SECTION INTERNET DU CLUB MEDERIC DE MARSEILLE

Internet Gazette

Site : http://aviquesnel.free.fr/Mederic

07 mai 2007
Numéro 49

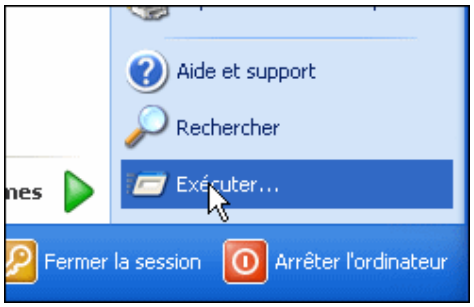
Sommaire

Désactiver le logiciel de gravure intégré de Windows XP

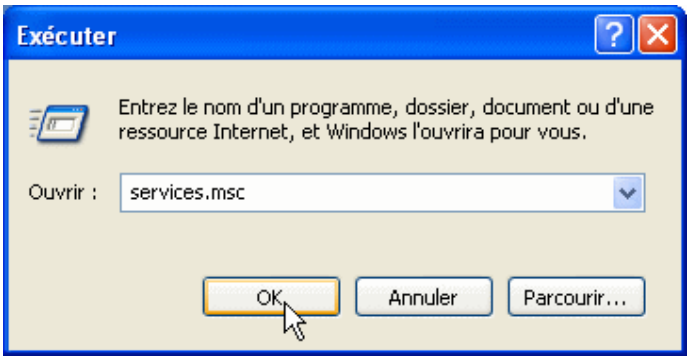
Windows XP dispose d'une version très allégée du logiciel de gravure Easy CD Creator. Malheureusement, ce logiciel est la cause de nombreux problèmes et de conflits si vous utilisez un autre programme tel que Nero, Clone CD, etc, pour graver vos CD.

Si vous utilisez un autre logiciel de gravure, nous vous conseillons de désactiver le logiciel de gravure intégré à Windows XP.

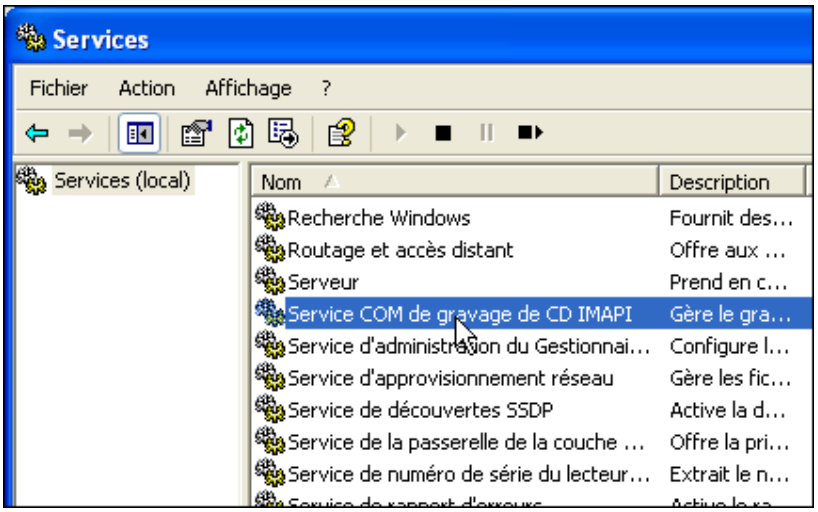
1. Cliquez sur le bouton **Démarrer** puis sur **Exécuter**.



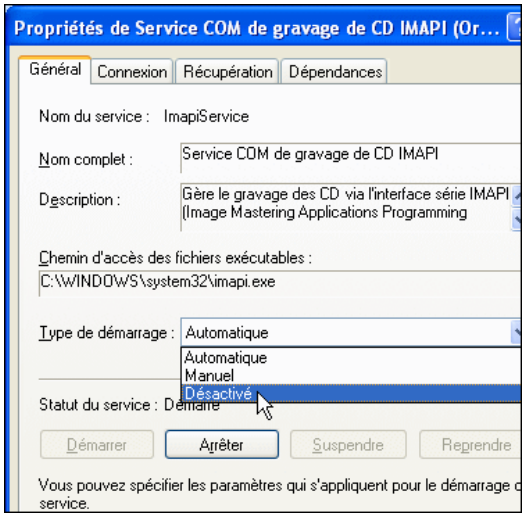
2. Saisissez la commande **services.msc** puis cliquez sur le bouton **Ok**.



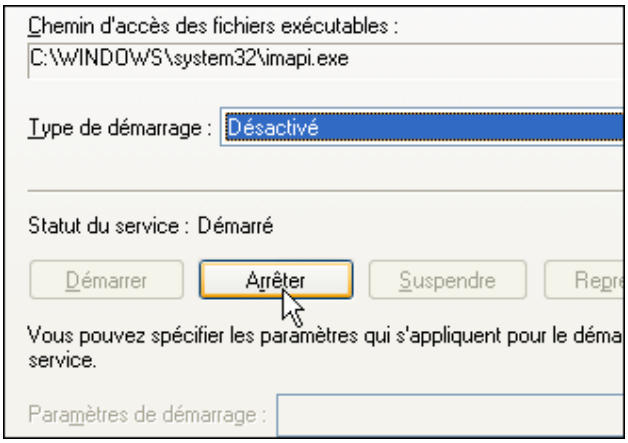
3. Dans la liste qui s'affiche, double cliquez sur **Service COM de gravage de CD IMAPI**.



4. Déroulez ensuite la liste **Type de démarrage** et sélectionnez l'option **Désactiver**.



5. Cliquez ensuite sur le bouton **Arrêter**.



6. Cliquez enfin sur le bouton **OK** puis fermez la console des services. Le service de gravure intégré à Windows XP est alors désactivé.

Etude anglaise sur la pertinence des grands moteurs

Un journaliste de la revue britannique IWR (Information World Review) a réalisé une petite étude destinée à mesurer la pertinence des 6 premiers moteurs de recherche (en terme de PdM) au Royaume Uni : Google, Yahoo!, Ask, Microsoft (Live Search), AOL et Orange.

Méthodologie : les moteurs ont été interrogés avec les 10 requêtes ci-dessous, couvrant différents aspects de la recherche sur le web (désambiguisation, localisation, langage naturel, date, parenthèses et booléens...). Puis, on été comptés, au sein des 10 premiers résultats (non sponsorisés), les résultats pertinents.

Les requêtes :
- *Apple Pie" –"Apple Computers"*
- *("Microsoft Office Online" OR "MS Office Online") NEAR (Outlook –"Outlook Express")*
- *Plumbers in New Cross*
- *Raleigh*
- *What time is it in Bangalore?*
- *iPAQ hw6900*
- *08700 100 222*
- *22/11/1963*
- *"pas de bourre"* (terme de ballet)
- *Information World Review :* sans guillemets

Pour chaque moteur, les résutlats sont commentés en détail. Au toal, cela donne le classement suivant :
Google : 70% de pertinence
Yahoo! 68%
Ask 41%
Microsoft 52%
AOL 64%
Orange 28%

Attention cependant à ces résultats quanti : l'écart de 2% entre Google et Yahoo! a peu de siginification car l'échantillon de résultats analysés (10x10 par moteurs) est faible.

Sécurité le web désormais plus dangereux que les emails

Si les messageries sont bien filtrées, il n'en va pas de même pour le Net. Selon l'expert en sécurité Trend Micro, l'accès aux sites web devient la principale menace pour les internautes. Et le business du piratage complique la tâche des éditeurs.

D'ici à 2008, les attaques propagées sur le web auront pris le pas sur celles affectant les e-mails prévoit le spécialiste de la sécurité Trend Micro, troisième éditeur mondial d'antivirus.

Jusqu'à aujourd'hui les messageries électroniques ont été la principale voie empruntée par les pirates pour diffuser chevaux de Troie ou virus sur les ordinateurs des internautes. Mais le web est de plus en plus utilisé pour prendre le contrôle de machines à l'insu des utilisateurs, qui téléchargent du code nocif lorsqu'ils accèdent à des pages truquées, comme l'ont expliqué des représentants de l'éditeur lors du Gartner Symposium and ITxpo à San Francisco cette semaine.

«On ne peut pas bloquer le port 80»

La raison est simple: les outils de sécurité pour les e-mails sont désormais bien implantés et fiables. Il en va autrement s'agissant de la navigation sur le Net. Les spécialistes de la sécurité admettent qu'il est difficile de contrôler au plus serré les contenus arrivant sur un réseau et une machine via le port 80, utilisé pour surfer sur la Toile à l'aide du protocole HTTP.

