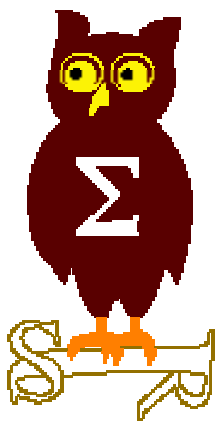
OSSIR
Groupe Sécurité Windows

Réunion du 13 février 2006



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/3)

- (Avis de sécurité Microsoft depuis le 9 janvier 2006)

- Janvier 2006
  - MS06-001 Patch WMF
    - Affecte : toutes les versions de Windows depuis 3.0
    - Exploit : ouverture d'un fichier image corrompu
    - Bulletins sorti "hors cycle"

  - MS06-002 "Heap overflow" dans le décodage des polices EOT
    - Affecte : toutes les versions de Windows supportées
      - Composant T2EMBED.DLL
    - Exploit : une police de type EOT (Embedded Open Type) sérialisée dans un mail, une page Web, …
    - Crédit : eEye

Dernières vulnérabilités
Avis Microsoft (2/3)

- MS06-003 "Buffer overflow" dans le support TNEF
  - Affecte : Outlook 2000/XP/2003, Exchange 5.5/2000
  - Exploit : une commande TNEF (Transport Neutral Encapsulation Format) passée dans un mail
    - La fameuse pièce jointe "winmail.dat"
  - Crédit : John Heasman et Mark Litchfield

Février 2006

- Windows Media Player : 1 bulletin "important"
- Windows : 4 bulletins allant jusqu'à "critique"
- Windows+Office : 1 bulletin "important"
- Office : 1 bulletin "important"

Dernières vulnérabilités
Avis Microsoft (3/3)

- **Advisories**
  - **Q904420**
    - **"BlackWorm", appelé Mywife.E par Microsoft**
  - **Q914457**
    - **Elévation de privilèges locale via des permissions trop laxistes**
    - **(cf. ci-après)**
  - **Q913333**
    - **Nouvelle faille WMF (Heap Overflow)**
    - **Affecte : IE versions antérieures à IE6 SP1**

- **Révisions**
  - **MS05-054 Patch cumulatif sur IE**
    - **Version 1.1 Ajout d'une référence au "Kill Bit"**

Dernières vulnérabilités
Infos Microsoft (1/5)

- Microsoft va vendre des licences d'accès au code source Windows
  - http://www.zdnet.fr/actualites/informatique/0,39040745,39305718,00.htm
- Rappel : les protocoles propriétaires Microsoft sont déjà en vente
  - Microsoft Communications Protocol Program (MCPP)
  - http://members.microsoft.com/consent/Info/default.aspx
  - Exemples gratuits :
    - Tickets Kerberos
    - CIFS
- Windows XP et Windows 2003 obtiennent la certification EAL 4+
    - http://www.fcw.com/article91728-12-14-05-Web
    - http://appserv.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcndaily2&story.id=37775
  - Le profil de protection :
    - http://niap.nist.gov/cc-scheme/pp/PP_CAPP_V1.d.pdf

