Les dossiers de Anonymat.org

Comment éradiquer les mouchards ?

1ere Edition du 10 Octobre 2000
Rev. 1.2

Table des matières

Nous vous rappelons que tous les programmes et correctifs de ce dossier (et des autres) sont sur notre CD-ROM PC « Internet Anonyme ».- Contactez-nous.

Les anti-mouchards universels !

AD-aware est un utilitaire gratuit de Lavasoft qui détecte et supprime un grand nombre de mouchards ou espiogiciels parmi lesquels :

- Aureate/Radiate
- Conducent/Timesink
- CometCursor 1 & 2
- CYDoor (Babylon Translator)
- Gator
- Web3000
- Flyswat.

La liste des freewares potentiellement infectés par ces différents spywares est disponible sur ce site.

Une version française de ce produit devrait faire son apparition sous peu.

Des méthodes alternatives existent pour chacun d'eux et nous vous en montrerons quelques unes comme pour Timesink, qui permet d'assurer le fonctionnement du programme hôte une fois le mouchard terrassé !

Le spyware Cydoor est repéré !

Son concurrent **OptOut** de *Steve Gibson* détecte et supprime pour sa part :

Pour la version gratuite :

- Aureate/Radiate pour lequel il a été spécifiquement conçu.

Pour la version Shareware (25$), il ajoute :

- Conducent/TimeSink
- CometCursor

1.- Les mouchards de Windows 98

Un expert américain en sécurité informatique, *Robert Smith*, a dévoilé le premier la présence d'un mouchard au sein de Windows 98 (et Windows 98 SE).

Lors de votre enregistrement en ligne par l'*assistant d'enregistrement* un numéro d'identifiant unique (GUID) nommé **MSID** (Microsoft ID), en fait, une valeur numérique de 32 chiffres, vous est attribué.

Ce **MSID**, outre qu'il est envoyé par le biais d'un ActiveX sur le serveur de Microsoft pour vous identifier et épier vos déplacements sur son site, est également incorporé, à votre insu, à tous les documents produits avec la suite Bureautique MS-Office et d'autres outils de développement signés Microsoft (voir ci-dessous).

Un second identifiant appelé *Hardware ID* (***HWID*** ou numéro d'identification matérielle), contenant divers renseignements sur la configuration matérielle du PC et probablement, d'après certains, sur les logiciels installés est également envoyé à Microsoft, officiellement « afin de simplifier le travail de l'équipe d'assistance téléphonique ».

Pour éradiquer le mouchard vous pouvez utiliser une des solutions suivantes :

- Sur le site de *Microsoft* un Patch est disponible sous l'intitulé (peu explicite) de '***Mise à jour de l'assistant d'inscription***' (13Ko).

- Télécharger le programme Spy Killer qui diagnostic et supprime le mouchard !

Ou opter pour la méthode manuelle :

1.- Cliquez sur le menu *Démarrer* puis *Exécuter* de la barre des tâches

2.- Tapez la ligne ci-dessous dans la boîte de dialogue (ou faites un copier/coller)

Regsvr32.exe -u c:\Windows\System\Regwizc.dll

3.- Validez en appuyant sur **<**Entrée**>**

Il existe également toute un série de fichiers situés dans le répertoire **/WINDOWS/ SYSTEM** qui permettent d'espionner les surfer :

anadsc.ocx	advert.dll	anadscb.ocx	htmdeng.exe	ipcclient.dll	msipcsv.exe	tfde.dll
dimage.dll	amcompat.tlb	amstream.dll	amcis.dll	amcis2.dll	advpack.dll	

La DLL *advpack* (ici en jaune) envoie de nombreuses informations aux sites que vous visitez (temps de connexion, etc).

Je vous recommande de les supprimer ou de les déplacer après les avoir soigneusement sauvegardés.

1.1.- Le mouchard de Microsoft Office

Comme nous l'avons vu ci-dessus, le numéro d'identification unique (ou GUID) de Windows 98 qui comprend des données du système, comme l'adresse MAC unique de votre carte réseau, est également incorporé dans vos documents MS-Office. Il est donc possible, par ce biais, de remonter jusqu'à l'ordinateur qui a produit le document Office !

