Computer Emergency Response Team
Industrie Services Tertiaire

# Forum Cert-IST 2008

## De la vulnérabilité à la crise : les processus internes des membres


Yvon KLEIN
Juin 2008

---

Cert IST Industrie Services Tertiaire

## Agenda

- De la vulnérabilité à la crise : rappels sur les menaces
- De la vulnérabilité à la crise : la réponse d(es) Cert(-IST)
- De la vulnérabilité à la crise : les processus

## Des attaques virales qui se professionnalisent … et exploitent les faiblesses

- Propagation
  - Utilisation des failles
  - Rapidité
  - Mutation
- Furtivité
  - Contournement
    - utilisation d'archives malformées
    - « bourrage » des en-têtes
- Persistance
  - Désactivation des protections
  - Rootkit
  - Résistance à la désinfection

**Se passer de la coopération de l'utilisateur final**

**Exploiter le délai de distribution des signatures**

**Contourner la détection par signatures**

**Contourner toute détection …**

**« S'incruster » si la fenêtre de vulnérabilité a pu être exploitée**

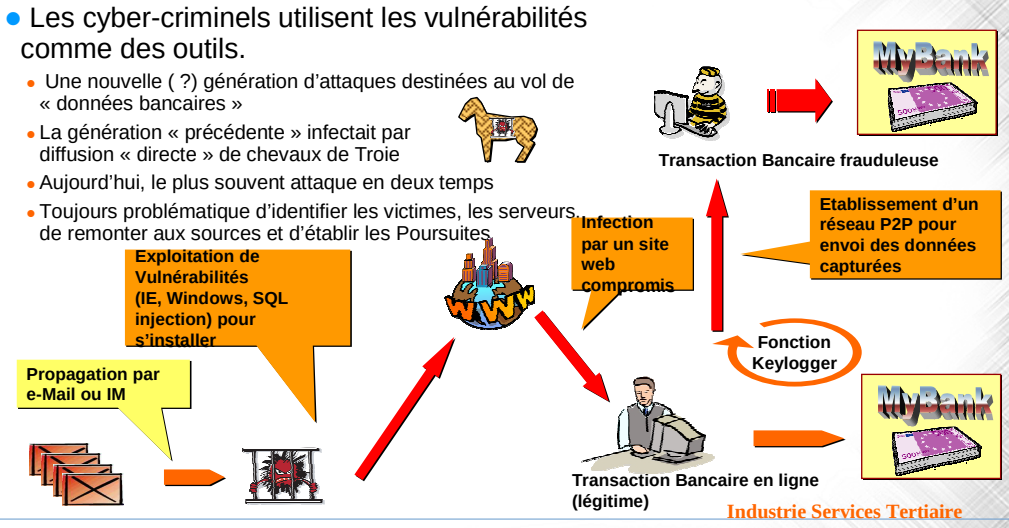
**Aujourd'hui ces caractéristiques de furtivité s'appliquent plus au botnet constitué (cf Storworm et P2P) qu'aux vecteurs de propagation eux-mêmes**

Industrie Services Tertiaire



## Attaques en fraude et phishing
## Plusieurs cas traités en coopération par les CERT

- Les cyber-criminels utilisent les vulnérabilités comme des outils.
  - Une nouvelle ( ?) génération d'attaques destinées au vol de « données bancaires »
  - La génération « précédente » infectait par diffusion « directe » de chevaux de Troie
  - Aujourd'hui, le plus souvent attaque en deux temps
  - Toujours problématique d'identifier les victimes, les serveurs, de remonter aux sources et d'établir les Poursuites




Industrie Services Tertiaire

## « Cyberterrorisme »
## Attaques en Déni de Service, espionnage industriel

- ESTONIAN DDOS
  - Un cas d'école en 2007
  - Nombreuses mises en cause de hackers « chinois » fin 2007, début 2008

Press Release
24 May 2007
http://www.enisa.europa.eu

enisa European Network and Information Security Agency

**ENISA commenting on massive cyber attacks in Estonia.**

**ENISA is commenting on the cyber attack on Estonia by clarifying its role as an (non-operational) Expert EU-advisory body.**

The Agency, as a Centre of Expertise, has no operational role and does not cover fighting cyber crime, since it is not within the mandate of ENISA. (Cybercrime is dealt with by Member State law enforcement authorities and e.g., Europol.). The Agency comments on the cyber attack on Estonia:

Events in Estonia highlight that pro-active security needs the support of Incident Response (IR) capabilities in the moments of crisis. Cyber attacks against Estonia, mainly in the form of Distributed Denial of Service (DDoS) attacks, primarily targeted the Estonian Government and police sites. Private sector banking and on-line media were also heavily targeted and the attacks affected the functioning of the rest of the network infrastructure in Estonia. As a result, the targeted sites were inaccessible outside of Estonia for extended periods in order to subdue the attacks and to maintain services within the country.

