

Sécurité et Réseaux

Les risques et menaces

Sécurité et Réseaux

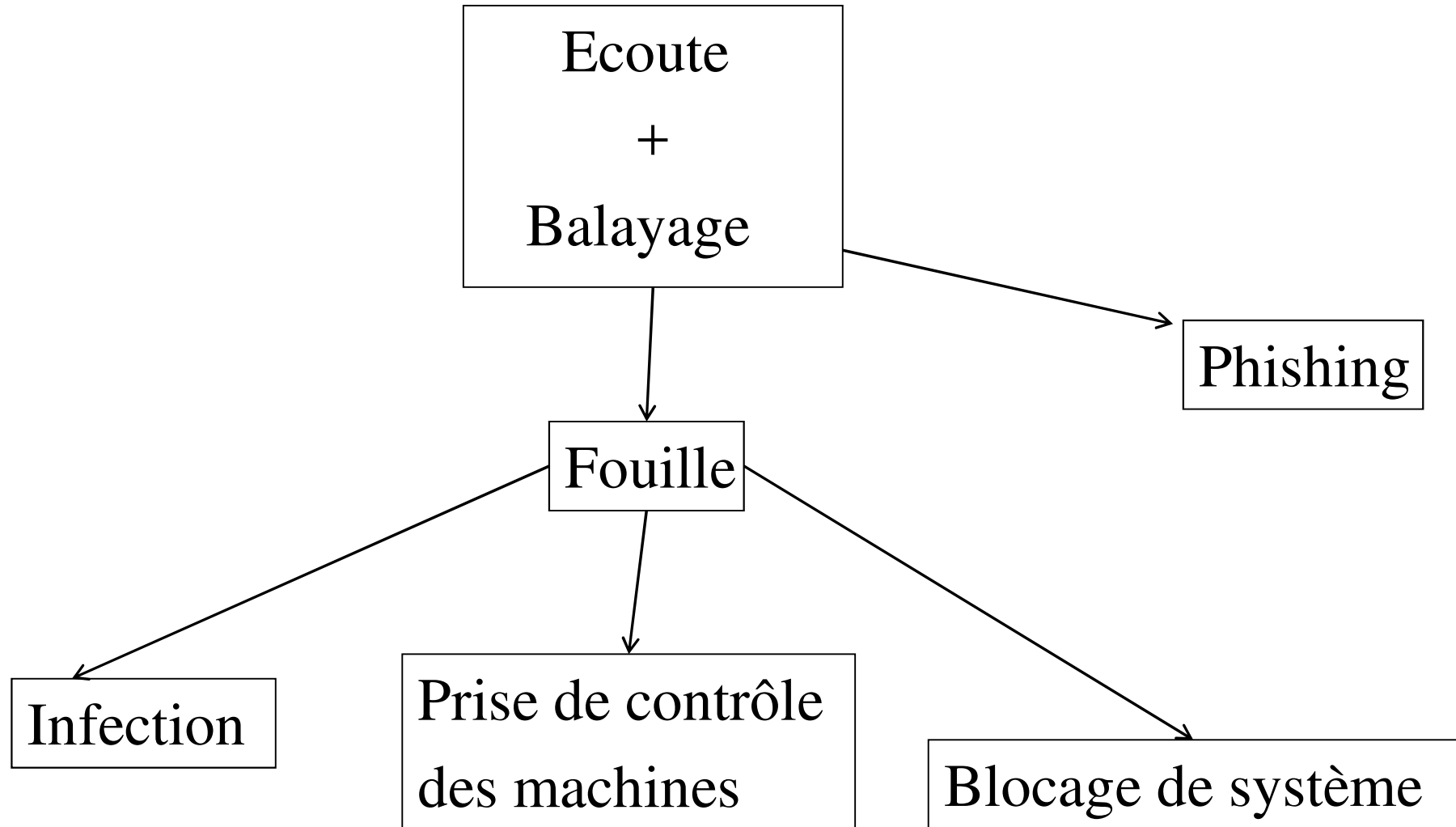
Les menaces

Introduction

La sécurité du Système d'Information repose sur trois critères

- **Confidentialité** : « La confidentialité est la propriété qu'une information n'est ni disponible ni divulguée aux personnes, entités ou processus non autorisés » norme ISO 7498-2 (ISO90).
 - **Disponibilité** : Propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs autorisés.
 - **Intégrité** : « L'intégrité est la prévention d'une modification non autorisée de l'information » norme ISO 7498-2 (ISO90).
- Il existe des menaces pouvant remettre en question chacun des trois critères sur lesquels repose la sécurité.