Microsoft a été contraint de proposer des utilitaires permettant de supprimer le tatouage des fichiers Office :

Utilitaire pour désactiver la fonction de tatouage

Utilitaire pour supprimer le tatouage des fichiers

Pour nettoyer vos fichiers MS-Office 97 vous pouvez également vous procurer le gratuiciel *Guideon* (68 Ko) qui permet également de supprimer le numéro de série unique présent dans vos documents Word, Excel, etc. sans affecter les données du fichier.

Cliquez ici pour télécharger Guideon !

Vous ne savez sans doute pas que tout document Office 97 génère des **meta-données** (metadata). Ces meta-données peuvent comporter diverses informations personnelles comme :

- Votre nom
- Vos initiales
- Le nom de votre société
- Le nom de votre ordinateur
- Le numéro de votre disque dur
- Le nom de votre serveur sur lequel vous stockez vos documents
- Le numéro de version et de révision du document
- Les anciens noms du document
- Les blocs de texte ou cellules cachées ou effacées
- Etc.

Microsoft donne quelques conseils afin de supprimer certaines méta-données pour Excel, Word ou PowerPoint.

Cliquez ici pour consulter les conseils de Microsoft

Enfin, la Privacy Foundation a publié un rapport qui démontre comment on peut incorporer un mouchard sous la forme d'un *Web bug*, dans un document Office. Des cookies permettent ensuite de suivre à la trace le document dans toutes ses pérégrinations… Aucune parade pour l'instant.

2.- Le mouchard d' ICQ

ICQ, prononcez « I seek you » (je te cherche), est un logiciel de messagerie instantanée ou en directe de la famille des « Chat » (converser).

Le problème d'ICQ c'est que vous n'êtes jamais anonyme, votre adresse IP est toujours visible, même si vous tentez de la cacher, et donc vous êtes vulnérable aux attaques des hackers. De nombreux sites undergrounds proposent en téléchargement une foule d'utilitaires dédiés à ICQ afin de mettre diversement en cause la sécurité du connecté.

Nous ne saurions que vous conseiller de rester éloigné de ce genre de produit. D'autant plus que ICQ intègre un mouchard qui ferait l'inventaire de vos programmes et numéros de séries associés avant de renvoyer le tout aux serveurs d'*ICQ* (actuellement propriété d'AOL).

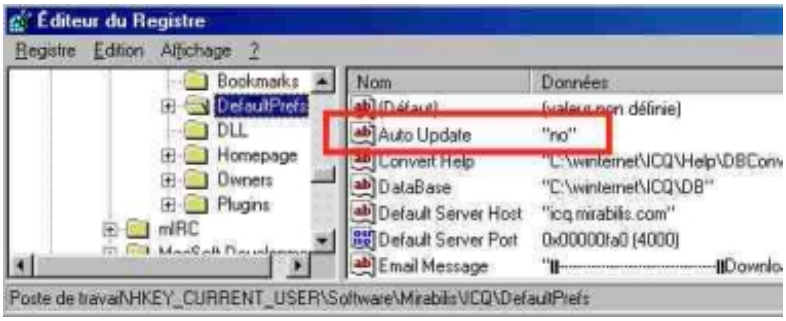
Avant toute manipulation de la base de registration de Windows, pensez à la sauvegarder à l'aide d'un utilitaire comme l'excellent Winsauve que vous trouverez dans notre rubrique téléchargement.

Voici comment désactiver ce mouchard :

1.- Lancez Regedit (Démarrer|Exécuter), l'éditeur de la base de registre.

2.- Placez vous sur HKEY_CURRENT_USER/Software/Mirabilis/ICQ/Defaultprefs

3.- Trouvez la clef « **Auto Update** » et changez la valeur de 'Yes' en '**No**'.



Désactivation du mouchard

Enfin, si vous ne vous sentez pas de taille à affronter la base de registration de Windows, vous pouvez utiliser un utilitaire qui fera le travail tout seul. Citons pas exemple l'excellent *Hulk Maximizer* qui, sous l'onglet « Mouchards », se propose de supprimer ce dernier.

3.- Le mouchard de Radiate : « mythe » ou réalité ?

Cette société anciennement baptisée Aureate Media, qui diffuse un gestionnaire de bandeaux publicitaires pour de nombreux freewares sponsorisés par la pub, a été l'objet d'une importante polémique ces derniers mois.

Un informaticien américain, *Steve Gibson*, prétend, sans en apporter la preuve irréfutable, que ces logiciels contiennent des modules espions qui profitent d'une connexion internet active pour envoyer discrètement des informations à votre sujet.