DDoS attacks are hard to mitigate and demand a lot of coordination and cooperation from various parties. CERT Estonia, established late last year, along with many local security managers and CERTs from other countries had to establish such a cooperative effort quickly to subdue the attacks. Various CERTs from Europe and beyond helped to involve the international CERT community in mitigating attacks in Estonia.

ENISA has the role to advise the European Bodies (such as the European Commission) and the Member States in NIS issues. As such, it has been promoting various good practices, including CERTs.

ENISA has been working closely with the CERT community, supports TRANSITS training and FIRST conferences and continues producing materials for promoting CERTs across Europe:

**http://www.enisa.europa.eu/pages/02_01_press_2007_05_24_ENISA_commenting_on_massive_cyber_attacks_in_Estonia.html**

Industrie Services Tertiaire



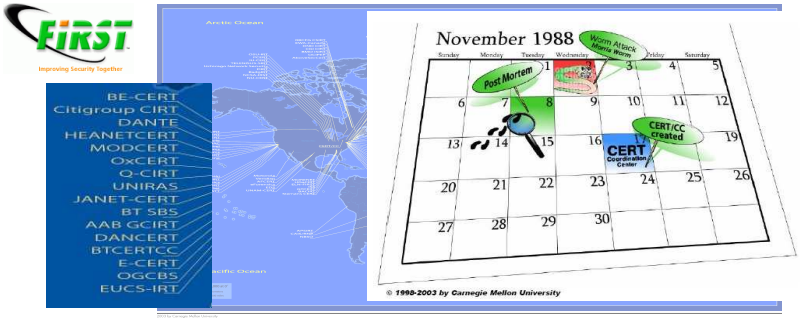
## Agenda

- De la vulnérabilité à la crise : rappels sur les menaces
- De la vulnérabilité à la crise : la réponse d(es) Cert(-IST)
- De la vulnérabilité à la crise : les processus

Industrie Services Tertiaire

## Cert-IST
## Partenaire d'un réseau National et International

- Le Cert-IST est un Computer Emergency Response Team



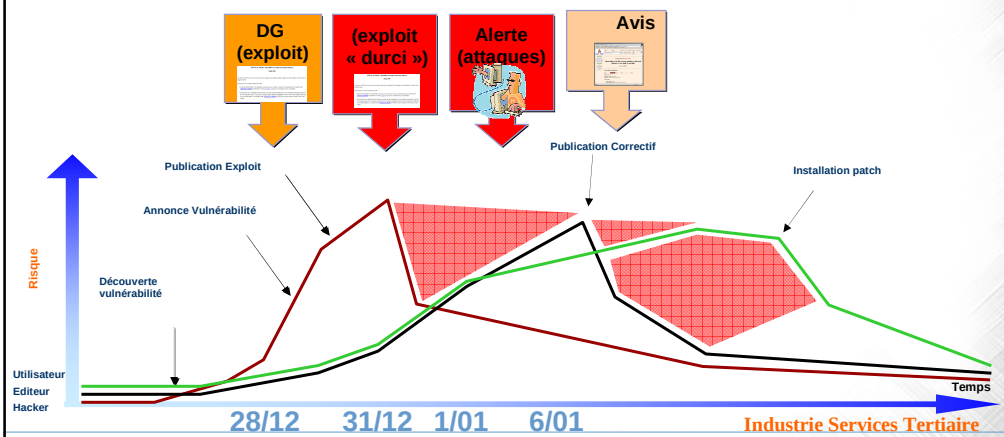

- Le FIRST identifie trois Certs en France :
  - CERT-Renater pour les universités et la recherche
  - CERT-A pour les administrations françaises
  - Cert-IST pour « la communauté Industrie, Services et Tertiaire »

