BitDefender : PayPal, eBay et HSBC, Danger Phishing
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 26/8/2010 0:00:00

BitDefender, Ã©diteur de solutions de sÃ©curitÃ©, vient de publier un rapport expliquant que le premier semestre 2010 a enregistrÃ© un fort accroissement du nombre de vers exploitant les diffÃ©rentes plateformes Web 2.0.

Le rapport se rÃ©fÃ¨re aux donnÃ©es enregistrÃ©es entre janvier et juin 2010 et aboutit Ã la conclusion que les rÃ©seaux sociaux et les services Web 2.0 sont devenus les canaux les plus en vogue pour la propagation de malwares au cours des six derniers mois.

Dans le mÃªme temps, les pirates sâattachent Ã se faire passer pour des sites tels que PayPal et eBay. Enfin, le volume du spam pharmaceutique (de type Viagra) reprÃ©sente aujourd'hui les deux tiers du volume total du spam.

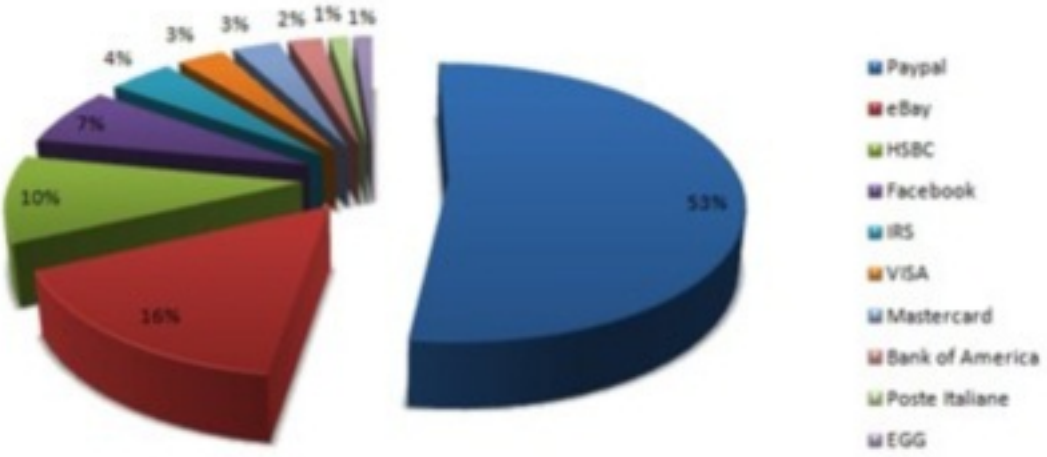
Spam et hameÃ§onnage : tendances au premier semestre 2010

Les organismes financiers et bancaires ont Ã©tÃ© les cibles prÃ©fÃ©rÃ©es des cyber-criminels, rassemblant Ã eux seuls 70 % du total des tentatives dâ hameÃ§onnage. Les rÃ©seaux sociaux ont Ã©galement Ã©tÃ© soumis Ã rude Ã©preuve, car ils constituent une mine d'informations personnelles et de donnÃ©es susceptibles d'Ãªtre utilisÃ©es pour le lancement d'attaques ciblÃ©es. Au cours de la premiÃ¨re moitiÃ© de 2010, les pirates ont consacrÃ© leurs efforts Ã usurper l'identitÃ© des entreprises PayPal et eBay. La banque HSBC arrive en troisiÃ¨me position, tandis que Poste Italiane et EGG occupent les derniers rangs de la liste des entitÃ©s les plus corrompues en ligne.

Le Top 10 des cibles de hameÃ§onnage entre janvier et juin 2010

La coupe du monde de football (FIFA World Cupâ¢) et les glissements de terrains qui ont affectÃ© le Guatemala sont deux des nombreux Ã©vÃ©nements utilisÃ©s pour optimiser le rÃ©fÃ©rencement Black-Hat SEO et amÃ©liorer la position des sites web diffuseurs de malwares. Cette pÃ©riode a Ã©galement vu la quantitÃ© de spam atteindre 86 % de l'ensemble du trafic de courrier Ã©lectronique, le spam pharmaceutique arrivant en tÃªte, atteignant de nouveaux sommets, en passant de 51 Ã 66 % de l'ensemble des envois de spam.

RÃ©partition du spam par catÃ©gorie au cours du premier semestre 2010 :



