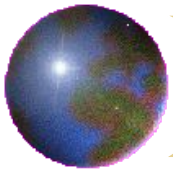
CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Menaces et attaques

Formation SIARS
Décembre 2004 - Lyon



Auteur(s)

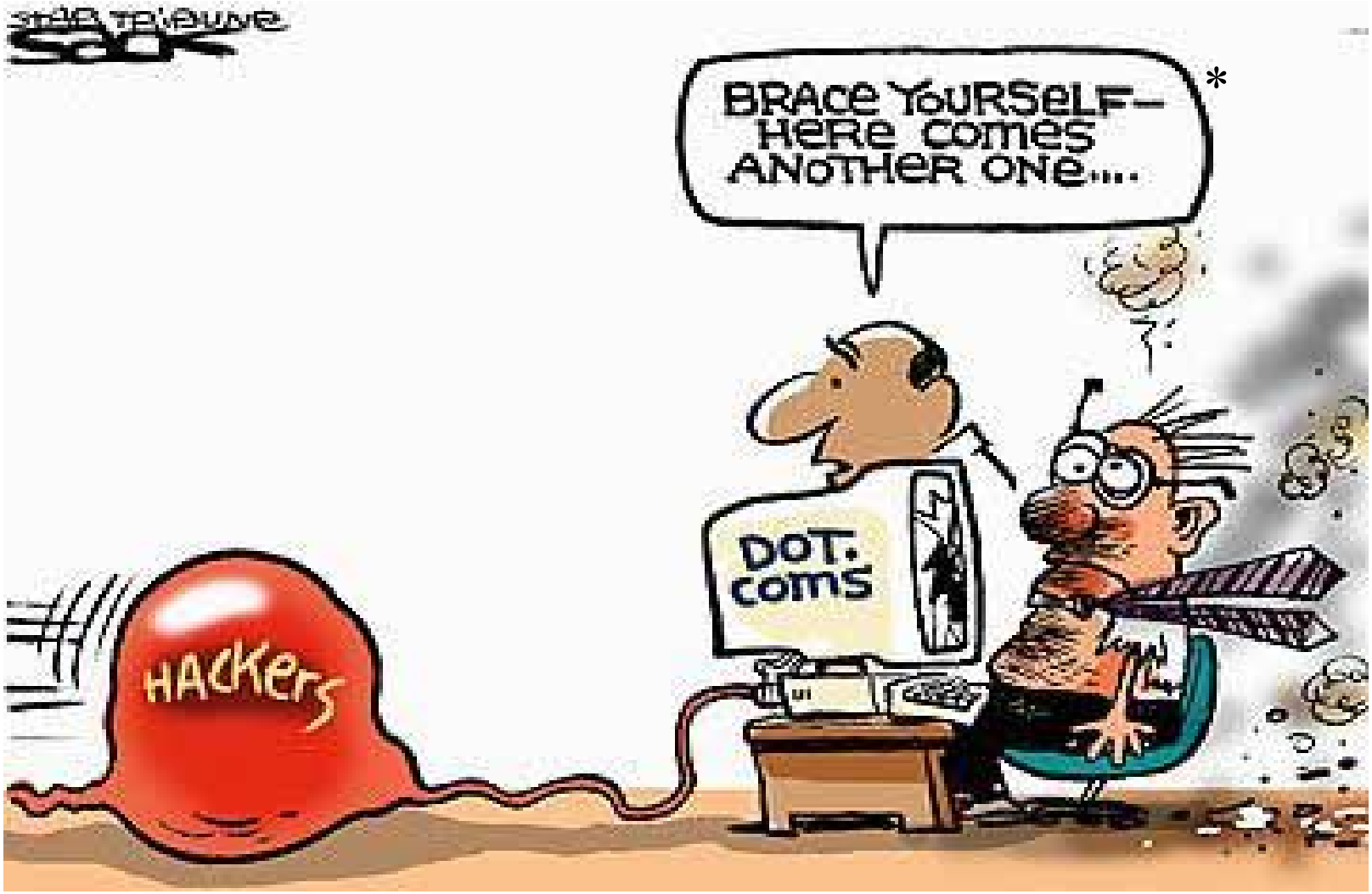
Cette présentation, élaborée dans le cadre de la formation SIARS, ne peut être utilisée ou modifiée qu'avec le consentement de ses auteur(s).

- Version 1.0 : 12/2004 : Denis Pugnère d.pugnere@ipnl.in2p3.fr
-

1) Menaces & attaques

2) Réaction face aux risques : politique de sécurité

No comment !