Introduction



Introduction

Principales menaces :

1. Ecoute : analyse des infos qui circulent sur le réseau
(confidentialité)
2. Balayage : « scan » de ports et recherche d'informations sur les services (confidentialité)
3. Fouille : parcours de fichiers sur une machine donnée (confidentialité)
4. Infection : exécution de code non désiré (intégrité)
5. Blocage de système : (Dos : « denis de service »)
(disponibilité)
6. Phishing (confidentialité, intégrité, disponibilité)

Les menaces

1

Ecoute :

analyse des infos qui circulent sur le réseau

L'écoute (ou sniffing)

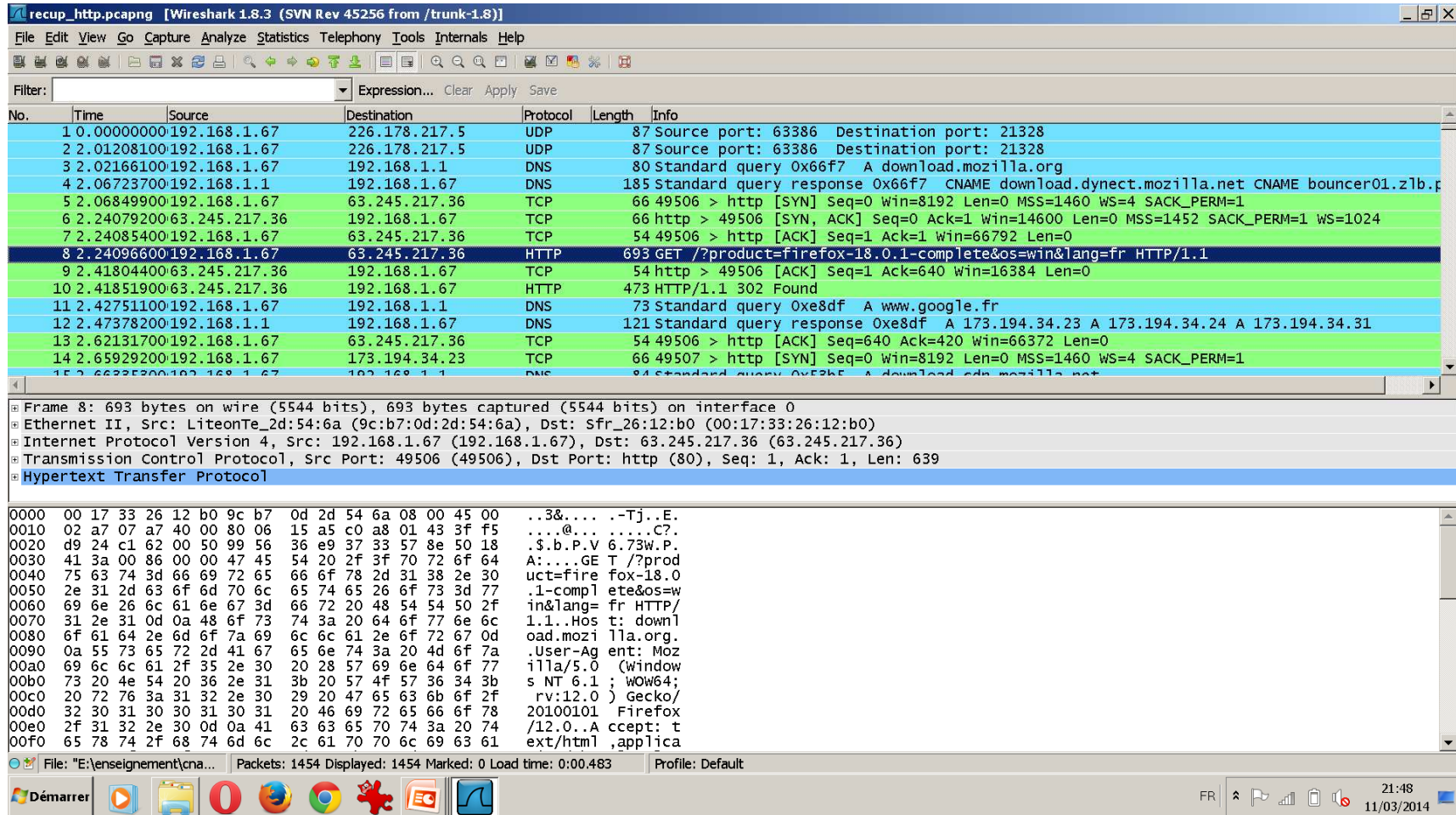
Cette méthode consiste à capturer les messages qui transitent (surtout sur Internet) pour en lire le contenu et ainsi voler un code d'identification ou utiliser le contenu du message à ses propres fins.