Industrie Services Tertiaire



## Evolution du service : DG et Hub de Crise
## S 'adapter à des attaques de plus en plus rapides

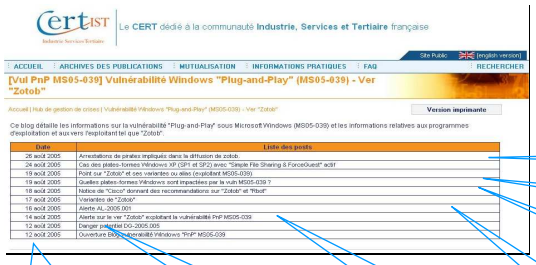
- L'attaque suit de plus en plus souvent et vite l'identification d'une faille
- Quand elle ne la précède pas … (zéro-day)




Industrie Services Tertiaire

## Le Hub de Gestion de Crise

- Anticipation et gestion des risques (prévention)
- Accompagnement jusqu'à la clôture des crises


Précisions sur les plates-formes (XP SP1)

Précisions sur les alias et variantes (Esbot, Bozori)

Notice de Cisco sur zotob et Rbot





Industrie Services Tertiaire



## Agenda

- De la vulnérabilité à la crise : rappels sur les menaces
- De la vulnérabilité à la crise : la réponse d(es) Cert(-IST)
- De la vulnérabilité à la crise : les processus

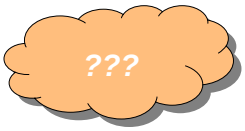
Industrie Services Tertiaire

## Processus de traitement des Avis Cert-IST Problématique 1/2

- Les vulnérabilités et ensuite ?


