LES MENACES ACTUELLES D'INTERNET

COMMENT S'EN PROTÉGER

Edition 2009/2010

Spam, virus, spyware, pharming ou autres chevaux de Troie, les menaces provenant d'Internet sont toujours plus nombreuses et insidieuses. Si certaines de ces attaques informatiques existent depuis plusieurs années déjà, les motivations qui les engendrent sont aujourd'hui bien différentes et par là-même beaucoup plus pernicieuses et difficiles à contrer.

Le piratage informatique était auparavant réalisé pour la gloire. Aujourd'hui il s'agit tout simplement de faire de l'argent. Oubliez l'image du pirate adolescent isolé dans sa chambre qui voulait se faire un nom ! Les pirates d'aujourd'hui sont déterminés à détourner des fonds. Pour ce faire les hackers appartiennent souvent désormais à des bandes de crime organisé pour le compte desquelles ils mettent en place des attaques visant à faire de l'argent facilement et à moindres dangers que le trafic de drogue ou la prostitution. Les pirates entrent en contact avec ces bandes criminelles via des forums clandestins ou des entretiens de recrutement sur des campus, louent leurs services au plus offrant. Toutes les organisations criminelles ont désormais un département "crime sur Internet". Les hackers y sont soit directement partie intégrante de l'organisation, soit employés en "free-lance".

De plus, les attaques étaient auparavant ultra-visibles. Par exemple le célèbre virus « I love you » était véritablement destiné à faire parler de lui au maximum. Dorénavant, les attaques sont discrètes et le pirate ne veut surtout pas se faire repérer. Par exemple une attaque de type phishing peut très bien ne durer que 2 heures, laissant le temps au pirate de récupérer quelques données utiles, tout en lui donnant l'assurance de ne pas se faire repérer.

Autre détail important, les attaques étaient massives et destinées à faire le maximum de dégâts dans le maximum de réseaux possibles. Encore une fois « I Love You » constitue un bon exemple de virus destiné à affecter le plus grand nombre. Aujourd'hui les attaques sont souvent ciblées, parfois au niveau d'une seule entreprise. On cherche par exemple à voler le secret de fabrication d'un fabricant ou à pénétrer dans un réseau bien particulier. Phishing, spyware, attaques de redirection de messages d'erreur : toutes ces attaques et menaces prennent souvent désormais pour cible un petit groupe d'utilisateurs ou d'entreprises.

Pour faire face à ces menaces, à ces nouvelles formes d'attaques et aux nouvelles motivations des pirates, les entreprises doivent mettre en place des solutions véritablement adaptées à l'Internet moderne, et les éditeurs et constructeurs de sécurité sont contraints à une innovation et une proactivité permanentes.

Dans ce livret il sera question de passer en revue les principales attaques sévissant actuellement sur Internet, ainsi que les différents logiciels malveillants (« malware » en anglais) employés par les pirates. Nous parlerons ensuite des solutions à mettre en place pour contrer ces fléaux du monde moderne de l'entreprise.

SOMMAIRE

LE PHISHING

Dans une attaque ***phishing*** classique le pirate crée un faux site aux couleurs d'une société commercialement reconnue, et envoie un e-mail à l'utilisateur lui demandant de se connecter à ce site, habituellement pour récupérer des informations confidentielles (par exemple les mots de passe). L'utilisateur se connecte alors sur le faux site et se fait pirater ses données.

Ce type d'attaques est favorisé par l'existence sur Internet de nombreux « kits de phishing », prêts à l'emploi et faciles à trouver, qui contiennent des outils permettant de faciliter la vie d'apprentis pirates ayant peu de connaissances techniques et souhaitant lancer facilement des attaques. Ces kits peuvent contenir un logiciel complet de développement de site Internet (pour créer le faux site ressemblant à un site légitime), ainsi que des logiciels de création de spam pour automatiser le processus d'envoi des e-mails.

Le phishing « classique » à base d'e-mail stagne actuellement, et laisse la place à de nouvelles tendances.

La plus importante est sans aucun doute le ***pharming***. Lors d'une attaque pharming, il n'y pas d'envoi d'e-mail. L'utilisateur se connecte par exemple sur le site de sa banque préférée, il est automatiquement re-dirigé de façon totalement transparente vers un site pirate, tape son code et son mot de passe (qui sont récupérés par le pirate), et ensuite se voit re-dirigé vers le bon site. Une attaque pharming est donc totalement transparente pour l'utilisateur et par là même vraiment difficilement détectable.

Ensuite, il a été constaté une forte croissance de ce que les anglo-saxons nomment le « ***spear phishing*** » ("pêche à la lance"). Il est possible de comparer ce type de phishing à une frappe chirurgicale, dans laquelle un e-mail est bien envoyé, mais de façon très ciblée, contrairement au phishing "classique". L'e-mail est dans ce cas envoyé à un groupe précis de destinataires, par exemple, les collaborateurs d'une seule entreprise, rendant ainsi le message beaucoup plus crédible. Le pirate se fait par exemple passer pour le DRH ou pour l'administrateur réseau, et demande aux collaborateurs de donner un certain nombre d'informations confidentielles (mot de passe, etc.). Ou encore, autre exemple, le pirate peut se faire passer pour un organisme réglementaire demandant à l'entreprise de révéler des informations techniques confidentielles sur un produit.

Ce type d'attaque permet ainsi aux pirates de récupérer des informations économiques ou techniques (secrets de fabrication, bilans et chiffres de l'entreprise, etc.). Le phishing tend donc aujourd'hui, comme les logiciels espions que nous détaillerons au paragraphe suivant, à être utilisé par le pirate comme un moyen de gagner de l'argent, en revendant par exemple les informations phishées à des concurrents de l'entreprise.

Enfin, l'utilisateur qui commet une simple faute de frappe (l'exemple classique était www.googkle.com) peut tres bien se retrouver sur un site dangereux qui infectera sa machine sans qu'il ne le sache. Ce type d'infection lié aux fautes de frappe de l'utilisateur est appelé ***attaque d'erreur typographique*** (***ou typosquatting***),le pirate créant un site a l'orthographe proche d'un site connu et le chargeant de codes malicieux.

D'après une étude de l'Anti-Phishing Working Group (APWG), plus du tiers des sites de phishing hostent également désormais du malware. Ainsi, l'utilisateur se fait non seulement voler ses données confidentielles, mais il télécharge aussi à son insu un logiciel espion sur son poste de travail qui continuera à lui voler ses données !

Enfin les sites relatifs à une attaque phishing ou pharming ne restent en ligne qu'un temps très court : la moyenne est désormais de 3 jours. Le pirate ne prend donc plus le risque de se faire repérer en fermant rapidement un site qui lui a permis de voler des informations confidentielles.

LE MALWARE (OU LOGICIELS MALVEILLANTS)

La plupart des logiciels malveillants modernes (ou malware en anglais) sont conçus pour aider quelqu'un à prendre le contrôle d'un poste, d'un dispositif réseau ou d'un réseau lui-même.

LES VIRUS ET VERS

Le mot "***virus***" a tendance à être un fourre-tout pour toutes les formes de codes malveillants. Cependant, en termes techniques, le virus est un code hostile qui se réplique en insérant des copies de lui-même dans d'autres codes ou documents. L'écrasante majorité des virus arrive sur les réseaux via la passerelle de messagerie. Les virus provenant de l'e-mail se présentent souvent sous forme de pièces jointes qui sont a priori des fichiers légitimes mais qui contiennent en fait des codes malicieux. Certains virus arrivent également sous forme de fichiers cryptés ou protégés, rendant leur détection très difficile par les anti-virus traditionnels. Par ailleurs, un virus a pour objectif premier de créer des dégâts sur une machine ou un réseau.

Un ***ver*** est une forme de logiciel malveillant qui se propage de lui-même. Plusieurs vers ont fait la première page des actualités ces dernières années en inondant les réseaux et en créant des dégâts majeurs. Le ver utilise une faille de sécurité pour s'installer sur un PC, puis scanne le réseau à la recherche d'autres postes ayant la même faille de sécurité. Grâce à cette méthode le ver se propage à grande échelle en quelques heures. Insidieux, ils ne dépendent pas de l'utilisateur pour se répandre, contrairement aux autres types de virus. En effet, la majorité de ces derniers attendent une action de l'utilisateur (ouverture d'une pièce jointe, lancement d'une application, redémarrage de l'ordinateur, etc.) pour se déclencher. Les vers sont eux capables de se diffuser de façon autonome. Citons par exemple le virus Explore.zip, qui est capable de repérer les clients de messagerie tels que Microsoft Outlook, puis de s'expédier lui-même à tous les membres du carnet d'adresses.

Les virus classiques sont aujourd'hui plutôt en déclin. En effet les pirates ne cherchent plus forcément à commettre des dégâts visibles ou à détruire des données, mais plutôt à récupérer des informations ou à transformer des postes en zombies (voir page 9).

LE SPYWARE

Les logiciels espions sont des applications installées sur des postes de travail, qui recueillent des informations et les envoient à des serveurs pirates externes. Il existerait aujourd'hui plus de 150 000 instances différentes de logiciels espions, ce chiffre étant en constante progression. Le spyware est véritablement devenu un problème mondial. Il serait facile de penser que des pays comme la Russie, les pays de l'Est ou la Chine soient les leaders au niveau émission. Mais détrompez-vous : la France a bel et bien rattrapé son retard en la matière. Elle se place désormais en cinquième position du classement mondial, avec environ 3% du spyware émis dans le monde.

Une première sous-catégorie extrêmement dangereuse du spyware concerne les ***keyloggers*** ou enregistreurs de frappes clavier. Ceux-ci sont capables d'enregistrer en arrière plan toutes les frappes clavier effectuées par un utilisateur.

