Sécurité des réseaux

Ayitic
Port-au-Prince, Haïti.
11 - 16 Août 2014

Lucien Loiseau

Les modèles d'attaques

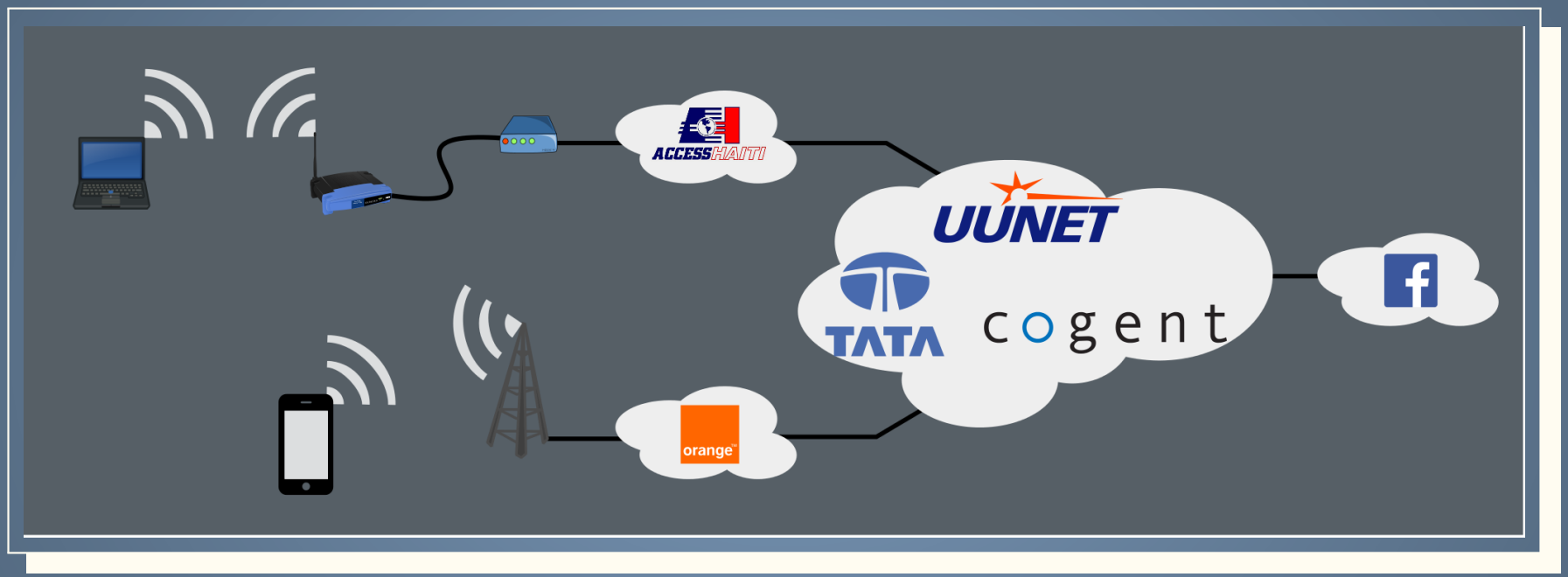
(a) Interception

(b) Interruption

(c) Modification

(d) Fabrication

Sauriez vous identifier les menaces potentielles sur cet exemple ?



Sauriez vous identifier les menaces potentielles sur cet exemple ?

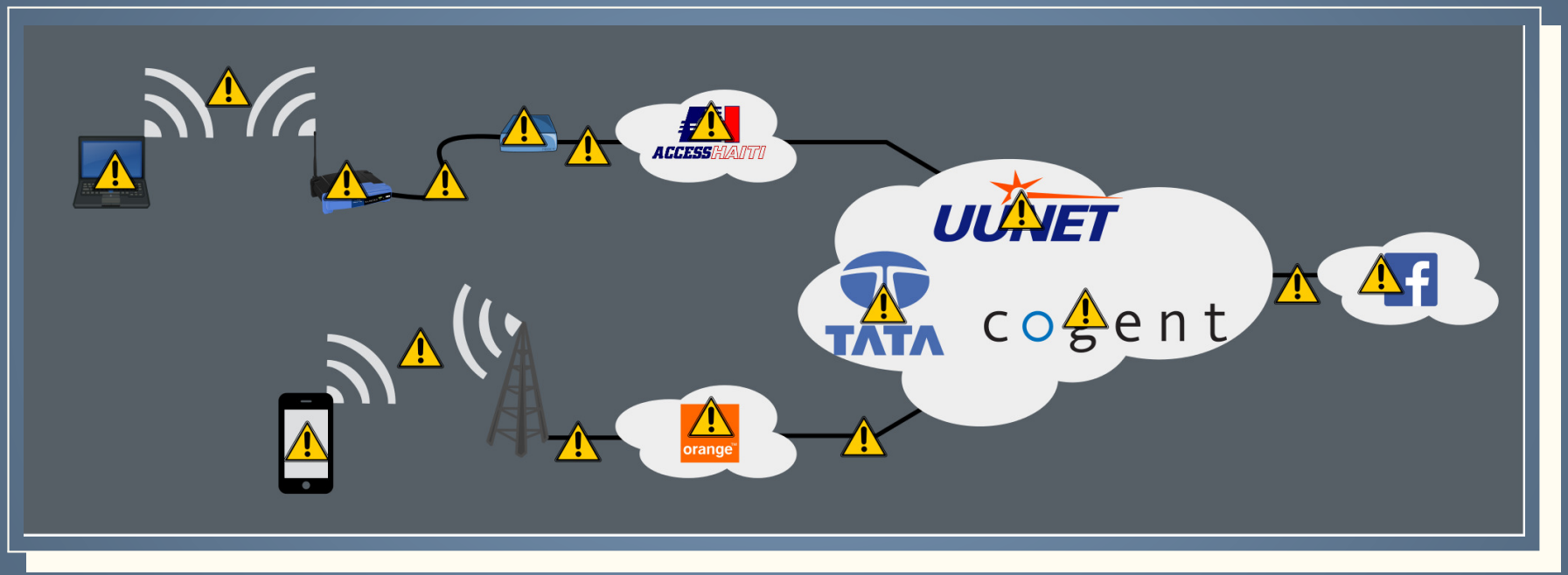
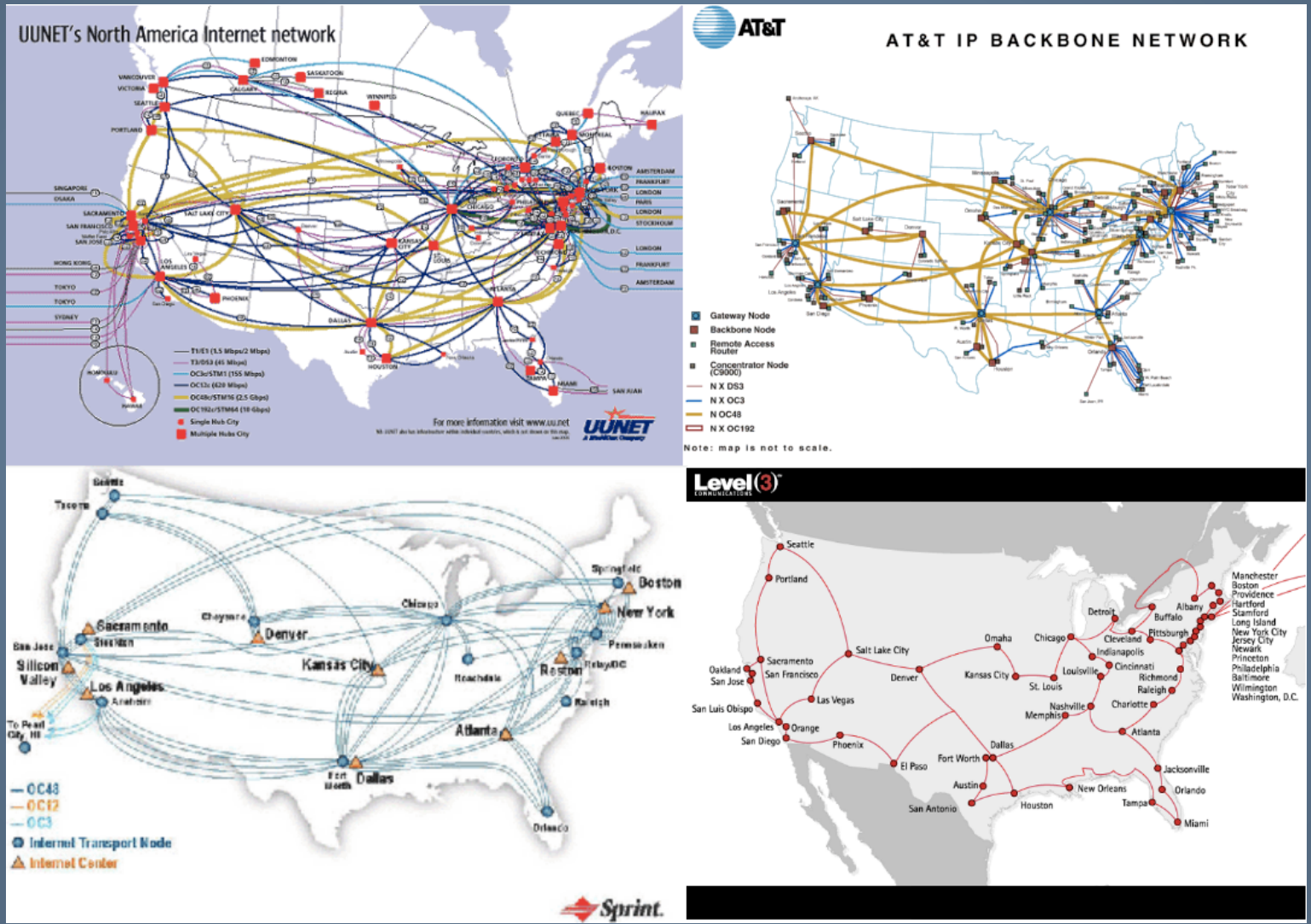


FIGURE: Lorsque vous êtes connecté à l'Internet
C'est **Internet** qui est connecté à vous !

Internet est un réseau d'interconnexion

Internet est un réseau d'interconnexion



Internet est un réseau d'interconnexion

Les éléments sur le chemin

Un routeur sur le chemin

- peut accéder au contenu des paquets
- peut les modifier
- peut les bloquer
- peut usurper l'une ou l'autre identité

Heuresement il n'y a que des professionnels de confiance sur le chemin ?

- les professionnels respectent la loi, la loi peut être mauvaise
- Internet n'a pas de frontière, la loi ne s'applique pas partout !
- Mais surtout ...

- Les attaques passives
- Les attaques actives

Les attaques passives

Principes

Une attaque passive consiste à écouter le trafic sans intéragir

- écouter des conversations GSM
- écouter une connexion wifi mal (ou peu) sécurisé
- écouter des câbles de fibre optique
- Bref tout ce qui consiste en collecte/analyse de donnée d'un medium de communication

FIGURE: Extrait du film "La vie des autres"

Les ondes électromagnétiques

Principes

- Les ondes électromagnétiques (wifi, gsm, radio, lumière, radar, etc.) se propagent dans toutes les directions
- Très pratique pour communiquer
- Très pratique pour écouter aussi !