«On ne peut tout simplement pas bloquer le port 80», explique Eva Chen, directrice générale de Trend Micro. «Contrairement aux e-mails, qui sont stockés avant d'être acheminés, la navigation s'effectue en temps réel. Et la rapidité est de mise, les internautes ne supportent pas d'attendre.»

Un marché souterrain juteux s'est par ailleurs développé, «les actes malveillants perpétrés à des fins financières constituant le gros de ces menaces sur le web», a complété Raimund Genes, chercheur en chef chez Trend Micro. «Le dernier vrai virus recensé, Melissa, remonte à 1999. Depuis, on a surtout vu des vers et des attaques sur le web».

Des pirates grassement récompensés

Des récompenses sont ainsi promises par des personnes ou sociétés malveillantes à qui décèlera des failles dans les systèmes d'exploitation populaires. Elles peuvent atteindre par exemple 75.000 dollars pour Windows XP et 50.000 dollars pour Windows Vista. Les sociétés spécialistes de la sécurité font de même, mais avec une puissance de tir largement moindre: iDefense de VeriSign et TippingPoint de 3Com proposent autour de 12.000 dollars.

En général, les professionnels signalent aux éditeurs concernés les failles qu'ils ont découvertes; elle sont ensuite rendues publiques une fois un correctif mis au point. Des précautions que ne prennent pas les pirates, qui passent à l'attaque sans attendre.

Les menaces provenant du web sont surveillées par nombre d'experts, tels que Websense, Surf Control et ScanSafe. Tous proposent des produits et services permettant de bloquer l'accès à des sites placés sur liste noire, ou d'analyser le trafic sur le web. Mais ils reconnaissent leur difficulté à suivre le rythme effréné des pirates, «le paysage des menaces étant en constante évolution», admet Eva Chen de Trend Micro

Comme ses concurrents éditeurs de sécurité, Sophos fait un constat simple. 2007 illustre un profond changement dans les vecteurs d'attaques utilisés par les pirates. Si jusqu'à présent le courriel était leur outil préféré, aujourd'hui le Web est devenu le moyen le plus utilisé pour piéger les internautes.

Les pirates exploitent à coeur joie les failles des pages URL, qu'il s'agisse d'image, de spoofing d'adresse, d'URL piégé... Ils utilisent également les possibilités des sites communautaires (type YouTube) et Web 2.0 qui

permettent de placer encore plus de malwares, notamment dans les photos et les vidéos. Il faut dire aussi que les utilisateurs savent de mieux en mieux se protéger contre les virus diffusés via les messageries électroniques.

Ainsi, au cours du premier trimestre 2007, Sophos a identifié 22.864 nouvelles menaces, soit plus de deux fois le nombre découvert pendant la même période de 2006 (9.450). Dans le même temps, le pourcentage de courriels infectés est tombé de 1,3% au premier trimestre 2006, soit un message sur 77, à 0,4% seulement (1 message sur 256) en 2007.

Dans le même temps, l'éditeur a identifié une moyenne **5.000** nouvelles pages Web infectées par jour, principalement par des chevaux de Troie.

Sophos précise que la majorité des pages infectées, soit 70%, sont des sites authentiques rendus vulnérables aux attaques car ils ne disposent pas des correctifs de sécurité, ont été mal programmés ou ne sont pas entretenus par leurs propriétaires.

Parmi les autres sites identifiés, 12,8% hébergent des scripts malveillants et 10,7% sont infectés par des programmes malveillants Windows. Des adwares ont été découvert dans 4,8% des pages, et des 'diallers' pornographiques (des programmes redirigeant automatiquement l'utilisateur vers une adresse surtaxée) sur 1,1% d'entre elles.

« Le plus inquiétant dans ces affaires est que de nombreux sites Web deviennent les victimes des pirates parce que leurs propriétaires ne les tiennent pas à jour, et en particulier n'appliquent pas les correctifs de sécurité adéquats », commente Michel Lanaspèze, Directeur Marketing et Communication de Sophos France et Europe du Sud.

Rappelons que selon le groupe WhiteHat Security, huit des dix plus grands sites du 3W sont vulnérables, permettant à des hackers de récupérer des données confidentielles.

Il faut noter que la France est le 7e pays de la planète à héberger des sites piégés, loin derrière la Chine (1er) et les Etats-Unis.

Vérifiez la sécurité de Windows

Une grande partie des problèmes de sécurité sous Windows sont dus **à des erreurs de configuration de la part des utilisateurs**. Comptes utilisateur dont les droits sont trop importants, accès anonymes activés, mot de passe trop courts ou trop anciens, points de vulnérabilité non bouchés alors que les correctifs existent, paramètres de sécurité mal définis, services inutiles en route, autant d'éléments que **vous devez vérifier afin de sécuriser au mieux Windows**.

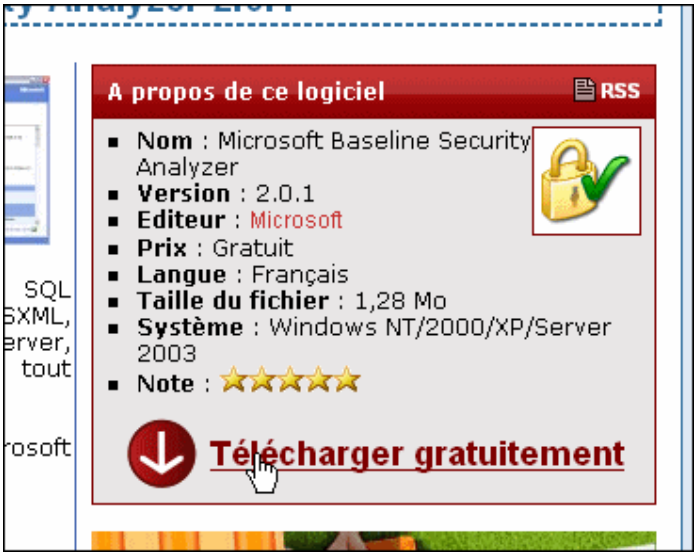
Conscient de cela et pour vous faciliter la tâche, Microsoft met à votre disposition gratuitement l'utilitaire MBSA (Microsoft Baseline Security Analyzer).

Ce dernier va vous permettre d'analyser votre système d'exploitation (Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003) ainsi que diverses applications (Internet Explorer, Outlook Express, Lecteur Windows Media, Office, IIS, SQL Server, Exchange Server, Microsoft Data Access Components, MSXML, Microsoft Virtual Machine, Commerce Server, Content Management Server, BizTalk Server et Host Integration Server), à la recherche de tout manquement à la sécurité.

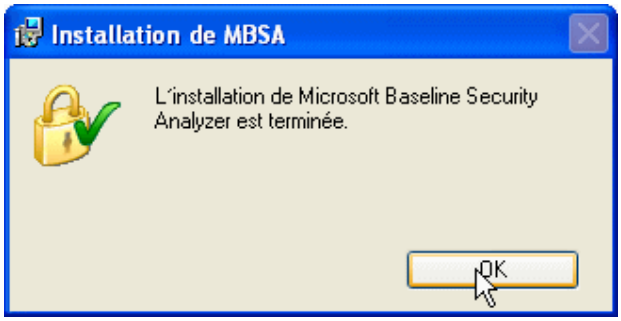
Nous allons donc voir dans ce dossier comment utiliser MBSA afin **d'analyser la sécurité de votre ordinateur** et **corriger les éventuels problèmes qu'il aurait détectés**.

Installer MBSA

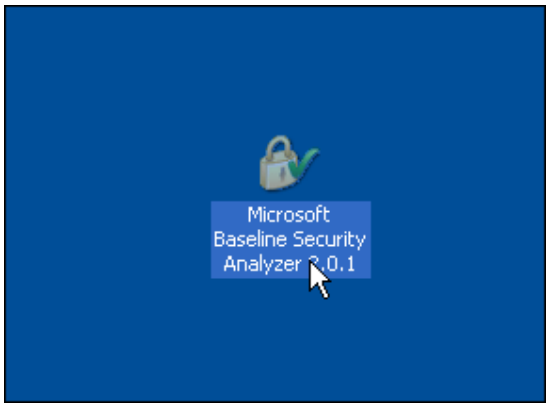
1. Pour télécharger la dernière version en français de Microsoft Baseline Security Analyzer, rendez-vous sur sa fiche dans la logithèque PC Astuces.



