



Série d'articles CASES : identifier les menaces

Formes d'attaque : tendances pour 2010

Pour plus de sécurité, adoptez les réflexes CASES !

Tout tourne autour de l'argent

L'argent se trouve dans la rue ou plus facilement encore sur Internet. Les monocultures et applications qui contiennent des données précieuses sont pour les cybercriminels un véritable eldorado. Faibles investissements et gros profits – Internet attire de plus en plus de criminels. La concurrence accrue réduit les marges bénéficiaires et demande des formes d'attaque toujours plus perfectionnées.

Des attaques encore inimaginables pour les experts de la sécurité il y a cinq ans font aujourd'hui partie du répertoire classique des cybercriminels. Est-il encore possible de trouver de nouvelles idées et de peaufiner les techniques des criminels ? À quoi l'internaute doit-il s'attendre en 2010 ?

Une chose est sûre : les pirates seront toujours présents, l'an prochain aussi. Les cybercriminels diversifieront leurs formes d'attaque à l'image d'une



entreprise active dans plusieurs domaines. La société de sécurité californienne Websense répertorie les attaques qu'elle classe en huit tendances pour 2010.

Formes d'attaque en 2010

Les attaques du Web 2.0, c'est-à-dire sur les réseaux sociaux d'Internet, seront plus sophistiquées et répandues. Les études réalisées en 2009 montrent une tendance nette à la propagation des spams et des attaques ciblées sur les utilisateurs de réseaux sociaux comme Facebook, Twitter, MySpace ou Google Wave. Les moteurs de recherche comme Google ou Topsy.com seront aussi

davantage la cible de cybercriminels. La raison ? Peu d'investissements pour des profits élevés. En 2009, les modèles d'action des criminels ont prospéré sur les sites Web 2.0 car les utilisateurs font preuve d'une très grande confiance tant envers ces plateformes qu'envers les autres utilisateurs de ces plateformes.

Où les criminels affluent éclatent aussi des rivalités. Les gangs qui gèrent les botnets, c'est-à-dire qui ont le contrôle d'une multitude d'ordinateurs privés et les mettent en réseau pour organiser leurs attaques, seront plus agressifs entre eux en 2010. On s'attend à ce que les pirates se

disputent les machines non protégées des utilisateurs. Ils tenteront de supprimer les programmes d'autres criminels sur une machine pour installer leur propre programme de contrôle. L'utilisateur ne remarquera même pas que des pirates se battent pour son ordinateur.

Les e-mails sont à nouveau une forme d'attaque privilégiée. Il faut s'attendre ici à des attaques très développées. Les pirates se serviront de thèmes actuels dans leurs e-mails offensifs pour inciter l'utilisateur à ouvrir l'e-mail et à cliquer sur sa pièce jointe ou sur le lien qu'il contient. C'est alors que la pièce jointe se révèle être un logiciel malveillant destiné à voler des données. Il en va de même avec les liens préparés par les criminels pour diriger les victimes vers des sites web spéciaux des pirates.

Le nouveau système d'exploitation de Windows Vista, Windows 7, sera davantage ciblé par les criminels. Les pirates essaieront de contourner le système d'avertissement des utilisateurs. Ils chercheront les failles de ce système d'exploitation. Ils exploiteront aussi mieux le navigateur Internet Explorer 8 et ses failles. D'autres navigateurs comme Mozilla Firefox ne seront pas épargnés.

Toute recherche sur Internet passe par un moteur de recherche, dont le meilleur

Attention aux cartes de vœux électroniques ! Leur envoi connaît un pic en période de Noël. Elles sont écologiques et appréciées mais comportent aussi un danger potentiel. Tant l'expéditeur que le destinataire de cartes électroniques peuvent se protéger de possibles attaques par l'application de réflexes de sécurité. Les utilisateurs ne doivent utiliser que les services de prestataires connus et dignes de confiance pour envoyer des cartes électroniques. Si un utilisateur a recours à un service payant, il doit d'abord vérifier si le site de commerce électronique est suffisamment protégé.