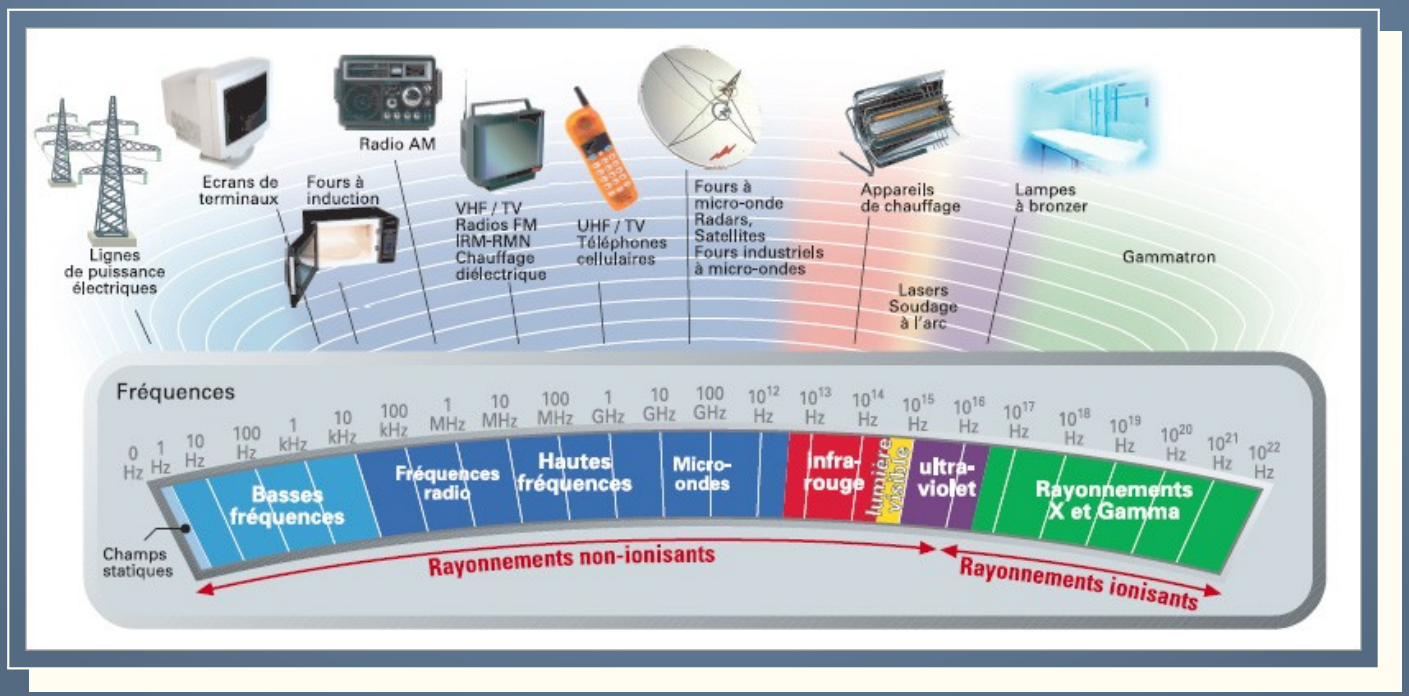


FIGURE: Différentes fréquences pour différents usages

Écouter les ondes électromagnétiques : Le chipset RTL2832U

À la base une clé TNT

- Permet d'écouter sur n'importe quelle fréquence de 24Mhz à 1850 Mhz
- Peut être utilisé pour faire de la radio logiciel (SDR)
- Coûte environ 15 euros

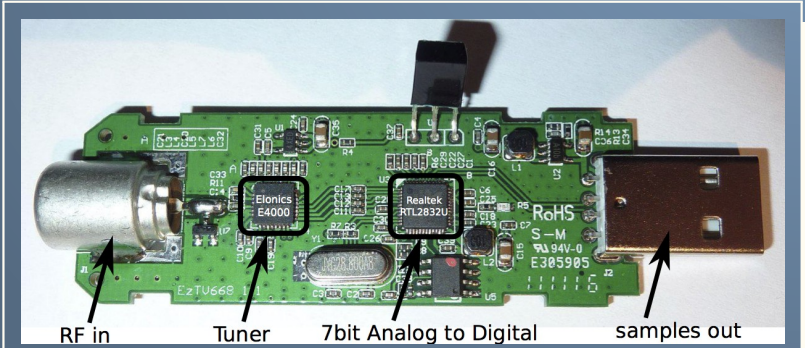


FIGURE: Différentes fréquences pour différents usages

Écouter les ondes électromagnétiques : RTL2832U

On peut faire quoi exactement avec ?

- Écouter le trafic radio amateur
- Écouter la radio FM
- scanner de radio
- Décoder les paquets APRS (radio amateur)
- Télévision Analogique Hertzienne
- Recevoir le trafic GPS
- Utiliser comme un vrai générateur de nombre aléatoire
- Communications de la police, ambulance, pompiers
- Contrôle du trafic aérien
- Balise ACARS émises par les avions
- Transmissions radio digitale (talkie walkie)
- Décoder le trafic POCSAG/FLEX pager
- Balises envoyées par les ballons météos
- trafic maritime
- Écouter les satellites et la station ISS
- Écouter (et déchiffer) du trafic GSM

etc..

Écouter les ondes électromagnétiques : Le chipset RTL2832U

Démonstration

Écouter les ondes électromagnétiques : Le programme Échelon

Au fait les USA et UK le font depuis les années 80...

FIGURE: Les radômes du réseau échelon à Menwith Hill, Yorkshire
Photo prise en novembre 2005

Échelon a fait des petits : Le DPI

DPI : Deep Packet Inspection

- Analyser en profondeur les paquets qui circulent sur les réseaux
- Utilisés par un nombre grandissant de pays (Syrie, Tunisie, Chine, USA, UK, la liste est longue)

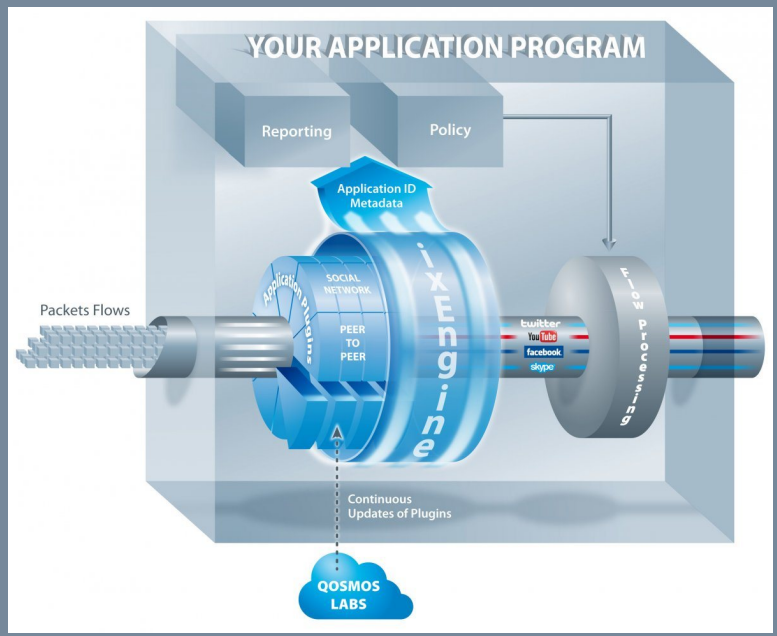


FIGURE: Une sonde DPI

Échelon a fait des petits : Le DPI

Mais ça doit prendre de la place de stocker toutes ces infos

- En effet...

FIGURE: Un datacenter de la NSA dans l'Ioha (NSA)

- Heuresement ça ne déchiffre pas les communication sécurisés
- Oui, mais...

Écoute des communication : Les metadata (1/3)

... Mais quelle information est la plus sensible ?

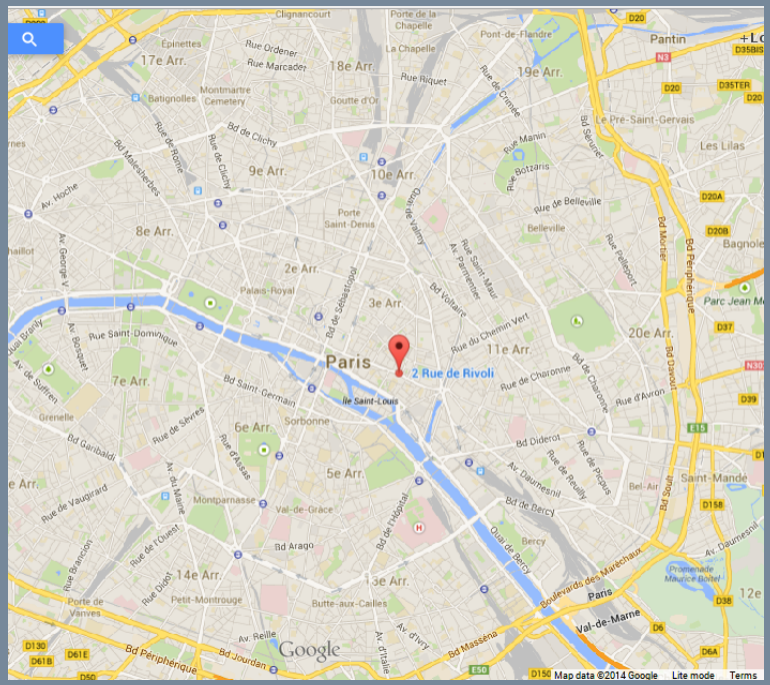
FIGURE: La donnée ?

EXIF	
Dimensions	3360 x 2680
Cropped	3360 x 2680
Exposure	1/250 sec at ƒ / 8.0
Exposure Bias	– ⅓ EV
Flash	Did not fire
Exposure Program	Aperture priority
Metering Mode	Center-weighted average
ISO Speed Rating	ISO 125
Focal Length	22 mm
Lens	12.0-24.0 mm f/4.0
Date Time Original	8/24/08 12:35:47 PM
Date Time Digitized	8/24/08 12:35:47 PM
Date Time	8/27/08 1:35:30 PM
Make	NIKON CORPORATION
Model	NIKON D200
Software	Adobe Photoshop CS3 Macintosh
GPS	45°16'48" N 122°42'26" W
Altitude	37.0 m

FIGURE: ou les meta-donnée ?

Écoute des communication : Les metadata (2/3)

La réponse est aisée...



