Computer Emergency Response Team
Industrie Service Tertiaire

“ Blaster, Sobig, Autoproxy, Mydoom ”

Comment faire face aux nouvelles crises virales ?

CERTIST
Industrie Services Tertiaire

Mai 2004

Plan de la présentation

- Le Cert-IST et la gestion des crises virales
- L'évolution de la menace virale
- Comment réagir ?
  - Prévention
    - Les moyens de protection
    - La veille sur les failles et les mécanismes d'alerte
  - Traitement de l'infection
    - Exemple « Blaster »
  - Gestion des crises
    - Les interlocuteurs
    - Éléments clefs de réussite
    - Coopération inter-entreprises

Le Cert-IST et la gestion des crises virales

- Centre d'alerte et de support pour les incidents informatiques
  - En opération depuis janvier 1999
    - Dédié au domaine « IST » : Industrie Service et Tertiaire
    - Association « loi 1901 » depuis mars 2003
    - www.cert-ist.com
  - Émission d'avis, d'alertes, etc…
  - Traitement d'incidents : coordination, analyse technique, etc..
  - Formations et Études sécurité
- La crise Blaster a poussé les adhérents et l'équipe technique du Cert-IST à repenser la façon de faire face aux crises virales.

L'évolution de la menace virale

L'évolution vers « Le tout virus »

- « Virus » = toute attaque massive visant essentiellement Windows
  - Difficile de faire encore une distinction : Ver / Virus / Cheval de Troie / etc..
  - Convergence de toutes les techniques d'attaques vers les « Virus » (vitesse) et vers « Windows » (universalité)

- Les virus « traditionnels »
  - Code répliquant véhiculé par e-mail ou par partages réseau (ex : MyDoom, SoBig)

- Les « nouveaux » virus
  - Exploitation de failles des logiciels et systèmes d'exploitation (ex: Blaster)
  - Infection via le navigateur Web (ex: Autoproxy (*))