Traitement des cartes électroniques dans la boîte e-mail.

Les utilisateurs peuvent se réjouir de recevoir une carte mais ne doivent pas en oublier leurs réflexes de sécurité. Tous les vœux ne sont pas désintéressés. Les criminels utilisent des périodes comme Noël pour obtenir des données privées d'utilisateurs par phishing ou logiciel malveillant ou prendre le contrôle d'ordinateurs. C'est pourquoi les utilisateurs ne doivent jamais cliquer sur les liens d'un tel e-mail ou le copier dans la fenêtre du navigateur. Ils doivent saisir le lien eux-mêmes dans cette fenêtre. Mais ils doivent d'abord s'assurer qu'il s'agit d'un site digne de confiance. Si l'expéditeur d'un e-mail est inconnu de l'utilisateur, il ne doit ouvrir aucune pièce jointe avant d'avoir vérifié l'origine de l'e-mail. Pour éviter les mauvaises surprises, il est indispensable de maintenir les critères de sécurité de l'ordinateur à jour.

Types de cartes électroniques. On distingue trois types de cartes électroniques : tout d'abord, les cartes de vœux jointes à un e-mail. Une interaction de l'utilisateur est nécessaire ici pour voir la carte. Il faut cliquer sur la pièce jointe qui peut renfermer un logiciel malveillant. Autre variante : les cartes électroniques uniquement accessibles via un site Internet. Ici aussi, une interaction de l'utilisateur est nécessaire. Mais le site Internet sur lequel l'utilisateur doit se rendre est-il sûr ? Pas facile de répondre à cette question pour l'utilisateur. Troisième variante : le destinataire voit directement la carte électronique dans l'e-mail. Aucune action n'est nécessaire. L'utilisateur trouvera des conseils de sécurité détaillés pour le traitement sûr de toutes les formes de cartes électroniques sur www.cases.lu.

Abus de confiance des utilisateurs. « Les cartes de vœux électroniques ne sont pas rares, surtout en période de Noël. Mais ce n'est pas pour rien que les spammeurs ont toujours recours à leurs vieilles combines. Les utilisateurs aiment les cartes électroniques et font confiance aux grands sites spécialisés comme BlueMontain.com. Mais, même si un e-mail semble légitime, les utilisateurs doivent être prudents et ne pas cliquer sur n'importe quoi », explique Tom Steding, président de la société de sécurité Red Condor, à propos de la dernière forme d'attaque des cybercriminels par cartes de Noël électroniques falsifiées.

exemple est Google. Les utilisateurs se fient aux résultats de ce moteur. À l'avenir, une plus grande prudence sera de mise. Les cybercriminels mettront tout en œuvre pour falsifier les résultats de recherche de ces applications via des attaques ciblées, afin de diriger les utilisateurs vers de faux sites Internet.

Les smartphones, une tendance qui se poursuit. De plus en plus d'utilisateurs possèdent ce genre d'appareil. L'iPhone, particulièrement, est très populaire. Comme le jeu en vaut la chandelle partout où utilisateurs ou données précieuses se bousculent, les criminels s'activeront aussi sur ce segment du marché. Les utilisateurs se servent de plus en plus des smartphones. Les applications commerciales se multiplient et ces appareils sont utilisés de plus en plus fréquemment pour des transactions de commerce électronique. Il existe déjà plusieurs exploits pour iPhone, c'est-à-dire des programmes qui exploitent les failles ou erreurs de fonctionnement de ces smartphones. Le premier logiciel malveillant spécifique avec fonction de bot (une fonction de contrôle de l'iPhone par un tiers) a déjà fait son apparition.

Les pirates se faciliteront aussi la tâche. Pourquoi corrompre serveurs et applications si d'autres

astuces fonctionnent ? Ils achèteront simplement plus de surfaces publicitaires sur Internet pour inciter les utilisateurs à visiter leurs sites remplis de logiciels malveillants. En 2009, le site du New York Times a déjà été détourné pour une telle attaque. Les criminels y ont acheté des espaces publicitaires où ils publiaient un avertissement de virus avec renvoi vers un antivirus. L'antivirus proposé n'était pas un programme de protection mais un logiciel malveillant.

