



EdelWeb

OSSIR

Le Spyware dans Windows XP

Nicolas RUFF / EdelWeb
Nicolas.ruff @edelweb.fr



1. **Introduction**
2. **Le noyau système**
 1. **Installation**
 2. **Activation du produit**
 3. **L'interface utilisateur (Explorer)**
 4. **Aide et support**
 5. **WindowsUpdate**
 6. **Rapports d'erreur**
 7. **Authentification Passport**
 8. **Login Web**
 9. **Synchro NTP**
3. **Les composants préinstallés**
 1. **Windows Media Player**
 2. **Internet Explorer**
 3. **Windows Messenger**
4. **Quelques mots sur Office XP**
5. **Comment se protéger ?**
6. **Conclusion**
7. **Annexe A : Sujets non traités**
8. **Annexe B. Liste des sites Microsoft**

1. Introduction (1/2)



EdelWeb

- **Le SpyWare et le respect de la vie privée sont des sujets à la mode**
 - **Terrorisme vs. Libertés individuelles**
 - **LSQ, LCEN, ...**

- **Microsoft fait naître de nombreuses angoisses**
 - **Alertes très médiatisées (« supercookie » Windows Media, ...)**
 - **« Product Activation » requis à partir de Windows XP**
 - **Initiative TCPA / Palladium**
 - **Etc.**

1. Introduction (2/2)



EdelWeb

■ Objectifs de la présentation

- Rester objectif
- Identifier les communications de Windows XP avec Internet
 - Serveurs, contenu échangé, possibilités d'exploitation par Microsoft
- Lister les zones d'ombre
- Préciser les risques réels et proposer des solutions

■ Moyens

- Un document Microsoft de référence
 - « Using Windows XP Pro SP1 in a Managed Environment : Controlling Communication with the Internet »
- Des travaux parallèles
 - Ad-Aware, XP AntiSpy, R&D EdelWeb, ...



- **Dès l'installation, Windows recherche une connexion réseau**
 - **Méthodes**
 - Automatique : autodétection de la configuration réseau (cf. ci-dessous)
 - Manuelle : possibilité de configurer un accès RAS ou réseau
 - **Actions**
 - Activation du produit (q.v.)
 - Recherche de correctifs (site WindowsUpdate – q.v.)
- **Mécanismes d'autodétection réseau**
 - **Via des options DHCP**
 - 12 Hostname = « machine_name »
 - 53 Message Type = « Inform »
 - 60 Vendor = « MSFT 5.0 »
 - 61 Client ID = Ethernet + MAC Address

2. Noyau Installation



EdelWeb

- 55 Parameters
 - 1 : subnet
 - 3 : router
 - 6 : DNS
 - 12 : hostname
 - 15 : domain name
 - 31 : router discovery
 - 33 : static route
 - 43 [vendor-specific]
 - 44, 46, 47 : NetBT configuration
 - 249 [Microsoft-specific] non documenté
 - 252 [Microsoft-specific] WPAD option (cf. Q296591)

- **Via une requête DNS**

- wpad.<domaine> (Web Proxy Auto Discovery)

- **Remarque : les mécanismes d'autoconfiguration ont été améliorés avec Windows 2003**

2. Noyau Activation (1/2)



EdelWeb

■ Présentation générale

- Ne pas confondre « activation » et « enregistrement »
- L'activation permet d'obtenir une licence définitive
- Les clés « en volume » outrepassent cette fonction
- Objectif principal pour Microsoft : lutter contre le piratage

■ Détails techniques

• Génération

– Paramètres 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

2. Noyau Activation (2/2)



EdelWeb

- Outil MSOOBE.EXE (%SystemRoot%\System32\OOBE)
- Algorithmes : MD5 et SHA-1
- **Transmission**
 - 2 méthodes : téléphone ou Internet
 - Site <http://wpa.one.microsoft.com/>
- **Stockage**
 - Un journal des opérations se trouve dans %SystemRoot%\setuplog.txt
 - La clé finale se trouve dans
 - %SystemRoot%\System32\wpa.dbf
 - HKLM\SYSTEM\WPA
- **Enregistrement**
 - Site <http://reg.register.microsoft.akadns.net/>
- **Références**
 - <http://www.microsoft.com/piracy/basics/activation/>
 - <http://www.licenturion.com/xp/>

2. Noyau Explorer.exe



EdelWeb

- **Nombreuses interactions entre Explorer et le monde extérieur**
 - Les raccourcis réseau et Web sont vérifiés à l'ouverture de session et lors de tout rafraîchissement
 - Option « rechercher automatiquement les dossiers et imprimantes partagées »
 - Option « cette copie de Windows est-elle légale ? »
 - Assistant Recherche
 - Interface complètement Web (avec scripts encodés)
 - Site de recherche par défaut : <http://ie.search.msn.com/>
 - Répertoire de stockage : %windir%\srchasst
 - Mise à jour automatique de cette fonctionnalité depuis Internet
 - Paramétrable par la clé « Use Search Asst »
 - Conservation des logs annoncée par Microsoft : 1 an
 - Affiche de la pub ...

