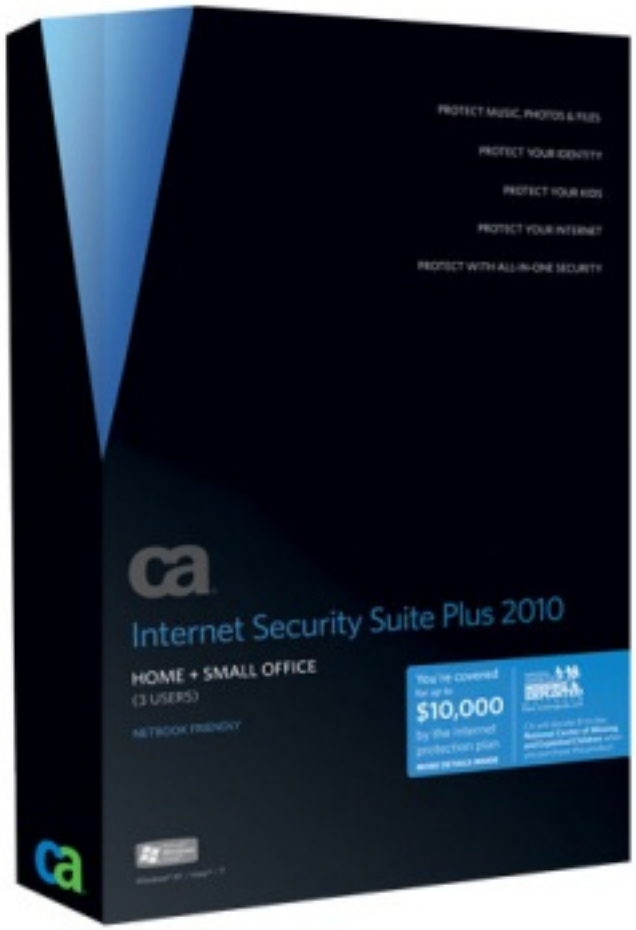
SÃ©curitÃ© : CA appelle Ã la vigilance pour les achats sur Internet
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 8/1/2010 15:00:00

Alors que les soldes battent leur plein dans les magasins et sur Internet, **CA appelle les consommateurs Ã la plus grande vigilance lors de leurs achats en ligne, â¦**

Un nouveau **rapport** publiÃ© par lâ€™Ã©diteur de logiciels CA, rÃ©vÃ¨le en effet un essor de la criminalitÃ© en ligne centrÃ©e sur les principaux moteurs de recherche, les rÃ©seaux sociaux, les faux logiciels de sÃ©curitÃ© et les programmes malveillants.

Lâ€™Ã©tude de CA met en lumiÃ¨re un doublement des programmes malveillants en 2009. Alors que les tentatives de phishing (hameÃ§onnage) et les spams continuent Ã progresser, la diffusion des programmes malveillants (Â« malware Â») reste dominante sur Internet (78 %), mais aussi via le courrier Ã©lectronique (17 %), notamment avec les piÃ¨ces jointes ou le phishing et Ã©galement les supports amovibles (5 %) tels que les disques durs externes, cadres photos numÃ©riques, etc.).



Â« *Les cybercriminels mÃ¨nent leurs attaques sur les cibles les plus populaires, prÃ©sentant naturellement les meilleures perspectives de gain. Ces derniers calquent leur stratÃ©gie sur les tendances, les Ã©vÃ©nements majeurs, les pÃ©riodes de congÃ©s (notamment la rÃ©cente pÃ©riode de NoÃ«l) dans lâ€™espoir dâ€™y rÃ©aliser des profits consÃ©quents. Les moteurs de recherche (Google, Yahoo, â¦) et les rÃ©seaux sociaux les plus frÃ©quentÃ©s comme Twitter ou*

Facebook exercent un attrait considÃ©rable sur les cybercriminels Â», dÃ©clare Don DeBolt, Directeur dâ□□Etudes sur les Menaces Internet chez CA. Â« *La frÃ©nÃ©sie des pÃ©riodes de grande activitÃ© commerciale telles que les soldes conduisent les consommateurs Ã ne pas porter une attention particuliÃ¨re Ã leurs actes dâ□□achats... AprÃ¨s les logiciels de sÃ©curitÃ©, la meilleure dÃ©fense contre ces menaces est indiscutablement une vigilance accrue pour ne pas se laisser distraire.* Â»

