Se protéger contre le spear-phishing

Bimal Parmar

Bimal Parmar, Faronics

Confrontées à un nombre croissant de menaces et de réglementations commerciales toujours plus strictes, les entreprises doivent constamment s'assurer que la sécurité et la conformité de leur infrastructure informatique sont suffisantes. Bien que les arnaques et entourloupes soient loin d'être récentes, leur vitesse et leur portée se sont considérablement amplifiées avec la dépendance croissante du monde vis-à-vis d'Internet, des e-mails et des médias sociaux. Plus spécifiquement, la prolifération des e-mails dans l'espace de travail a facilité la réussite des entreprises, mais elle a aussi ouvert la voie à des menaces de taille pour la sécurité.

Selon IDC, on comptait plus de 400 millions de boîtes e-mail d'entreprise à l'échelle mondiale en 2010, ce nombre continuant d'augmenter1. Il est donc maintenant quasiment impossible d'imaginer de travailler sans e-mail, et c'est peut-être pour cela qu'il n'est pas surprenant que les pirates en soient venus à utiliser les courriers électroniques comme principal vecteur d'attaque. Et alors que ces campagnes se focalisaient autrefois sur les consommateurs de faible valeur, les pirates visent désormais des cibles plus lucratives, et commencent à développer de plus en plus de tours d'ingénierie sociale pour trouver et exploiter des victimes de haute valeur.

« Si vous voulez une preuve de l'efficacité de ces attaques, regardez un peu la récente série d'infractions de haut niveau qui se sont produites, notamment celles subies par Google et RSA »

À en juger par les histoires d'actualités quasi-quotidiennes relatives aux dernières infractions à la sécurité, il devient évident que de nombreuses entreprises ont du mal à se défendre contre ces dernières attaques complexes. Si leurs pratiques de sécurité sont devenues si impuissantes, c'est notamment parce qu'elles continuent à se baser sur les technologies établies qui ne sont pas préparées pour se protéger contre ces menaces émergentes. L'un des meilleurs exemples est la technologie des listes noires. Bien que de nombreuses entreprises investissent des sommes considérables dans, par exemple, des solutions anti-virus - un logiciel à base de signatures qui maintient éloignés les logiciels malveillants connus – la sophistication croissante des cyber-menaces permet désormais aux attaquants de passer outre ces défenses, exposant ainsi dangereusement les réseaux de l'entreprise.

Le spear-phishing en est un parfait exemple. Évoluant depuis des campagnes de hameçonnage par e-mails en masse qui étaient à l'origine envoyés à plusieurs milliers d'utilisateurs dans l'espoir que certains mordraient à l'appât, les attaques de spear-phishing sont bien plus ciblées et impliquent de duper des individus particuliers d'une entreprise spécifique pour les inciter à télécharger sans le savoir un logiciel malveillant sur leur machine. Ces attaques portent leur fruit car elles envoient des e-mails crédibles et personnalisés semblant provenir d'une source digne de confiance. En effet, les statistiques de l'industrie montrent que les attaques de spear-phishing ont un taux de réussite de 19 %, un chiffre non négligeable par rapport aux 5 % de réussite des attaques de hameçonnage (phishing) standard et de moins d'1 % pour le spam2. Si vous voulez une autre preuve de l'efficacité de ces attaques, regardez un peu la récente série d'infractions de haut niveau qui se sont produites, notamment celles subies par Google et RSA. Ces incidents rappellent de manière brutale à quel point il est facile pour ces e-mails personnalisés d'éviter d'être détectés par les outils de sécurité traditionnels.

Caractéristiques d'une attaque

Contenant généralement un lien vers un faux site Web ou incitant le destinataire à télécharger une pièce-jointe dissimulant un logiciel malveillant, les e-mails de spear-phishing deviennent de plus en plus convaincants. Ils sont conçus pour être hautement personnalisés, améliorant ainsi leur authenticité et leur légitimité et augmentant la probabilité que l'individu se conforme à leur requête.

Si l'utilisateur se fait duper et télécharge un logiciel malveillant, il est probable que le pirate obtienne un accès à distance ou n'enregistre ses frappes et ne finisse par obtenir l'accès à sa machine et, plus grave encore, au réseau auquel elle est liée.

