Le Spyware dans Windows XP

Nicolas Ruff

EdelWeb
Nicolas.ruff@edelweb.fr

1 Introduction

1.1 Contexte

Le SpyWare, en lien avec le respect de la vie privée, est un sujet à la mode en ce moment - tout particulièrement dans ce contexte de lutte contre le terrorisme où nos libertés individuelles sont menacées.

En France des lois de plus en plus restrictives sont adoptées (Loi Sécurité Quotidienne, Loi sur la Confiance dans l'Economie Numérique), dont certaines autorisent des formes d'espionnage "légal" (écoute, conservation de traces).

Le géant Microsoft fait naître de nombreuses angoisses compte-tenu de l'hégémonie du système d'exploitation Windows et de la facilité avec laquelle celui-ci pourrait se transformer en instrument d'espionnage mondial (si ça n'est déjà le cas).

De nombreuses alertes - dont la médiatisation n'est pas toujours proportionnelle au risque réel (ex. "supercookie" Windows Media), ainsi que les nouveautés de Windows XP telles que le "Product Activation", ont contribué à diminuer la confiance des utilisateurs finaux que nous sommes. Sans parler des initiatives TCPA et Palladium, dont il ne sera pas question ici, mais qui préfigurent un avenir "connecté".

1.2 Objectif

L'objectif de cette présentation est de faire un tour d'horizon des principales nouveautés de Windows XP dont la fonction est de près ou de loin dépendante d'une communication avec un serveur Web Microsoft. Une analyse factuelle des sites contactés, des informations échangées et des possibilités d'exploitation de ces informations par Microsoft sera réalisée –lorsque cela est possible.

Cette présentation souhaite rester objective sans alimenter de fantasmes, tout en mentionnant les zones d'ombre qui persistent des mécanismes échappant à l'analyse. Enfin des solutions concrètes et applicables pour limiter les flux à destination d'Internet seront proposées en guise de conclusion.

1.3 Moyens

Le document de référence de cette étude est un "white paper" Microsoft de près de 200 pages dédié au thème des communications avec Internet :

"Using Windows XP Pro SP1 in a Managed Environment : Controlling Communication with the Internet"

Ce document a été décortiqué et validé sur différentes plateformes de test au sein du laboratoire R&D de EdelWeb. Les résultats de ces travaux, ainsi que d'autres menés par des sociétés tierces (tels que les auteurs des outils "Ad-Aware" ou "XP AntiSpy") sont présentés ici.

2 Noyau

3 Installation

Dès l'installation, Windows recherche une connexion réseau afin d'accéder aux sites de mise à jour et d'activation produit.

Windows dispose pour cela de 2 méthodes :

- Configuration manuelle
- Autodétection de la configuration réseau, selon les méthodes décrites ci-dessous

Méthode 1 : via des options DHCP

Si la configuration de l'interface réseau a été obtenue depuis un serveur DHCP, Windows envoie un message DHCP "Inform" à ce serveur pour lui demander les options suivantes :

- Informations envoyées
  - 12 Hostname = "machine_name"
  - 53 Message Type = "Inform"
  - 60 Vendor = "MSFT 5.0"
  - 61 Client ID = Ethernet + MAC Address
  - 55 Parameters (cf. ci-dessous)
- Informations demandées
  - 1 : subnet
  - 3 : router
  - 6 : DNS
  - 12 : hostname
  - 15 : domain name
  - 31 : router discovery
  - 33 : static route
  - 43 [paramètres spécifiques au vendeur] Non documenté
  - 44, 46, 47 : NetBT configuration
  - 249 [extension Microsoft] Non documenté
  - 252 [extension Microsoft] Option WPAD (cf. Q296591)

Méthode 2 : via une requête DNS

Windows utilise l'extension WPAD (*Web Proxy Auto Discovery*) : il effectue une résolution DNS sur le nom wpad.¡domaine¿, où ¡domaine¿ instancie tous les domaines connus du client.