Les utilisateurs du système d'exploitation Mac doivent aussi se préparer à une année riche en attaques. Comme ils s'imaginent à l'abri des attaques avec ce système, bon nombre d'utilisateurs n'adoptent pas les réflexes de sécurité nécessaires. Ce manque de vigilance offre aux pirates, tant que leurs modèles d'action fonctionnent, un environnement optimal pour attaquer, ce dont ils ne se privent pas.

Test de connaissances : types d'attaque courants sur le Net

« Connaissez-vous les types d'attaque courants sur le Net ? Pouvez-vous en citer cinq ou dix ? Ce n'est qu'en connaissant et en reconnaissant les types d'attaques que vous pourrez vous en protéger correctement », déclare

Pascal Steichen du Ministère de l'Économie et du Commerce extérieur, qui vous propose de tester vos connaissances. Steichen sait de quoi il parle : il est responsable de la mise sur pied et du renforcement d'un système d'avertissement précoce contre les attaques pour le Luxembourg, un genre de pompier d'Internet appelé Computer Emergency Response Team dans le jargon. Avec d'autres experts du domaine de la sécurité de l'information, il est confronté quotidiennement aux failles, aux attaques sous différentes formes et à leurs implications pour les utilisateurs, les organisations et les entreprises.

La société de sécurité Version répertorie les formes d'attaque courantes, en commençant par les enregistreurs de frappe et les logiciels-espions qui surveillent les activités des utilisateurs sur leur ordinateur et interceptent par exemple les mots de passe. Les « backdoors » (portes dérobées) permettant aussi à un tiers de contrôler discrètement un système sont également citées. La liste mentionne encore les attaques sous forme d'injections SQL. Il s'agit ici d'attaques spéciales qui ciblent les sites web. Les injections SQL tentent d'exploiter le type de communication du site avec des banques de données créées. Le but des pirates est

d'avoir accès aux données ou systèmes.

Le détournement de droits d'accès spécifiques d'individus et les accès non autorisés par l'utilisation de mots de passe courants, à l'effet comparable à celui d'un pied-de-biche, comptent aussi parmi les principales formes d'attaque. Il faut encore citer les détournements non intentionnels ou ciblés de règles d'utilisation définies et l'accès illégal via des listes de contrôle d'accès peu protégées ou mal configurées. Les systèmes d'exploitation et programmes peuvent normalement limiter l'accès aux données et fonctions par des listes de contrôle d'accès. Cette protection est ici détournée.

Les « paket sniffers » interceptent des paquets de données dans les réseaux ou

surveillent même tout le réseau. Des processus automatisés testent toutes les combinaisons possibles de mots de passe pour craquer un compte utilisateur sans connaître le mot de passe. On parle ici d'attaques par force brute. Mais le vol physique de contenus précieux, la disparition de preuves d'autorisation et le contournement de processus d'authentification font également partie des principales formes d'attaque.

Les prétextes et techniques où les criminels mettent au point des scénarios pour convaincre ou manipuler l'utilisateur ou l'amener à faire certaines actions ou à divulguer des informations sont d'autres attaques aujourd'hui répandues. Connue sous le nom de Social Engineering a recours à la communication

électronique. C'est essentiellement en période de Noël que les réflexes de sécurité sont nécessaires.

Ce n'est que le 9.12.2009 que la société Red Condor, spécialisée dans la sécurité des e-mails, a publié un message d'avertissement sur les cartes de vœux électroniques. Les utilisateurs reçoivent dans leur boîte e-mail une carte de Noël qui semble venir du prestataire connu BlueMountain.com. En réalité, il s'agit d'un e-mail frauduleux. Un logiciel malveillant est caché derrière les vœux électroniques qui ont pris l'apparence pour l'utilisateur d'une carte Blue Mountain légitime. Il suffit d'un clic pour installer le logiciel sur l'ordinateur, selon les paramètres de sécurité du navigateur et de la machine de l'utilisateur.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu