L'Actu Sécurité n°4

xmco Partners

PLAN

"Peut-on converger indéfiniment ? "

Il semble aujourd'hui que la convergence soit LE but ultime de tout un chacun -du moins, à en croire les constructeurs informatiques...-
Qui a dit que la convergence était si essentielle ? Et pourquoi s'arrêterait-on à l'informatique : A quant les machines à laver qui intègrent un fer à repasser ?! A quand le four à micro-onde avec fonction congélateur ?!

Evidemment, ces exemples font sourire, mais transposés dans un contexte technologique, c'est plutôt de l'admiration qui en ressort : envoyer des mails à partir de son blackberry, écouter des MP3 à partir de sa montre, ou de son navigateur GPS portable, regarder la télévision à partir de son ibook muni d'un adaptateur TNT sur clé USB...

Et bien pour être franc, j'en ai un peu marre de cette convergence, qui conduit nos clients à multiplier leurs budgets par 3 pour espérer une hypothétique diminution des coûts de 25 %...
Pourquoi : parce que dès qu'il s'agit d'informatique, tout est permis. Un constructeur peut, dès qu'il acquiert le savoir-faire, développer produire et vendre n'importe quelle nouveauté sans prendre le temps d'informer ses clients, de former la société sur les bouleversements que sa découverte peut engendrer.
Savez-vous qu'aujourd'hui, certaines familles ont réduit leur budget alimentaire pour assumer leurs factures de téléphones portables ? (4 abonnement à 50 euros / mois, ça commence à être significatif, sans compter les dépassements...)

Certes, des bienfaits évidents ont découlé de l'ingéniosité de milliers d'inventeurs, et loin de moi l'idée de vouloir retourner à l'âge de pierre. Cependant, que penser des vulnérabilités de téléphone que l'on a vu apparaître, dont le bluetooth est le principal vecteur...

Il semble, de toute façon que la société n'arrive plus à digérer le rythme effréné des découvertes et des technologies. Est-ce qu'il ne faudrait pas que les constructeurs se penchent maintenant sur la sensibilisation et la formation de leurs clients et utilisateurs ?

D'immenses progrès ont été réalisés dans tous les domaines : Médecine, Sciences, Technologies, Transports, ... Et chaque domaine s'est adapté à la société, aux mentalités : que je sache, même si les chercheurs savent faire tenir un repas idéal complet dans une petite pilule, le monde de la restauration se porte toujours aussi bien.
En informatique les technologies, les innovations se multiplient à vue d'oeil, pour le plus grand plaisir des acteurs du marché, et souvent au détriment des utilisateurs... Il est devenu quasiment impossible de s'y retrouver dans l'étendue de nouveautés qui inondent notre espace.

Et bien j'avoue, que j'ai parfois du mal à avaler certaines pilules...

Marc Behar

1. POINT JURIDIQUE:

LA LOI DE SÉCURITÉ FINANCIÈRE (LSF).

Le Gouvernement d'Entreprise et les questions sur la transparence de l'information financière sont au centre des débats depuis quelques années en France. L'éclatement de la bulle financière a déstabilisé les marchés et entaché la confiance des investisseurs.

Face à ces menaces, le législateur a du intervenir. Aujourd'hui, ce sont donc des lois, telles que le Sarbanes Oxley Act aux Etats-Unis ou la Loi de Sécurité Financière en France, qui codifient les recommandations en matière de gouvernement d'entreprise pour protéger les investisseurs.

XMCO | Partners

Petit rappel

Qu'est ce que la LSF ?

Le Parlement français a adopté le 17 juillet 2003 la Loi de Sécurité Financière (appelée Loi Mer). Elle renforce les dispositions légales en matière de Gouvernement d'Entreprise.

Cette nouvelle loi s'applique à toutes les sociétés anonymes ainsi qu'aux sociétés faisant appel à l'épargne publique ; ces dispositions sont applicables pour les exercices comptables ouverts à partir du 1er janvier 2003.

Comme la loi Sarbanes-Oxley, la Loi de Sécurité Financière repose principalement sur :

- Une responsabilité accrue des dirigeants
- Un renforcement du contrôle interne
- Une réduction des sources de conflits d'intérêt

A travers le renforcement du contrôle interne, la LSF devrait permettre de produire une information financière de meilleure qualité et ainsi d'accéder aux demandes du marché pour plus de transparence. La Loi Mer prévoit, par exemple, que le Président du Conseil d'Administration (ou du Conseil de Surveillance) doit rendre compte des procédures de contrôle interne mises en place par la société.

Cette évaluation sera intégrée au rapport de gestion sur les comptes sociaux et consolidés. (L. Art. 225-37). Les Commissaires aux Comptes devront apprécier, dans leur rapport, l'évaluation du contrôle interne faite par le Président du Conseil d'Administration.

Elle aborde d'autre part, le contrôle du fonctionnement des cabinets d'audit et les conflits d'intérêt qui peuvent s'y rattacher. A ce titre, elle crée un Haut Conseil du Commissariat aux comptes chargé :

- d'assurer la surveillance de la profession,
- d'examiner les normes qui lui sont applicables
- de renforcer la prévention des conflits d'intérêt, notamment en assurant la séparation de l'audit et du conseil.
- accroître la transparence dans les processus de décision des organes dirigeants et délibérants des sociétés
- améliorer les procédures de contrôle que les entreprises mettent en oeuvre.

Certaines dispositions concernant l'information financière, qui appartenaient jusqu'ici aux recommandations du gouvernement d'entreprise, sont maintenant intégrées à la loi.

Les entreprises doivent donc relever aujourd'hui le défi de l'adaptation à ces nouvelles règles du jeu. Le programme de changement, pour se mettre en conformité à ces dispositions, nécessite dans un premier temps l'identification précise des enjeux pour les sociétés.

Deux prérogatives pour un meilleur gouvernement d'entreprise

Le contrôle interne

L'environnement de contrôle interne doit garantir que l'ensemble des opérations s'est déroulé conformément aux procédures et doit correspondre à l'activité réelle de l'entreprise.

Ceci implique une forte intégration des procédures de contrôle avec les systèmes d'information et les différents intervenants participant à la réalisation des processus comptables et financiers et leur contrôle.

Ceci demande une maîtrise améliorée de trois types de processus ainsi que des flux d'information associés :

- les processus courants comme l'enregistrement des opérations routinières en comptabilité, la planification et la préparation des budgets, etc
- les processus associés à des évènements exceptionnels comme ceux gérés lors de fusion, de rachat, de désinvestissement, etc
- les processus de communication financière en direction des marchés et des tiers.

La communication financière

La loi instaure, par exemple, l'obligation de communiquer tout changement dans la structure ou toute opération de nature à affecter la valorisation de l'entreprise. Ainsi, une entreprise qui réduit de façon significative ou qui stoppe une relation avec un client important doit le communiquer en « temps réel ».

L'enjeu pour les entreprises consiste à mettre en place l'organisation et les outils à même de soutenir le processus de communication financière. Pour être capable de délivrer les informations exactes dans les meilleurs délais, il est notamment nécessaire de maîtriser les processus de collecte et de production de l'information financière et de maîtriser et standardiser les canaux de diffusion de celle-ci.

Ces exigences, très ambitieuses en matière de communication financière, placent les entreprises dans l'obligation d'analyser en détail leur « chaîne de l'information financière ». Elles doivent être en mesure de tracer l'information émise et de remonter la chaîne pour identifier les données (faits générateurs, écritures comptables,…) et décisions à l'origine de l'information.

Enjeux

Des répercutions directes sur le système d'information

Afin de supporter efficacement la production d'un reporting fiable, les sociétés peuvent donc investir dans plusieurs types de solutions parmi lesquelles :

- une solution de documentation des activités supportant, la description des processus, l'identification des risques et l'évaluation de l'environnement de contrôle interne,
- des outils de reporting intégrés dans le système d'information permettant via une production rapide des états financiers avec une information fiable à destination des cadres dirigeant internes et des analystes financiers ou des autorités de tutelle externes,
- une solution de gestion du contenu de type « Enterprise Content Management » pour conserver, gérer et mettre efficacement à disposition les informations de l'entreprise. Cette solution peut ainsi contribuer à sécuriser et à qualifier toutes les informations nécessaires au reporting financier et comptable.

En fonction de l'organisation, des systèmes d'information déjà en place et de la stratégie qu'elles ont chosies, les entreprises doivent adopter un plan d'action afin de répondre aux enjeux « informatiques » posés par les nouvelles réglementations.

Une revue de la cartographie applicative globale permet de donner une idée précise des flux, des contrôles, et des données dont la gestion doit être améliorée ou supportée par les systèmes.

La plupart des entreprises soumises à ces contraintes de sécurité financière vont donc devoir réagir et leurs dirigeants se positionner.

Cette nouvelle législation survient dans un contexte évolutif, dans la mesure où, au même moment, les entreprises doivent composer avec les nouvelles normes comptables IAS. Comme cela a été mis en évidence, la mise en oeuvre des nouvelles réglementations en matière de gouvernement d'entreprise, telle que Sarbanes-Oxley aux Etats-Unis ou la Loi de Sécurité Financière en France, sont autant de défis pour les systèmes d'information, dans la mesure où elles impliquent d'importants changements, tant en terme organisationnel qu'au sein de l'nformatique.

La prise en compte de ces lois exige une modification des processus correspondants. Ceci a impacté les systèmes d'information, source des données financières de manière considérable.

Pour réaliser ces deux objectifs (contrôle et communication financière), les entreprises utilisent deux leviers, qui sont beaucoup plus efficaces s'ils sont utilisés ensemble :

- La refonte des processus comptables, financiers et documentaires
- Les outils informatiques

Pour mettre en place ces réglementations, soit les entreprises acquièrent ou re-développent un nouveau système d'information financière, avec les inconvénients de coûts et de délais que cela suppose, soit elles procèdent à une rénovation par partie du système d'information déjà existant. Il va de soi que, dans le contexte actuel, les directions générales n'envisagent que très rarement le premier scénario.