Cette information fut démantie par *Robert Smith,* expert en sécurité, qui est à la base de la découverte de nombreux mouchards dont celui de Windows 98 et RealJukebox et qui a analysé ces utilitaires.

Selon Radiate, la DLL Aureate ne récupère ni ne renvoie aucune information personnelle en dehors des informations relatives à la gestion des bandeaux publicitaires.

Néanmoins, d'après *Steve Gibson*, la DLL Aureate créée un trou de sécurité. Un pirate pourrait rediriger la communication de la DLL vers un serveur pirate et prendre le contrôle de la DLL, pour insérer du code destructeur.

De nombreuses interrogations subsistent qui démontreraient les intentions pour le moins suspectes de Radiate :

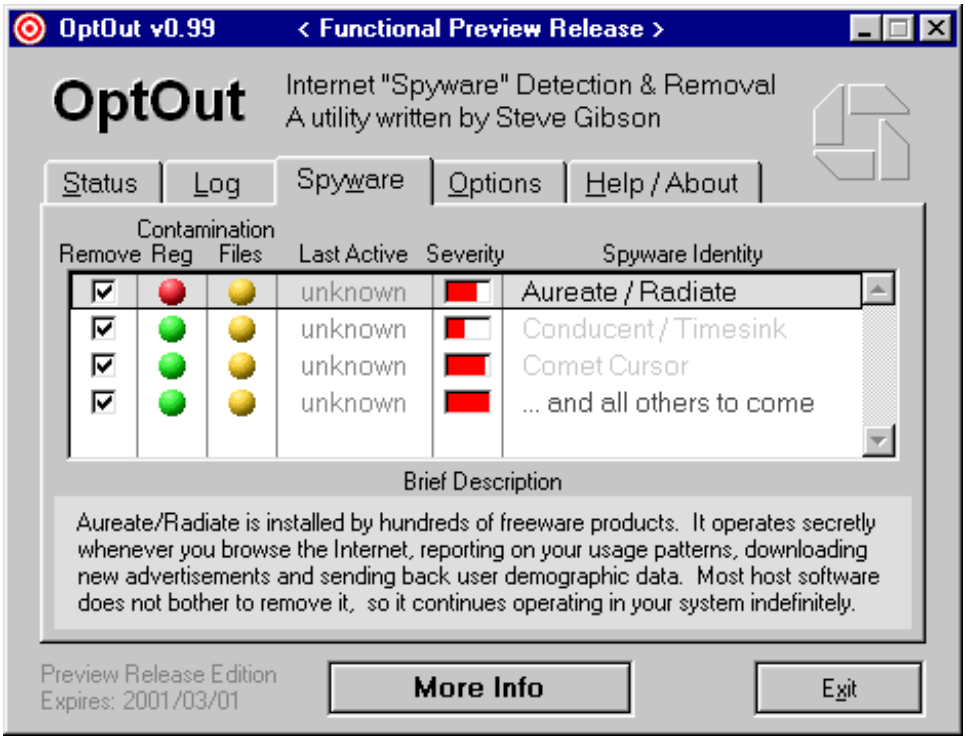
- Pourquoi aucune mention n'en est faite dans les nombreux utilitaires associés ?
- Pourquoi la désinstallation du freeware n'entraîne jamais la désinstallation du « mouchard » qui continue même de fonctionner indépendamment ?
- A quoi servent les fichiers installés ? mystère !

Quelles sont les applications concernées ? des centaines ! dont certaines très connues, citons Go!Zilla, CuteFTP, BuddyPhone, Zip Express, GetRight, Add/Remove plus, etc. La liste « officielle » est sur le site de Radiate, la liste officieuse sur ce site francophone dédié aux spywares qui recence 411 programmes infectés !

Steve Gibson a d'ailleurs développé un utilitaire gratuit, nommé OptOut, afin de supprimer le « mouchard », les applications continuant, sauf à de rares exceptions près, à fonctionner normalement.

Cliquez ici pour télécharger OptOut !

OptOut est un fichier directement exécutable, il n'a pas besoin d'être installé. Il propose un diagnostic immédiat de votre machine et vous saurez d'un coup d'œil si elle est infectée ou non.



