SSTIC 2004

Quel avenir pour la sécurité Windows ?

Nicolas RUFF

EdelWeb / Groupe ON-X

nicolas.ruff@edelweb.fr

Ordre du jour

- **Un peu d'histoire**
  - Lorsque la sécurité n'existait pas ...
  - "Microsoft Security Initiative"
  - "Get Secure, Stay Secure"
  - "La défense périmétrique"
- **Les nouveautés majeures**
  - Windows XP/2003 : les révolutions silencieuses
  - Windows XP : les nouveautés du SP2
- **Vers une informatique de confiance ?**
  - Prochaines pistes de recherche
  - Sécurisation de l'environnement
  - Sécurité matérielle
- **Les nouveaux risques**
- **Conclusion**

1. Un peu d'histoire …

1. Un peu d'histoire
Lorsque la sécurité n'existait pas …

- **29 juillet 1996 : sortie de Windows NT4**
  - Croissance rapide des problèmes documentés (ou non)
  - Premiers codes d'exploitation publics ("Red Button", L0phtCrack, etc.)
- **Q4 1997 : virus Cabanas (premier virus Win32)**
- **1er juin 1998 : premier bulletin de sécurité (MS98-001)**
  - "Disabling Creation of Local Groups on a Domain by Non-Administrative Users"
- **26 mars 1999 : ver Melissa (Word)**
- **19 juillet 2001 : ver Code Red (IIS)**
- **25 janvier 2003 : ver Slammer (SQL Server)**
- **12 août 2003 : ver Blaster (Windows RPC)**

1. Un peu d'histoire
"Microsoft Security Initiative"

- **Moyens**
  - Audit de code
    - Manuel et automatique : outils internes PREFix / PREFast
  - Formation des développeurs
    - Ouvrage "Writing Secure Code"
  - 2 mois, 200 millions de dollars

- **Résultats**
  - Nombreux bogues identifiés (et corrigés silencieusement)
    - Combien en reste-t-il ? Est-ce significatif ?
  - Ver Blaster
    - Utilise une défaillance triviale dans le code
    - Détecté par des Polonais n'ayant pas accès au code source !

1. Un peu d'histoire
"Get Secure, Stay Secure"

- **Moyens**
  - Guides de configuration gratuits
  - Incitation au déploiement des patches
    - Ex. Windows Update activé par défaut dans Windows XP
  - Outils de mise en œuvre gratuits
    - MSUS (requière XP SP1), MBSA, HFNetChk, …
    - Distribution de CDs
- **Résultats**
  - Effort d'exploitation des guides important
  - Problèmes liés au "patch management" (*LE* sujet de l'année 2004)
    - Nomadisme, gestion des masters, gestion de parc, continuité de service
  - Ver Blaster
    - Les particuliers n'appliquent pas les patches ni les guides de configuration
      - Et les entreprises ?
    - Les défaillances les plus graves se situent dans le "cœur" de Windows pour lequel une sécurisation proactive est impossible
      - RPC, SMB, services Workstation, etc.
  - Ver Slammer
    - Les patches pour MSDE ne sont pas gérés via MSUS
    - Seule la plateforme Windows / IE est prise en compte
  - Et les failles (IE) non corrigées ?

1. Un peu d'histoire
"Défense périmétrique"

- **Moyens**
  - Firewall ICF activé par défaut en mode "Deny All"
  - Autodéploiement quasi forcé des patches
  - Intégré dans XP SP2 (=> le SP2 est présenté juste après)

- **Résultats prévisibles**
  - Calvaire de déploiement pour les administrateurs
  - Désactivation des fonctions de sécurité par utilisateurs domestiques *et les applications* (via l'API INetFw*)
  - Application automatique des patches désactivée en entreprise

  - "Défense périmétrique" n'est pas "défense en profondeur"
    - L'utilisateur est administrateur local du poste
    - Les services s'exécutent sous le compte SYSTEM
  - Virus Mimail, MyDoom, Dumaru, etc. toujours possibles
    - Exploitent un bogue non corrigé
    - ICF ne filtre pas les connexions sortantes

  - Le poste de travail (et son utilisateur) reste le point faible

2. Les nouveautés majeures
Windows XP/2003 (1/2)

- **Nouveauté majeure dans Visual Studio.NET : la protection de pile**
  - Option de compilation /GS
  - Cf. StackGuard sous Unix
  - Protège contre l'exploitation simple d'un "buffer overflow"
  - Utilisé pour compiler :
    - Windows 2003 (dont IIS 6.0)
    - .NET Framework, Visual Studio 2003, Office 2003 (?), etc.