Bilan des menaces 2009 mises en lumiÃ¨re par les experts de la sÃ©curitÃ© de CA

â□¢ Contamination des index de recherche â□□ Google est une cible rÃ©currente dâ□□attaques en ligne sophistiquÃ©es menÃ©es Ã travers des outils dâ□□optimisation de recherche visant Ã manipuler le classement des liens sponsorisÃ©s et de modifier de maniÃ¨re frauduleuse les rÃ©sultats des requÃªtes. Les utilisateurs sont alors dirigÃ©s vers des sites frauduleux ou contaminÃ©s par des programmes malveillants.

â□¢ RÃ©seaux sociaux/Web 2.0 â□□ Les communautÃ©s en ligne, les blogs et les sites les plus populaires de socialisation (YouTube, MySpace, Facebook, Twitter, etc.) sont Ã©galement des cibles prioritaires pour la cybercriminalitÃ© qui a crÃ©Ã© des centaines de profils afin de mener leurs manÅ□uvres frauduleuses (diffusion de programmes malveillants, spam, vol dâ□□identitÃ©s en ligne, etc.) prÃ©alablement Ã dâ□□autres attaques.

â□¢ Squatteurs et sites Â« miroir Â» â□□ Il sâ□□agit ici de sites Web imitant des sites lÃ©gitimes afin que les utilisateurs y mÃ¨nent leurs transactions et activitÃ©s en toute confiance.

â□¢ Faux logiciels de sÃ©curitÃ© â□□ Ces outils, se prÃ©sentant comme des solutions de protection sont en rÃ©alitÃ© des programmes malveillants, et ont Ã©tÃ© trÃ¨s en vogue en 2009 notamment au premier semestre. CA a dÃ©tectÃ© 1 186 nouvelles variantes de ces systÃ¨mes â□□ une croissance de 40 % par rapport au deuxiÃ¨me semestre 2008.

â□¢ Menaces Mac OS X â□□ Les risques de sÃ©curitÃ© pÃ¨sent dÃ©sormais aussi sur les Mac et, en 2009, CA ISBU a ajoutÃ© pas moins de 15 signatures de dÃ©tection de menaces spÃ©cifiques Ã cette plate-forme. La plus rÃ©pandue est Â« OSX/Jahlav Â» (anciennement Â« OSX/Rsplug Â» Ã©galement connu sous le nom de Â« DNSChanger Â») distribuÃ©e par le rÃ©seau de robots Zeus â□□ dont CA a identifiÃ© et contrÃ´lÃ© plus de 250 sites Web de relai et capturÃ© 53 variantes diffÃ©rentes.

Perspectives pour 2010

1. Lâ□□exploitation de failles de sÃ©curitÃ© et de fausses banniÃ¨res de publicitÃ©s (Â« Malvertising Â») continuera Ã progresser comme vecteur premier de diffusion des programmes malveillants.

2. Lâ□□essor des rÃ©seaux sociaux sera naturellement accompagnÃ© de celui des menaces qui les ciblentâ□¦

3. Les attaques en dÃ©nis de service (DoS) devraient Ã©galement connaÃ®tre une Â« popularitÃ© Â» croissante comme vecteur dâ□□action politique. Les sites majeurs de socialisationâ□□ et notamment Twitter et Facebook â□□ seront probablement victimes dâ□□attaques en 2010 comme cela sâ□□est produit en 2009.

4. Chevaux de Troie bancaires â Ces menaces liÃ©es aux activitÃ©s bancaires ont pour vocation de dÃ©rober des identitÃ©s afin de rÃ©aliser des gains financiers.

5. Des Â« vers Internet Â» de nouvelle gÃ©nÃ©ration (tels que Conficker) devraient Ã©merger en raison de leur succÃ¨s passÃ©.

6. La criminalitÃ© organisÃ©e devrait se focaliser sur les plates-formes 64 bits et les Macintosh. Les activitÃ©s de phishing et les spams devraient rester stables sans quâaucune dÃ©crue ne soit prÃ©visible.

10 conseils de protection

1/ Ãviter Ã tout prix les Â« clics dâenthousiasme Â» ! La plus grande prudence reste de mise dÃ¨s qu'il s'agit de suivre un lien inconnu.