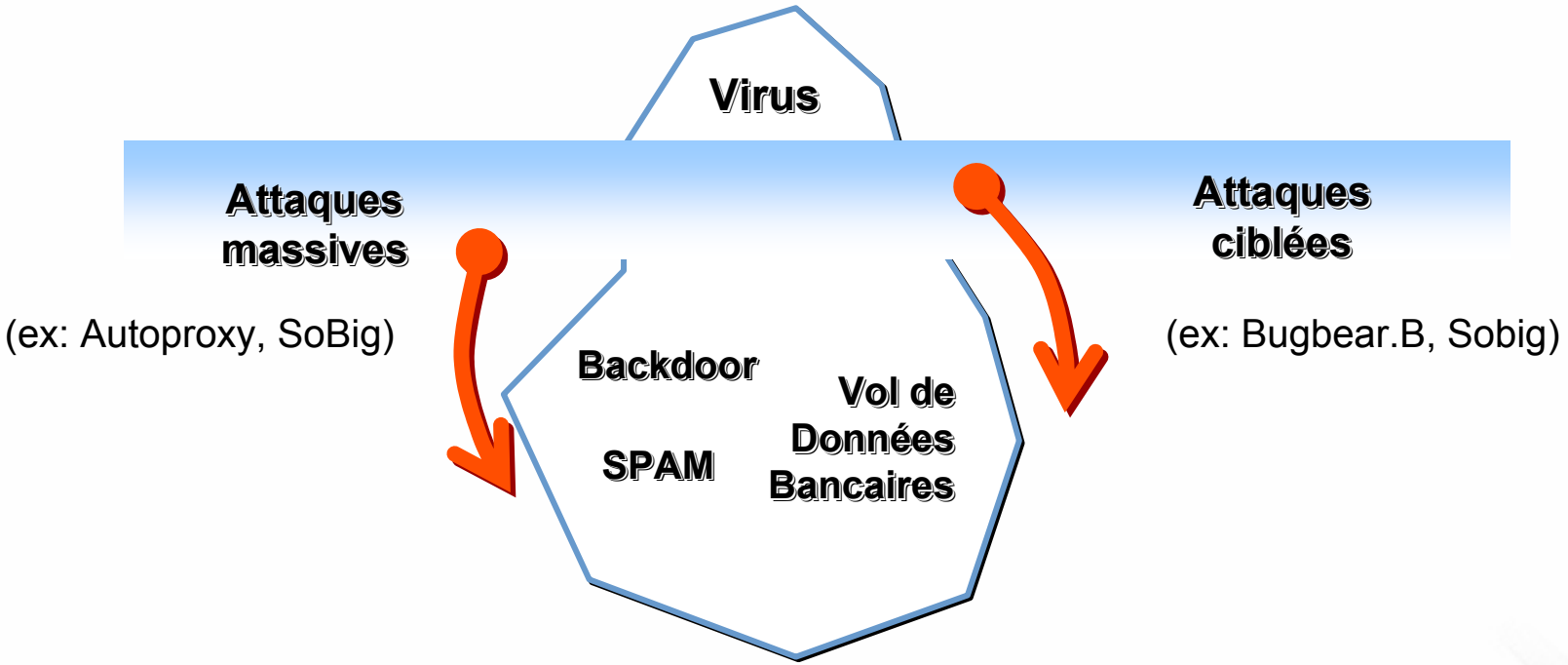
(*) : cf. incident NOOS

Evolutions : La montée de la menace pour l'entreprise

- Ces attaques sont de plus en plus fréquentes et sophistiquées
  - Un « simple » virus « MyDoom » (« .exe » envoyé par email) connaît une propagation incroyablement élevée.
  - Une faille exploitable à distance dans Windows donnera « forcement » lieu à un virus
- Ces attaques produisent des effets dont l'impact va au-delà des cibles visées
  - Saturation des infrastructures réseau
  - Gel des Systèmes d'Information
- Les virus mettent en évidences de nouveaux problèmes
  - Vulnérabilité des postes mobiles (accès VPN ou poste nomade)

Evolutions : Le Virus en tant que vecteur d'attaque

- Le virus est la partie visible d'un danger plus large
  - Le virus devient un « outil »
    - pour déposer une backdoor ou préparer une attaque de masse:



  - L'année 2003 montre une évolution des motivations et du profil des attaquants

Exemples : Exploitation de failles

- Historique des « vers » exploitant des failles systèmes
  - CodeRed (juillet 2001) et Nimda (septembre 2001) :
    Faille IIS => Serveurs Web
  - Spida (mai 2002) et Slammer/Sapphire (janvier 2003) :
    Failles SQL-Server => Environnements de production
  - Blaster (août 2003) :
    Faille RPC/DCOM => Tout le monde