Menaces et Failles

Incidents


RSSI et décideurs

Utilisateurs

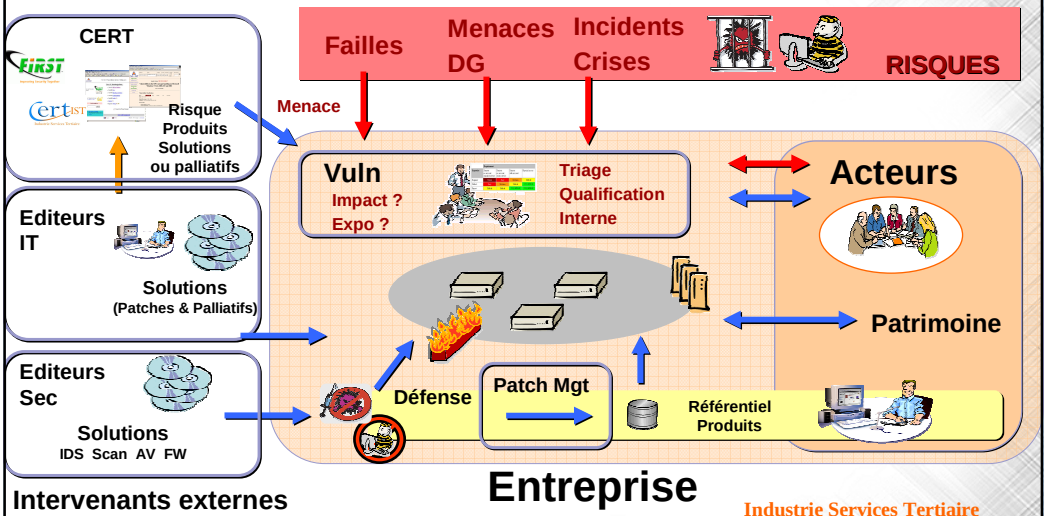
Administrateurs systèmes et réseaux

**Entreprise**

Industrie Services Tertiaire

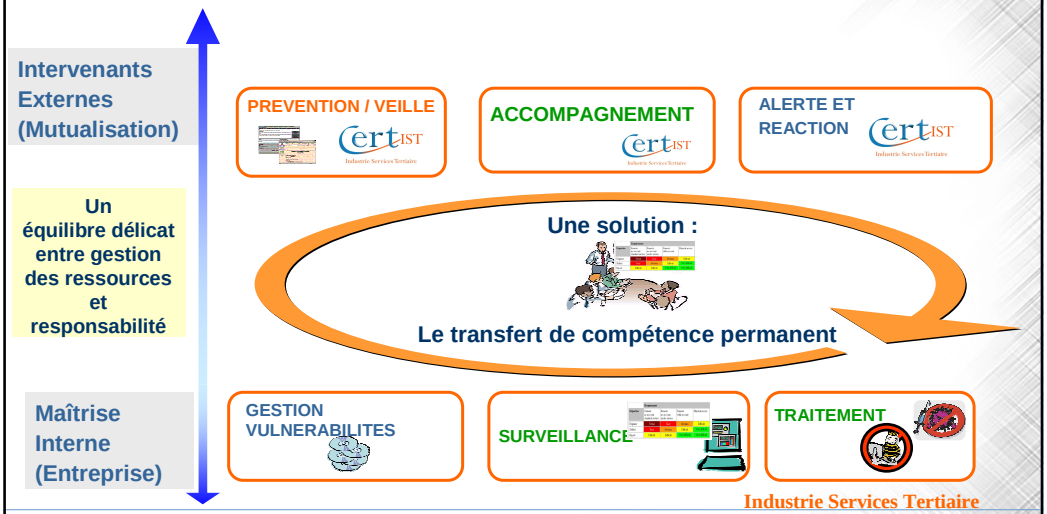


## Processus de traitement des Avis Cert-IST Problématique 2/2




Industrie Services Tertiaire

## Processus de traitement des avis : de nombreux intervenants impactés ou acteurs




Industrie Services Tertiaire



## Questions clés pour la journée

- **1/ Quel est le risque (entreprise-organisme) que représentent les failles et vulnérabilités non corrigées ?**
- **2/ Quel est, quel doit être le process pour les corriger ? (Bonnes pratiques)**
- **3/ Qu'est-ce qu'une crise ? (au sens général et/ou Sécurité des Systèmes d'Information)**
- **4/ Comment, quand, considère-t-on qu'on passe de la routine à la crise ?**
- **5/ Quel est le meilleur moyen pour éviter ou surmonter une crise ?**
- **6/ Pourquoi dois-je connaître mes cibles critiques ? (urgence, impact)**
- **7/ Quel est le rôle attendu des Cert**
- **8/ Quel est le rôle attendu des organismes de l'état (CERTA, COSSI, et surtout OCLCTIC)**

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

# Forum Cert-IST 2007

## De la vulnérabilité à la crise : les processus internes des membres


Juin 2007


## Agenda de la journée
## Matinée

| | |
|---|---|
| 9h00 | Accueil |
| | **Ouverture : Les processus internes des membres** |
| | *M. Yvon KLEIN* *Président du Cert-IST / CNES* |
| 9h30 | **De la vulnérabilité à la crise : scénarii et bonnes pratiques** |
| | *M Stanislas de MAUPEOU, chef du CERTA / COSS* |
| 10h | **De la vulnérabilité à la crise : retours d'expérience et bonnes pratiques** |
| | *Christian AGHROUM, Commissaire divisionnaire - Chef de l'OCLCTIC - Direction Centrale de la Police Judiciaire* |
| | *Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication* |
| | 10h30 **De la vulnérabilité à la crise : gestion des cibles critiques** |
| | *Pierre-Dominique LANSARD – France TELECOM* |
| | *11h15 Pause* |
| 11h30 | **De la vulnérabilité à la crise : optimiser sa réponse** |
| | *Equipe prestataire Cert-IST – (présentation des résultats de l'enquête)* |
| 12h15 | **Table ronde animée par M Christian AGHROUM, Chef de l'OCLCTIC** : |
| | « De la vulnérabilité à la crise : les bonnes pratiques». |

Industrie Services Tertiaire

## Agenda de la journée
## Mi-journée et après-midi

12h15 Table ronde

13h15 Cocktail Déjeunatoire

**Echanges sur des problématiques techniques**

14h30 Tendances et attaques : Analyse des nouvelles attaques (web, plug-in ...)

*Philippe Bourgeois* *Directeur Technique, Cert-IST*

15h20 Séquence Simulation sur une gestion de crise

Concertation façon jeu de rôle, activation d'une gestion de crise collective et partage d'expériences.
En partant d'une vulnérabilité, simulation d'un évènement aggravant avec forte propagation constatée :
avec la participation de représentants des éditeurs (Microsoft) et des partenaires.

*17h00 Clôture des débats et conclusion.*

Industrie Services Tertiaire



## Coordonnées du Cert-IST

- Coordonnées téléphoniques du Cert-IST
  - Tel : 05 34 39 44 88
    Fax : 05 34 39 44 89
    E-mail : cert [à] cert-ist.com

Attention :
Nouvelles coordonnées !

- Adresse postale de l'association
  - 9, rue du Président Allendé
    94 526 Gentilly Cedex
    France
- Adresse postale de l'équipe technique
  - C/O Alcatel-Lucent France
    8, avenue Yves Brunaud
    Parc Saint Exupéry - BP 10125
    31772 COLOMIERS Cedex
    FRANCE

Attention :
Nouvelles coordonnées !

Industrie Services Tertiaire