Les pirates combinent ces keyloggers à des tâches plus sophistiquées, capables par exemple de regarder l'adresse en ligne d'une banque, enregistrer le nom de l'utilisateur et son mot de passe, et transmettre ces informations au serveur pirate, qui va ensuite les exploiter en transférant des fonds du compte de l'utilisateur piraté. Désormais, les keyloggers sont également souvent utilisés pour récolter des informations économiques sensibles. Par exemple, un keylogger placé sur la machine d'un Directeur Financier ou d'un Directeur Général pourra capter des informations financières importantes ou des données confidentielles comme un plan social concernant le personnel, ou le lancement d'un nouveau produit. Le keylogger possède un accès à toutes les applications : il est capable d'obtenir des informations sur des pages Web et interagir avec la messagerie et les bases de données.

Les ***screenloggers*** sont une variante des keyloggers : ils permettent en plus des données du clavier et de la souris d'enregistrer en simultané des captures d'écran, associant ainsi un clic clavier ou souris à un écran particulier. Ce type de code permet ainsi de contourner les systèmes de sécurité utilisés par certains sites Web, où les utilisateurs sont amenés à s'authentifier sur un clavier numérique à l'écran (méthode mise en place pour justement contourner les keyloggers…).

Une autre forme de spyware est le détourneur de navigateur (***browser hijacker***). Celui-ci va modifier les réglages du navigateur d'un poste client et rediriger les requêtes de l'utilisateur (URL mal tapées, page d'accueil et autres requêtes) vers des sites indésirables ou infectés. Un des premiers détourneurs de navigateur Web était Cool Web Search (CWS) qui redirigeait les URL invalides vers son propre moteur de recherche. Ils sont maintenant plus souvent utilisés pour générer des menaces sur la sécurité des réseaux. Par exemple, certains détourneurs de navigateur vont rediriger l'utilisateur vers une page qui va lui signifier « Attention : votre PC est infecté par un logiciel espion », et ne libérera la page que lorsque l'utilisateur aura cliqué sur un pop up qui va en fait lui installer un spyware ! D'autres vont réclamer l'achat d'un anti-spyware afin de libérer la page. Les détourneurs de navigateurs vont véritablement perturber la navigation web et induire des menaces de sécurité pour les entreprises.

LES CHEVAUX DE TROIE

Les ***Chevaux de Troie*** sont une autre forme de logiciel malveillant qui infecte une machine en se faisant passer pour une application non malveillante. Le Cheval de Troie va ensuite ouvrir une porte dérobée sur la machine infectée, se connecter à un serveur pirate externe et télécharger un ou plusieurs codes malveillants. Un Cheval de Troie peut par exemple être distribué par un site qui offre des vidéos musicales, mais qui demandent l'installation d'un codec spécial pour les lire. Lorsque l'utilisateur télécharge le codec, il récupère également sans le savoir un cheval de Troie qui s'installe en arrière-plan sur son poste.

Pour éviter la détection le cheval de Troie ne contient quasiment jamais de code malicieux. Il va s'installer et récupérer le code malicieux depuis un serveur externe, en utilisant parfois des ports réseaux différents du port 80 (le port HTTP standard). Les chevaux de Troie, à la différence des virus ou des vers, ne se propagent pas d'eux-mêmes et ont besoin d'une intervention de l'utilisateur pour s'exécuter. Cependant, la croissance exponentielle des contenus et applications Web crée des opportunités quotidiennes pour des chevaux de Troie intelligents.

La forte augmentation de ce type de logiciels malveillants est due à l'utilisation massive des chevaux de Troie dans la création et la diffusion de parcs d'ordinateurs zombies (voir page 9).

LES ROOTKITS

Une autre forme extrêmement dangereuse de logiciel malveillant est le "rootkit". Un rootkit est un morceau de logiciel qui s'attache directement au coeur du système d'exploitation du poste, afin de contourner les restrictions de sécurité du système. Le rootkit peut également avoir pour mission de camoufler les portes dérobées installées sur un poste par un cheval de Troie. Les systèmes d'exploitation reposent souvent sur des API (Application Program Interface) pour fonctionner. Par exemple l'action d'ouvrir un document est une action liée à une API. Un rootkit permet la manipulation de ces API. Ainsi, lorsque par exemple le système d'exploitation demande un document particulier, le rootkit peut potentiellement lui retourner n'importe quel autre objet. Ce niveau de contrôle est quasiment impossible à contrer et une fois le rootkit présent sur un poste, la meilleure solution est de réinstaller ce dernier.

LES RÉSEAUX DE ZOMBIES (OU « BOTNETS »)

DÉFINITION ET USAGES

Un ordinateur zombie est une machine sur laquelle est installé un code malicieux à l'insu de l'utilisateur, mais qui ne commet pas d'action malveillante à l'instant où il est installé. A l'issue de l'installation, le pirate peut demander à distance au poste infecté de réaliser lui-même une attaque ou d'exécuter tout type d'action malfaisante. Le poste infecté devient donc un véritable zombie aux ordres du pirate, et ce, à l'insu du propriétaire de la machine. Ces machines infectées sont de plus en plus souvent organisées en réseau par les pirates : c'est ce que l'on appelle les réseaux d'ordinateurs zombies (ou réseaux de robots - botnets en anglais), et il s'agit d'une des menaces les plus sérieuses pour la sécurité des systèmes d'information. Il devient alors en effet très difficile de localiser le véritable initiateur de l'attaque, d'autant plus qu'un pirate va utiliser des réseaux de zombies disséminés dans de nombreux pays.

Habituellement, le pirate contrôle les postes zombies à l'aide d'un serveur de commande et de contrôle, qui va envoyer ses ordres aux postes zombies.

Les ordinateurs zombies ont plusieurs utilités pour les hackers.

Les attaques de dénis de service distribuées
Tout d'abord, les attaques de dénis de service distribuées (DDoS) représentent une utilisation fréquente des réseaux de zombies. Ceux-ci vont attaquer en s'y connectant de façon simultanée des passerelles HTTP ou des sites Internet connus, les saturant ainsi complètement, et les empêchant donc de fonctionner normalement voire même de rester en état de fonctionnement. Cela peut résulter en des pertes de chiffre d'affaires colossales, par exemple pour des sociétés de commerce en-ligne. Il est aussi à noter que certains pirates louent leurs réseaux de robots : il est désormais possible d'attaquer son concurrent et de faire tomber son site Internet au moyen d'une attaque DDoS lancée par des zombies loués !

De même, il existe des attaques de déni de service distribuées concernant la messagerie, qui visent à déborder un relais ou un serveur de messagerie par un énorme volume de messages. Le serveur est alors obligé d'interrompre des connexions ou de refuser des e-mails légitimes.

Le spam
Ensuite les réseaux de zombies servent également souvent à envoyer du spam. Le spammeur se camoufle ainsi derrière des postes qui effectuent le sale travail à sa place. Cisco estime aujourd'hui

que plus de 80% du spam mondial proviendrait de postes zombies. Une attaque spam d'importance peut généralement utiliser des zombies éparpillés dans plus d'une centaine de pays.

Phishing
Les zombies servent également aux pirates à lancer leurs attaques phishing : les e-mails envoyant des liens vers des sites frauduleux partent ainsi de machines tierces, rendant très difficile la localisation du pirate.

Cyber-extorsion : le chantage sur Internet
Enfin, les zombies ont donné naissance à ce que la presse a appelé la cyber-extorsion : les pirates contactent les entreprises en leur demandant de payer une somme d'argent si elles ne veulent pas être attaquées par des réseaux de milliers de zombies. Ce type d'attaques et de chantage est déjà très répandu : une étude réalisée aux Etats-Unis par la Carnegie Mellon University's H. John Heinz III School of Public Policy, en conjonction avec Information Week, a par exemple démontré que 17% des entreprises ont avoué avoir été victimes de cyber-extorsion.

COMMENT DEVIENT-ON ZOMBIE ?

Les alertes virales
Le terme d'«alerte virale» s'applique plus aujourd'hui à la diffusion de vers ou de chevaux de Troie destinés à permettre aux pirates de prendre le contrôle de postes à distance qu'à la diffusion de virus à proprement parler. Les attaques virales sont toujours très virulentes et posent des problèmes de sécurité majeurs aux entreprises. En effet, une alerte se déroule en plusieurs phases :

1. Un code malicieux est détecté au niveau mondial, exploitant le plus souvent une vulnérabilité logicielle.

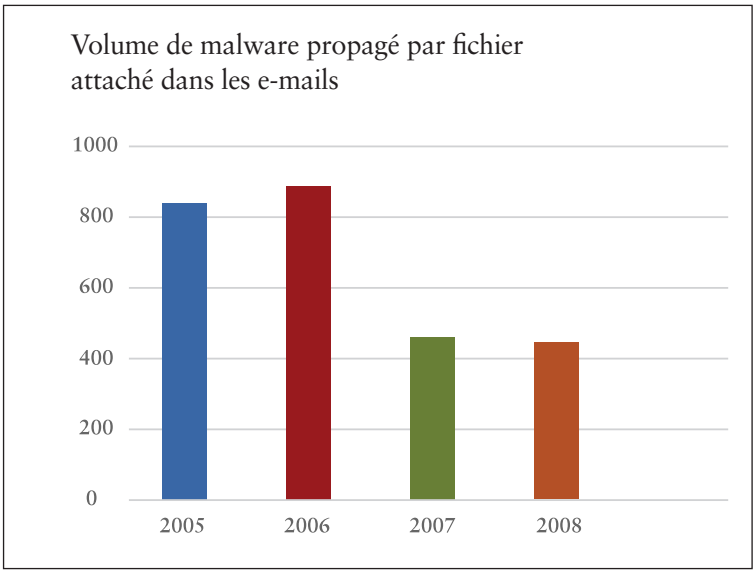
2. L'éditeur anti-virus/anti-spyware doit mettre en action ses équipes de recherche pour trouver un antidote.