2. NOUVELLE TENDANCE

LES SOLUTIONS ANTI-SPAM

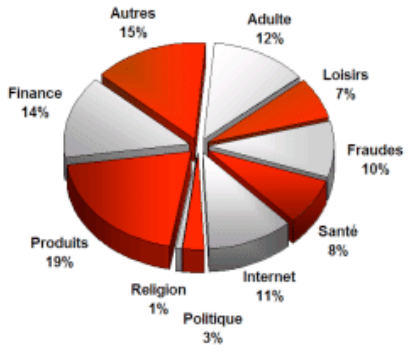
Le dernier fléau provenant d'Internet est sans nul doute le spam. Ces simples flux réseaux de quelques octets occupent aujourd'hui de nombreux chercheurs et sont devenus le cauchemar de tous les administrateurs. La multiplication des solutions anti-spam s'explique par le coût engendré de ces emails. En effet, celui-ci se situe entre 600 et 1000 euros par an et par salarié. Une étude menée par l'Université du Maryland aux Etats-Unis révèle que la facture globale pour les entreprises américaines représenterait 22 milliards de dollars par an.
Malheureusement, malgré les efforts de chacun, il semblerait que rien ne puisse endiguer le problème. La mise en place de solutions anti-spam devient de plus en plus complexe et de nouvelles sociétés spécialisées dans ce domaine apparaissent. Cependant en recherchant le moyen absolu de stopper tous les courriels non désirés, ne prenons-nous pas le problème à l'envers ?

XMCO | Partners

Définitions et perspectives

Qu'est ce qu'un SPAM ?

La CNIL [1] (Commission Nationale de l'Informatique et des Libertés) a clairement défini ce problème. Le "spamming" ou "spam" est « l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière ». Ainsi, il ne faut pas confondre spam et message publicitaire ou encore lettre d'information. Un message publicitaire correspond à un envoi de messages par un organisme qui a procédé à une collecte loyale des adresses électroniques. C'est-à-dire, que lors de la saisie de son email, l'utilisateur a été informé de son utilisation à des fins commerciales ou de sessions à des tiers, tout en ayant la possibilité de refuser cette diffusion. Une lettre d'information, ou newsletter, est quant à elle, envoyée depuis un site Internet sur lequel l'internaute s'est préalablement inscrit.



Répartition des contenus des spams

La propagation et l'essor des spam proviennent de leur simplicité d'élaboration. En effet, la mise en place d'un robot spammeur nécessite peu de temps et peu de ressources. Les emails générés seront ensuite envoyés à plusieurs milliers voire millions de personnes. Plus de la moitié des emails circulant sur Internet proviendraient de serveurs de spam.

La lutte contre les SPAMS

De nombreuses solutions pour se protéger du spamming ont vu le jour. Le coût moyen est de 20 à 40 euros par an et par salarié. Bien que celles-ci soient moins coûteuses que le spamming en lui même, ne faudrait-il pas investir cet argent dans une protection en amont ? Par ailleurs, nous disposons d'outils libres très puissants et très fiables en cryptographie comme la mise en place de la signature électronique qui est encore très peu exploitée. Cette technique serait à même de fournir une authentification universelle de l'expéditeur. Les robots spammeurs, envahissent des serveurs SMTP trop permissifs ou présentant des vulnérabilités. La sécurisation de ces machines, l'intégration d'une authentification entre les serveurs relais ainsi que la signature des emails limiterait le champ d'action du spam même si, bien entendu, il n'existe pas de solution miracle contre ce fléau.

Les mesures de protection

Les techniques

Il existe de nombreuses techniques pour lutter contre les courriers indésirables. Auparavant, un simple filtre sur des mots clés au sein du contenu du message, comme « sex, easy money, etc… », était suffisant. Aujourd'hui, les techniques utilisées ayant évolué, les contre-mesures se sont donc multipliées. Voici un inventaire succint des méthodes les plus courantes.

L'analyse lexicale constitue un ensemble de règles représentées sous forme d'expressions régulières ou de mots clefs. Ces règles permettent d'effectuer des recherches au sein des entêtes et des corps des mails, sur des caractéristiques connues des spams.

Les filtres bayésiens utilisent une méthode probabiliste de filtrage des courriels. Ils fonctionnent par apprentissage ou se basent sur des mots clefs présents dans les mails. Ce type d'algorithme demeure très efficace dans la durée. Le point critique reste la période durant laquelle il sera nécessaire de valider ou non les emails afin que le système apprenne les caractéristiques des spams.

Le respect de la conformité du protocole qui régit l'échange des emails, établi par les normes RFC 821 (SMTP) et RFC 1651 (ESMTP), n'est pas respecté par de nombreux spams.

Les bases collaboratives de spams sont similaires aux bases de signatures des virus. Celles-ci sont alimentées par les utilisateurs de solutions antispams. Les bases les plus couramment utilisées sont : Razor, Distributed Checksum Clearinghouses (DCC) et Pyzor. A l'instar des antivirus, chacune de ces bases dispose de ses propres règles et ce, afin de définir une signature. Il est donc préférable d'en croiser plusieurs.

L'enregistrement DNS vérifie la corrélation entre l'adresse IP du serveur source et son nom via une requête DNS inverse. Généralement, les véritables serveurs de messagerie possèdent une adresse IP fixe et un nom de domaine associé.

Les listes noires, ou RBL (Realtime Blackhole List), correspondant à des listes de serveurs ou de réseaux connus pour favoriser le spamming.

Les listes blanches, contrairement aux listes noires, contiennent des listes de sites, d'hôtes, de domaines ou encore d'adresses sûres. Le problème reste l'usurpation de ces adresses par les spammeurs.

La pondération par l'historique des transactions consiste en un système d'auto-apprentissage des transactions effectuées entre un expéditeur et un destinataire. Cette technique permet généralement d'accélérer le temps de traitement des émetteurs déjà testés et considérés comme sûrs.

L'analyse des URL présentes dans le corps du message identifie et filtre le mail en fonction de l'action souhaitée (exemple : le click de l'utilisateur sur un lien promotionnel). Cette analyse est basée sur la détection des URLs suspectes.

Le Teergrubing est une technique utilisée pour réduire significativement la vitesse de réponse du serveur SMTP sur certaines connexions considérées comme suspectes.

Ceci permet de bloquer temporairement les serveurs de spams afin de limiter toute réexpédition ultérieure.

Le greylisting est une technique anti-spam récente. Elle consiste à rejeter temporairement un message, par émission d'un code de refus temporaire au serveur émetteur. Ce dernier réexpédiera le mail après quelques minutes, alors que la plupart des serveurs de spams ne prennent pas cette peine.

Toutes ces mesures présentent des avantages et des inconvénients. Le bon compromis consisterait à combiner ces méthodes qui doivent être implémentées selon les beoins de l'entreprise.

Les sociétés anti-spams

Devant un tel fléau et de si nombreuses mesures de protections, il n'a pas fallu longtemps pour voir apparaître des entreprises dédiées à la lutte contre le spam. Ces sociétés suivent principalement deux philosophies qui ont, toutes deux, fait leurs preuves :

- L'authentification de l'émetteur.
- L'analyse du contenu du courrier.

Pour illustrer le premier cas, citons la société française "MailInBlack" [3]. Cette entreprise propose une solution qui repose sur une authentification humaine de l'expéditeur. Une messagerie, protégée par leur service, bloquera tout nouvel email reçu dont la source est inconnue. Une demande d'authentification via un captcha [2] sera alors automatiquement envoyée à l'émetteur (voir le Schéma 1). Ainsi, la messagerie ne reçevra que des courriers dont l'adresse d'émission aura été préalablement validée. L'outil propose aussi plusieurs options comme la validation automatique de certains contacts, mais à grande échelle, ces opérations risquent de devenir très fastidieuses.

Schéma 1 : Captcha de vérification de l'expéditeur par MailInBlack

Contrairement à l'authentification de l'expéditeur, l'analyse du contenu est transparente pour l'émetteur ainsi que pour le récepteur. Cette technique, qui consiste à

appliquer différents filtres au courriel, est implémentée au sein de la solution de la société "BlackSpider" [4] (voir le Schéma 2).

Les tests proposés permettent d'affecter une note au courriel qui, en fonction de celle-ci, permettra de considérer le mail comme du spam ou non. Il existe de multiples solutions reposant sur cette philosophie. Certaines incluent même des réseaux de neurones afin de permettre une évolution autonome de la protection. Bien configurées, ces solutions permettent de lutter efficacement et de façon transparente, contre les courriers non désirés.

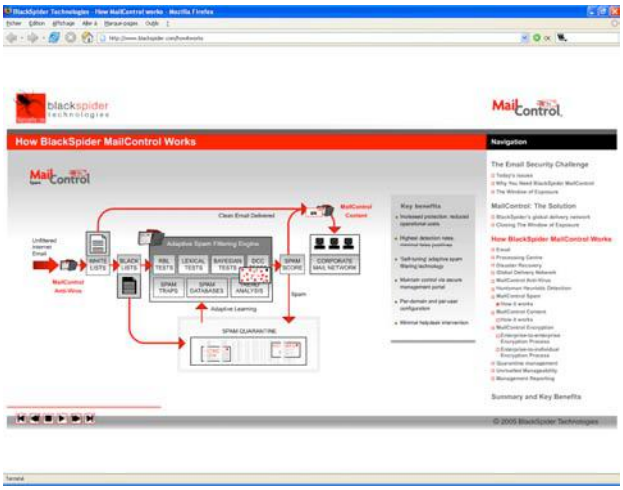


Schéma 2 : Mécanisme de vérification des emails par BlackSpider.

Les logiciels libres

Le monde de l'Open Source contribue également à la lutte contre le spamming. Le projet SpamAssassin [5] de la fondation Apache est un bon exemple. Notons que celui-ci est souvent intégré silencieusement au sein de certaines solutions antispams. Cet outil, flexible et interfaçable avec des antivirus, propose certes une solution très efficace mais nécessite cependant une configuration minutieuse. SpamAssassin utilise, entre autres, des filtres bayésiens sur le même principe que la solution de BlackSpider.