Outils de base :

Tcpdump

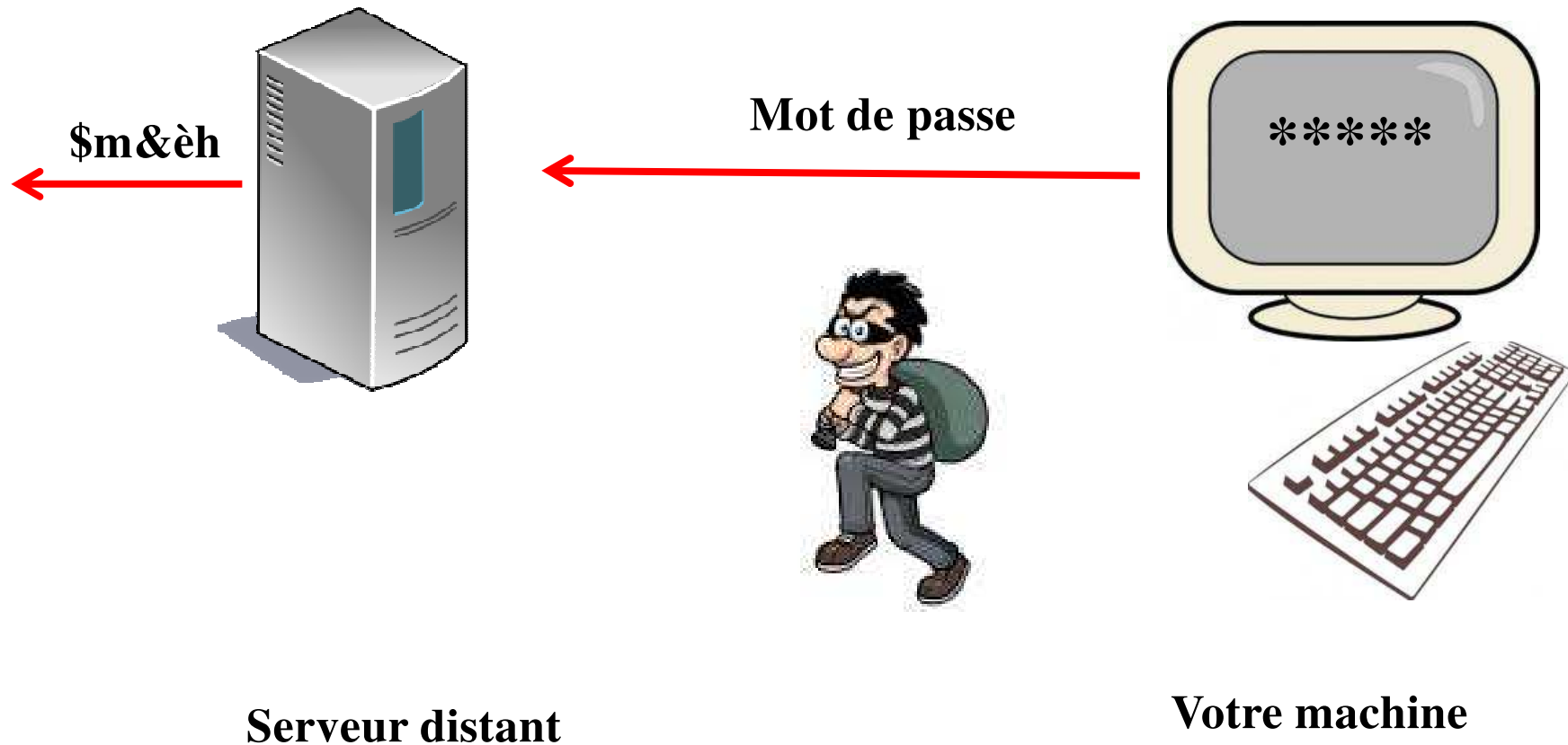
Wireshark

L'écoute (ou sniffing)



Exemple : wireshark

L'écoute (ou sniffing)



Il est possible d'intercepter des informations confidentielles entre votre machine et le serveur distant.