3. L'éditeur anti-virus/anti-spyware doit envoyer cette nouvelle signature à sa base clients.

4. Chaque client doit déployer ses signatures.

Ainsi, entre la découverte du code malicieux, l'installation de la nouvelle base de signatures et/ou la mise en oeuvre du patch destiné à combler la vulnérabilité logicielle, si toutefois ils sont fournis, il peut se passer plusieurs heures, voire plusieurs jours. Parfois même la nouvelle base de signatures ou le patch ne sont jamais déployés. Durant cette fenêtre d'exposition les réseaux sont totalement vulnérables face à ces logiciels malveillants. Depuis 2005, l'objectif principal des codes malicieux diffusés est alors de prendre le contrôle du poste et de le transformer en zombie.

Depuis 2007 les codes malicieux diffusés par le réseau de zombies Storm, rejoint par les réseaux Kraken et Asprox en 2008, ont représenté la majorité des attaques : il s'agissait donc de diffusion de codes malicieux par des zombies, destinée à transformer d'autres postes en zombies (voir page 12).



Le volume de codes malicieux propagés par e-mail a toutefois décliné ces dernières années.

En effet, les entreprises protègent de plus en plus leur passerelle e-mail, et les pirates se tournent donc vers le Web pour diffuser leurs codes malicieux, la plupart du temps via des URL infectées.

Les alertes à l'URL

Meme si les alertes virales diffusées par un fichier attache dans un message restent majoritaires, les alertes diffusées par un lien URL contenu dans un e-mail connaissent une forte croissance depuis 2007.

Cette nouvelle technique de diffusion de malware permet aux pirates de contourner les quarantaines dynamiques ainsi que les filtres anti-virus traditionnels. Elle se présente en général sous la forme de messages spam contenant des liens qui renvoient les utilisateurs vers des sites infectés (voir aussi page 22). Ces sites téléchargent du malware sur les postes, qui deviennent partie intégrante du reseau de zombies.

DEPUIS LE RESEAU STORM : UNE NOUVELLE GENERATION DE ZOMBIES

En 2007 est apparue une nouvelle génération de réseau de zombies : le réseau "Storm". Storm a touché au total 40 millions de PC à travers le monde entre janvier 2007 et février 2008 selon les chercheurs de Cisco. A son point culminant, Storm représentait plus de 20% de l'ensemble des messages de spam et avait infecté activement 1,4 million d'ordinateurs simultanément. Il a ensuite continué d'infecter environ 900 000 machines par mois. Storm combine différentes technologies empruntées aux sites de type Web 2.0 : il est difficile à déceler, se déplace rapidement, et est dynamique tant au niveau de son périmètre que de ses actions, utilisant des techniques d'attaques mixtes mêlant e-mail et web.

Storm a par exemple été la source des attaques spam de type Excel, PDF ou MP3 (voir page 21).

Caractéristiques clés du réseau Storm

- Se reproduit – Storm nécessite une intervention de l'utilisateur pour s'étendre et repose sur une technique simple d'attaque – le social engineering, ou en français l'abus de la confiance que peut accorder un utilisateur à un message qu'il reçoit. Storm envoie automatiquement des volumes énormes de spam pour se reproduire. Ces messages contiennent des URL qui renvoient les utilisateurs qui cliquent sur les liens vers des sites infectés, où ils téléchargent de façon automatique (voir le drive-by download, page 15) un code malveillant qui exploite une vulnérabilité du navigateur web. Une fois infectés, ces postes font désormais partie intégrante du réseau Storm.

- Coordonné – Storm envoie, grâce à certains postes zombies du réseau, des campagnes de spam qui pointent vers des pages web infectées, hébergées sur d'autres postes du réseau, démontrant ainsi une extrême sophistication et coordination dans la façon qu'a ce réseau de lancer des attaques.

- Utilise le Peer-to-Peer – Auparavant, les réseaux classiques de zombies étaient gérés par le hacker grâce à un serveur de commande et de contrôle. Les réseaux utilisaient souvent des communications IRC, attendant des commandes du hacker. Toutefois, cette architecture présentait une faiblesse : bloquer l'accès au serveur de commande « coupait » en quelque sorte la tête du réseau de zombies, rendant celui-ci inefficace. Les zombies du réseau Storm sont, quant à eux, organisés de façon décentralisée, et se connectent directement entre eux en mode peer-to-peer, rendant inefficaces les mesures de protection des éditeurs de solutions de sécurité (par exemple blacklister les adresses IP des serveurs repérés de commande de zombies).

- Réutilisable – Storm peut être utilisé pour de nombreux types d'attaques : spam classique, spam de « recrutement » pour le réseau, phishing, déni de service, etc. Il a même corrompu des réseaux de messagerie instantanée et a posté du spam de blogs, le rendant ainsi menaçant pour une grande variété de protocoles réseaux. Si auparavant le malware était plutôt destiné à n'être utilisé qu'une fois, la « plate-forme malware » qu'est Storm introduit un nouveau type de design qui sera sans doute copié et perfectionné dans les années à venir.

- S’auto-défend – Pour maintenir sa longévité, Storm contient des fonctionnalités d’auto-défense. Il est capable de lancer des attaques (potentiellement automatisées) de déni de service s’il est surveillé de trop près. Storm a ainsi lancé des attaques massives contre des chercheurs en sécurité, des éditeurs de solutions ou autres organisations anti-spam.

Storm, né en 2007 et toujours actif en 2008, est devenu l’exemple type du réseau de zombies de “nouvelle génération”. Cependant, de nouveaux réseaux sont découverts en permanence, comme par exemple les réseaux Kraken et Asprox qui ont contesté la suprématie de Storm dans le domaine du piratage Internet.

Kraken a notamment compris des postes appartenant au moins à 50 des 500 entreprises les plus riches du monde, montrant par là-même que l’infection en tant que zombies ne concerne pas que les postes du grand public mais aussi ceux des entreprises les plus aguerries en termes de sécurité informatique.

En 2008, Asprox est également devenu un des réseaux de zombies les plus efficaces de l'Internet. Asprox était à l'origine un vieux cheval de Troie, utilisé dans des milliers d'attaques par injection SQL (voir page 16) pour créer un réseau ultra-sophistiqué de zombies. Un outil d'injection SQL était utilisé pour contaminer des sites Web par attaque iFrame, qui contaminaient alors les utilisateurs s'y connectant.

Des données Cisco montrent, qu'à son apogée, Asprox contaminait 31 000 sites Web différents par jour, infectant par là même des milliers de postes, se transformant alors en zombies.

Enfin, au premier semestre 2009 est apparu le réseau Conficker, autre record d'infections de l'histoire d'Internet.

Le ver Conficker a commencé à exploiter des postes vulnérables (vulnérabilité provenant de Windows) au dernier trimestre 2008, et a continué à se propager début 2009, infectant des dizaines de milliers de machines par jour.

Plus de 150 pays ont détecté des alertes à Conficker, le Brésil, la Chine et la Russie étant parmi les plus touchés. Il est rapidement apparu que le but de ce ver était la création d'un immense réseau de zombies, peut être le plus grand de l'histoire. Le réseau pouvait alors être loué pour lancer d'autres attaques spam ou malware. Le réseau Conficker reste aujourd'hui actif, même si les taux d'infection sont désormais moindres.

LES VECTEURS DE DIFFUSION DES MENACES

Durant de nombreuses années les codes malicieux sont entrés dans les entreprises via l'e-mail. A mesure que les menaces se sont développées, les entreprises se sont équipées de différents types de solutions de sécurité : anti-virus installés sur des postes clients, sur des serveurs de fichiers et de messagerie, ainsi que sur la passerelle de messagerie, solutions de mise en quarantaine dynamiques permettant de bloquer des fichiers suspects avant l'émission de signatures anti-virus, ou encore des solutions de filtrage de contenu e-mail bloquant certains types de fichiers.

Les pirates ont alors réagi en développant le vecteur d'infection Web, permettant ainsi de contourner ces solutions qui ne s'occupent que de la messagerie…

LA MESSAGERIE, TOUJOURS LA MESSAGERIE...

90% des messages électroniques envoyés dans le monde sont considérés comme étant une forme ou une autre de spam. Dans ces conditions, la messagerie électronique reste le vecteur le plus important de contamination des réseaux d'entreprise. On estime encore aujourd'hui qu'environ 80% des codes malicieux pénètrent dans l'entreprise via l'e-mail. Les virus et autres codes malicieux peuvent se présenter sous forme d'attachements, mais il est également possible de se faire infecter simplement en lisant l'e-mail ou en le pré-visualisant. Dans ce dernier cas, il s'agit de scripts automatisés qui vont infecter le poste.

LE WEB, VECTEUR EN FORTE CROISSANCE

Le Web représente désormais 20% des codes malicieux qui pénètrent dans le système d'information de l'entreprise. Ce pourcentage est en constante progression.

L'infection via le Web est souvent beaucoup plus pernicieuse que par l'e-mail. En effet lorsqu'un utilisateur reçoit un spam ou un virus via la messagerie électronique, il s'en rend parfaitement compte (même si c'est trop tard dans le cas du virus !). Dans le cadre du Web, nous parlons de spyware ou de malware qui sont par définition des menaces cachées. L'utilisateur ne sait pas que son poste a été infecté, ce qui rend d'autant plus dangereux une infection.

Alors, quelles sont les différentes façons de se faire infecter via le Web ?

Les attaques « piggyback » : un logiciel malveillant embarqué dans une application non malveillante

Dans un premier temps, le logiciel malveillant peut tout simplement être embarqué dans une autre application a priori non malveillante. Par exemple, un utilisateur télécharge une vidéo sur Internet, qui au moment de la lire lui demande de downloader un codec. L'utilisateur télécharge alors et installe le codec. La vidéo fonctionne désormais, mais l'utilisateur a sans le savoir également téléchargé et installé un logiciel espion.

Le « social engineering » qui pousse l'utilisateur à télécharger un code malicieux

Une autre forme courante d'infection sur le Web est le clic d'un utilisateur sur une publicité ou un pop-up, qui entraîne le téléchargement du logiciel malveillant. Le pirate va dans ce cas pousser l'utilisateur à cliquer sur ce pop-up, en lui proposant une offre alléchante ou une image pornographique, ou encore même en lui demandant de cliquer pour effectuer un scan anti-spyware, alors même que ce clic va déclencher le téléchargement du dit spyware !