Les démarches juridiques

Dans le cadre d'éventuels actions repressives, il est nécessaire de conserver les entêtes des messages.
Ensuite, la première action à mener consiste à prévenir le propriétaire du serveur de messagerie utilisé par le spammeur, généralement un fournisseur d'accès Internet ou un hébergeur.
Vous pouvez, toutefois, déposer une plainte directement auprès de votre commissariat. Par ailleurs des informations complémentaires sont disponibles dans notre article sur la BEFTI et l'OCLCTIC dans l'édition du mois de Mai 2006 [6]. Enfin, un site Web du Ministère de la Justice est mis à votre disposition afin de vous fournir de plus amples informations sur le dépôt de plainte [7].

L'avenir des spams

Des appliances et de nouvelles solutions logicielles, promettant la suppression de tous les spams, apparaissent constamment. On assiste à une escalade entre les techniques de spamming et les contres mesures associées. Il n'est pas rare de constater que les courriers indésirables ressemblent de plus en plus à de vrais emails. En contre partie, la majorité des serveurs et des clients implémentent des protocoles sécurisés mais ne les utilisent pas. Citons en exemple, le protocole SMTP avec TLS, celui-ci assure une authentification des 2 parties à l'aide de certificats (client/serveur ou serveur/serveur), ainsi que la confidentialité des échanges. Pour ces raisons, plutôt que de toujours ajouter des "rustines temporaires" à nos infrastructures, ne serait-il pas temps de lutter contre la réelle source du problème ?

Webographie

[1] La CNIL
http://www.cnil.fr

[2] Captcha :
Mécanisme qui consiste à poser une question à laquelle une machine, et donc un robot spammeur, ne saurait répondre, comme la recopie d'un texte contenu dans une image.

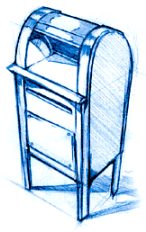
[3] MailInBlack
http://www.mailinblack.com

[4] BlackSpider
http://www.blackspider.com/

[5] Le projet SpamAssassin
http://spamassassin.apache.org/

[6] Actu-Sécu du mois de Mai 2006
http://www.xmcopartners.com/actu_secu.html

[7] Site Internet du ministère de la Justice
http://www.justice.gouv.fr/publicat/portezplainte.htm



3. TEST :

PRESENTATION DE LA SECURITE DE WINDOWS VISTA

La nouvelle mouture du célèbre système d'exploitation de Microsoft, a partiellement été dévoilée aux beta-testeurs. Il nous a été possible d'étudier les nouveautés et de nous concentrer sur la partie sécurité du successeur de Windows XP.

Nous analyserons, à travers l'installation d'une machine dédiée, les améliorations et les oublis concernant la sécurité de cet OS tant attendu.

XMCO | Partners

Premiers constats

Les améliorations de Vista sont assez nombreuses. Le but de notre test n'est donc pas de présenter toutes les nouveautés mais de vous décrire brièvement les changements notables. Nous tâcherons d'analyser concrètement la sécurité de cet OS désormais passé à la version 6.0 du noyau Windows.

L'installation

La mise en route de Vista a été plus que laborieuse. En effet, nous avons, à plusieurs reprises, essayé d'installer Vista sur différentes machines virtuelles disposant de ressources apparemment suffisantes (512 Mo de RAM). Malheureusement, seule la machine physique avec un pentium 4 , 1Go de ram et une carte vidéo de 128Mo de mémoire, a passé le test de l'installation. Un ordinateur très récent pourra implémenter un tel OS, pour les autres, le changement de la carte vidéo sera le strict minimum. Une fois la bonne machine trouvée, l'installation de Vista fut assez pratique et rapide. Seules deux boites de dialogues vinrent interrompre le cours de l'installation. Ces dernières proposent différents choix à l'utilisateur. Après une demi-heure d'attente, Vista fut enfin disponible.

La première remarque concerne la gestion des mots de passe par défaut. Lors de la création du compte principal, aucun contrôle n'est effectué sur le mot de passe entré par l'utilisateur. Le système d'exploitation aurait pu tester la sécurité du mot de passe en refusant ceux de moins de 7 caractères.

Une fois ces informations entrées, une deuxième boîte de dialogue apparaît.
Il est alors possible de choisir 3 étapes de mise à jour de l'OS :

- Le téléchargement et l'installation par défaut des mises à jour et des spywares
- L'installation des mises à jour de sécurité seulement
- Le passage à l'étape suivante

Cette mesure de sécurité est efficace car peu d'utilisateurs prennent le temps de télécharger les mises à jour de Windows. Cette boîte de dialogue oblige l'utilisateur à mettre son ordinateur à jour par un système d' icônes qui l'incite ensuite à suivre les conseils dictés par Microsoft.

L'installation est donc simple pour l'utilisateur final. Les choix restent limités et l'ensemble de la configuration est choisi par défaut. Cette nouvelle politique plaira sans aucun doute aux novices. Les experts devront se pencher davantage sur la configuration de Vista à travers le panneau de configuration qui est assez déroutant. Les icônes, les titres et les fonctions ont changé. Il faut donc un petit temps d'adaptation pour reprendre ses habitudes et configurer correctement son ordinateur.

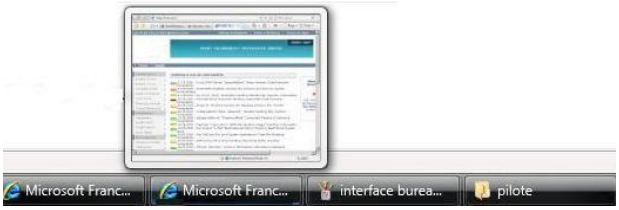
Une interface user-friendly

D'un point de vue esthétique, Vista possède de gros avantages sur son frère aîné. L'interface graphique a été revue et corrigée et se nomme désormais Avalon.

Nouveau Bureau avec le nouveau moteur graphique « Aero »

Le moteur graphique "Aero" vient ensuite se greffer pour donner des effets visuels assez impressionnants (3D, graphismes soignés, icônes…). Désormais, les fenêtres s'ouvrent et se ferment comme sur Mac OS X. La transparence est aussi une nouveauté agréable et confortable.

Enfin, le très utile "ALT+TAB" tourne les fenêtres de façon dynamique. D'autres changements notables sont à signaler. La barre des tâches et le menu Démarrer ont été joliment remaniés.
En passant sur une des fenêtres ouvertes par l'utilisateur, sur la barre des tâches, un aperçu permet de visualiser rapidement le contenu.



Aperçu du contenu de chacune des tâches ouvertes

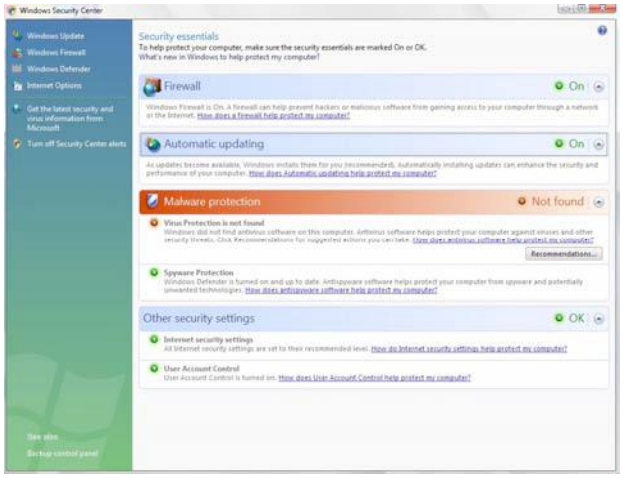
La sécurité de Windows Vista

Selon les responsables de Vista, les vulnérabilités logicielles sont réduites de 80%. Un chiffre optimiste. Vista a même été jugé comme "invulnérable" par le Chef Exécutif de Microsoft.
La montée en puissance des vers, des virus et des malware en tout genre depuis l'année dernière (54,2% à 66,4%) a même démontré qu'un ordinateur équipé de Windows XP sans protection particulière et connecté à Internet serait, dans 40% des cas, infecté en moins de 10 minutes. Microsoft compte protéger davantage ses clients et mettre en place des mécanismes capables d'endiguer ce phénomène grandissant.

En effet, la guerre contre les pirates semble bel et bien lancée avec l'apparition de cet OS. Vista est pourvu de nombreuses options de sécurité, d'un pare-feu bidirectionnel, d'un anti-spyware et pourrait même être équipé d'un anti-virus intégré dans sa dernière version.
Suivant le principe du "centre de sécurité" de Windows XP, Vista possède son "Windows Security Center". Il intègre le pare-feu, la gestion des mises à jour, la protection contre les malwares (virus non intégré, protection contre les spyware) et autres paramètres de sécurité. L'utilisateur peut donc gérer simplement l'ensemble de la sécurité de son système.
Microsoft a choisi de mettre en place de nombreuses nouveautés pour faciliter et vulgariser la sécurité des postes utilisateur.

