

MINISTÈRE DE L'ÉCONOMIE  
ET DU COMMERCE EXTÉRIEUR

# Les mécanismes de protection face aux nouvelles attaques

**ISD 2.0**  
**08.05.2008**



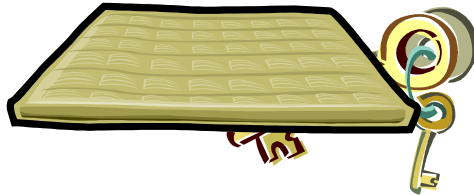


## Agenda

1. La notion du risque
2. Les 10 menaces majeures par SANS
3. Conclusion



## La notion du risque



**Vulnérabilité :**  
Clés sous le tapis



**Menace :**  
Cambrioleur essaie  
d'entrer



**Impact :** Cambrioleur  
casse l'armoire, vole de  
l'argent, crée des ennuis

$$\text{Risque} = \text{Vulnérabilité} * \text{Menace} * \text{Impact}$$



## Les vulnérabilités

Plusieurs catégories et types de vulnérabilités

- Vulnérabilités humaines
  - curiosité
  - nature avare
  - désirs romanesques
  - naïveté
  - compassion
  - arrogance
  - ...
- Vulnérabilités techniques
  - Configurations erronées
  - Contre-mesures inexistantes ou démodées
  - Logiciels non gérés et pleins d'erreurs
  - ...



## Les menaces

Plusieurs catégories et types de menaces

- Menaces générales
  - Vers, virus
  - bots
  - Hoax
  - Phishing
  - ...
- Menaces ciblées
  - Espionnage
  - Social engineering
  - Spear Phishing
  - ...



## Les impacts

Plusieurs catégories d'impacts

- Impacts financiers
- Impacts judiciaires
- Impacts sur la réputation
- Impacts sur le « savoir faire »
- Impacts sur le temps



# Les 10 plus grandes menaces pour 2008





## 1. Attaques menées depuis des sites web

Des attaques progressivement plus sophistiquées, menées de plus en plus souvent depuis des sites web dans lesquels on a généralement confiance.

**Menace** : Outils automatisés (Mpack, iFrame)

**Vulnérabilités** : - Vulnérabilités techniques; la non mise à jour des logiciels et du système d'exploitation;  
- mauvaises configurations

**Impact** : Compromission de la machine; renommée; financier,...

Référence: Bank of India

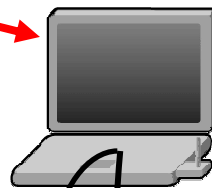


## 1. Attaques menées depuis des sites web

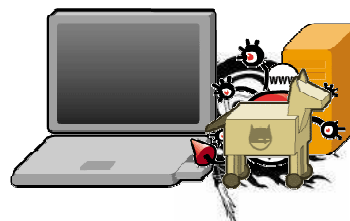
Vulnérabilités exploitées

- Microsoft (Ms06.014)
- Un 0Day pour Windows 2000 (Ms06-044)
- Faille pour XP 2k3 WebViewFolderIcon
- WinZip ActiveX
- Quicktime
- ...

Client



<iframe>



attaquant

Vulnérabilités exploitées

- Mauvaises configurations
- ...



## Contremesures

### Patch:

Activez la mise à jour automatique  
Faites les mises à jour pour **tous** les logiciels  
PSI de SECUNIA

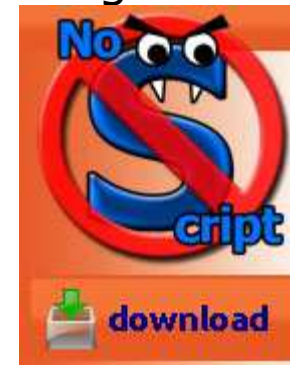


### Firewall

### Antivirus

### Browser:

Désactivation des scripts



### Configuration sites web:

[www.CASES.lu](http://www.CASES.lu) : Référentiel de sécurité pour  
applications web





## 2. Botnets de plus en plus efficaces

Les botnets deviennent de plus en plus efficaces, opaques et résistants surtout grâce à des moyens de coordination et de contrôle beaucoup plus sophistiqués.