Les métadonnées sur Internet (3/4)

Un mail chiffré... ou pas ?

```
OpenPGP: id=BF4F61A8;
        url=http://teupos.fr/~lucien/pub.key
Content-Type: multipart/encrypted;
 protocol="application/pgp-encrypted";
 boundary="QTd7Upqrmoib8Sr4R7b0gmlTfAUcADV1p"

This is an OpenPGP/MIME encrypted message (RFC 48
--QTd7Upqrmoib8Sr4R7b0gmlTfAUcADV1p
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identificat

Version: 1

--QTd7Upqrmoib8Sr4R7b0gmlTfAUcADV1p
Content-Type: application/octet-stream; name="enc
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA0ktXxs1hNOlAQf+NOBb4cH1XkRQSXolG80n8W7zySryc
XiviZ0F406/j9r2Ew74q+PmMHyBIUWjCZMtfzqND57/36jX+T
```

FIGURE: Les données sont chiffrées

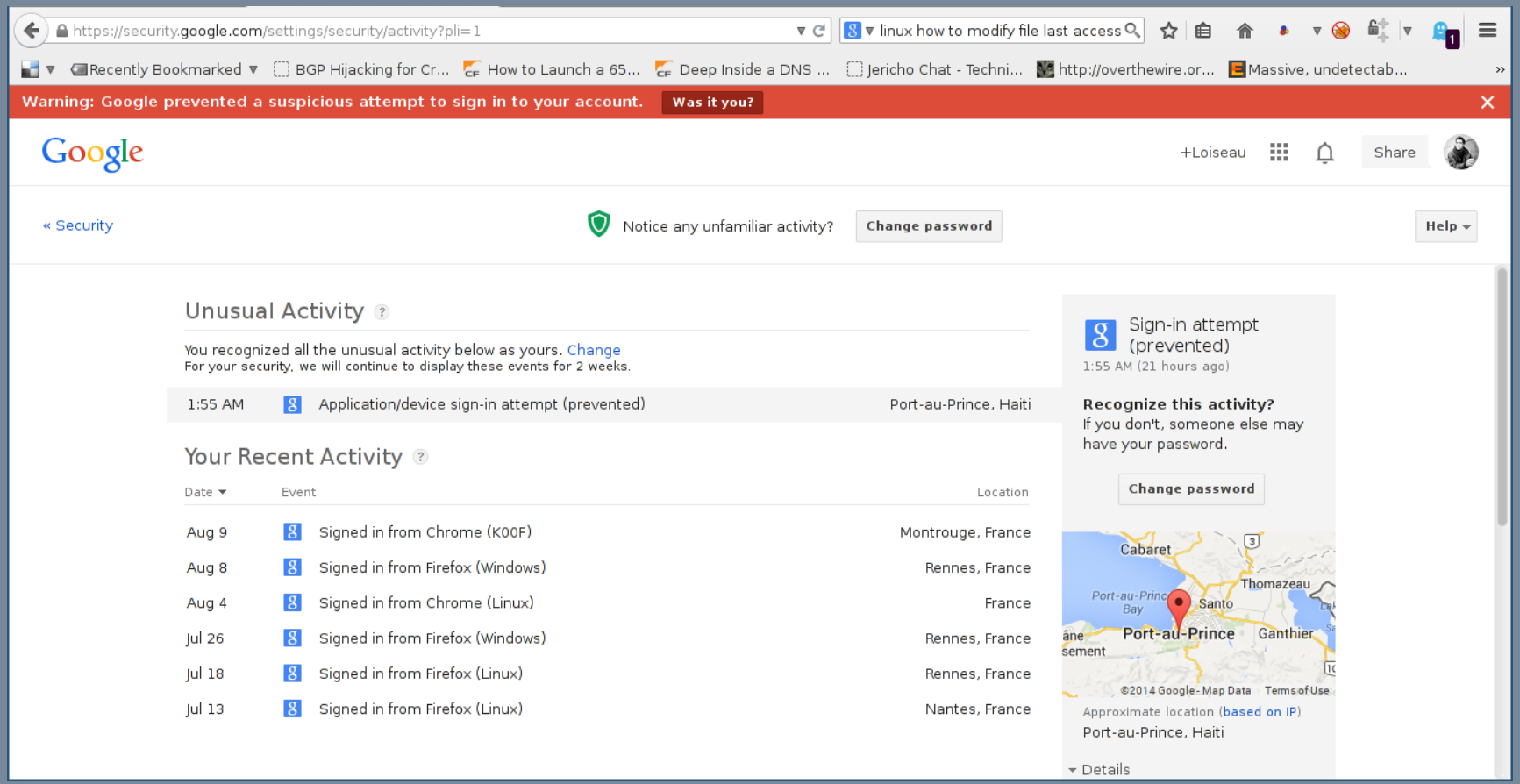
```
Delivered-To: loiseau.lucien@gmail.com
Received: by 10.216.148.138 with SMTP id v10csp187651wej;
        Fri, 8 Aug 2014 02:03:15 -0700 (PDT)
X-Received: by 10.180.74.198 with SMTP id w6mr2701694wiv.7.1407488595764;
        Fri, 08 Aug 2014 02:03:15 -0700 (PDT)
Return-Path: <lucien@teupos.fr>
Received: from mail.teupos.fr (digi00846.digicube.fr. [95.130.10.198])
        by mx.google.com with ESMTP id hv4si10670972wjb.119.2014.08.08.02.03.15
        for <loiseau.lucien@gmail.com>;
        Fri, 08 Aug 2014 02:03:15 -0700 (PDT)
Received-SPF: none (google.com: lucien@teupos.fr does not designate permitted
sender hosts) client-ip=95.130.10.198;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: lucien@teupos.fr does not designate permitted
sender hosts) smtp.mail=lucien@teupos.fr
Received: from [10.254.254.205] (unknown [10.254.254.205])
        by mail.teupos.fr (Postfix) with ESMTPSA id E67C891053B
        for <loiseau.lucien@gmail.com>; Fri,  8 Aug 2014 11:08:24 +0200 (CEST)
Message-ID: <53E49260.9080508@teupos.fr>
Date: Fri, 08 Aug 2014 11:03:28 +0200
From: Lucien Loiseau <lucien@teupos.fr>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20100101
Thunderbird/24.6.0
MIME-Version: 1.0
To: "loiseau.lucien@gmail.com" <loiseau.lucien@gmail.com>
Subject: lettre =?ISO-8859-1?Q?=E0_moi_m=EAme?=
```

FIGURE: Mais pas les méta-données

Les métadonnées sur Internet (4/4)

Ce qu'on laisse comme information quand on se connecte à un site (même chiffré)

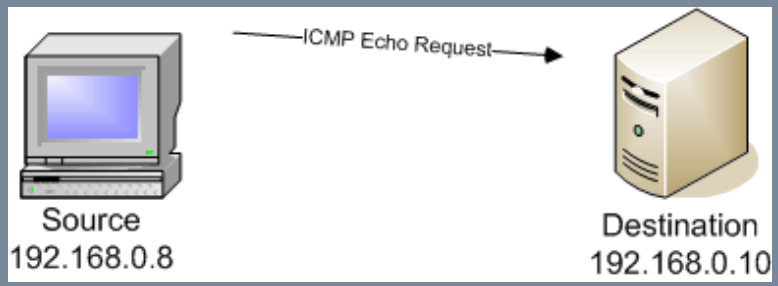
- adresse IP + port TCP source/destination (qui parle avec qui ?)
- volume et forme du trafic échange (vidéo, voix ?)
- durée de la connexion

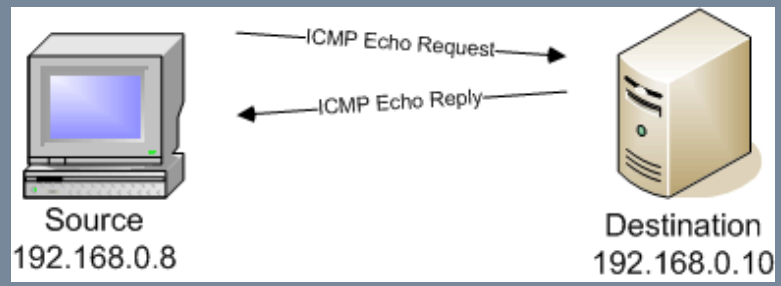


Attaques semi-passive

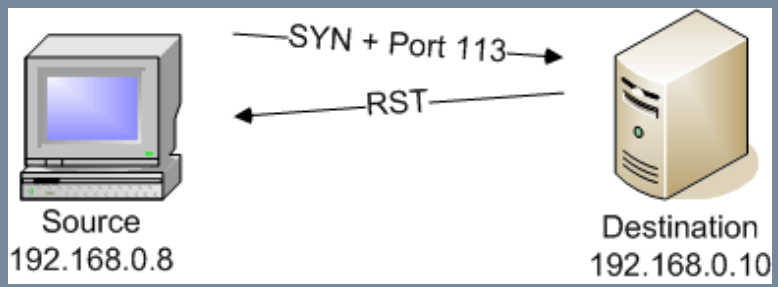
Scanner un réseau

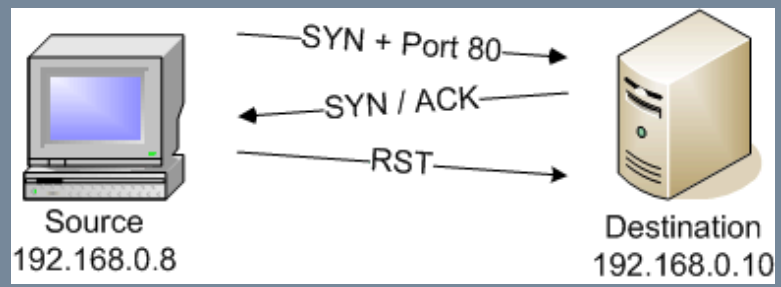
- permet de dessiner la carte du réseau
- Détecter qu'une machine est allumée





- détecter qu'un service TCP est disponible (HTTP, Mysql, FTP)





