Rapport

Prévisions 2011 en matière de menaces

McAfee® Labs™

Le paysage des menaces a connu des bouleversements considérables au cours de l'année écoulée. McAfee Labs a observé une forte augmentation de la sophistication et du ciblage des logiciels malveillants (*malwares*), ainsi qu'une hausse du volume global quotidien des menaces. Nous constatons également depuis peu une évolution importante des types de menaces visant l'iPhone d'Apple et d'autres périphériques mobiles. D'autres nouvelles sont plus réjouissantes, notamment la diminution importante des volumes quotidiens de spam dans les e-mails. Ces hauts et ces bas nous amènent à nous interroger sur l'évolution des menaces.

Fidèle à une tradition ancrée depuis plusieurs années, McAfee Labs se penche sur sa boule de cristal pour vous présenter ses prédictions en matière de menaces pour 2011 et au-delà. Nous vous conseillons vivement de tenir compte de ces avis pour vous préparer aux menaces en constante mutation que l'avenir nous réserve.

Sommaire

Exploitation des médias sociaux

L'année 2010 marque un tournant radical dans la manière dont le code et les liens malveillants sont distribués. Ainsi, en fin d'année, le taux de spam dans la messagerie électronique a atteint un taux historiquement bas, de plus en plus d'utilisateurs abandonnant les moyens de communication traditionnels « plus lents » au profit de méthodes plus immédiates telles que la messagerie instantanée et Twitter. Ce virage va totalement modifier le paysage des menaces en 2011.

« A terme, les connexions aux médias sociaux vont détrôner la messagerie électronique comme principal vecteur de distribution de code et de liens malveillants. »

Dans la mesure où particuliers et professionnels continuent à affluer vers les médias sociaux et les sites de réseau social pour communiquer et partager des données sans délai, nous nous attendons à une hausse des tentatives ciblées d'usurpation d'identité et de vol de données personnelles. A terme, les connexions aux médias sociaux vont détrôner la messagerie électronique comme principal vecteur de distribution de code et de liens malveillants. Le volume considérable des données personnelles en ligne et la méconnaissance des utilisateurs sur la façon de sécuriser ces données vont permettre aux cybercriminels de s'adonner à des usurpations d'identité et à du profilage d'utilisateurs avec une facilité déconcertante. Les attaques par phishing ciblées, ou *spear phishing*, vont se concentrer sur Twitter et les technologies similaires tant ces canaux facilitent le choix des utilisateurs et des groupes à exploiter.

Deux domaines associés aux médias sociaux retiendront également l'attention l'an prochain : les URL courtes et les technologies de localisation.

Utilisation abusive des services de raccourcissement d'URL — L'usage d'URL courtes est pertinent dans les médias sociaux ou dans d'autres circonstances. En effet, les liens courts sont plus faciles à copier ou à saisir. Le problème (et le danger) tient au fait qu'il est impossible pour les utilisateurs de savoir où ces liens raccourcis les mènent réellement tant qu'ils ne les ont pas sélectionnés... la voie royale vers une exploitation abusive. Les spammeurs se sont déjà emparés des URL courtes pour déjouer les filtres traditionnels. McAfee Labs pense que l'utilisation abusive des URL courtes va envahir toutes les autres formes de communication Internet. Nous suivons et analysons actuellement plus de 3 000 URL courtes par minute parmi de nombreuses applications de médias sociaux et la totalité des services de raccourcissement d'URL. Nous assistons à une augmentation du nombre de ces URL dans diverses activités malveillantes, telles les escroqueries et les attaques de spam. Cette fonctionnalité aura un impact considérable sur le succès des cybercriminels et des fraudeurs alors qu'ils tirent parti de l'immédiateté des médias sociaux par rapport à la messagerie traditionnelle.