- **Autres risques (pour mémoire)**
 - L'interface Explorer par défaut est une page Web
 - Prise en compte du modèle « folder.htt »
 - Affichage incorrect des extensions de fichier même si l'option globale est activée (ex. .SHS, .<GUID>)
 - Exécution de fichiers indépendamment de leur extension via la ligne de commande
 - Ordre de recherche des exécutables dangereux (clé SafeDllSearchMode)

2. Noyau Aide et support



EdelWeb

■ Aide et support

- Interface complètement Web
 - %WinDir%\PCHealth\HelpCtr\
 - %WinDir%\PCHealth\HelpCtr\Config\NewsSet.xml et News\NewsVer.xml
 - <http://go.microsoft.com/fwlink/?LinkID=11>
 - <http://windows.microsoft.com/windowsxp/newsver.xml>
- Certaines sections proviennent directement d'Internet
 - Rubrique « Le saviez-vous ? »
 - Recherche dans MSDN
 - Transmet la langue et le type de produit installé
- Paramétrable
 - Clé Headlines
 - Options de recherche

■ Prise en main du poste par Microsoft via Remote Assistance

- Compte SUPPORT_388945a0
 - Membre de HelpServicesGroups
- Extensible par les OEM
- Site <https://webresponse.one.microsoft.com/>

2. Noyau WindowsUpdate (1/2)



EdelWeb

■ Composants

- **Composant ActiveX : « UpdateClass » (taille ~100 Ko)**
 - <http://v4.windowsupdate.microsoft.com/CAB/x86/unicode/iuctl.CAB>
- **Sites**
 - <http://www.windowsupdate.com/> (alias)
 - <http://windowsupdate.microsoft.com/>
- **Traitement partagé**
 - Script côté client
 - Liste des versions à jour sur
 - <https://v4.windowsupdate.microsoft.com/getmanifest.asp>
 - <https://v4.windowsupdate.microsoft.com/consumerdrivers/getmanifest.asp>
- **Répertoires de travail**
 - C:\Program Files\WindowsUpdate
 - C:\WUtemp
- **Journaux**
 - Historique des installations IUHIST.XML
 - %SystemRoot%\Windows Update.log
 - Journal global des installations : Setupapi.log

2. Noyau WindowsUpdate (2/2)



EdelWeb

■ Remarques

- **Exploite le service « Uploadmgr »**
 - Effectue des transferts en arrière plan
 - Démarré par SVCHOST => difficile à filtrer
 - Non documenté !
- **N'utilise pas HTTPS (sauf pour la base XML) mais les correctifs sont signés**
- **Même mécanisme pour les fonctions de type « Dynamic Update », « Auto Update »**

- **Adresse IP « en dur » dans le contrôle ActiveX : 207.46.226.17 (inexistante !)**
- **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)”
- **Rappel : ce site ne concerne que les mises à jour Windows / IE (ce qui exclut Office, SQL, Exchange, etc.)**

2. Noyau

Rapport d'erreur (1/2)



EdelWeb

■ Informations incluses (application)

- 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 »

2. Noyau

Rapport d'erreur (2/2)



EdelWeb

- **Informations incluses (noyau)**
 - 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
- **Remarque**
 - Les informations sont transmises au reboot suivant
- **Principes communs**
 - Composant %SystemRoot%\System32\dwwin.exe
 - Site <http://watson.microsoft.com/>
 - Protocoles HTTP et HTTPS
 - Site « Corporate Error Reporting » (<http://oca.microsoft.com/>)
 - Consultation des rapports reçus par Microsoft pendant 180 jours