- Les attaques passives
- Les attaques actives

L'attaque Man-In-The-Middle

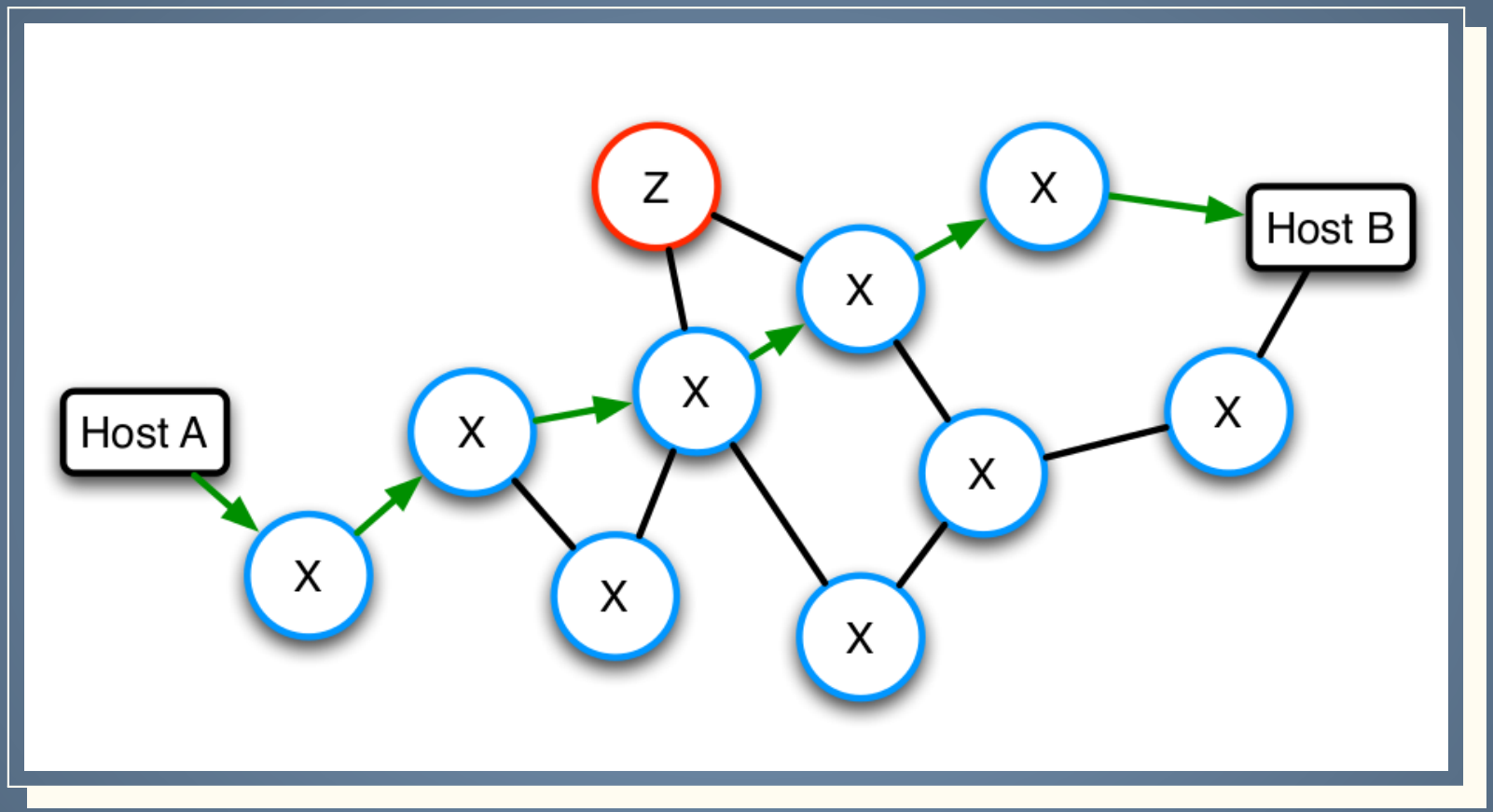


FIGURE: Connexion normal entre deux ordinateurs

L'attaque Man-In-The-Middle

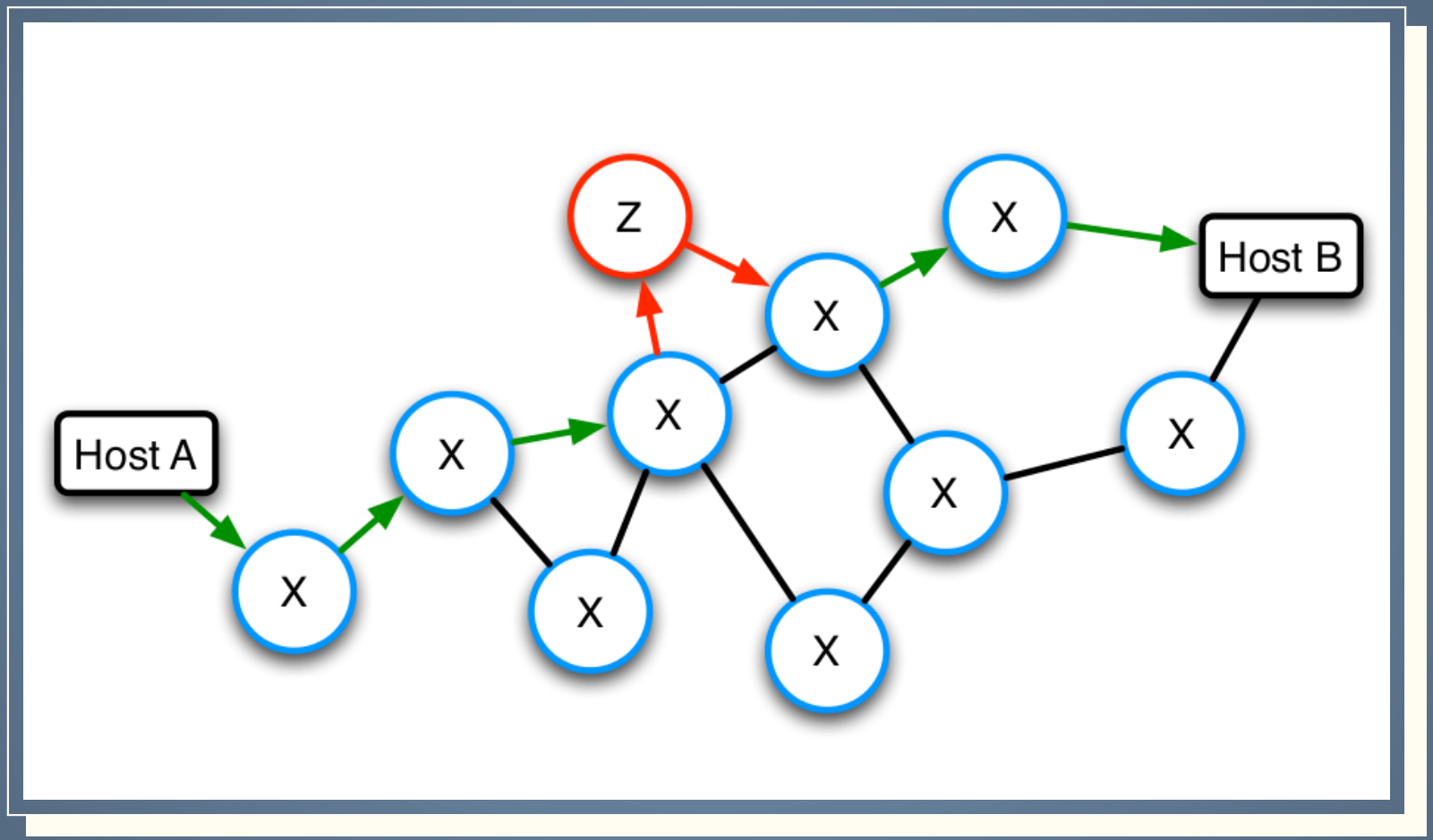
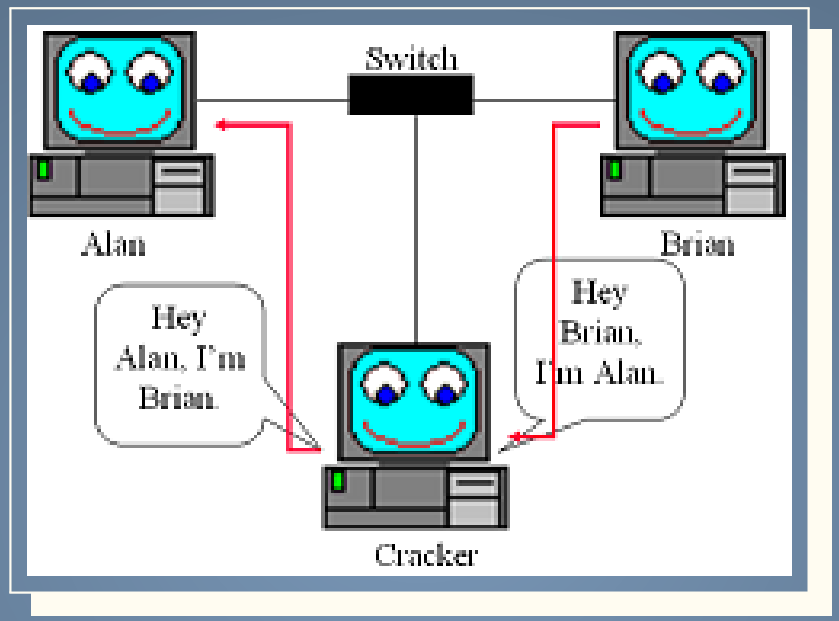


