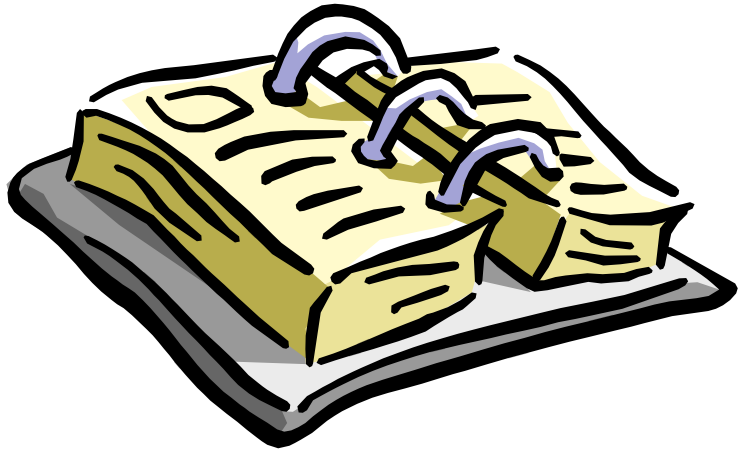
EdelWeb

La fuite d'informations dans Office et Windows

Patrick CHAMBET patrick.chambet@edelweb.fr – http://www.chambet.com
Nicolas RUFF nicolas.ruff@edelweb.fr

Planning

- Objectifs
- Généralités
- Fuite d'informations dans MS Office
- Spyware dans Windows XP/2003
- Recommandations
- Conclusion



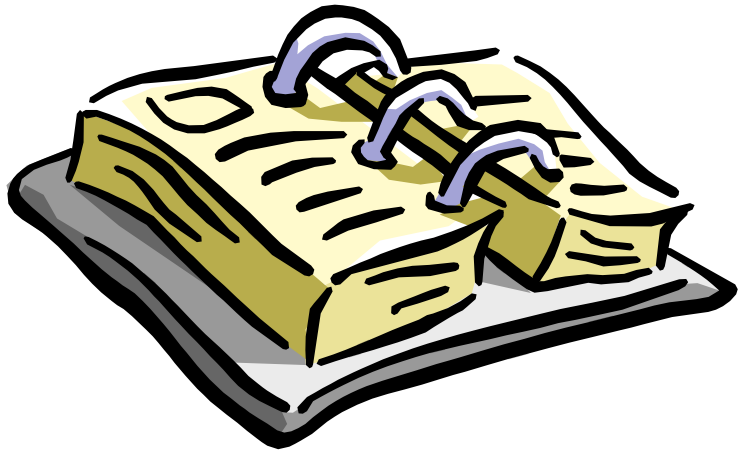
Objectifs

- Présenter certaines caractéristiques importantes des documents propriétaires complexes
- Décrire les faiblesses de certains formats propriétaires
- Décrire les différents spywares présents dans Windows
- Présenter quelques cas concrets de fuites d'informations
- Présenter des recommandations permettant de contrer la fuite d'informations
- Conclure sur la confidentialité du couple Office + Windows

Planning

EdelWeb

- Objectifs
- Généralités
- Fuite d'informations dans MS Office
- Spyware dans Windows XP/2003
- Recommandations
- Conclusion



Généralités (1/2)

- Les formats propriétaires de documents sont de plus en plus complexes
  - Modèle objet élaboré
  - Non documenté
  - Reverse engineering partiel

- Ex: quelques headers Word
  - `DC A5 65 00`
  - `DC A5 68 00`
  - `97 A6 68 00`
  - `EC A5 C1 00`