Les risques

L'écoute (ou sniffing)

capture-messagerie.pcapng [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

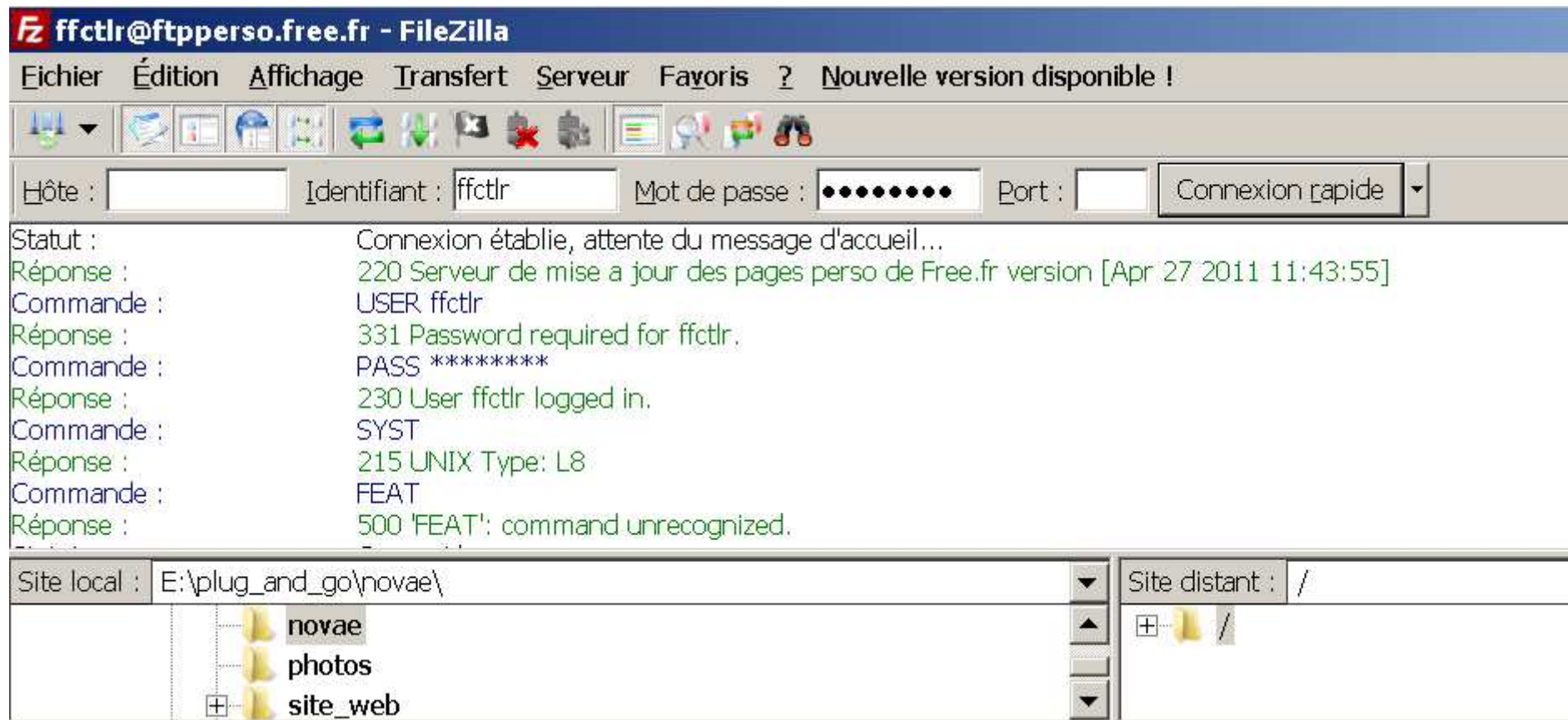
Filter: pop && tcp.port == 49776 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
34	11.704999000	192.168.1.67	193.251.214.115	POP	87	C: USER garcia.francis@laposte.net
41	11.768453000	193.251.214.115	192.168.1.67	POP	83	S: +OK name is a valid mailbox
42	11.768866000	192.168.1.67	193.251.214.115	POP	69	C: PASS z0ny0d4
57	12.044159000	193.251.214.115	192.168.1.67	POP	89	S: +OK user exist with that password
58	12.044444000	192.168.1.67	193.251.214.115	POP	60	C: STAT
62	12.148679000	193.251.214.115	192.168.1.67	POP	68	S: +OK 6 418084
63	12.149004000	192.168.1.67	193.251.214.115	POP	60	C: UIDL
65	12.255509000	193.251.214.115	192.168.1.67	POP	208	S: +OK unique-id listing follows
66	12.255977000	192.168.1.67	193.251.214.115	POP	60	C: LIST
71	12.380824000	193.251.214.115	192.168.1.67	POP	139	S: +OK scan listing follows
74	12.467638000	192.168.1.67	193.251.214.115	POP	62	C: RETR 6
81	12.593865000	193.251.214.115	192.168.1.67	POP	1506	S: +OK Message follows
82	12.594493000	193.251.214.115	192.168.1.67	IMF	1506	, , , , Les partenaires de Tom et Jul=