Vista par défaut

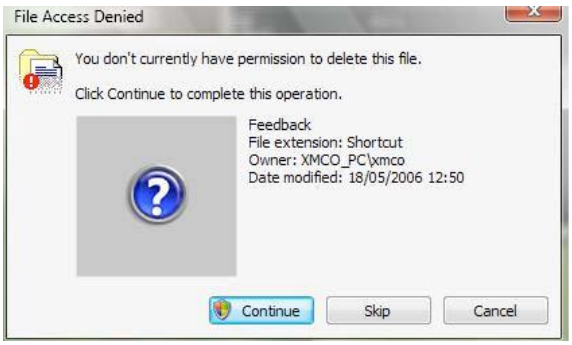
Nos premiers tests se sont portés sur les ports et les services ouverts par défaut. En scannant les ports de la machine test, nous avons remarqué un point intéressant qu'il est important de souligner. Les échos aux « Ping » d'une machine distante ne sont pas envoyés. En effet, Vista ne répond pas aux messages ICMP qui proviennent du réseau. Cette option peut bien sûr être modifiée mais reste cependant un premier obstacle aux pirates. Les attaquants cherchent souvent leurs victimes en lançant un scan. Il ne reste plus qu'à attendre les réponses ICMP pour identifier les machines en ligne et de fait, disponibles.
Peu de ports sont ouverts (135 : rpc, 139 : netbios et le port 445). Le pare-feu et l'antispyware sont activés par défaut. Par ailleurs, la gestion des options de sécurité d'Internet Explorer est accessible via le centre de sécurité. Un utilisateur non spécialisé peut donc facilement identifier les options lui qui permettent de sécuriser son navigateur (contrairement à Windows XP où l'onglet « Sécurité » est caché dans des options). Enfin, les gestions de comptes peuvent désormais se faire entièrement depuis cette interface. En parcourant attentivement l'ensemble de ce menu, l'utilisateur pourra atteindre un seuil de sécurité satisfaisant sans trop d'effort.



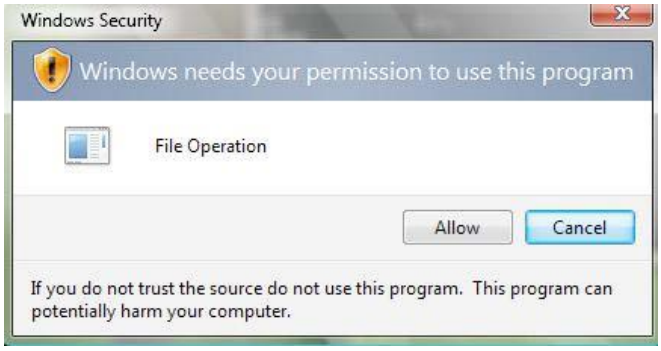
Centre de sécurité de Windows Vista

Ces premiers points confirment la volonté réelle de Microsoft de faciliter la configuration des paramètres de sécurité et renforcent la protection native de Windows Vista.
Cependant, cette protection accrue laisse entrevoir certains points négatifs. En effet, Vista scanne en permanence les fichiers exécutés. Une boîte de dialogue demande donc la confirmation de chaque action ce qui est assez désagréable. Il faut, ainsi, valider 3 boîtes de dialogue avant de pouvoir lancer la suppression d'un simple raccourci du bureau!

1ère boite de dialogue de suppression « classique »



2ème boite de dialogue en fonction des permissions

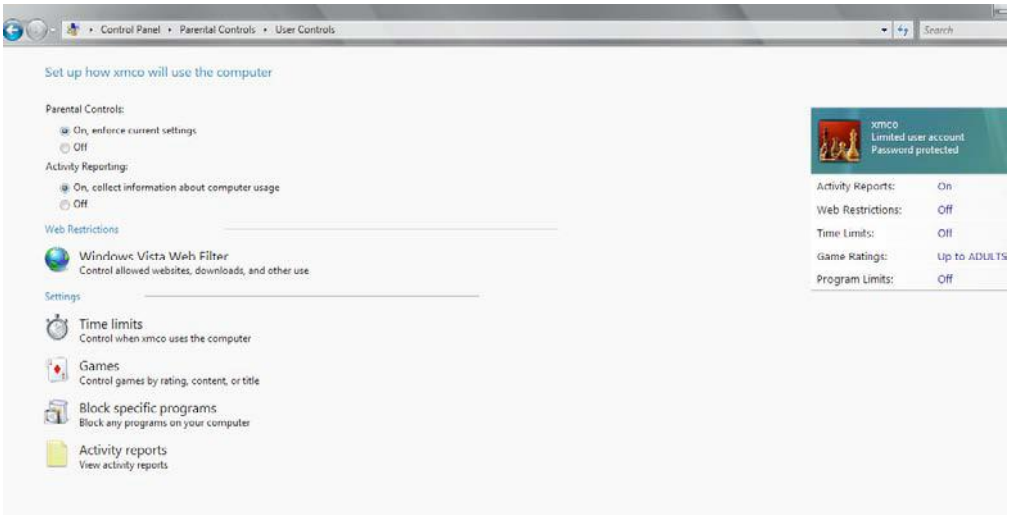


3ème boite de dialogue

Ces boîtes de dialogue et d'alertes à répétition sont certes utilisées pour prévenir l'utilisateur d'éventuelles actions malencontreuses, mais deviennent particulièrement gênantes dès la deuxième suppression de fichiers.

Contrôle parental

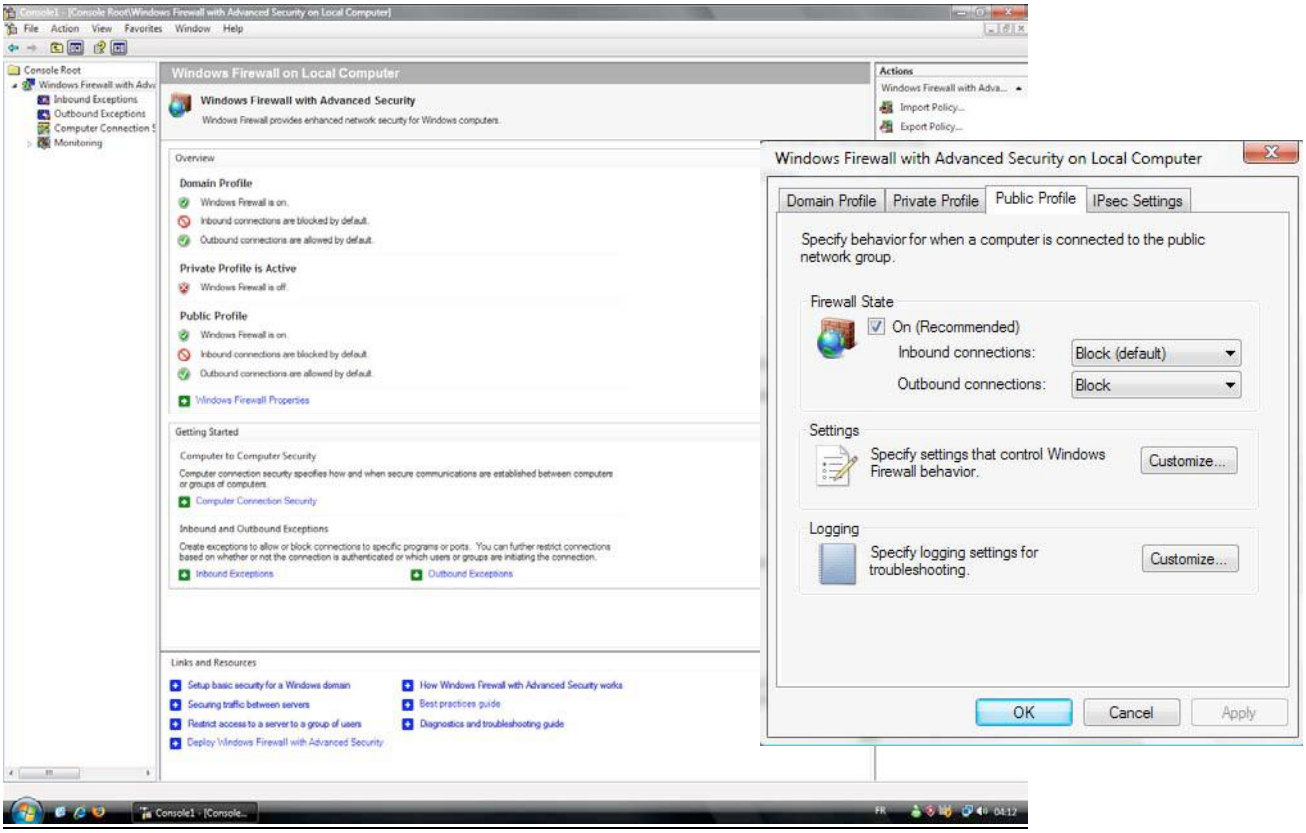
Une autre service, utile et pratique, pour les utilisations familiales de l'ordinateur, a été mise en place. Il est maintenant possible de contrôler efficacement l'activité de comptes sous-jacents afin de réprimer et d'interdire l'accès à certaines ressources et/ou programmes. Les sites web peuvent être bloqués et les droits de chacun peuvent être configurés à partir des tranches d'âges et des heures d'accès des différents utilisateurs. L'accès aux jeux est aussi contrôlé par deux systèmes de classification : l'ESBR (Entertainment Software Rating Board) et le PEGI (Pan-European Game Information). Toutes les actions sont ensuite loguées et consultables par l'administrateur.
Le contrôle parental est donc une option intéressante pour un usage familial de la machine. En effet, toutes les activités d'un compte peuvent être enregistrées et/ou bloquées.



