Communiqué de presse

À Montrouge, le mardi 24 août 2010

Les sites PayPal, eBay et HSBC principales cibles du phishing

La Chine et la Russie principaux diffuseurs de malwares

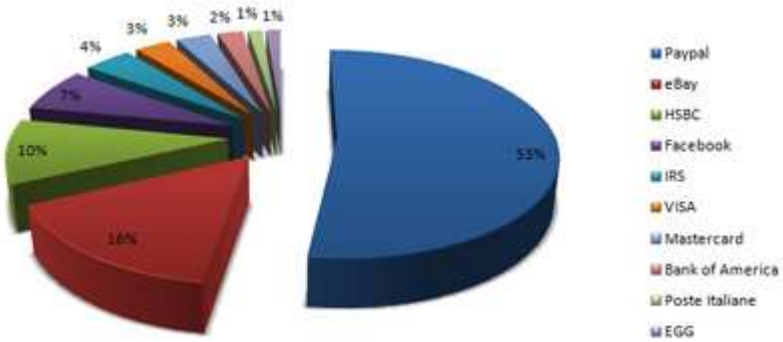
Prévisions de développement des malwares pour seconde moitié de l'année

***BitDefender*®,** éditeur de solutions de sécurité, vient de publier un rapport expliquant que le premier semestre 2010 a enregistré un fort accroissement du nombre de vers exploitant les différentes plateformes Web 2.0. Le rapport se réfère aux données enregistrées entre janvier et juin 2010 et aboutit à la conclusion que les réseaux 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 même temps, les pirates s'attachent à se faire passer pour des sites tels que PayPal et eBay. Enfin, le volume du spam pharmaceutique (de type Viagra) représente aujourd'hui les deux tiers du volume total du spam.

Spam et hameçonnage : tendances au premier semestre 2010

Les organismes financiers et bancaires ont été les cibles préférées des cyber-criminels, rassemblant à eux seuls 70 % du total des tentatives d' hameçonnage. Les réseaux sociaux ont également été soumis à rude épreuve, car ils constituent une mine d'informations personnelles et de données susceptibles d'être utilisées pour le lancement d'attaques ciblées. Au cours de la première moitié de 2010, les pirates ont consacré leurs efforts à usurper l'identité des entreprises PayPal et eBay. La banque HSBC arrive en troisième position, tandis que Poste Italiane et EGG occupent les derniers rangs de la liste des entités les plus corrompues en ligne.

Le Top 10 des cibles de hameçonnage entre janvier et juin 2010



La coupe du monde de football (FIFA World Cup™) et les glissements de terrains qui ont affecté le Guatemala sont deux des nombreux événements utilisés pour optimiser le référencement Black-Hat SEO et améliorer la position des sites web diffuseurs de malwares. Cette période a également vu la quantité de spam atteindre 86 % de l'ensemble du trafic de courrier électronique, le spam pharmaceutique arrivant en tête, atteignant de nouveaux sommets, en passant de 51 à 66 % de l'ensemble des envois de spam.

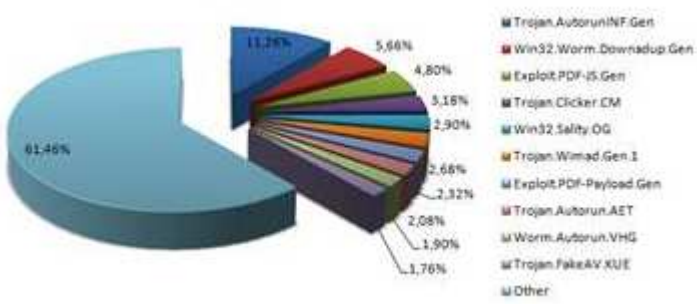
Répartition du spam par catégorie au cours du premier semestre 2010 :

- Médicaments divers – 66 %
- Produits contrefaits – 7 %
- Prêts et assurances – 5 %
- Malware empaqueté – 3,5 %
- Casinos et jeux d'argent – 3,5 %

Statistiques des menaces de type malware

Trojan.AutorunINF.Gen, qui exploite la fonction Autorun de Windows®, arrive en tête du classement, totalisant plus de 11 % du nombre total d'infections, tandis que les vers MBR ont fait leur retour après actualisation de leurs mécanismes d'infection virale. La fin janvier a aussi vu l'émergence de Win32.Worm.Zimuse.A, associant virus, rootkit et ver. Au moment de l'infection le ver commence à compter les jours. Quarante jours après l'infection, il efface le Master Boot Record du disque dur, rendant ainsi le système d'exploitation incapable de démarrer. La Chine et la Fédération 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



Vulnérabilités, « exploits » et brèches de sécurité

De dangereux « exploits » de type zero-day, profitant des failles de sécurité de logiciels aussi courants que le navigateur Internet Explorer de Microsoft®, Adobe® Reader®, Adobe® Flash Player® et même Adobe® Photoshop® CS 4. Certains « exploits » d'Internet Explorer ont même été utilisés dans des attaques à l'encontre de sociétés aussi importantes que Google®, Adobe® et Rackspace®.

Prévisions concernant les e-menaces

Les experts de BitDefender sont préoccupés par le fait que, alors que les six premiers mois de 2010 ont été marqués par des menaces classiques de type chevaux de Troie ou vers, de

nombreux types d'exploits visant des applications tierces ont rapidement gagné du terrain ces derniers temps. Comme on a pu le voir dans le cas de Exploit.Comele.A, les vulnérabilités « zero-day » peuvent être utilisées à des fins qui vont au-delà du vol d'identité ou de coordonnées bancaires, mais aussi pour mener de véritables « cyber-guerres » et mener des actions d'espionnage industriel.

« Au moment où Facebook® atteint 500 millions d'utilisateurs, la plupart des auteurs de malwares s'intéressent à ce réseau pour y déployer leurs plus récentes trouvailles en terme d'attaque. Certaines d'entre elles vont consister à utiliser des astuces d'ingénierie sociale et d'autres vont tenter d'exploiter les différentes vulnérabilités ou fonctions déjà présentes sur la plateforme », indique Catalin Cosoi, Directeur du Laboratoire d'étude des menaces en ligne BitDefender.

Les experts de BitDefender pensent également que la divulgation d'informations personnelles va beaucoup contribuer à la réussite d'attaques variées, notamment quand les données recueillies sont confirmées sur des blogs personnels, dans des C.V. et autres références du même ordre. On peut également s'attendre à ce que des applications tierces jouent un rôle important dans les abus ciblant les réseaux sociaux.

« L'arrivée de HTML5, la prochaine révision importante du HTML classique, va apporter des niveaux supplémentaires 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 exploitée par les auteurs de malwares pour compromettre la sécurité des navigateurs » a ajouté Mr Cosoi.

À propos de BitDefender®

*BitDefender est la société créatrice de l'une des gammes de **solutions de sécurité** les plus complètes et les plus certifiées au niveau international, reconnues comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les **solutions de sécurité** BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Plus d'informations sur BitDefender et ses solutions sont disponibles via le **Centre de presse**. Retrouvez également sur le site **www.malwarecity.fr** les dernières actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.*

À propos des Editions Profil

Editions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Editions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la

protection des données en général. Editions Profil édite notamment les solutions de sécurité BitDefender et de contrôle parental Parental Filter 2, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.