BitDefender : Les 8 plaies numÃ©riques pour l'annÃ©e 2010
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 4/1/2010 0:00:00

Les dix plaies d'Ã□gypte sont les dix chÃ¢timents qu'aurait infligÃ©s Dieu Ã l'Ã□gypte dans la tradition judÃ©o-chrÃ©tienne et bien pour BitDefender l'annÃ©e 2010 comptera quelques 8 plaies numÃ©riques, **des Botnets Ã Windows, il faudra Ãªtre vigilant.**

Les menaces ciblant les sites de rÃ©seaux sociaux, les systÃ¨mes dâ□□exploitation et les technologies de Â« cloud computing Â» devraient augmenter et les botnets demeureront trÃ¨s rÃ©pandus en 2010

Selon BitDefender, Ã©diteur de solutions de sÃ©curitÃ© antimalwares, en 2010, il faudra particuliÃ¨rement surveiller les botnets, les applications malveillantes et les malwares ciblant des sites de rÃ©seaux sociaux. BitDefender prÃ©voit Ã©galement quâ□□en 2010, les cybercriminels sâ□□attaqueront aux systÃ¨mes dâ□□exploitation, aux appareils mobiles et aux technologies dâ□□entreprise telles que le Â« cloud computing Â».

Â« *Lâ□□annÃ©e 2009 a Ã©tÃ© marquÃ©e par une large gamme de menaces de sÃ©curitÃ© ciblant Ã la fois les utilisateurs finaux et les rÃ©seaux dâ□□entreprise* Â» affirme **Catalin Cosoi**, spÃ©cialiste antispam BitDefender. Â« *Le ver Conficker a beaucoup progressÃ© et est parvenu Ã rester lâ□□une des trois principales menaces mondiales en 2009. Bien quâ□□il ne soit pas rÃ©ellement dangereux, ses mÃ©canismes de diffusion et sa rÃ©sistance Ã la dÃ©tection pourraient servir de base Ã de futurs malwares extrÃªmement destructeurs.* Â»

Les prÃ©visions de BitDefender pour la sÃ©curitÃ© informatique en 2010 :

Lâ□□activitÃ© des botnets

Le spam envoyÃ© par les botnets sera au cÂ□ur des e-menaces en 2010. Des attaques par dÃ©ni de service distribuÃ© serviront dâ□□Â« exemple Â» Ã de futurs ou potentiels acheteurs de botnets. Si un client souhaite louer un botnet, mais nâ□□est pas sÃ»r des capacitÃ©s du rÃ©seau quâ□□il veut louer, il peut souhaiter assister Ã une Â« dÃ©monstration de force Â».

Les applications malveillantes

La plupart des applications malveillantes ont pour objectif de gÃ©nÃ©rer des gains financiers illicites. BitDefender estime que les malwares augmenteront significativement en 2010, en particulier les applications adwares et les faux logiciels antivirus (Rogue). Les malwares plus complexes, tels que les infecteurs de fichiers rootkits et les vers utilisant de multiples vecteurs dâ□□infection (les protocoles peer-to-peer, de messagerie et de messagerie instantanÃ©e) devraient Ã©galement progresser.

Les rÃ©seaux sociaux

Les sites de rÃ©seaux sociaux seront sans doute parmi les principaux vecteurs dâ□□infection en 2010. Exploitant leur expÃ©rience de ces rÃ©seaux sociaux, les auteurs de malwares devraient poursuivre sur cette voie avec la Â« Google wave Â» au fur et Ã mesure que le service de messagerie instantanÃ©e du moteur de recherche gagnera en popularitÃ©. Les sites Internet de rÃ©seaux sociaux demeureront Ã©galement les cibles spÃ©cifiques de certaines menaces. Le spam et les tentatives de phishing ciblant les utilisateurs de ces rÃ©seaux devraient Ã©galement augmenter.

Les systÃ¨mes dâ□□exploitation

Le rÃ©cent systÃ¨me dâ□□exploitation WindowsÂ® 7 de Microsoft sâ□□est avÃ©rÃ© Ãªtre bien plus sÃ»r que ses prÃ©dÃ©cesseurs. Cependant, plus les utilisateurs passeront de Vista et XP Ã Windows 7, plus les crÃ©ateurs de malwares rechercheront Ã tirer profit des vulnÃ©rabilitÃ©s logicielles et des brÃ¨ches de sÃ©curitÃ© dans le systÃ¨me dâ□□exploitation.