2/ Des cartes trop bien intentionnÃ©esâ¦ Les messages bienveillants sont souvent les plus dangereux ; mÃ©fiez-vous particuliÃ¨rement de tous ceux qui vous promettent un avenir radieuxâ¦ Surtout sâils sont personnalisÃ©s et intimes (Â« Cher Jacques Â»).

3/ Astuces contre le phishing â Les tentatives de hameÃ§onnage exigent une vigilance permanenteâ¦ Les cibles privilÃ©giÃ©es des dÃ©tournements restent PayPal, eBay et Amazon ainsi que les e-mails de notification bancaire ou dâalerte aux fraudes sur cartes de crÃ©dit.

4/ Navigation dÃ©sastreuse â Le surf sur Internet reste une activitÃ© Ã haut risque exigeant de vÃ©rifier lâactivation permanente des mesures de protection en ligne (pare-feux, prÃ©vention dâintrusion, logiciels de protection, etc.). Les derniÃ¨res attaques dites dâoptimisation des moteurs de recherche manipulent les rÃ©sultats pour diriger le trafic vers des sites frauduleux.

5/ Des offres festives â Tout ce qui semble trop beau pour Ãªtre vrai lâest effectivement ! Ces attaques sont parfois trÃ¨s sÃ©duisantes (offre dâemploi, remise exceptionnelle, gains de jeu, etc.). Dans la plupart des cas, les instructions pour collecter ses Â« gains Â» exigeront un paiement initial ou la fourniture dâinformations confidentielles (cartes de crÃ©dit, etc.).

6/ Fraudes caritatives â Ne vous laissez pas aller sans vigilance Ã la gÃ©nÃ©rositÃ©â¦ Assurez-vous que la cause est juste ; ne prenez pas de dÃ©cision hÃ¢tive en suivant un e-mail Â« Ã©mouvant Â» ou en visitant un site inconnu. **Prenez le temps nÃ©cessaire pour vous documenter et nâhÃ©sitez pas Ã investiguer.**

7/ Des affaires trop exceptionnelles â Dans une Ã©conomie incertaine, nombreux cherchent Ã maximiser leur pouvoir dâachat. Internet exerce toujours un fort attrait Ã travers des remises exceptionnelles, des cartes de rÃ©duction, des offres gratuitesâ¦ Mais attention, ces offres allÃ©chantes sâaccompagnent souvent de versements initiaux (abonnements, cotisations dâadhÃ©sion, etc.) et prÃ©sentent des risques de vols de donnÃ©es personnelles. Les fervents des achats en ligne sont Ã©galement appelÃ©s Ã se mÃ©fier des sites douteux proposant des Â« comparaisons de prix Â».

8/ TÃ©lÃ©chargements et installations dangereux â Les logiciels malveillants recourent pour leur diffusion Ã des techniques dâingÃ©nierie sociale Ã©voquant des Â« ProblÃ¨mes de livraison Â» dans un e-mail semblant provenir dâun Ã©metteur lÃ©gitime (UPS, DHL, FedEx, etc.) suffisamment convainquant pour conduire lâutilisateur Ã initialiser manuellement le tÃ©lÃ©chargement et lâinstallation de logiciels malveillants. (message du type : Â« Relevez votre numÃ©ro de suivi postal Â» ou Â« Retrait disponible auprÃ¨s de Western Union Â», etc.).

9/ Vol dâidentitÃ© â Les pirates, voleurs de mots de passe et chevaux de Troie bancaires sont plus particuliÃ¨rement actifs.

Les sites de socialisation sont Ã©galement une cible privilÃ©giÃ©e oÃ¹ ils sont particuliÃ¨rement utilisÃ©s (Ã©changes dâ□□informations personnelles, partage de photos, etc.). Des menaces telles que Â« Koobface Â» profitent dâ□□Ã©vÃ¨nements festifs pour dÃ©ployer des visuels personnalisÃ©s maximisant les chances dâ□□infection.

10/ Activation des protections de sÃ©curitÃ© â□□ La protection en ligne est naturellement capitale et exige une mise Ã jour rÃ©guliÃ¨re des logiciels de sÃ©curitÃ©. Notons quâ□□il est Ã©galement prÃ©fÃ©rable d'Ã©teindre les ordinateurs non-utilisÃ©s.