0000 20 71 73 61 74 65 64 20 70 72 65 6c 74 61 62 6c quoted-printable
00c0 65 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 4c 65 73 e.....Les
00d0 20 70 61 72 74 65 6e 61 69 72 65 73 20 64 65 20 partena ires de
00e0 54 6f 6d 20 65 74 20 4a 75 6c 3d 0d 0a 69 65 0d Tom et Jul=..ie.
00f0 0a 0d 0a 0d 0a 0d 0a 3c 61 20 73 74 79 6c 65 3d< a style=
0100 33 44 22 63 6f 6c 6f 72 3a 20 23 30 30 30 30 30 3d"color : #00000
0110 30 22 20 68 72 65 66 3d 33 44 22 68 74 74 70 3a 0" href= 3d"http:
0120 2f 2f 6e 6f 64 65 73 2e 3d 0d 0a 61 64 65 76 30 //nodes. =..adev0
0130 31 67 6f 2e 63 6f 6d 2f 6d 69 2d 38 37 33 36 36 lgo.com/ mi-87366
0140 2d 34 38 2d 31 38 30 34 37 33 31 36 22 20 3e 53 -48-1804 7316" >S
0150 75 69 76 65 7a 20 63 65 20 6c 69 65 6e 20 70 6f uivez ce lien po
0160 75 72 20 63 6f 6e 73 75 6c 74 65 72 20 63 65 20 ur consu lter ce
0170 6d 65 73 3d 0d 0a 73 61 67 65 20 65 6e 20 6c 69 mes=..sa ge en li
0180 67 6e 65 3c 2f 61 3e 0d 0a 41 66 69 6e 20 64 27 gne. .Afin d'
0190 26 65 63 69 72 63 3b 74 72 65 20 73 26 75 63 69 êt re s&uci
01a0 72 63 3b 72 28 65 29 20 64 65 20 72 65 63 65 76 rc;r(e) de recev
01b0 6f 69 72 20 6e 6f 73 20 70 72 3d 0d 0a 6f 63 68 oir nos pr=..och
01c0 61 69 6e 65 73 20 6f 66 66 72 65 73 2c 20 6d 65 aines of fres, me
01d0 72 63 69 20 64 27 61 6a 6f 75 74 65 72 20 6c 27 rci d'aj outer l'
01e0 61 64 72 65 73 73 65 0d 0a 0d 0a 20 20 20 20 20 adresse. ...
01f0 3c 61 20 68 72 65 66 3d 33 44 22 6d 61 69 3d 0d <a href= 3d"mai=.