Vous pouvez également utiliser avantageusement l'excellent programme spécialisé dans l'éradication des mouchards : **Ad-aware** de Lavasoft dont nous reparlerons plus loin.

Enfin, sachez que Radiate propose sur son site un outil pour désinstaller sa DLL, son utilisation induit de ne plus utiliser le ou les programmes hôtes associés car les auteurs ne seront plus rétribués par la publicité et l'utilisation de leur « œuvre » deviendrait frauduleuse (piratage).

Cliquez ici pour désinstaller la DLL Radiate

4.- Le mouchard de Conducent Technologies

TSAdBot de Conducent (ex-TimeSink) est également un module de gestion de bandeaux publicitaires pour les *freewares* et *sharewares,* soupçonné de récupérer des informations à votre insu.

D'après Conducent TSAdBot renvoie le système d'exploitation utilisé, votre adresse IP et un numéro d'identification de licence du programme utilisé, ainsi que le nombre de bandeaux publicitaires présentés et cliqués. Parfois un questionnaire est associé à l'installation du programme hôte, ces informations sont également envoyées.

Ce mouchard se trouve par exemple dans l'utilitaire **PKZip** mais dans ce cas (rare) sa présence est mentionnée quelque part dans la licence d'utilisation du logiciel.

Vous pouvez déterminer sa présence en mémoire en affichant le gestionnaire de tâches (Ctrl+Alt+Del) et en remarquant la présence d'une entrée « TSADBOT ».
Mais il peut être présent sur votre disque dur sans être actuellement actif dans ce cas cherchez le fichier TSAD.DLL dans le répertoire de Windows et TSAD.EXE dans un sous-dossier nommé AdGateway.

Bien que ce mouchard soit éradiqué par l'utilitaire **AD-aware**, cette méthode que nous devons au site Web-Sécurité, que nous saluons, permet de ne pas endommager l'application hôte du mouchard, qui continue à fonctionner normalement.

- Cliquez sur Démarrer puis Exécuter de la barre des tâches
- Tapez « msconfig » puis validez
- Dans l'onglet « Démarrage » trouvez la ligne du programme **tsAdbot.exe**
- Décochez la boite de sélection associée à sa gauche
- Notez le répertoire où se situe le programme.
- Redémarrez votre machine
- Allez dans le répertoire du programme et renommez l'exécutable (par exemple modifiez son extension) ce qui le rendra définitivement inactif.

A noter : Vous devez supprimer les programmes incriminés si vous refusez TSAdBot puisque dans ce cas les auteurs ne seront pas rémunérés et l'utilisation de leur « œuvre » devient frauduleuse.

5.- Le mouchard de Web3000

La société Web3000 fournit aux développeurs d'applications un composant similaire à celui de *Radiate* et *Conducent Technologies* afin de gérer l'affichage de messages publicitaires au sein de leurs logiciels.

Des messages marketings sont affichés dans la barre de titre du navigateur ou dans sa barre d'état (en bas) ou encore via des écrans d'accueil. Un petit bouton est également ajouté à coté des boutons système (cas de Netcaptor 6.x).

Ce module fonctionne, comme les autres, de manière totalement indépendante du programme « hôte ». L'oter n'empêche généralement pas le programme de fonctionner normalement.

Une nouvelle fois on soupçonne que des informations privées soient émises à destination du serveur de Web3000.

Vous trouverez une liste complète des utilitaires et applications utilisant ce module marketing sur le site de Web3000. On y trouve des dizaines d'utilitaires comme Netcaptor (un navigateur à vues multiples), CD Extractor, KFTP, PowerZip, MediaPlayer, etc.

Pour oter le mouchard il suffit de lancer **AD-aware** de *lavasoft* ou si vous aimez (comme moi) mettre les mains dans le « cambouis » supprimez les fichiers suivants (après les avoir sauvegardés !) situés dans le répertoire d'installation de Windows :

- NetSonic.w3k
- W3KNET_W3I.DLL
- W3knetdemo.ini
- W3Knet2.num
- W3knet.dll

Cette dernière DLL peut refuser la suppression. Dans ce cas désactivez-la dans la base de registre à l'emplacement suivant et seulement après avoir préalablement sauvegardé votre base de registre à l'aide de l'utilitaire Wisauve par exemple :

HKEY_Local_Machine/Software/Microsoft/Windows/Run

Le bouton de Web3000 doit disparaître des applications !