Remarque : d'après la documentation disponible, les mécanismes d'autoconfiguration ont été améliorés dans Windows 2003.

3.1 Activation

Présentation générale Il ne faut pas confondre "activation" et "enregistrement" du produit.

- L'activation permet d'obtenir une licence définitive à partir de la clé de licence collée sur le boîtier du CD. Elle est obligatoire sous 90 jours. Les clés de licence dites "en volume" outrepassent cette fonction. L'objectif principal annoncé par Microsoft est la lutte contre le piratage.
- L'enregistrement permet de déclarer auprès de Microsoft l'installation de logiciels. Cette opération est facultative.

Détails techniques Le processus d'activation du produit est complexe et très bien documenté par le site `http://www.licenturion.com/xp/`. Pour résumer, la clé de licence temporaire est utilisée en conjonction avec les paramètres ci-dessous et d'autres éléments tels qu'une clé Microsoft et un aléa pour générer un ID d'installation. A cet ID correspond une clé de licence définitive qui ne peut être calculée que par le support Microsoft. Les algorithmes utilisés (MD5 et SHA-1 entre autres) sont à sens unique et ne permettent pas de reconstituer les informations initiales.

Paramètres matériels pris en compte :

- Numéro de série de la partition système
- Adresse MAC de l'interface réseau
- Chaîne d'identification du CD-ROM
- Chaîne d'identification de la carte graphique
- CPU ID
- Chaîne d'identification du disque dur
- Chaîne d'identification de la carte SCSI
- Chaîne d'identification du contrôleur IDE
- Modèle de CPU
- RAM installée (en puissances de 32 Mo)
- Système amovible ou non

Dès lors que plus de 3 des paramètres ci-dessus sont modifiés, le produit doit être réactivé.

L'outil d'enregistrement est MSOOBE.EXE (`%WinDir%\System32\OOBE`) - pour "*Out Of the Box Experience*". Celui-ci supporte 2 méthodes de transmission : le téléphone ou Internet. Dans ce dernier cas, c'est le site `http://wpa.one.microsoft.com/` qui est contacté.

Le stockage de la clé de licence défintive s'effectue dans :

```
%WinDir%\System32\wpa.dbl
HKLM\SYSTEM\WPA
```

Un journal des opérations se trouve dans `%WinDir%\setuplog.txt`

Pour plus d'informations, se reporter au site `http://www.microsoft.com/piracy/basics/activation/`

A titre indicatif l'enregistrement du produit s'effectue via le site `http://reg.register.microsoft.akadns.net/` (noter le DNS dynamique !).

3.2 Explorer.exe

"Explorer" est l'interface graphique utilisateur par défaut. Il existe de nombreuses interactions entre Explorer et le monde extérieur dans la configuration par défaut :

- Les raccourcis réseau ("Favoris réseau") et Web sont vérifiés à l'ouverture de session et lors de tout rafraîchissement (ex. touche F5).
- Option (active par défaut) "rechercher automatiquement les dossiers et imprimantes partagées"
- Option "cette copie de Windows est-elle légale ?" affichant une page du site Microsoft

L'outil "assistant recherche" du menu démarrer est particulièrement représentatif de ce point de vue :

- Son interface est complètement Web (HTML + VBE)
- Le site de recherche par défaut est `http://ie.search.msn.com/` (personnalisable - il est possible d'utiliser Nomade, etc.)
- Le répertoire de stockage des fichiers de l'application est `%WinDir%\srchasst`
  - Ceux-ci se mettent à jour automatiquement depuis Internet à chaque usage de la fonction !
- Paramétrable par la clé de base de registre "*Use Search Asst*".
- Le délai de conservation des journaux côté serveur (recherches effectuées) annoncé par Microsoft est de 1 an.
- Ce composant affiche de la pub ...

