



LA CAMPAGNE PRESIDENTIELLE PROVOQUE L'ENVOI D'UN NOMBRE RECORD DE SPAMS POLITIQUES

Paris, le 1er octobre 2008 – SonicWALL, Inc. (NASDAQ: SNWL), le leader de la sécurisation des infrastructures réseau, annonce qu'il prévoit que plus de 5 milliards de spams à caractère politique seront envoyés aux électeurs un mois avant l'élection présidentielle, qui aura lieu le 4 novembre 2008. Depuis les élections primaires, le nombre de spams politiques a augmenté de façon considérable, et ce phénomène continuera d'augmenter jusqu'à 45 jours avant l'élection elle-même. Rien que dans les trois derniers mois, SonicWALL estime à 20 % l'augmentation du spam à caractère politique.

« Nous surveillons de très près l'évolution du niveau des spams politiques envoyés pendant la campagne présidentielle. En 2004, nous avons déjà vu juste en prévoyant l'envoi d'un milliard deux cent cinquante millions de spams, et ce avant même l'élection. Etant donné l'augmentation générale du nombre de spam, le chiffre de 5 milliards paraît légèrement sous-estimé. L'email est devenu, depuis la dernière campagne électorale de 2004, l'un des principaux moyens de communication pour les candidats briguant un mandat politique, quel qu'il soit. Les spammeurs profitent donc de l'agitation provoquée par les élections à venir. Les entreprises et les particuliers doivent mettre en place des mesures de protection contre le flot croissant de spam qu'ils recevront lors des 45 prochains jours. » déclare Andy Klein, Directeur du marketing produit chez SonicWall.

L'email politique est souvent envoyé par ou au nom d'un candidat à une fonction politique, ou également pour soutenir une cause ou une initiative. Ce type d'email a atteint son paroxysme lors de cette campagne présidentielle. Les spammeurs et autres pirates, les militants et opposants s'appuieront sur l'élection pour leurrer et atteindre leurs cibles ainsi que pour contourner les filtres anti-spam.

Selon SonicWALL, le spam politique pourrait représenter de 1 à 2 % du spam global le jour des élections et recommande donc aux entreprises et aux particuliers de bien connaître les trois types spams politiques et ainsi mieux s'en protéger :

- 1) **Le vrai spam** : utilise l'élection comme appât pour encourager l'utilisateur à ouvrir le message. Le contenu du mail n'a strictement rien à voir avec les élections. On peut inclure dans cette catégorie les sondages "en direct" conçus pour faire cliquer l'utilisateur sur un lien ou image qui le redirigera sur le site d'un spammeur, soit 90 % des spams politiques environ.
- 2) **Le spam "plaidoyer"** : un individu ou un groupe envoie un email pour défendre un point de vue. L'email politique n'est pas obligatoirement conforme au Can-Spam Act, ainsi les partis politiques spammer tant qu'ils le souhaitent. Ce type d'email représente 7 à 8 % du spam politique.
- 3) **Les attaques de type phishing** : n'importe quelle ruse visant à récupérer les données personnelles ou bancaire d'un utilisateur en se servant de l'élection entre dans cette catégorie. En 2004 est apparu le premier email de phishing s'appuyant sur la course à l'investiture : une campagne de soutien à John Kerry qui visait à collecter des numéros de cartes de crédit. Même si les autorités fédérales surveillent de très près ces "arnaques", elles continuent d'apparaître de temps à autre et représentent 2 à 3 % des spams politiques.

Pour ses prévisions, SonicWALL se base sur des études mathématiques et statistiques menées lors de plusieurs campagnes électorales. Grâce à son GRID Network qui récupère 1 milliard d'emails par jour, SonicWall sait identifier de façon dynamique les nouvelles menaces et garder les utilisateurs totalement protégés. Pour savoir comment se protéger contre le spam, le phishing et les autres menaces de messagerie, connectez-vous à www.anti-spam.sonicwall.com

À propos de SonicWALL, Inc

SonicWALL s'engage à améliorer les performances et la productivité des petites et des grandes entreprises, ainsi qu'à diminuer les coûts et la complexité d'un réseau sécurisé. SonicWALL a déjà vendu plus d'un million d'applications via un réseau international de dix mille partenaires de canal. Ainsi, des dizaines de millions d'utilisateurs du monde entier peuvent contrôler et sécuriser leurs données professionnelles. SonicWALL conçoit, développe et produit des solutions étendues de sécurisation des réseaux, d'accès sécurisé à distance, de protection permanente des données (stockage et réparation inclus), de techniques organisationnelles et de gestion professionnelle. Pour trouver plus d'informations sur l'entreprise, rendez-vous sur son site web à <http://www.sonicwall.com/>.

Safe Harbor Regarding Forward-Looking Statements

Certain statements in this press release are "forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995. The forward-looking statements include but are not limited to statements regarding the benefits of the benefits associated with the Network Security Appliance Series and the benefits of the integration of Application Firewall into the Network Security Appliance Series. These forward-looking statements are based on the opinions and estimates of management at

the time the statements are made and are subject to certain risks and uncertainties that could cause actual results to differ materially from those anticipated in the forward-looking statements. In addition, please see the "Risk Factors" described in our Securities and Exchange Commission filings, including our Annual Report on Form 10-K for the year ended December 31, 2006, for a more detailed description of the risks facing our business. All forward-looking statements included in this release are based upon information available to SonicWALL as of the date of the release, and we assume no obligation to update any such forward-looking statement.

NOTE: SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.