Un exemple : interception d'une connexion à la messagerie

L'écoute (ou sniffing)



Un exemple : connexion à un serveur FTP

Les risques

L'écoute (ou sniffing)

15	7.04466600	212.27.63.105	192.168.1.67	FTP	72 Response: 500 Acces refuse
45	31.8787100	212.27.63.3	192.168.1.67	FTP	140 Response: 220 Serveur de mise a jour des pages perso de Free.fr
48	33.2032680	192.168.1.67	212.27.63.3	FTP	55 Request: U
50	33.5424750	192.168.1.67	212.27.63.3	FTP	55 Request: S
52	33.7423380	192.168.1.67	212.27.63.3	FTP	55 Request: E
54	33.9312610	192.168.1.67	212.27.63.3	FTP	55 Request: R
57	34.4994260	192.168.1.67	212.27.63.3	FTP	55 Request:
59	34.9976440	192.168.1.67	212.27.63.3	FTP	55 Request: f
61	35.1679560	192.168.1.67	212.27.63.3	FTP	55 Request: f
63	35.3471010	192.168.1.67	212.27.63.3	FTP	55 Request: c
65	35.5667410	192.168.1.67	212.27.63.3	FTP	55 Request: t
67	36.0943390	192.168.1.67	212.27.63.3	FTP	55 Request: l
70	36.4739170	192.168.1.67	212.27.63.3	FTP	55 Request: r
79	38.5457040	192.168.1.67	212.27.63.3	FTP	56 Request:
81	38.5966720	212.27.63.3	192.168.1.67	FTP	89 Response: 331 Password required for ffctlr.
83	39.6030630	192.168.1.67	212.27.63.3	FTP	55 Request: P
92	39.9036420	192.168.1.67	212.27.63.3	FTP	56 [TCP Retransmission] Request: PA
94	40.1708340	192.168.1.67	212.27.63.3	FTP	55 Request: S
97	40.3802790	192.168.1.67	212.27.63.3	FTP	55 Request: S
99	40.8299320	192.168.1.67	212.27.63.3	FTP	55 Request:
101	41.8867170	192.168.1.67	212.27.63.3	FTP	55 Request: c
103	42.1956260	192.168.1.67	212.27.63.3	FTP	55 Request: e
126	42.8131360	192.168.1.67	212.27.63.3	FTP	55 Request: 2
144	43.5610590	192.168.1.67	212.27.63.3	FTP	55 Request: f
146	43.9800240	192.168.1.67	212.27.63.3	FTP	55 Request: p
149	44.4279770	192.168.1.67	212.27.63.3	FTP	55 Request: b
153	45.0665590	192.168.1.67	212.27.63.3	FTP	55 Request: 3
155	45.4741850	192.168.1.67	212.27.63.3	FTP	55 Request: t
160	47.3281050	192.168.1.67	212.27.63.3	FTP	56 Request:
162	47.3692020	212.27.63.3	192.168.1.67	FTP	82 Response: 230 User ffctlr logged in.
165	48.6146530	192.168.1.67	212.27.63.3	FTP	55 Request: P
167	49.5286780	192.168.1.67	212.27.63.3	FTP	57 [TCP Retransmission] Request: PWD
170	50.3688480	192.168.1.67	212.27.63.3	FTP	56 Request:

Un exemple : connexion à un serveur FTP

Les risques

L'écoute (ou sniffing)

Créer un outil d'écoute est simple.

Pour faire un outil d'écoute il suffit de demander à récupérer dans un programme toutes les trames .

2 possibilités :

- les bibliothèques xpcap (paquet capture) , offrent aux programmeurs un ensemble d'outils pour traiter les trames du réseau. Il existe des bibliothèques pour chaque langage de programmation (libpcap en C, jpcap en java, winpcap sous windows, ...)
- la programmation directe au travers de sockets RAW.

L'écoute (ou sniffing)

A quel endroit peut-on intercepter vos informations ?

1 – Sur votre machine

2 – Dans le réseau ou vous trouvez

Et si le serveur se trouve à l'extérieur de votre établissement :

3 – N'importe où en France ou dans le monde ????