Pour mémoire, il semble judicieux de rappeler ici que l'interface Explorer souffre de nombreux problèmes de sécurité autres que les accès Internet :

- L'interface Explorer par défaut est une page Web, personnalisable à l'aide du modèle "folder.htt". Elle partage son moteur de rendu (et ses vulnérabilités) avec Internet Explorer.
- Certaines extensions de fichier ne sont pas affichées par défaut même si l'option globale est activée (ex. ".SHS", "`.<GUID>`")
- Il est possinble d'exécuter des fichiers indépendamment de leur extension via la ligne de commande (ex. renommer un .EXE en .PDF permet toujours de le lancer via un CMD).
- L'ordre de recherche par défaut des exécutables est dangereux puisqu'il inclut le répertoire courant avant les répertoires système
  - Pour les DLLs, ce comportement est paramétrable par la clé de base de registre "*SafeDllSearchMode*".
- Etc...

Toutes ces failles étant ou pouvant être exploitées par du code malveillant (ex. virus).

3.3 Aide et support

La fonction d'aide et support dispose elle aussi d'une interface complètement Web, stockée dans le répertoire :

"`%WinDir%\PCHealth\HelpCtr\`".

Certaines sections proviennent directement d'Internet :

- Rubrique "*Le saviez-vous ?*", mise en cache dans le répertoire : "`%WinDir%\PCHealth\HelpCtr\Config\`" (fichiers "*NewsSet.xml*" et "`\News\NewsVer.xml`"), et issue des liens
  - `http://go.microsoft.com/fwlink/?LinkID=11`
  - `http://windows.microsoft.com/windowsxp/newsver.xml`
- Recherche dans MSDN (qui transmet la langue et le type de produit installé)

Ce fonctionnement est paramétrable via la clé de base de registre "*Headlines*" et les "*Options de recherche*".

Enfin une des fonctions les plus impressionnantes est la possibilité de prise en main du poste par Microsoft via la fonction "Remote Assistance". Pour cela Microsoft dispose du compte préinstallé "*SUPPORT_388945a0*", membre du groupe "*HelpServicesGroups*". Il suffit à l'utilisateur de se connecter au site `https://webresponse.one.microsoft.com/`.

A noter que cette fonction est extensible par les OEM.

3.4 WindowsUpdate

WindowsUpdate est le site de distribution des mises à jour logicielles (incluant les mises à jour de sécurité) pour les produits Windows / Internet Explorer. Ce site peut être consulté manuellement, via un raccourci du menu démarrer, ou via les fonctions de type "*Dynamic Update*", "*Auto Update*", etc. – les mécanismes sous-jacents sont identiques.

Attention : ce site ne diffuse aucune mise à jour pour d'autres produits tels que Office, SQL, Exchange, etc. – c'est une des raisons de la propagation du ver SQL/Slammer.

Le fonctionnement de ce site est relativement complexe et repose sur plusieurs composants :

- Un contrôle ActiveX signé : "*UpdateClass*" (de taille ≈ 100 Ko)
  - `http://v4.windowsupdate.microsoft.com/CAB/x86/unicode/iuctl.CAB`
- Un site Web
  - `http://www.windowsupdate.com/` (alias)
  - `http://windowsupdate.microsoft.com/`
- Un moteur de traitement partagé entre client et serveur
  - Script côté client
  - Fichier XML côté serveur
    - `https://v4.windowsupdate.microsoft.com/getmanifest.asp`
    - `https://v4.windowsupdate.microsoft.com/consumerdrivers/getmanifest.asp`

- Des répertoires de travail côté client
  - `C:\Program Files\WindowsUpdate`
  - `C:\WUTemp`
- Des journaux d'installation
  - Historique des installations IUHIST.XML
  - `%WinDir%\Windows Update.log`
  - `%WinDir%\Setupapi.log` (journal global des installations)

Une analyse des échanges réseau confirme qu'aucune information nominative ou sensible ne transite sur le réseau. On notera toutefois les points suivants :

- WindowsUpdate, ainsi que d'autres fonctions système telles que le rapport d'erreur, exploitent le service "*Upload Manager*", qui effectue des transferts en arrière plan. Ce service présente des zones d'ombre car :
  - Il effectue des transferts de manière asynchrone donc difficilement analysables
  - Il est démarré par SVCHOST donc difficile à filtrer même avec un firewall personnel
  - Son API n'est pas documentée
- Les communications avec le serveur n'utilisent pas HTTPS pour le téléchargement des correctifs. Ceux-ci sont signés, mais les mécanismes de vérification de la signature ne sont pas connus (serait-il possible de présenter n'importe quel exécutable signé ou celui-ci doit-il provenir de Microsoft ?)