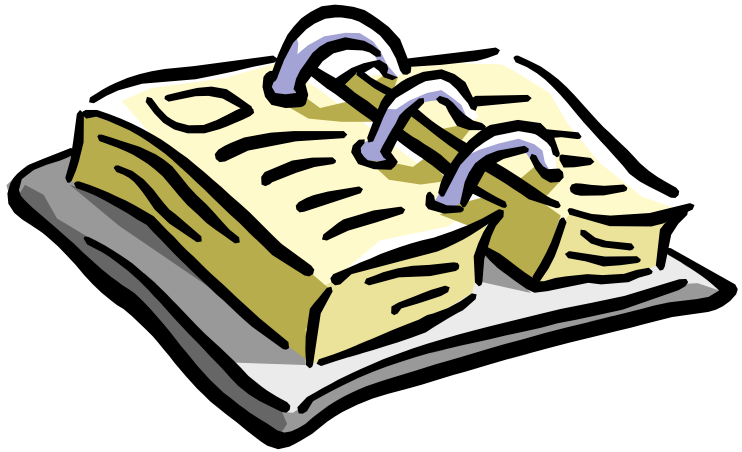
Généralités (2/2)

- La tendance est à l'inclusion et/ou à la récupération d'informations de nature très diverse, à l'insu de l'utilisateur
  - Informations personnelles
  - Informations "marketing"
    - Temps d'utilisation
    - Habitudes d'utilisation
    - Relations avec d'autres documents, applications, ressources réseau (y compris Internet)
    - Sites consultés
    - "Profil commercial" de l'utilisateur
      - Âge
      - Sexe
      - Centres d'intérêt
      - Coordonnées (email -> spam)

Planning

EdelWeb

- Objectifs
- Généralités
- ✓ Fuite d'informations dans MS Office
- Spyware dans Windows XP/2003
- Recommandations
- Conclusion



Microsoft Word (1/5)

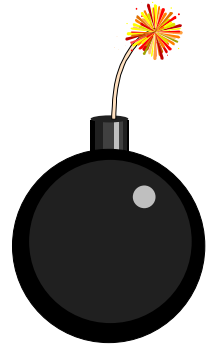
- **Informations lisibles directement dans les propriétés du document**
  - **Nom de l'auteur**
  - **Entreprise de l'auteur**
  - **Date et heure de création**
  - **Temps passé à l'édition**
  - **Heure d'impression**
  - **Etc…**

- **Si un document de 100 pages a un temps d'édition de 5 minutes, c'est qu'il provient d'un copier-coller !**
- **Attention au mode de suivi des modifications: accès aux versions antérieures !**
  - **Exemple: affaire Alcatel**

Microsoft Word (2/5)

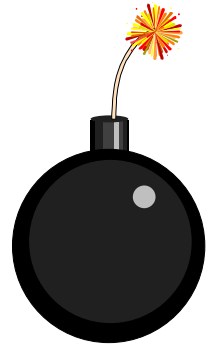
- Ouverture du document avec un éditeur hexa
  - Nom des rédacteurs successifs
    - Cf outils (« Analyse doc Word », « OfficeAnalyzer »)
  - Nom de la machine
  - Chemin complet du document sur les disques des rédacteurs successifs
    `C:\Documents and Settings\Stagiaire Dupont\Confidentiel\Clients mauvais payeurs\Contrat.doc`
  - Chemin complet du modèle de document
    `\\SRV_FICH\PUBLIC\MODELES-WORD\Document Générique GIE.dot`

    => On en déduit le nom du serveur de fichiers de l'entreprise



Microsoft Word (3/5)

- Serveurs d'impression et imprimantes
  `\\SRV_PDC\HPPCL5MS LaserJet 4 Plus`
  => On en déduit le nom du PDC du domaine



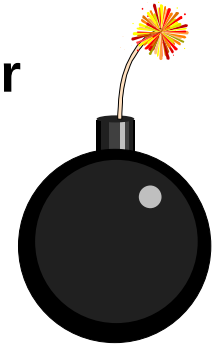
- Nom et chemin des fichiers inclus dans le document
  - Ex: fichiers images

- GUID (Global Unique Identifier)
  - Chercher après « _PID_GUID » :
    `{F165CB92-D166-12D5-AB67-0010A41432AF}`
  - Les 12 derniers chiffres sont l'adresse MAC de la carte réseau !
  - Présent dans les documents Office mais aussi Visual C++, les ActiveX, etc...