2. Noyau Authentification Passport



EdelWeb

- **Passport = SSO à l'échelle du Web**
 - Accès aux services Microsoft (MSDN, Beta Previews, etc.)
 - Accès aux « spin-offs » Microsoft : MSN, Hotmail, Messenger ...
 - Accès aux sites partenaires (cf. <http://www.passport.net/>)
- **Principe**
 - **Serveur central d'authentification (base de données utilisateurs)**
 - <http://register.passport.net/>
 - <https://login.passport.com/>
 - <https://nexus.passport.com/> (remarque : « nexus » est un terme utilisé dans Palladium)
 - **Mode d'authentification natif supporté par Windows / IE / IIS / ...**
- **Risques**
 - **Base de données d'informations nominatives partagée entre tous les partenaires**
 - L'utilisateur est censé conserver un niveau de contrôle sur la diffusion de l'information
 - Remplace avantageusement les cookies pour un « tracking » mondial
 - **Vol d'information**
 - Vulnérabilités déjà identifiées
 - Ex. Cookie « PPTProf=... »
- **Concurrence**
 - **Liberty Alliance (<http://www.projectliberty.org/>) – peu avancé**
- **Références**
 - <http://www.tcpdemux.com/products/netintercept/casestudies/passport>
 - **Passport SDK**

2. Noyau Login Web (1/2)



EdelWeb

- **Deux types de login**
 - Natif HTTP (de type « .htaccess »)
 - Login applicatif (formulaire)
- **Natif**
 - **Modes d'authentification supportés par IE 6.0 SP1**
 - 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)
 - **Authentification par défaut**
 - Zone Internet, Sites sensibles : demander le mot de passe
 - Zone Intranet, Sites de confiance : login automatique (avec le login Windows !)
 - **Remarque : même comportement avec le client Telnet**
 - Authentification NTLM par défaut (cf. MS00-067)

2. Noyau Login Web (2/2)



EdelWeb

■ Applicatif

- **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 »**
 - Emplacement : HKCU\Software\Microsoft\Protected Storage System Provider (invisible par défaut)
 - Chiffrés avec le mot de passe de login Windows
 - Récupérables
 - Cf. outil « IE Password Revealer », sites LostPassword, Elcomsoft, etc.

2. Noyau Synchro NTP



EdelWeb

- **Par défaut les postes XP utilisent une synchro horaire**
 - **Machine en domaine**
 - **Serveur par défaut : DC**
 - **Machine en « Workgroup »**
 - **Serveur par défaut : time.windows.com**
 - **Autre serveur : time.nist.gov**
 - **Intervalle par défaut : 1/semaine**
- **Paramétrable**
 - **Clé : HKLM\System\CCS\Services\W32Time**
- **Remarques**
 - **Le protocole NTP standard est utilisé**
 - **Aucune information indésirable n'est transmise**

3. Composants préinstallés Windows Media Player



EdelWeb

- Version livrée avec Windows XP SP1 : 8.0 (non téléchargeable)
- Dernière version (toutes plateformes) : 9.0
- Liste des fonctions accédant à Internet
 - Acquisition de licences (DRM)
 - Accès à des services « en direct » (contenu à la demande, radios)
 - Métadonnées CD et DVD (en lecture/écriture)
 - Téléchargement de codecs
 - Mises à jour logicielles
 - Skins et visualisations
 - « Media Library », « Media Guide », Newsletter MSN, ...
- Risques (majeurs)
 - Superbe outil de marketing personnalisé
 - Le lecteur Windows Media possède un GUID
 - Il s'agit d'un composant ActiveX scriptable par des tiers => notion de « Supercookie »
 - Les skins et visualisations sont des archives ZIP incluant du contenu actif => risque d'infection
 - Etc.
- Sites
 - http://*.windowsmedia.com/

3. Composants préinstallés Internet Explorer (1/2)



EdelWeb

- **Version livrée avec Windows XP SP1 : 6.00.2600.1106**
- **Liste des fonctions accédant à Internet**
 - **Page initiale (=> statistiques d'installation)**
 - <http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome>
 - **Spyware « Alexa » (détecté par Ad-Aware)**
 - En lien avec l'option « effectuer des recherches depuis la barre d'adresses »
 - **« Vérifier les signatures des programmes téléchargés »**
 - **« Vérifier la révocation des certificats »**
 - **« Vérifier la révocation des certificats de l'éditeur »**
 - **« Vérifier automatiquement les mises à jour de IE »**
 - **« Mise à jour des certificats racine » (option Windows)**
 - Si un certificat SSL signé par une autorité inconnue est présenté, une mise à jour de la base des autorités racine est déclenchée
 - Site
<http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt>

3. Composants préinstallés Internet Explorer (2/2)



EdelWeb

■ Autres risques

- **IE est une source privilégiée pour l'installation de Spywares**
 - **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 ...**