Depuis 2008, les attaques utilisant des messages électroniques incluant des liens vers des sites diffusant du malware sont nombreuses; à chaque fois elles prennent pour prétexte un sujet chaud de l'actualité : l'élection d'Obama, la grippe H1N1, etc.

Ainsi, l'alerte mondiale autour du virus H1N1 qui a commencé en Avril 2009 est un bon exemple. Cette pandémie a aussi entraîné une alerte d'un autre genre : des volumes importants de messages spam utilisant cette grippe comme appât. Fin Avril 2009, des pirates ont commencé à envoyer des e-mails ayant pour sujet "US swine flu fears" ou "Swine flu in Hollywood." Les destinataires qui ouvraient les messages se voyaient proposer des médicaments miracles (bien entendu inexistants) ou des liens vers des sites malicieux.

Au plus fort de l'attaque, le spam relatif à la grippe H1N1 représentait à lui seul plus de 4% du spam mondial.

Le « drive-by download », ou le téléchargement automatique par exploitation d'une vulnérabilité du navigateur Web

Enfin, et ce de plus en plus souvent, ce type de téléchargement se fait sans que l'utilisateur ne voie quoi que ce soit, et sans même qu'il ne clique sur une quelconque fenêtre. Le logiciel malveillant va tout simplement exploiter une vulnérabilité du navigateur Web pour s'installer tout seul sur le poste de l'utilisateur. Cette forme de téléchargement automatique du logiciel malveillant sans aucune action de l'utilisateur et sans que celui-ci ne s'en rende compte représente désormais la majorité des infections Web. Ce « drive-by download » est désormais fréquemment couplé à des attaques iFrame ou à des injections de contenus malicieux sur des sites Web 2.0, décrites dans le paragraphe suivant.

LES INJECTIONS DE CONTENUS DANS LES SITES LÉGITIMES

Le drive-by download est d'autant plus dangereux que les infections Web ne viennent pas la plupart du temps de sites suspects. En effet, selon Cisco, plus de 87% des menaces sur le Web utilisent des sites légitimes piratés. Ce qui signifie que la plupart des logiciels malveillants ne sont pas téléchargés depuis des sites à problèmes potentiels (musique, pornographie, etc.) mais distribués à la base par des sites légitimes, utilisés comme véritables plate-formes de distribution du malware. Enfin, d'après l'étude White Hat Security (Website Sec Statistics Report), 9 sites sur 10 sur le Web sont vulnérables à une forme d'attaque !

Les attaques iFrame

Un grand nombre d'attaques visant les navigateurs Web utilisent aujourd'hui la balise HTML iFrame.

Le langage HTML est basé sur l'utilisation de balises permettant de présenter et de formater les informations, textes, images, sons, vidéos, etc. que l'on souhaite afficher sur une page Web. La balise iFrame est l'une des composantes du langage HTML utilisée pour créer des pages Web sur Internet.

Quelques-unes des balises les plus connues sont <b> pour la mise sous caractères gras, <font> pour définir les règles de présentation des caractères (taille, couleur, etc.), <script> permettant d'inclure du code script tel que JavaScript, par exemple, pour dynamiser ou ajouter des fonctionnalités aux pages, <frame> pour inclure un cadre dans la page, etc. La balise iFrame signifie inline frame et s'écrit en HTML <iFrame>. Elle est utilisée pour inclure à l'intérieur d'une page HTML un autre document HTML.

A la différence de la balise <frame> utilisée pour subdiviser d'un point de vue logique le contenu d'une page HTML en différentes pages enregistrées sur un même serveur, la balise <iFrame> est utilisée pour insérer, au sein d'une même page Web, des informations stockées sur différents sites Internet. Les concepteurs de sites ont le plus souvent recours à la balise <iFrame> pour permettre l'affichage de publicités, ces dernières étant hébergées sur des serveurs leur étant dédiés.

Le schéma classique d'une attaque iFrame respecte les étapes suivantes :

1- Un pirate, grâce à une vulnérabilité du serveur Web ou à des failles dans le code des pages, parvient à corrompre une des pages d'un site web (disons par exemple une page d'un site de diffusion d'informations en ligne, donc considéré habituellement comme un site de confiance, www.newsenligne.com). Cette corruption se fait de plus en plus souvent par une technique dite d'injection SQL, consistant à injecter des instructions (par exemple la création de la balise iFrame) en langage SQL dans des formulaires sur le site concerné. Le pirate ajoute sur une page du site une balise iFrame qui redirige les utilisateurs à leur insu vers un site contenant des contenus malveillants, géré par le pirate, disons par exemple le site www.yourspyware.com . De plus, il rend cette balise invisible à l'affichage grâce à une instruction HTML.

2- En se connectant sur ce site très fréquenté, l'utilisateur télécharge le contenu du site et l'affiche dans son navigateur Web. Si l'utilisateur consulte la page infectée par le pirate, la page envoyée au poste de l'utilisateur contient désormais la balise iFrame invisible.

3- Tandis que l'utilisateur lit la page du site newsenligne, des connexions se lancent à son insu vers le site www.yourspyware.com. Son poste télécharge alors automatiquement des logiciels malveillants, par exemple un cheval de Troie, grâce à l'exploitation de vulnérabilités dans le navigateur web.

4- Le pirate a désormais accès au poste de l'utilisateur grâce à la porte dérobée ouverte par le Cheval de Troie. Le poste peut alors par exemple faire partie d'un réseau de zombies. Ou alors le pirate peut envoyer un keylogger sur le poste qui volera des informations personnelles sur celui-ci.

Les attaquants utilisent des techniques de plus en plus complexes pour échapper aux outils de détection, par exemple en multipliant les re-directions entre le site légitime de base corrompu, et le site final distribuant le malware.

L'utilisation des sites Web 2.0

Une autre technique fréquemment utilisée est de se servir des sites Web 2.0 qui permettent aux utilisateurs de contribuer en termes de contenu sur les pages, par exemple via des forums ou des blogs. Le contenu apporté par un utilisateur peut être du texte mais également du HTML, comme par exemple des liens vers des images ou d'autres contenus extérieurs. Un pirate peut ainsi directement publier sur ce type de sites collaboratifs des liens vers des sites infectés, qui exécuteront des codes malveillants sur les machines d'autres utilisateurs. MySpace, Facebook ou encore YouTube ont été victimes de ce type d'attaques. Or, de plus en plus d'utilisateurs se connectent à ces sites depuis des postes d'entreprises, et peuvent ainsi infecter les réseaux entiers.

LA MULTIPLICATION DES APPLICATIONS EMPRUNTANT INTERNET

Lors de ces dernières années, un grand nombre d'applications véhiculées sur Internet ont vu le jour et se sont pour certaines généralisées auprès des utilisateurs du monde entier.

La messagerie instantanée
Dans la quasi-totalité des entreprises aujourd'hui, il est courant de trouver des utilisateurs en train de « chatter » au travers d'outils de messagerie instantanée du type MSN ou Skype. Via ceux-ci, il est possible de recevoir des fichiers qui, s'ils s'avèrent malicieux, peuvent infecter le réseau de l'entreprise.

Le Webmail
Un grand nombre d'utilisateurs consulte ses mails personnels provenant par exemple d'Hotmail ou de Gmail lors de leurs heures de travail, avec leur PC d'entreprise. Les mails de ces comptes de messagerie en ligne peuvent contenir, au même titre que leurs cousins de la messagerie SMTP de l'entreprise, des pièces jointes malicieuses.

Le transfert de fichiers basé sur des sites de stockage en ligne
Des sites tels que Megaupload ou encore Rapidshare se sont rapidement généralisés en tant que vecteur de transfert et de diffusion de fichiers lourds en ligne. Les fichiers téléchargés par des utilisateurs au moyen de leur PC d'entreprise peuvent s'avérer malicieux et ainsi contaminer l'intégralité du réseau.

Le Peer-to-Peer
Même s'il est combattu depuis de nombreuses années déjà dans les entreprises, le peer-to-peer (eMule, Bittorrent, etc.) est toujours largement utilisé au sein des réseaux des entreprises. Ces applications sont mêmes aujourd'hui capables de s'adapter aux mesures de blocage prises par les entreprises et les contourner.

Le trafic SSL et les applications chiffrées
Le trafic SSL, en chiffrant les communications entre un utilisateur de l'entreprise et un site Web externe, protège les données confidentielles, mais est par là même une véritable faille de sécurité au sein du réseau. En effet un malware pourra être téléchargé en toute tranquilité via une connexion SSL puisque celle-ci n'est généralement pas analysée par les filtres mis en place au niveau de la passerelle Internet. Des applications chiffrées, comme par exemple la messagerie instantanée Skype, sous couvert de protéger les communications des utilisateurs, échappent en fait à tout contrôle !

LE SPAM, DÉMULTIPLICATEUR D'ATTAQUES

UN JEU DU CHAT ET DE LA SOURIS

Il n'existe pas de définition officielle du mot « Spam ». Le mot est, à l'origine, une marque anglaise de jambon en boîte de faible qualité vendu en conserve (SPAM étant la contraction de SPiced hAM ou jambon épicé en anglais). Ce sont les Monthy Python, célèbres comiques anglais, qui, dans un de leurs fameux sketchs où ils répétaient sans cesse le mot « Spam » dans une conversation, ont ajouté à ce mot une notion de désagrément.

Aujourd'hui, le mot « Spam » est communément utilisé pour caractériser un courrier électronique non sollicité envoyé en masse à une multitude de destinataires. Ce courrier provoque soit une gêne dans le meilleur des cas, soit une menace de sécurité pour les destinataires.