â¢ MÃ©dicaments divers â 66 %

â¢ Produits contrefaits â 7 %

â¢ PrÃªts et assurances â 5 %

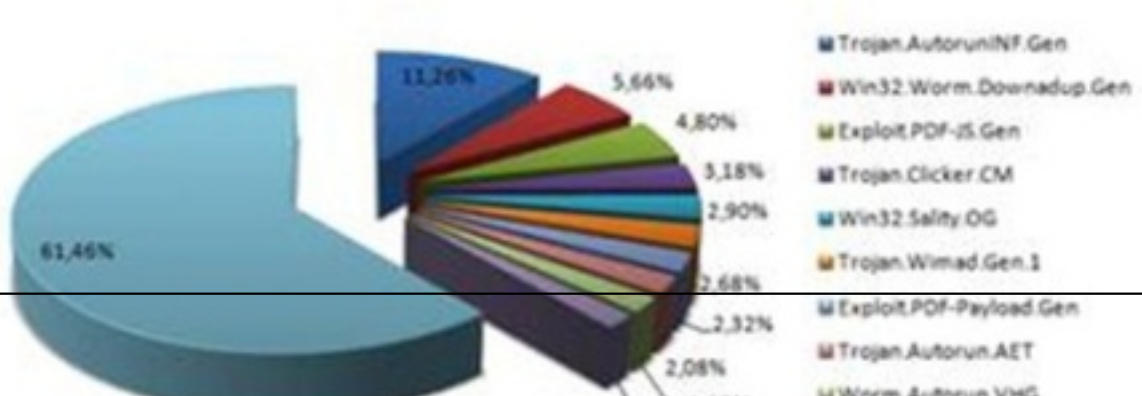
â¢ Malware empaquetÃ© â 3,5 %

â¢ Casinos et jeux d'argent â 3,5 %

Statistiques des menaces de type malware

Trojan.AutorunINF.Gen, qui exploite la fonction Autorun de WindowsÂ®, arrive en tÃªte du classement, totalisant plus de 11 % du nombre total d'infections, tandis que les vers MBR ont fait leur retour aprÃ¨s actualisation de leurs mÃ©canismes d'infection virale. La fin janvier a aussi vu l'Ã©mergence de Win32.Worm.Zimuse.A, associant virus, rootkit et ver. Au moment de l'infection le ver commence Ã compter les jours. Quarante jours aprÃ¨s l'infection, il efface le Master Boot Record du disque dur, rendant ainsi le systÃ¨me d'exploitation incapable de dÃ©marrer. La Chine et la FÃ©dÃ©ration de Russie sont les championnes du monde de la diffusion de ce malware avec des taux respectifs de 31 et 32%.

Le Top 10 des malwares entre janvier et juin 2010



VulnÃ©rabilitÃ©s, Â« exploits Â» et brÃ¨ches de sÃ©curitÃ©

De dangereux Â« exploits Â» de type zero-day, profitant des failles de sÃ©curitÃ© de logiciels aussi courants que le navigateur Internet Explorer de MicrosoftÂ®, AdobeÂ® ReaderÂ®, AdobeÂ® Flash PlayerÂ® et mÃªme AdobeÂ® PhotoshopÂ® CS 4. Certains Â« exploits Â» d'Internet Explorer ont mÃªme Ã©tÃ© utilisÃ©s dans des attaques Ã l'encontre de sociÃ©tÃ©s aussi importantes que GoogleÂ®, AdobeÂ® et RackspaceÂ®.

PrÃ©visions concernant les e-menaces

Les experts de BitDefender sont prÃ©occupÃ©s par le fait que, alors que les six premiers mois de 2010 ont Ã©tÃ© marquÃ©s par des menaces classiques de type chevaux de Troie ou vers, de nombreux types d'exploits visant des applications tierces ont rapidement gagnÃ© du terrain ces derniers temps. Comme on a pu le voir dans le cas de Exploit.Comele.A, les vulnÃ©rabilitÃ©s Â« zero-day Â» peuvent Ãªtre utilisÃ©es Ã des fins qui vont au-delÃ du vol d'identitÃ© ou de coordonnÃ©es bancaires, mais aussi pour mener de vÃ©ritables Â« cyber-guerres Â» et mener des actions dâespionnage industriel.

Â« *Au moment oÃ¹ FacebookÂ® atteint 500 millions d'utilisateurs, la plupart des auteurs de malwares s'intÃ©ressent Ã ce rÃ©seau pour y dÃ©ployer leurs plus rÃ©centes trouvailles en terme dâattaque. Certaines dâentre elles vont consister Ã utiliser des astuces dâingÃ©nierie sociale et d'autres vont tenter d'exploiter les diffÃ©rentes vulnÃ©rabilitÃ©s ou fonctions dÃ©jÃ prÃ©sentes sur la plateforme* Â», indique **Catalin Cosoi**, Directeur du Laboratoire dâÃ©tude des menaces en ligne BitDefender.

Les experts de BitDefender pensent Ã©galement que la divulgation d'informations personnelles va beaucoup contribuer Ã la rÃ©ussite d'attaques variÃ©es, notamment quand les donnÃ©es recueillies sont confirmÃ©es sur des blogs personnels, dans des C.V. et autres rÃ©fÃ©rences du mÃªme ordre. On peut Ã©galement s'attendre Ã ce que des applications tierces jouent un rÃ´le important dans les abus ciblant les rÃ©seaux sociaux.

Â« *L'arrivÃ©e de HTML5, la prochaine rÃ©vision importante du HTML classique, va apporter des niveaux supplÃ©mentaires d'interaction entre l'utilisateur et les pages web et probablement modifier le Web tel que nous le connaissons. Il est hautement probable que la nouvelle technologie sera exploitÃ©e par les auteurs de malwares pour compromettre la sÃ©curitÃ© des navigateurs* Â» a ajoutÃ© **Mr Cosoi**.