FIGURE: Connexion reroutée vers l'attaquant

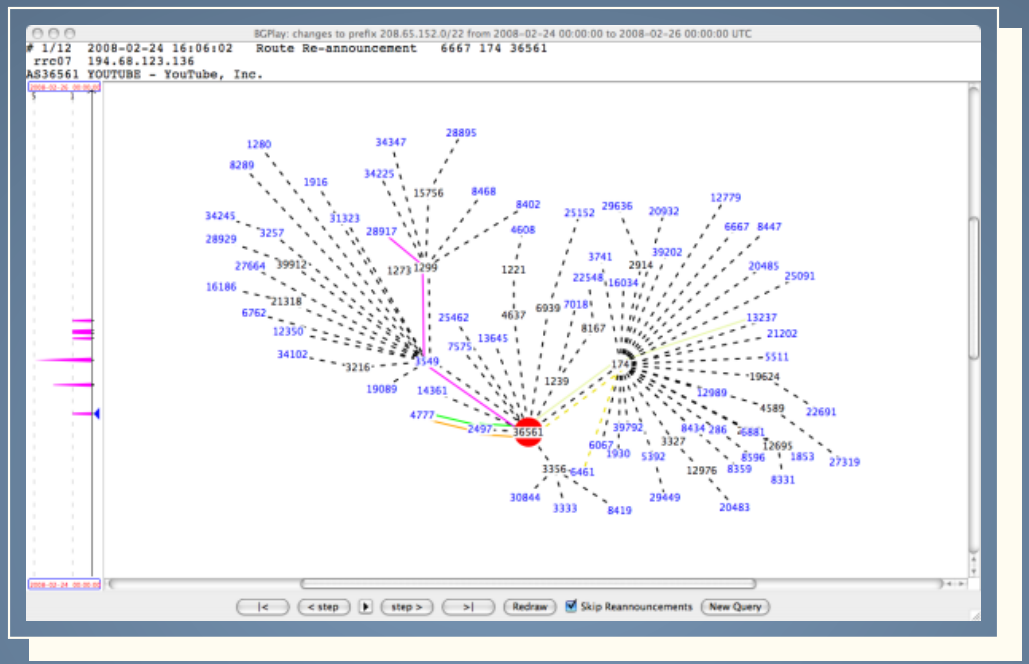
MITM sur un réseau local



ARP Cache Poisonning

- Envoie des fausses requête ARP
- Extrêmement simple à mettre en œuvre

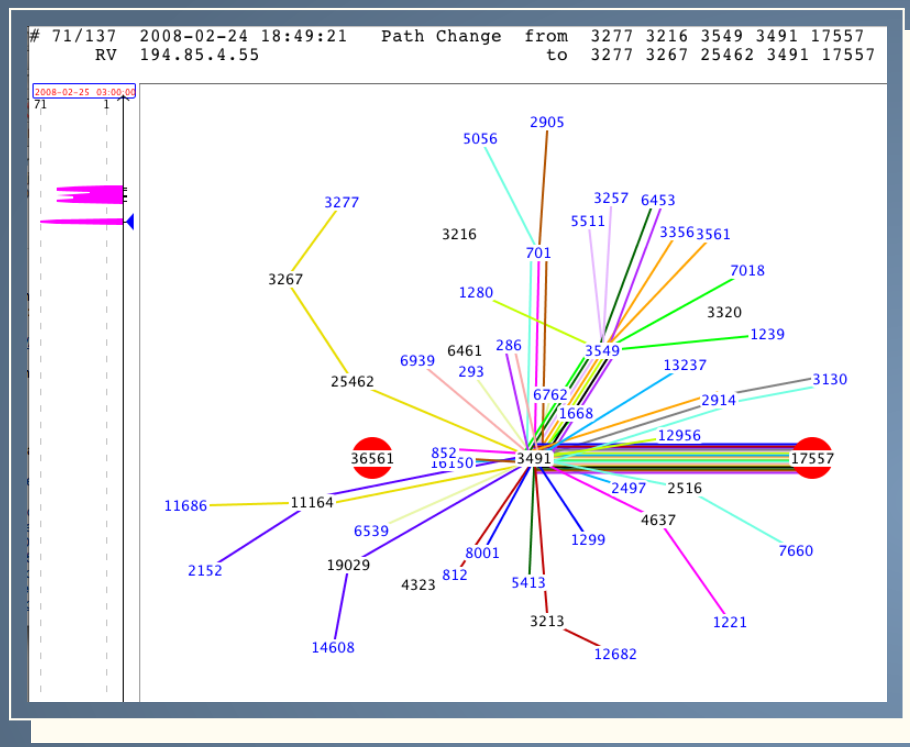
MITM sur Internet : Le Routage BGP

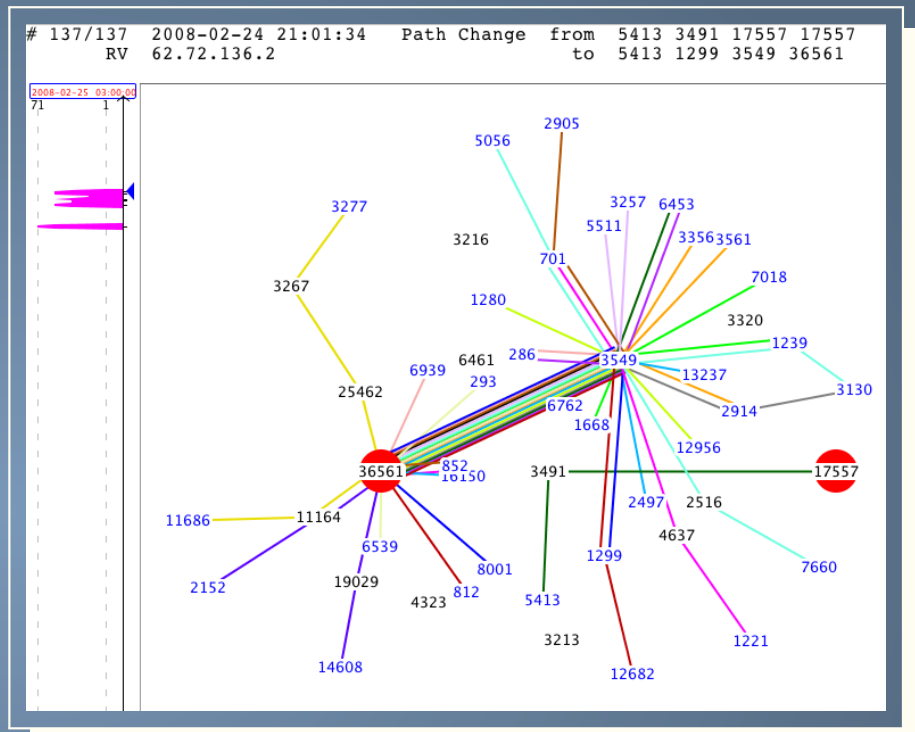


BGP : Le protocole de routage de l'Internet

- Chaque opérateur possède un numéro d'AS et un ou plusieurs préfixes IP
- Chaque AS distribue ses préfixes IP avec ses voisins
- Les préfixes IP sont diffusés de proche en proche pour former des routes
- Un routeur BGP fait confiance à ses voisins ! (il ne devrait pas toujours)

MITM sur Internet : Le Routage BGP attaqué

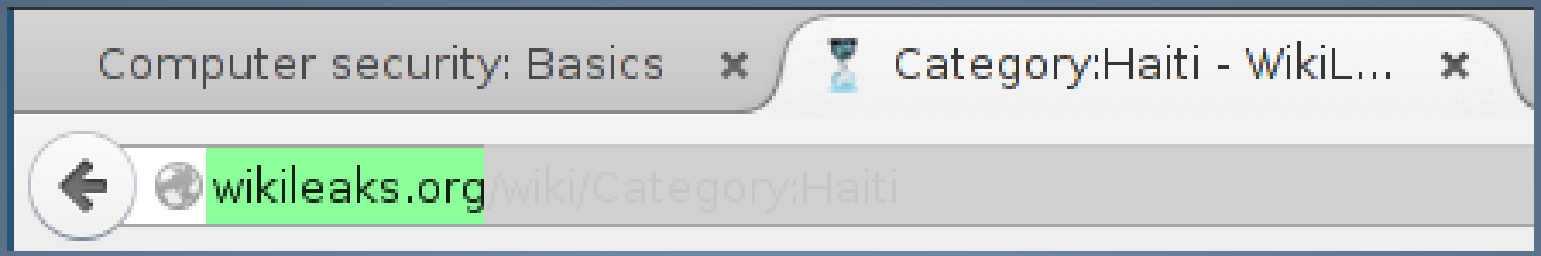




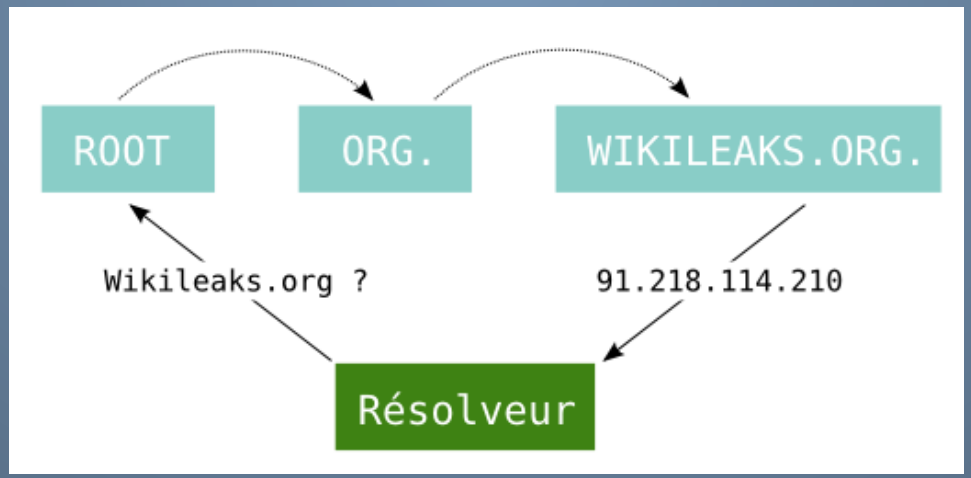
Pakistan Telecom vs Youtube

- Situation Normale : Youtube diffuse par BGP les prefixes `208.65.152.0/22`
- Situation Anormale : Pakistan Telecom diffuse les prefixes `208.65.152.0/23` et `208.65.154.0/23`
- Retour à la normale : Youtube diffuse `208.65.152.0/24`, `208.65.153.0/24`, `208.65.154.0/24`, `208.65.155.0/24`

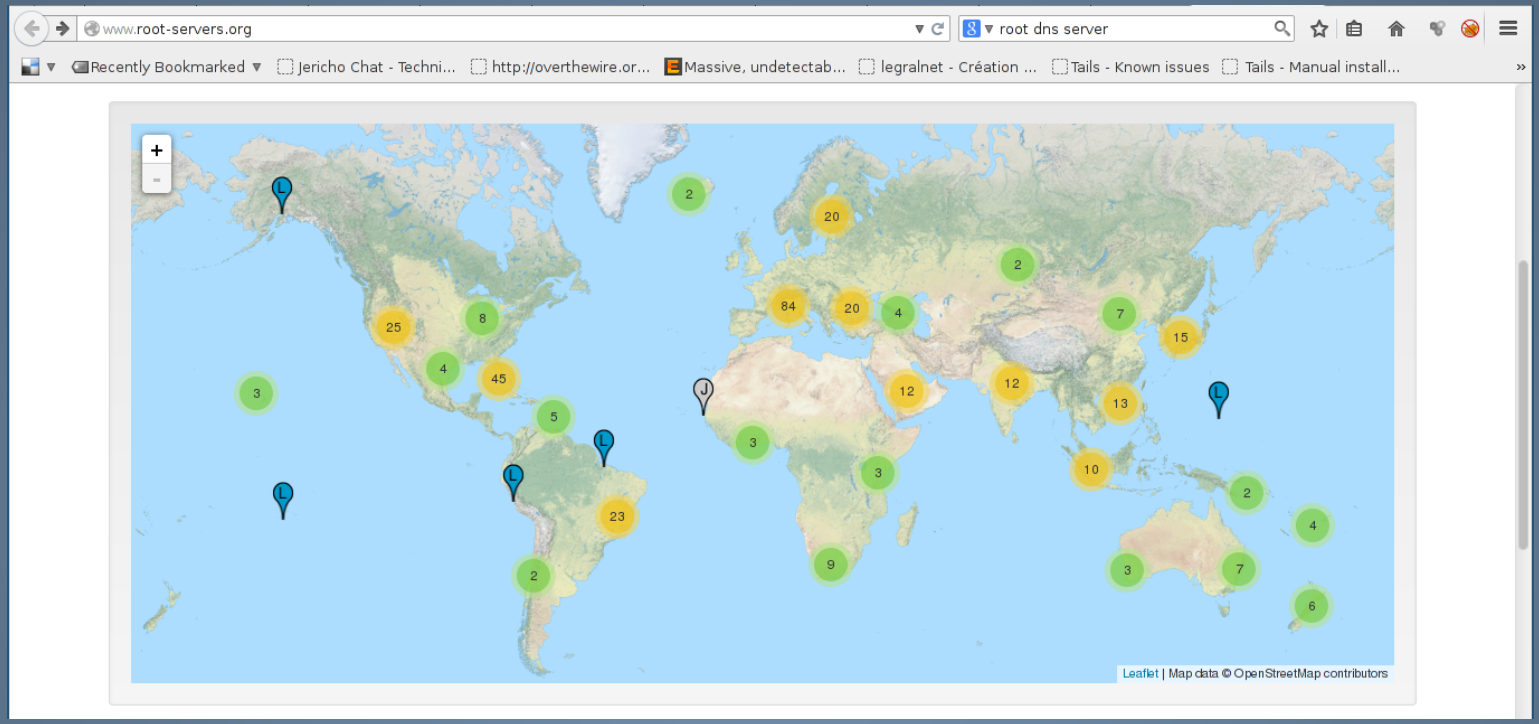
Le DNS : Domain Name System



- Le navigateur doit d'abord résoudre `wikileaks.org`
- Le DNS permet de connaître l'adresse IP associé à un nom de domaine

