

COMMUNIQUÉ DE PRESSE

Websense offre la protection la plus aboutie du marché contre les cybercriminels exploitant les services de raccourci d'URL

La passerelle Web sécurisée classifie en temps réel les contenus spécifiques des pages Web afin que les entreprises puissent tirer parti des avantages du Web 2.0, avec une protection immédiate contre les menaces et le contenu inapproprié

Paris, 31 août 2009. Websense, Inc. (NASDAQ : WBSN) confirme que ses solutions de sécurité des contenus fournissent une protection poussée contre le nombre croissant des raccourcis d'URL, utilisés et partagés sur les sites de réseaux sociaux comme Facebook et Twitter et dans les commentaires de blog.

Contrairement aux autres solutions de sécurité Internet qui reposent essentiellement sur des signatures antivirus pour détecter un programme malveillant, Websense propose une fonction inédite et exclusive dans [Websense® Web Security Gateway](#). Si un raccourci d'URL conduit l'utilisateur vers un site Web 2.0 comportant du contenu dynamique, Websense Web Security Gateway analyse en temps réel le contenu de cette page et autorise l'utilisateur à y accéder si le contenu est réputé sans risque et approprié, ou empêche l'utilisateur de visiter la page si tel n'est pas le cas. Websense Web Security Gateway est la seule passerelle de sécurité Web capable d'analyser les propriétés de contenu Web 2.0 en temps réel selon plus de 90 catégories.

« Depuis des années, les solutions de sécurité Internet Websense protègent les utilisateurs contre les URL qui tentent de les rediriger vers des sites Web malveillants », déclare Bill Gardner, Senior Director, en charge du marketing technique de Websense. « Nombre de sites Web 2.0 actuels à usage professionnel sont des mixages de différentes applications. En outre, les sites Web 2.0 acceptent les applications tierces et le contenu créé par l'utilisateur, qui peuvent changer instantanément. Websense Web Security Gateway protège les utilisateurs contre les toutes dernières menaces, telles que les raccourcis d'URL malveillants ».

[La présentation des dangers induits par les raccourcis d'URL est disponible sur Slideshare](#)

Quelques chiffres et faits marquants

- L'utilisation de services de raccourci d'URL tels que TinyURL, Snipurl, Bit.ly et Cligs explose en raison de la popularité grandissante de Twitter, des blogs, des sites de réseaux sociaux et d'autres sites Web 2.0, qui acceptent le contenu créé par l'utilisateur et lui permettent souvent de partager des liens avec des amis, des collègues et des abonnés.
- En juin 2009, des hackers sont parvenus à exploiter une faille dans le logiciel d'édition d'URL Cligs, ce qui leur a permis de pirater 2,2 millions de liens Cligs.
- En mai 2009, les [laboratoires de sécurité Websense ont émis une alerte](#) sur le ver Koobface, qui a infecté des sites de réseaux sociaux comme Facebook, MySpace et Hi5, et qui a été disséminé au sein de réseaux d'amis avec des URL TinyURL et d'autres liens.
- Du fait de la commodité de ces services, l'usage professionnel des raccourcis d'URL se développe rapidement. La plupart des acteurs du secteur proposent désormais des outils

d'analyse gratuits qui permettent aux entreprises un suivi d'éléments importants, tels que le nombre de personnes qui ont cliqué sur les liens, leur localisation et bien d'autres données.

- Les fournisseurs de services de raccourci d'URL présentent une forte croissance. D'après des rapports de presse, [Bit.ly sert à créer 5 à 7 millions de raccourcis d'URL chaque jour, et Snipurl en a fourni 53 milliards depuis son lancement](#).
- Malgré les risques, les entreprises continuent à adopter les technologies Web 2.0 pour les multiples avantages qu'elles offrent. En fait, une étude récente de Websense menée auprès de 1300 responsables informatiques du monde entier, et baptisée [Web 2.0 @ Work](#), a révélé que 95 % des personnes interrogées autorisent actuellement leur personnel à accéder à certains sites et applications Web 2.0 et que 62 % de ces responsables estiment qu'il s'agit d'outils nécessaires à leurs activités.
- Cette même étude indique également que ces responsables informatiques sont bien moins protégés contre les menaces propres au Web 2.0 qu'ils ne le croient.

« Le volume des raccourcis d'URL et leur utilisation croissante par les entreprises ont suscité l'attention des cybercriminels car il s'agit d'un excellent moyen d'inciter un utilisateur peu méfiant à cliquer sur un lien de spam ou malveillant. L'identité des URL est masquée à l'utilisateur et on les rencontre si fréquemment sur des sites comme Twitter, les réseaux sociaux et les blogs que les internautes n'hésitent pas à cliquer dessus », explique Bill Gardner. « Sans une solution de sécurité du contenu Web 2.0 qui analyse le site vers lequel le lien tente de diriger l'utilisateur et le type de contenu de la page, en temps réel, les raccourcis d'URL malveillants vont continuer à infecter les entreprises et le grand public ».

Les solutions de sécurité Internet Websense, notamment les derniers produits Websense [Web Security](#) et [Web Filter](#) version 7, offrent une protection contre les raccourcis d'URL. Lorsqu'un utilisateur clique sur un raccourci d'URL, la technologie Websense détermine si le site Web cible diffuse du spam ou un programme malveillant ou enfreint les règles d'usage du Web de l'entreprise, pour la préserver de ces menaces.

A 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 44 millions de salariés 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 codes malveillants, à prévenir la perte d'informations confidentielles et à appliquer des règles de sécurité et d'accès Internet. Pour en savoir plus, consultez www.websense.com.

###

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