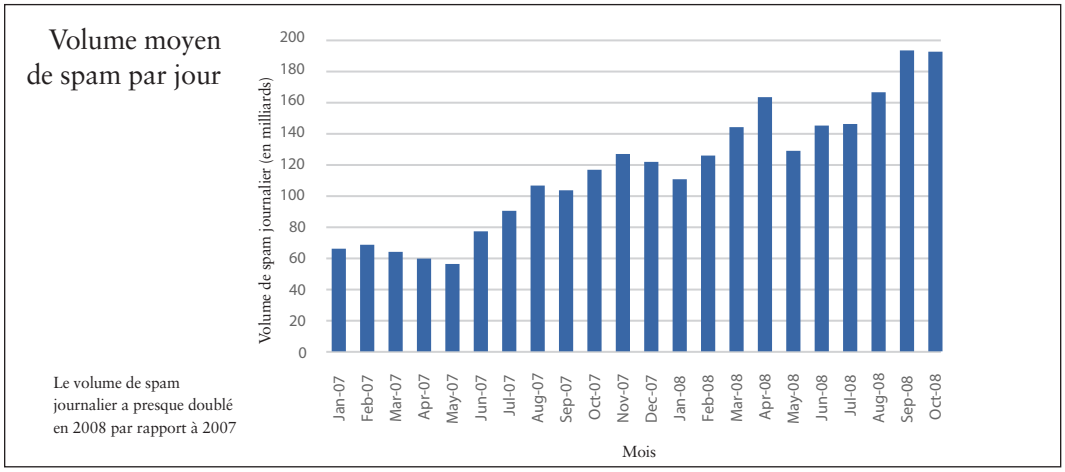
Le spam est présent massivement dans nos messageries électroniques depuis 2002. Cette déferlante de courriels indésirables trouve une grande motivation dans l'appât du gain. Les spammeurs ont tout d'abord réalisé des profits sur la vente de divers produits à faible marge (compléments à base de plantes, prêts immobiliers à faible taux d'intérêt, souris ergonomiques…) mais aussi grâce à des activités criminelles (fraudes aux cartes de crédit, pornographie, vente illicite de médicaments…). Ces profits sont ensuite réinvestis dans de nouvelles technologies et infrastructures de diffusion de spam. Aujourd'hui le spam est également un véritable démultiplicateur pour lancer des attaques profitant de failles dans la sécurité des réseaux des entreprises, facilitant le pillage d'adresses, les attaques phishing, la diffusion de virus, etc.

Lorsque le problème du spam est apparu, les entreprises et les particuliers ont commencé à déployer des filtres de première génération. Ces filtres s'appuyaient principalement sur une analyse heuristique, consistant à examiner les mots dans un message et, au moyen d'une formule de pondération, à calculer la probabilité que le message soit du spam. Face à la généralisation de ces solutions, les spammeurs se sont mis à élaborer de nouvelles tactiques plus poussées afin de contourner les filtres. Il s'en est donc ensuivi un jeu du chat et de la souris, dans lequel les spammeurs ont imaginé un nouveau stratagème pour passer au travers des mailles du filet, à la suite de quoi les éditeurs d'outils anti-spam ont ajouté une nouvelle technique à leur « arc » afin de contrer les spammeurs, qui à leur tour ont inventé une nouvelle tactique, et ainsi de suite.

Les trois premières générations ont chacune comblé les lacunes de la génération précédente, mais toutes souffraient d'une faiblesse commune. Chacune est en effet à la merci des spammeurs car elle opère sur un élément dont ces derniers ont la totale maîtrise : le contenu du message. Cela revient à bâtir une maison sur des fondations fragilisées. Les techniques de camouflage des spammeurs ont réussi à mettre en échec la plupart des filtres à base de contenu. On a ainsi vu le spam faire appel à des techniques de camouflage de plus en plus élaborées. Tout d'abord les spammeurs ont par

exemple décomposé les mots (si le mot Viagra était bloqué, ce n'était pas le cas de V.i.a.g.r.a.). Ensuite la plupart des messages de spam ont comporté des blocs de texte contenant des mots réputés comme n'étant pas du spam - souvent des termes techniques ou un extrait d'un livre. D'autres astuces consistaient à remplacer des lettres par des chiffres (par exemple 0 - zéro - au lieu de la lettre O).

La croissance du volume de spam s'est encore accélérée ces dernières années : le volume de messages considérés comme du spam a été multiplié par 6 en 3 ans entre début 2006 et fin 2008, pour dépasser 190 milliards de messages par jour.



Il existe deux raisons principales à cette nouvelle explosion : le développement exponentiel des réseaux de zombies que nous avons abordé au début de ce document, et les nouvelles techniques utilisées par les spammeurs.

Le spam image, apparu massivement en 2006, a été responsable d'une bonne partie de cette explosion. Il se présentait sous la forme d'un fichier image joint (.gif ou .jpg) qui incluait du texte, mais sans texte compréhensible dans le corps du message. Et ce, par opposition à la plupart des spams classiques, qui contiennent du texte en clair et/ou une URL cliquable, que les filtres anti-spam peuvent détecter. En déjouant nombre de techniques anti-spam, le spam image a réduit les taux d'interception et a augmenté le volume de courrier indésirable reçu. Des criminels ingénieux ont exploité le spam image pour lancer un flux ininterrompu d'attaques lucratives pour quelques-uns et préjudiciables pour tous les autres. Témoin les propositions d'achat d'actions boursières faiblement cotées (« penny stocks ») faites sous forme de publicités image, auxquelles ont cédé des destinataires naïfs, ce qui fait artificiellement grimper le cours des titres en question et permet au spammeur de réaliser un rapide bénéfice sur la vente des actions qu'ils avaient eux achetés en masse au fil de l'eau. Ces escrocs ont ainsi conçu des systèmes complexes de maquillage d'images et de diffusion de spam, pour lancer des milliards de messages et investir leurs capitaux sur des marchés boursiers publics soumis à une stricte réglementation. La colère des petits porteurs et les pannes de messagerie qui en ont résulté ne sont pour eux que des dommages collatéraux.

Les éditeurs d'anti-spam à base de contenu ont bien sûr réagi et référencé ces images dans leurs bases de signatures, mais les spammeurs ont réagi et ont permis au spam image de gagner encore en efficacité. La principale innovation a résidé dans la génération aléatoire de multiples copies d'une image, qui apparaissaient similaires à l'oeil humain mais totalement différentes pour des filtres anti-spam. Par exemple, les spammeurs envoyaient un fichier .gif dans lequel de minuscules points avaient été insérés au hasard. Ou bien ils jouaient sur les nuances de couleur, l'épaisseur et la trame d'une bordure, ou encore sur la police de caractères, pour produire de subtiles variantes d'une même image. Ou enfin, ils découpaient une image en une multitude de sous-images qui recomposait cette grande image, ce découpage étant aléatoire et donc unique pour chaque email envoyé. Dans tous les cas, le destinataire ne percevait aucune différence, mais la somme de contrôle du fichier était différente, et l'anti-spam reposant sur des signatures ne pouvait reconnaître les variantes de ce spam.

Pour contrecarrer ces techniques, les éditeurs de filtres à base de contenu ont alors émis des règles de plus en plus dures en réaction à ces innovations criminelles, et ont souvent risqué de supprimer de temps à autre des messages de bonne foi contenant des mots associés à du spam, générant ainsi de plus en plus de « faux positifs ».

Fichiers attachés dans les messages spam par année

2007	2006	2005
image/gif	image/gif	image/gif
application/pdf	image/jpeg	image/jpeg
image/jpeg	image/png	
image/png	application/msword	
application/x-msdownload		
application/msword		
application/vnd.ms-excel		
image/pjpeg		
image/bmp		
audio/mpeg		
application/zip		
text/calendar		
application/rtf		
application/x-zip-compressed		
application/vnd.ms-powerpoint		
image/x-png		

Courant 2007, les spammeurs ont abandonné le spam image pour passer au spam « avec attachements ». Les attaques spam étaient alors de plus en plus courtes, mais de plus en plus fréquentes, et utilisaient une technique différente à chaque fois. Ainsi, plus de 20 types différents de pièces jointes ont été utilisées dans diverses attaques éclair : PDF, Excel, MP3, etc. Le contenu du spam n'était pas situé dans le corps du message mais dans un fichier attaché au format Excel, PDF ou encore MP3.

La seule solution pour la majorité des filtres anti-spam traditionnels, qui ne bénéficient pas de moteurs capables d'analyser en profondeur les fichiers attachés, était alors de bloquer systématiquement tous les fichiers Excel ou PDF par exemple, action néanmoins peu applicable compte tenu du nombre élevé de faux positifs que cela aurait généré, sans parler du mécontentement potentiel d'utilisateurs bloqués dans leur travail, car ne pouvant plus recevoir de fichiers de ce type.

Comme on le constate les spammeurs ont sans cesse innové et appliqué des techniques toujours plus avancées pour contourner les solutions proposées par les éditeurs et constructeurs de sécurité.

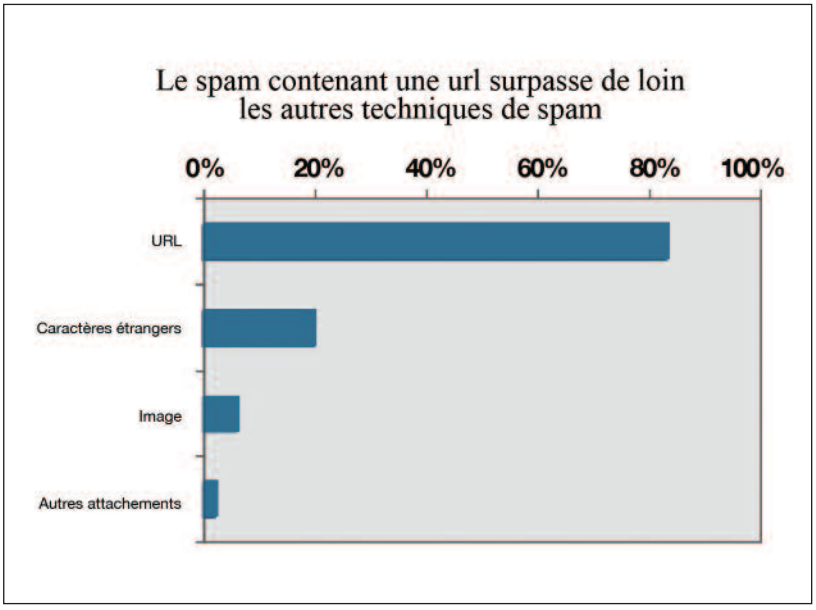
Plus le nombre de spams passant au travers des mailles du filet est élevé, plus la productivité des utilisateurs et la charge de travail des équipes informatiques s'en ressentent, et plus le réseau de l'entreprise est vulnérable aux menaces sur sa sécurité.