A titre anecdotique, on notera les points suivants :

- Il existe une adresse IP "en dur" dans le contrôle ActiveX : 207.46.226.17. Cette adresse ne correspond pas à une machine accessible depuis Internet.
- Commentaire tiré d'une page WindowsUpdate
  - *// Do not Remove this "else". Bug 16783 (If u remove this else, then for IE5 when we redirect to another page in above line, then it flashes an Action Cancelled page for a sec)*

3.5 Rapport d'erreur

Il existe 2 types de rapport d'erreur : le rapport d'erreur applicatif et le rapport d'erreur système (noyau). Dans les 2 cas Windows propose de remonter l'information sur le site Microsoft `http://watson.microsoft.com/`.

Les informations suivantes figurent dans un rapport d'erreur applicatif :

- Adresse IP (lors de la transmission)
- Product ID
- Minidump (documenté dans le Platform SDK)
  - Threads (informations "standard" et "étendues").
  - Modules (chargés et déchargés).
  - Données d'allocation mémoire (32 et 64 bits).
  - Gestionnaire d'exceptions.
  - Informations système.
  - Commentaires.
  - Handles.
  - Fonctions exportées.

Windows 2003 Données du processus (ID, temps d'exécution).
– Champs "réservés" (inutilisés dans Windows XP)

Les informations suivantes figurent dans un rapport d'erreur système :
– Adresse IP (lors de la transmission).
– Informations matérielles.
– Processeurs, RAM.
– Drivers installés et drivers chargés (verbeux).
– Informations logicielles (OS, version, langue).
– Message d'erreur.
– Contexte d'exécution.
– Pile noyau.

Ces informations sont transmises au reboot suivant à l'aide du service "*Upload Manager*".

Dans les deux cas aucune information sensible ne transite volontairement dans le rapport d'erreur, toutefois les "dumps" mémoire peuvent fort bien contenir des bribes de documents, des clés ou des mots de passe. Il est regrettable que l'utilisateur ne puisse pas sélectionner individuellement les informations qu'il souhaite transmettre, comme c'est le cas avec le service de rapport d'erreur de Netscape par exemple.

Le composant responsable de la génération du rapport est DrWatson :

`%WinDir%\System32\dwwin.exe).`

La transmission s'effectue à l'aide des protocoles HTTP et HTTPS (pour le contenu du rapport uniquement).

Il est intéressant de connaître le site "*Corporate Error Reporting*" (`http://oca.microsoft.com/`), qui permet la consultation des rapports transmis pendant 180 jours.

3.6 Authentification Passport

"*Passport*" est une solution de SSO à l'échelle du Web, développée par Microsoft et intégrée nativement aux dernières versions de Windows (XP, 2003), Internet Explorer (6.0) et IIS (6.0). Cette authentification est d'ores et déjà indispensable pour accéder aux services suivants :
– Services Microsoft (MSDN, Beta Previews, etc.).
– "Spin-offs" Microsoft : MSN, Hotmail, Messenger ...
– Sites partenaires (liste complète sur `http://www.passport.net/`)

Le seul concurrent direct de cette initiative est le projet Liberty Alliance (`http://www.projectliberty.org/`) qui n'en est qu'à ses débuts.