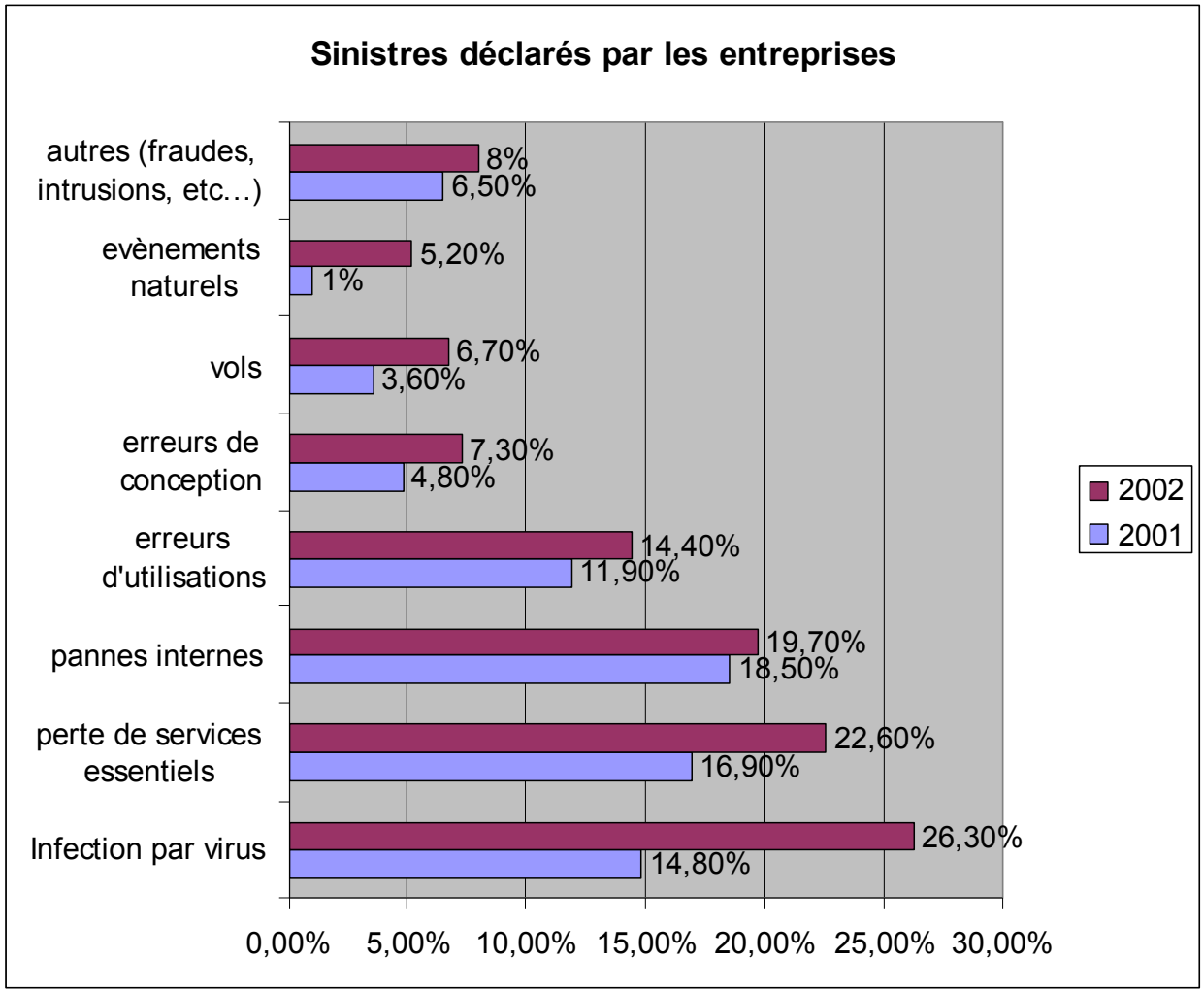


* : accroches toi, il en arrive un autre...

Connexions réseaux : toc toc toc…

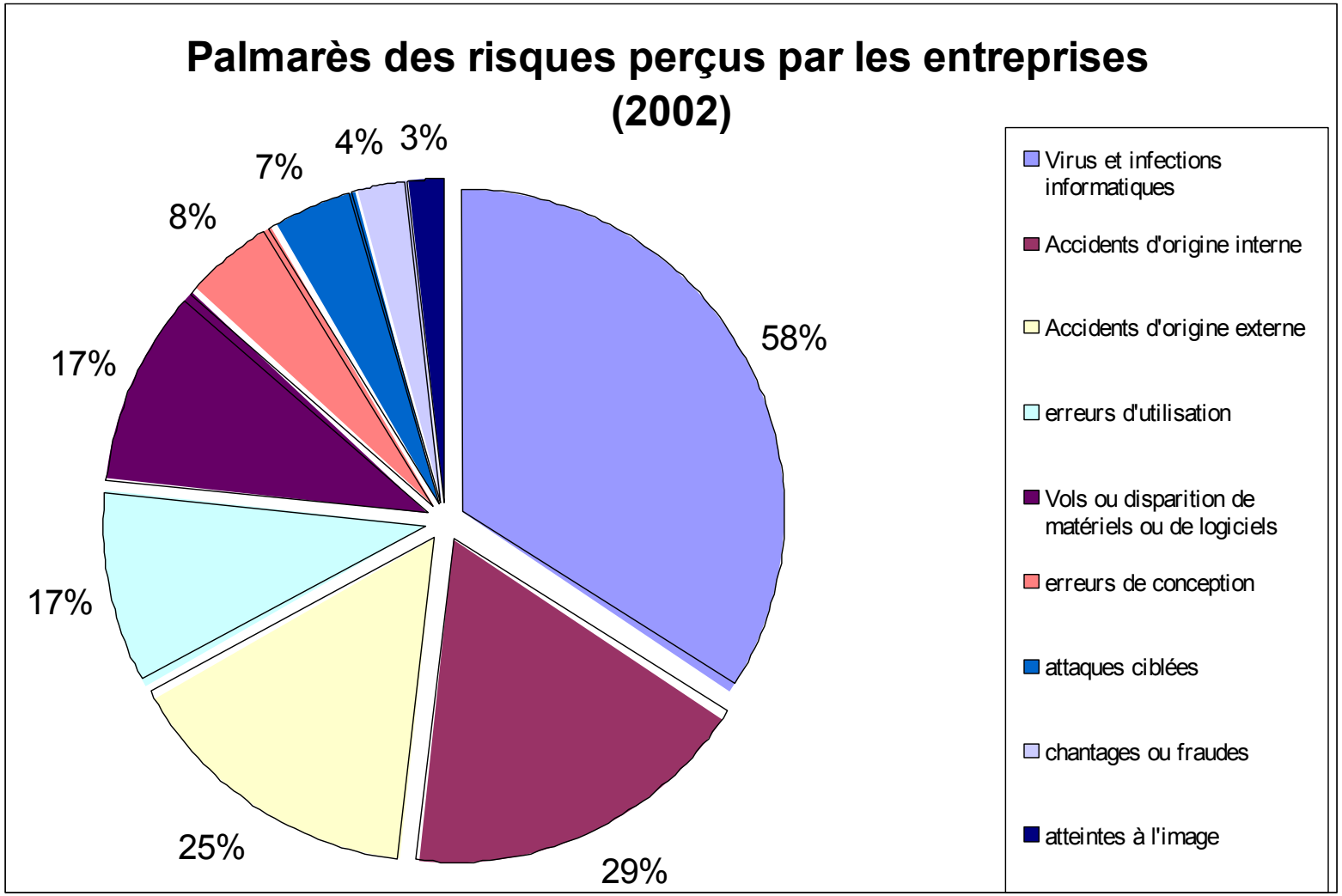
- Quelques secondes après la connexion d'un système à Internet : réception de paquets
  - Virus,
  - Sondes,
  - Scans
- Moins d'une minute après :
  - Sans antivirus : infection virale (reboot, spam, backdoor…)
  - Sans firewall :
    - Win32 : infection par un « ver » exploitant les vulnérabilités windows
    - Linux, MacOS X, Un*x : exploitation des services réseaux vulnérables

Menaces



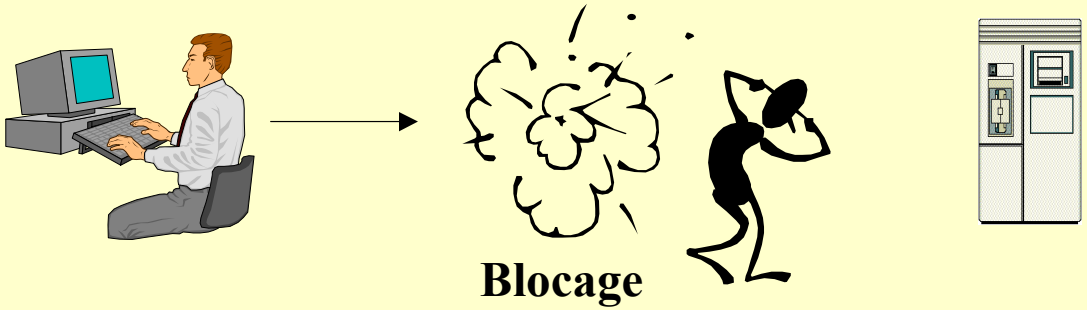
Sources : Etudes statistiques sur la sinistralité informatique en France (2002). Etude commandée par le Clusif et réalisée auprès d'un panel de 600 entreprises (52% d'entre elles ayant entre 10 et 199 salariés)

Menaces ... perçues



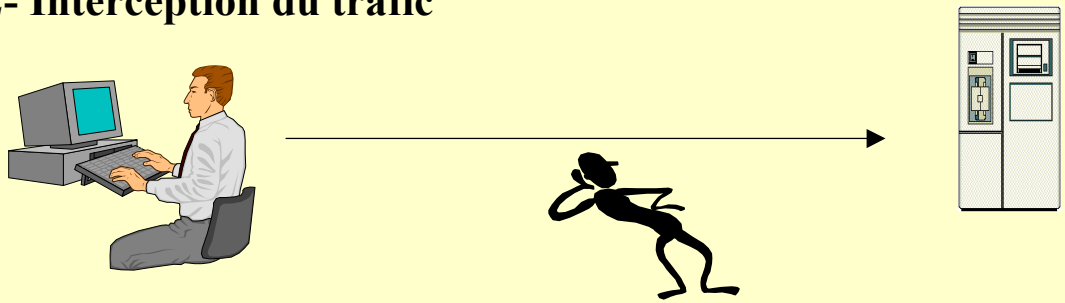
Différents types (1/3)

1- Interruption de service



Moyens utilisables :
- **destruction physique**
- **modifications logicielles**
- **altérations des paquets en transit**
- **etc.**

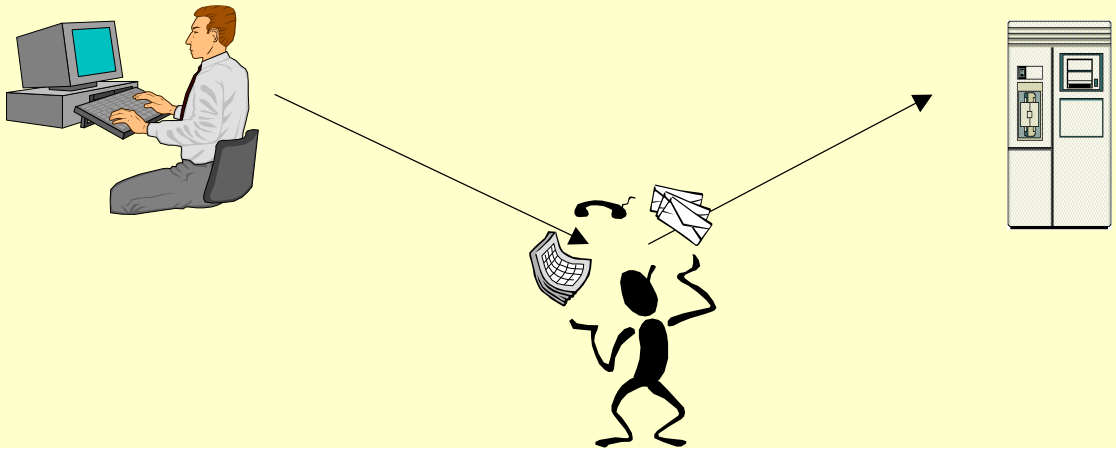
2- Interception du trafic



Moyens utilisables :
- **simple accès non autorisé à l'information**
- **analyse réseau (renifleurs)**
- **copie illicite de programmes ou de fichiers**
- **etc.**

Différents types (2/3)

3- Altération de l'intégrité des données



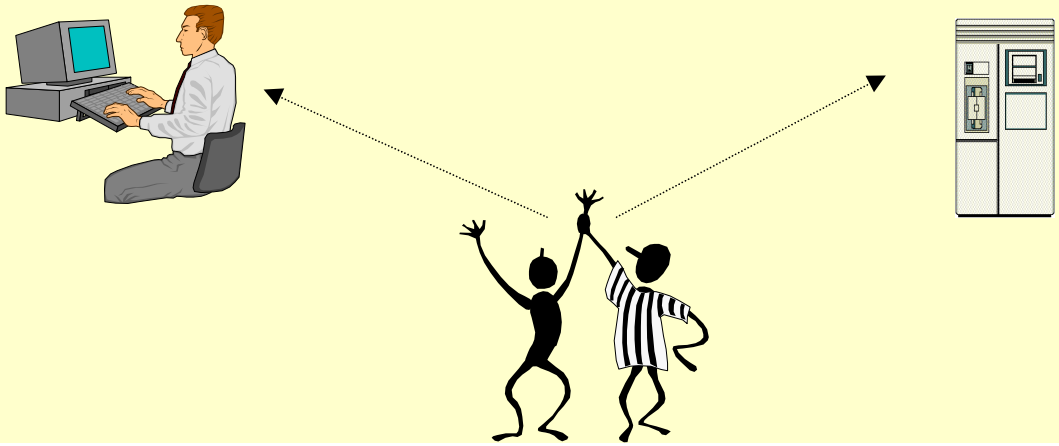
Moyens utilisables :
- interception des flux
- modification des données

4- Mascarade

Moyens utilisables :
- usurpation d'identité
- diffusion de fausses informations sous une fausse identité : spam, intoxication, etc.

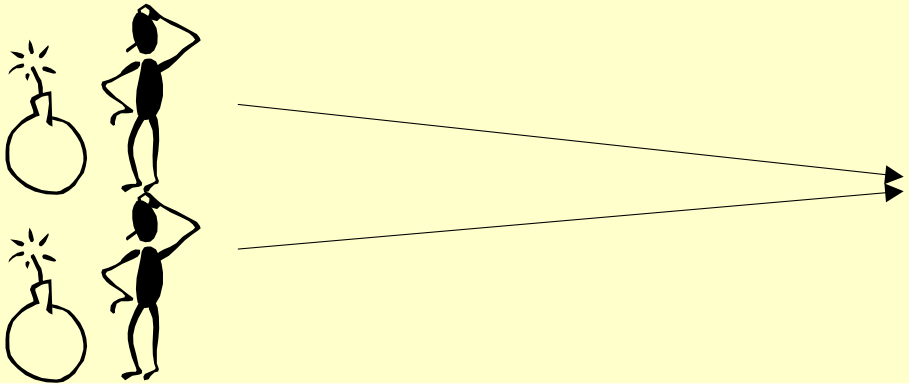
Différents types (3/3)

5- Infiltration



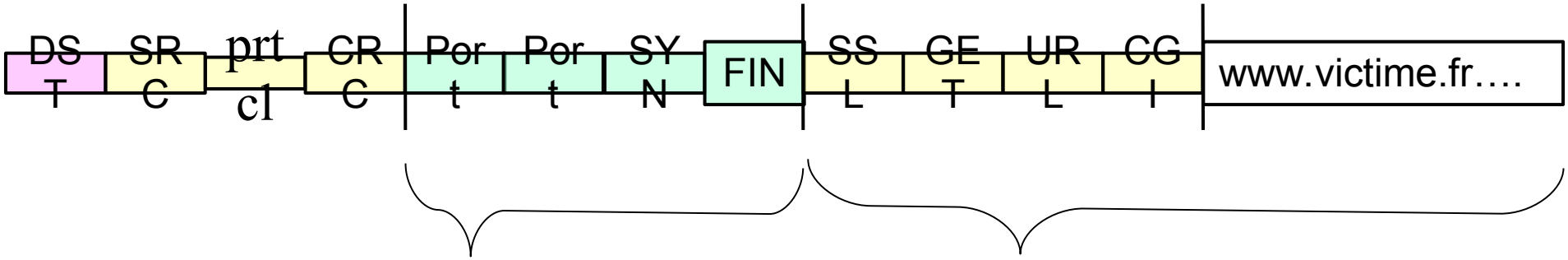
Moyens utilisables :
- **intervention physique sur les matériels ou actions à distance**
- **virus, chevaux de Troie**

6- Attaques frontales



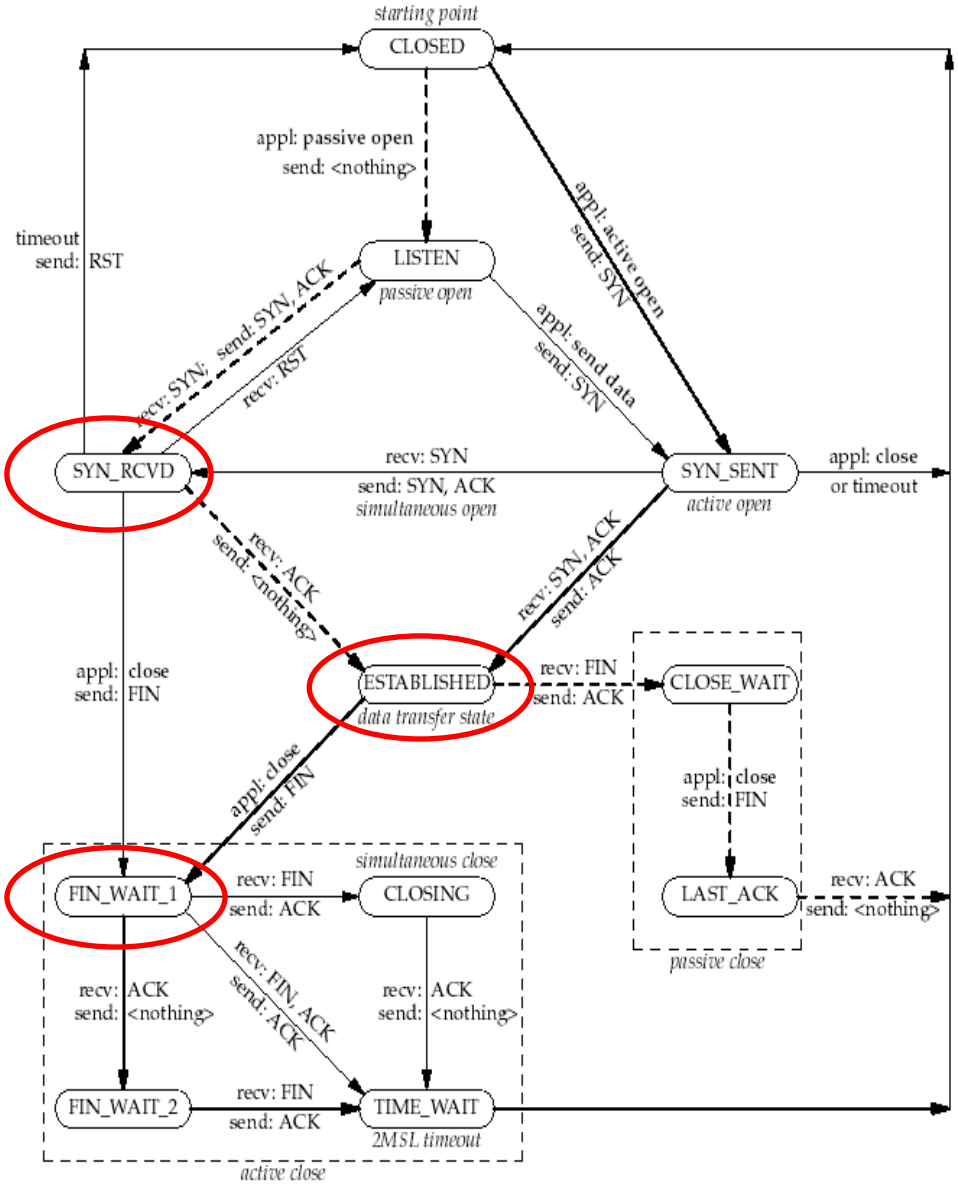
Moyens utilisables :
- **smurf, attaques coordonnées**
- **déni de service**
- **exploitation de vulnérabilités**

Attaques selon le protocole

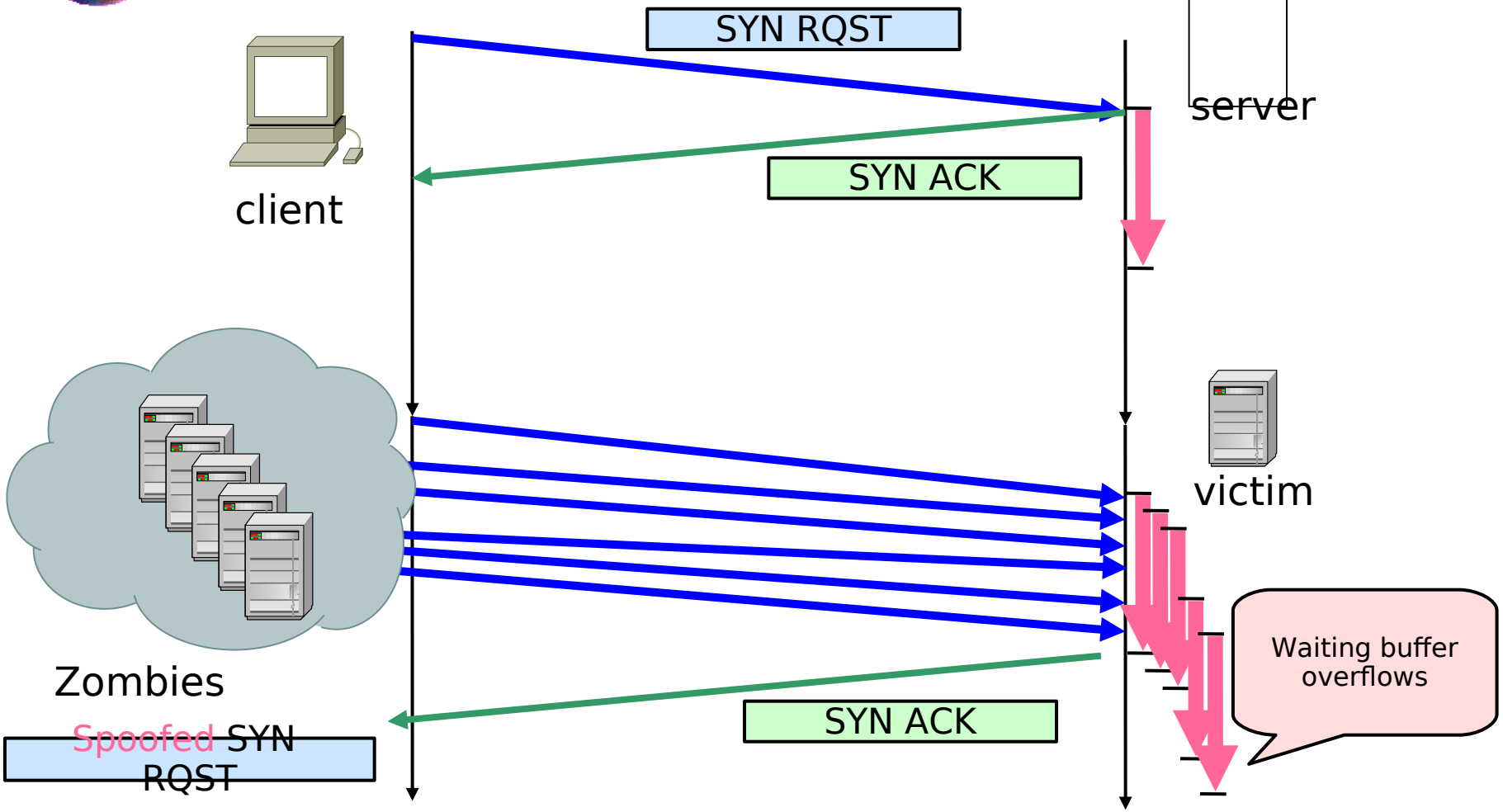


- Attaque sur couche 3 :
  - ICMP broadcast
  - ARP spoofing
- Attaque sur couche 4 :
  - TCP :
    - SYN receive
    - Establish
    - FIN_WAIT_1
  - UDP spoofing
- Sur couches applicatives :
  - 404 File Not Found Flood
  - SSL
  - CGI
  - DNS Bogus requests attack

Attaques sur le protocole TCP

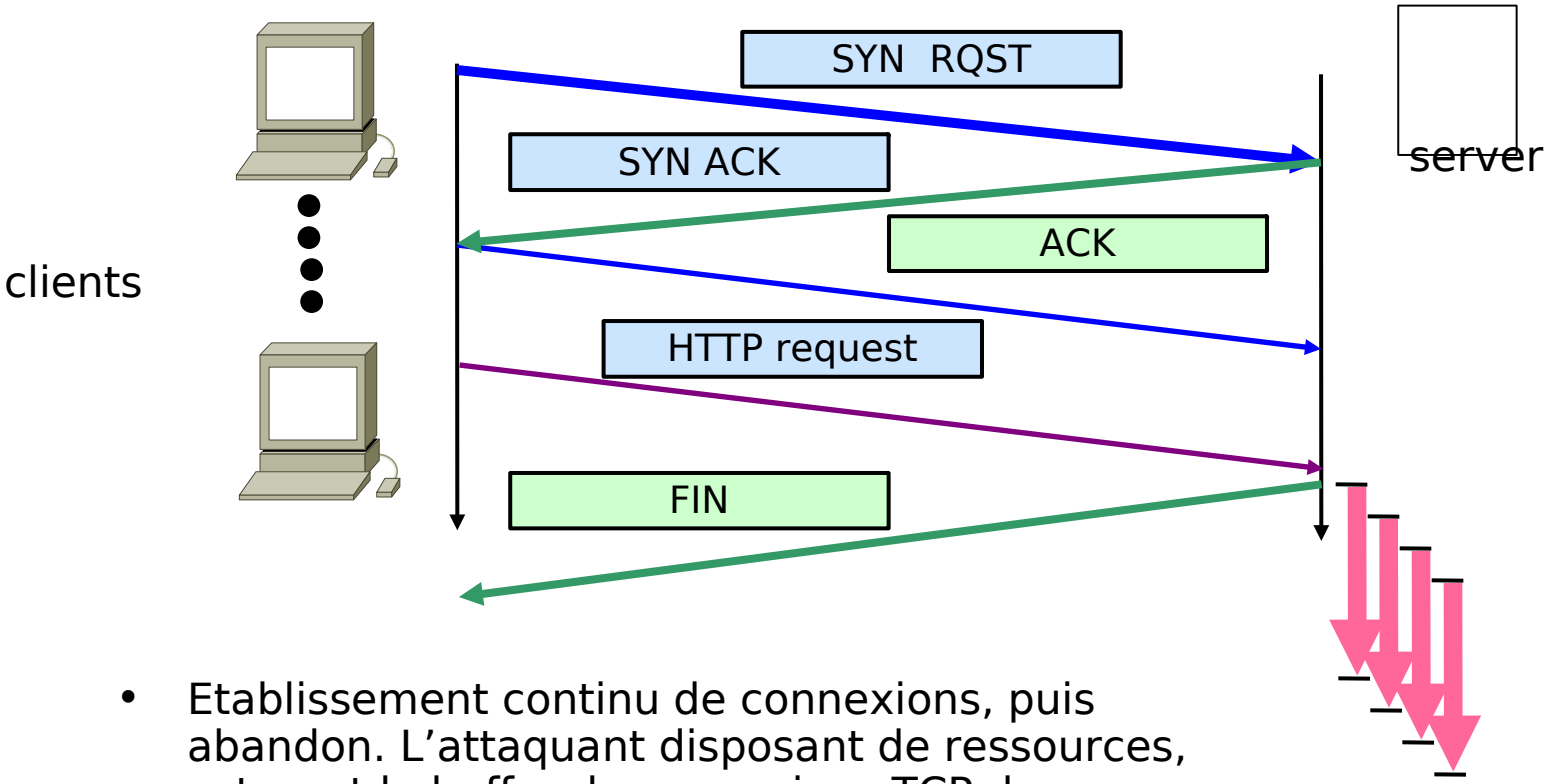


TCP SYN flood (semi-ouvertes)



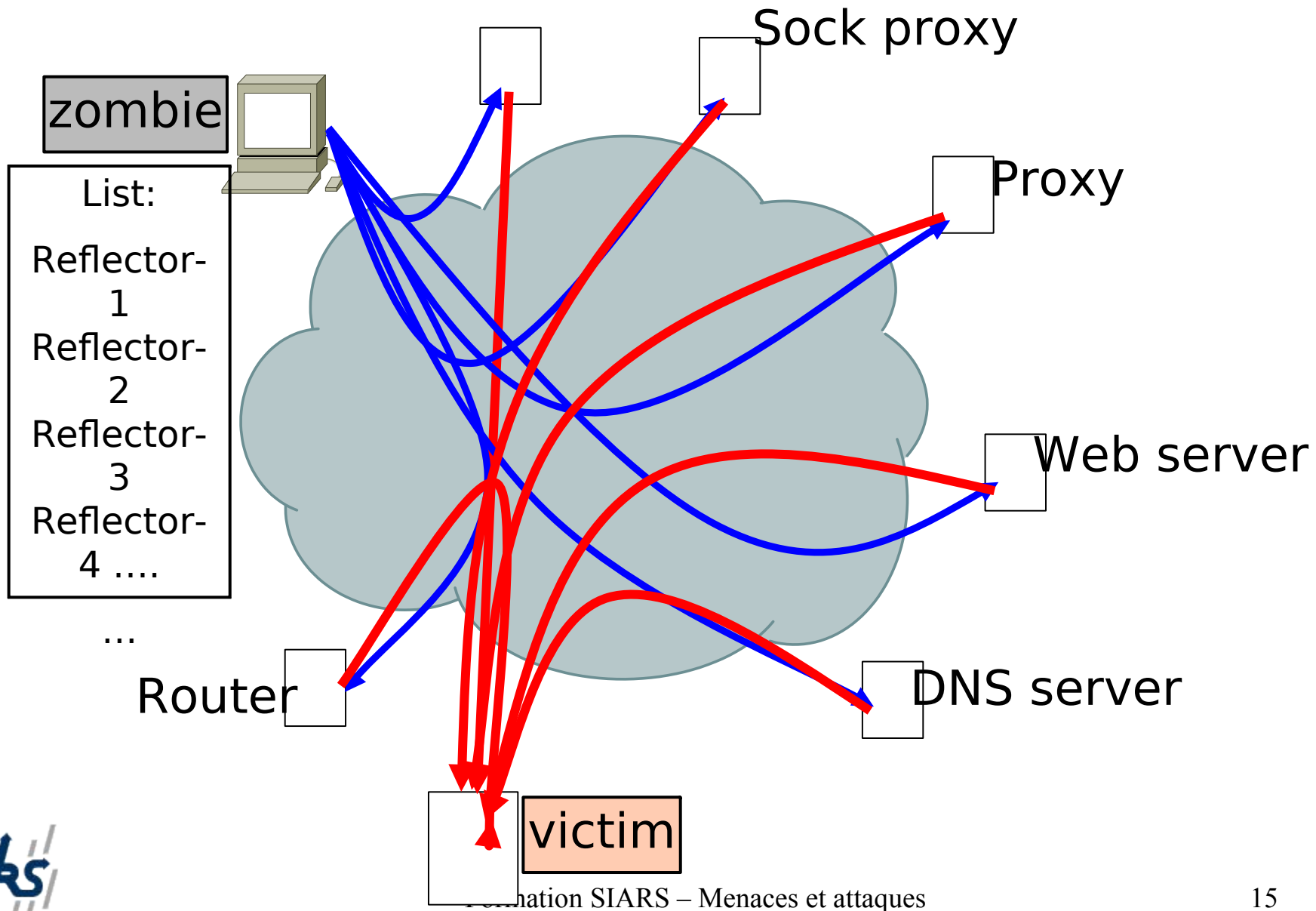
- Un des premiers CERT DDoS bulletins publiés – 09/1996
- http://www.cert.org/advisories/CA-1996-21.html

Connexions TCP semi-fermées

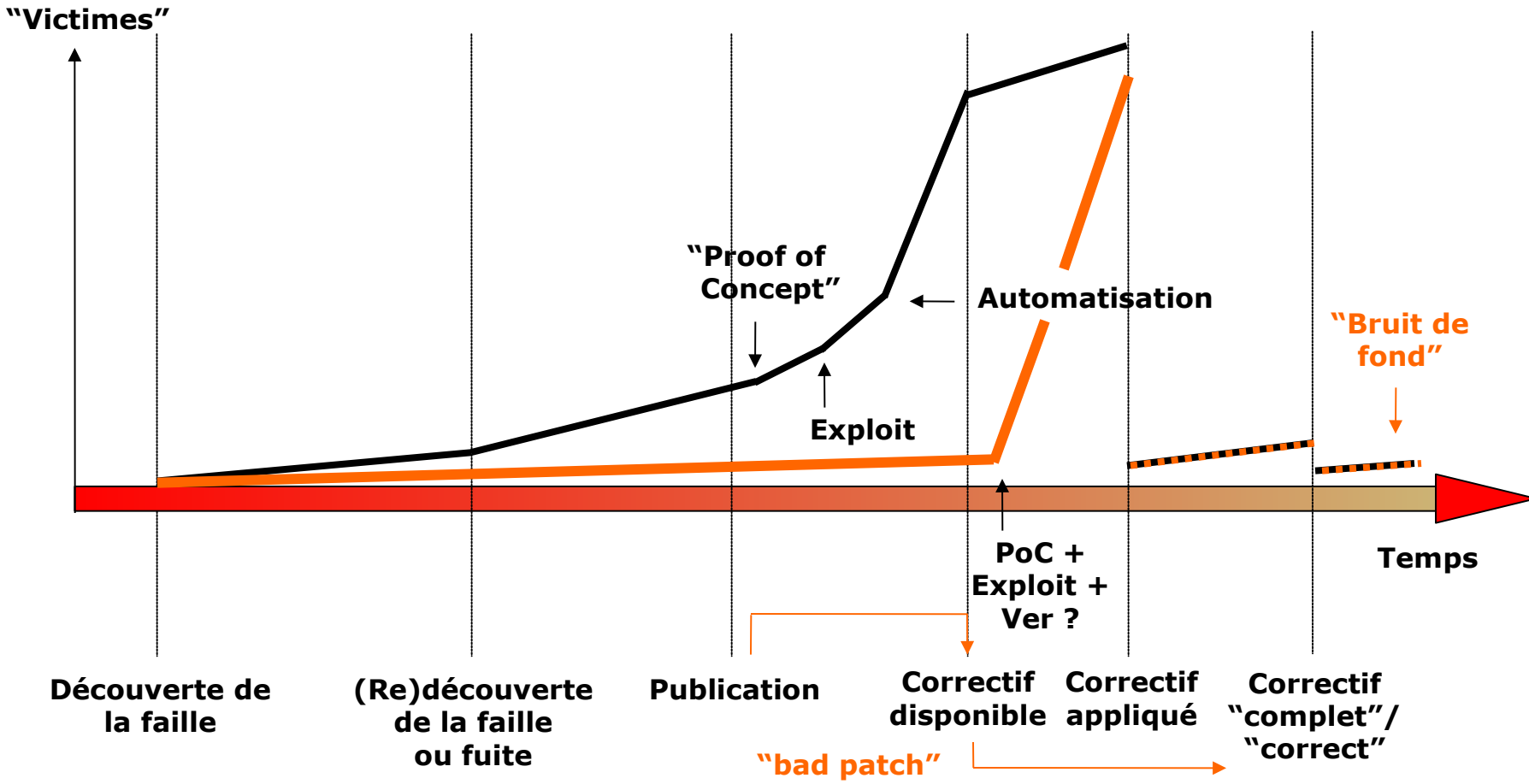


- Etablissement continu de connexions, puis abandon. L'attaquant disposant de ressources, saturant le buffer de connexions TCP du serveur
- Multiple connexions dans l'état FIN_WAIT_1 dans le serveur
- http://people.internet2.edu/~shalunov/netkill

