



Le jeudi 15 janvier 2009

BitDefender publie son rapport sur l'état des e-menaces

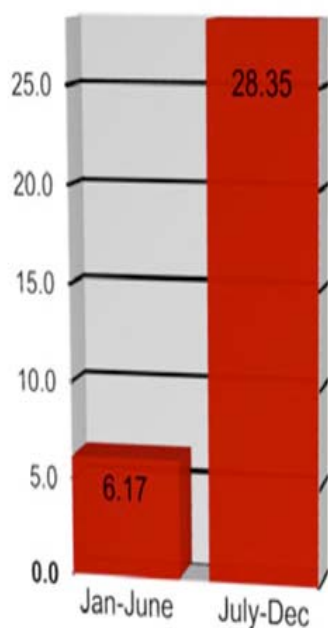
Les principales e-menaces au second semestre 2008

BitDefender®, l'un des fournisseurs les plus récompensés de solutions antivirus et de sécurité des données, publie son rapport sur les principales e-menaces au second semestre 2008, ainsi que ses prévisions pour l'année 2009.

Les tendances observées par les Laboratoires BitDefender dans leur précédent rapport sur les e-menaces (E-threats Landscape Report) montraient que les créateurs de malwares se consacraient principalement à produire et à diffuser des chevaux de Troie ainsi qu'à exploiter les vulnérabilités système. Les utilisateurs d'Internet ont dû faire face à l'apparition et à la mutation d'environ 2 000 virus par jour, et à presque 50 000 tentatives de phishing par mois. On compte plus de 1 000 000 d'ordinateurs contrôlés à distance par des pirates et qui diffusent des bots, des rootkits, des chevaux de Troie et autres types de malwares cette année.

Le monde de la sécurité IT a été confronté, au cours des six derniers mois de 2008, à différents types de menaces, dont les principales sont présentées ci-dessous.

Plus de 80% des malwares transmis dans le monde appartiennent encore à la catégorie des chevaux de Troie.



La diffusion de malwares via des sites Web infectés a été multipliée par 4,59 entre le premier et le second semestre 2008.
Source: les laboratoires antiMalwares BitDefender

¾ des chevaux de Troie intègrent déjà des mécanismes de mise à jour élaborés, la capacité de télécharger et de transmettre furtivement des données et la possibilité de diffuser des spywares ou des rootkits.

Le volume de menaces issues du web a augmenté de 460%.

Les exploitations de failles JavaScript via injections SQL ont triplé.

Les thèmes les plus utilisés pour la diffusion d'e-menaces au cours du deuxième semestre étaient : la supposée volonté des Etats-Unis d'envahir l'Iran, les Jeux Olympiques de 2008 et les élections américaines.

Le texte simple continue d'être le format préféré pour l'envoi de spam par e-mail ; il a été utilisé dans 80% des cas fin 2008, contre seulement 1,5% pour le spam-image.

Le nombre d'e-mails non sollicités contenant des fichiers joints infectés ou des liens vers une page où l'on demandait à l'utilisateur de télécharger un malware a augmenté de 400%.

5% du spam lié à des tentatives de phishing comprenait des pièces jointes au format HTML destinées à voler des données confidentielles via des scripts PHP (contre 1% au premier semestre 2008).

Afin d'augmenter l'efficacité du spam, les spammers ont concentré leurs efforts sur les mécanismes confirmant la réception des messages envoyés.

Les spams les plus diffusés ont été :
Médicaments et autres drogues (« Viagra ») 49%
E-mail contenant une pièce jointe infectée 10%
E-mail de phishing 9.50%