Nous recommandons vivement aux utilisateurs de Mac OS X dâ□□Apple dâ□□adopter une suite antimalware afin dâ□□Ã©viter les infections. Outre les tentatives de phishing et de spam qui concernent tous les systÃ¨mes dâ□□exploitation et qui ciblent tous les utilisateurs dâ□□ordinateurs connectÃ©s Ã Internet, la transition dâ□□Apple vers la plateforme Intel sâ□□accompagnera de nouvelles opportunitÃ©s pour les pirates qui crÃ©ent actuellement des malwares pour Windows.

Les systÃ¨mes dâ□□exploitation mobiles

La derniÃ¨re version de lâ□□iPhone 3G a considÃ©rablement fait augmenter le parc dâ□□utilisateurs dâ□□iPhones en 2009. Beaucoup dâ□□entre eux ont dÃ©cidÃ© de Â« jail-breaker Â» (dÃ©bloquer) le systÃ¨me dâ□□exploitation afin dâ□□installer des applications tierces. Cette opÃ©ration nÃ©cessite lâ□□activation du service SSH avec un accÃ¨s Â« root Â» et un mot de passe par dÃ©faut. BitDefender pense que de nouvelles e-menaces apparaÃ®tront en 2010, exploitant les plateformes mobiles Ã la mode, en particulier des vers et des chevaux de Troie voleurs de mots de passe.

Les utilisateurs dâ□□Android et de Maemo, seront, Ã priori, Ã©pargnÃ©s. Leur part de marchÃ© Ã©tant modeste comparÃ©e Ã Windows Mobile, Symbian et iPhone OS, les auteurs de malwares nâ□□essaieront pas de trouver des vulnÃ©rabilitÃ©s, mais se consacreront plutÃ´t Ã des attaques de type Â« ingÃ©nierie sociale Â».

Les menaces pour les entreprises

Les technologies de virtualisation de VMWare vSphere et Windows Server 2008 R2 Hyper-V de Microsoft ont offert de nouvelles possibilitÃ©s aux petites et moyennes entreprises. Faire fonctionner plusieurs serveurs sur une seule machine grÃ¢ce Ã la virtualisation contribuera Ã rÃ©duire considÃ©rablement les coÃ»ts. En 2010, on sâ□□attend Ã ce que des pirates recherchent des vulnÃ©rabilitÃ©s logicielles leur permettant de prendre le contrÃ´le de lâ□□hyperviseur et de toutes les machines virtuelles dÃ©ployÃ©es sur le systÃ¨me.

Les services de Â« ***cloud computing*** Â» connaissent aussi de beaux jours. Quâ□□ils soient utilisÃ©s

pour lâ□□envoi dâ□□e-mails ou pour la sauvegarde et le stockage de donnÃ©es, les technologies Â« cloud Â» contiennent et traitent de grandes quantitÃ©s de donnÃ©es sensibles. BitDefender prÃ©voit quâ□□en 2010, les attaquants se tourneront vers ces infrastructures, afin de prendre le contrÃ´le de ces ressources Â« in the cloud Â» ou d'en limiter lâ□□accÃ¨s.

Enfin, les netbooks et les assistants numÃ©riques personnels (PDA) sont suseptible de reprÃ©senter un risque sÃ©curitaire croissant pour les entreprises alors que leur usage gagne en popularitÃ©. Les netbooks ne comprenant pas de puce TPM ou dâ□□autres solutions de cryptage matÃ©riel/logiciel pouvant Ãªtre administrÃ©s Ã distance (afin dâ□□effacer le contenu du disque dur en cas de perte ou vol), des donnÃ©es sensibles pourraient se retrouver entre de mauvaises mains.

Â« *Les utilisateurs dâ□□ordinateurs doivent garder Ã lâ□□esprit que les cybercriminels adaptent constamment leurs menaces afin de ne pas se faire attraper, ce qui les rend encore plus dangereuses* Â» explique Catalin Cosoi. Â« *Il est donc essentiel que les particuliers ainsi que les petites et moyennes entreprises disposent dâ□□une solution de sÃ©curitÃ© fiable, installÃ©e et mise Ã jour, sur leurs systÃ¨mes.* Â»

Pour Ãªtre informÃ© des derniÃ¨res e-menaces et informations sur nos produits et Ã©vÃ©nements, inscrivez-vous au **service RSS de BitDefender**.