OSSIR
Groupe Sécurité Windows

Les nouveautés du SP2

Nicolas RUFF

nicolas.ruff@edelweb.fr

Plan

EdelWeb

- Introduction
- Présentation des nouveautés
  - Liste globale
  - COM / DCOM
  - RPC
  - WebDAV
  - ICF
  - IE
  - Windows Update / Microsoft Update
  - Windows Installer 3.0
- Conclusion
- Bibliographie

Introduction

EdelWeb

- **Windows XP SP2 RC1**
  - Rendu public le 19 mars 2004
  - Sortie prévue cet été
- **Introduit des changements considérables**
  - "Change to Functionnality" White Paper : 156 pages …
  - Fort impact sur les applications à prévoir
- **Très médiatisé**
  - Nombreux White Papers et conférences Microsoft sur le sujet
  - Bill Gates se déplace en personne à la conférence "RSA Security"
    - http://www.microsoft.com/billgates/speeches/2004/02-24rsa.asp

Nouveautés
Liste (1/3)

EdelWeb

- Liste des nouveautés (* = décrite ci-après)
  - Protection réseau
    - Services "Alerter" et "Messenger" désactivés par défaut
    - Support Bluetooth natif
    - Ajout des fonctions "rechercher …" et "sélectionner des utilisateurs, des ordinateurs ou des groupes" aux outils d'administration
    - Restrictions COM / DCOM [*]
    - Restrictions RPC [*]
    - Redirecteur WebDAV [*]
    - ICF [*]
  - Windows Media Player
    - Installation obligatoire de Media Player 9
  - Windows Messenger
    - Blocage des fichiers "dangereux" envoyés par des inconnus
    - Nickname obligatoirement différent de l'adresse email

Nouveautés
Liste (2/3)

EdelWeb

- Wireless Provisioning Service
  - Envoi de paramètres de configuration par les hotspots …
  - Le Wireless Network Registration Wizard permet de donner son numéro de carte bleue aux opérateurs WiFi OEM …
- Support du flag NX
  - Processeurs AMD64 et Itanium uniquement
  - Désactivable dans le panneau de configuration (globalement ou par application)
- Outlook Express
  - Lecture en texte par défaut (rendu RTF au lieu de HTML)
  - Pas de téléchargement du contenu HTML externe
  - "Sandbox" d'exécution des pièces jointes
    - API AES ("Attachment Execution Service") [*]
- Internet Explorer [*]

Nouveautés
Liste (3/3)

EdelWeb

- Maintenance
  - Le menu ajout/suppression de programme est trié
    - Correctifs de sécurité listés à part
  - Client "WindowsUpdate" / "MicrosoftUpdate" [*]
  - Calcul du RSoP
  - "Security Center" (Centre de Sécurité)
    - Alerte l'utilisateur sur les fonctions de sécurité suivantes : antivirus, firewall, mises à jour
  - Windows Installer 3.0 [*]

- Détection des programmes antivirus installés
  - Participation de Microsoft à la Virus Information Alliance
    - http://www.microsoft.com/technet/security/topics/virus/via.mspx
  - Quels éditeurs seront reconnus ?

- Recompilation de tous les fichiers système avec /GS

Nouveautés
COM / DCOM

EdelWeb

- COM
  - Séparation des contrôles d'accès entre l'invocation locale et l'invocation distante
    - Launch / Activate / Call font maintenant la différence entre les accès locaux (LPC) et distants (RPC)

- DCOM
  - Contrôle d'accès global aux interfaces
    - Évite l'utilisation (fastidieuse) de DCOMCNFG sur chaque composant
  - L'activation anonyme à distance n'est plus possible par défaut
  - Options de journalisation des erreurs
  - Clés HKLM\Software\Microsoft\Ole\...
    - MachineAccessRestriction
    - MachineLaunchRestriction
    - ActivationFailureLoggingLevel
    - CallFailureLoggingLevel
    - InvalidSecurityDescriptorLoggingLevel

Nouveautés
RPC / WebDAV

EdelWeb

- **RPC**
  - **Clé RestrictRemoteClients**
    - **Permet de limiter les connexions anonymes aux serveurs RPC**
    - **Ne s'applique pas aux connexions via des tubes nommés (ncacn_np)**
  - **Clé EnableAuthEpResolution**
    - **L'accès au "end-point mapper" ne peut plus s'effectuer de manière anonyme**
    - **Désactivé par défaut**