Attaques combinées : exemple des réflecteurs

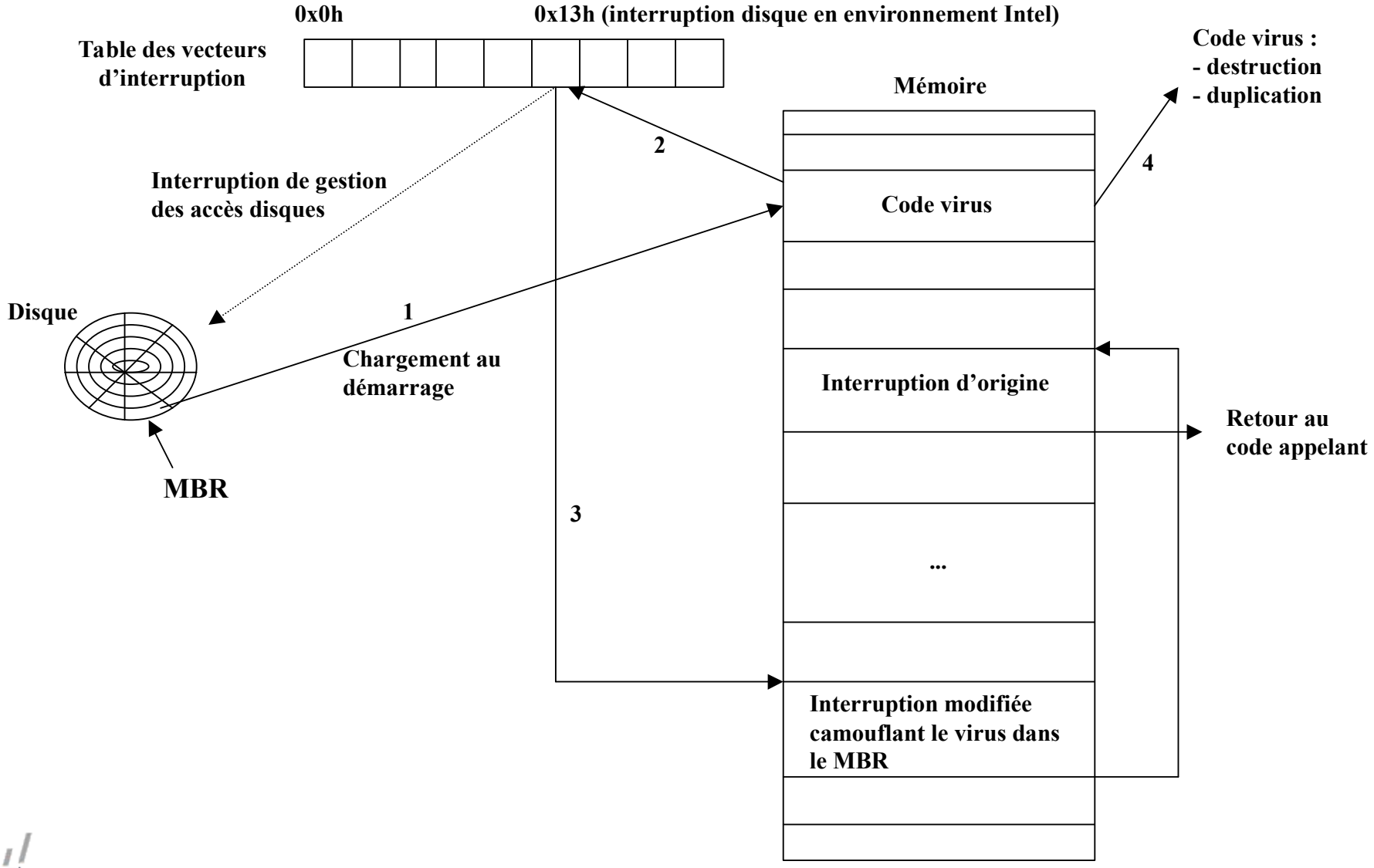


Evolution d'une vulnérabilité: le potentiel "ver"



Source : Nicolas FISCHBACH (Colt-Telecom)

Fonctionnement d'un virus



Virus et vers

- Les intentions (cachées)
  - Zombie/agent pour déni de service mutualisé (*bot)
  - Relais ouvert (open proxy)
  - Client/Serveur/Relais de messagerie (SMTP agent)
  - Calcul distribué, etc.
- Ce qui a changé
  - “Ingénierie sociale”
    - Messagerie (types “sûrs” ? ZIP, PDF, BMP, MP3: failles clients)
    - Phishing
  - Ce n’est plus que pour le “fun”
  - Collaboration : copier&coller entre les auteurs
  - Prise de conscience des différents acteurs (efforts de certains FAI “grand public”)

Motivation des attaquants

- Les activités “courantes”
  - [Virtual] Money:
    - Routeurs “BGP”
    - SPAM, botnets, relais ouverts, etc.
    - Numéros de CB, comptes eBay, etc.

- Et aujourd’hui ? L’argent !
  - “Pay or get DDoSed”
  - Vers pour diffuser du courrier non sollicité
  - Crime organisé/organisations mafieuses appliquant des techniques ancestrales à l’Internet (racket)
  - Cibles: commerce en ligne, sites de gaming, gambling, betting
  - Intelligence économique

Modes d'intrusion sur les systèmes (1/2)

- Généralement du à des problèmes de programmation :
  - Débordement de pile (buffer overflow)
    - Manque de contrôle de la taille données entrantes (saisie clavier, buffer réseau)
  - Concurrence (race condition) :
    - manque de contrôle d'accès aux fichiers temporaires
    - Utilisation des privilèges d'une application pour modifier un fichier
  - Combinaisons non testées :
    - Manque de vérification de la validité des données :
      - Sub shell (;), null character (\0), SQL injection, quotes...
      - Embarquement de code : javascript et/ou html dans les réponses formulaires HTML (XSS : cross-scripting)

Modes d'intrusion sur les systèmes (2/2)

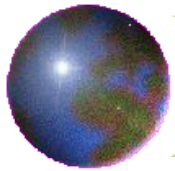
- Insertion / modification des librairies appelées dynamiquement :
  - Kernel modules
  - Shared libraries
- Combinaison de programmes :
  - Sudo
  - Accès aux devices

Quelques considérations initiales

- Configurations par défaut non adaptées
  - Pas de prise en compte de la composante de sécurité
  - Automatisation poussée
- Problème d'administration
  - Pas de correction des failles
  - Gestion inadaptée des comptes et privilèges
  - Pas de sauvegarde
  - Manque de moyens ?
- Pas de politique globale
  - Manque de méthode
  - Manque d'interêt de la direction

1)Menaces & attaques

2)Réaction face aux risques : politique de sécurité



Définitions

- Une définition de la **sécurité** peut être la suivante :

  « la sécurité peut se définir comme un état pour lequel l'information est valide, les infrastructures garantissent l'intégrité des données et il est possible de détecter les actions malveillantes »

- Une **menace** :

  Rend compte simplement de l'existence d'une activité potentiellement nuisible, activité qui peut se concrétiser ou non en terme d'attaques.

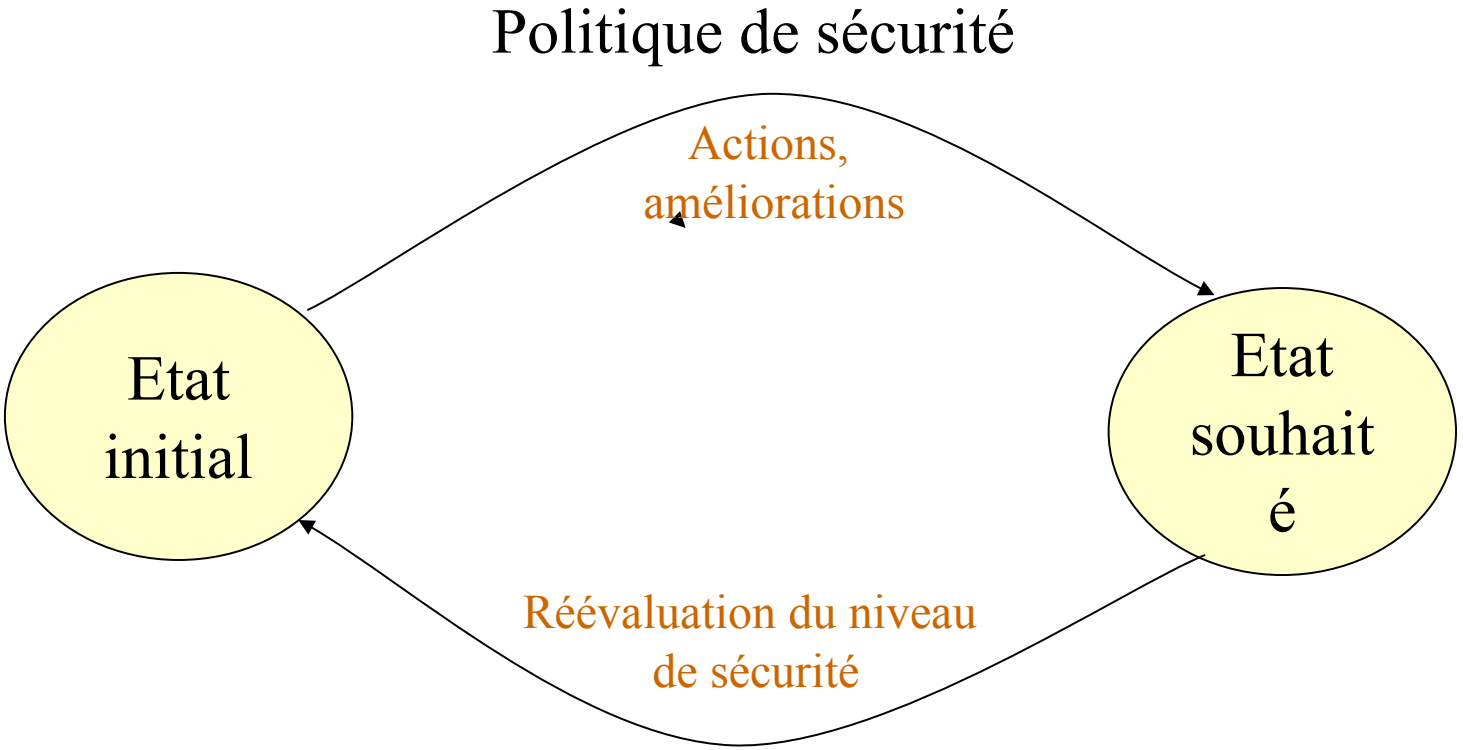
  Une menace est donc « ce qui peut arriver »

  Une attaque correspond à « ce qui arrive ».

Politique de sécurité

- Analyse des menaces
- Analyse des risques
- Application de la politique de sécurité en rapport aux menaces et risques :
  - mise en place d'infrastructures adéquates,
  - Identification et authentification des intervenants sur le système d'information,
  - Mise en place de tableaux de bords (moyens de détection, indicateurs, alarmes)
- Administration :
  - gestion de la confidentialité et de l'intégrité des données
  - disponibilité des équipements et des services
  - Suivi des tableaux de bord, adaptation
- Veille :
  - Réévaluation récursive des risques et menaces à chaque modification d'un élément du système
  - Réévaluation périodique des menaces et risques en fonction de l'évolution technologique

Cycle de vie d'un état de sécurité



Nouvelles menaces, risques, évolutions du périmètre...

Matrice des applications et services réseaux

Application	Protocole	Lieu d'hébergement	Lieu d'utilisation
Messagerie	POP3 & IMAP	Serveur SMTP labo	Interne
Messagerie	IMAPS	Serveur SMTP du labo	Interne et externe au laboratoire
Messagerie	POP3	Serveurs POP3 des FAI	Interne au laboratoire
XLAB	SMB & RDP	Serveur Windows 2000 dans réseau laboratoire	Interne au laboratoire
Partage de fichiers	NFS & SMB	Serveur NAS dans réseau laboratoire	Interne au laboratoire
Calculs	SSH	Ferme de calculs	Interne et externe au laboratoire
Serveur FTP	FTP	Serveur FTP dans réseau laboratoire	Interne et externe au laboratoire
Intranet	HTTPS	Serveur HTTP dans réseau laboratoire	Interne et externe au laboratoire

Détection d'intrusion

- Par scénarios :
  - On connait à priori les traces
  - On recherche l'occurence des traces relatives à ces signatures d'attaque,
  - Recherche de l'exaustivité pour déceler le maximum
  - Pas d'occurence des nouvelles attaques (non connues)
- Comportementales :
  - se basent sur une modification des profils de comportement (comportement d'un utilisateur, profil de la charge d'une machine, etc.)
  - Phase d'apprentissage
  - Beaucoup de faux positifs

Exemples de traces d'intrusions

- Tentatives de connexions non abouties (sur routeurs, firewall, services réseaux, PABX)
- Connexions à des horaires non habituels
- Modification de fichiers (contenus, droits, dates)
- Modification du comportement d'un système
  - Reboot, lenteur, erreurs de librairies, réponse différente
- Trous dans les traces (incohérence de traces)

Familles d'outils pour la détection d'intrusion

- Outils de « reporting »
  - Génération de traces d'activité
  - Génération de traces de tentatives
  - alertes,
- Outils d'analyse
  - En continu : charge système, nombre de connexions, disponibilité réseau et services
  - Périodique : statistiques d'utilisation, recherche de motifs
- Stockage et conservation des traces
  - Pour y faire référence ultérieurement
  - Pour remonter à l'origine d'une compromission

Bibliographie

- Cours SIARS : Menaces et attaques (O. PORTE)
- http://www.urec.cnrs.fr/cours
- http://www.ossir.org
- http://www.securite.org