# La cybercriminalité au quotidien

B. Chervy - 3IL

Février 2010

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL

## Intervenants 3iL

⇨ B. Chervy
⇨ P. Naneix

⇨ 3iL Ecole d'Ingénieurs (www.3il.fr)
- Institut d'Ingénierie Informatique de Limoges
- Titre d'ingénieurs reconnu par la CTI
- Ecole internationale (France, Maroc, Cameroun)
- Réseau des écoles cs2i : Bachelor, CSI, Master Européen

⇨ Laboratoire lr2i (www.lr2i.3il.fr)
(Laboratoire de Recherche et de Ressources Informatiques)
400 systèmes d'exploitation, 40 serveurs, 11 permanents + étudiants

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL



## Introduction

- Les individus et les entreprises de toutes tailles peuvent être confrontées **au quotidien** à des **risques réels de cybercriminalité** :
  - ⇨ Vols de données bancaires (carte de paiement)
  - ⇨ Fraude sur l'achat en ligne
  - ⇨ Vols ou destructions d'informations numériques
  - ⇨ Divulgations d'informations sensibles
  - ⇨ Deffacement de site Internet
  - ⇨ Chantage et extorsion
  - ⇨ Perte de disponibilité des systèmes informatiques
  - ⇨ …
- Un tiers des entreprises subit des accès non autorisés à son système d'information et 15% sont victimes d'intrusions (FBI)
- Les fraudes et actions cybercriminelles coûteraient près de 1000 milliards de $ par an aux entreprises dans le monde (McAfee)

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL



## Quelques faits

- Les techniques communément utilisées :
  - ⇨ Phishing (arnaque par @mail ou réseau social)
  - ⇨ Malware (Virus, vers, spyware, rootkits, botnet, …)
  - ⇨ Ingénierie sociale auprès des collaborateurs
  - ⇨ Attaque et exploitation de failles techniques de postes utilisateurs
  - ⇨ Attaques et intrusions sur le système d'information
  - …
- Un phénomène en pleine expansion :

⇒ Vol de données informatiques aux entreprises = près de 760 milliards d'€ de préjudices au niveau international (étude McAfee 2008)

⇒ Revente de données bancaires piratées générant un « chiffre d'affaires » proche des 7 milliards d'€ chaque année

⇒ La découverte d'une vulnérabilité dans un système informatique se paye de 500 à 200.000 dollars

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL

## L'utilisateur et son poste pour cible

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL



## Exemple : Phishing

- Phishing : une réactivité alarmante ⇒ attaque presque temps réel

Ex : copie d'une campagne @mail PayPal + faux site piégé imitant le site de la croix rouge ⇒ mis en place en moins de 24h

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL



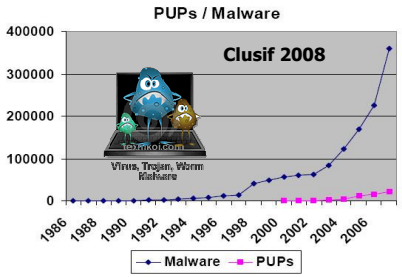
## Les « Malwares »

- Virus / Spyware / Trojans / Adware / Worm / …

- Ensemble des codes malveillants en circulation
- Espionnage, prise en main à distance, collecte d'informations sensibles, altérations diverses, …
- Vecteur d'infection : sites Internet à risque, messageries, logiciels gratuits douteux, …

Symantec : plus de 1 Million de programmes malveillants traités par son antivirus
Sophos : plus de 20000 détectés au quotidien

85% des malwares maintenant disséminés sur le Web, et non plus envoyés par e-mails
(WebRoot 2008)




© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL

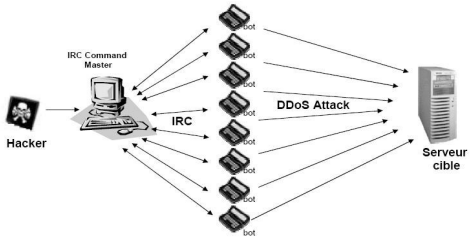


## Le cas des Botnets

- **Robots (spybot - botnet) :**

⇨ Ensemble de machines compromises (zombies), regroupées dans des réseaux « botnets » et utilisées simultanément pour des attaques