Une récente attaque illustrant à quel point les attaques de spear-phishing sont difficiles à détecter – et à quel point il est facile pour l'attaquant de réussir - a été celle portée à Google. Après avoir identifié au sein de Google un individu ayant accès à des informations de haute valeur, le pirate a simplement suivi l'activité en ligne de sa cible pendant quelques mois, rassemblé des informations personnelles via des sites de médias sociaux puis envoyé un lien Internet depuis le compte Facebook d'un ami menant à un tout nouveau logiciel malveillant. L'utilisateur, pensant ce message crédible car venant d'un ami, cliqua innocemment sur le lien. Et ce simple tour finit par laisser le pirate accéder au serveur central de Google. Non seulement cela illustre à quel point il est difficile de reconnaître une attaque, mais cela démontre aussi à quel point les réseaux d'entreprise restent vulnérables.

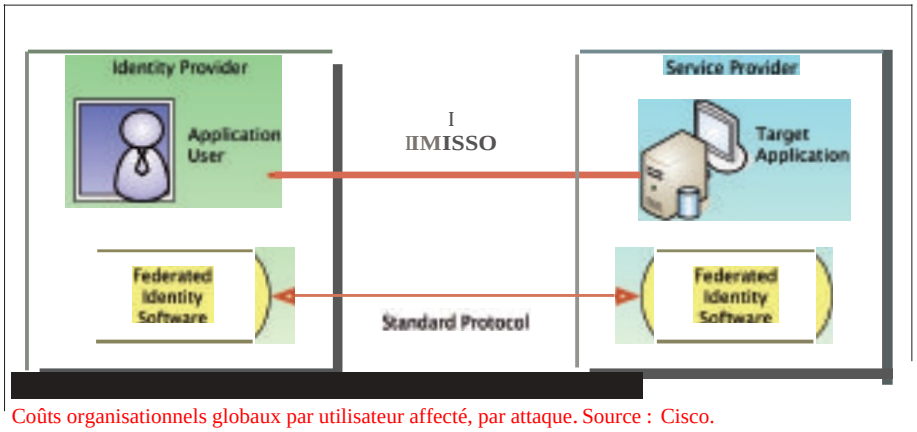
« Bien que les attaques de spear-phishing soient bien plus complexes, longues à exécuter et ainsi plus coûteuses à entreprendre, la récompense est bien plus grande »

Une popularité en hausse

Selon un récent rapport de Cisco Security Intelligence Operations (SIO),

bien que les activités de cyber-criminalité causées par des e-mails en masse aient diminué de plus de moitié au cours de l'année passée, les attaques hautement personnalisées se développent rapidement, leur nombre ayant triplé sur la même période3.

Si le spear-phishing est devenu si présent, c'est notamment parce qu'il offre un gain financier bien plus considérable que les attaques de hameçonnage traditionnel. Bien que les attaques de spear-phishing soient bien plus complexes, longues à exécuter donc plus coûteuses à



Coûts organisationnels globaux par utilisateur affecté, par attaque. Source : Cisco.

entreprendre, la récompense est bien plus grande. Dans le même rapport de Cisco, on estime que bien qu'une attaque hautement ciblée de spear-phishing puisse coûter cinq fois plus cher qu'une campagne de hameçonnage traditionnel, elle peut générer au minimum 10 fois plus de gains.

S'attaquer au point faible de l'homme

Le succès du spear-phishing est dû à un certain nombre de facteurs. D'abord, il tire avantage de la psychologie de base de l'homme. Lorsqu'ils voient qu'un e-mail semble provenir d'une source connue et fiable, telle qu'une banque, un collègue de travail ou un ami, certains individus sont inévitablement enclins à répondre, même s'ils sont bien au courant du danger des menaces pour la sécurité. Prenez, par exemple, le cas d'un employé travaillant chez le groupe d'édition international Conde Nast. Après avoir reçu ce qui semblait être un e-mail légitime de son fournisseur en impression lui demandant à ce que tous les paiements à venir soient payés sur un compte alternatif, Conde Nast a fini par envoyer près de 8 millions de dollars US sur le compte d'un escroc en seulement 44 jours.

« Les utilisateurs continuent de faire confiance aux sites de réseautage social tels que Facebook, LinkedIn et Twitter, qui détiennent d'importantes quantités d'informations personnelles et sensibles

Cet exemple est peut-être extrême, mais il illustre bien à quel point les cyber-attaques peuvent coûter cher. Les entreprises paient donc un prix élevé, les chiffres indiquant que la perte d'argent moyenne due à une cyber-attaque au Royaume-Uni s'élevait à 1,9 million de livres sterling en 2010, et cela sans prendre en compte les amendes de plus en plus importantes émises pour les insuffisances de sécurité[4]. Cela a été évident en juillet 2009 lorsque HSBC, la plus grande banque du Royaume-Uni, a dû payer une amende de 3,2 millions de livres sterling pour avoir perdu des informations confidentielles.