Utilisation abusive des services de localisation — De plus en plus d'utilisateurs Internet, à tous les niveaux, ajoutent des informations de géopositionnement (GPS) à leur mises à jour sur les médias sociaux pour permettre à leurs amis et collègues de voir où ils se trouvent. De nombreux services de localisation offrent également des badges et des récompenses aux utilisateurs pour accroître leur popularité. Il est facile d'imaginer comment les cybercriminels et les fraudeurs peuvent potentiellement tirer parti de telles informations. Des services de positionnement tels que foursquare, Gowalla et Facebook Places permettent de rechercher, de suivre et de localiser aisément des amis ou de parfaits étrangers. La fonctionnalité de cartographie de Bing, par exemple, permet de localiser tous les tweets avec fonction GPS dans une zone déterminée. Rien de plus simple que de mettre ces données en corrélation par sujet ou domaine d'intérêt. En seulement quelques clics, les cybercriminels peuvent connaître en temps réel les expéditeurs de tweets, leur emplacement, ce qu'ils disent, quels sont leurs centres d'intérêt et quels systèmes d'exploitation et applications ils utilisent. Développer une attaque ciblée à partir des informations recueillies auprès de ces services devient un jeu d'enfant pour les pirates.

Le fait que ces services permettent à quiconque de voir et de suivre des individus et des groupes (notamment ce qu'ils aiment ou non, leurs affiliations et centres d'intérêt) et de prendre des mesures en un temps très rapide ne manquera pas de susciter un intérêt certain chez les cybercriminels et autres escrocs en 2011 et par la suite.

Equipements mobiles

Les menaces visant les périphériques mobiles sont au cœur des préoccupations du secteur de la sécurité informatique depuis plusieurs années. Nous nous attendons à ce que des attaques surviennent à tout moment, mais aucune n'a encore véritablement eu lieu. Néanmoins, McAfee Labs estime que 2011 prendra une toute autre tournure. L'an passé, nous avons observé de nombreuses nouvelles menaces visant les périphériques mobiles, mais de faible prévalence : des rootkits pour la plate-forme Android, des exploits de type « jailbreaking » (modification des droits) sur l'iPhone et l'apparition de Zeus (un célèbre cheval de Troie/réseau de robots bancaire). L'adoption massive des périphériques mobiles dans les environnements professionnels, combinée avec ces attaques et d'autres, va probablement provoquer l'explosion attendue depuis longtemps. Au vu de la fragilité historique de notre infrastructure cellulaire et de la lente progression du chiffrement, les données des utilisateurs et des entreprises courent un grave danger.

Apple

Tout professionnel de la sécurité qui navigue sur les forums InfoSec en ligne ou qui participe à des conférences sait que la plate-forme Mac OS X est une cible privilégiée des pirates de tous bords. La communauté WhiteHat (« chapeaux blancs ») a longtemps exploré cette plate-forme à la recherche de vulnérabilités. Même s'il n'a pas fréquemment été pris pour cible par des pirates malveillants — ou BlackHat (« chapeaux noirs ») — par le passé, le système d'exploitation Mac est très largement répandu. Cette année pourtant, McAfee Labs a observé des logiciels malveillants de plus en plus sophistiqués le ciblant. Nous pensons que cette tendance va progresser en 2011. La popularité de l'iPad et de l'iPhone en environnement professionnel et la portabilité aisée du code malveillant entre ces périphériques pourraient mettre en danger de nombreux utilisateurs et entreprises dès l'année prochaine.
Nous pensons que les menaces telles que la divulgation de données confidentielles et d'identité vont s'intensifier. Le manque de compréhension de la part des utilisateurs des risques de divulgation sur ces plates-formes et le peu de solutions de sécurité déployées créent un terrain propice aux activités des cybercriminels. McAfee Labs estime que les chevaux de Troie et les réseaux de robots, jusque-là assez rares, vont devenir plus courants sur les plates-formes Apple en 2011.