Microsoft Word (4/5)

- **Inclusion d'informations du disque local**
  - **La directive INCLUDETEXT peut être utilisée pour inclure automatiquement le contenu d'un document du disque dur dans le document courant**

```
{ IF { INCLUDETEXT { IF { DATE } = { DATE }
"C:\\confidentiel.txt" "C:\\confidentiel.txt"
} \* MERGEFORMAT } = "" "" \* MERGEFORMAT }
```



- **Autres inclusions**
  - **Observation d'inclusions curieuses (mémoire ? presse-papier ?)**
- **Office 2003**
  - **Cliparts en ligne**
  - **Aide en ligne**
  - **Gestion des droits numériques en ligne (IRM, futur RMS)**

Microsoft Word (5/5)

EdelWeb

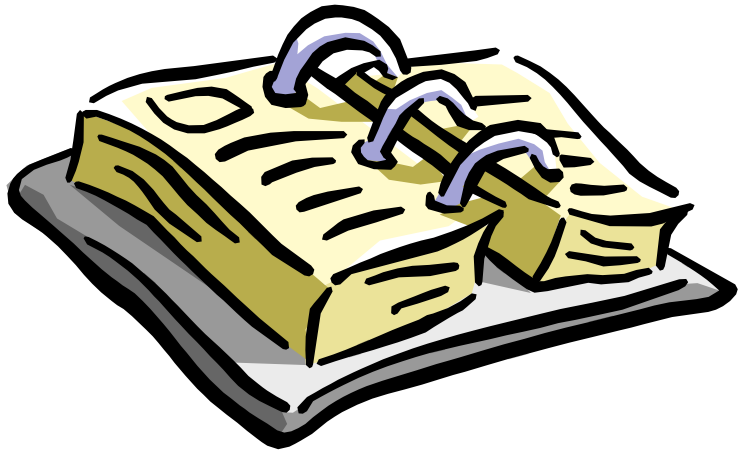
- **Les « Word bugs »**

- **Permettent à *l'auteur* de recueillir de l'information sur les *lecteurs* des documents (processus inverse)**
  - **Moment de la lecture**
  - **Lieu de la lecture (adresse IP)**
  - **Informations diverses sur l'identité et sur l'environnement du lecteur (logiciel utilisé, langue, etc...) et sur son type de connexion Internet**

Planning

EdelWeb

- Objectifs
- Généralités
- Fuite d'informations dans MS Office
- ✓ Spyware dans Windows XP/2003
- Recommandations
- Conclusion



Le spyware dans Windows (1/4)

- Le contexte général
  - 2002 : 56 types de Spyware, 125 sites (source : Eric Howes)
  - 2003 : 493 types, 1317 sites

  - Projets américains (ex. "Magic Lantern")
  - Virus contenant des spywares comme charge finale (spammeurs)
  - Protections logicielles douteuses (ex. "Surcode DVD-DTS Pro")
  - Lois françaises autorisant une surveillance accrue des internautes (LSQ, LCEN, …)

- Le contexte Microsoft
  - Bugs IE permettant l'installation automatique de spywares
  - Alertes très médiatisées (ex. "supercookie" Windows Media)
  - "Product Activation" requis à partir de Windows XP / Office XP
  - Initiative TCPA / Palladium / NGSCB
- => Microsoft fait peur

Le spyware dans Windows (2/4)

- Activation du produit
  - Ne pas confondre activation et enregistrement du produit
  - Valeur de hachage générée à partir des éléments suivants
    - 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
  - "Product Key" vérifiable par rapport à une clé publique "en dur"
  - f("Product Key") + "Public Key Index" + aléa = "Product ID"