MOINS DE VENTES, PLUS DE MENACES

Enfin, et cela représente une évolution majeure depuis 2007, le spam porte désormais moins sur la vente de produits que sur le développement de réseaux de zombies. Auparavant le spam avait en effet comme objectif principal la vente de produits (pharmaceutiques, prêts à faibles taux, valeurs boursières, etc.). Aujourd'hui, une très forte majorité des messages spam comportent des liens pointant vers des sites Web qui diffusent des codes malveillants, ces derniers ayant pour but d'étendre la taille et la portée du réseau de zombies à l'origine du spam. Le spam est donc de moins en moins utilisé pour vendre, mais plutôt pour démultiplier des attaques.

En effet, des réseaux de zombies coordonnés et s'auto-propageant tels que le réseau Storm envoient des attaques qui utilisent des messages courts incluant une URL pointant vers un site infecté appartenant à la galaxie Storm, dans le seul but d'infecter de nouvelles machines et de faire croître le nombre de zombies gérés dans le réseau.

Ainsi, le spam atteint des niveaux record. Les spammeurs ont réagi aux défenses de plus en plus sévères mises en place par les fournisseurs de solutions de sécurité tout simplement en augmentant de façon importante le nombre de messages qu'ils envoient, et ce afin que le même nombre de messages atteigne finalement les boîtes de réception des utilisateurs. L'efficacité des systèmes de prévention du spam est donc plus critique que jamais. Les techniques utilisées par les spammeurs évoluent en complexité et en rapidité d'exécution, et il est vain de vouloir tenter de bloquer le spam à partir de filtres analysant uniquement le contenu du message. La réputation de l'émetteur du message et la réputation de l'URL incluse dans celui-ci sont également à prendre en compte.



Les entreprises doivent mettre en place des solutions de sécurité E-Mail mais aussi Web pour pouvoir prétendre stopper le spam auprès de leurs utilisateurs.

LES ATTAQUES « PILLAGE D'ANNUAIRES »

Les spammeurs lancent également régulièrement des attaques dites de « pillage d'annuaires ». Une attaque « pillage d'annuaires» sert à identifier les adresses e-mail valides d'un domaine donné. Pour ce faire un spammeur envoie un grand nombre de combinaisons noms-prénom vers un nom de domaine donné. Si un message d'erreur n'est pas renvoyé pour une adresse donnée, le spammeur en déduit que cette adresse est bien valide, et l'ajoute à sa liste d'adresses valides pour cette société donnée.

Le but premier de ces attaques est de collecter des listes d'adresses e-mail pour mener ultérieurement des attaques de spam ou les revendre à des spammeurs. Cependant, ce type d'attaques sert aussi désormais à tenter de pénétrer sur le réseau de l'entreprise. En effet, avec l'adoption croissante d'Active Directory, et du Single Sign-On, il est possible à un pirate ayant collecté des adresses e-mail valides d'une société de pénétrer sur le réseau, en devinant le mot de passe associé à telle ou telle adresse e-mail, qui sert souvent d'identifiant. Pour se protéger d'une telle attaque, les outils de sécurité ne suffisent pas : il est nécessaire de mettre en place un relais de messagerie qui propose une gestion avancée des messages d'erreur, et qui propose éventuellement des fonctionnalités anti-attaques «pillages d'annuaires».

LES ATTAQUES DE REDIRECTION DE MESSAGES D'ERREUR

Les spammeurs utilisent également leur réseau de zombies pour lancer un autre type d'attaque dangereuse : la redirection de messages d'erreur. Lors de l'envoi d'un spam à des milliers de destinataires, que ce soit pour du spam classique ou pour lancer une attaque de pillage d'annuaires, il est certain qu'un nombre important de messages comporteront des destinataires invalides. Le relais de messagerie du domaine signifiant ces destinataires invalides va en général émettre des messages notifiant l'erreur d'adresse à l'expéditeur de l'e-mail. Cela veut dire que lors de l'envoi d'un spam, l'expéditeur, le spammeur, va devoir faire face au retour potentiel de milliers de messages d'erreur.

Pour contourner ce problème, le spammeur va envoyer des spams en volume sur un ou plusieurs domaines, mais en mettant comme adresse de retour dans l'e-mail une entreprise X qu'il souhaite attaquer. Tous les messages d'erreur seront ainsi renvoyés sur l'entreprise X …

Ce type d'attaque offre au pirate-spammeur le double avantage d'envoyer du spam sans gérer le retour des messages d'erreur tout en attaquant une entreprise en lui faisant courir le risque d'un déni de service.

Il est estimé que plus de 55% des 500 plus grosses entreprises mondiales ont subi ce type d'attaques, qui représentent aujourd'hui 9% de l'e-mail mondial.

QUELLES SOLUTIONS FACE À CES MENACES ?

Les taux d'infection par des logiciels malveillants connaissent une forte croissance à travers le monde, quelle que soit la taille de l'entreprise, et ce malgré le fait que plus de 65% des entreprises concernées aient déployé un anti-virus ou un anti-spyware sur les postes de travail. Au cours d'une enquête réalisée récemment aux Etats-Unis, Cisco estime que le coût d'infection par un logiciel malveillant est de 150$ par PC et par an. Et ce chiffre ne concerne que les coûts informatiques directs associés au contrôle et au nettoyage des codes malicieux, sans tenir compte des milliers voire millions d'euros en jeu en cas de fuite ou de perte d'informations confidentielles liées à une infection.

La nature séquentielle et multi-protocolaire de ces nouvelles attaques rendent les solutions de protection traditionnelles inefficaces. Par exemple les filtres anti-spam traditionnels à base de contenu sont dépassés par le volume de spam à traiter ainsi que par la diversité des techniques utilisées. Les proxies Web traditionnels (utilisés pour la fonction de cache et de filtrage URL par catégorie gérant les accès Internet des employés) sont désormais eux aussi insuffisants quand il s'agit de protéger les utilisateurs contre les nouvelles menaces liées au flux HTTP décrites dans les premières parties de ce document.

Comme nous l'avons vu, ces menaces empruntent deux vecteurs principaux qui transmettent la quasi-totalité des logiciels malveillants : la messagerie et le Web. Il convient donc de mettre en place au sein de votre organisation des solutions adaptées pour chacun de ces vecteurs. Les contraintes d'utilisation liées à ces deux vecteurs de communication sont très différentes, et il est par là-même difficile de faire coexister de façon performante au sein d'une même solution une protection efficace sur la messagerie et le Web. Nous parlerons donc dans ce paragraphe de deux solutions distinctes pour ces deux passerelles de communication.

SÉCURISER LA PASSERELLE DE MESSAGERIE

Le relais de messagerie, véritable fondation de la sécurité E-Mail

Le premier élément important permettant aux entreprises d'avoir une infrastructure de messagerie saine et performante n'est pas un outil de sécurité à proprement parler, mais le relais de messagerie lui-même. Celui-ci doit être capable dans un environnement moderne de gérer un grand nombre de connexions simultanées, de savoir gérer les connexions et les files d'attente de messages de façon intelligente, de proposer des solutions pertinentes pour protéger la réputation de l'entreprise sur Internet, et de savoir filtrer et limiter le trafic en fonction des domaines de façon à proposer des ripostes adaptées aux différentes attaques.

Le relais de messagerie doit ensuite s'interfacer parfaitement avec des solutions anti-spam qui combinent une analyse complète et contextuelle du contenu à une analyse de la réputation de l'expéditeur pour plus d'efficacité, ainsi qu'à des solutions anti-virus, de filtrage du contenu et de chiffrement des emails.

Gérer le spam en vérifiant la réputation de l'émetteur

Nous avons vu précédemment que les techniques employées par les spammeurs évoluent rapidement. Les filtres anti-spam traditionnels, analysant le contenu des messages, ne peuvent pas suivre le rythme de ces innovations. En effet, il leur faudrait prévoir à l'avance toutes les nouvelles techniques possibles, et développer des signatures pour chaque variante, ce qui est véritablement impossible. Désormais, il ne faut plus uniquement tenir compte des contenus du spam, mais également d'un élément qui pourra contrer potentiellement toutes les nouvelles attaques spam : la réputation de l'adresse IP qui envoie le message de spam. En effet si l'on se base sur la réputation de l'émetteur de l'e-mail, il sera possible de le classer ou non en spam, et ce quel que soit son contenu ou la nouvelle méthode employée par les spammeurs. Associer un filtre à base de réputation à un relais de messagerie est la première étape nécessaire à une bonne protection des flux e-mail.

Bloquer les alertes virales avant l'émission des signatures anti-virus

Les solutions anti-virus couplées au relais de messagerie doivent également être capables de bloquer les attaques virales avant la livraison des antidotes par les éditeurs d'anti-virus. En effet, le réseau d'une organisation est vulnérable durant le laps de temps entre le lancement de l'alerte virale et l'émission d'une signature anti-virus par les éditeurs concernés. Les entreprises doivent donc déployer des systèmes de protection préventifs en temps réels, de type quarantaine dynamique, pour bloquer les fichiers suspects en attendant l'émission de ces signatures.

Protéger les données dans les communications sortantes

Des données sensibles et critiques d'une organisation peuvent être envoyées à l'extérieur par un logiciel espion. La fuite de données vers l'extérieur peut d'ailleurs aussi être le résultat malveillant d'un utilisateur interne, ou le plus souvent le résultat d'une erreur humaine (tel utilisateur qui envoie telle information à quelqu'un qui n'aurait pas dû la recevoir ou qui aurait dû la recevoir à un moment différent). Ces fuites peuvent avoir de graves conséquences pour l'entreprise (pertes commerciales, financières, ou non-conformité à une loi ou une réglementation).