Applications

« En 2011, la vente effrénée de produits non sécurisés va ouvrir la voie à des attaques orientées application ciblant plus particulièrement les données confidentielles. »

Quelles que soient nos préférences en matière de plate-forme ou de périphérique, nous vivons dans un monde submergé d'applications. Le problème vient de la portabilité des applications entre les périphériques mobiles et les futures plates-formes de télévision connectée à Internet, lesquels feront des menaces provenant d'applications malveillantes et vulnérables un sujet d'inquiétude majeur en 2011. En plus du code malveillant, McAfee Labs prévoit l'apparition d'applications ciblant ou exposant les données confidentielles et d'identité. Ce danger finira par déboucher sur des divulgations de données ou des menaces par le biais de nouvelles plates-formes multimédias telles que Google TV.

A mesure que la popularité des applications contrôlant les périphériques et les environnements professionnels et domestiques augmente, celles-ci seront de plus en plus prises pour cible. Ces outils, entourés de pratiques de développement et de sécurité connues pour leur faiblesse, vont permettre aux cybercriminels de manipuler une large gamme de périphériques physiques via des applications compromises ou contrôlées. Ces attaques vont hisser l'efficacité des réseaux de robots à un nouveau niveau.

En 2011, McAfee Labs prévoit une hausse du nombre d'applications suspectes et malveillantes ciblant les plates-formes mobiles et les systèmes d'exploitation les plus répandus. Des applications mal conçues ont déjà permis la divulgation de données d'identité. Les développeurs et les responsables du marketing succomberont sans doute à la tentation d'une mise sur le marché accélérée à mesure que ces applications vont se banaliser. Les plates-formes pour lesquelles les modèles de développement et de distribution font l'objet d'un contrôle insuffisant seront particulièrement en danger. En 2011, cette vente effrénée de produits non sécurisés va ouvrir la voie à des attaques orientées application ciblant plus particulièrement les données confidentielles.

Cette année, McAfee Labs a déjà noté une progression des réseaux de robots contrôlés par des applications dans Twitter et LinkedIn. Nous pensons que ceux-ci vont devenir la norme à partir de 2011, dans la mesure où le déploiement et l'utilisation des applications se généraliseront. L'année 2011 verra-t-elle l'avènement des réseaux de robots mobiles contrôlés par des applications téléchargées ?

Quand la sophistication donne un air de légitimité

Cette année, nous avons constaté la sophistication de certaines menaces. Les logiciels malveillants « signés » qui imitent des fichiers légitimes vont se multiplier en 2011, entraînant une recrudescence des vols de clés et la progression des techniques et des outils de conception de fausses clés utilisées dans ce type d'attaque.

Les « tirs amis » (dans lesquels les menaces semblent véhiculées par des amis) venant de vers propagés sur les médias sociaux tels que Koobface et VBMania vont continuer à se répandre. Parallèlement, les réseaux sociaux vont subir un nombre croissant d'abus, si bien qu'ils finiront par prendre le pas sur la messagerie électronique en tant que vecteur principal d'attaque.

Nous prévoyons également une augmentation des attaques de type « bombe intelligente », conçues pour se déclencher dans certaines conditions uniquement. Ces menaces exigent que la victime suive le chemin d'attaque indiqué — contrecarrant les pièges à pirates, les moteurs de balayage et les chercheurs en sécurité — tout en affectant considérablement des cibles vulnérables et désignées. Face à de telles menaces, Global Threat Intelligence devra plus que jamais assurer une protection contre les attaques observées dans des circonstances spécifiques.

Les attaques personnalisées sont sur le point de devenir bien plus « personnelles ».

Survie des réseaux de robots

Comme expliqué dans la section consacrée aux applications, les réseaux de robots constituent toujours l'une des menaces les plus dangereuses et sophistiquées auxquelles McAfee Labs est confronté. Et les années à venir devraient voir l'essor des fonctionnalités d'exfiltration de données. Tout au long de 2010, nous avons constaté que les cybercriminels menaient de plus en plus d'attaques ciblées. Nous nous attendons par conséquent à ce que les réseaux de robots servent de plus en plus à soutirer des données à partir d'ordinateurs et d'entreprises ciblées plutôt qu'à envoyer du spam, comme c'est actuellement le cas. Les réseaux de robots vont également développer des fonctionnalités de collecte de données avancées et se concentrer plus fortement sur le ciblage et l'exploitation abusive des réseaux sociaux.