2. Une fois téléchargé, double cliquez sur le fichier **MBSASetup-fr.msi** pour démarrer l'installation. Celle-ci ne pose aucun problème, il vous suffit de suivre les instructions données à l'écran puis de valider par **OK** lorsqu'elle est terminée.

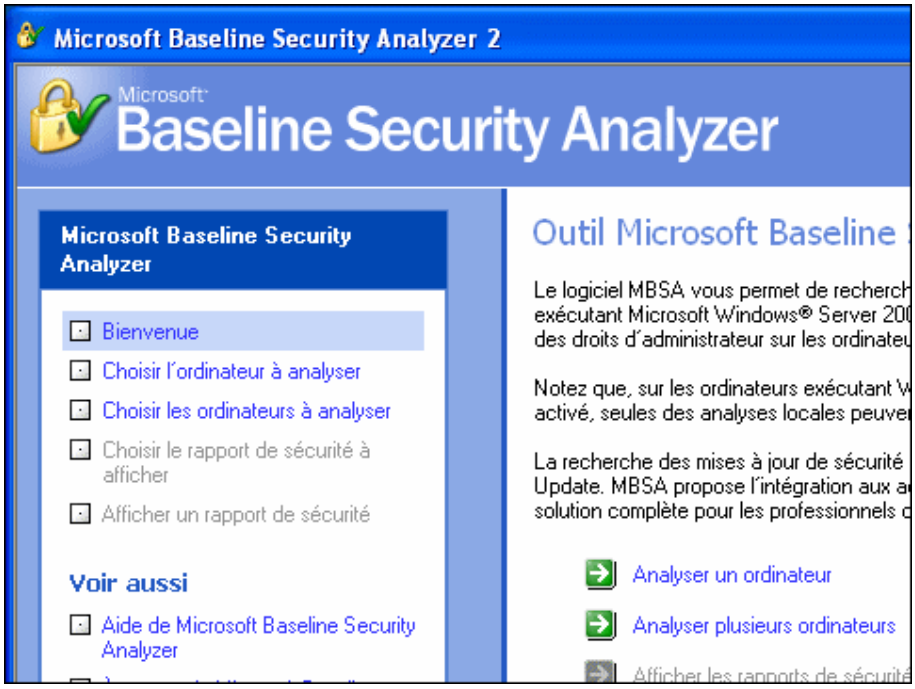


3. Microsoft Baseline Security Analyzer a rajouté une icône sur le Bureau. Double cliquez dessus pour exécuter le programme. Vous êtes alors prêt à analyser votre système.



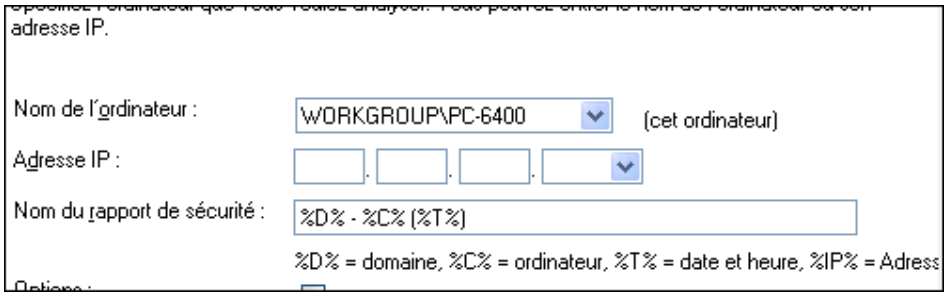
Analyser votre système

Après avoir lancé MBSA, vous vous retrouvez sur l'écran de bienvenue de l'outil où vous devez sélectionner l'étendue de votre analyse, c'est-à-dire si celle-ci concerne un ou plusieurs ordinateurs (tous ceux de votre réseau par exemple). Dans ce dernier cas, il vous faudra spécifier ensuite le nom du domaine où se trouvent les ordinateurs à analyser ou bien la plage d'adresse IP.



1. Vous souhaitez analyser votre ordinateur, cliquez donc sur le lien **Analyser un ordinateur**.

2. Le nom de l'ordinateur sur lequel vous vous trouvez est automatiquement détecté. Si vous souhaitez tester un autre ordinateur de votre réseau saisissez son nom dans le champ adéquat ou bien son adresse IP.

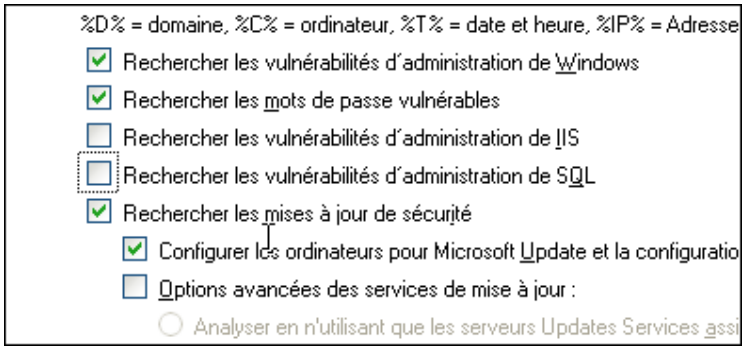


3. Vous devez ensuite sélectionner les options d'analyse, c'est-à-dire choisir les éléments à analyser en cochant les cases des options que vous désirez.

Option d'analyse	Description
Vérifications des vulnérabilités administratives du système Windows	Permet d'analyser les problèmes de sécurité inhérents au système d'exploitation Windows, notamment l'état du compte Invité, le type de système de fichiers, les partages de fichiers disponibles et les membres du groupe Administrateurs.
Vérification des mots de passe vulnérables	Recherche la présence de mots de passe vides et vulnérables lors d'une analyse.
Vérifications des vulnérabilités administratives des services IIS	Permet d'analyser les problèmes de sécurité inhérents aux versions 4.0, 5.0 et 6.0 des services IIS (Internet Information Services), notamment les exemples d'applications et certains répertoires virtuels présents dans l'ordinateur. L'outil permet également de vérifier si l'Outil de verrouillage IIS (IIS URL Lockdown) a été exécuté sur l'ordinateur. Si vous n'avez pas installé IIS sur votre ordinateur, inutile d'activer ce test.
Vérifications des vulnérabilités administratives de SQL Server	Permet d'analyser des vulnérabilités administratives dans chaque instance SQL et MDSE (Microsoft Data Engine) relevée sur l'ordinateur, notamment le type du mode d'authentification, l'état du mot de passe du compte d'administrateur système et les appartenances aux comptes de service. Toutes les vérifications individuelles sont réalisées sur chaque instance SQL et MSDE.
Vérification des mises à jour de la sécurité	Utilise une base de données XML que Microsoft met constamment à jour pour vérifier l'état des mises à jour de la sécurité sur les ordinateurs analysés. Les produits

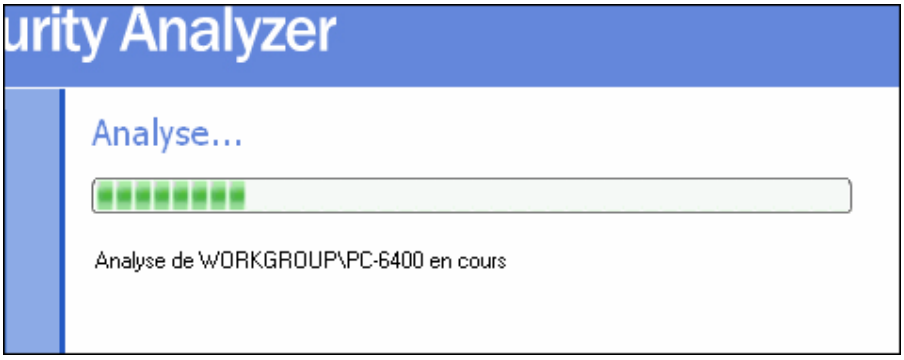
	suivants sont supportés : □ Microsoft Windows NT 4.0, Windows 2000, Windows XP et Windows Server 2003 □ Services IIS (Internet Information Server), versions 4.0, 5.0 et 6.0 □ SQL Server 7.0, SQL Server 2000 (y compris Microsoft Data Engine 1.0 et 2000) □ Internet Explorer 5.01 et version ultérieure □ Windows Media Player 6.4 et version ultérieure □ Microsoft Exchange Server 5.5, Exchange Server 2000 et Exchange Server 2003 (y compris les Outils d'administration Exchange) □ Microsoft Data Access Components (MDAC) 2.5, MDAC 2.6, MDAC 2.7 et MDAC 2.8 □ Machine virtuelle Microsoft □ MSXML 2.5, MSXML 2.6, MSXML 3.0 et MSXML 4.0 □ Content Management Server 2001, Content Management Server 2002 □ Commerce Server 2000, Commerce Server 2002 □ BizTalk® Server 2000, BizTalk Server 2002, BizTalk Server 2004 □ SNA Server 4.0, Host Integration Server 2000, Host Integration Server 2004) □ Microsoft Office

