



EdelWeb

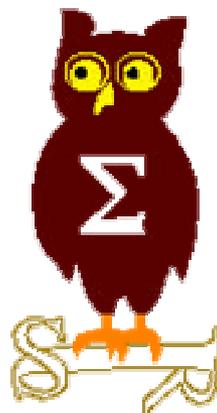
OSSIR

Groupe Sécurité Windows

Les vers RPC : analyse

Nicolas RUFF

nicolas.ruff@edelweb.fr





- **16 juillet 2003**
 - Publication de la vulnérabilité par LSD et Microsoft (MS03-026)
- **25 juillet 2003**
 - Publication du shellcode par FlashSky sur le site (chinois) XFocus
 - Nombreux shellcodes parallèles dans les jours qui suivent
- **7 août 2003**
 - Publication de l'exploit OC192 (shellcode "universel")
- **10 août 2003**
 - Ver Blaster
- **18 août 2003**
 - Ver Welchia
- **10 septembre 2003**
 - Nouvelles vulnérabilités critiques découvertes
 - eEye, NSFocus, Renaud Deraison
 - Publication du bulletin MS03-039



■ Vulnérabilité

- Un simple "buffer overflow" dans une fonction DCOM
 - CoGetCreateInstanceFromFile("\\COMPUTER\\file", ...)
 - Nom NetBIOS limité à 20 caractères mais la fonction en accepte 200

■ Exploitation

- Triviale, mais très dépendante du système visé
 - Problème de l'adresse de retour en fonction du système cible
 - Au début recherche d'un JMP ESP dans les DLL classiques (KERNEL32, USER32, ...)
 - Adresse "universelle" dans SVCHOST.EXE
 - Autre méthode d'exploitation ?
 - Ex. JMP <reg>, SEH, corruption de EBP, etc.
- Sous 2003, exploitation difficile
 - Tous les exécutables ont été recompilés avec l'option /GS
 - LSD prétend y être parvenu
- Sous NT4, exploitation impossible ?
 - RPCSS.EXE et non SVCHOST.EXE
 - Message d'erreur "Abstract Syntax Not Supported"



■ Blaster

- Un ver très simple qui utilise un shellcode modifié pour "piper" des commandes TFTP
- Utilise l'adresse de retour Windows XP à 80% et Windows 2000 à 20%
 - En cas de plantage du service RPC, l'action par défaut est de redémarrer au bout de 1 minute
- Scan IP séquentiel de la classe C dans 40% des cas
 - Peu optimisé et pourtant propagation rapide
- Charge finale : attaque du site WindowsUpdate (pour la variante .A)
 - Contre-attaque : WindowsUpdate redirigé temporairement vers 127.0.0.1

■ Welchia

- "Contre-ver" appliquant le correctif Microsoft
- Autodestruction prévue en janvier 2004
- Effets de bord : charge réseau et CPU très importante

■ Exemple de cibles impactées

- **Blaster**
 - Base USAF d'Edwards
 - Aéroport de Toronto
 - Panne d'électricité à NY (?)
 - <http://www.reuters.com/newsArticle.jhtml?storyID=3281792>
- **Welchia**
 - US Navy : <http://www.nwfusion.com/news/2003/0819navy.html>
 - Air Canada : <http://www.cyberpresse.ca/internet/article/1,150,1505,082003,401902.shtml>
- **Slammer avait pénétré une centrale nucléaire dans l'Ohio**
 - <http://www.securityfocus.com/news/6767>

■ Conséquences

- **Un suspect arrêté pour la variante Blaster.B**
 - Jeffrey Lee Parson alias "teekid", 18 ans
- **Un suspect arrêté en Roumanie**
 - http://biz.yahoo.com/rc/030903/tech_internet_virus_1.html
- **Effets sur la fréquentation des sites**
 - Technet +1100%
 - WindowsUpdate +76%
 - Symantec +302%
 - ZoneLabs +73%



■ Réactions de Microsoft

- La prochaine version de Windows XP (fin 2004) inclura un Windows Update obligatoire
- La prochaine version de Windows XP aura le firewall intégré actif par défaut
- Achetez des firewalls matériels !
 - <http://www.microsoft.com/windowsxp/expertzone/columns/northrup/02august12.asp>

■ Responsabilités Microsoft

- Plusieurs failles triviales passées au travers de la relecture de code ...
 - Échec de l'initiative "trusted computing")
 - Nouvelle initiative "périmètre de défense"
- Le code "hérité" n'est plus maintenable ?
 - Cf. découvertes du projet SAMBA



■ Architecture de l'OS

- Concentration de tous les services sur un port (ici TCP/135)
 - Ex. même le copier/coller local ne marche plus lorsque le service RPC est arrêté !
- Aucune protection proactive n'est possible une fois le ver sur un LAN
- Même scénario reproductible si une faille affecte les services NetBIOS (137-139), Web (80), etc.

■ Responsabilités des entreprises

- Encore une fois le ver est passé à travers des firewalls mal configurés (cf. Slammer)
- Aucune entreprise ne peut se considérer comme "étanche" (problème des portables, des filiales connectées directement à Internet, etc.)
- Les patches ne sont pas appliqués ...



- **Très forte activité dans le domaine de la sécurité**
 - Réactivité des hackers (moins de 15 jours pour identifier le problème et produire un shellcode)
 - Nombreux shellcodes publiés et diffusés

- **Encore un ver ménageant les administrateurs**
 - Ver très facile à filtrer
 - Utilise TFTP + des ports fixes (TCP/4444)
 - Ver très facile à détecter
 - Pas de "rootkit", écrit des fichiers sur le disque, fait des modifications grossières du système
 - Pas de charge utile destructrice

- **On a évité le pire**



■ Questions / réponses