Les réseaux de robots subissent également des pertes. L'application de la législation à l'échelle mondiale a permis récemment de mettre à mal les réseaux de robots Mariposa et Bredolab, ainsi que certains réseaux Zeus. Les réseaux de robots continuent cependant à évoluer. Nous pensons que la fusion récente de Zeus avec SpyEye va engendrer des robots plus sophistiqués suite aux améliorations apportées d'une part aux mécanismes de contournement de la sécurité et d'autre part à la surveillance des autorités judiciaires. Les fusions et les acquisitions ont finalement fait leur entrée dans le monde des logiciels malveillants.

Les réseaux de robots qui emploient actuellement Facebook et Twitter vont se développer et inclure des sites de réseau social populaires tels que foursquare, Xing, Bebo, Friendster, etc. L'utilisation accrue de ces sites par les particuliers et les entreprises est un facteur que les cybercriminels ne peuvent ignorer. McAfee Labs prévoit également une intégration accrue des fonctions de géolocalisation au sein des réseaux de robots étant donné l'essor des fonctionnalités GPS.

Cyberactivisme

« Le cyberactivisme s'imposera comme la nouvelle forme d'expression des convictions politiques en 2011. »

Les attaques à motivation politique ne sont pas un fait nouveau. Nous en observons toutefois de plus en plus régulièrement et elles seront bien plus nombreuses en 2011. Outre les dégradations de site web, qui constituent l'activité principale des cyberactivistes, et les attaques par déni de service distribué (la dernière activité à la mode), de nouvelles formes d'attaques sophistiquées vont voir le jour. Le vol d'informations, ensuite divulguées afin de discréditer des opposants politiques, va certainement augmenter. D'autres groupes vont suivre l'exemple de Wikileaks, car les cyberactivistes clament leur indépendance de tout gouvernement ou mouvement. Que les gouvernements dirigent secrètement ces manipulations et activités est sujet à discussion, mais il est assez probable que les Etats adopteront une approche de type « corsaire ». Le cyberactivisme comme moyen de diversion pourrait être le premier pas vers une cyberguerre. Toute personne active dans le monde de la sécurité informatique, des journalistes aux chercheurs, se devra d'être vigilante afin de distinguer toute activité de cyberactivisme des prémices d'une cyberguerre.

Nous pensons que les réseaux sociaux seront utilisés plus souvent comme vecteur de cyberactivisme au cours de l'année prochaine. Tout comme la cybercriminalité est passée d'individus isolés (capables de créer des logiciels malveillants) à des groupes non structurés (capables de lancer des attaques par déni de service distribué), il faut s'attendre à ce que les groupes cyberactivistes voient leur organisation et leurs structures étendues et renforcées en 2011.

A partir de 2011, le cyberactivisme s'imposera comme la nouvelle forme d'expression des convictions politiques. Libérant la rue, les organisateurs politiques vont se tourner vers Internet pour lancer des attaques et envoyer des messages au grand jour ou en un temps record. Et comme dans le monde réel, nous pensons que les attaques des cyberactivistes vont inspirer et fomenter des émeutes et d'autres manifestations bien réelles.

Menaces persistantes avancées

La révélation en janvier 2010 du piratage de Google dans le cadre de l'opération Aurora a permis d'établir une nouvelle catégorie de menaces : les menaces persistantes avancées (*Advanced Persistent Threat* en anglais, ou APT). Celles-ci ont alimenté de nombreux débats dans le secteur de la sécurité informatique et dans la presse pendant la majeure partie de l'année. Pourtant, une grande confusion demeure sur la véritable nature de ces attaques.