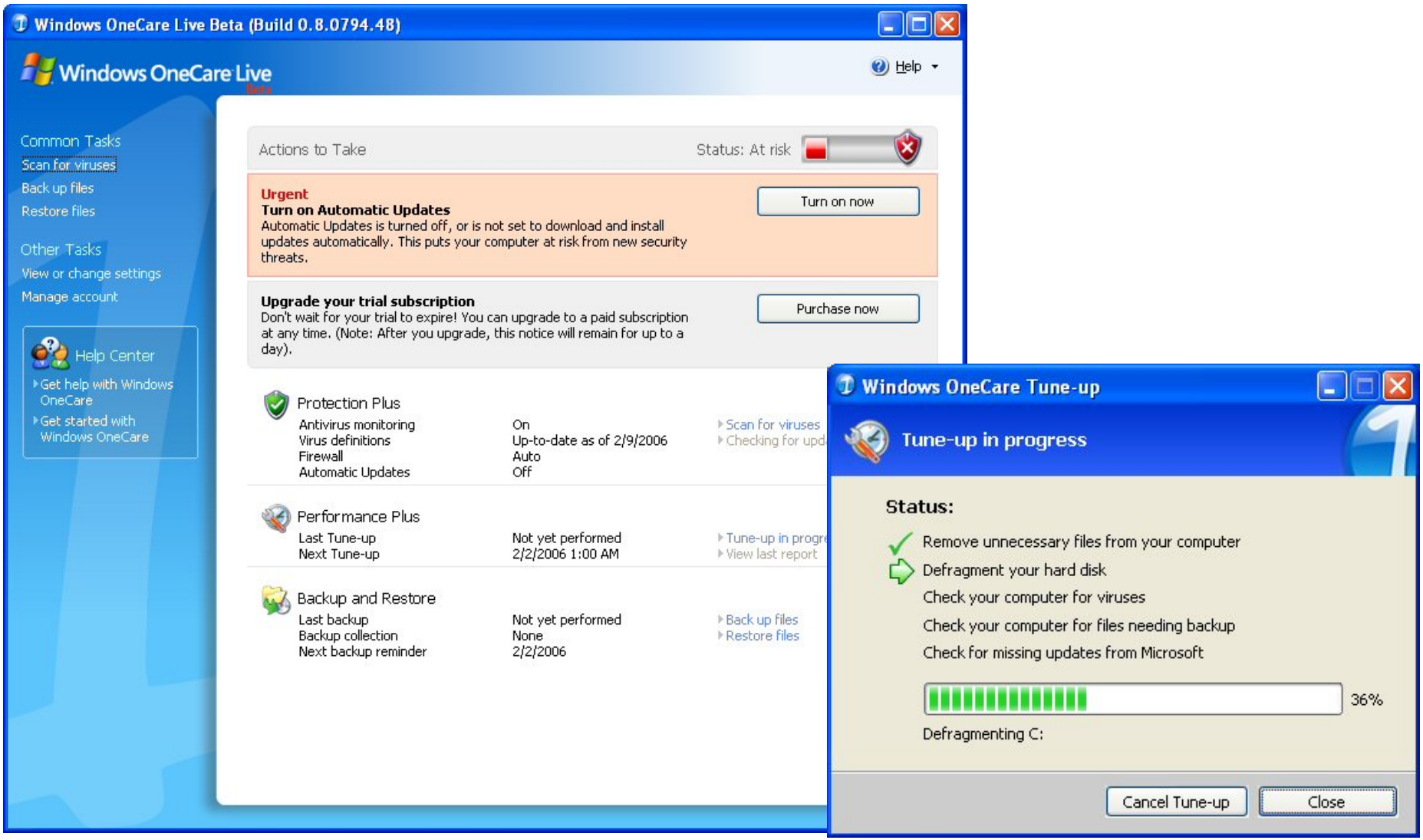
Dernières vulnérabilités
Infos Microsoft (2/5)

- **Le firewall Vista bloque aussi les connexions sortantes**
  - **http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5246**
- **Microsoft ferme un blog sur MSN à la demande du gouvernement Chinois**
  - **Contenait les mots interdits "democracy" et "human rights"**
  - **http://www.nytimes.com/2006/01/06/technology/06blog.html**
- **Microsoft contraint à supprimer une fonction d'Office suite à un procès**
  - **Fonction de liaison de données Access -> Excel (!)**
  - **Procès Amado vs. Microsoft**
    - **http://www.msd.uga.edu/announcement.php?news_item_id=1050**
  - **La fonction sera enlevée dans Office 2003 SP2**
    - **http://support.microsoft.com/default.aspx/kb/904953/**

Dernières vulnérabilités
Infos Microsoft (3/5)

- Il est possible d'obtenir les correctifs mensuels Microsoft sur une image ISO
  - http://support.microsoft.com/kb/913086
- Windows 2003 R2 version finale
  - http://www.microsoft.com/windowsserver2003/default.mspx
- Windows XP SP3 prévu pour … mi-2007 !
  - http://www.microsoft.com/windows/lifecycle/servicepacks.mspx
- IE 7 Beta2 pour Windows XP SP2
  - http://www.microsoft.com/windows/ie/ie7/default.mspx
- Windows OneCare Beta
  - Inclus un antivirus …
- Disponibilité du "COM+ Hotfix Rollup 35" pour Windows 2000 (Q910370)
  - Corrige 5 nouveaux bogues dont 4 non documentés

Dernières vulnérabilités
Infos Microsoft (4/5)



Dernières vulnérabilités
Infos Microsoft (5/5)

- KMDF (Kernel Mode Driver Framework) disponible
  - Nouveau modèle de drivers pour Vista
  - http://www.osronline.com/article.cfm?article=430
- Seuls les drivers signés autorisés sur Vista 64 ?
  - http://www.osronline.com/article.cfm?article=435

Dernières vulnérabilités
Autres avis (1/7) - failles

- **Failles WiFi dans Windows**
  - Connues depuis 1 an mais forte publicité autour de la ShmooCon
  - Plusieurs types de failles
    - Windows recherche tous les réseaux favoris antérieurs
    - Windows crée automatiquement le premier nœud d'un réseau ad-hoc (si dans les favoris)
    - Entre chaque intervalle de recherche, Windows annonce un SSID aléatoire et se reconnecte automatiquement s'il existe (!)
    - Certains drivers acceptent le fallback en clair même sur des réseaux WEP