Vente de contrefaçon 7%
Pseudo prêts financiers – 6.50%

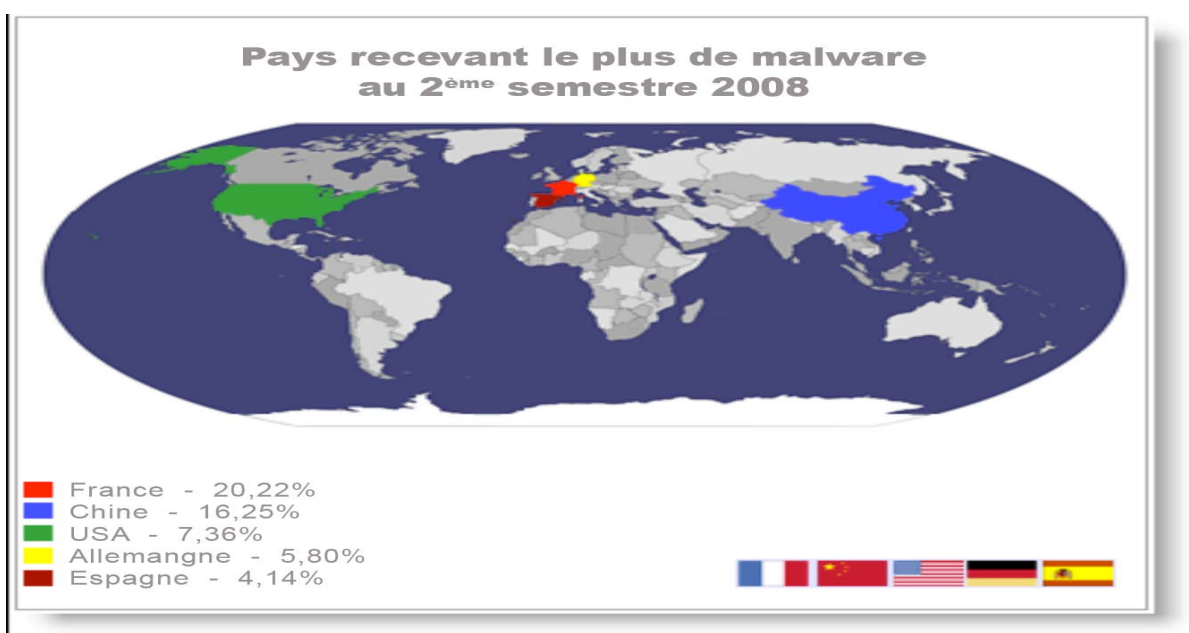
Fin 2008, environ 70% des tentatives de phishing faisaient référence au contexte financier international.

Les établissements bancaires dont l'identité a été la plus souvent usurpée sont : Bank of America, Chase Bank, Citibank, HSBC et Halifax Bank.

Le 3ème semestre a été marqué par l'apparition de spam imitant la présentation de newsletters et de messages provenant d'agences de presse comme CNN, CBS ou ABC.

Le phishing ayant pour cible ou sujet les sites de réseaux sociaux a augmenté à la fin de l'année.

Les pays les plus touchés par les malwares au second semestre 2008 sont : la France, la Chine, les Etats-Unis, l'Allemagne et l'Espagne (voir carte ci-dessous) :



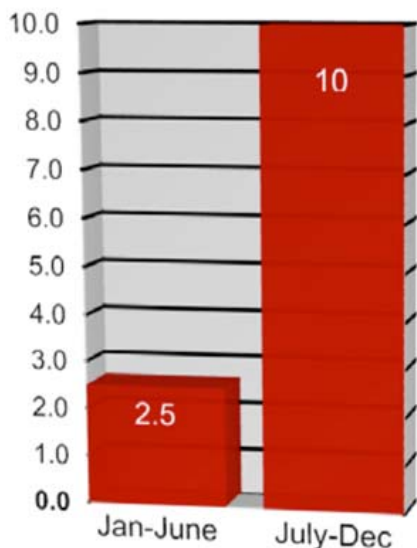
Prévisions 2009 pour les e-menaces

Presque 45% des e-menaces dans le monde sont transmises exclusivement par e-mail ou dépendent de ce mode de diffusion dans une certaine mesure. Dans ce contexte, sécuriser les communications par e-mail devrait devenir une priorité en 2009.

En 2009, la production de malwares continuera probablement sur une courbe ascendante et exploitera les capacités Web intégrées par les chevaux de Troie, les spywares et les rootkits. On a observé fin 2008 une augmentation de 460% du nombre d'infections sur Internet et de 400% du nombre de SPAM diffusant des chevaux de Troie. Il est certain que de nombreuses familles d'e-menaces connaîtront d'importantes mises à jour et de mutations en termes de furtivité et d'automatisation des mécanismes de diffusion.



L'année 2009 exploitera également les vulnérabilités des applications, comme le montre la détection récente d'un programme de détournement de mots de passe que les chercheurs BitDefender ont identifié début décembre. Dissimulé sous la forme d'un plugin pour Mozilla® Firefox® « Trojan.PWS.ChromeInject.A » récupère les données envoyées par les utilisateurs vers plus de 100 sites bancaires en ligne.



Le volume de spam diffusant des chevaux de Troie a augmenté de 400% au deuxième semestre 2008.

Source: Laboratoires antiMalwares BitDefender.

Il convient de prêter une attention particulière au nombre croissant de sites Web 2.0 et à leur développement rapide. En 2009, les applications Web 2.0 les plus visées par les malwares demeureront les réseaux sociaux. Fin 2008 a vu l'apparition de « Win32.Worm.KoobFace.A » qui touchait à la fois les utilisateurs de Facebook® et ceux de MySpace™.

Dernière menace et non des moindres, il est probable que les smart phones et autres appareils 'intelligents' ayant un accès permanent à Internet seront en 2009 la cible des nouvelles générations de malwares pour plateformes mobiles.

Pour consulter le rapport complet (en anglais) [cliquez ici](#)

À propos de BitDefender®

BitDefender est la société créatrice de l'une des gammes de solutions de sécurité la plus complète et la plus certifiée 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.com 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

Éditions 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. Éditions 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. Éditions Profil édite notamment les solutions de sécurité BitDefender et Parental Filter, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.