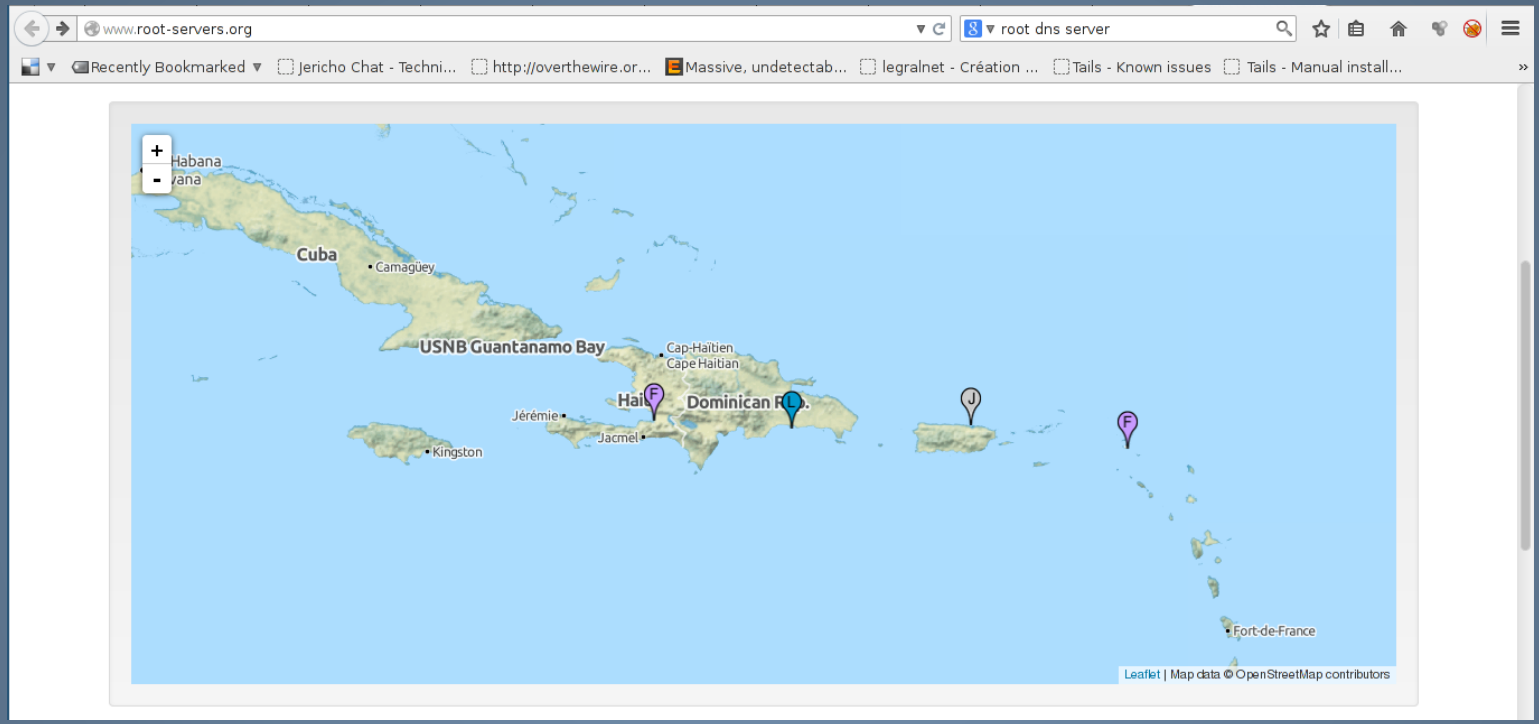


Le DNS : Domain Name System



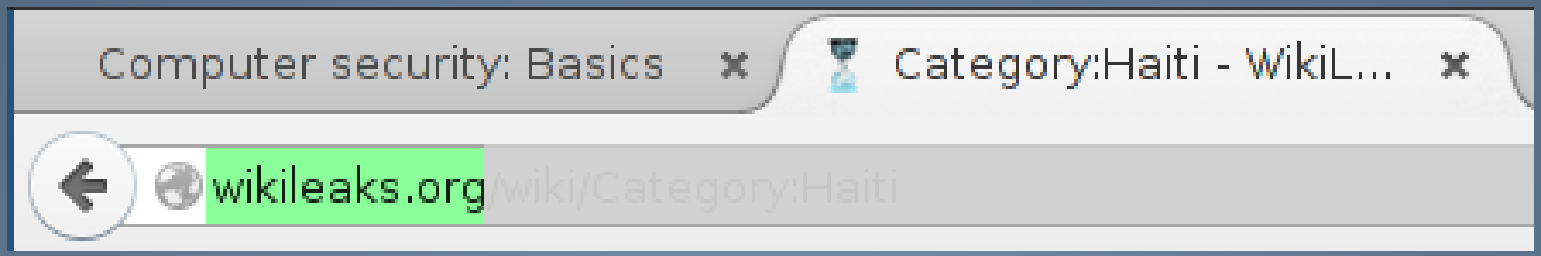
- On utilise généralement le root server le plus proche
- Il y a 386 root serveurs dans le monde...

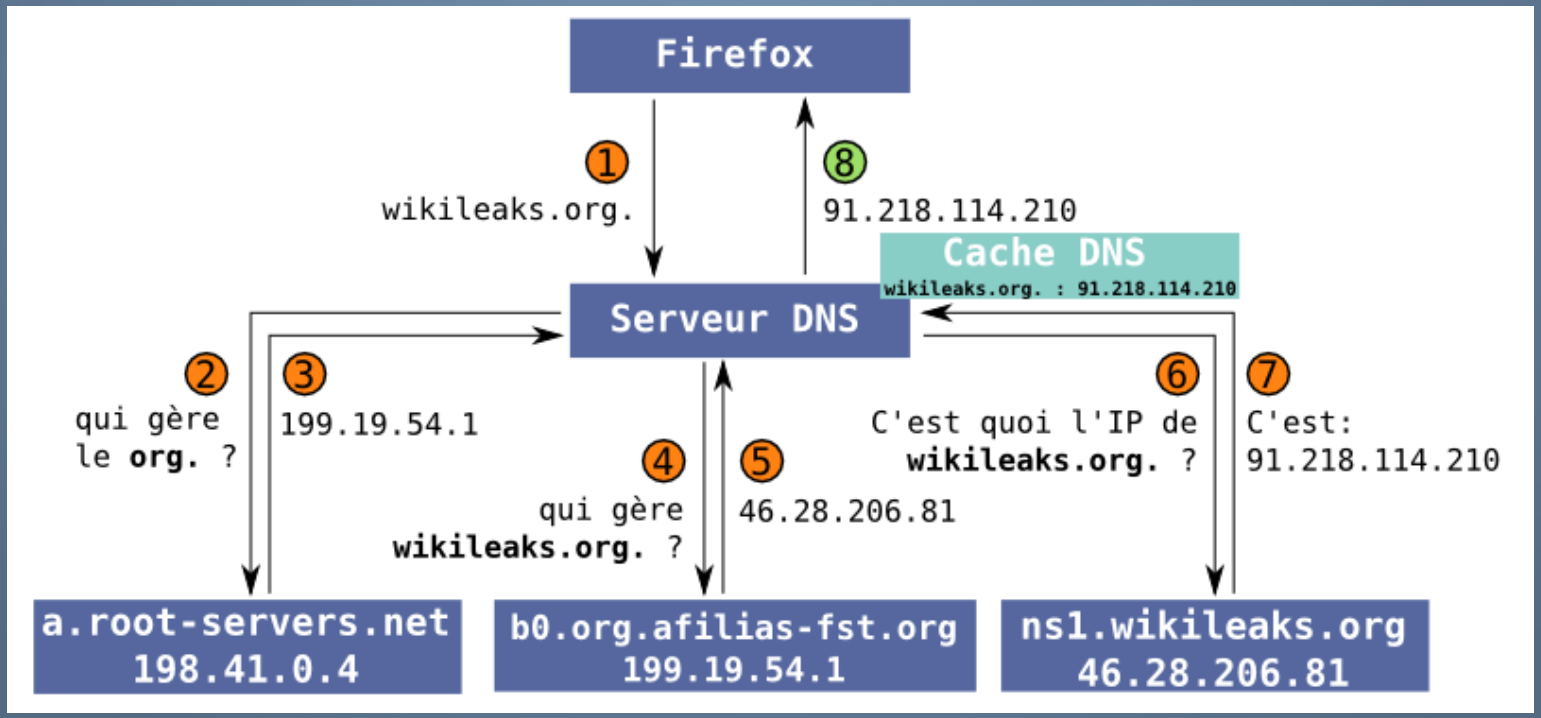
Le DNS : Domain Name System



- En général on choisit le root server le plus proche
- Il y a 386 root serveurs dans le monde...
- Dont un à Port-Au-Prince

Le DNS : Exemple d'une requête





Une requête DNS normal

On demande l'IP de facebook ?

```
[lucien@archlinux:~/work/breizh-entropy/chinanet] [mer. août 06 14:14:42]
% dig facebook.com

; <<>> DiG 9.9.2-P2 <<>> facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15595
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;facebook.com.                  IN      A

;; ANSWER SECTION:
facebook.com.           900     IN      A       173.252.110.27

;; AUTHORITY SECTION:
facebook.com.           172800  IN      NS      a.ns.facebook.com.
facebook.com.           172800  IN      NS      b.ns.facebook.com.

;; Query time: 77 msec
;; SERVER: 10.254.254.1#53(10.254.254.1)
;; WHEN: Wed Aug  6 14:20:17 2014
;; MSG SIZE  rcvd: 92
```

FIGURE: La requête à mis 77 msec

Une requête DNS normal

On étudie le chemin

```
[lucien@archlinux:~/work/breizh-entropy/chinanet] [mer. août 06 14:20:38]
% traceroute 173.252.110.27
traceroute to 173.252.110.27 (173.252.110.27), 30 hops max, 60 byte packets
 1  LIVEBOX.local (192.168.1.1)  4.926 ms  6.989 ms  10.496 ms
 2  80.10.127.82 (80.10.127.82)  46.803 ms  50.143 ms  51.876 ms
 3  10.125.253.10 (10.125.253.10)  55.835 ms  55.841 ms  58.092 ms
 4  ae44-0.nista301.Paris.francetelecom.net (193.252.159.158)  60.972 ms  63.277 ms  64.986 ms
 5  81.253.184.18 (81.253.184.18)  75.668 ms  82.843 ms  84.624 ms
 6  level3-1.GW.opentransit.net (193.251.255.80)  80.476 ms  35.577 ms  47.298 ms
 7  vl-3501-ve-115.csw1.London1.Level3.net (4.69.166.129)  118.094 ms vl-3504-ve-118.csw1.Londo
.csw1.London1.Level3.net (4.69.166.129)  125.047 ms
 8  ae-57-112.ebr1.London1.Level3.net (4.69.153.117)  127.375 ms ae-59-114.ebr1.London1.Level3.
evel3.net (4.69.153.117)  138.044 ms
 9  * * *
10  ae-61-61.csw1.Paris1.Level3.net (4.69.161.78)  153.080 ms ae-81-81.csw3.Paris1.Level3.net (
t (4.69.161.82)  156.543 ms
11  * * *
12  ae-44-44.ebr2.Washington1.Level3.net (4.69.137.62)  116.659 ms ae-41-41.ebr2.Washington1.Le
gton1.Level3.net (4.69.137.62)  125.169 ms
13  ae-62-62.csw1.Washington1.Level3.net (4.69.134.146)  123.184 ms ae-82-82.csw3.Washington1.L
ington1.Level3.net (4.69.134.150)  127.111 ms
14  ae-4-90.edge3.Washington4.Level3.net (4.69.149.210)  138.804 ms ae-2-70.edge3.Washington4.L
ngton4.Level3.net (4.69.149.146)  156.305 ms
15  4.53.116.78 (4.53.116.78)  154.168 ms  158.130 ms  161.276 ms
16  be2.bb02.iad3.tfbnw.net (31.13.24.8)  144.751 ms  147.460 ms be3.bb01.iad3.tfbnw.net (173.2
17  ae12.bb03.frc3.tfbnw.net (31.13.24.88)  140.521 ms be18.bb01.frc3.tfbnw.net (31.13.24.32)
635 ms
18  ae89.dr03.frc1.tfbnw.net (173.252.65.97)  138.350 ms ae88.dr02.frc1.tfbnw.net (173.252.64.1
1)  136.680 ms
19  * * *
20  * * *
21  edge-star-shv-13-frc1.facebook.com (173.252.110.27)  134.040 ms  133.173 ms  133.131 ms
```