- **Redirecteur WebDAV**
  - **Rappel : DAVRdr est utilisé pour accéder aux partages réseau via HTTP**
  - **Authentification basique désactivée sur HTTP**
    - **Clé UseBasicAuth**
    - **Requière HTTPS**
  - **Possibilité de désactivation globale de l'authentification basique au niveau WinINet !**
    - **Clé DisableBasicOverClearChannel**

Nouveautés ICF (1/3)

EdelWeb

- Évolution majeure
- Concurrence des produits commerciaux ?
  - Principale limite : le logiciel ne filtre pas les connexions sortantes

- Principales nouveautés
  - Activé par défaut sur toutes les interfaces
    - Bloque toutes les connexions entrantes en IPv4 *et IPv6*
    - Impacts : l'administration distante et l'accès aux partages est impossible
  - Politique de blocage par défaut au boot
    - Avant le lancement du service ICF
    - Autorise DNS, DHCP et communications avec le DC
  - Configuration
    - Configuration globale de ICF (pour toutes les interfaces)
    - Configuration via NETSH (ligne de commande) ou par GPO
  - Possibilité de définir les adresses du sous-réseau local
    - Ouvre UDP/137, UDP/138, TCP/139, TCP/445 (SMB)
    - Ouvre UDP/1900, TCP/2869 (UPnP)
    - Autorise le partage de fichiers et d'imprimantes sur ce sous-réseau

Nouveautés ICF (2/3)

EdelWeb

- "White list" des applications autorisées à écouter sur des ports
  - Les applications "SP2-aware" peuvent se déclarer elles-mêmes ou autoriser dynamiquement des ports
    - Requière les privilèges Administrateur
    - SVCHOST ne peut pas s'autoriser ☺
  - APIs
    - INetFwAuthorizedApplication
    - INetFwOpenPort
    - INetFwProfile
  - Traitement des autorisations
    - Le processus doit s'exécuter sous le compte LocalSystem, LocalService ou NetworkService pour accéder à l'API
    - Pour les processus exécutés sous des comptes utilisateur, la "White List" est utilisée
  - Remarque : pas de filtrage des connexions sortantes
    - Mais suivi des connexions TCP
    - Pour les connexions UDP, le délai de réponse est de 90 secondes (paramétrable)
  - Traitement spécial des RPC
    - Clé PrivilegedRpcServerPermission

Nouveautés ICF (3/3)

EdelWeb

- Mode "panique" ou "client only"
  - Bloque toutes les connexions entrantes
- Doubles stratégies pour les nomades (maison, bureau)
  - Ne s'applique pas aux machines en Workgroup
- Option "restore default settings"
- Configuration à l'installation (même "unattended")
- Support du multicast et du broadcast
  - Attente d'une réponse pendant 3 secondes (paramétrable)

Nouveautés IE (1/3)

EdelWeb

- **Affichage des fichiers téléchargés et des pièces jointes plus clair**
  - Affiche également l'auteur et les signatures éventuelles
  - "Sandbox" (utilisation de l'API "AES")
  - Indicateur de texte masqué
- **API "AES" (Attachment Execution Service)**
  - Point d'entrée unique ("hook") pour le filtrage des pièces jointes Outlook / MSN / IE
- **Gestion des suppléments dans IE**
  - Affiche l'auteur et les signatures éventuelles
  - Il est facile d'obtenir la liste des suppléments installés (lutte contre le Spyware)
  - Fonctionnement en "white list" ou "black list"
  - Les suppléments provoquant des erreurs sont désactivés
- **A propos de la signature de code …**
  - Possibilité de "black lister" des autorités de certification
  - Blocage automatique des exécutables avec signature invalide

Nouveautés IE (2/3)

EdelWeb

- Gestion des "Binary Behaviors"
  - BB = extensions de rendu HTML en code machine
  - Peuvent être désactivés dans la "Restricted Zone"
- Une seule popup de blocage des ActiveX
  - Confirmation par page et plus par contrôle
- Modification des drapeaux "safe for scripting" et "safe for initialization"
  - Appliqués dans toutes les zones
  - Appliqués aux objets initialisés depuis un site tiers (<OBJECT CODEBASE=...>)
- "Information Bar"
  - Remplace les popups multiples
  - Contrôle les add-ons, les téléchargements, les ActiveX bloqués, les pop-ups bloquées
- Blocage des popups
  - window.open()
  - window.external.navigateAndFind()
  - showHelp()