4. Si vous n'êtes pas certains de savoir quoi analyser ou non, laissez toutes les cases cochées.



5. Lorsque vous êtes fin prêt, cliquez sur le lien **Démarrer l'analyse**.

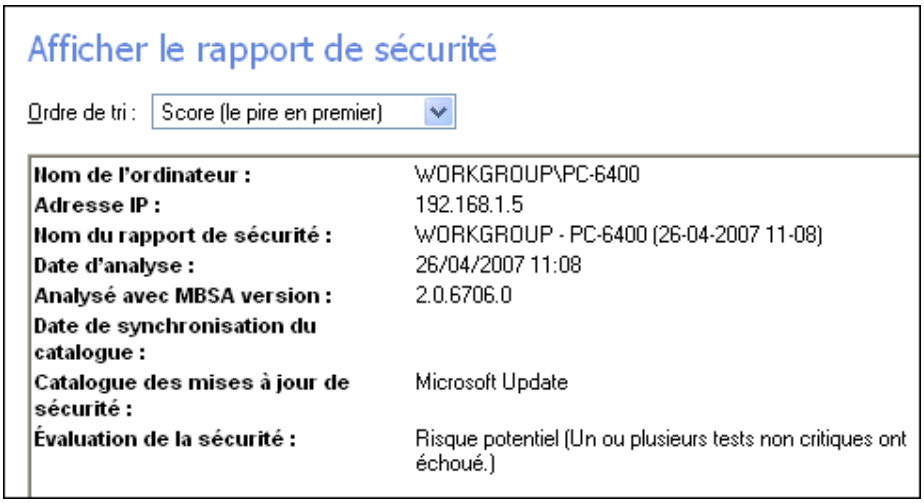
6. MBSA télécharge alors depuis Microsoft les dernières informations de sécurité puis effectue l'analyse de votre système.



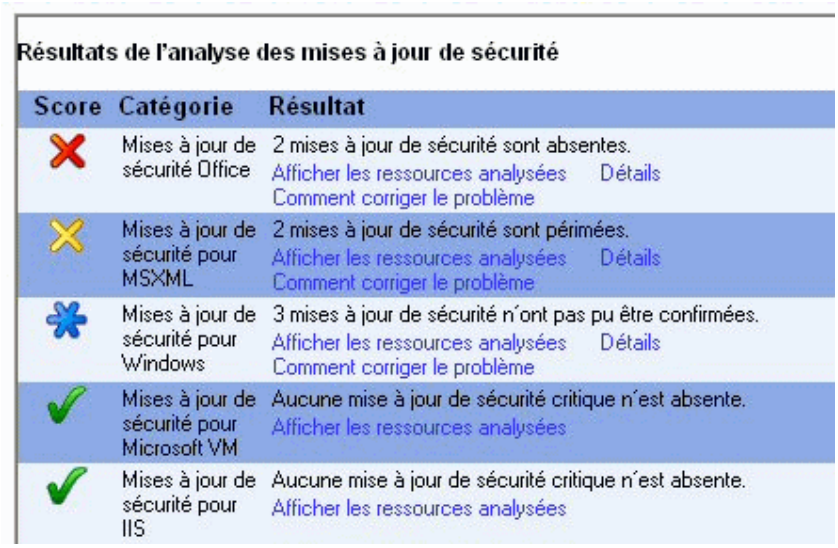
Considérer les résultats et corriger les problèmes

Après quelques minutes d'analyse, le rapport de sécurité est enfin affiché.

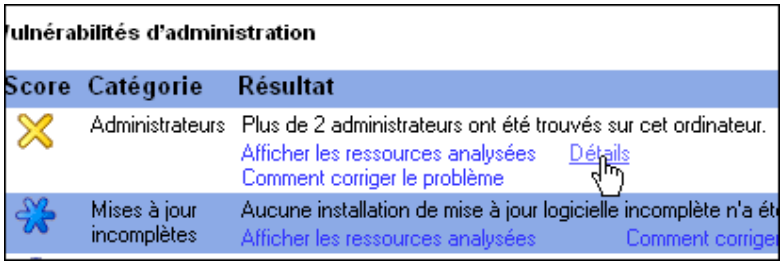
1. Dans la première partie du rapport, vous trouverez Le niveau de sécurité de votre configuration à savoir **Risque important**, **Risque potentiel**…



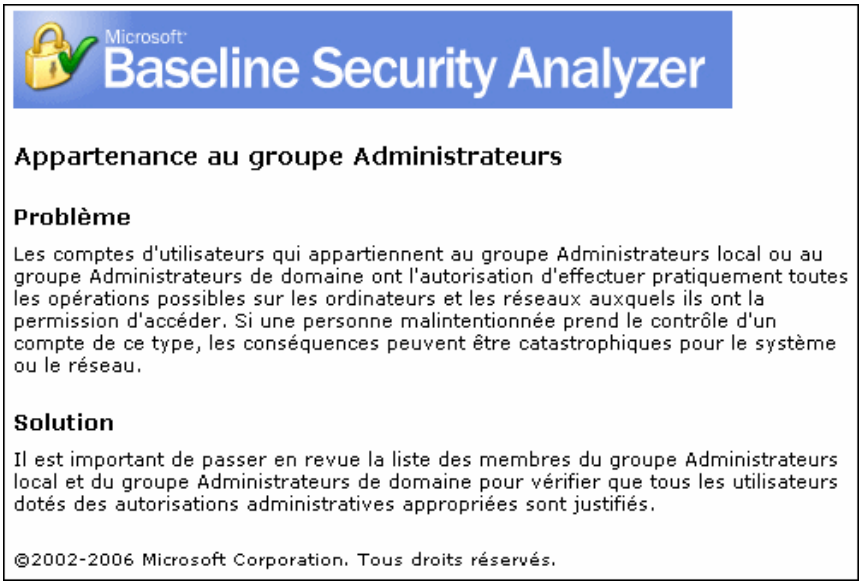
2. La seconde partie présente les résultats de chaque test classés par groupe de vérifications. Un score est attribué à chaque test. Ainsi, une croix rouge vous indique que le test critique a échoué, une croix jaune que le test non critique a échoué et enfin une croix verte pour vous signaler que le test est réussi.



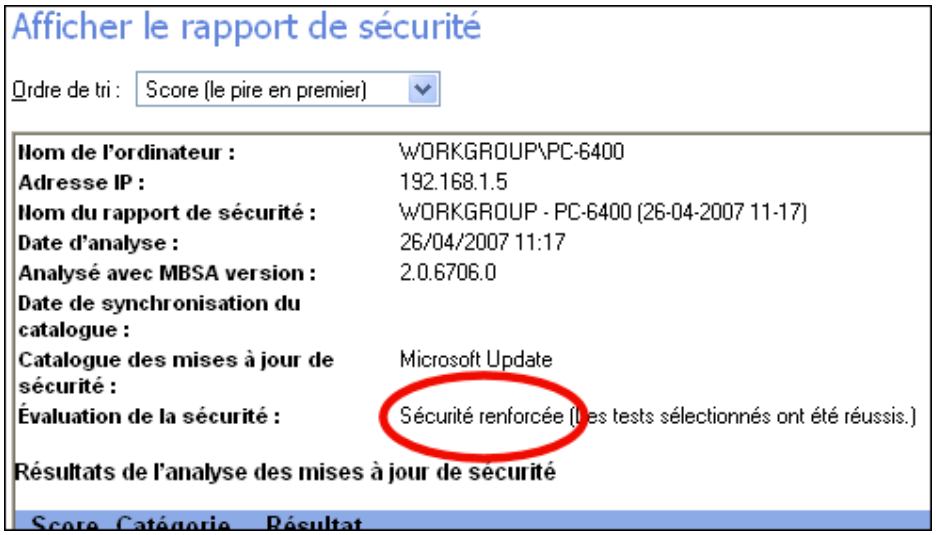
3. L'objectif est donc de mieux configurer votre système afin de réussir tous les tests et limiter ainsi les risques de sécurité. Pour chaque test qui a échoué, une petite description du problème est indiquée. Pour avoir plus d'informations sur le problème, cliquez sur le lien **Détails**.