Le principe de fonctionnement repose sur un serveur central d'authentification (base de données utilisateurs) et l'utilisation de cookies sur le poste client. Les sites centraux sont :
– `http://register.passport.net/`
– `https://login.passport.com/`
– `https://nexus.passport.com/` (remarque : "*nexus*" est un terme utilisé dans Palladium)

Les risques pour la confidentialité des données nominatives fournies au système Passport (allant jusqu'à des numéros de carte bleue) sont très importants :

- La base de données d'informations nominatives est partagée entre tous les partenaires - l'utilisateur est censé conserver un niveau de contrôle sur la diffusion de l'information mais rien ne lui garantit que ses "préférences" sont respectées par le système central.
- Ce système permet un "tracking" à des fins marketing de l'activité utilisateur.
- Les risques de vol d'information par des tiers malveillants sont réels, puisque des vulnérabilités ont déjà identifiées par le passé : ex. cookie "PPTProf=..." contenant des informations en clair.

Pour plus d'informations on se reportera au Passport SDK. A titre d'information sur les vulnérabilités :

`http://www.tcpdemux.com/products/netintercept/casestudies/passport`

3.7 Login Web

Ce chapitre couvre deux modes très différents de gestion des authentifiant par Internet Explorer :

- L'authentification native HTTP (de type ".htaccess").
- L'authentification applicative (formulaires).

Authentification native Les modes d'authentification supportés par IE 6.0 SP1 sont :

- Anonymous (pas d'authentification)
- Basic (mot de passe en clair - RFC2617)
- Basic sur connexion SSL
- Digest Authentication (MD5 avec secret partagé - RFC2617)
- Challenge/Response
  - NTLM
  - Passport
- Client Certificates (certificats clients SSL).
- Fortezza (solution à base de certificats).

Le risque est bien entendu qu'un authentifiant connu du système (ex. login Windows) soit passé par défaut dans un contexte de connexion inapproprié (ex. accès à un site Internet). Suite à des avis de sécurité sur le sujet, les paramètres d'authentification par défaut sont désormais :

- Zone Internet, Sites sensibles : demander le mot de passe.
- Zone Intranet, Sites de confiance : login automatique (avec le login Windows !).

Les risques sont donc limités au réseau interne. On notera que le client Telnet présentait le même type de comportement dangereux (cf. MS00-067).

Authentification applicative Internet Explorer propose plusieurs options de "saisie semi-automatique" :

- Adresses Web.
- Contenu des formulaires.
- Logins dans les formulaires.
- Mots de passe dans les formulaires.

Les mots de passe sont stockés dans le "*Protected Storage*", c'est-à-dire la clé : "`HKCU\Software\Microsoft\Protected Storage System Provider`" (invisible par défaut, même aux administrateurs).

Suite à de nombreux problèmes de sécurité dans les versions antérieures de Windows, ce "*Protected Storage*" offre désormais une API de stockage sécurisé unique pour les applications. Cet emplacement de stockage est chiffré avec le mot de passe de login Windows.

Il est toutefois possible (sous certaines conditions) d'accéder aux données contenues dans cet emplacement (cf. outils "*IE Password Revealer*", sites Lost-Password, Elcomsoft, etc.).

Il est donc recommandé de désactiver toute forme de saisie semi-automatique dans Internet Explorer.

3.8 Synchronisation horaire

Par défaut les postes XP utilisent une synchronisation horaire

- Dans le cas d'une machine en domaine, le serveur par défaut est le contrôleur de domaine défini comme source de temps.
- Dans le cas d'une machine en "*Workgroup*", le serveur par défaut est "*time.windows.com*" (alternativement "time.nist.gov"). L'intervalle de mise à jour par défaut est de 1 semaine.

Ce comportement est paramétrable dans la clé de base de registre "`HKLM\System\CCS\Services\W32Time`".

Le protocole NTP standard est utilisé. Aucune information indésirable n'est transmise.

4 Composants préinstallés

4.1 Windows Media Player

La version de Windows Media Player livrée avec Windows XP SP1 est la 8.0. Curieusement celle-ci n'est pas téléchargeable sur le site de Microsoft, seule les versions 6.4, 7.0 et 9.0 étant publiques.