**Menace** : Malware comme ver

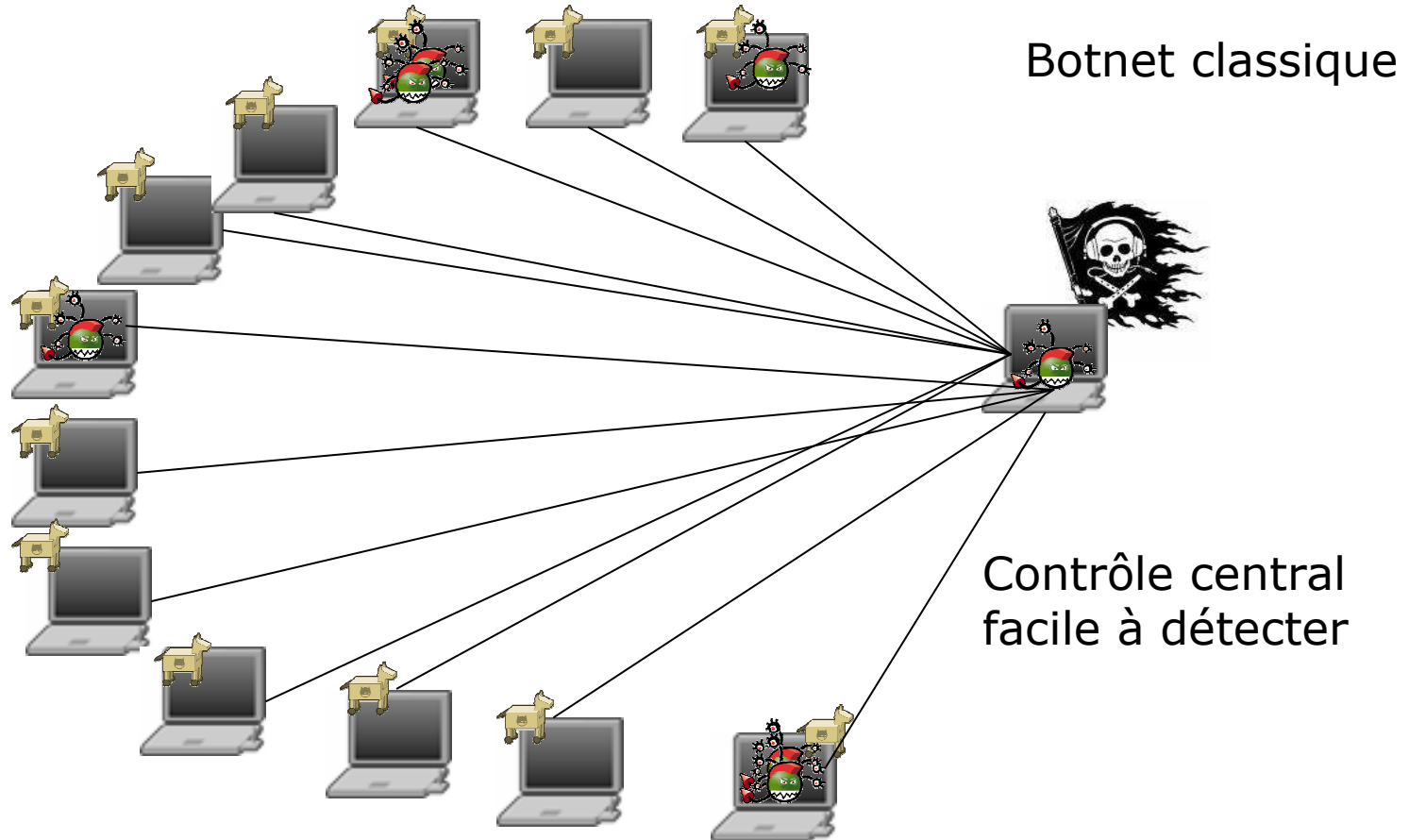
**Vulnérabilités** : Vulnérabilités techniques; la non mise à jour des logiciels et du système d'exploitation

**Impact** : compromission de la machine, judiciaire,...

Référence: Storm Worm, peer2peer, single flux, double flux

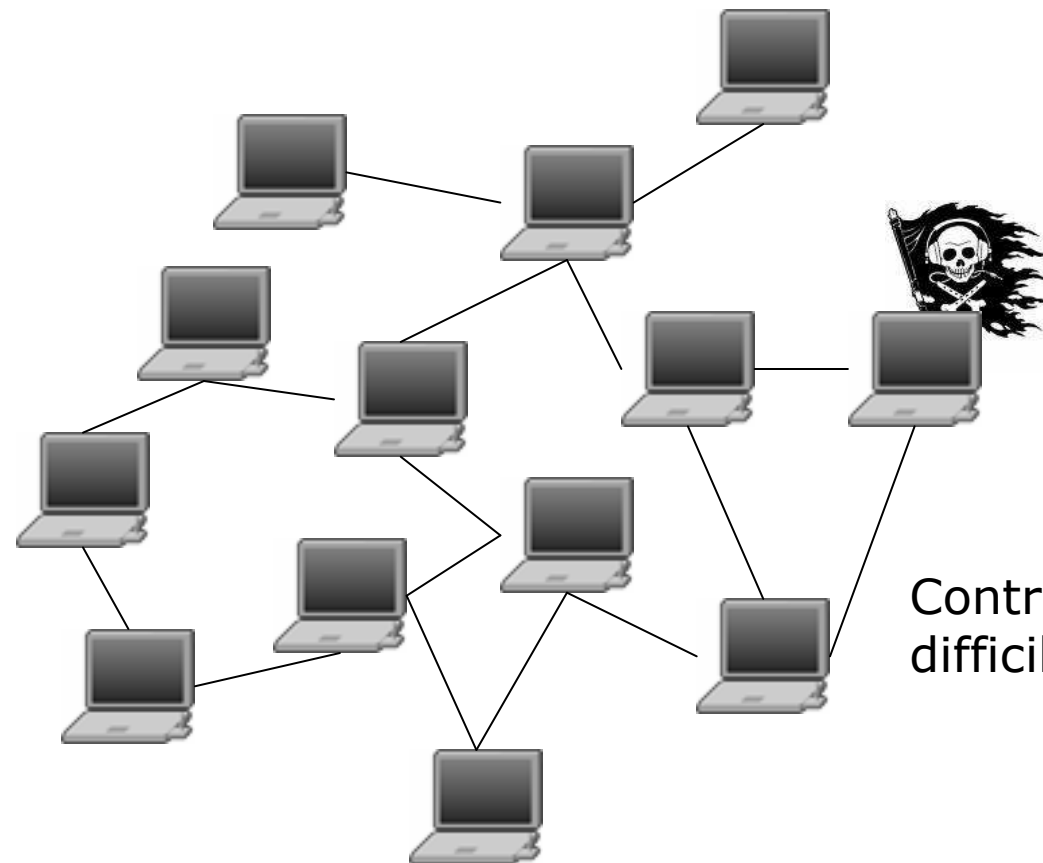


## 2. Botnets de plus en plus efficaces





## 2. Botnets de plus en plus efficaces





## Contremesures

### Patch:

Activez la mise à jour automatique  
Faites les mises à jour pour **tous** les logiciels  
PSI de SECUNIA

**Firewall**

**Antivirus**

**Sensibilisation au social engineering**





### 3. Espionnage croissant

Des efforts d'espionnage, cherchant à récupérer de grands volumes d'informations, sont de plus en plus souvent perpétrés par des organisations bien équipées, utilisant surtout des techniques du domaine du phishing.

**Menace** : Espionnage par des moyens techniques et humaines

**Vulnérabilités** : Vulnérabilités techniques et humaines;

**Impact** : compromission de la machine, financier, judiciaire,...

Référence: Espionnage perpétré aux Etats-Unis et ...