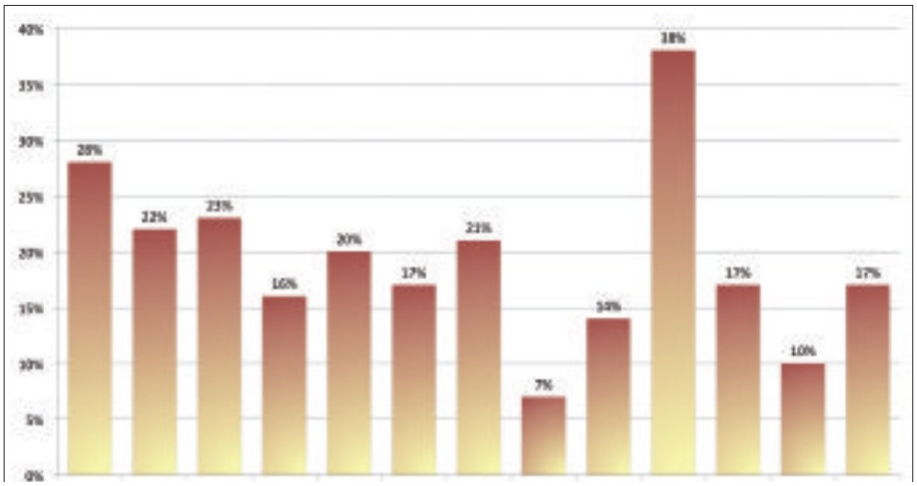
Autre défi de taille contribuant à l'insécurité globale : la prolifération des appareils mobiles. Aujourd'hui, les employés ouvrent et répondent régulièrement à des e-mails pendant leurs déplacements, avec peu d'égard pour la sécurité. Avec le nombre élevé d'e-mails reçus, et la distraction souvent plus grande en dehors du bureau, les utilisateurs sont plus susceptibles de lire un e-mail sans s'assurer auparavant qu'il ne constitue pas une menace. Dans le même temps, les limites des réseaux deviennent moins distinctes avec la croissance du télétravail et de l'utilisation d'appareils mobiles. Il n'est donc pas forcément surprenant d'apprendre que d'après le Ponemon Institute, 29 % des violations de données étaient liées à l'utilisation de téléphones portables. Ce manque d'attention vis-à-vis de la sécurité ne fait que renforcer la nécessité de défense et de politiques de sécurité plus strictes. Les pirates exploitant les faiblesses de l'homme, ainsi que celles de la technologie, les entreprises peuvent finir par devoir dépenser des milliers de livres sterling en investissant dans les tout derniers logiciels anti-virus ou pare-feu, tout cela pour qu'ils finissent par devenir complètement redondants si un employé se fait duper en coopérant avec des cyber-criminels à son insu.

L'inconvénient des médias sociaux

Les tentatives de spear-phishing sont rendues encore plus simples avec la grande disponibilité des informations placées sur Internet, visibles par tous. Les utilisateurs continuent de faire confiance aux sites de réseautage social tels que Facebook, LinkedIn et Twitter, qui comportent d'importantes quantités d'informations personnelles et sensibles, telles que leur adresse, leur emploi, leur date de naissance et leurs hobbies. Ce type d'informations peut facilement être récolté par les cyber-criminels sans aucun savoir-faire technique et avec très peu d'efforts. Les mises à jour de statut constituent un moyen facile pour les pirates de rassembler tous les renseignements dont ils ont besoin pour rédiger un e-mail qui soit personnel et pertinent pour l'individu ciblé.

C'est exactement ce qu'il s'est passé dans le cas de la récente violation de RSA. Dans le cas en question, des cyber-criminels ont ciblé un employé des RH en lui envoyant un e-mail contenant un faux plan de recrutement pour 2011, après avoir recherché l'individu sur LinkedIn. Et bien que l'e-mail ait été placé dans le filtre anti-spam, l'employé l'a lui-même récupéré dans sa boîte de courrier indésirable, pensant qu'il y avait été envoyé par erreur, et a ensuite téléchargé la pièce jointe. Un logiciel malveillant fut alors installé sur la machine, offrant un contrôle à distance de l'ordinateur au pirate, qui n'eut plus ensuite qu'à voler librement les données sur le réseau. Bien que l'impact total de la violation de RSA n'ait pas encore été déterminé, elle pourrait potentiellement affecter plus de 100 millions d'utilisateurs, tandis que plusieurs clients importants ont depuis annoncé des violations de leurs propres systèmes suite à celle de RSA, qui, selon eux, auraient été engendrées par l'attaque contre RSA.