Le spyware dans Windows (3/4)

- Intégration de plus en plus forte d'Internet dans les produits
  - Explorer
    - Mise à jour automatique des raccourcis et des "favoris réseau"
    - Assistant recherche
      - Charge du contenu actif depuis http://ie.search.msn.com/
      - Conservation des logs par Microsoft : 1 an
      - Affiche des bandeaux de pub
    - Montage de lecteurs WebDAV
    - Fonction "cette copie de Windows est-elle légale ?"
    - Remarque : Explorer souffre de nombreux failles de conception + utilise le moteur IE (MSHTML.DLL)
  - Aide
    - Se met à jour automatiquement depuis le MSDN
    - Assistance à distance depuis le support Microsoft
      - Compte SUPPORT_388945a0
      - Site https://webresponse.one.microsoft.com/
      - D'autres comptes peuvent être ajoutés par les OEM

Le spyware dans Windows (4/4)

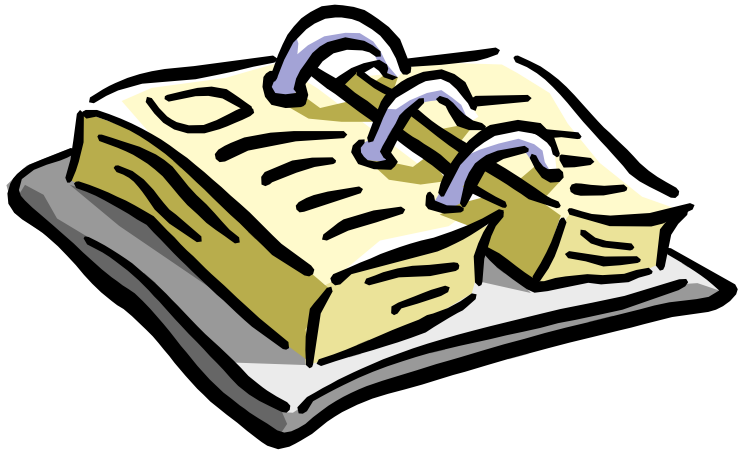
- **Passport**
  - **Indispensable sur de nombreux sites Microsoft aujourd'hui**
  - **Permet un "tracking" mondial**
  - **Sécurité souvent remise en cause (solution basée sur un cookie)**

- **Autres sujets d'(inqui)étude**
  - **Rapport d'erreur**
  - **WindowsUpdate**
  - **Windows Media Player (ex. skins = fichiers ZIP contenant du code actif)**
  - **MSN Messenger**
  - **Etc.**

Planning

EdelWeb

- Objectifs
- Généralités
- Fuite d'informations dans MS Office
- Spyware dans Windows XP/2003
- Recommandations
- Conclusion



Recommandations (1/4)

- **Solutions**
  - **Quasiment toutes les options dangereuses sont désactivables dans la base de registre**
    - **Mais elles sont toutes activées par défaut**
  - **Tous les logiciels intégrés à Windows partagent la configuration du Proxy**
    - **Mettre une configuration nulle (127.0.0.1 : 80)**
    - **Utiliser des logiciels dont le proxy est configurable (ex. Mozilla)**
  - **Utiliser un Firewall personnel**

- **Autres "astuces"**
  - **Outil "XP AntiSpy"**
  - **Désinstaller les composants inutiles (cf. SYSOC.INF)**
  - **Utiliser la restriction d'exécution (Windows XP)**
  - **Utiliser des miroirs internes (ex. MSUS)**

Recommandations (2/4)

- **Ne pas diffuser un document ayant été retouché**
- **Recréer les documents ex nihilo avant diffusion publique**

  ⇒ ***TRES CONTRAIGNANT !***

- **Opter pour un traitement de texte libre et en partie compatible avec les leaders du marché**
  - **StarOffice**
  - **OpenOffice (gratuit)**