3. Composants préinstallés Windows Messenger (1/2)



EdelWeb

- Version livrée avec Windows XP SP1 : 4.7
- Utilise les 3 services suivants
 - Exchange 2000 (si configuré)
 - Serveur SIP (Session Initiation Protocol) – RFC 2543
 - Serveur Microsoft avec authentification Passport
 - <http://messenger.hotmail.com:1863/>
 - POST
<http://gateway.messenger.hotmail.com/gateway/gateway.dll?Action=open&Server=NS&IP=messenger.hotmail.com HTTP/1.1>
- Protocole HTTP encapsulant 2 sous-protocoles
 - XYZ [paramètre 1] [paramètre 2] [...]
 - XYZ = commande
 - Données de type MIME propriétaire
 - Ex. « application/x-msn-messenger », « text/x-msmsgsprofile », ...
 - Partiellement brouillées
- Risques
 - Divulgence d'informations personnelles en clair
 - Système à serveur central
 - Niveau d'information réel inconnu à cause du brouillage des données

3. Composants préinstallés Windows Messenger (2/2)



EdelWeb

■ Exemple

- **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**
- **BDayPre: 2**
- **Birthday: 2.821600e 004**
- **Wallet: 0**
- **Flags: 1027**
- **sid: 507**
- **kv: 4**
- **MSPAAuth:**
4n3lltj1DTLjIKvsjAeFx3NL3kmxyhI5V5207HY!tFCSReUcuFi62d5Z86Fq*6Bea*I5Qsl3lt...
- **ClientIP: 212.xxx.xxx.xxx**
- **ClientPort: 0**

4. Office XP



EdelWeb

■ Contexte

- **Suite fortement intégrée à Windows**
 - Ex. Word devient l'éditeur HTML par défaut
- **Produits fortement intégrés entre eux**
 - Ex. envoyer un document Word avec Outlook modifie les propriétés du document

■ Risques

- **Propriétés du document (auteur, temps d'édition, chemins UNC)**
- **Historique du document (versions antérieures)**
- **« Word bugs »**
- **Macros**
- **Champs de fusion**
- **GUID = adresse MAC**
- **Etc.**

■ Référence

- **MISC n°7 « La fuite d'information dans les documents propriétaires »**

5. Les solutions



EdelWeb

■ Intégrées

- **Tous les composants sont paramétrables (le paramétrage par défaut est souvent insatisfaisant)**
 - Interface graphique
 - Clés de base de registre
 - GPO
 - « Administration Kits »
- **Configuration globale du Proxy**
 - Certains logiciels (ex. Netscape) gèrent des paramètres Proxy personnalisés
- **Désinstallation des composants cachés (fichier SYSOC.INF)**
- **Utiliser la fonction de restriction d'exécution**
- **Mettre en place des miroirs internes (ex. MSUS)**

■ Externes

- **Utiliser un firewall personnel**
- **Utiliser des outils tiers de recherche de configuration « anti-spyware »**

- **Couper tout accès Internet ...**

6. Conclusion



EdelWeb

- **Windows XP SP1 communique régulièrement avec des sites Web**
 - **Ces fonctions sont activées par défaut (mais désactivables)**
 - **Les informations collectées sont individuellement peu significatives**
 - **Mais le recoupement permettrait d'obtenir un puissant outil de marketing personnalisé**
 - **Les informations transmises bénéficient d'un niveau de protection très hétérogène**
 - **HTTP, HTTPS, chiffrement, brouillage, protocole propriétaire, ...**
 - **Il existe des moyens de se protéger**
 - **Le plus simple étant de ne pas configurer l'adresse de son Proxy**

- **Le sujet est loin d'être clos (cf. annexe A)**

- « Using Windows XP Pro SP1 in a Managed Environment : Controlling Communication with the Internet »
 - <http://technet.microsoft.at/includes/file.asp?ID=4668>

- « XP Anti-Spy »
 - <http://www.xp-antispy.de/>

- « Windows XP shows the direction Microsoft is going »
 - <http://www.hevanet.com/peace/microsoft.htm>

Annexe A. Sujets non traités (1/3)



EdelWeb

- « 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>
 - 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)
- 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
- Ports utilisés : 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
 - 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
- MSN Explorer
 - Portail Internet Microsoft



■ Sites 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>

Annexe B. Sites Microsoft (2/2)



EdelWeb

- **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/redirect.asp?ext=AAA>