Windows Media est typiquement une application faisant un usage immodéré d'Internet, par exemple pour les fonctions suivantes :

- Acquisition de licences (DRM).
- Accès à des services "en direct" (contenu à la demande, radios).
- Base de métadonnées CD et DVD (en lecture/écriture).
- Téléchargement de codecs.
- Mises à jour logicielles.
- Skins et visualisations.

– "*Media Library*", "*Media Guide*", *Newsletter MSN*, ...

Le site de référence pour tous ces accès est `http://www.windowsmedia.com/`.

Les risques associés sont très importants. Outre les problèmes d'atteinte à la vie privée, Windows Media étant un superbe outil de marketing personnalisé, il existe des problèmes de sécurité intrinsèques :

– Le lecteur Windows Media possède un identifiant unique (GUID), utilisé techniquement pour assurer la qualité de service sur les serveurs de contenu à la demande. Windows Media étant un composant ActiveX scriptable par des tiers, ce GUID permet d'identifier un poste de manière unique via un navigateur : il s'agit de la notion de "*supercookie*".
– Les "*skins*" et visualisations sont des archives ZIP incluant du contenu actif, d'où un risque d'exécution de code malveillant.

4.2 Internet Explorer

Windows XP SP1 est livré avec la version 6.00.2600.1106 d'Internet Explorer. Bien que les couches superficielles du logiciel puissent être supprimées, il n'est effectivement pas possible de désactiver le moteur de rendu HTML contenant la majorité des bogues, celui-ci étant exploité par d'autres outils tels que Explorer.

Les accès Internet inattendus effectués par IE sont les suivants :

– Page initiale, permettant l'élaboration de statistiques d'installation.
  – `http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome`
– Spyware "*Alexa*" (détecté par l'outil "*Ad-Aware*").
  – En lien avec l'option "*effectuer des recherches depuis la barre d'adresses*".
– Option "*Vérifier les signatures des programmes téléchargés*".
– Option "*Vérifier la révocation des certificats*".
– Option "*Vérifier la révocation des certificats de l'éditeur*".
– Option "*Vérifier automatiquement les mises à jour de IE*".
– Option Windows "*Mise à jour des certificats racine*".
  – Si un certificat SSL signé par une autorité inconnue est présenté, une mise à jour de la base des autorités racine est déclenchée depuis le site `http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt`

Internet Explorer dans sa configuration par défaut communique donc régulièrement avec des sites Microsoft, toutefois aucune information sensible n'est échangée. A noter qu'Internet Explorer est aussi une source privilégiée pour l'installation de Spywares "*tierce partie*" par le biais des mécanismes suivants :

– Gestion des cookies (par défaut le navigateur utilise P3P).
– Options "*Activer les extensions tierce partie*", "*Activer l'installation à la demande*", "*Éléments installables du bureau*".
– Bogues permettant d'exécuter du code ...

4.3 Windows Messenger

Windows XP SP1 est livré préinstallé avec Windows Messenger 4.7.

Ce composant utilise indifféremment et simultanément les 3 services d'annuaire suivants :

- Exchange 2000 (si configuré).
- Serveur SIP (Session Initiation Protocol) - RFC 2543.
- Serveur Microsoft avec authentification Passport.
  - En direct : `http://messenger.hotmail.com:1863/`.
  - Via un proxy : POST. `http://gateway.messenger.hotmail.com/gateway/gateway.dll?Action=open&Server=NS&IP=messenger.hotmail.comHTTP/1.1`

Le protocole de base est HTTP, celui-ci servant à encapsuler 2 sous-protocoles propriétaires :

- Des commandes de type XYZ [paramètre 1] [paramètre 2] [...].
- Des données de type MIME propriétaire (ex. "*application/x-msn-messenger*", "*text/x-msmsgsprofile*", ...) véhiculant des données partiellement brouillées selon un algorithme inconnu.