Selon la définition généralement acceptée, une menace persistante avancée est une attaque de cyberespionnage ou de cybersabotage ciblée qui est menée avec l'approbation ou sous la direction d'un Etat pour des raisons autres que purement financières ou criminelles ou de manifestation politique. Toutes les attaques de cette catégorie ne sont pas hautement avancées et sophistiquées, de même que toutes les attaques ciblées très complexes et bien exécutées ne constituent pas des menaces persistantes avancées. Les motivations de l'adversaire — et non le niveau de sophistication ou l'impact — sont le principal élément distinctif entre une menace persistante avancée et une attaque cybercriminelle ou cyberactiviste.

Par exemple, le piratage de RBS WorldPay, qui a conduit au vol de 9 millions de dollars par un gang de cybercriminels d'Europe de l'Est, n'était pas une menace persistante avancée, malgré son haut niveau de sophistication et de coordination. Les menaces persistantes avancées ne sont pas lancées par un adversaire isolé. De nombreuses équipes d'attaque sont disséminées de par le monde, avec des degrés divers de capacités et d'expertise. Tout comme il existe des équipes de premier et de second rang dans la hiérarchie cybercriminelle organisée, il en va de même pour les menaces persistantes avancées. Certaines équipes ont accès à des ressources considérables (matérielles, logicielles et humaines) et disposent même de capacités de renseignement, de surveillance et de reconnaissance classiques. D'autres empruntent, volent ou achètent des outils prêts à l'emploi proposés et fréquemment utilisés par des gangs de cybercriminels et fonctionnent elles-mêmes comme des gangs, sauf en ce qui concerne le type des données qu'elles essaient d'exfiltrer de leurs cibles. Les sociétés de toutes tailles qui sont impliquées dans des activités touchant à la sécurité nationale ou à l'économie mondiale (même en périphérie, tel un cabinet d'avocats conseillant un conglomérat d'entreprises démarrant des activités à l'étranger) doivent s'attendre à devenir la cible de menaces persistantes avancées omniprésentes et permanentes visant leurs archives de messagerie, banques de documents et de propriété intellectuelle et autres bases de données.

Les auteurs

Ce rapport a été rédigé par Dmitri Alperovitch, Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget et Craig Schmugar de McAfee Labs.

A propos de McAfee Labs™

McAfee Labs est l'équipe de recherche mondiale de McAfee, Inc. Seul organisme de recherche spécialisé dans tous les vecteurs de menace (logiciels malveillants, vulnérabilités, menaces visant les environnements web, la messagerie électronique et les réseaux), McAfee Labs collecte des renseignements provenant de ses millions de sondes et de son service dématérialisé McAfee Global Threat Intelligence. L'équipe de 350 chercheurs pluridisciplinaires de McAfee Labs, présente dans 30 pays, suit l'éventail complet des menaces en temps réel, identifiant les vulnérabilités des applications, analysant et mettant en corrélation les risques et permettant des corrections instantanées pour protéger les entreprises et les particuliers.

A propos de McAfee, Inc.

Société basée à Santa Clara en Californie, McAfee, Inc. est la plus grande entreprise au monde entièrement vouée à la sécurité informatique. McAfee consacre tous ses efforts à trouver des réponses aux plus grands défis de sécurité de notre époque. A cette fin, notre société fournit des solutions et des services proactifs réputés assurant la sécurisation des systèmes et des réseaux dans le monde entier. Les utilisateurs peuvent ainsi se connecter à Internet, surfer et faire des achats en ligne en toute sécurité. Avec le soutien d'une équipe de recherche saluée par de nombreux prix, McAfee crée des produits innovants à l'intention des particuliers, des entreprises, du secteur public et des fournisseurs de services, pour les aider à se conformer aux réglementations, à protéger leurs données, à prévenir les perturbations dans le flux des activités, à identifier les vulnérabilités ainsi qu'à surveiller et à améliorer en continu leurs défenses. www.mcafee.com/fr

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

17800rpt_threat-predictions_1110_fnl_ETMG