# Retour d'expérience du Cert-IST sur le ver "Blaster"

**Stéphane ROZES – Cert-IST**

Stephane.Rozes@Cert-IST.com

- **Agenda :**
  - **Traitement au niveau du Cert-IST**
  - **"Blaster" chez les membres du Cert-IST**
  - **La suite de la "saga" des failles RPC**
  - **Conclusion**

# Traitement au niveau du Cert-IST

- **17 juillet 2003 - *AVIS* (*CERT-IST/AV-2003.227*) sur la faille RPC de Windows**
- **28 juillet 2003 - *INFORMATION* (*CERT-IST/IF-2003.004*) sur des attaques possibles via la vulnérabilité Windows RPC/DCOM (présence de programme d'exploitation) + *AVIS VERSION 2.0* sur la faille RPC de Windows (présence de programme d'exploitation)**
- **01 août 2003 - *ALERTE* (*CERT-IST/AL-2003.005*) sur l'exploitation de la vulnérabilité RPC de Microsoft + *Seconde vulnérabilité du service RPC (DoS) non corrigée* [corrigée dans le bulletin MS03-039]**

# Traitement au niveau du Cert-IST

- **6 août 2003 – AVIS (*CERT-IST/AV-2003.253*) sur un cheval de Troie exploitant la vulnérabilité RPC ("Autorooter")**
- **12 août 2003 - *Post sur la liste des "contacts virus"* concernant la propagation du ver "Blaster" + *AVIS* (*CERT-IST/AV-2003.257*) sur le ver "Blaster" + *ALERTE VERSION 2* sur l'exploitation de la vulnérabilité RPC de Microsoft**
- **14 août 2003 - *AVIS* (*CERT-IST/AV-2003.259*) sur un ver exploitant la vulnérabilité RPC ("RpcSpybot")**
- **19 août 2003 - *AVIS* (*CERT-IST/AV-2003.261*) sur un ver "blanc" exploitant la vulnérabilité RPC ("Nachi")**

# "Blaster" chez les membres du Cert-IST

- **Profil des membres du Cert-IST :**
  - Secteur industriel (multinationales)
  - Moyens humains dédiés (équipes sécurité)
  - Infrastructures sécurisées (politique de sécurité, garde-barrière, scanner de messagerie, anti-virus personnels sur PC et serveurs, …)
- **Infection :**
  - Infections parfois tardives (effet "retour de vacances")
  - "Blaster" a infecté de 0,8% à 2,6% du parc machines (8000 à 100 000 machines)
- **Principales sources d'infection :**
  - Les PC Portables des utilisateurs nomades (non à jour)
  - Des connexions de PC personnels à travers le service d'accès distant (RAS) de l'entreprise
  - Des connexions locales de PC personnels sur le réseau de l'entreprise

# "Blaster" chez les membres du Cert-IST – Les réactions

## Mise en place de Cellule de crise

- Profil : 5 à 30 personnes (30 étant un nombre jugé trop élevé)
  - **Service Sécurité (RSSI)**
  - **Service Réseau (LAN)**
  - **Service Télécom (WAN)**
  - **Service Messagerie**
  - **Service Bureautique**
  - **Administrateurs des systèmes**
- **Buts :**
  - **Suivi de l'évolution du ver**
  - **Suivi de la mise à jour des correctifs de Microsoft**
  - **Décision de filtrage de ports**
  - **Blocage de sous-réseau**

# "Blaster" chez les membres du Cert-IST - Actions prises

- Mise à jour plus fréquente des anti-virus
- Filtrage réseau (filtrage à des fins de protection, filtrage à des fins de détection)
- Déploiement des correctifs Microsoft de manière plus soutenue
- Utilisation de scanner de vulnérabilités
- Gestion des postes nomades
- Analyse des journaux d'exploitation des équipements filtrant
- Mise à disposition d'outils vers les utilisateurs (Intranet ou CD-ROM)
- Communication (papier, e-mail, Intranet, SMS)

# "Blaster" chez les membres du Cert-IST - Difficultés rencontrées

- **Niveau organisationnel :**
  - Périodes de congés
  - Centre de décision
  - Remontée d'informations (état des lieux)
  - Filiales de petites tailles
- **Niveau technique :**
  - Déploiement des correctifs (SMS, LDMS, Tivoli)
  - Hétérogénéité du parc (problème de niveau des correctifs et des Service Packs)
  - Postes nomades (connexions non permanentes)
  - Machines hors contrôle

# La "saga" continue

- **Nouvel avis de Microsoft MS03-039 le 10 septembre 2003.**
  - **Avis (*CERT-IST/AV-2003.285*) et Information (*CERT-IST/IF-2003.006*) du Cert-IST vers sa communauté**
  - **Information publique sur le site du Cert-IST http://www.cert-ist.com (Avis + Synthèse sur ces vulnérabilités)**

- **Surveillance étroite (et test) des nouveaux programmes d'exploitation.**
  - **Blaster 2 ?**
  - **Beaucoup d'exploits, mais ne "marchent" pas … jusqu'à quand ….**

# Conclusion

- **Blaster a eu un effet limité :**
  - **Au prix d'une réaction immédiate et d'un effort soutenu**

- **Améliorations : Nécessité d'une coordination inter-entreprise**
  - **Canal de communication dédié en temps de crise**
  - **Mutualisation de moyens en temps de crise (résultats des tests de correctifs, …)**
  - **Mutualisation des bonnes pratiques de gestion de crise virale de chaque membre**

Cert-IST = Fédérateur

**Extension des retours sur Blaster dans le cadre du projet EISPP au niveau des PME.**