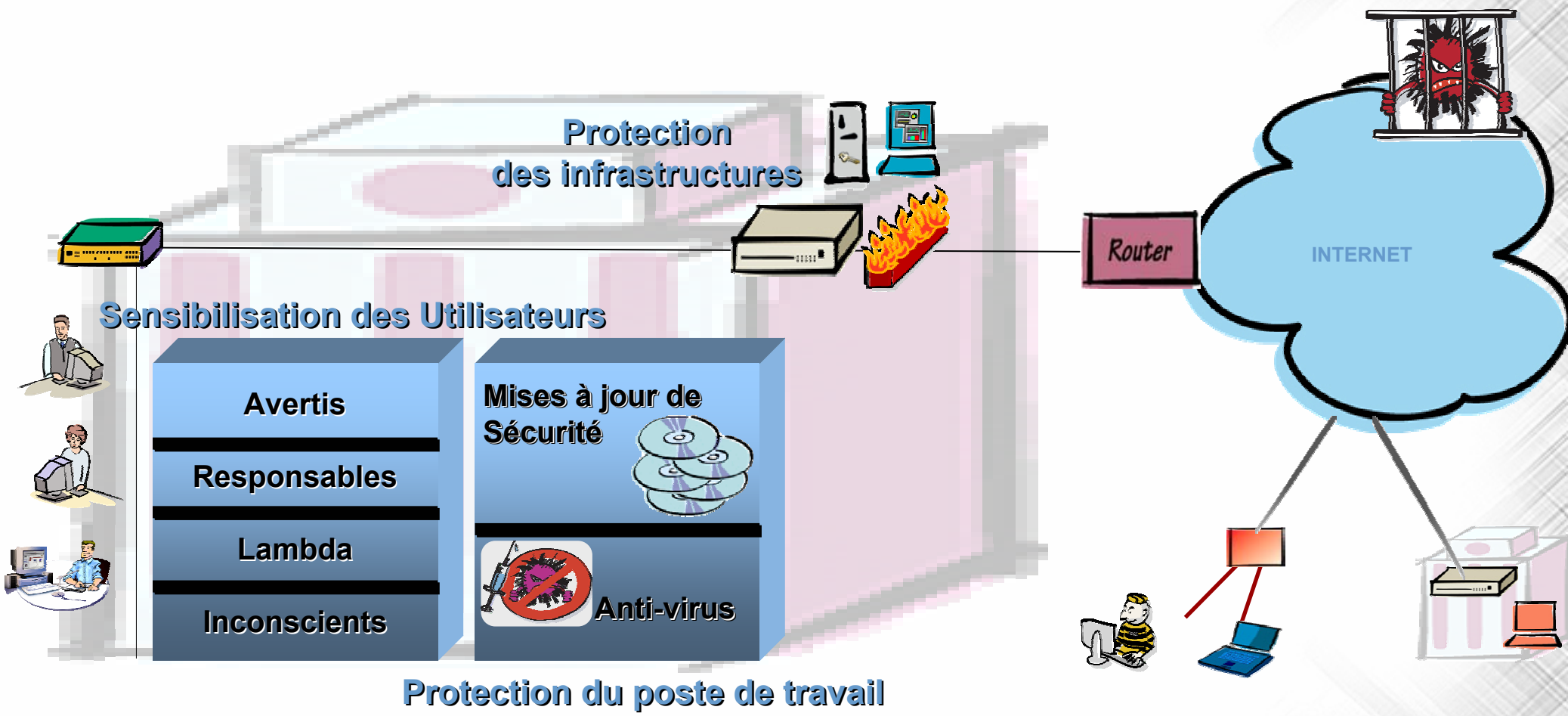
Bagle : La mutation d'un virus

Bagle	Bagle A 18/01/2004	Bagle B 17/02/2004	Bagle C,D,E 28/02/2004	Bagle F,G 29/02/2004	Bagle H,I 01/03/2004	Bagle J 02/03/2004	Bagle M,N,O,P 13/03/2004	Bagle Q 18/03/2004
Titre	"Hi"	Id […]thanks	aleatoire: (pricelist,account,melissa)	"feminin": mew-mew,katrina	"Hi, mew-mew"	** e-mail **	** e-mail **, Re:msg reply	** e-mail **, Re:msg reply
Corps	** test **			aleatoire: I love,hobbies	hey dude, I don't bite	** e-mail account **	** e-mail account, antivirus, spam **	HTML
pièce jointe	dxju....exe	qlli.exe	acdab.zip	.exe,.scr,.zip, katrina, mygallery	.zip encrypted, msg,info, document	.exe, .pif, encrypted .zip, attach, info	.exe, .pif, .rar, encrypted .zip, .bmp, .gif, .jpg	NON
					password in text	password in text	password in BITMAP	
et apparence	calculatrice	fichier son	feuille excel	dossier windows	dossier windows	notepad	police truetype	html
	Ingénierie Sociale							
adresse émetteur		falsifiée	falsifiée		falsifiée	mail provider	mail provider, support, ou correspondant	mail provider, support, ou correspondant
diversion		magneto snrec.exe	notepad windows					
dangerosité	pour simplets		pour simplets		pour simplets			Automatique, exploite vulnérabilité Microsoft
porte dérobée ouverte	TCP 6777	TCP8866	TCP2745	TCP2745	TCP2745	TCP2745	TCP2556	TCP2556
action sur le système	non	non	OUI	OUI	OUI	OUI	oui	oui
action sur les antivirus	non		OUI	OUI	OUI	OUI	oui ++	oui ++
mode de propagation	mail	mail	mail	mail + SHARE	mail + share	mail + share	mail + share	mail + share + auto

Comment réagir ?

CERTIST
Industrie Services Tertiaire

Prévention : Les moyens de protection



Prévention : Les Moyens de protection

- Protection du poste de travail
  - Mise à jour des postes et protection virale
  - Mais … la maîtrise complète du parc reste difficile
    - Hétérogénéité du parc
    - Éléments hors contrôle (ex : sous-traitants et filiales, postes administrateurs)
- Sensibilisation des utilisateurs
  - Formation au risque viral
  - Préparation aux situations de crise
- Protection des infrastructures
  - Passerelles anti-virus (email, trafic web)
  - Architecture permettant la coupure / l'isolation de segments réseaux

Prévention : La veille sur les failles et mécanismes d'alertes

Faille

17 juillet 2003 - *AVIS* (*CERT-IST/AV-2003.227*) sur la faille RPC de Windows

Exploit

28 juillet 2003 - *INFORMATION* (*CERT-IST/IF-2003.004*) sur des attaques possibles via la vulnérabilité Windows RPC/DCOM (présence de programme d'exploitation)