4. Enfin, pour avoir les instructions pour corriger les problèmes, cliquez simplement sur le lien **Comment corriger le problème**. Des informations sur les moyens de corriger le problème sont alors affichées. **Suivez-les**.



5. Lorsque vous pensez avoir comblé toutes les failles potentielles de la configuration de Windows, n'hésitez pas à refaire une analyse complète pour vérifier que la sécurité est alors renforcée. Redémarrez votre ordinateur avec chaque modification pour être sûr qu'elle soit prise en compte par le test.



Freefax: envoyer des fax avec une Freebox

Free vient d'ajouter un nouveau service à la Freebox, une ligne fax. Pour cela, une deuxième ligne dédiée est créée sans surcoût pour l'abonné. Le service est accessible en ligne dans l'interface de gestion de compte d'abonné à partir de n'importe quel accès Internet (en déplacement à l'étranger par exemple). En conséquence, envoyer et recevoir des fax devient possible sans avoir besoin d'être équipé d'un télécopieur.

Un nouveau numéro dédié au service de fax est attribué automatiquement à tous les abonnés : ce numéro de fax est déterminé à partir des 6 derniers chiffres de leur numéro de téléphone Freebox. Lorsque le numéro de téléphone de l'abonné est 095 B XXX XXX, son numéro de fax dédié est 095 (B+5) XXX XXX.

Depuis son interface de gestion, l'abonné saisit le numéro de fax de son correspondant et choisit le document qu'il souhaite lui transmettre. Une fois le fax envoyé, un accusé de réception est transmis à l'expéditeur sur son e-mail de contact et le destinataire reçoit ce fax sur son télécopieur. Si le fax est envoyé à un abonné Freebox sur son numéro de fax dédié, ce dernier le recevra alors en pièce jointe (PDF) sur son e-mail de contact.

L'envoi de fax est soumis à la tarification des appels téléphoniques Freebox disponible sur la grille tarifaire en ligne : les envois de fax vers 49 destinations dont la France sont donc inclus dans le forfait.

L'offre est soumise à la validation des conditions générales de ventes.

Nouveauté ? Pas tout à fait. Depuis août 2006, les Freenautes pouvaient déjà envoyer et recevoir des télécopies grâce un service pour partie gratuit (ou payant, c'est selon ;-) proposé par Free en collaboration avec la société *eFax* (cf. **http://www.aduf.org/archives/pdf/0606.pdf**), une commodité qui venait alors pallier à la non-garantie de fonctionnement d'un fax traditionnel sur une ligne téléphonique Freebox (cf. article 6.1 des CGV, **http://adsl.free.fr/cgv/CGV_FORFAIT_hors_opt_01022007.pdf**).

Aujourd'hui, un communiqué de presse de Free annonce un nouveau service fax amélioré et 100 % gratuit : **http://iliad.fr/presse/2007/CP_250407.pdf**. Je connais quelques PME qui s'en frotteront les mains... encore que ponctuel ce télécopieur virtuel sera également utile aux particuliers. Il y a toujours un assureur, un banquier ou une administration pour vous demander un document dans la minute. ;-)

Mode d'emploi :

Après avoir saisi vos identifiants sur la page d'accueil de votre console gestion (cf. **http://subscribe.free.fr/login**), rendez-vous dans la rubrique *GESTION DE MES SERVICES DE TÉLÉPHONIE/Envoyer un Fax*. Une interface indiquant votre nom et n° de fax Freebox vous invite à saisir le numéro du télécopieur destinataire. Le coût de l'envoi est soumis aux conditions tarifaires Freebox, c'est-à-dire, gratuité vers 49 destinations, etc... (cf. **http://adsl.free.fr/tel/tarifs**). Enfin, 49 destinations, en théorie... car à l'heure où nous rédigeons cet article, il est encore impossible de saisir un n° de destinataire supérieur à dix chiffres. Pour l'étranger, c'est donc râpé.

Notez que votre n° de fax est distinct de votre n° de téléphone Freebox. Vous ne pourrez ni le choisir, ni en changer. Il vous est automatiquement attribué par Free en incrémentant le 4ème chiffre de votre n° de téléphone de 5 unités.
Exemple : au n° de téléphone Freebox 09 51 XX XX XX sera associé le n° de fax 09 56 XX XX XX.

De la même façon que vous attacheriez une pièce-jointe à un email, cherchez - sur votre disque dur - le document à expédier en cliquant sur le bouton *Parcourir*. Attention, ce document doit être au format PDF, ce qui suppose de le « PDFiser » si à l'origine il était au format Word, Excel, ou toute autre application. Pour cela, un logiciel gratuit comme *PDFCreator* (téléchargeable ici : **http://www.clubic.com/telecharger-fiche11085-pdfcreator.html**) fera parfaitement l'affaire.

Le document chargé, il suffira finalement de cliquer sur *Envoyer*. Une confirmation d'envoi s'affichera sous l'interface. Le destinataire recevra votre fax sur son télécopieur et vous recevrez un récipissé d'envoi par email à votre adresse de contact (veuillez à la tenir à jour dans la rubrique *MODIFICATION DE MES INFORMATIONS/Modifier mon email de contact*).

Vous l'aurez compris, dans le sens inverse, en réception, vos fax vous parviendront au format PDF, là encore, sur votre adresse de contact.

Retenez enfin que pour l'heure (cela devrait changer à l'avenir) la parution de votre n° de fax dans l'annuaire est liée aux conditions que vous avez définies dans la rubrique *GESTION DE MES SERVICES DE TÉLÉPHONIE/Gérer le référencement de mon numéro de téléphone Freebox dans l'annuaire*. En clair, si vous avez opté pour la non-parution de votre n° de téléphone Freebox (ou pour la parution restrinte de vos données personnelles), votre n° de fax Freebox n'y apparaîtra pas non plus.

Orange monte la taille des boîtes aux lettres et offre l'antispam

Orange Internet a décidé de monter l'espace de la Messagerie Orange à 500 Mo et d'y inclure l'option Antispam+. Ce sera effectif le 14 mai prochain. Orange Mobile fera de même avec son Mail Orange.
Orange Internet va donc proposer un espace de stockage des mails (et des pièces jointes) de 500 Mo en permet tant à chaque compte Orange d'avoir 5 adresses mail (une adresse mail + 4 alias mail) pour le même espace de messagerie. Un alias mail est une adresse mail qui envoie les messages vers la boîte aux lettres d'une autre adresse mail, comme le fait un Alias (Unix-Linux-Mac) ou un Raccourci (Windows) avec un fichier ou un dossier. Le Webmail de la Messagerie d'Orange va bénéficier d'une refonte et va intégrer un agenda pour la gestion des tâches et des rendez-vous.

A partir du 14 Juin, l'Antispam+ sera inclus dans les forfaits Internet Orange. Pour les abonnés sans Antispam+, l'option sera proposée gratuitement. Les abonnés à Antispam+ ne payeront plus pour l'option (au lieu de 1,5€/mois). Les abonnés au Mail Protégé (Antispam+ et Antivirus Mail) passeront à l'option Antivirus Mail (donc de 4€ à 3€/mois). Les abonnés Mail Premium (Antispam+, Antivirus Mail et Giga Mail) se verront proposer la même option avec Antivirus Mail et Giga Mail mais à coût moindre.

Pour Orange Mobile, le service Mail Orange va aussi changer. Le service offrira une messagerie avec une adresse mail "nom@orange.fr", 50 alertes SMS par mois informant l'abonné de la réception de courriel sur sa boîte, l'envoi de 1000 mails par mois et un antispam. Ce service est proposé gratuitement à tous les abonnés Orange (de la Mobicarte aux forfaits Orange Pro en passant par les forfaits bloqués M6 Mobile).

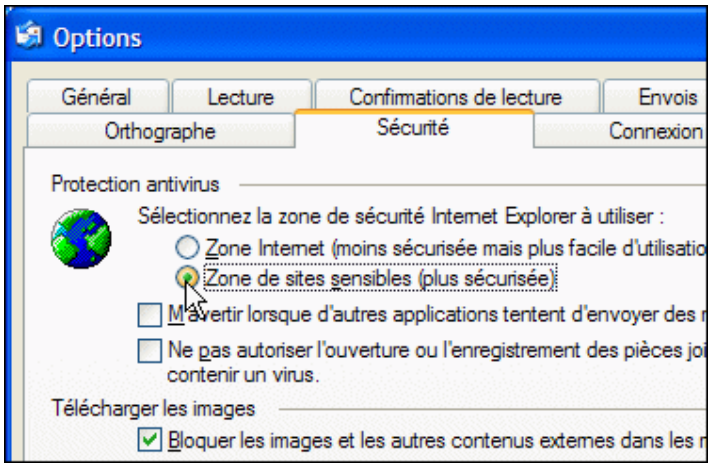
Orange Mobile et Orange Internet proposeront gratuitement l'option Mes Services Unifiés à leurs abonnés communs. Mes Services Unifiés permettra de n'avoir qu'un seul compte Orange pour les sites Web d'Orange Internet et d'Orange Mobile et un seul espace mail pour les 2 adresses (l'adresse Internet et l'adresse Mobile) avec les 50 alertes SMS du Mail d'Orange et l'Antispam+ de la Messagerie Orange. Mes Services Unifiés remplacera l'option Mes Services Perso.

