



Le rapport 2011 de Blue Coat sur la sécurité Web fait le point des nouvelles tendances de la cybercriminalité

Une protection en temps réel s'impose pour contrer les nouvelles menaces du Web toujours plus dynamiques et sophistiquées

Paris le 23 février 2011 – Blue Coat Systems, Inc. (Nasdaq: BCSI), un grand fournisseur de solutions de [sécurité Web](#) et [d'optimisation WAN](#), annonce la publication de son rapport 2011 sur la sécurité Web qui examine les comportements des internautes et les programmes malveillants auxquels ils sont le plus fréquemment exposés. Au travers de l'analyse des quelques 3 milliards de requêtes Web en temps réel que le service Blue Coat® WebPulse™ enregistre chaque semaine, ce rapport établit un panorama des nouvelles tendances d'utilisation d'Internet et répertorie les nouvelles méthodes d'attaque des cybercriminels.

« Les liens Internet dynamiques sont aujourd'hui la meilleure arme des cybercriminels et les mises à jour des classements Web sont beaucoup trop lentes quand quelques minutes suffisent aux assaillants pour tromper leurs victimes », explique Steve Daheb, directeur du marketing et vice-président senior de Blue Coat Systems. « Seule une protection en temps réel peut apporter aux internautes les garanties de sécurité qu'ils recherchent. C'est le cas du service Blue Coat WebPulse, qui sait évaluer les contenus dynamiquement et tracer les multiples niveaux d'attaques de programmes malveillants, du début à la fin. »

Voici quelques-unes des tendances d'utilisation du Web parmi les plus surprenantes que révèle ce rapport :

- **Les réseaux sociaux sont la nouvelle plate-forme de communication** : les sous-catégories les plus demandées étant, dans l'ordre, les pages personnelles/blogs, les logiciels de chat/messagerie instantanée et les applications de messagerie (e-mails). Les messageries en ligne arrivent en 17^{ème} position des requêtes Web les plus fréquentes en 2010, alors qu'elles étaient en 9^{ème} position en 2009 et en 5^{ème} position en 2008. Leur baisse de popularité se confirme et s'explique par l'adoption croissante des réseaux sociaux comme plate-forme de communication préférée des internautes.

- **L'utilisation du Web se fait plus professionnelle** : la difficulté à trouver un emploi et les problèmes financiers que continuent de subir les internautes partout dans le monde expliquent que l'utilisation récréative d'Internet laisse davantage la place à des recherches d'ordre professionnel. En 2010, Blue Coat a assisté à une baisse très nette des requêtes Web dans les catégories Rencontres amoureuses, Pornographie et Contenus pour adultes qui occupaient respectivement en 2009 les quatrième, cinquième et huitième places du Top 10 des catégories les plus demandées. En 2010, ce sont les Clips audio/vidéo, les Actualités/Médias et les Sites de références qui ont dominé ce classement.

Le paysage des menaces véhiculées par Internet continue de gagner en sophistication, avec une combinaison de techniques d'attaques, déroulées en plusieurs étapes. Voici les grandes tendances de 2010 à cet égard :

- **Les réseaux sociaux comme vecteur d'attaques** : en 2010, les cybercriminels ont abusé des relations de confiance entre amis pour infecter autant de nouveaux adeptes des réseaux sociaux que possible. Les deux types d'attaques via les réseaux sociaux les plus employées en 2010 sont le phishing et le click-jacking (détournement de clic). La recrudescence des attaques de phishing par les réseaux sociaux s'explique par la volonté d'obtenir des internautes des identifiants pouvant eux-mêmes déboucher sur d'autres données confidentielles (informations bancaires, financières, d'autres comptes en ligne) protégées par les mêmes mots de passe.
- **Le détournement de sites légitimes** : l'une des nouveautés majeures de 2010 est la migration des infrastructures d'attaques depuis les domaines gratuits vers des sites connus, à la réputation établie et en bonne place dans les classements des catégories acceptables. En piratant ainsi des sites de confiance, les cybercriminels hébergent leurs infrastructures d'attaques derrière des sites apparemment insoupçonnables.
- **L'hébergement de programmes malveillants dans des catégories Web acceptables** : de tout temps, les programmes malveillants se sont cachés dans des catégories que les règles de bonne utilisation d'Internet auraient de toute façon bloquées. Pourtant, les sites de Stockage en ligne et de Contenus ouverts/mixtes, respectivement à la seconde et à la sixième place de la liste des sites hébergeant des programmes malveillants, sont ceux qui enregistrent la plus