Les risques associés à l'utilisation de ce composant sont :

- La divulgation d'informations personnelles en clair (via le protocole HTTP).
- Un système à serveur central donc adapté à la traçabilité et au contrôle.
- Un niveau d'informations échangées inconnu à cause du brouillage des données.

Exemple de contenu capturé :

- `Content-Type: text/x-msmsgsprofile; charset=UTF-8`
- `EmailEnabled: 1`
- `MemberIdHigh: 9xxxx`
- `MemberIdLow: -2114xxxxxx`
- `lang_preference: 1036`
- `preferredEmail: xxxxxxx@hotmail.com`
- `country: FR`
- `PostalCode: 75010`
- `Gender: m`
- `Kid: 0`
- `Age: 26`
- verb+BDayPre : 2+
- verb+Birthday : 2.821600e 004+
- verb+ Wallet : 0+
- verb+Flags : 1027+
- verb+sid : 507+
- verb+kv : 4+
- verb+MSPAuth : 4n3lILtj1DTLjIKvsjAeFx3NL3kmxyhl5V5207HY !tFCSReUcu...+
- verb+ClientIP : 212.xxx.xxx.xxx+
- verb+ClientPort : 0+

5 Office XP

Les problèmes de confidentialité liés à la suite Office XP ne seront que brièvement évoqués, puisque le sujet a été traité dans le magazine MISC n°7 ("*La fuite d'information dans les documents propriétaires*").

Les principaux reproches adressés à la suite Office sont :

- Forte intégration avec le système Windows.
  - Ex. Word devient l'éditeur HTML par défaut.
  - Forte intégration des produits entre eux.
  - Ex. envoyer un document Word avec Outlook modifie les propriétés du document.

Parmi les risques bien documentés on peut citer :

- La verbosité des propriétés du document (auteur, temps d'édition, chemins UNC).
- L'enregistrement de l'historique du document (versions antérieures).
- Les "*Word bugs*".
- Les risques liés aux macros et l'absence de solution satisfaisante.
- Le vol de données par les champs de fusion.
- L'utilisation de l'adresse MAC comme GUID.
- Etc...

6 Les solutions

Tous les problèmes évoqués précédemment ne sont pas sans solution (heureusement). A l'aide des possibilités offertes par le système lui-même, il est possible de modifier le paramétrage par défaut (souvent insatisfaisant) et de désactiver les accès Internet des composants :

- Via l'interface graphique.
- Via des clés de base de registre.
- Via les GPO.
- Via les "Administration Kits" (ex. IEAK).

A noter que Windows possède un paramètre de configuration global du Proxy, qui permet de rediriger les accès Internet indus vers "*/dev/null*". Il reste ensuite à utiliser des logiciels gérant des paramètres Proxy personnalisés (ex. Netscape).

Enfin d'autres mesures pourraient être :

- Désintaller les composants cachés (fichier SYSOC.INF).
- Utiliser la fonction de restriction d'exécution.
- Mettre en place des miroirs internes (ex. MSUS).

Lorsque le système s'avère insuffisant pour bloquer un composant spécifique, il est possible d'utiliser des outils tiers tels que firewall personnel ou logiciel de configuration "*anti-spyware*".

Une solution radicale consiste à isoler les systèmes Windows XP de tout accès Internet, ...

7 Conclusion

Le sujet des interactions entre Windows XP et les sites Microsoft est loin d'être clos (voir annexe A),...

Windows XP SP1 communique régulièrement avec des sites Internet, de manière plus ou moins documentée et/ou configurable. Ces fonctions sont activées par défaut mais dans la plupart des cas désactivables.

Une étude plus poussée montre que les informations collectées par Microsoft sont individuellement peu significatives, mais leur recoupement permettrait d'obtenir un puissant outil de marketing personnalisé. Seules quelques fonctions (telles que Remote Assistance ou Passport) mettent en péril de façon significative la sécurité du système ou des informations qu'il contient.

D'autre part les informations transmises bénéficient d'un niveau de protection très hétérogène (protocoles HTTP ou HTTPS, chiffrement, brouillage, protocole propriétaire, etc...).