Les entreprises doivent donc déployer des solutions de protection des données incluant des moteurs d'analyse de contenu classiques (recherche par mot-clé dans le message ou dans un fichier attaché, par type et taille de fichiers, etc.), mais aussi des filtres automatiques qui appliqueront des politiques prédéfinies (par exemple des filtres de conformité à SOX, ou encore des filtres capables de reconnaître automatiquement un numéro de carte bancaire dans un message, et ce afin de pouvoir en déduire des actions de remédiation conformes au standard PCI, etc.). Ensuite ce moteur devra être capable de remédier à cette analyse de différentes façons : mise en quarantaine du message suspect, alerte de l'administrateur, reporting, et chiffrement du message. Ce chiffrement doit de plus se faire automatiquement au niveau de la passerelle, en coordination avec le relais de messagerie, afin de pouvoir appliquer systématiquement les politiques. Il est par ailleurs important que la technologie de chiffrement utilisée ne repose pas sur le besoin pour le destinataire d'un logiciel client sur son poste pour déchiffrer le message, et ce afin de pouvoir diffuser largement des e-mails chiffrés lisibles finalement par tous.

Suivre les messages importants
Avec les menaces qui deviennent de plus en plus complexes, les défenses se durcissent. En réaction, les filtres anti-spam traditionnels vont bloquer les messages de moins en moins finement et vont générer beaucoup de faux positifs. Compte tenu du grand nombre de messages circulant dans les organisations aujourd'hui, il est important de mettre en place des outils permettant de véritablement retrouver la trace de tous les e-mails en cas de besoin.

SÉCURISER LES TRAFICS WEB

Compte tenu du fait que les attaques provenant du Web continueront d'être de plus en plus malicieuses et sophistiquées, IDC estime que les solutions de sécurité Web joueront un rôle de plus en plus important dans les systèmes d'informations, venant ainsi s'ajouter aux solutions firewall et anti-virus traditionnelles.

Le filtrage URL par catégorie pour gérer le trafic connu
Le trafic Web peut être découpé en deux grandes parties.

D'une part, il existe un trafic « connu », correspondant à un nombre restreint et connu de sites bien catégorisés (business, news, sport, éducation, services publics, shopping, etc.), qui ont de forts volumes de connexions. Celui-ci peut être géré par l'intermédiaire d'une solution de filtrage URL par catégorie, solution qui sera alors utilisée pour gérer les accès Internet des employés, en autorisant, limitant ou bloquant les accès aux sites en fonction de leur catégorie.

Ces solutions de filtrage URL par catégorie permettent aussi de bloquer les accès aux sites connus de phishing ou connus pour être infectés par du malware et catégorisés comme tels. Ces solutions sont toutefois uniquement réactives, et en cas d'apparition d'un malware sur un site donné, le temps que le site soit bien catégorisé et que la règle soit transmise aux clients, le code malicieux aura eu potentiellement le temps d'infecter l'entreprise. Reposer sur une liste de sites catégorisés pour gérer sa sécurité Web ne permettrait de se protéger que face à des menaces ou attaques connues. Or sur le Web nous avons vu qu'à partir du moment où une attaque ou menace existe déjà depuis quelques jours, elle est abandonnée par le pirate qui va alors trouver d'autres méthodes.

Il faut donc se contenter d'utiliser les solutions de filtrage URL par catégorie pour gérer une politique d'usage acceptable d'Internet au sein de sa société, mais pas pour mettre en place une politique de sécurité Web.

Filtrer les pages Web en vérifiant la réputation du site
Au-delà du trafic « connu » décrit ci-dessus, il existe d'autre part un nombre potentiellement illimité de sites « inconnus », non catégorisables, qui peuvent héberger du malware. Ces sites ne sont parfois en ligne que pour quelques heures, correspondant à la durée d'une attaque. Les URL peuvent d'ailleurs être générées de façon aléatoire et illimitée pour contourner les solutions de filtrage URL par catégorie, qui n'ont pas le temps de classifier ces sites.

Le trafic « inconnu » (ou les redirections de trafic vers des sites infectés générées par des attaques iFrame) doit lui être géré via des systèmes de réputation Web. Ces solutions vont analyser un certain nombre de paramètres concernant potentiellement tout serveur Web sur Internet, et donner à celui-ci une note de réputation. En fonction de cette note, le système va appliquer une action : par exemple, bloquer les accès aux sites dont la note de réputation est mauvaise, ou encore appliquer un filtrage à base de signatures pour les sites « intermédiaires », et laisser passer les bons sites. Appliquer un filtrage complémentaire à base de signatures uniquement aux flux « tendancieux » permet ainsi de gagner en performance. Les solutions à base de réputation comblent les lacunes des solutions à base de catégories : en effet si un nouveau serveur Web apparaît sur Internet et connaît des pics de trafic, il va se voir attribuer une note de réputation neutre ou légèrement négative, ce qui soit permettra directement de le bloquer, soit par exemple de lui appliquer un filtrage supplémentaire à base de signatures.

Ce type de solutions est également efficace contre les attaques iFrame. Par exemple, si une URL est légitime mais infectée par un iFrame qui redirige l'utilisateur vers un site frauduleux, la réputation Web va bloquer la redirection (le site frauduleux aura une réputation négative). Enfin, dans le cadre d'une URL légitime qui contient des liens HTML renvoyant vers des publicités qui au final renvoient vers un serveur d'images infectées distribuant un code malicieux, si la réputation de ce site reste neutre ou légèrement positive malgré cette infection, il faudra toutefois compléter le filtre à base de réputation par un système anti-malware à base de signatures qui va alors bloquer l'objet malicieux tout en laissant l'utilisateur accéder aux parties « propres » de ce site légitime.

L'anti-malware à base de signatures, complément indispensable

Que ce soit dans le cadre d'un trafic web connu ou inconnu, les entreprises doivent également mettre en place des solutions anti-malware à base de signatures. Ces dernières sont souvent déployées sur les postes de travail mais rarement sur la passerelle, en raison des problèmes de performance que cela peut engendrer. En effet le Web est un protocole en temps réel, et les utilisateurs veulent y accéder en temps réel. Les systèmes traditionnels à base de signatures, s'ils étaient installés sur la passerelle, ajouteraient plusieurs secondes de latence à l'affichage de chaque page. L'utilisateur aurait alors l'impression d'utiliser un vieux modem au lieu de sa connexion ultra-rapide d'entreprise. Ainsi, un filtrage à base de signatures au niveau de la passerelle se doit d'être ultra-rapide pour éviter les problèmes de latence. IDC indique dans une étude récente sur le marché de la Sécurité de Contenu qu'en raison de la nature en temps réel des protocoles HTTP et HTTPS et de leur flux de données, des fonctionnalités de scanning en temps réel (en mode streaming) plus sophistiquées sont nécessaires pour s'assurer que le trafic Web reste sécurisé et à l'abri des attaques.

Contrôler les différents flux applicatifs empruntant la passerelle Internet

Les communications empruntant la messagerie instantanée, le Webmail, les sites de stockage en ligne ou encore le peer-to-peer, doivent être sécurisées au même titre que les communications émises par la messagerie SMTP « traditionnelle » de l'entreprise. Il convient d'analyser ces flux à la recherche de fichiers infectés pouvant contaminer le réseau. Des applications comme Skype, capables de s'adapter aux outils de contrôle et de chiffrer leurs communications, doivent être rigoureusement suivies voire bloquées afin de limiter les risques de sécurité.

Ainsi, s'il n'est pas toujours possible d'analyser les flux Skype en raison de l'utilisation par cette application d'un protocole propriétaire qui sort par le port 443, il est toutefois possible d'interdire tout ce qui sort en 443 sans être du SSL...

Gérer les flux SSL

Il faut aussi préciser que les flux SSL, s'ils permettent de sécuriser certains échanges de données, sont également un moyen pour les pirates d'introduire en toute impunité du malware au sein des réseaux des entreprises, car ils ne sont pour la plupart du temps pas inspectés. Une solution efficace de sécurité Web se doit donc de déchiffrer ces flux, mais de le faire de façon intelligente, éventuellement en fonction de la catégorie (par exemple scanner le trafic provenant des sites de webmail afin d'analyser les fichiers joints inclus dans les messages) ou de la réputation du site web, pour ne pas déchiffrer inutilement des flux sûrs (par exemple une connexion d'un utilisateur à son site de banque en ligne) et par là même éviter les problèmes liés à la confidentialité des données.

Empêcher vos postes déjà infectés de communiquer avec l'extérieur

Les responsables de la sécurité informatique doivent également prendre en compte le risque représenté par les postes de travail infectés, soit avant la mise en place des solutions de filtrage décrites ci-dessus, soit par des connexions à Internet en dehors du réseau de l'entreprise qui les ont exposés à des menaces, soit encore à cause d'une clé USB infectée qui a été connectée au poste. Pour cette raison, il est important de scanner les ports et les protocoles et de bloquer les communications des codes malicieux avec l'extérieur, qu'il s'agisse d'envois effectués par du spyware vers l'extérieur, de téléchargements réalisés par des chevaux de Troie vers le réseau de l'entreprise, ou encore de communications de postes transformés en zombies sur le réseau avec leurs serveurs de commande et de contrôle.

Cette analyse va s'effectuer à l'aide d'outils de monitoring ou de surveillance du trafic qui vont repérer les communications suspectes et potentiellement les bloquer.

Une solution efficace de protection de la passerelle Web se doit aujourd'hui, compte tenu de la complexité des menaces et de la variété du trafic Web, de combiner les différentes approches décrites ci-dessus.