Cela illustre parfaitement qu'une entreprise n'est pas seulement confrontée à une perte financière, mais court aussi le risque de compromettre sa réputation et la fidélité de ses clients. Les pratiques de sécurité inadéquates ne coûtent plus simplement du temps et de l'argent aux entreprises :



Taux de détection des solutions anti-virus en cas de découverte initiale, du 20 au 22 avril 2010. Source : Cyveillance.

elles portent également préjudice à ses relations publiques, lui font perdre de futures recettes, détériorent la fidélité des clients et endommagent même le prix de ses actions. La Commission européenne devant renforcer les législations relatives à la divulgation obligatoire des violations de données dans un proche avenir, la mauvaise publicité et toutes ses répercussions auront bientôt un impact encore plus considérable.

Éducation, éducation, toujours l'éducation

Pour contrer ces menaces, les entreprises doivent davantage sensibiliser l'opinion aux dangers du spear-phishing et informer continuellement leurs clients et employés des manières d'éviter la cyber-fraude. L'éducation, ou la défense par le « bon sens », est une composante clé dans la lutte contre ces cyber-menaces. Le spear-phishing est simplement un équivalent du XXIème siècle aux entourloupes traditionnelles non technologiques telles que le vol à la tire ; donc plus un utilisateur est intelligent et malin, moins il aura de chance d'en devenir une victime.

Ce point est parfaitement illustré par l'exercice de William Pelgrin. Ce dernier, Directeur du Bureau d'Etat de la Coordination de l'Infrastructure critique et de la Cyber–sécurité (CSCIC) de New York, a envoyé un e-mail de spear-phishing élaboré avec attention à 10 000 employés de l'Etat de New York les incitant à cliquer sur un lien leur demandant d'indiquer leur adresse e-mail et leur mot de passe. Près de 15 % d'entre eux ont tenté de saisir leur mot de passe avant d'être interrompus et de recevoir une note leur expliquant qu'il s'agissait d'un exercice et qu'ils ont commis une erreur. Lorsqu'un message similaire a été envoyé quatre mois plus tard, seuls 8 % ont tenté d'interagir avec le faux site Web.

« Non seulement les terminaux sont les points auxquels bon nombre des données d'un réseau résident, mais ils peuvent aussi constituer une route directe vers le réseau tout entier d'une entreprise pour un pirate.

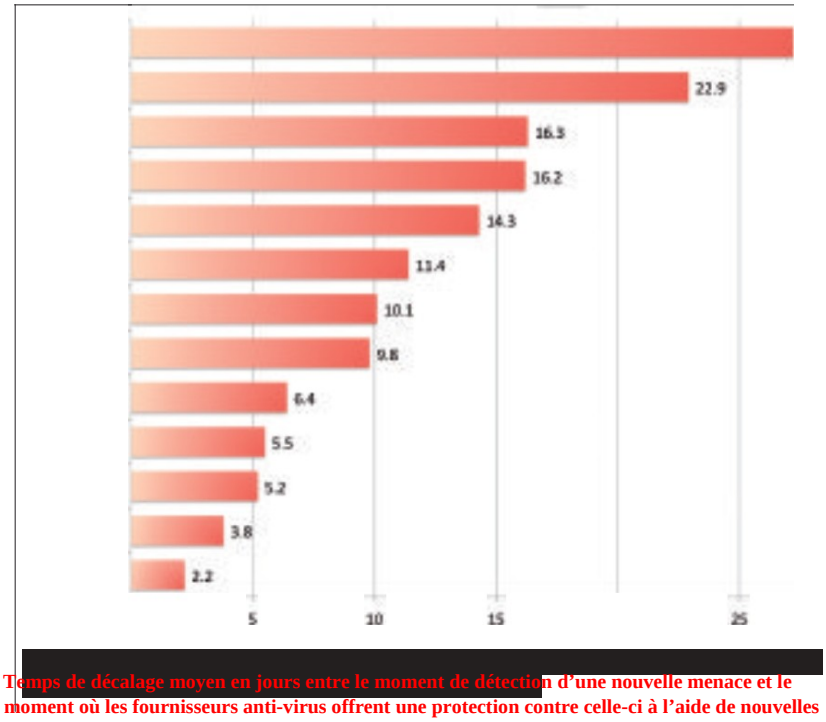
Les exercices comme celui-ci prouvent que les utilisateurs peuvent apprendre à se montrer plus vigilants. Mais le problème, c'est qu'il suffit d'un clic innocent sur un lien malveillant ou du téléchargement d'une pièce jointe infectée d'une personne non informée pour qu'une entreprise tout entière prenne le risque d'encourir de graves préjudices financiers et des atteintes à la réputation. Cela suffit à démontrer, si l'on considère aussi le fait que le paysage des menaces est en constante évolution, que l'éducation n'est pas une solution suffisante en elle-même. Les entreprises doivent aussi s'assurer d'avoir mis en place une stratégie solide de sécurité des terminaux. Non seulement les terminaux sont les points auxquels bon nombre des données d'un