Interface du paramétrage du contrôle parental

Le pare-feu

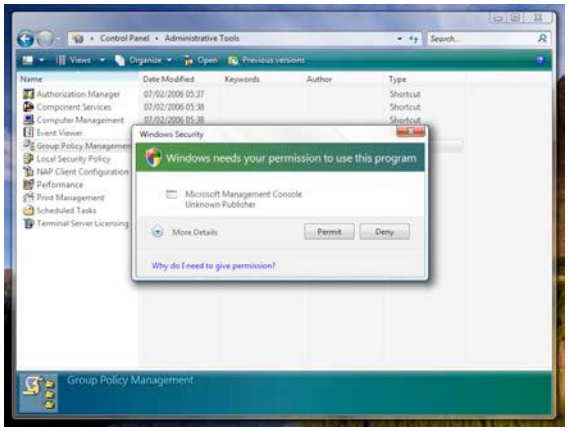
L'augmentation des attaques en tout genre, ont poussé les responsables de Vista à intéger un firewall digne de ce nom. En effet, la version finale disposera d'un véritable firewall capable de rivaliser avec les concurrents de ce marché. L'outil de configuration avancé est paramétrable via la console MMC (Microsoft Management Console) et permet d'obtenir toutes les options nécessaires à la sécurité (liste des processus autorisés, protocoles, etc…). Les flux sortants sont donc à présent contrôlés. La fonction est, par défaut, désactivée mais désormais disponible.
Cependant, il faudra attendre un peu avant de voir apparaître la version finale de ce produit. En effet, toutes les fonctionnalités ne sont pas encore disponibles…

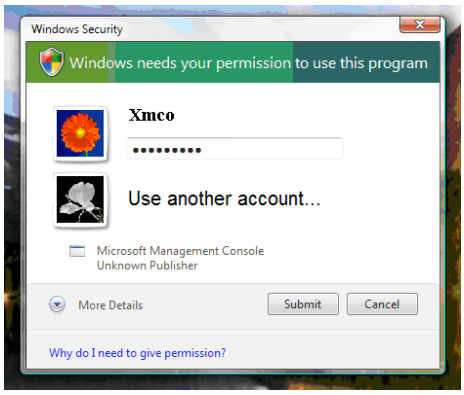


Configuration avancée du pare-feu

Les comptes utilisateurs

Une des grandes nouveautés reste la gestion des comptes. Auparavant, seul un compte « administrateur », utilisé par la majorité des utilisateurs, et un compte « invité » avec des droits restreints, étaient disponibles. En ce qui concerne le compte « administrateur », la compromission d'un système permettait une prise totale de la machine cible. C'est pour cette raison que Vista intègre un compte « utilisateur limité » qui ne pourra pas accéder au cœur du système. Le compte « administrateur » ne sera plus proposé par défaut et le mot de passe sera demandé lorsque les actions nécessiteront une élévation de privilèges. Enfin, les boîtes de dialogue, utilisées à outrance, permettront de limiter les actions de logiciels malveillants. La confirmation manuelle devient ainsi obligatoire et limitera les exécutions automatiques.

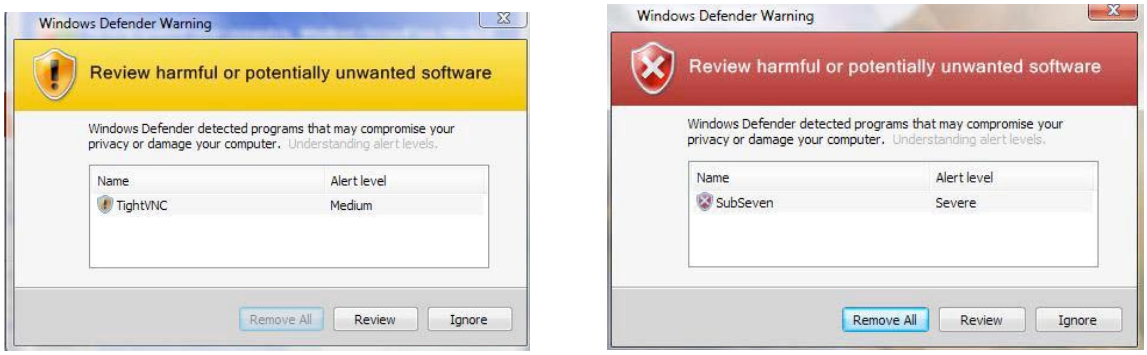




Demande d'autorisation pour l'exécution d'actions sensibles

Windows Defender (anti-spyware)

Un nouvel outil intègre également cette nouvelle mouture. Microsoft s'était déjà essayé à la recherche de spywares en tout genre (adware, keyloggers, chevaux de Troie). Microsoft décide ainsi d'intégrer Microsoft AntiSpyware qui devient « Windows Defender » dans Vista. Ce programme devrait renforcer considérablement la sécurité du système. Cet outil protège et détecte en temps réel tous les programmes malicieux. Windows Defender est inclus nativement dans Vista et est chargé en mémoire avant l'exécution d'un fichier malicieux. Cet utilitaire a déjà prouvé son efficacité et reste l'un des logiciels les plus efficaces dans ce domaine.
Nous avons testé Windows Defender en exécutant un troyen connu (« Subseven »). Ce dernier fut immédiatement reconnu. Une boîte de dialogue suggère alors les différentes actions à entreprendre.

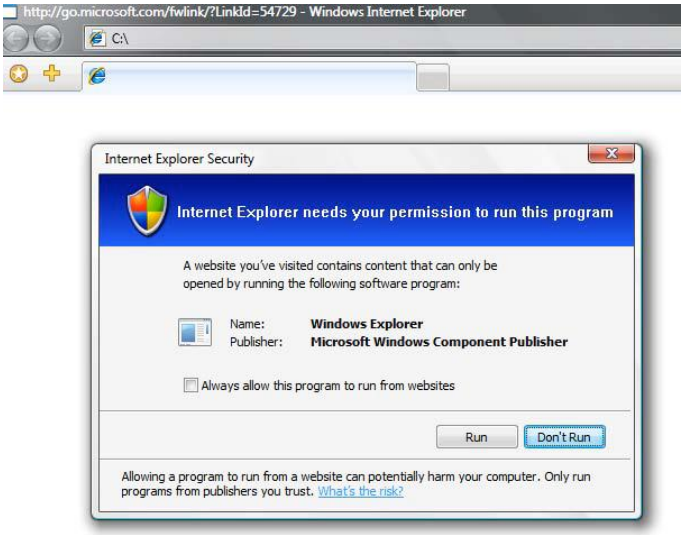


Alerte pour les logiciels dangereux utilisés

Internet Explorer 7

La nouvelle mouture du célèbre navigateur de Microsoft est incluse dans Vista. Cette application offre des options intéressantes. Par exemple une option anti-phishing qui permet de prévenir l'utilisateur des sites douteux qu'il visite. En effet, une liste des sites frauduleux est régulièrement mise à jour par Microsoft et alerte immédiatement l'utilisateur lors d'une visite d'un tel site (barre d'adresse vire au rouge).

De plus, le mode de fonctionnement d'IE a été revu. En effet, l'exécution du navigateur est désormais réalisée au sein d'une zone protégée. Ceci renforce la sécurité et établit une frontière distincte entre le système d'exploitation et le navigateur. L'accès aux disques durs via IE est donc devenu impossible. Aucune interaction directe n'aura donc lieu et les attaques via IE seront donc fortement limitées voir quasiment impossible. Il faudra donc attendre la version finale de cette fonction pour juger de sa pertinence.



Accès aux disques durs impossible via Internet Explorer 7

Windows Mail

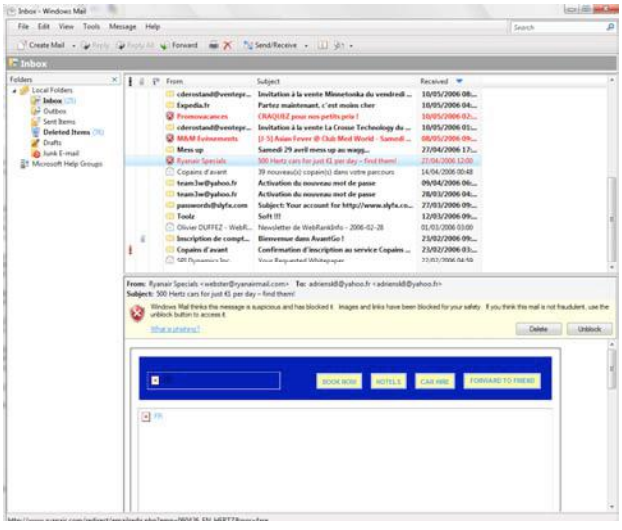
Windows Mail remplace le célèbre Outlook. Le gestionnaire de mail est désormais puissant. Il gère les flux RSS et apparaît plus clair et plus facile à utiliser. Différentes options de sécurité sont intéressantes à décrire. Par exemple, il est dorénavant possible d'établir une liste noire des envoyeurs douteux.

Un filtre « anti-phishing » a été mis en place. Windows Mail se base sur des mots-clefs qui pourraient être associés à de tels emails :

Filtre Anti-phishing

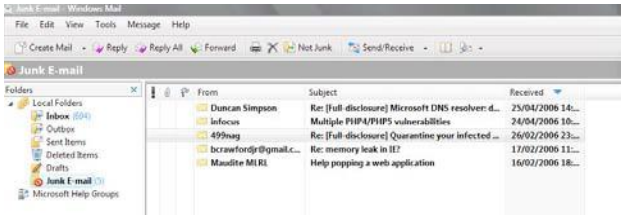
Par ailleurs, l'application détecte, dès la réception, les emails douteux. Les images et les scriptes capables d'être exécutés à l'ouverture d'un email sont bloqués et un message prévient clairement l'utilisateur :

"Windows Mail pense que ce message peut être suspect et a été bloqué. Les images et les liens ont également été bloqués pour la sécurité de votre système. Si vous pensez que cet email n'est pas malicieux, utilisez le bouton 'Débloquer' pour avoir accès à votre message".



Dossier « Junk email » réservé aux emails douteux

Enfin un filtre anti-spam a été intégré. Cette option, proposée dans Outlook 2003, repose sur l'utilisation d'algorithmes bayésiens. Trois différents modes sont donc paramétrables : le niveau « bas », le niveau « haut » et le niveau « paranoïaque ». La différence est uniquement basée sur le filtrage. Par exemple le dernier mode aura, la particularité de bloquer les emails qui ne viennent pas de votre carnet d'adresses. Tous les emails douteux seront alors placés dans un dossier nommé « Junk email ».



Dossier « Junk email » réservé aux emails douteux

Dossier Junk email

En vrac

D'autres points sont importants à signaler.
Les partages par défauts (images) ne sont pas activés. Il est donc nécessaire d'autoriser les utilisateurs du réseau à accéder aux dossiers partagés. Enfin, plusieurs utilitaires seront particulièrement appréciables pour des administrateurs ou des utilisateurs exigeants. Le premier, nommé Bit Locker Drive Encryption, permet de chiffrer à la volée les données. Ceci afin de sécuriser davantage les fichiers stockés. Le second, baptisé Tighter Control, limitera l'accès aux supports amovibles. Les administrateurs pourront ainsi contrôler l'accès équipements USB sur leur parc informatique.