## Contremesures

### Patch:

Activez la mise à jour automatique  
Faites les mises à jour pour **tous** les  
PSI de SECUNIA



**Firewall**

**Antivirus**

**Sensibilisation au social engineering**

### Limiter les droits:

GSM : Ne laissez pas Bluetooth allumé en permanence

Classification et propriété des données

WiFi

Encryption

Authentification forte

SE	VIT	7
CO		6
RE	IMP	5
IN		4
PU	NOR	3
		2
		1



## 4. Menaces contre téléphones mobiles et VoIP

Menaces contre les téléphones mobiles, plus particulièrement contre les iPhone ou encore les Androïde-Based phones de Google et net accroissement des menaces contre VoIP

**Menace** : Malware, outils d'attaque, attaques ciblées

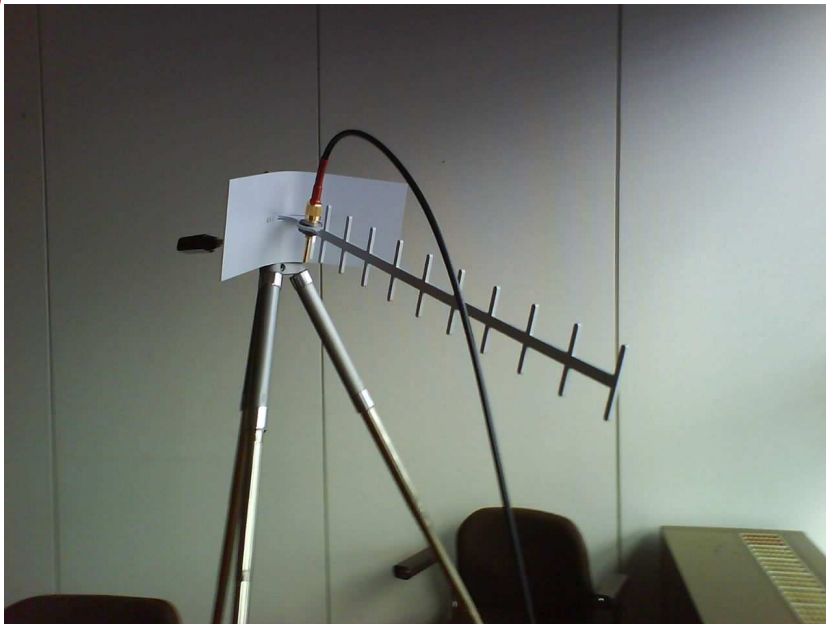
**Vulnérabilités** : Vulnérabilités techniques et humaines;  
convergence

**Impact** : compromission de données, financier, judiciaire,...

Référence: Malwares, BT-Info, ...



## 4. Menaces contre téléphones mobiles et VoIP



Envoie-moi ton carnet d'adresses

Bien sûr le voici.





## Contremesures

### Patch:

Activez la mise à jour automatique  
Faites les mises à jour pour **tous** les  
PSI de SECUNIA



**Firewall**

**Antivirus**

**Sensibilisation au social engineering**

### Limiter les droits:

GSM : Ne laissez pas Bluetooth allumé en permanence  
WiFi  
Encryption  
Authentification forte

SE	VIT	7
CO		6
RE	IMP	5
IN		4
PU	NOR	3
		2
		1



## 5. Attaques d'initiés

Des attaques d'initiés sont lancées par les employés malhonnêtes, par des consultants ou encore des sous-traitants depuis l'intérieur et depuis l'extérieur d'une entreprise.

**Menace** : Humaines

**Vulnérabilités** : Vulnérabilités techniques et humaines;

**Impact** : compromission du réseau, financier, judiciaire, réputation,...

Référence: banques, ...



## Contremesures

### Patch:

Activez la mise à jour automatique  
Faites les mises à jour pour **tous** les  
PSI de SECUNIA



**Firewall**

**Antivirus**

**Sensibilisation au social engineering**

### Limiter les droits:

GSM : Ne laissez pas Bluetooth allumé en permanence  
Classification et propriété des données  
Encryption  
Authentification forte

SE	VIT	7
CO		6
RE	IMP	5
IN		4
PU	NOR	3
		2
		1



## 6. Vols d'identité

Une nouvelle génération de vols d'identité est perpétrée par les bots qui subsistent sur des machines pendant trois à cinq mois, rassemblant des mots de passe, collectant des informations bancaires, étudiant le comportement sur le web, volant des comptes de courrier électronique fréquemment utilisés, etc.

**Menace** : Malware, Phishing

**Vulnérabilités** : Vulnérabilités techniques et humaines

**Impact** : réputation, financier, judiciaire,...

Référence: Malwares, BT-Info, ...