Utilisés pour :
⇨ Blocage de site Internet (DDoS)
⇨ Envoi massif Spam/Phishing
⇨ Stockages et téléchargements illicites




⇒ 5 000 machines suffisantes pour bloquer n'importe quel site « classique » dans le monde
⇒ Logiciel commercialisé sur des forums russes underground pour environ 700$
⇒ Etude IBM 2007 : de 5% à 11% des machines connectées infectées, soit entre 32 et 71 millions, appartiennent à des réseaux de machines zombies
⇒ Lancement en 2007 par le FBI de l'opération Bot Roast pour enrayer le phénomène

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL

# Quelques exemples de Botnet

- **Storm Bot / Storm Worm** :
  - ⇒ génération de vers / botnets se propageant notamment par mail ou par sites piégés ou « défacés »
  - ⇒ neutralisation de Pare-feu, installation d'un troyen, échanges en P2P
  - ⇒ estimé à 230 000 ordinateurs
- **Botnet Shadow** : réseau de 100 000 PCs démantelé aux Pays-Bas en 2008
- **Confiker.C** (alias Downadup, Kido, Shadow.base etc) - 2009
  - ⇒ réseau P2P fonctionnant sur 2 ports TCP et UDP
  - ⇒ embarque une mine de technologies de dernières générations pour s'auto-défendre (anti reverse engineering, cryptage MD6, patcher les règles de pare-feux logiciels, blocage des mises a jour Windows, contre-mesures sur les permissions NTFS, dns changer, …)
  - ⇒ MS a proposé une prime de 250 000 $ à qui dénoncerait les auteurs
  - ⇒ plusieurs 10zaines de millions de stations infectées
  - ⇒ victimes : Marine française, Ministère Britannique de la Défense, Royal Navy

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL

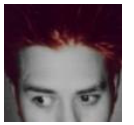

# 1° vulnérabilité : le facteur humain

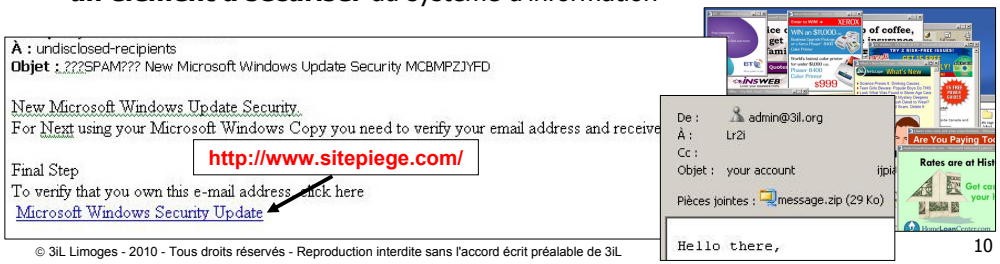
« Le véritable maillon faible de la sécurité, c'est le facteur humain »
*Kevin Mitnick*

⇨ Le risque humain prépondérant **:**

⇒ **L'utilisateur est le point le plus vulnérable des systèmes d'informations**

⇒ Le personnel de l'entreprise doit être considéré comme **un élément à sécuriser** du système d'information



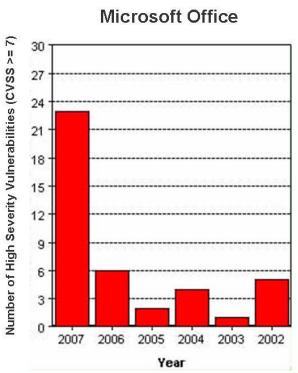



© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL


# 2° vulnérabilité : les failles techniques

- Faille de sécurité des postes utilisateurs

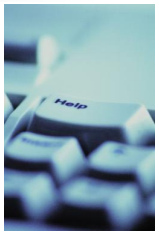
(système d'exploitation ou composantes logicielles)
- Affecte régulièrement : système d'exploitation, Navigateurs Internet, Suite bureautique, …
⇒ Permet la compromission des ordinateurs (attaque directe, exécution de malware, …)
⇒ Nécessite une veille technologique et une mise à jour permanente