11 réseau résident, mais ils peuvent aussi constituer une route directe vers le réseau tout entier d'une entreprise pour un pirate. En compromettant un seul PC, il devient possible pour lui de passer outre la sécurité de l'ensemble du réseau.

Défauts des listes noires

Bien que populaires, les solutions de listes noires traditionnelles comportent un problème : les sociétés doivent savoir exactement à quelles menaces elles font face si elles veulent pouvoir s'en protéger de manière appropriée. Connu sous le nom d'attaque du jour zéro, si le logiciel malveillant est tout nouveau, il y a fort à parier que son exécution sera autorisée et causera des dégâts avant de rejoindre la liste noire de l'éditeur anti-virus.

Les fournisseurs anti-virus estimant l'apparition de nouveaux logiciels malveillants à près de 60 000 par jour, on comprend aisément



Temps de décalage moyen en jours entre le moment de détection d'une nouvelle menace et le moment où les fournisseurs anti-virus offrent une protection contre celle-ci à l'aide de nouvelles signatures. Source : Cyveillance, 2010.

Janvier 2012

à quel point il est difficile pour les méthodes de défense traditionnelles, telles que les anti-virus, de rester à jour.

Les entreprises doivent aussi prendre en considération le fait que les logiciels malveillants évoluent constamment, leur permettant d'échapper continuellement aux technologies de listes noires anti-virus. De la même manière que l'e-mail d'une attaque de spear-phishing est personnalisé, le logiciel malveillant téléchargé est également conçu sur mesure. Lorsque l'on considère que les plus grands fournisseurs d'anti-virus ont besoin en moyenne de 11,6 jours pour reconnaître un logiciel malveillant, il peut être extrêmement dangereux de compter exclusivement sur cette solution[5]. En effet, selon un récent rapport de NSS Labs, les produits anti-virus ont manqué entre 10 et 60 % des menaces créées par des cyber-criminels, souvent parce qu'un logiciel malveillant attrapé via un point d'entée n'est pas toujours détecté lorsqu'il est introduit via un autre vecteur[6].

Une approche à plusieurs niveaux

Les technologies traditionnelles basées sur les listes noires ne constituent plus une défense suffisante face aux cyber-attaques. Les entreprises doivent plutôt s'assurer de posséder une approche à plusieurs niveaux de la sécurité des terminaux. Cela ne signifie pas que les pare-feu et les solutions anti-virus n'ont pas leur rôle à jouer, ce sont de bonnes solutions de sécurité à avoir. Cependant, ils ont des limites. Bien qu'ils soient des outils précieux contre les menaces connues telles que les virus, les vers et les chevaux de Troie, avec des menaces plus sophistiquées comme les attaques de spear-phishing qui se répandent de plus en plus, il devient essentiel que les entreprises prennent des mesures pour renforcer leurs couches de défense.

« Contrairement aux listes noires, avec les listes blanches d'applications, les fichiers malveillants n'ont pas besoin d'être attrapés une première fois, et les listes n'ont pas à attendre des mises à jour de la base de données de l'éditeur anti-virus »