## 6. Vols d'identité



41 % des utilisateurs de Facebook sont prêts à révéler des informations personnelles sans contrôler d'où provient la demande



## Contremesures

### Patch:

Activez la mise à jour automatique  
Faites les mises à jour pour **tous** les  
PSI de SECUNIA

**Firewall**  
**Antivirus**

### Limiter les droits:

Encryption  
Authentification forte





## 7. Spyware de plus en plus malveillant

Le malware deviendra plus collant sur les machines cibles et il sera de plus en plus difficile de les retirer.

**Menace** : Malware, outils d'attaque

**Vulnérabilités** : Vulnérabilités techniques

**Impact** : réputation, financier, judiciaire,...

Référence: storm worm, antivirus visés



## Contremesures

### Patch:

Activez la mise à jour automatique  
Faites les mises à jour pour **tous** les  
PSI de SECUNIA



**Firewall**

**Antivirus**

**Sensibilisation au social engineering**

### Limiter les droits:

GSM : Ne laissez pas Bluetooth allumé en permanence  
Classification et propriété des données  
Encryption  
Authentification forte

SE	VIT	7
CO		6
RE	IMP	5
IN		4
PU	NOR	3
		2
		1



## 8. Applications web visées

Un haut pourcentage de sites web ont des vulnérabilités du type « cross site scripting » ou sont vulnérables à des attaques de type SQL injection ou encore d'autres vulnérabilités résultant d'erreurs de programmation.

**Menace** : Malware, attaques ciblées

**Vulnérabilités** : Vulnérabilités techniques

**Impact** : réputation, financier, judiciaire,...

Référence: storm worm, iFrame



## Contremesures

### Patch:

Activez la mise à jour automatique  
Faites les mises à jour pour **tous** les logiciels

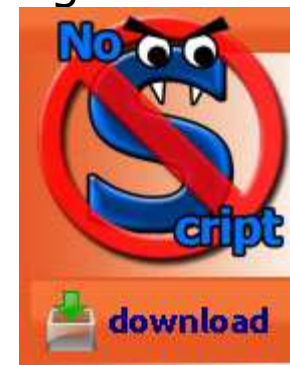
PSI de SECUNIA

**Firewall**

**Antivirus**

**Browser:**

Désactivation des scripts



### Configuration sites web:

[www.CASES.lu](http://www.CASES.lu) : Référentiel de sécurité pour applications web





## 9. Social engineering

Social engineering de plus en plus sophistiqué comprenant des attaques combinées Phishing avec VOIP et « event Phishing »

**Menace** : Humaines

**Vulnérabilités** : Vulnérabilités humaines

**Impact** : réputation, financier, judiciaire,...

Référence: VoIP, spear phishing



## Contremesures

### Antivirus

### Sensibilisation au social engineering

#### Limiter les droits:

GSM : Ne laissez pas Bluetooth allumé en permanence

Classification et propriété des données

Encryption

Authentification forte

SE	VIT	7
CO		6
RE	IMP	5
IN		4
PU	NOR	3
		2
		1



## 10. Attaques sur des chaînes d'approvisionnement

Attaques sur les chaînes d'approvisionnement infectant des dispositifs du consommateur (commandes de stick d'USB, systèmes de GPS, cadre électriques, etc...) Distribué par des organismes de confiance

**Menace** : Humaines

**Vulnérabilités** : Vulnérabilités techniques et humaines

**Impact** : réputation, financier, judiciaire,...

Référence: USB stick,



## Contremesures

### Patch:

Activez la mise à jour automatique  
Faites les mises à jour pour **tous** les  
PSI de SECUNIA

**Firewall**  
**Antivirus**





# Conclusions





## Les mesures de protection humaines

1) **Vigilance**

4) **Connaissances**

[www.cases.lu](http://www.cases.lu)



2) **Méfiance**

3) **Expérience**



## Analyse de risques

- Analyser et comprendre les menaces
- Analyser les vulnérabilités
- Analyser et quantifier les impacts
- Analyser et classier les « assets »

Agir de façon consciencieuse, réfléchiée et coordonnée.



## Management de la sécurité

- Formation
- Sensibilisation
- Politiques de sécurité
- Application des standards
- Communication et coordination
- Certification



**Merci pour votre attention**

**François Thill**