Exemple :
- Fin 2009-2010 : Adobe Reader, IE8, Firefox, …
- 2009 : version 1.5.6 du CMS Joomla,
points d'accès WLAN de Cisco, …
- en 2007 : 3600 vulnérabilités affectant des logiciels

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL


# Contre mesures de sécurité

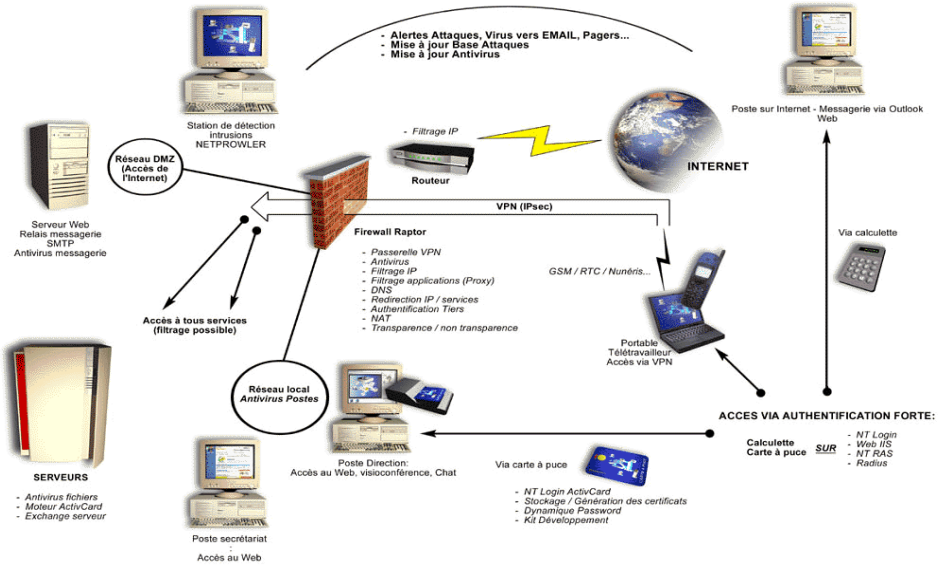


- Sécurité par management :
  Sensibilisation, formation, contrôle, charte, …
- Sécurité logique
  Politique de droits d'accès, système de sauvegarde
  Antivirus, Firewall, Moyens de cryptographie, …
  Politique de suivi et de mise à jour (systèmes, applicatifs, …)
  Système de surveillance et détection, …
- Moyens de continuité d'activité
  Politique de sauvegarde, Dispositif de secours, …
  Plan de continuité informatique, Plan de crise, …

⇒ Ensemble efficace si mis en place dans le cadre d'une **politique de sécurité informatique** réfléchie, adaptée et suivie.

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL

# Utilisation de technologies appropriées




# Conclusion

- La cybercriminalité est une composante quotidienne de l'insécurité informatique et doit être prise en compte dans toute réflexion sur la sécurité informatique.

- La meilleure solution : établir une politique de sécurité informatique globale adaptée à votre entreprise
  ⇒ démarche **complexe** mais **primordiale**
  ⇒ c'est une affaire de direction
  ⇒ permet notamment la prise en compte et la prise en charge des utilisateurs et des failles techniques

  « La sécurité d'une société est une question d'équilibre. Si la sécurité pèche par défaut, votre entreprise est vulnérable. Si elle pèche par excès, cela conduit plutôt à délaisser les affaires courantes, paralysant la croissance et la prospérité. Le défi consiste à atteindre un équilibre entre sécurité et productivité. » *Kevin Mitnick*

© 3iL Limoges - 2010 - Tous droits réservés - Reproduction interdite sans l'accord écrit préalable de 3iL