Attaques

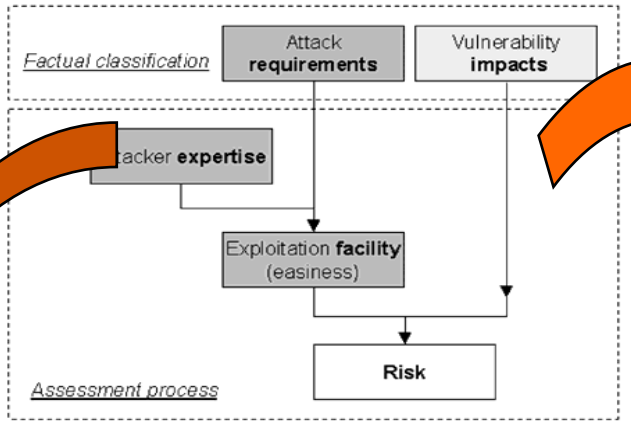
01 août 2003 - *ALERTE* (*CERT-IST/AL-2003.005*) sur l'exploitation de la vulnérabilité RPC de Microsoft
+ *Seconde vulnérabilité du service RPC (DoS) non corrigée* [corrigée dans le bulletin MS03-039]

Virus

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

Prévention : L'évaluation du risque

- Le processus de Qualification du risque/criticité
  - facilité et impact



	Impact severity			
Exploitation facility	Take control	Get limited access Gain limited privilege	DoS Integrity impact Confidentiality impact	Disrupt service Leverage Hiding
Trivial	Very high	High	High	Medium
Easy	Very high	High	High	Medium
Medium	Very high	High	Medium	Medium
Difficult	High	Medium	Medium	Low
Very difficult	High	Medium	Low	Low

	Requirement			
Expertise	Remote no account standard service	Remote no account exotic service	Remote with account	Physical access
Beginner	Trivial	Easy	Medium	Difficult
Skilled	Easy	Medium	Difficult	Very difficult
Expert	Difficult	Difficult	Very difficult	Very difficult

Risk	Recommandation
Very high	Act immediately on all systems
High	Act immediately on front-end systems and servers
Medium	Action can be delayed, but a security maintenance operation must be scheduled now
Low	Action can be delayed until the next scheduled maintenance operation

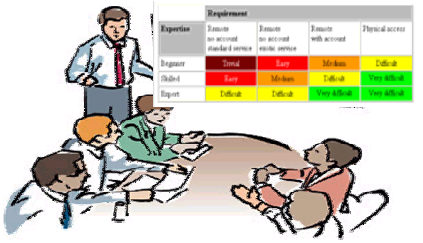
Traitement de l'infection (exemple Blaster)

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

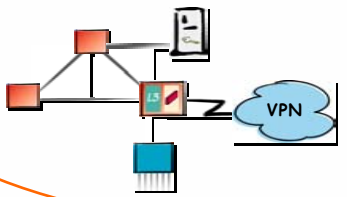
Gestion des crises : les interlocuteurs

- Comité stratégique : Décision
  - Qualification de la gravité
  - Gestion de Crise

- Cellule Sécurité : Expertise
  - Analyse des risques & sélection des Solutions
  - Contrôle des mises à niveau



- Operations : Maîtrise des équipements
  - Identification des plates-formes systèmes et réseaux critiques (ou pertinentes)
  - Gestion des solutions / surveillance



Gestion des crises : les éléments clefs

- Organisation et préparation
  - Identification des interlocuteurs clefs
  - Procédures spécifiques à la gestion de crise virale
- Capacité technique de maîtrise de l'infection
  - Outil de déploiement des correctifs / Contrôle du déploiement effectif
  - Filtrage ou isolement de sous-réseaux
  - Gestion de utilisateurs nomades / Gestion des intervenants externes
- Facteurs de gains en phase de crise
  - Communication active
  - Mutualisation des efforts / Coopération inter-entreprise

Gestion des crises : La coopération inter-entreprises

- **Motivations pour la coopération**
  - Vitesse de réaction (multiplication des ressources)
  - Efficacité : mise en commun des résultats (méthode de filtrage, tests de correctifs, …)
- **Méthode de coopération**
  - Échanges au travers du Cert-IST
    - Prend en charge les efforts induits par la mutualisation
    - Valide les informations échangées
    - Anonymise les contributions (si besoin)
- Moyens pour la mise en œuvre
  - Moyens de communication dédiées à la crise virale
  - Mutualisation via le serveur Web privé

Gestion des crises : Analyse post-incident

- Le cycle de mise en oeuvre de la sécurité