6.- Le mouchard de CometCursor

Comet Cursor est un outil gratuit pour les développeurs de site qui permet de modifier l'apparence du pointeur de la souris en fonction d'une page ou d'un site.
Pour fonctionner il nécessite un *plug-in* pour *Netscape* ou un contrôle ActiveX pour le navigateur de *Microsoft*.

Lors de la visite de certains sites Web supportant cette technologie, Comet Cursor assigne un numéro de série unique et récupère des informations à votre insu.

Chaque fois que Comet Cursor entre en fonction, le numéro de série ainsi que l'adresse du site visité est envoyé discrètement à son éditeur Comet Systems, permettant à ce dernier de retracer le parcours de leurs utilisateurs.

C'est en visitant le site de Dilbert, la BD des intellos, que *Richard Smith* (encore lui !), déjà à l'origine de la découverte du mouchard de Windows 98, RealJukebox et Amazon-zBubbles, à découvert ce nouveau mouchard et analysé son mode de fonctionnement.

Pour plus d'informations techniques sur ce mouchard, lisez notre article sur CometCursor dans nos Archives.

2 techniques d'éradications sont possibles : soit vous décidez de supprimer définitivement le programme, soit vous appliquez un correctif (Patch) qui permet de conserver les curseurs animés tout en bloquant l'envoi du numéro d'identification(ID).

Cliquez ici pour désinstaller CometCursor !

Le désinstalleur de Comet Cursor.

Vous pouvez également utiliser **OptOut** et **Ad-aware** (voir plus haut) pour le diagnostic et l'éradication du CometCursor.

Cliquez ici pour Patcher CometCursor !

Cette adresse détecte votre navigateur. Pour *Internet Explorer* le correctif est automatiquement chargé et installé en ligne via une page sécurisée. Pour *Netscape* un fichier est téléchargé de façon classique (comet_patch.exe – 3Ko). A vous de l'installer manuellement.

7.- Le mouchard de RealJukebox

Le consultant en sécurité Richard Smith, a (encore) mis à jour un mouchard dans le logiciel RealJukebox de *RealNetworks*.

Ce logiciel est un « player » de fichiers audio très puissant (lecture de CD audio, lecture MP3 et encodage MP3) et gestion des bibliothèques de titres. Cette version est diffusée à plus de 12 millions de copies durant l'hiver 1999 ! A chaque fois que l'on joue un CD, le player affiche le nom du CD, l'artiste et la liste de toutes les chansons du CD. Ces informations sont obtenues depuis une base de données sur un serveur Web de **RealNetworks.**

Richard Smith, intrigué par des échanges d'informations permanentes avec le serveur, analyse les données à l'aide d'un renifleur de réseau (Sniffer) et découvre que de nombreuses informations sont transmises à l'insu de l'utilisateur via l'Internet, comme :

- Les catégories (types musicaux) des titres lus
- Le nombre de titres stockés sur le disque dur de l'utilisateur
- Le nom des albums écoutés
- Les formats de fichiers les plus utilisés (mp3,...)
- Le modèle du player MP3 utilisé (WinAmp...)

Un **GUID**, numéro d'identification unique est généré qui identifie l'utilisateur.

Pour plus d'informations techniques sur ce mouchard, lisez notre article sur realJukebox dans nos Archives.

RealNetworks a été contraint d'éditer une mise à jour logicielle de RealJukebox. Cette nouvelle version empêche la transmission de certaines données utilisateur à *RealNetworks* pendant le téléchargement de musique (Get Music) et désactive l'ID RealJukebox.

Avant de télécharger le correctif lisez bien la page ci-contre :

Mise à jour de RealJukebox

Cliquez ici pour télécharger le Patch RealJukebox !

8.- Le cas DoubleClick

La Régie publicitaire en ligne *DoubleClick* a mis en place un système de gestion sophistiquée des bannières publicitaires avec une méthodologie statistique complexe basée sur deux technologies différentes pour espionner les internautes.

Quand un utilisateur individuel visite pour la première fois un site Web qui appose les bandeaux publicitaires de *DoubleClick*, ce dernier lui assigne un numéro unique d'identification (GUID) et mémorise ce numéro dans un *cookie* sur l'ordinateur de l'internaute.