Améliorer la sécurité d Outlook Express

Modifier le niveau de sécurité :

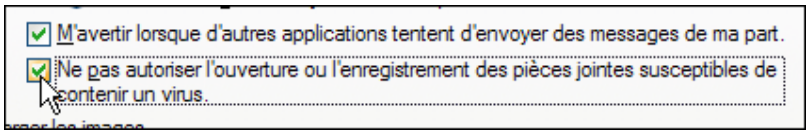
1. Dans Outlook Express, déroulez le menu **Outils** puis cliquez sur la commande **Options**.

2. Cliquez ensuite sur l'onglet **Sécurité**. Choisissez d'utiliser la **Zone de sites sensibles** qui est plus sécurisée. Elle supprime l'exécution des composants ActiveX qui peuvent utiliser par des scripts malicieux contenus dans les mails.



3. Cochez la case **M'avertir lorsque d'autres applications essaient d'envoyer des messages électroniques de ma part**. De cette façon, une boite de dialogue apparaîtra pour vous demander confirmation si un programme tente d'utiliser les options d'envoi d'un de vos comptes de messagerie.

4. Activez ensuite la case à cocher **Ne pas autoriser l'ouverture ou l'enregistrement des pièces jointes susceptibles de contenir un virus** afin de bloquer les fichiers exécutables arrivant par mail et qui peuvent contenir des virus.



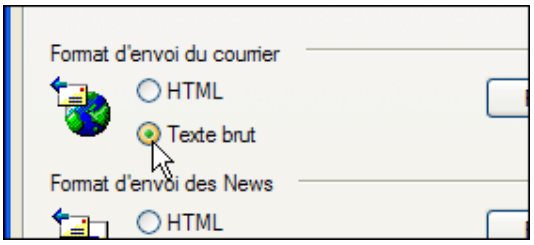
5. Validez enfin par **OK**.

Utiliser le format de courrier Texte :

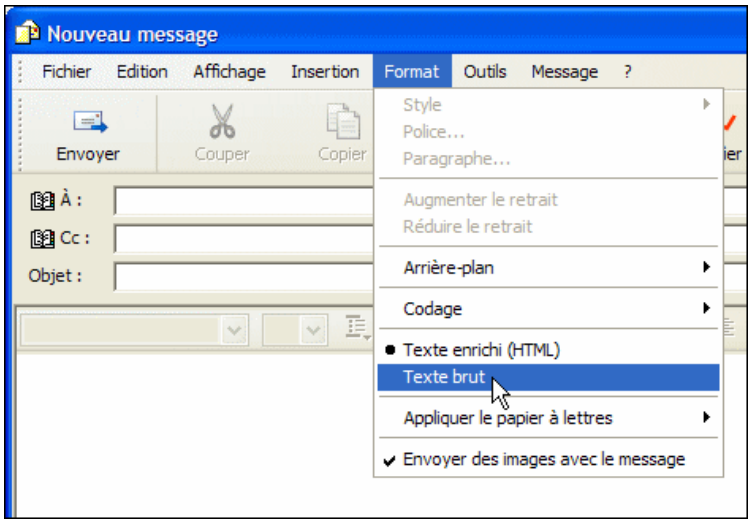
Vous pouvez aussi réduire le risque d'envoi de virus en envoyant vos messages en texte brut au lieu d'utiliser le format HTML. Offrant moins de fonctionnalités que le format HTML, le format texte est plus sûr car il ne contient aucun code, seulement du texte. De plus, vos messages seront ainsi plus léger et transiteront plus rapidement.

1. Pour configurer l'envoi de vos messages en texte brut de façon globale, cliquez sur le menu **Outils** puis sur **Options**.

2. Cliquez ensuite sur l'onglet **Envois** puis sélectionnez l'option **Texte brut** de la rubrique **Format d'envoi du courrier**.



3. Si vous souhaitez envoyer seulement au cas par cas vos messages au format texte, lors de la rédaction d'un message, déroulez le menu **Format** puis sélectionnez l'option **Texte brut**.



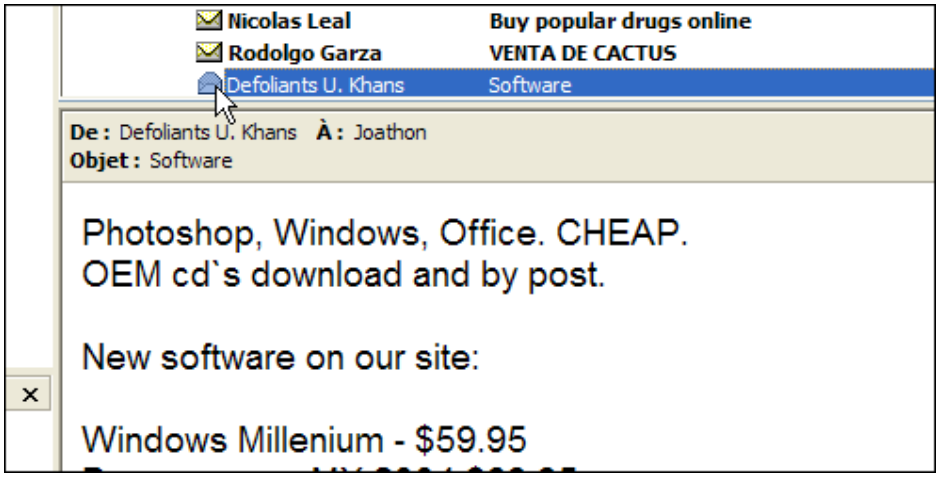
4. Confirmez l'avertissement en cliquant sur **OK**

Mise en forme et texte brut

Sachez que si vous rédigez vos messages en texte brut, vous ne disposez pas des options de mises en forme du format HTML. Ainsi, finis les tableaux, le texte en gras, italique ou souligné, la couleur, ...

Désactiver le panneau de visualisation :

Certains virus ou codes malicieux contenus dans les messages que vous recevez peuvent être exécutés simplement à leur ouverture dans Outlook Express. Or lorsque vous sélectionnez un message, pour le supprimer par exemple, il est affiché dans le volet de visualisation et le code qu'il contient est exécuté. Pour éviter cela, mieux vaut désactiver le panneau de visualisation.



1. Exécutez Outlook Express puis déroulez le menu **Affichage** puis cliquez sur la commande **Disposition**.

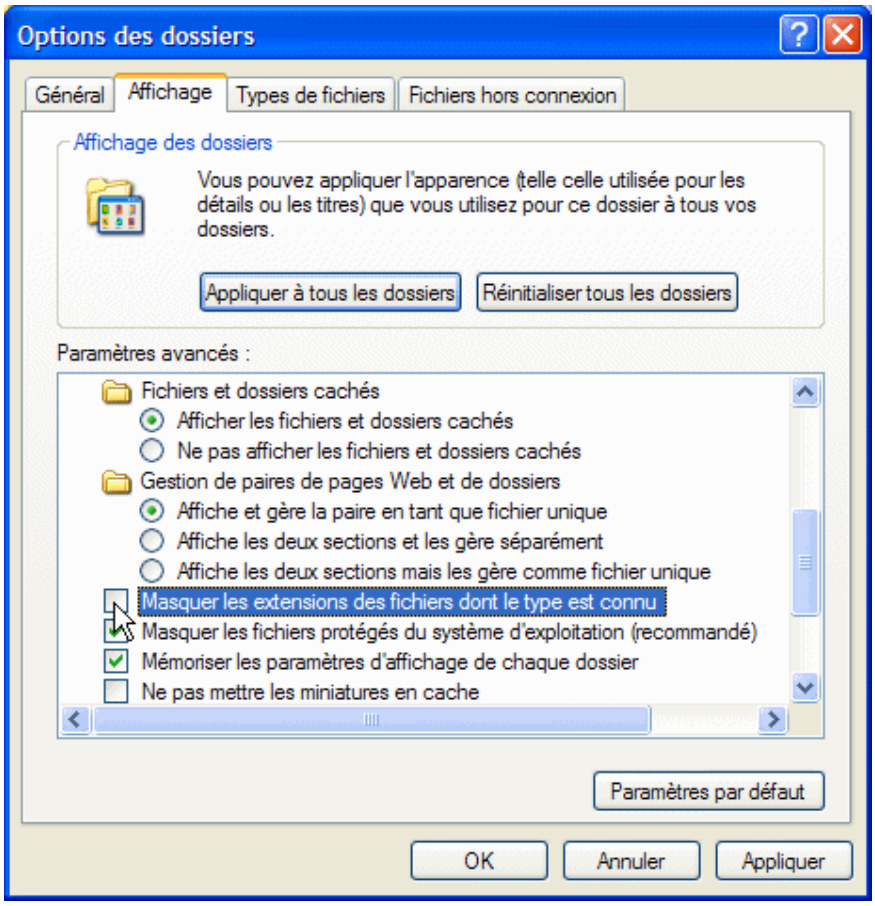
2. Dans la rubrique **Volet de visualisation** de la fenêtre qui apparaît, décochez la case **Afficher le volet de visualisation**. Validez enfin par **OK**.