forte progression en 2010. Le nombre de nouveaux sites de Stockage en ligne hébergeant des programmes malveillants a augmenté de 13 % tandis que le nombre de nouveaux sites de Contenus ouverts/mixtes hébergeant des programmes malveillants a augmenté de 29 %. Ces deux catégories sont pourtant jugées acceptables dans la plupart des entreprises.

Sur la base de ces conclusions, le rapport propose aux entreprises des recommandations pour mieux protéger leurs employés et leurs données confidentielles :

- **Adopter une protection dynamique contre les programmes malveillants :** les cybercriminels utilisent des liens dynamiques pour bâtir leurs infrastructures d'attaques et ne changer ainsi que l'emplacement du livrable malveillant. Pour bloquer les programmes malveillants, les scams et les tentatives « call home » et de phishing, il faut une protection capable de réagir dynamiquement, d'évaluer les contenus nouveaux et inconnus et d'analyser les liens dynamiques qui font de plus en plus partie des attaques.
- **Privilégier les classements Web en temps réel :** les protections qui n'analysent pas les requêtes Web en temps réel et ne produisent pas de classements immédiats laissent les internautes à la merci d'attaques dont la durée de vie peut n'être que de quelques heures.
- **Moins compter sur les classements dits de réputation :** pour tromper l'ennemi, les cybercriminels piratent de plus en plus des sites légitimes ayant bonne réputation et les utilisent pour héberger leurs infrastructures d'attaques. Une protection qui se baserait uniquement sur les classements de réputation expose ceux qui l'utilisent à ce type d'attaques.
- **Protéger aussi les utilisateurs distants :** l'ubiquité d'Internet impose une sécurité Web fonctionnant partout, 24h/24 et 7j/7.
- **Limiter les pertes de données pilotées par des programmes malveillants :** aucune politique de gouvernance, ni aucune prévention automatisée ne mettra fin aux pertes de données provoquées par des programmes malveillants. Les entreprises doivent donc se doter d'une protection Web dynamique, capable d'identifier les serveurs d'origine, de bloquer leurs requêtes et d'empêcher que des données leur soient envoyées.



Pour en savoir plus sur l'évolution des menaces véhiculées par le Web et comment les contrer, téléchargez la version intégrale du rapport à partir de :

www.bluecoat.com/doc/15802.

Ce rapport se fonde sur les informations collectées par le service Blue Coat WebPulse et le laboratoire de sécurité Blue Coat Security Lab. Le service WebPulse reçoit les requêtes Web en temps réel de quelque 70 millions d'utilisateurs de tous horizons, qu'il analyse en temps réel en vue d'identifier les contenus Web nouveaux, inconnus ou en mutation, dont il communique immédiatement les renseignements à toute la communauté. Grâce aux technologies évoluées du service WebPulse, le laboratoire Blue Coat Security Lab cartographie l'écosystème Web et suit à la trace les multiples niveaux d'attaques, du début à la fin. Ainsi, Blue Coat est davantage en mesure d'établir des profils précis des nouvelles attaques et de comprendre l'évolution des tactiques des cybercriminels.

A propos de Blue Coat Systems

Blue Coat Systems Inc. est le leader technologique des environnements réseaux de distribution d'applications (ADN – Application Delivery Networking). Blue Coat propose aux entreprises une infrastructure ADN offrant la visibilité, l'accélération et la sécurisation nécessaires à une optimisation fiabilisée des flux d'informations en tout point du réseau d'entreprise. Cette intelligence applicative leur permet d'aligner parfaitement leurs investissements réseaux avec leurs impératifs stratégiques, d'accélérer leurs processus de prises de décisions et de sécuriser leurs applications d'entreprise pour renforcer leur compétitivité sur le long terme. Pour toute information complémentaire, visitez le site www.bluecoat.com.