On notera avec plaisir qu'il existe des moyens de se protéger, le plus simple étant de ne pas renseigner l'adresse de son Proxy au niveau de Windows.

Références

1. *Using Windows XP Pro SP1 in a Managed Environment : Controlling Communication with the Internet*, `http://technet.microsoft.at/includes/file.asp?ID=4668`
2. *XP Anti-Spy*, `http://www.xp-antispy.org/`
3. *Windows XP shows the direction Microsoft is going*, `http://www.hevanet.com/peace/microsoft.htm`
4. *Microsoft Secrets*, `http://www.securityoffice.net/mssecrets/`

A Sujets non traités

- "*Application Help*" / "*Driver Protection*" / Assistant Compatibilité. Microsoft maintient une base d'applications incompatibles et de correctifs : `APPHELP.SDB + SYSMAIN.SDB / DRVMAIN.SDB`.
  Cette liste est mise à jour par WindowsUpdate.
- "*Device Manager*".- Les pilotes signés peuvent être mis à jour en 1 click. Cette fonction est gérée par WindowsUpdate.
- Journal d'événements.- La plupart des événements système contiennent un raccourci vers un site explicatif : `http://go.microsoft.com/fwlink/events.asp`. Ce site est configurable via les clés suivantes :
  - *MicrosoftRedirectionURL*.
  - *MicrosoftRedirectionProgram*.
  - MicrosoftRedirectionProgramCommandLineParameters.
- Associations de fichiers.- Cliquer sur un fichier dont l'extension n'est pas associée provoque la redirection vers un site Microsoft : `http://shell.`

`windows.com/fileassoc/nnnn/xml/redir.asp?ext=AAA` (Nnnn = langue, AAA = extension) Cette option est configurable via la clé NoInternetOpenWith.
- Jeux "*on line*".- Se connectent au site `http://www.zone.msn.com/`
- Netmeeting.- Se connecte à un serveur ILS au choix (par défaut : *netmeeting.microsoft.com*). Les ports utilisés sont : TCP/389, TCP/522, TCP/1503, TCP/1720, TCP/1731 + ports dynamiques.
- "*Online Device Help*", Plug-and-Play.- Aide en ligne pour la recherche de drivers si un périphérique inconnu est détecté ou lors de l'insertion de nouveaux périphériques. Transmet le profil matériel du périphérique (PnP ID). Site `http://www.microsoft.com/windows/catalog/`
- Outlook Express 6.
- Universal Plug-and-Play.- Requêtes UDP/1900 pour la détection de matériel réseau.
- MSN Explorer.- Portail Internet Microsoft.

B Sites Microsoft cités dans la présentation

Microsoft.com
- `http://oca.microsoft.com/`
- `http://go.microsoft.com/fwlink/?LinkID=11`
- `http://go.microsoft.com/fwlink/events.asp`
- `http://watson.microsoft.com/`
- `http://windows.microsoft.com/windowsxp/newsver.xml`
- `http://windowsupdate.microsoft.com/`
- `http://wpa.one.microsoft.com/`
- `http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome`
- `http://www.microsoft.com/windows/catalog/`
- `http://www.microsoft.com/piracy/basics/activation/`
- `http://v4.windowsupdate.microsoft.com/CAB/x86/unicode/iuctl.CAB`

MSN.com, hotmail.com
- `http://messenger.hotmail.com:1863/`
- `http://gateway.messenger.hotmail.com/`
- `http://ie.search.msn.com/`
- `http://www.zone.msn.com/`

Passport.net
- `http://www.passport.net/`
- `http://register.passport.net/`

WindowsUpdate
- `http://www.windowsupdate.com/`
- http ://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt

Autres
- `http://reg.register.microsoft.akadns.net/`
- `http://www.windowsmedia.com/`

– `http://shell.windows.com/fileassoc/nnnn/xml/redir.asp?ext=AAA`