Conclusion

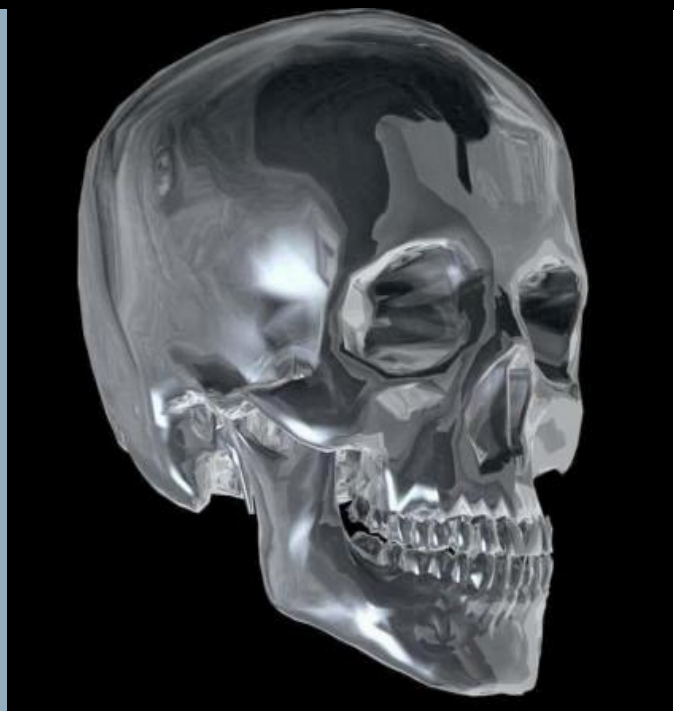
Microsoft a donc compris que les menaces et la compromission d'un système passe par le net. La sécurité a été revue sur tous les points sensibles. Tous les logiciels sont désormais protégés. Par ailleurs, pour l'utilisateur final, Vista offre une sécurité accrue. En suivant les mises à jour et les conseils de Vista, les utilisateurs lambda devront être à même de surfer sur Internet sans trop de problème.
Enfin, reste à savoir combien de temps ces menaces externes continueront d'être contrées…

4. ATTAQUES MAJEURES :

TOP 5 DU MOIS DE MAI :

Le mois de Mai a été marqué par des failles de sécurité critiques au sein des logiciels des plus grands acteurs du marché.
Microsoft a été victime d'un exploit "zero-day" basé sur une faille de Word. IBM a également publié un correctif pour plusieurs failles présentes dans Websphère. Symantec, qui a limité la fuite d'informations, a découvert une faille au sein de son antivirus. Enfin Novell a été victime d'une faille de sécurité au sein de son service d'impression NDPS

XMCO | Partners



WORD

Attaque distante via un document Word contrefait dissimulant un Cheval de Troie.

Une vulnérabilité critique et un exploit « zero-day » ont été publiés sur Internet. En effet, une faille de sécurité dans Microsoft Word a été découverte le lundi 22 Mai.

Cette faille est due à un débordement de tampon provoquée par l'ouverture d'un fichier Word judicieusement contrefait. L'exploitation de cette faille permet d'exécuter du code. Un cheval de Troie dissimulé au sein d'un tel document est ainsi exécuté et installé.

Les vecteurs d'attaque sont multiples. Le document Word spécialement conçu peut être hébergé sur un site Web malicieux ou envoyé par email. L'attaquant doit seulement inciter la future victime à ouvrir ce document ce qui provoque l'exécution immédiate du Troyen.

Une fois installé sur la machine cible, le programme malicieux s'efface de lui-même du fichier Word et commence des actions malveillantes (collecte d'informations, niveau des correctifs, type d'antivirus, lancement au démarrage de la machine infectée) en s'appuyant sur des techniques de rootkits pour dissimuler ses composants sur le système. Puis il se connecte à un serveur pirate hébergé en Chine (par le port 80 afin de contourner les pare-feux) et envoie les données récoltées.

Différents noms ont été attribués à ce programme malicieux : W32/Ginwui.A.dr, Backdoor.Ginwui, W32/Ginwui.A, Trojan.Mdropper.H, Troj/Oscor-B ou encore "BackDoor-CKB!cfaae1e6".

Notons que l'infection des autres postes sera effective que lorsque les cibles auront tenté d'ouvrir le document Word contrefait.

Ce programme malicieux effectue les actions suivantes lorsqu' il infecte une machine :

1. Exécution d'un cheval de Troie dès l'ouverture du fichier Word malicieux.
2. Suppression du code malveillant du document Word qui devient sain.
3. Installation de la librairie winguis.dll
4. Modification de la base de registre de manière à se lancer automatiquement à chaque redémarrage de la machine vérolée. La clef de registre modifiée est la suivante ([HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows]"AppInit_DLLs" = "%WinSysDir%\winguis.dll").

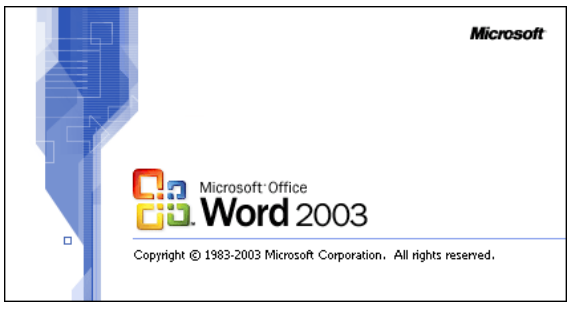
Actions réalisées par le cheval de Troie

Programmes vulnérables :

- Word 2002
- Word 2003

Criticité : Elevée

Référence Xmco : n° 1148284079



Microsoft Exchange

Une vulnérabilité dans Microsoft Exchange pourrait permettre l'exécution de code à distance (MS06-019)

Un correctif relatif aux différentes versions du serveur de messagerie Exchange a été publié par Microsoft. Il s'agit d'un type cumulatif qui remplace le précédent correctif MS05-048.

Cette faille provient d'une mauvaise gestion de certains contenus MIME par des interfaces Exchange. Un attaquant distant pouvait exploiter cette vulnérabilité dans le but d'exécuter du code arbitraire et prendre ainsi le contrôle total du système affecté.

Cette vulnérabilité concerne les systèmes possédant le serveur de messagerie Exchange.
Il est probable que des virus ou que des vers qui exploitent cette vulnérabilité voient prochainement le jour. En effet, aucune identification n'est nécessaire, les serveurs Exchange pourront donc devenir victime d'attaques virales.

Programmes vulnérables :
- Microsoft Exchange Server 2003 SP1/SP2/SP3

Criticité : Elevée

Référence Xmco : n° 1147244818

Websphere

Plusieurs vulnérabilités dans le logiciel d'IBM Websphere

Plusieurs failles de sécurité au sein du produit WebSphere Application Server d'IBM ont été découvertes. Ces failles de sécurité résultent d'erreurs diverses permettant à un attaquant de récupérer des informations sensibles ou de contourner des mesures de sécurité.
En effet, sept vulnérabilités ont été identifiées.

La première faille de sécurité concerne la mauvaise gestion de l'authentification. Par défaut, l'utilisateur de l'application doit s'authentifier sur la page « http://ServerHost/webapp_context/homepage.jsp ». Or, en forgeant une url spécifique, il serait possible d'accéder à l'application sans identification préalable.
En utilisant l'url suivante : "http://ServerHost/webapp_context/", le pirate serait logué sans être redirigé vers la page d'authentification.

Le deuxième problème est lié au stockage non sécurisé de mots de passe. En effet, lors de l'ajout de nœud réseau dans DMGR, des informations sensibles sont alors sauvegardées dans le fichier addNode.log en clair. Ce fichier permettrait à un pirate d'utiliser le compte d'un autre utilisateur à des fins malveillantes.

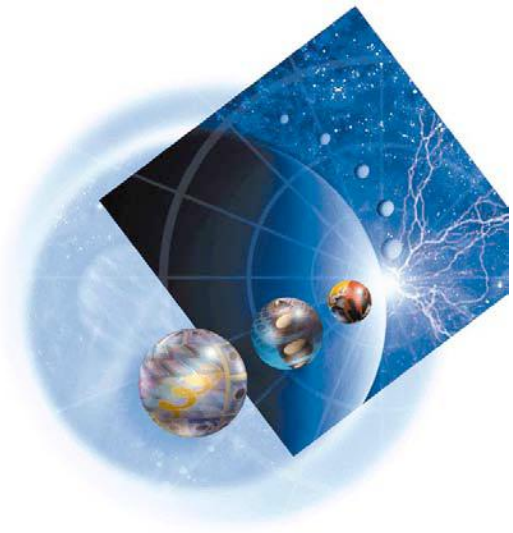
Le troisième problème résulte d'une erreur du module de traitement des requêtes HTTP. En effet, un attaquant distant serait en mesure d'accéder à des informations sensibles en soumettant des requêtes HTTP judicieusement contrefaites. D'autre part, des injections de scripts seraient également possibles en soumettant des urls spécialement forgées.

Enfin plusieurs vulnérabilités non précisées de la console d'administration, du module « WebSphere Common Configuration and CommonArchive » ainsi que le module de traitement de jetons LTPA malformés ont été corrigées.

Programmes vulnérables :
- IBM Websphere Application Server 5.x
- IBM Websphere Application Server 6.x

Criticité : Elevée

Référence Xmco : n° 1147170869



Symantec

Compromission d'un système via un fichier spécialement conçu

SYMANTEC a publié une mise à jour de sécurité pour son Antivirus. En effet, un utilisateur malveillant pouvait exploiter cette faille à distance afin de prendre le contrôle total de la machine.

Le problème provient d'un mauvais traitement des fichiers malformés. En envoyant un fichier judicieusement conçu, un attaquant pouvait causer un débordement de tas et exécuter du code arbitraire a distance en disposant des privilèges SYSTEM.

