Cisco IronPort bloque l'attaque de grippe porcine

Issy-les-Moulineaux ? 5 mai 2009 ? Cisco IronPort Anti-Spam protège les utilisateurs contre les attaques de spam exploitant des techniques de «social engineering». En effet, durant la récente attaque « Swine Flu », Cisco IronPort Anti-Spam a bloqué les messages de spam quelques secondes après l'apparition du premier message.

Cisco IronPort Web Reputation Filters a également bloqué les sites Web vers lesquels pointaient ces messages. Cette technologie de filtrage Web à base de réputation protège les utilisateurs contre les codes malveillants diffusés par des sites Web contaminés, qui peuvent ne pas être identifiés par le filtrage d'URL classique ou l'analyse de signature.

Cisco Botnet Traffic Filters a en plus identifié et bloqué l'activité de « zombies ». Ce filtre anti-botnet permet de détecter des postes clients infectés à partir, notamment, de Cisco Security Intelligence Operations reposant sur plus d'un millier de serveurs collecteurs de menaces, et recevant des informations en provenance de 700.000 points de capture (sensors) et de 500 sources de partenaires tiers.

Rappel des faits :
§ Le 27 avril 2009, des cybercriminels ont commencé à envoyer des messages de spam concernant la grippe porcine (« Swine Flu » en anglais). Voici quelques exemples de titres de ces messages : « Swine flu worldwide », « Swine flu in USA », « US swine flu fears », « First US swine flu victims », « Swine flu in Hollywood », « Salma Hayek caught swine flu » ou encore « Madonna caught swine flu ».

§ Le vif intérêt du public pour la grippe porcine incitant les destinataires à ouvrir des messages de spam évoquant cette épidémie, les spammeurs ont donc employé ce leurre pour attirer les internautes vers de pseudo-sites pharmaceutiques.

« Outre les utilisations massives de sites légitimes comme plate-formes de distribution du malware, les pirates mettent en place des techniques simples dites de « social engineering » pour convaincre l'utilisateur de ramener la menace sur son poste de travail. Ainsi l'utilisation de thèmes porteurs dans l'actualité pousse les utilisateurs à se connecter sur les liens inclus dans les messages spam envoyés, renvoyant vers des sites les contaminant avec un logiciel espion ou les transformant en PC zombie», indique Sébastien Commérot, Responsable Marketing Europe du Sud, Moyen-Orient et Afrique, chez Cisco IronPort. « Alors que les menaces deviennent multi protocolaires par nature, Cisco IronPort aide à sécuriser les réseaux des entreprises afin de permettre à celles-ci de gagner en efficacité tout en atténuant les risques de perte de productivité et de ressources. »

Par ailleurs, au cours des semaines et mois à venir, Cisco IronPort s'attend à voir fleurir d'autres spams surfant sur les gros titres de l'actualité.

A propos de Cisco Systems

Cisco (NASDAQ: CSCO) est le leader mondial des technologies réseaux qui transforment la façon dont les gens communiquent, se connectent et travaillent ensemble. Vous trouverez davantage de renseignements sur Cisco à http://www.cisco.com. Pour des informations en continu, rendez-vous sur http://newsroom.cisco.com.