



Communiqué de presse

Une nouvelle étude des laboratoires de sécurité Websense indique que 75 % des sites malveillants correspondent à des sources fiables et légitimes **NOUVELLE ÉTUDE : Les sites Web 2.0 et « légitimes » sont le dernier terrain de jeu des hackers s'adonnant au vol d'informations**
avec une « bonne » notation de réputation

Paris, le mercredi 30 juillet 2008 - Websense, Inc. (NASDAQ : WBSN)

Faits marquants :

- **60 % des 100 premiers sites Web, en termes de popularité, ont hébergé du contenu malveillant ou ont redirigé vers un site malveillant de manière masquée pour leurrer les utilisateurs sans méfiance, [selon une nouvelle étude que viennent de publier les laboratoires de sécurité Websense™](#). Les [100 premiers sites Web en termes de popularité](#), dont une grande partie sont des sites de réseaux sociaux, Web 2.0 ou de recherche, représentent la majorité de toutes les pages Web affichées et constituent des cibles privilégiées pour les hackers. En raison de leur vaste audience, leur bonne réputation et la prise en charge des applications Web 2.0, ces sites offrent aux créateurs de code malveillant de nombreuses possibilités.**
- **Plus de 45 % de ces 100 premiers sites Web permettent à l'utilisateur de générer du contenu.**
- **Au cours du premier semestre 2008, plus de 75 % des sites Web que Websense® a classés comme malveillants étaient en fait des sites de « bonne » réputation en apparence qui avaient été compromis par des hackers. [Cela représente une hausse de 50 % par rapport au second semestre 2007.](#)**
- **Les laboratoires de sécurité Websense ont découvert que 29 % des attaques Web malveillantes présentaient du code de vol de données, ce qui prouve que les hackers s'intéressent aux informations et données essentielles.**
- **La convergence des menaces Web et email combinées continue de progresser. Les laboratoires de sécurité Websense signalent que plus de 76,5 % de tous les emails en circulation au cours des six derniers mois contenaient des liens vers des sites de spam et/ou des sites Web malveillants. Cela représente une augmentation de 18 % depuis décembre 2007.**
- **Les laboratoires de sécurité Websense utilisent la technologie [ThreatSeeker™ Network](#) de Websense (brevet en instance) pour identifier, classer et contrôler les menaces Internet et les tendances globales. [ThreatSeeker™ Network](#) assure une veille Internet pour les chercheurs en sécurité, ce qui englobe plus de 50 millions de systèmes collecteurs de données en temps réel qui analysent chaque jour plus d'un milliard de contenu, pour déceler des tendances et protéger les entreprises.**

Tags / Mots-clés :

Laboratoires de sécurité Websense, Web 2.0, sécurité, Web, réseau ThreatSeeker, code malveillant, sécurité Internet, veille sur les menaces, protection des informations essentielles, protection des données, AV, IDS, IPS, recherche en sécurité

Liens / URL :

- PodCasts :
 - PodCasts des laboratoires de sécurité :
 - David Saunders, Directeur de recherche en sécurité des emails chez Websense, présente les dernières menaces et tendances en matière de messagerie : http://securitylabs.websense.com/content/Assets/DS_jul08.mp3
 - Autres PodCasts connexes :
 - PodCasts du SC Magazine : Super Cybercrime avec le CTO de Websense, Dan Hubbard : http://podcasts.scmagazine.com/show/2_2008-01-28T14_46_20-08_00
- Chaîne YouTube Websense : <http://www.youtube.com/user/WBSNMKTG>
- Del.icio.us : <http://del.icio.us/informationprotection>
- Livre blanc sur le réseau ThreatSeeker du laboratoire de sécurité Websense : <http://www.websense.com/welcome/MiscLandings/ThreatSeekerNetwork/index.php>
- Présentation des laboratoires de sécurité Websense pour CanSec 2008 : « Web-Wreckutation » http://securitylabs.websense.com/content/Assets/websense_cansec_2008.pdf
- Site des laboratoires de sécurité Websense : <http://securitylabs.websense.com/>

Vidéo YouTube

<http://fr.youtube.com/watch?v=yDcsBU2eAmk>

Citations :

- « Aujourd'hui, les hackers délaissent carrément la création de leurs propres sites malveillants et ciblent des sites Web légitimes ayant déjà une base constituée de visiteurs. Dans le paysage Web 2.0, on croit que les sites Web fréquentés chaque jour sont sûrs, mais les hackers exploitent leur bonne réputation pour lancer des attaques. La plupart des technologies actuelles de sécurité Internet et de filtrage d'URL reposent largement sur la réputation des sites Web, mais ce procédé est dépassé. En termes de sécurité, l'URL ne revêt plus d'importance, tout réside dans le contenu dynamique servi par la page. Désormais, pour utiliser Internet en toute sécurité, les entreprises ont besoin d'une solution de protection pouvant analyser le contenu d'une page Web en temps réel », explique Dan Hubbard, Directeur technique (CTO) de Websense.
- Pour Tim Lawrence, analyste en sécurité informatique chez AutomationDirect, « les sites Web légitimes auxquels notre personnel peut tenter d'accéder à des fins professionnelles s'avèrent de plus en plus compromis par des hackers, c'est pourquoi la recherche sur les dernières menaces et la protection Internet fournies par Websense sont cruciales pour notre entreprise. En tant que client de Websense, je sais que notre personnel et nos informations vitales sont protégés contre les dernières menaces Internet et que l'utilisation de sites Web et Web 2.0 ne présentent aucun risque ».

Images disponibles :

- Image : [le paysage Web tel que vu par Websense](#)
- Image : [exemple d'un mixage Web 2.0](#) ; l'URL ne revêt plus d'importance, tout réside dans le contenu de la page
- Image : [Dan Hubbard](#), CTO de Websense

Fils RSS de l'actualité Websense : [Tout le flux RSS de l'actualité Websense](#)

Fils RSS des alertes des laboratoires de sécurité Websense :

<http://securitylabs.websense.com/content/alertsRSS.xml>

Fils RSS du blog des laboratoires de sécurité Websense :

<http://securitylabs.websense.com/content/blogsRSS.xml>

À propos de Websense, Inc.

Websense, Inc. (NASDAQ : WBSN), leader mondial des technologies intégrées de sécurité Web et de protection des courriels et des données, offre l'Essential Information Protection™ à plus de 42 millions de salariés dans plus de 50 000 entreprises du monde entier. Distribués au travers d'un réseau mondial de partenaires, les logiciels et les solutions de sécurité hébergées Websense aident les entreprises à bloquer les séquences de code malveillantes, à éviter la perte d'informations confidentielles et à mettre en vigueur des règles de sécurité et d'accès Internet. Pour en savoir plus, consultez www.websense.com.

Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.