Ces droits d'accès étant supérieurs à ceux de l'administrateur, le pirate hériterait du contrôle total de la machine infectée sans aucune intervention de l'utilisateur.
Cette faille de sécurité présente tous les ingrédients nécessaires pour devenir un véritable vecteur de vers.

Programmes vulnérables :

- Symantec Antivirus 10.1
- Symantec Client Security version 3.1

Criticité : Elevée

Référence Xmco : n°1148885733

Novell

Débordement de tampon au sein du service d'impression NDPS

Une vulnérabilité distante a été découverte et corrigée au sein de Novell Netware. L'exploitation à distance de celle-ci permettait la compromission ou l'altération d'un système vulnérable.

Le problème provient d'une erreur de type "Integer Overflow" du module NetWare Distributed Print Services (NDPS/iPrint). Ce module ne traitait pas correctement certaines requêtes malformées, ce qui pouvait être exploité par une personne malveillante afin d'exécuter du code arbitraire.

Programmes vulnérables :

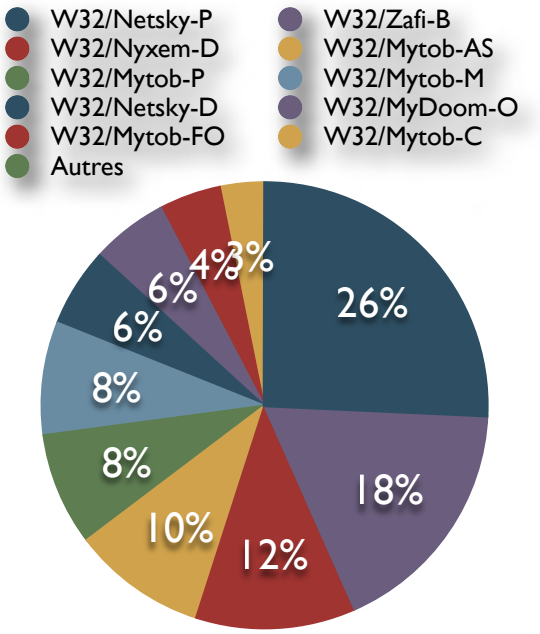
- Novell Netware (Toutes les versions)
- Novell Open Enterprise Server (Toutes les versions NetWare)
- Novell Netware Client for Windows (Toutes les versions)

Criticité : Elevée

Référence Xmco : n° 1147704408

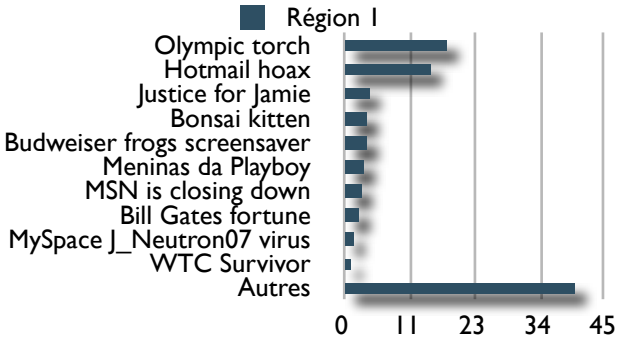
Sinon....

Activité virale du moi de Mai 2006



Activité virale du moi de Mai 2006

Canulars du moi de Mai 2006



5. OUTILS LIBRES :

FOCUS SUR 5 PRODUITS LIBRES

Chaque mois, nous vous présenterons les outils libres qui nous paraissent indispensables. Les logiciels abordés sont variés : utilitaires de sécurité et autres programmes nécessaires au sein d'une entreprise.

Pour ce quatrième numéro, nous avons choisi d'analyser un utilitaire bootable de maintenance, deux logiciels de chiffrement, un antispyware et un outil d'administration réseau.

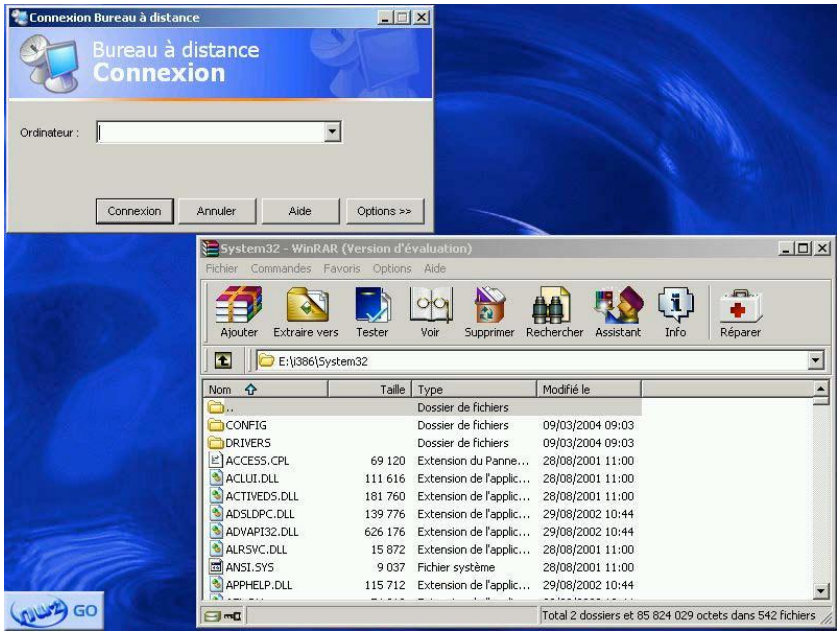
- *BartPE : utilitaire de création d'images ISO bootable permettant de démarrer son PC sans OS*
- *Search&Destroy : antispyware pour les postes de travail*
- *GnuPG : version libre de l'utilitaire de chiffrement PGP de mails*
- *TrueCrypt : outil de chiffrement de fichier*
- *ArpWatch : table dynamique d'adresses Mac et IP d'un réseau*

Vous trouverez à la fin de cette section un tableau récapitulatif des versions de tous les logiciels présentés lors des précédents numéros d' « Actu Sécurité ».

XMCO | Partners

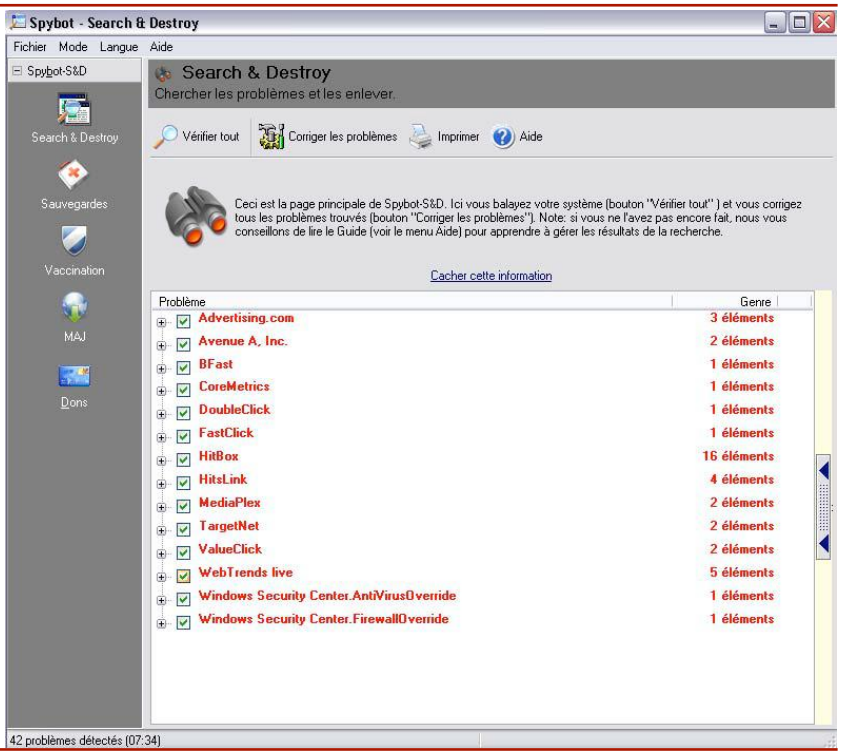
BartPE

Utilitaire de création de Live CD Windows

Version actuelle	Bart's PE Builder V3.1.10a
Utilité	★★★★★
Type	Outils de création de fichier ISO bootable pour la maintenance de machines Windows
Description	BartPE est un logiciel qui permet de créer des fichiers ISO bootable. A partir d'un système d'exploitation Windows, ce programme permet de créer une version de Windows allégée possédant ses propres utilitaires. La maintenance d'un système est alors facilitée et les données d'un ordinateur sans OS (ou possédant un OS qui ne démarre plus) peuvent être récupérées. Le CD remplaçera toutes les disquettes ou clefs USB bootables. Chaque soft choisi peut avoir un interêt réel (gravure, connexion à un partage réseau…).
Capture d'écran	
Téléchargement	BartPE est disponible à l'adresse suivante : http://severinterrier.free.fr/Boot/PE-Builder/#download
Sécurité de l'outil	L'outil étant méconnu, aucune faille n'a été découverte à ce jour.
Avis XMCO	BartPE est un logiciel pratique pour effectuer de nombreuses opérations sur un système qui ne possède pas d'OS. Il est ainsi possible de récupérer des donnée, de graver et d'accéder au réseau sans pour autant installer un système d'exploitation. Le CD créé est entièrement paramétrable et facile à réaliser. Cet un outil qui deviendra vite indispensable aux techniciens et aux administrateurs système.