- **Utiliser un firewall personnel pour interdire certaines applications d'accéder à Internet**

Recommandations (3/4)

- **Dans MS Word**
  - **Désactiver l'enregistrement rapide**
  - **Désactiver le suivi des modifications**
  - **Désactiver toutes les macros (y compris signées)**
  - **Configurer les fichiers modèles (.dot) en "lecture seule"**

- **Depuis Office XP/2002**
  - **Cocher « Supprimer les informations personnelles de ce document lors de la sauvegarde »**
  - **Cocher « Avertir avant d'imprimer, de sauvegarder ou d'envoyer un fichier qui contient du suivi de modifications ou des commentaires»**

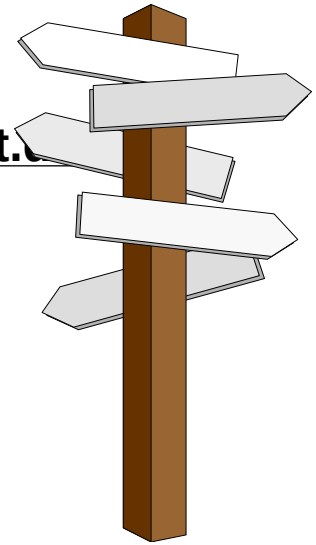
Recommandations (4/4)

- **Signature numérique**
  - **Ne pas signer un document potentiellement dynamique: DOC, XLS, …**
  - **Préférer pour la signature des documents à la structure moins riche: RTF, …**
  - **Etudier avec prudence les formats que vous ne connaissez pas avant d'accepter de les signer ou d'en accepter la signature**
- **Sensibiliser les utilisateurs**
- **Il est recommandé d'inclure la problématique des documents complexes dans les politiques de sécurité**

Conclusion

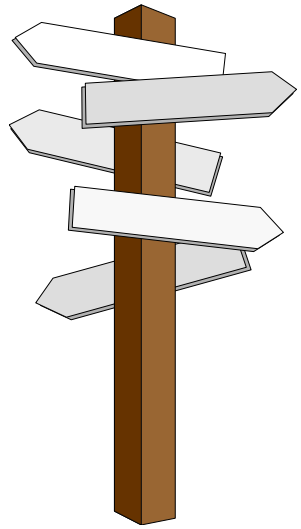
- La tendance n’est pas à la simplification des formats propriétaires (malgré le succès mitigé de XML)
- Les spywares et le recueil de données marketing ont de beaux jours devant eux
- Les cas évoqués sont graves car ils se produisent aussi dans des environnements sensibles (entreprises, administrations)
- Toute organisation doit donc considérer la gestion de la fuite d’informations en fonction du degré de confidentialité de ses informations
- Il est recommandé d’inclure cette problématique dans les politiques de sécurité

Pour aller plus loin… (1/2)



- Affaire Alcatel
  - http://www.landfield.com/isn/mail-archive/2001/Apr/0096.html
  - Document Alcatel: http://web.morons.org/external/CPE_statement.
- Fichiers d'exemples
  - http://www-rocq.inria.fr/codes/Eric.Filiol/SSI/AdobeTestFile.pdf
  - http://www-rocq.inria.fr/codes/Eric.Filiol/SSI/misc7_word.zip
- Windows
  - Activation
    - http://www.licenturion.com/xp/
  - Using Windows XP Pro SP1 in a Managed Environment : Controlling Communication with the Internet
    - http://technet.microsoft.at/includes/file.asp?ID=4668
  - XP Antispy
    - http://www.xp-antispy.de/

Pour aller plus loin… (2/2)



- **TCPA**
  - **http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html**
  - **En Français: http://www.lebars.org/sec/tcpa-faq.fr.html**

- ***MISC* (premier journal technique français sur la sécurité des SI)**

  - **http://www.miscmag.com**

Questions

EdelWeb