FIGURE: traceroute d'une connexion à Facebook

Une requête DNS normal

On étudie le chemin

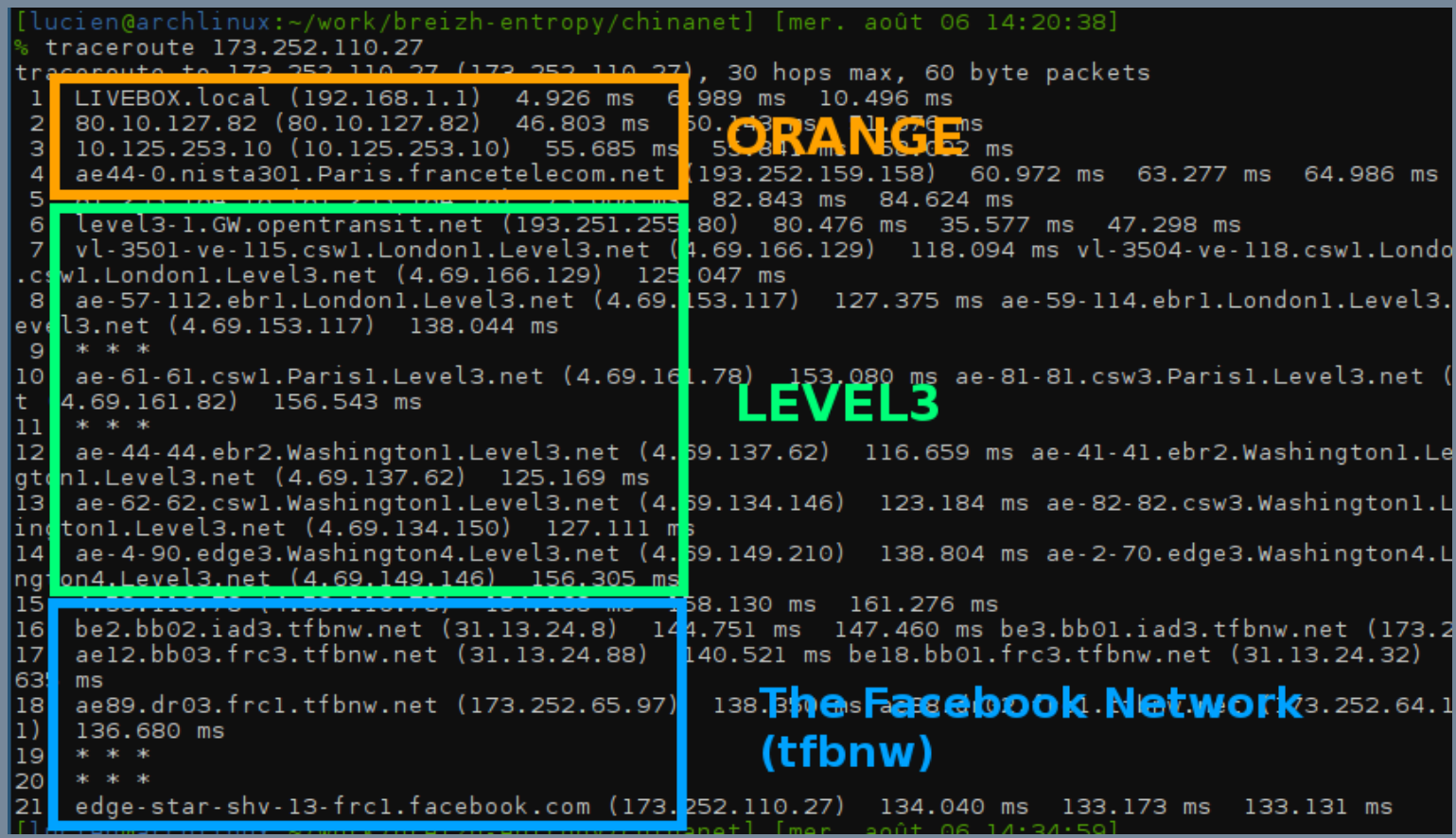


FIGURE: Chemin normal, composé de plusieurs opérateurs (Orange -¿ Level3 -¿ Facebook

Une requête DNS anormale : Les DNS menteurs chinois

Si on demande l'IP de facebook depuis la chine ?

```
; <<>> DiG 9.9.2-P2 <<>> facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4684
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;facebook.com.                  IN      A

;; ANSWER SECTION:
facebook.com.           4320    IN      A       159.106.121.75

;; Query time: 4 msec
;; SERVER: 218.30.19.50#53(218.30.19.50)
;; WHEN: Wed Feb 12 08:05:58 2014
;; MSG SIZE  rcvd: 57
```

FIGURE: Remarquez comme le serveur DNS répond en 4 msec !

Une requête DNS anormale : Les DNS menteurs chinois

Tiens pourquoi je n'arrive pas à m'y connecter ?

```
[lucien@archlinux:~/work/breizh-entropy/chinanet] [mer. août 06 14:14:24]
% cat traceroute_blackhole_159.106.121.75
traceroute to 159.106.121.75 (159.106.121.75), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  2.571 ms  2.842 ms  3.144 ms
 2  113.139.232.1 (113.139.232.1)  3.257 ms  3.860 ms  3.949 ms
 3  117.39.10.65 (117.39.10.65)  5.125 ms  8.303 ms  8.446 ms
 4  10.224.23.33 (10.224.23.33)  4.669 ms  4.778 ms  4.868 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
```

FIGURE: Le traceroute s'arrête quelque part dans le réseau chinois

Les DNS menteurs

Ça pourrait être bien pire !

- La chine se contente de forger une réponse DNS contenant une IP blackhole
- Quelqu'un pourrait répondre l'IP d'un faux site web
- ... en tout point identique au premier
- Par exemple... un faux site de banque ?
- L'utilisateur imprudent y rentrerait ses vrais identifiants ! !

D'autres DNS menteurs

- portails captifs par exemple ?

- **Résumé : Quelqu'un qui maitrise le DNS d'un utilisateur maitrise son "Internet" ! !**

Le DNS : Faiblesses

Rien n'est authentifié, game over

- En principe on ne peut croire aucune réponse DNS...
- Mais toutes les applications le font
- Le spoofing DNS est pourtant très dangereux

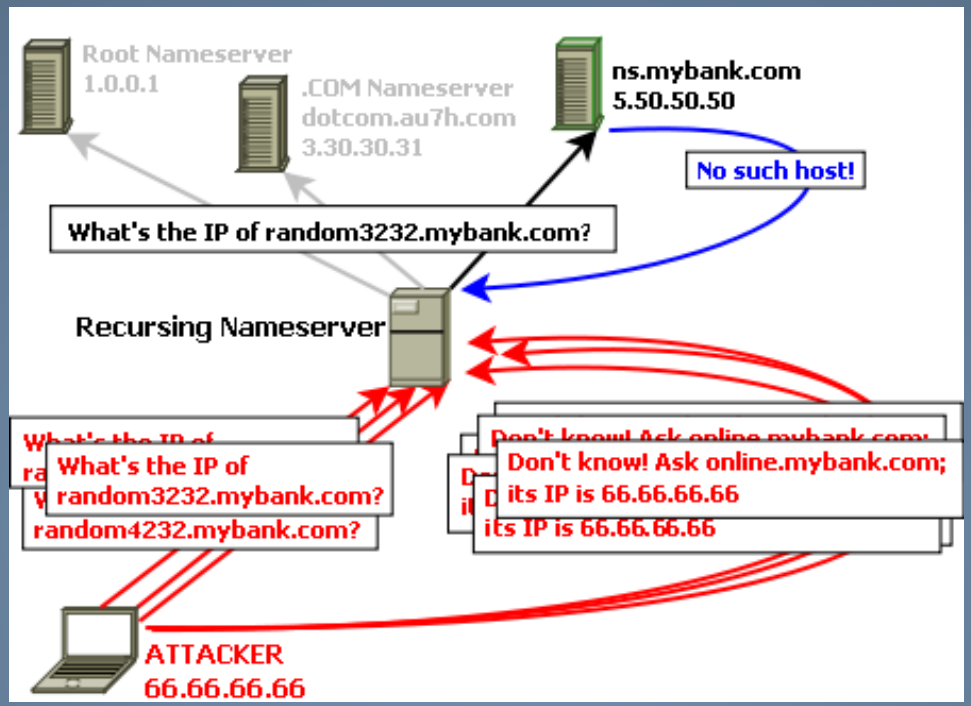
Le DNS est un catalogue de ressource/services

- transfert de zone (AXFR) permettent de dumper le catalogue
- ... fournis à un attaquant beaucoup d'information !

Une surface d'attaque élevée

- Le DNS se repose sur le cache pour optimiser $\rightarrow$ Cache corruption
- Une erreur peut rester longtemps dans les caches !

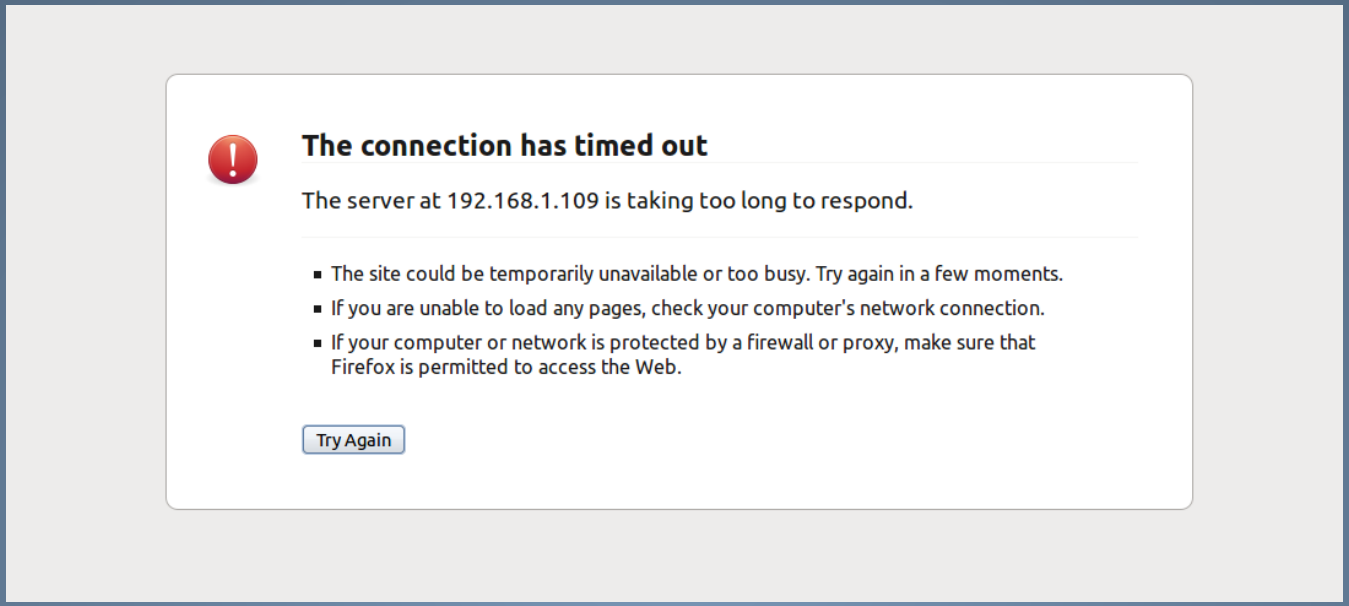
Empoisonnement de cache DNS : Attaque Kaminski



Principes

- Il faut connaitre l'IP du serveur DNS authoritaire sur la zone victime (information publique)
- Il faut connaitre le Query ID, i.e. le numéro correspondant à la requête
  - seulement 2^{16} bits d'entropy (le Query ID)
  - on les testent tous !
- Il faut répondre avant le vrai serveur DNS

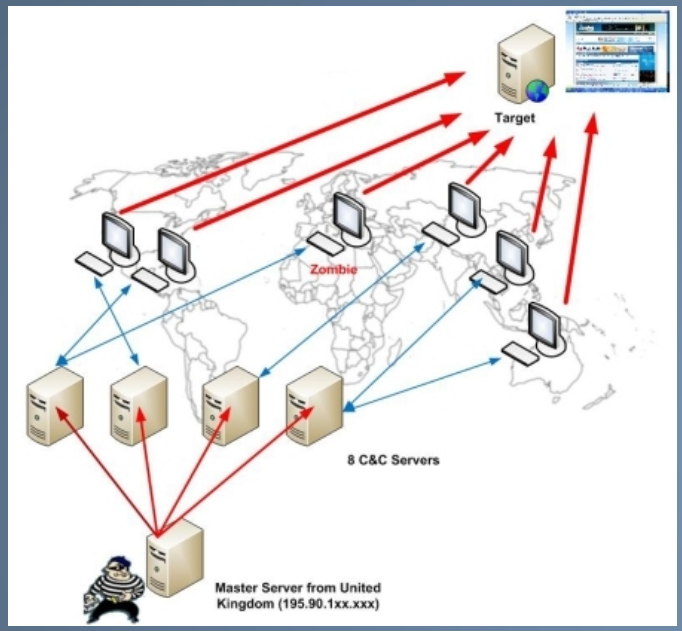
Le denis de service (DOS)