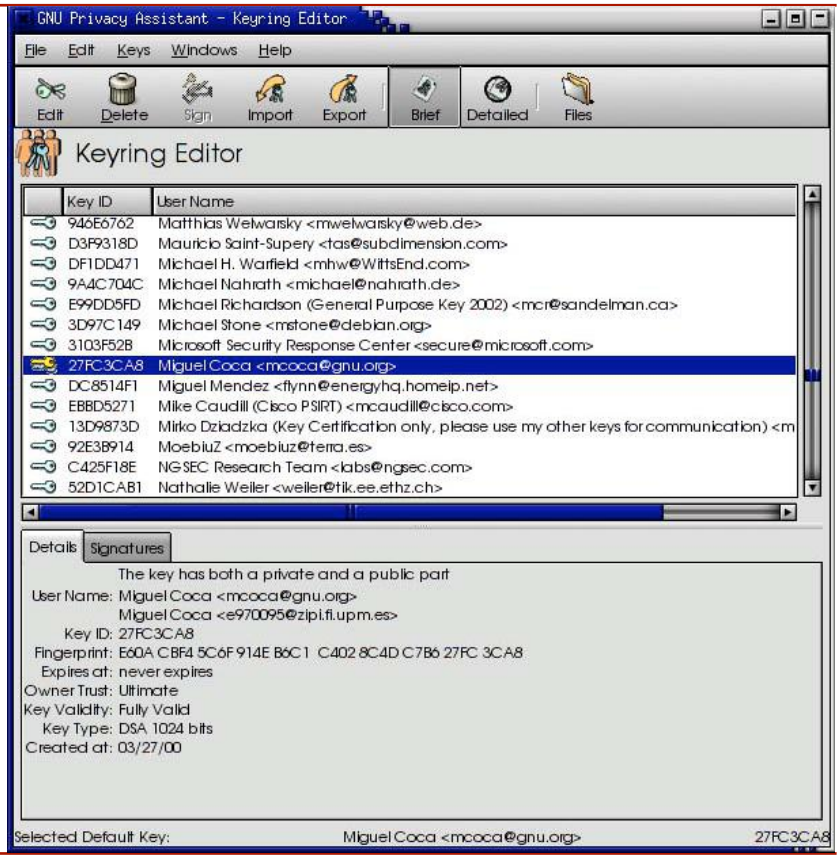
Search&Destroy

Utilitaire anti-spyware

Version actuelle	Search & Destroy 1.4
Utilité	
Type	Antispyware
Description	Search&Destroy est un anti-spyware capable de détecter et d'éliminer un nombre impressionnant de logiciels espions en tout genre. Sa base de connaissance comporte près de 40 000 signatures. Il élimine rapidement les logiciels espions (cheval de Troie, Keyloggers…) et les adware (publicité). Sa base de connaissance enrichie chaque jour des derniers programmes malicieux, permet de tenir à jour son ordinateur et d'éviter les attaques et les problèmes en tout genre.
Capture d'écran	
Téléchargement	Disponible en 51 langues, Search&Destroy reste la référence dans ce domaine. Seulement utilisable sur des plateformes Windows : http://www.safer-networking.org/fr/mirrors/index.html
Sécurité de l'outil	Aucune faille n'est connue à ce jour.
Avis XMCO	Search&Destroy reste la référence en matière d'outils anti-spyware. Peu de logiciels tiennent vraiment la route dans ce domaine. Windows Defender, principal rival, n'est pas aussi efficace dans la recherche d'adware et de chevaux de Troie. Son utilisation est cependant recommandée sur un poste final.

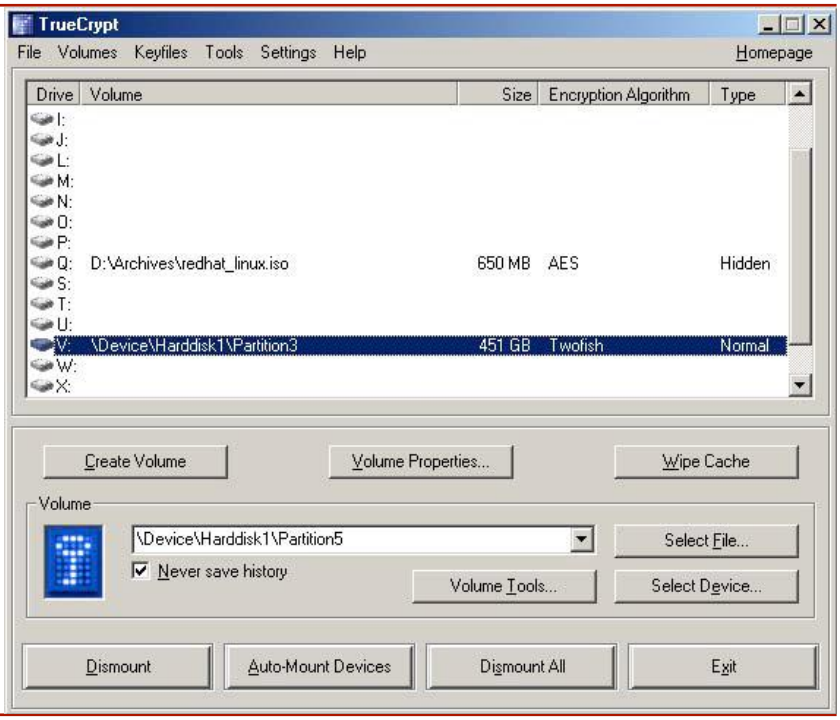
GnuPG

Logiciel de chiffrement d'emails

Version actuelle	GPG 1.4.3 .
Utilité	★★★★★
Type	Logiciel de communication sécurisée
Description	GnuPrivacy Guard (Gardien de vie privée), est un logiciel de communication sécurisé utilisant le chiffrement asymétrique. Il remplace PGP développé par le célèbre chercheur, Philip Zimmermann et est devenu la version gratuite et libre du standard de cryptographie forte OpenPGP. Celui-ci permet d'intégrer, au sein du client de messagerie, une authentification, d'assurer la confidentialité et la non-répudiation des emails.
Capture d'écran	
Téléchargement	GnuPG 1.4.3 est disponible sur toutes les plateformes à l'adresse suivante : http://www.gnupg.org/(fr)/download/
Sécurité de l'outil	Très peu de failles ont été identifiées pour les trois dernières versions de GnuPG. Cet outil est donc sûr. http://secunia.com/product/2573/ http://secunia.com/product/309/ http://secunia.com/product/2591/ http://secunia.com/product/8087/
Avis XMCO	GnuPG est un logiciel incontournable de chiffrement de courrier électronique. Gratuit, puissant et simple d'utilisation, il restera encore longtemps la référence des logiciels qui assure la confidentialité des messages électroniques.

TrueCrypt

Utilitaire de chiffrement de fichiers

Version actuelle	TrueCrypt 4.2
Utilité	
Type	Outil de chiffrement de fichiers
Description	TrueCrypt est un logiciel qui permet de chiffrer à la volée chaque document sauvegardé, de façon transparente pour l'utilisateur. Utilisant des algorithmes forts (AES, Triple DES…), cet outil se configure simplement. Il suffit de créer un fichier appelé "conteneur" qui stockera les fichiers chiffrés. Ce conteneur doit être affecté à un volume qui ne pourra seulement être accessible qu'avec un mot de passe entré dans l'interface du logiciel. Ainsi, lorsque ce volume est « démonté », personne ne pourra accéder à vos données.
Capture d'écran	
Téléchargement	TrueCrypt est disponible à l'adresse suivante : http://www.truecrypt.org/downloads.php
Sécurité de l'outil	L'outil étant méconnu, aucune faille n'a été découverte à ce jour.
Avis XMCO	TrueCrypt est un logiciel pratique. Toutes vos données écrites sur un volume créé au préalable sont chiffrées de manière transparente. Les informations sensibles peuvent donc être gardées et stockées en toute tranquillité.

ArpWatch

Utilitaire réseau

Version actuelle	ArpWatch
Utilité	★★★★★
Type	Logiciel de contrôle d'accès au réseau.
Description	Arpwatch est un outil qui permet de gérer l'activité d'un réseau en maintenant une base de données des IP et des adresses MAC à partir des requêtes ARP. Dès qu'un ordinateur se connecte sur le réseau local, l'affichage mis à jour permet de repérer les nouveaux équipements du réseau. Des fonctions de suivi par email sont également disponibles. Basé sur la librairie libpcap, ce logiciel contrôlera et logguera toute tentative d'intrusion physique sur votre réseau.
Capture d'écran	
Téléchargement	ARPWatch est disponible à l'adresse suivante : ftp://ftp.ee.lbl.gov/arpwatch.tar.gz
Sécurité de l'outil	L'outil étant très léger et méconnu, aucune faille n'a été découverte à ce jour.
Avis XMCO	Arpwatch est un outil réseau très utile dans le monde de l'entreprise. Les administrateurs réseau peuvent ainsi gérer simplement leurs infrastructures et repérer les connexions non autorisées.

Suivi des versions

Versions actuelles des outils libres présentés dans les numéros précédents.

Nom	Dernière version	Date	Lien
Debian Sarge	Version stable 3.1 r2	19/04/2006	http://www.debian.org/CD/netinst/
Snort	2.4.4	14/04/2006	http://www.snort.org/dl/
MySQL	5.0.21		http://dev.mysql.com/downloads/mysql/5.0.html
	5.1.9-Bêta		http://dev.mysql.com/downloads/mysql/5.1.html
Apache	2.2.2		http://www.apachefrance.com/Telechargement/4/
	1.3.36		http://www.apachefrance.com/Telechargement/4/
Nmap	4.03	01/04/2005	http://www.insecure.org/nmap/download.html
Firefox	1.5.0.4	06/2006	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	1.5.0.2	04/2006	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.1.2	25/05/2006	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.58		http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV	0.88.2.3	05/2006	http://www.clamav.net/stable.php#pagestart http://www.clamwin.com/content/view/18/46/
Ubuntu	6.06 Drapper Drake	06/2006	http://www.ubuntu-fr.org/telechargement
Postfix	2.2		ftp://ftp.club-internet.fr/pub/mirrors/ftp.porcupine.org/postfix-release/index.html
Squid	2.5	20/05/2006	http://www.squid-cache.org/Versions/v2/2.5/
Filezilla	2.2.24a		http://filezilla.sourceforge.net/
OpenSSH	4.3	01/02/2006	http://www.openssh.com/