Afficher toutes les extensions de fichiers :

La majorité des virus qui arrivent par mails tentent de tromper votre vigilance en employant une double extension pour les pièces jointes, du type "rapport.doc.vbs". C'est cette deuxième extension, .vbs ici qui est celle du fichier.

Or par défaut, Windows masque les extensions de fichiers. Ainsi, croyant ouvrir un document Word (.doc), vous ouvrez un script vbs qui peut être très dangereux. Vous devez donc demander à Windows d'afficher toutes les extensions de fichiers pour ne pas vous faire avoir.

1. Ouvrez une fenêtre d'Explorateur puis cliquez sur le menu **Outils** puis sur **Options des dossiers**.
2. Dans la fenêtre qui apparaît, ouvrez l'onglet **Affichage**.
3. Décochez alors la case **Masquer les extensions des fichiers dont le type est connu**.



4. Cliquez enfin sur **OK**.

L Etat veut il tuer Internet en France ?, par Philippe Jannet

LE MONDE | 20.04.07 | 13h22 •

Discrètement, en marge de la campagne, le gouvernement prépare un décret qui, s'il était appliqué, tuerait l'Internet "made in France". En effet, sous prétexte de surveiller au plus près les internautes, un décret d'application de la loi sur la confiance dans l'économie numérique du 21 juin 2004, exige que les éditeurs de sites, les hébergeurs, les opérateurs de téléphonie fixe et mobile et les fournisseurs d'accès à Internet, conservent toutes les traces des internautes et des abonnés au mobile, pour les délivrer à la police judiciaire ou à l'Etat, sur simple demande.

Au-delà du coût incroyable que cette conservation représenterait, cette mesure ne pourrait que déclencher une défiance immédiate des Français à l'égard de leur téléphone mobile ou fixe, comme à l'égard des acteurs français d'Internet, assassinant instantanément l'économie numérique française, pourtant décrite comme stratégique par nos chers candidats.

Le décret en préparation exprime le fantasme "Big Brother" : tout savoir sur tout et tous, même l'impossible. Selon ce texte, les opérateurs téléphoniques, les fournisseurs d'accès à Internet, les hébergeurs et les responsables de services en ligne (sites Web, blogs, etc.), devraient conserver pendant un an à leurs frais toutes les coordonnées et traces invisibles que laissent les utilisateurs lors d'un abonnement téléphonique ou à Internet, lors de leurs déplacements avec un téléphone allumé, lors de chaque appel ou de chaque connexion à Internet, de chaque diffusion ou consultation sur le Web d'un article, d'une photo, d'une vidéo, ou lors de chaque contribution à un blog.

En substance, devraient être conservés les mots de passe, "pseudos", codes d'accès confidentiels et autres identifiants, numéros de carte bancaire, détails de paiement, numéros de téléphone, adresses e-mail, adresses postales, le numéro de l'ordinateur ou du téléphone utilisé, le moyen d'accès à un réseau, les date et heure d'appel, de connexion et de chacune de leurs consultations ou contributions sur un site Internet.

A tant vouloir être exhaustif, le texte imposerait d'identifier quiconque, en France, aura mis en ligne, modifié ou supprimé une virgule dans son blog, un "chat", ou sur le Web. Techniquement, on peut, certes, tenter de savoir qui s'est connecté à un site et constater sur Internet ce qu'il diffuse à un instant donné.

Mais en cherchant à conserver la trace de la publication d'un contenu qui aura, par la suite, été retiré, le texte impose de facto de mémoriser systématiquement tout ce qui est mis en ligne, modifié et supprimé sur "l'Internet français". De l'avis unanime des spécialistes, c'est économiquement et techniquement impossible. Même les Etats-Unis de George W. Bush et leur "Patriot Act" post-11-Septembre n'ont jamais envisagé pareille conservation ou réglementation, qui soulèverait sans doute l'opinion publique américaine d'aujourd'hui, mais s'opère sans bruit en France.

Le coût, aussi bien pénal qu'économique, d'un tel dispositif serait colossal pour la France. En cas de résistance, ou juste de passivité, la sanction encourue est lourde : les fournisseurs d'accès à Internet ou les sites Internet français qui ne conserveraient pas toutes ces données seront passibles de 375 000 euros d'amende et leurs dirigeants, d'un an d'emprisonnement et 75 000 euros d'amende, sans compter la fermeture de l'entreprise, l'interdiction d'exercer une activité commerciale, etc.

Lors d'une réunion organisée en catimini le 8 mars 2007 par les ministères de l'intérieur et des finances - le ministère de la justice jouait, une nouvelle fois, les absents -, certains professionnels ont fait valoir, notamment, que cette conservation leur coûterait très cher en stockage informatique et en moyens humains. De plusieurs dizaines de milliers à plusieurs millions d'euros par an de perte nette.

Pourtant, la plupart des sites Web, les Web radios, les blogs, la vidéo à la demande ou mobile, sont encore en quête d'un modèle économique pérenne. Déjà insécurisée par la complexité des enjeux de propriété intellectuelle, l'économie numérique de demain - celle du contenu et pas seulement de l'accès - serait encore fragilisée par une telle surenchère réglementaire franco-française.

En imposant aux entreprises françaises d'être des auxiliaires de justice ou des "indics", l'Etat fragilise tout un pan de l'économie de demain et de la démocratie d'aujourd'hui, en favorisant qui plus est, la domination déjà outrancière des grands acteurs internationaux de l'Internet, qui ne seront pas impactés à l'étranger. Jusqu'alors, seuls les fournisseurs français d'accès à l'Internet et hébergeurs étaient soumis à cette exigence et l'Etat, qui avait promis des compensations financières aux coûts induits par une surveillance des moindres faits et gestes de leurs clients, met tant de mauvaise grâce à s'acquitter des indemnités dues que certains d'entre eux ont renoncé à en réclamer le règlement, préférant envisager la délocalisation pure et simple de leurs activités...

Ces menaces proférées par quelques poids lourds de l'Internet en France font sourire Bercy, qui semble n'avoir pas encore compris qu'Internet est un réseau mondial dont de nombreux prestataires peuvent s'établir et payer leurs impôts presque où bon leur semble.

Il reste que la confusion des genres est totale. Toutes les données conservées seraient accessibles à la police administrative (RG, DST, etc.) comme à la police judiciaire, pendant un an. Les réquisitions administratives pour la *"prévention du terrorisme"* seraient également conservées un an dans des fichiers tenus par les

ministères de l'intérieur et de la défense. Les réponses à ces mêmes réquisitions - nos traces, donc - seraient, pour leur part, conservées pendant trois ans supplémentaires et communicables à la police judiciaire.

Ainsi, des données récoltées sur la base de requêtes administratives initialement motivées par la prévention du terrorisme pourraient se retrouver dans le dossier d'un juge d'instruction en charge d'une affaire de droit à l'image, de diffamation ou de contrefaçon, par exemple, sans que les personnes mises en cause par des traces informatiques vieilles de 4 ans, puissent connaître - ni contester - l'origine ou la pertinence de ces données, ni le contexte dans lequel elles avaient été recueillies, en dehors de toute procédure judiciaire, sans magistrat ni contradictoire, quatre ans auparavant.