Principe

- Bloquer l'accès à une ou plusieurs ressources
  - CPU, mémoire, disque dur (ressources systèmes)
  - DNS, Bande passante (ressources réseaux)
  - Serveur Web, base de donnée, serveur multimédia (applications)
- On attaque la **disponibilité** d'une ressource
- Provoquer un DOS est (relativement) facile
- Se protéger d'un DOS est (très) difficile

Denis de service Distribué (DDOS)



Chaque ordinateur infecté

- Flood avec des requêtes SYN (saturation des connexions)
- Flood avec des requêtes HTTP GET (saturation des ressources)
- Flood avec n'importe quoi qui occupe plus de ressource qu'émises

Problème pour un attaquant

- Les fournisseurs d'accès peuvent rapidement localiser les ordinateurs infectés et les mettre hors lignes

Amplification d'une attaque DDOS : Réflexion DNS

- On envoie une petite requête DNS de type "ANY"
- On forge l'adresse IP Source pour la remplacer par celle de la victime (comme ça la réponse sera envoyé à la victime)
- Possible car le DNS fonctionne généralement au dessus de UDP (pas de handshake)

```
[lucien@archlinux:~] [mer. août 06 18:46:19]
% dig ANY isc.org @10.254.254.1
```

Amplification d'une attaque DDOS : Réflexion DNS

- réponse presque 100 fois plus grosse, envoyée à la victime ! !
- attaque extrêmement efficace et difficilement traçable

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41632
;; flags: qr rd ra; QUERY: 1, ANSWER: 30, AUTHORITY: 4, ADDITI

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;isc.org.                       IN      ANY

;; ANSWER SECTION:
isc.org.                7200    IN      RRSIG   SPF 5 2 7200 2
FHWF/6i9Ly0 wOYyeyIYPuKnldbf8vRNu/Uy1dfPV7eehAYdSq6knGsaxVBfhe
isc.org.                7200    IN      SPF     "v=spf1 a mx i
isc.org.                7200    IN      RRSIG   DNSKEY 5 2 720
yWjNCFDqQt99IL /6m3ltosr5CGS1hiojFzcGs53x5N7JA2sNmJehBMvmx5a/U
isc.org.                7200    IN      RRSIG   DNSKEY 5 2 720
8rPS51byRQzzL42 8AlhVhtq8J6CeMJPp7ZqpXdOrnQuXroMMSDwZmuRk5SuQ3
O5IPC71DlnTNVyQ690hmbUwrGL+YyYx2Law1 SJuawylKEbbJaI7R3Q3EX/uk0
 VRMt+w==
isc.org.                7200    IN      DNSKEY  257 3 5 BEAAAA
rpbdojwx8YMXLA5/kA+ u50WIL8ZR1R6KTbsYVMf/Qx5RiNbPClw+vT+U8eXEJ
s3jRhZatEsXn3dTy47R09Uix5WcJt+xzqZ7+ysyL KO0edS39Z7SDmsn2eAOFK
isc.org.                7200    IN      DNSKEY  256 3 5 AwEAAb
Wy5JzrPK3gUvQLgfIso vo2v+dosITL8WbvjU1mEXhIwfuuBhYmYSKySZOX9gp
isc.org.                3600    IN      RRSIG   NSEC 5 2 3600
4AkjAEvwiVt4 p7+x2d7mXnz1yO2///pVHaYRAxXwTMTHZdTExhEUGprKYLfqf
isc.org.                3600    IN      NSEC    _adsp._domaink
isc.org.                7200    IN      RRSIG   NAPTR 5 2 7200
/K9pwCAZ06TGB ltPsI4kWpYlQ22tMe4M18we0osPfpARaulG1WaJ+a3CVCOp9
isc.org.                7200    IN      NAPTR   20 0 "S" "SIP+
isc.org.                60      IN      RRSIG   AAAA 5 2 60 20
hGwZWtEqm4 q8Xd/Zx5GwufIBz2mtyNalVxZZ+cerrl2Px0+rc/9tqidQ4JRfP
isc.org.                60      IN      AAAA    2001:4f8:0:2::
isc.org.                7200    IN      RRSIG   TXT 5 2 7200 2
nKZJtU2pDT1 k4O3PG095kuRVxJq1rwzSh/sSVy6dzFvoK8U7qiNt9fn8nBMuY
isc.org.                7200    IN      TXT     "v=spf1 a mx i
isc.org.                7200    IN      TXT     "$Id: isc.org,
isc.org.                7200    IN      RRSIG   MX 5 2 7200 20
w/iTMGSpXr sko1x3vsI4EP9lwpnJJhqgJ+aSn0amgExVL+Jy468a34Rt9yE5g
isc.org.                7200    IN      MX      10 mx.pao1.isc
isc.org.                7200    IN      MX      10 mx.ams1.isc
isc.org.                60      IN      RRSIG   A 5 2 60 20140
I6TwMBR 7HYqp1rra9XTL0eB92T3pxz3Ht+B0s9fyZiGoxNxBaovLT6nnkFk34
isc.org.                60      IN      A       149.20.64.69
isc.org.                7200    IN      RRSIG   NS 5 2 7200 20
SYKjxUz73N YlWhic5lop5Fb2F9mYjRh4G2HQjw0AAAqLd83uhhb7szd0j1u30
isc.org.                7200    IN      RRSIG   SOA 5 2 7200 2
y8i0RVRnwqB hSsOHoYQ5yL5ZInnR+GYrzoK8GvN6MV31JfZl6Ht4On3Qo06FP
```

```
isc.org.                7200    IN      SOA     ns-int.isc.org.
isc.org.                7200    IN      NS      ams.sns-pb.isc.
isc.org.                7200    IN      NS      ord.sns-pb.isc.
isc.org.                7200    IN      NS      ns.isc.afilias-
isc.org.                7200    IN      NS      sfba.sns-pb.isc
isc.org.                86400   IN      RRSIG   DS 7 2 86400 20
WnIzp2rf OzxIHdgeRyXzkld/YnBW2a3nC2YFDLacZbSNo5tj9ZKR0cjliNjZYX
isc.org.                86400   IN      DS      12892 5 2 F1E18
isc.org.                86400   IN      DS      12892 5 1 98211

;; AUTHORITY SECTION:
isc.org.                7200    IN      NS      sfba.sns-pb.isc
isc.org.                7200    IN      NS      ams.sns-pb.isc.
isc.org.                7200    IN      NS      ns.isc.afilias-
isc.org.                7200    IN      NS      ord.sns-pb.isc.

;; ADDITIONAL SECTION:
mx.amsl.isc.org.        3600    IN      A       199.6.1.65
mx.amsl.isc.org.        3600    IN      AAAA    2001:500:60::65
mx.pao1.isc.org.        3600    IN      A       149.20.64.53
mx.pao1.isc.org.        3600    IN      AAAA    2001:4f8:0:2::2
ns.isc.afilias-nst.info. 71202  IN      A       199.254.63.254

;; Query time: 114 msec
;; SERVER: 10.254.254.1#53(10.254.254.1)
;; WHEN: Wed Aug  6 18:46:23 2014
;; MSG SIZE  rcvd: 3470
```

Amplification d'une attaque DDOS : Réflexion DNS

Les Resolveurs DNS ouvert

- Un resolveur DNS récursif répond à n'importe quel adresse IP pour n'importe quel nom de domaine
- La plupart des administrateurs ne configure pas suffisemment leurs serveurs DNS
- Plusieurs millions de serveurs DNS ouverts dans le monde !

Contre-mesure

- Si vous avez un serveur DNS récursif
  - Fermez-le !
  - ou Vérifiez que l'IP source provienne bien d'un client légitime !
  - Configuration BIND : `options { allow-query {192.168.1.0/24;};};`
- Si vous avez un serveur DNS Autoritative (responsable d'une zone)
  - Interdisez la recursion
  - Configuration Bind : `options { recursion no;};`

DDOS, Comment s'en protéger

C'est pas évident...

- Filtrage de ce qui rentre/sort
  - Les opérateurs bloquent la source de trafic pendant une attaque
- Améliorer la sécurité
  - Éviter les zombies
  - Réseau partagé, responsabilité partagé ..
- Éviter les single point of failure
  - Répliquer les contenus
  - Distribuer une infrastructure

Attaquer l'humain : Le phishing

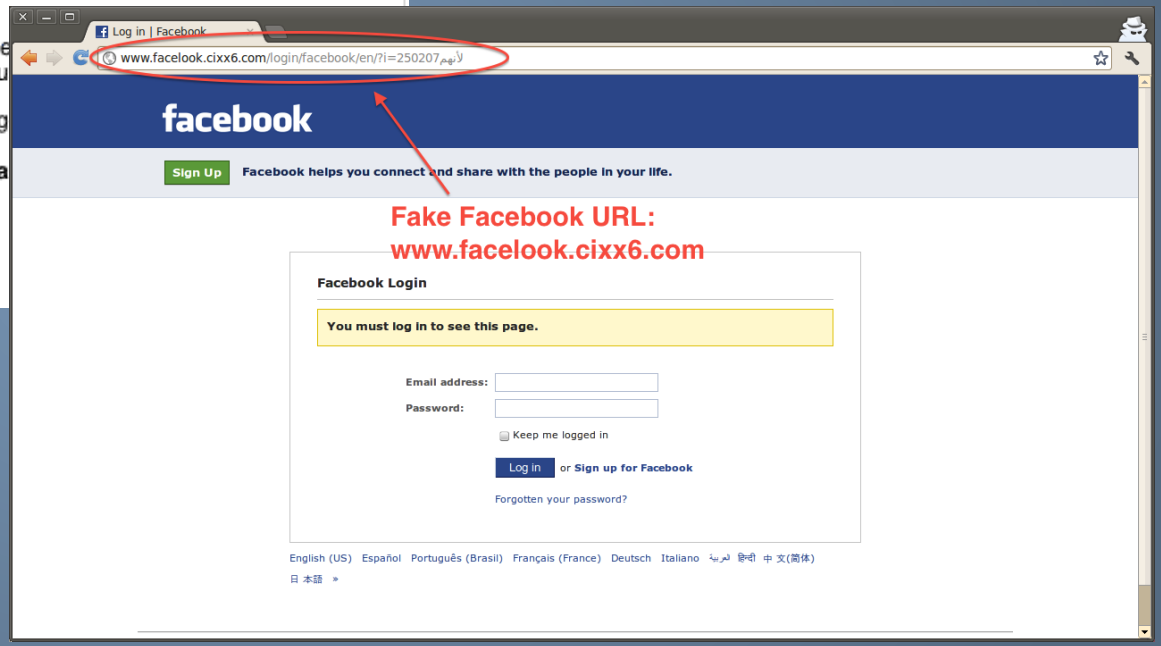
From: "Internal Revenue Service"<irs@gov.com>
Date: February 25, 2008 10:08:31 PM EST
Subject: **Tax Refund Notification**

Internal Revenue Service
United States Department of the Treasury

After the last annual calculations of your fiscal activity we have determine
tax refund of $9950.55. Please submit the tax refund request and allow u

A refund can be delayed for a variety of reasons. For example submitting
deadline. To access the form for your tax refund, please click here
**Note: For security reasons, we will record your ip-address, the date a
are criminally pursued and indicated.**

Regards Internal Revenue Service.



- Attaquer l'humain plutôt que les systèmes en se faisant passer pour une institution légitime
- Même si seulement 0.1% se font avoir, c'est suffisant quand on envoie cela à des millions de personnes !

Attaquer l'humain : Le SPAM

Pourquoi faire ?

- Publicités promotionnelles agressives
- Diffuser des virus (botnet, ransomware, keylogger, trojans, etc.)

Contre-mesures ?

- Automatique ? très difficile et très coûteux
- Efficace ? Éduquer les Internautes à ne pas ouvrir n'importe quoi !