Lorsque le visiteur revient sur l'un des 13 000 sites Web portant une bannière publicitaire fournie par *DoubleClick*, ce dernier lit son *cookie* et enregistre dans une base de données géante son numéro unique, auquel est rattaché le nom du site visité et d'éventuels renseignements personnels que l'internaute aura pu saisir pour passer une commande (nom, adresse, numéro de carte de paiement et de téléphone, etc.).

On peut donc, en juxtaposant les sites parcourus par un visiteur (traçabilité) et les produits achetés en ligne, se faire un portrait précis des préférences de cet internaute afin d'afficher automatiquement des publicités correspondants à ses centres d'intérêts.

DoubleClick a été contraint de proposer une procédure d'exclusion appelée **OptOut** sur son site Web qui consiste à remettre à zéro le *cookie* en remplaçant le numéro d'identification (id) par la mention id=OPT_OUT qui indique que vous ne souhaitez ni être identifié ni être pisté.

Pour supprimer votre numéro d'identification, **cliquez sur le bouton ci-dessous** :

Vous pouvez également utiliser les « zones de sécurité » de Microsoft Internet Explorer (menu *Options Internet* onglet *Sécurité*) pour ajouter une nouvelle zone de sécurité « *personnalisée* » avec un niveau de sécurité « *élevé* » qui ne permettra par défaut ni les Scripts ni les ActiveX ni les *cookies* pour les sites sensibles intégrant des bandeaux publicitaires de DoubleClick dont vous entrerez les adresses à l'aide du bouton « *Sites* ».

Dave Methvin de Winmag.com a conçu un fichier « .reg » afin de créer une nouvelle zone de sécurité dans Internet Explorer 5.x nommée « Tracking sites » et y a associé une centaine de sites sensibles dont ceux de Aureate, CometCursor, DoubleClick, etc. liste que vous pouvez complèter à loisir.

Téléchargez le fichier tracking.reg (13Ko) et double cliquez desssus, la base de registration sera mise à jour et les modifications immédiatement disponibles sous Internet Explorer.

Cliquez ici pour télécharger tracking.reg !

Attention : avant toute manipulation de la base de registre pensez à la sauvegarder à l'aide de Winsauve qui saura la restaurer sous DOS en cas de problème.

9.- Le mouchard de Mattel

Un logiciel-espion se cachait dans des cédéroms pour enfants de **Mattel** dans le but d'envoyer, en tâche de fond, des informations cryptées à l'insu de ses utilisateurs.

Bien cacher au fond du disque dur le « DSSAgent » issue de la technologie *Brodcast* se connecte à l'Internet avec insistance, afin d'envoyer son lot d'information. Même en « rebootant » la machine la connexion se rétablie d'elle même !

Plusieurs jeux **Mattel** en son pourvu dont *Reader Rabbit*, *Little Bear*, etc.

Mattel propose désormais un correctif (cleanbc.exe - 135K) pour se débarrasser de ce mouchard.

Cliquez ici pour télécharger le patch de Mattel

10.- Les mouchards de AOL-Netscape.

Le logiciel compagnon de Netscape 4.5 « *SmartDownload* » est suspecté de recueillir des informations sur les utilisateurs et les fichiers téléchargés.

Ce dernier s'active automatiquement quand l'internaute télécharge des fichiers sur le Web. Permettant l'interruption et la reprise libre du téléchargement, *SmartDownload* en profiterait également pour transmettre des informations concernant l'utilisateur et les fichiers téléchargés.

Pour l'instant, à ma connaissance , aucune contre-mesure n'a été trouvée mais *AOL* qui est en procès va devoir revoir sa copie.

La fonction « What's Related » qui permet d'obtenir une liste de « sites associés » au site actuellement consulté en cliquant sur un bouton, est également décriée : elle permet de « profiler » l'utilisateur car elle envoie la page actuellement consultée aux serveurs de *Netscape*, qui en retour renvoie une liste de sites similaires. Netscape peut ainsi tout savoir de ce que vous visitez.

La liste des sites associés est gérée par *Netscape* et la société Alexa. Cette dernière n'est pas une inconnue, cette même société est présente dans l'affaire du mouchard de la célèbre librairie en ligne Amazon (voire nos archives) qui utilisait déjà le même principe des « sites similaires » afin de renseigner ses bases de données d'informations privées…

Pour plus d'information sur les mouchards de Netscape 4.5 allez sur le site suivant.