Ce projet de décret constitue donc une véritable menace de mort. Il est inquiétant pour trois raisons essentielles. D'abord, le coût. A vouloir faire conserver et restituer par les entreprises, sous peine d'investissements à perte, de prison et d'amendes, des traces qu'elles n'ont pas de raisons ou de possibilité d'avoir, la France créerait une distorsion de concurrence au détriment de sa propre économie numérique, pourtant motrice de notre croissance. Un internaute choisira plus aisément un site non surveillé qu'un site français pour s'informer, même s'il n'a rien à craindre de sa recherche.

Ensuite, la confusion entre le renseignement d'Etat et la justice, qui relègue la séparation des pouvoirs au rang de fiction juridique. Enfin, le risque qu'un tel dispositif ferait peser sur la régularité des procédures judiciaires au regard de notre procédure pénale. C'est-à-dire le risque de priver une politique de sécurité de toute efficacité.

Certes, le gouvernement consultera la CNIL, brandie en épouvantail par les ministères. Mais l'avis de celle-ci, même défavorable, sera dépourvu du moindre effet juridique depuis la refonte de la loi informatique et libertés intervenue en 2004. Certes, l'équilibre entre sécurité, croissance, libertés et efficacité est complexe. Au demeurant, aucune de ces valeurs ne s'illustre dans ce projet de décret, dont la rédaction est aujourd'hui laissée à un consensus entre technocrates et techniciens qui, quels que soient les résultats des échéances électorales, seront encore là demain.

Ce qui pourrait n'être qu'un décret illisible de plus est aujourd'hui une menace de mort pour le développement du numérique en France et pour tous les acteurs concernés de près ou de loin par celui-ci, de la presse aux blogueurs, en passant par la grande distribution, les opérateurs de téléphonie, les fournisseurs de logiciels, les fabricants d'ordinateurs, etc.

Sous prétexte de lutter contre la menace réelle du terrorisme, l'Etat français prend - comme aucun autre - le risque de tuer une part non négligeable de l'avenir du pays, sans aucun état d'âme et dans le silence assourdissant d'une campagne présidentielle omniprésente sur Internet, mais muette sur le développement de l'Internet.

Philippe Jannet est président du Groupement des éditeurs de sites en ligne (Geste).

Le Geste regroupe les principaux éditeurs de sites en ligne français, qu'il s'agisse de portails généralistes (Yahoo ! France, Google), d'organismes ou d'entreprises (INA, UFC Que choisir, Manpower, Comareg, France Télécom, Bouygues Télécom, etc.), ou encore de sites de chaînes de télévision (TF1, France télévision, M6, etc.), de radios (Radio France, Skyrock, RTL, RFI, etc.), d'agences (AFP), de journaux (*Le Figaro*, *Les Echos*, *Libération*, *Le Monde*, *L'Equipe*, *Le Point*, *L'Express*, *Le Nouvel Observateur*, *Le Parisien* et les journaux du groupe Hachette Filipacchi Multimedia, etc.).

Eradiquer les rootkits

Après les virus et les vers, les rootkits risquent bien d'être la principale menace pour nos ordinateurs. Selon une étude récente, près de 20 % des PC domestiques seraient déjà transformés en zombie.

La généralisation des accès ADSL et des PC connectés en permanence à internet ouvre une voie royale pour les tentatives de prise de contrôle à distance de PC par le biais de l'installation de rootkit, programmes invisibles

installés, à votre insu, et conçus pour cacher la présence sur votre ordinateur d'autres applications malveillantes.

Lorsqu'il est infecté, votre ordinateur continue à se comporter tout à fait normalement jusqu'au moment où l'attaquant le sollicitera pour participer à une campagne massive de spam ou à une opération ciblée de déni de service. Des réseaux de PC zombies constitués de plus 400 000 PC ont déjà été créés.

Pour faire face à cette nouvelle menace, des solutions existent pour scanner son PC et s'assurer que vous êtes bien le seul maître à bord.

AVG Antirootkit (gratuit)
Télécharger

F-Secure BlackLight (gratuit)
Télécharger

Gmer (gratuit)
Télécharger

RootKit Hook Analyzer (gratuit)
Télécharger

RootkitRevealer (gratuit)
Télécharger

Sophos Anti-Rootkit (gratuit)
Télécharger

Brancher un PC sur une télévision pour regarder des DVD

La grande majorité des ordinateurs actuels est équipée de lecteurs de DVD. Génial, on peut désormais regarder des films sur son PC en qualité numérique ! Cependant, l'écran d'ordinateur n'est pas toujours adapté, en particulier en termes de dimensions. Pourquoi ne pas mettre à contribution votre bonne vieille TV ?

C'est facile, à partir du moment où l'on dispose d'une carte graphique permettant l'affichage TV, d'une carte son équipée d'une sortie audio et des câbles appropriés.

Matériel nécessaire :
- Un ordinateur équipé d'un lecteur de DVD pour lire votre DVD
- Une carte graphique dotée d'une sortie TV pour disposer des fonctions d'affichage sur écran de télévision
- Une carte son équipée d'une sortie audio pour envoyer le son du film sur la TV
- Une TV dotée d'une entrée Péritel, Composite ou S-Vidéo pour recevoir un signal son et image en provenance d'un appareil externe
- Des câbles et/ou adaptateurs nécessaires pour relier l'ordinateur à la TV

Comment procéder ?

- **Première étape** donc, repérer la sortie TV à l'arrière de l'ordinateur.

- **Deuxième étape**, repérer le format des connecteurs d'entrée à l'avant ou à l'arrière de votre téléviseur. Selon le format, il faut ensuite vous procurer le câble correspondant : S-Vidéo du côté ordinateur, puis S-Vidéo, Composite ou Péritel du côté TV. Et voilà pour l'image !

Pour le son : il faut relier au moyen d'un câble mini-jack / RCA la sortie "Out" de votre carte son à l'entrée son du téléviseur, ou l'entrée auxiliaire de votre chaine hi-fi si vous souhaitez profiter d'un meilleur son.

- **Troisième étape**, repérer le format des connecteurs d'entrée à l'avant ou à l'arrière de votre téléviseur. Selon le format, il faut ensuite vous procurer le câble et les adaptateurs correspondant : S-Vidéo du côté ordinateur, puis S-Vidéo, Composite ou Péritel du côté TV. Le mieux étant de disposer d'une entrée S-Vidéo sur sa TV, ce qui offre la meilleure qualité d'image possible.

Ensuite, les possibilités sont multiples : si votre entrée côté TV est au format Péritel, il vous faudra un adaptateur S-Vidéo / Péritel. Certaines cartes graphiques sont livrées avec câbles, il suffira alors de les utiliser et d'y adjoindre un adaptateur si nécessaire.

Ces câbles comportent en général une prise S-Vidéo d'un côté, et une prise Composite ET S-Vidéo de l'autre (dans ce cas, utiliser la fiche qui correspond à la prise côté TV).

- **Quatrième étape**, démarrez l'ordinateur, puis faites un "clic droit / propriétés" sur le bureau Windows. Une boite de dialogue "Propriétés d'affichage" apparaît. Sous l'onglet "Paramètres", vous trouverez un bouton "Avancés". Cliquez dessus, le gestionnaire d'affichage spécifique à votre carte vidéo se lance.

Il faut rechercher dans celui-ci la fonction qui permet de basculer en affichage TV.

La marche à suivre dépend du programme gestionnaire fourni avec votre carte graphique. Il faudra vous référer à sa documentation.

Une fois le logiciel correctement paramétré, il reste à allumer la TV, basculer sur le bon canal (A/V), et voilà ! Votre bureau Windows apparaît maintenant sur l'écran du téléviseur, il ne vous reste plus qu'a lancer votre film DVD comme d'habitude et à profiter de votre nouvelle installation !

Si l'image est en noir et blanc...
Il arrive assez régulièrement que l'image obtenue sur le téléviseur soit en noir et blanc.Ce problème peut-être lié à la norme du signal vidéo. Pour la France votre téléviseur attend un flux PAL B.

Avec certaines cartes graphiques (Ati notamment), c'est à vous de spécifier la nature de ce signal, retenez donc cette norme dans les paramètres d'affichage du gestionnaire de votre carte graphique.

Les réglages du téléviseur et de la chaîne A/V sont une autre piste à explorer, parfois l'acquisition est réglé sur composite alors que vous utilisez un câble S-vidéo, ou bien le contraire. Il faut donc changer manuellement ce réglage selon votre dispositif.

Enfin, si votre téléviseur est assez ancien (plus de 10 ans), il se peut qu'il ne soit pas compatible PAL auquel cas vous ne pourrez pas obtenir la couleur.