- **Modification du gestionnaire d'exceptions**
  - Principes
    - Le contrôle ne peut pas être transféré en pile
    - Les principaux registres sont effacés avant le traitement de l'exception
    - Les exceptions peuvent être déclarées dans le format PE
      - Dans ce cas les exceptions inconnues ne sont pas honorées
  - Remarque
    - Technique dite SEH déjà employée par Code Red en 2001

2. Les nouveautés majeures
Windows XP/2003 (2/2)

- **Utilisation de ".NET" pour les nouveaux composants**
  - Par conception, ".NET" n'est pas vulnérable aux "buffer overflows"
  - D'autres problèmes spécifiques à cette technologie ne manqueront pas d'être identifiés

- **Options de sécurité activées par défaut**
  - Exemples
    - Pas d'accès depuis le réseau avec un mot de passe vide
    - "Anonymous" n'appartient pas au groupe "Everyone"
    - Modification de la permission par défaut sur les partages créés
    - L'énumération anonyme des comptes et groupes est désactivée
  - Remarque
    - L'accès à C$ avec le compte "administrator" a longtemps été dans le Top 10 du SANS

2. Les nouveautés majeures
Windows XP SP2 (1/6)

- **Microsoft tire les leçons du passé**
  - Blaster, spam via popups, bogues IE, etc.
- **Une liste de nouveautés impressionnante**
  - 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 / RPC
      - Désactivation de l'accès anonyme par défaut
      - Journalisation accrue
      - Granularité des permissions accrue
    - Redirecteur WebDAV
      - "Basic auth" interdit sur HTTP

2. Les nouveautés majeures
Windows XP SP2 (2/6)

- Support du flag NX
  - Processeurs AMD64 et Itanium uniquement
  - Désactivable dans le panneau de configuration (globalement ou par application)
- API "AES" (Attachment Execution Service)
  - Point d'entrée pour un filtrage antivirus
  - Commune à IE / OE / Messenger
- Windows Messenger
  - Blocage des fichiers "dangereux" envoyés par des inconnus
  - Nickname obligatoirement différent de l'adresse email
- Outlook Express
  - Lecture en texte par défaut (rendu RTF au lieu de HTML)
  - Pas de téléchargement du contenu HTML externe
- Windows Media Player
  - Installation obligatoire de Media Player 9

2. Les nouveautés majeures
Windows XP SP2 (3/6)

- Wireless Provising 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 …
- Maintenance
  - Les correctifs de sécurité n'apparaissent plus dans ajout/suppression de programme
  - Client "Windows Update v5" / "Microsoft Update"
  - Calcul du RSoP
  - "Security Center"
    - Alerte l'utilisateur sur les fonctions de sécurité suivantes : antivirus, firewall, mises à jour
  - Windows Installer 3.0

❑ Autres nouveautés

- Détection des antivirus installés
- Recompilation avec /GS

2. Les nouveautés majeures
Windows XP SP2 (4/6)

- **ICF**
  - Nombreuses nouveautés
    - Toutes les fonctions d'un produit commercial
    - A l'exception (notable) du filtrage des connexions sortantes !
    - Atout : configurable par GPO et par script
  - Mode "deny all" actif par défaut en workgroup
    - En domaine, le sous-réseau est autorisé
  - APIs de configuration accessibles aux applications
    - INetFwAuthorizedApplication
    - INetFwOpenPort
    - INetFwProfile
  - Quelques "astuces"
    - Seuls les processus exécutés sous les comptes LocalSystem, LocalService ou NetworkService pour accéder à l'API
    - SVCHOST ne peut pas accéder à l'API
    - Traitement spécial des RPC (clé PrivilegedRpcServerPermission)
    - Ouverture des ports UDP en réponse pendant 90 secondes
    - Ouverture des ports UDP en réponse à un broadcast ou un multicast pendant 3 secondes