Nouveautés IE (3/3)

EdelWeb

- Nouvelles "Feature Control" (= options de sécurité)
  - "MIME sniffing" = reconnaissance par signature et pas par extension (+ contrôles additionnels)
  - Pas d'exécution dans un contexte plus privilégié que l'URL de base
  - Création et déplacement des fenêtres par script limités
  - Contrôlable par GPO
- Verrouillage de la zone "poste de travail"
  - Cf. outil QwikFix
  - Affecte les ".mht" mais pas les ".hta"
  - L'entête dit "Mark of the Web" permet de retrouver la fonctionnalité classique
    - <!-- saved from url=(0013)about:internet -->
- JVM
  - Possibilité de désactiver simplement la JVM Microsoft
  - JVM désactivée dans la Restricted Zone
- Protection du cache et du contexte de sécurité
  - Pas d'accès aux objets entre les domaines
  - Les objets externes doivent être ré-instanciés dans les scripts avant utilisation

Nouveautés
Microsoft Update / Windows Installer

EdelWeb

- **Client compatible Windows Update / Microsoft Update**
  - Intègre Office, SQL, Exchange et les drivers
  - Catégorisation personnalisable des mises à jour
  - Priorités de téléchargement (correctifs critiques en premier)
  - Installations beaucoup plus silencieuses (y compris les mises à jour du client de mise à jour)
  - BITS 2.0
  - API scriptable
  - Administration des correctifs par GPO
- **Windows Installer 3.0**
  - Support des patches
  - Support des patches différentiels (sans accès au fichier source d'origine)
  - Accès aux sources d'installation
  - Séquencement des installations
  - Plus d'accès via FTP et GOPHER
  - Le service (SYSTEM) WindowsInstaller n'est plus interactif

Conclusion (1/2)

EdelWeb

- Gros effort d'amélioration de la sécurité Windows
  - En local : protection proactive contre les bogues IE et Outlook
    - Ex. immunité native au bogue IE non patché "ms-its"
  - En réseau : tous les ports fermés par défaut
    - Pas d'exception dans l'installation par défaut sauf "Remote Assistance"
- Les critiques lues dans la presse
  - Ajout de fonctionnalités = ajout de failles ?
  - Pas de changements fondamentaux dans l'architecture Windows
  - Fonctionnement en mode "pompier"
    - Protection contre les failles exploitées, pas contre les failles exploitables
  - Très orienté "home users"
  - Concurrence des produits commerciaux
- Mes observations personnelles
  - Franchement très efficace
  - Mais gain nul si l'impact sur les applications est trop fort
    - Toutes les fonctions de sécurité seront désactivées manuellement ou par les éditeurs d'applications
  - Les failles viendront de l'usage (ouverture de ports, désactivation des sécurités)
  - Taille du Service Pack = 300 Mo … (risque de rater la cible "home users")

Conclusion (2/2)

EdelWeb

- **Recommandations**
  - Faire des tests de compatibilité exhaustifs
  - En domaine, prévoir de laisser au moins le port 445 ouvert après installation
  - Ne pas désactiver toutes les fonctions de sécurité
    - Identifier les fonctions incompatibles avec l'existant
    - Utiliser les nouvelles GPO pour les désactiver provisoirement
  - Prévoir obligatoirement de pouvoir désinstaller le SP2

- **Autres pistes de recherche pour Microsoft**
  - Visual Studio "Whidbey" : favorise le développement d'applications non administrateur
  - Outils d'analyse de code source PREfast / PREfix
  - Ouverture de plus en plus large du code source aux gouvernements
  - Certifications et re-certifications CC (imposées par le gouvernement américain)

Bibliographie

EdelWeb

- Preview
  - http://www.microsoft.com/sp2preview
- Documentation officielle
  - http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.mspx
  - Deploying Internet Connection Firewall Settings for Microsoft® Windows® XP with Service Pack 2
    - http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=en
  - Windows XP Service Pack 2 White Paper Overview
    - http://download.microsoft.com/download/6/6/c/66c20c86-dcbe-4dde-bbf2-ab1fe9130a97/windows%20xp%20sp%202%20white%20paper.doc
- Analyses tierces
  - Paul Thurrott
    - http://www.winsupersite.com/reviews/windowsxp_sp2_preview2.asp
  - Steve Friedl
    - http://www.unixwiz.net/techtips/xp-sp2.html