LES SOLUTIONS CISCO IRONPORT

Cisco IronPort, une division de Cisco Systems, est un des fournisseurs leaders de passerelles de sécurité destinées aussi bien aux grandes entreprises qu'aux PME. La société a développé une gamme de boîtiers de :

- Sécurité E-mail : Cisco IronPort Série C (voir l'annexe 1 page 30 pour plus de détails)
- Sécurité Web : Cisco IronPort Série S (voir l'annexe 2 page 31 pour plus de détails)
- Gestion de la Sécurité : Cisco IronPort Série M, permettant de centraliser des fonctionnalités de déploiement, d'administration et de reporting concernant divers boîtiers S ou C.

Ces boîtiers s'appuient sur Cisco SensorBase, le plus ancien et le plus vaste réseau de surveillance du trafic e-mail et web mondiaux. SensorBase collecte des données provenant de pas moins de 130 000 réseaux différents à travers le monde, représentant plus de 30% du trafic e-mail planétaire, et surveille plus de 150 paramètres distincts relatifs à un expéditeur ou un site Web donnés.

SensorBase contrôle ainsi plus de 90 paramètres réseau concernant toute adresse IP émettrice de courrier électronique sur Internet : volume global envoyé depuis cette adresse, date depuis laquelle l'adresse expédie du courriel, pays d'origine, détection d'un proxy ou d'un relais ouvert, présence sur des listes noires ou blanches, configuration du DNS, acceptation de courrier en retour, etc.

SensorBase contrôle également un grand nombre de paramètres réseau concernant toute adresse IP hébergeant un serveur Web, comme l'historique du site, son pays, son volume de trafic, sa présence sur des listes noires ou blanches, etc.

En accédant à un très large échantillon de données, SensorBase est ainsi en mesure d'évaluer avec une extrême précision le comportement et la réputation de chaque expéditeur ou de chaque site. SensorBase applique des algorithmes qui analysent ces paramètres de niveau réseau et en tirent un «score de réputation » (e-mail ou Web) compris entre -10 et +10. Ce score est ensuite communiqué en temps réel aux boîtiers Cisco IronPort lorsqu'un message est reçu d'un expéditeur quelconque, ou lorsqu'un utilisateur tente d'accéder à un site.

Cisco emploie de nombreux techniciens et statisticiens multilingues dans son Centre opérationnel d'identification des menaces (TOC, Threat Operations Center), 24 heures sur 24, 7 jours sur 7, pour le contrôle et la gestion des données de SensorBase. L'équipe du TOC a développé un moteur de qualification des données qui traite et pondère les informations originaires de différentes sources pour une interprétation plus fiable. L'équipe veille à l'actualisation et à la précision des données SensorBase, afin que les administrateurs puissent s'en remettre à celles-ci pour automatiser la sécurité e-mail et Web.

Pour toute information sur les solutions Cisco IronPort, rendez-vous sur www.ironport.com.

CISCO IRONPORT SERIE C

RELAIS DE MESSAGERIE

AsyncOS est l'OS IronPort dédié, durci et optimisé pour la messagerie, qui peut gérer jusqu'à 10 000 connexions simultanées, soit 100 fois plus que les équipements UNIX équivalents traditionnels. Le boîtier résiste ainsi à des pics potentiels de messages.

Un système de ***files d'attentes*** et des réémissions de messages distinctes pour chaque ***domaine*** permet de ne pas bloquer le relais si un domaine n'est pas accessible. Un système de ***limitation*** (ou «throttling») des flux permet d'adopter des ripostes graduées.

Des ***outils d'administration*** permettent la gestion des politiques, la création de rapports et le tracking des e-mails. ***Bounce Verification*** vous protège contre des éventuels dénis de service liés à des attaques de redirection de messages d'erreur massives, estampille les messages sortants pour ensuite protéger la passerelle contre les redirections frauduleuses de messages d'erreur. Les messages de notification d'erreur en arrivée ne comportant pas ce tampon seront refusés.

Directory Harvest Attack Prevention enregistre le nombre de destinataires invalides contactés par un expéditeur donné. Dès lors qu'un seuil défini par l'administrateur est franchi, le courrier de cet expéditeur est bloqué sans que ne soit généré de message d'erreur. Cette technologie protège l'entreprise des attaques de « pillage d'annuaires ».

DEFENSE ANTI-SPAM

Les IronPort Reputation Filters™ bloquent environ 90% du spam entrant au niveau de la connexion TCP, en analysant la note de réputation de l'émetteur du message.

IronPort Anti-Spam™ examine 4 critères pour chaque message : le contenu, la structure, la réputation de l'émetteur du message, laréputation du site web dont le lien est présent dans l'e-mail.

DEFENSE ANTI-VIRUS

IronPort Virus Outbreak Filters™ identifie et bloque les virus plusieurs heures avant la disponibilité des signatures des éditeurs traditionnels d'anti-virus.
Sophos Anti-Virus et/ou ***McAfee Anti-Virus*** procurent un second rempart de protection anti-virus, à base de signatures et entièrement intégré, s'appuyant sur la technologie de détection de virus la plus performante du marché.

PROTECTION DES DONNÉES

L'analyse de contenu se fait selon l'adresse IP source ou de destination, le domaine ou l'adresse, l'en-tête, des mots-clés dans le corps du message, la taille ou le type des pièces jointes, des mots-clés ou des objets embarqués dans les pièces jointes, ou la réputation de l'expéditeur. Dans le cadre de la protection des données de l'entreprise, il est également possible d'appliquer des filtres automatiques de conformité (SOX, PCI, etc.), des dictionnaires de conformité (reconnaissance de mots-clés liés à ces réglementations), ainsi que des « Smart Filters » permettant notamment de reconnaître automatiquement les numéros de carte bancaire contenus dans les messages.

Suite à l'analyse des contenus, il est possible d'appliquer différentes actions : reporting, alerte de l'administrateur, mise en quarantaine ou encore chiffrement des e-mails.

CHIFFREMENT DES E-MAILS

La technologie ***IronPort PXE*** permet d'envoyer des messages chiffrés sans besoin de logiciel client sur le poste du destinataire et quel que soit son OS ou son client de messagerie. Les messages sont chiffrés au niveau de la passerelle en fonction de politiques mises en place par l'administrateur (en fonction de l'émetteur, du destinataire, d'un mot clé dans le message, de la reconnaissance d'un numéro de carte bancaire, etc.) .

CISCO IRONPORT SERIE S

PROXY WEB SECURISE

- ***AsyncOS for Web***, l'OS IronPort dédié et optimisé pour les flux Web, peut prendre en charge jusqu'à 100 000 connexions TCP entrantes et sortantes simultanées.
- ***Un cache à base de réputation***, unique sur le marché, permet d'accélérer les performances.
- ***Des outils d'administration*** permettent la gestion des politiques et la création de rapports.

CONTRÔLE DE L'USAGE DU WEB

Les IronPort URL Filters permettent une gestion des accès des employés en fonction de la politique d'utilisation acceptable de l'Internet définie par l'entreprise.

Le moteur DVS (Digital Vectoring & Streaming) permet de ***contrôler les applications*** exécutées par les utilisateurs, en se basant sur une liste de « users agents » suspects. De plus, DVS permet de bloquer les flux applicatifs qui proviennent de l'extérieur en réponse aux requêtes émises par les applications exécutées par les utilisateurs de l'entreprise.

DVS analyse aussi ***les contenus Web*** : il peut bloquer les objets Web téléchargés en fonction de leur taille ou de leur nature (MP3, vidéo, etc.).

DEFENSE ANTI-MALWARE

Un moniteur de trafic intégré de niveau 4 scrute tous les ports afin de détecter et bloquer les envois de données de spyware vers l'extérieur, ou les réceptions de codes malveillants téléchargés par des chevaux de Troie. Le moniteur de trafic vérifie que le trafic sortant n'est pas destiné à des adresses IP de serveurs de contrôles de zombies regroupées sur une blacklist.

Utilisant SensorBase, ***les IronPort Web Reputation Filters***™ analysent plus de 60 paramètres pour évaluer avec précision le degré de confiance d'une URL. Des techniques évoluées de modélisation de la sécurité servent à pondérer séparément chaque paramètre afin d'en tirer une note unique, sur une échelle de -10 à +10. Des règles configurées par l'administrateur sont appliquées de façon dynamique, en fonction des notes de réputation.

Dans le cas d'une note neutre ou intermédiaire (par exemple entre -5 et +5), la Série S peut alors pratiquer un ***déchiffrement SSL sélectif***. Les flux HTTPS provenant de sites à la réputation douteuse seront ainsi déchiffrés pour être inspectés, alors que la confidentialité des flux HTTPS légitimes sera respectée. Les transactions SSL vers des sites à mauvaise réputation seront systématiquement coupées au niveau de la connexion, ne nécessitant donc pas non plus de déchiffrement.

L'IronPort Anti-Malware System™ garantit la meilleure protection possible contre les menaces Web les plus diverses. Il inclut plusieurs bases de signatures anti-malware et anti-virus web provenant de différents éditeurs du marché, au premier rang desquels ceux de ***Webroot*** et de ***McAfee***, leaders sur les marchés de l'antispyware et de l'anti-virus selon IDC. Le moteur scanne les objets Web en mode streaming : le scan commence en même temps que le téléchargement de l'objet, et si un code malveillant est identifié, le téléchargement est immédiatement stoppé, ce qui accélère de façon sensible la capacité de traitement du boîtier.

SECURITE DES DONNEES

La Série S contient également des fonctionnalités simples de prévention contre la perte de données, reposant sur ***une analyse des métadonnées***, regardant la nature du fichier, sa taille et son nom. Les métadonnées, combinées à l'ID de l'utilisateur, la catégorie et la réputation du site de destination, vont déclencher des actions automatiques : permettre ou bloquer la connexion et l'upload du fichier, ou la garder en log. Des fonctionnalités d'analyse plus poussée des contenus sont disponibles sur des boîtiers d'éditeurs partenaires.

LES MENACES ACTUELLES D'INTERNET

COMMENT S'EN PROTÉGER

Edition 2009/2010

Cisco a plus de 200 bureaux ou filiales dans le monde. Les adresses, numéros de téléphone et numéros de fax sont listés sur le site web Cisco à l'adresse www.cisco.com/go/offices.