2. Les nouveautés majeures
Windows XP SP2 (5/6)

- **Internet Explorer**
  - Nombreuses nouveautés
  - "Information Bar"
  - Une seule popup de sécurité par page
  - Gestion facilitée des "add-ons"
    - Plug-ins de navigation
    - "Binary Behaviors"
  - Blocage des popups
  - Nouvelles "Feature Control"
    - "MIME sniffing"
      - Reconnaissance par signature et pas par extension
    - Pas d'exécution dans un contexte plus privilégié que l'URL de base
    - Création et déplacement des fenêtres par script limités

2. Les nouveautés majeures
Windows XP SP2 (6/6)

- **Un point de vue sur le SP2 (personnel)**
  - Gros effort d'amélioration de la sécurité Windows
    - Salué par la presse américaine
  - Nombreuses critiques également
    - 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
  - 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
  - Recommandations
    - Faire des tests de compatibilité exhaustifs
    - Prévoir obligatoirement de pouvoir désinstaller le SP2

3. Vers une informatique de confiance ?
Prochaines pistes de recherche

- **Recherches actuelles de Microsoft**
  - Visual Studio "Whidbey"
    - Favorise le développement d'applications n'ayant pas besoin des privilèges administrateur (enfin !)
  - Outils d'analyse de code source PREfast / PREfix
    - Déjà disponibles dans le DDK Windows 2003
  - Ouverture de plus en plus large du code source aux gouvernements
  - Certifications et re-certifications CC
    - Imposées par le gouvernement américain

- **Autres idées développées ailleurs**
  - Protection de type PaX / GRSecurity
    - Adresses aléatoires
    - Pages non exécutables (sans support matériel)
      - Cf. produits Windows SecureStack, Overflow Guard
  - Séparation des privilèges
  - Chroot

3. Vers une informatique de confiance ?
Sécurisation de l'environnement

- **Idée**
  - Le poste client peut être compromis
    - Risque accru par la mobilité
  - Concept de "défense en profondeur"

- **Solution**
  - Effectuer un contrôle externe de l'état du poste

- **Exemples d'implémentations**
  - Service de quarantaine de Windows 2003 serveur
    - Se base sur le résultat d'exécution d'un script côté client
  - Contrôle antivirus sur les routeurs
    - Annonces Cisco, Checkpoint

3. Vers une informatique de confiance ?
Sécurité matérielle

- **Le drapeau NX**
  - Un premier pas vers une sécurité matérielle

- **TCPA / NGSCB**
  - Une plateforme matérielle "sécurisée"
  - Restes des questions en suspens …
    - Spécifications encore floue
    - Comportement du marché inconnu
    - Gain en sécurité pour l'utilisateur final ?

4. Les nouveaux risques

- **Mobilité**
  - Développement du code mobile multi-plateformes
    - Ex. téléphones portables intégrant MIDP + synchronisation PC
    - Ex. "assemblies" .NET
- **Intégration de plus en forte d'Internet dans les applications Microsoft**
  - Ex. activation des produits, aide en ligne, compte Passport, Office 2003, etc.
- **Encapsulation des flux**
  - Tunnels HTTP et absence de firewalls applicatifs adaptés
    - Très prisé par Microsoft
    - Ex. RPC sur HTTP
  - Chevaux de Troie furtifs
    - Injection dans des processus autorisés
- **Risques applicatifs**
  - Bogues applicatifs dans les services Web
    - Risques classiques : injection SQL, XSS, etc.
  - Extension des fonctionnalités => extension de risques
    - Technologies SOAP / CORBA / .NET / etc.
    - Sérialisation d'objets via des connexions HTTP
  - Bogue dans le .NET Framework
- **Remarque : aucune des technologies vues précédemment ne protège contre ces risques**
  - Le flag NX n'est pas efficace contre le code interprété (Java, .NET, scripts)

5. Conclusion

- **L'équation à résoudre : sécuriser un système …**
  - … versatile
    - Grand public, postes de travail, serveurs Web, contrôleurs de domaine, etc.
  - … intégré
    - Applications et services exigent des privilèges élevés
    - Frontière entre le système et les applications très floue
    - Frontière entre le système et Internet de plus en plus floue également
  - ... ouvert
    - Leader incontesté du marché
    - Diversité applicative énorme
    - Communauté peu sensibilisée à la sécurité
  - … hérité
    - Besoin de compatibilité protocolaire
    - Besoin de compatibilité avec le parc logiciel
    - Les nouvelles fonctions de sécurité doivent être comprises par les développeurs