- **Encore des failles Oracle critiques**
  - 82 failles critiques
    - http://www.computerworld.com/securitytopics/security/story/0,10801,107825,00.html?source=x10
    - Certaines connues depuis plus de 3 ans
  - Crédit :
    - http://www.red-database-security.com/advisory/published_alerts.html

Dernières vulnérabilités
Autres avis (2/7) - failles

- Tous les produits Avaya basés sur Windows sont vulnérables au bogue WMF
  - http://news.yahoo.com/s/zd/20060109/tc_zd/168834
- "0day" Winamp publié sur une "mailing list"
  - Mettre à jour en version 5.13
  - http://isc.sans.org/diary.php?storyid=1080
- "0day" dans Microsoft Help Workshop
  - Risque très faible : il faut ouvrir le ".hhp" dans Help Workshop pour être infecté
- Pluie de failles dans Mozilla/FireFox
  - 8 failles patchées dans FireFox 1.5.0.1
    - http://www.mozilla.org/security/announce/mfsa2006-[01|08].html
  - Et une faille non patchée
    - https://bugzilla.mozilla.org/show_bug.cgi?id=324253
    - La propriété "-moz-binding" permet d'exécuter des scripts et/ou d'accéder aux cookies

Dernières vulnérabilités
Autres avis (3/7) - failles

- Attaque WinVal
  - Framework d'audit des permissions en PROLOG ☺
  - Résultat : les services SSDP et UPnP peuvent être configurés (SC_CHANGE_CONFIG) par un utilisateur non privilégié
  - L'attaque est triviale
    - sc config weakService binPath=c:\attack.exe obj=".\LocalSystem" password=""
    - sc stop weakService
    - sc start weakService
  - http://www.cs.princeton.edu/~sudhakar/papers/winval.pdf
  - Alerte Microsoft Q914457
- Nombreuses failles trouvées dans les implémentations BlueTooth en fuzzing
  - http://www.secuobs.com/news/05022006-bluetooth10.shtml
  - Crédit : Pierre Betouin

Dernières vulnérabilités
Autres avis (4/7) – virus et spywares

- Le "BlackWorm"
  - Aucun intérêt technique
    - Appli Visual Basic se propageant par mail
    - Se propage également via les partages réseau et la commande AT
  - Payload dangereux : destruction de fichiers tous les 3 du mois
  - Plus de 1 million de personnes infectées

- La société Frame4 met en ligne une base de données de souches virales
  - Payante pour les codes les plus récents
  - http://www.frame4.net/mdpro/

- AntiSpyware Coalition
  - http://www.antispywarecoalition.org/

- Symantec utilise des techniques de "rootkit" pour sa corbeille protégée
  - Fonction qui peut être abusée par des virus
  - http://www.eweek.com/article2/0,1895,1910077,00.asp

Dernières vulnérabilités
Autres avis (5/7) – virus et spywares

- **Un nouveau type de ver : le blogworm ☺**
  - **http://www.moox.nl/blogworm/**
  - **http://news.com.com/2061-10789_3-6031795.html**

Dernières vulnérabilités
Autres avis (6/7)

- Une analyse intéressante des délais de patch
  - http://blogs.washingtonpost.com/securityfix/2006/01/a_timeline_of_m.html
- Recrudescence des attaques en extraction d'annuaire SMTP
  - Etude de la société Tumbleweed
  - http://www.secuobs.com/news/20012006-annuaires.shtml
- Le retour du brevet logiciel en Europe ?
  - http://www.secuobs.com/news/20012006-brevet.shtml
- Des chiffres sur l'utilisation de FireFox le dimanche
  - Date : mars 2005
  - Résultats :
    - Allemagne 21%
    - France 12%
    - UK 11%
  - http://www.xitimonitor.com/etudes/equipement4.asp

Dernières vulnérabilités
Autres avis (7/7)

- L'indexation des métadonnées Office dans Windows Vista pose des problèmes à Gartner
  - http://www.computerworld.com/printthis/2005/0,4814,107338,00.html
  - http://www.eweek.com/print_article2/0,1217,a=168055,00.asp
  - http://news.com.com/2102-1012_3-6006290.html?tag=st.util.print

- La plus grosses condamnation pour spam au monde
  - Robert Kramer vs. James McCalla (spammer basé en Floride)
  - Condamné à 11,2 milliard de dollars de dommages et intérêts
  - http://www.computerworld.com/printthis/2006/0,4814,107598,00.html
  - http://www.wired.com/news/politics/1,69966-0.html

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **13 mars 2006**
- **N'hésitez pas à proposer des sujets et des salles**