Le concept d'une stratégie de protection à plusieurs niveaux, ou « défense en profondeur », est plutôt bien connu. Cependant, de nombreux responsables informatiques négligent certaines des couches de défense les plus solides disponibles : les méthodes de listes blanches d'applications et de restauration du système. Fonctionnant à l'inverse des listes noires, les listes blanches permettent aux responsables informatiques d'identifier exactement quels programmes doivent être autorisés à fonctionner, offrant une assurance supplémentaire que des virus ou logiciels malveillants inconnus ne s'infiltreront pas dans le réseau. Contrairement aux listes noires, avec les listes blanches d'applications, les fichiers malveillants n'ont pas besoin d'être attrapés une première fois, et les listes n'ont donc pas à attendre des mises à jour de la base de données des menaces connues de l'éditeur anti-virus ». Ceci est important pour la sécurité des terminaux car, contrairement aux solutions anti-virus, les listes blanches ne dépendent pas des mises à jour de définitions. Fait décisif, cela signifie que les virus en mutation et les menaces exécutables qui, en règle générale, passeraient outre votre protection anti-virus et attaqueraient vos réseaux, sont désormais stoppés par la deuxième ligne de défense. Dernier point crucial, la couche de défense est une méthode permettant la restauration des systèmes à leurs paramètres d'origine. Fondamentalement, cela permet à l'utilisateur de redémarrer son ordinateur à la seule pression d'un bouton et de supprimer tout logiciel malveillant indésirable ayant pu se faufiler à travers les autres outils de sécurité.

Dans la mesure où des cyber-attaques plus sophistiquées et ciblées et de nouveaux codes malveillants apparaissent constamment, il n'y a jamais eu de meilleure occasion pour les entreprises de mener une sérieuse évaluation des risques de leur infrastructure et de s'assurer qu'elles soient préparées à faire face aux menaces évoluées, telles que le spear-phishing. L'application d'une stratégie de sécurité à plusieurs niveaux combinant des solutions de listes noires et de listes blanches apporte une réelle valeur ajoutée, non seulement en contribuant à maintenir la productivité des employés, en minimisant les risques liés à la conformité, mais aussi en offrant le filet de sécurité suprême aux entreprises, dans le cas où un individu serait victime d'une attaque convaincante.

À propos de l'auteur

Bimal Parmar est VP du marketing chez Faronics. Fort de plus de 18 années d'expérience dans l'industrie, il supervise la gestion de tous les produits Faronics pour s'assurer qu'ils continuent de résoudre les problèmes de sécurité et d'exploitation. Faronics aide les entreprises à gérer, simplifier et sécuriser leurs infrastructures informatiques, et leur offre une solution de sécurité complète à plusieurs niveaux se composant d'une protection anti-virus, de listes blanches d'applications et d'une fonction de restauration instantanée du système.

Références

1. Erin Traudt. « Worldwide Email Usage 2010-2014 Forecast: Email Adoption Remains Despite Continued Spamming and Rise in Social Networking Popularity » (Prédictions de l'utilisation des e-mails à l'échelle mondiale entre 2010 et 2014 : l'adoption des e-mails persiste malgré la constance des spams et le gain en popularité des médias sociaux). IDC, mai 2010.

2. « Ready for some spear-phishing » (Préparez-vous à faire face au spear-phising). SearchSecurityChannel, septembre 2006. Consulté en janvier 2012. http://searchsecuri tychannel. tech target.com/feature/Ready-for-some-spear-phishing.

3. « Email attacks: This time it's personal » (Les attaques par e-mail : cette fois-ci, c'est personnel). Cisco, juin 2011. Consulté en janvier 2012. www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf.

4. « 2010 Annual Study: UK Cost of Data Breach » (étude annuelle de 2010 : le coût de la violation des données au Royaume-Uni). Ponemon Institute, mars 2011. Consulté en janvier 2012. ww.symantec.com/content/en/us/about/media/pdfs/UK_Ponemon_CODB_2010_031611.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach.

5. « Malware Detection Rates for Leading AV Solutions » (Les taux de détection des logiciels malveillants des plus importantes solutions AV). Cyveillance, août 2010. Consulté en janvier 2012. http://www.cyveillance.com/web/docs/WP_MalwareDetectionRates.pdf.

6. « Corporate Endpoint Protection Group Test Anti-EvasionQ3 2010 » (Test de groupe de protection des terminaux d'entreprise d'Anti-Evasion au T3 2010) et « Corporate Endpoint Protection Group Test Socially Engineered Malware via Multiple Attack Vectors Q3 2010 » (Test de groupe de protection des terminaux d'entreprise contre les logiciels malveillants d'ingénierie sociale via de multiples vecteurs d'attaque au T3 2010), NSS Labs, 9 mars 2011. Consulté en janvier 2012. www.nsslabs.com/company/news/press-releases/av-industry-fails-to-cover-the-basics.html.