Les risques

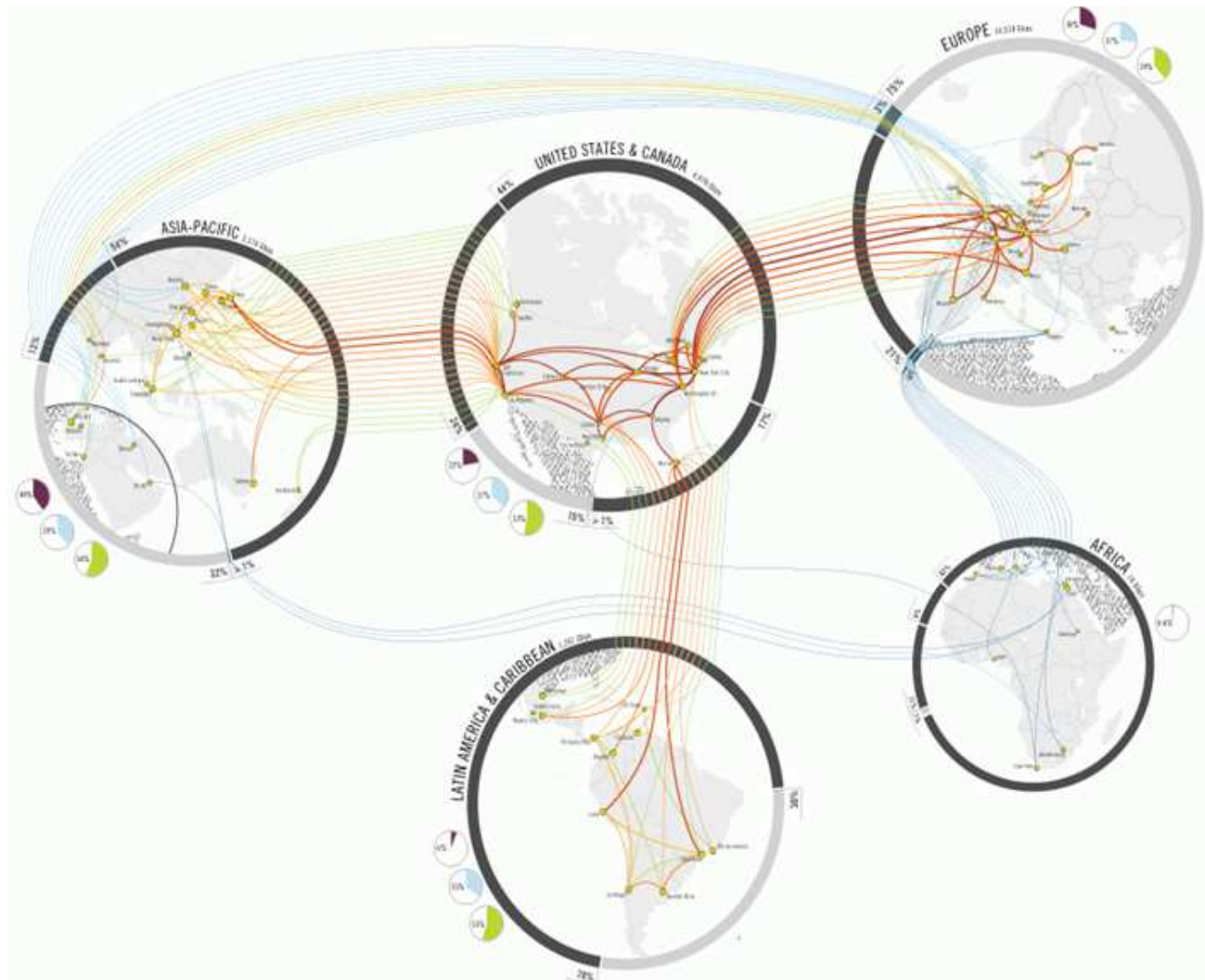
L'écoute (ou sniffing)



En effet, pour aller d'un point à un autre vos messages doivent passer par plusieurs intermédiaires (Routeurs)

Les risques

L'écoute (ou sniffing)



A l'échelle mondiale, 70% du trafic de l'internet, transite par les USA !!!!

Les risques

L'écoute (ou sniffing)

Espionnage aux Etats-Unis : «J'avais le pouvoir d'écouter n'importe qui»

LIBERATION 10 JUIN 2013 À 12:50

Réfugié à Hongkong, l'Américain Edward Snowden, la source qui a fait fuiter des informations sur le programme de surveillance des communications, est sorti de l'ombre face à une caméra du «Guardian».

Le quotidien britannique *The Guardian* a publié sur son site ce lundi un entretien vidéo dans lequel Edward Snowden, la source dans l'affaire du programme américain de surveillance des communications aux Etats-Unis, apparaît à visage découvert. Il explique sa décision de porter les informations et documents dont il disposait au grand jour et les risques auxquels il s'expose en révélant son identité.

Les risques

Les menaces

2

Balayage :

« scan » de ports et recherche d'informations sur
les services

Balayage (ou scan)

Le balayage consiste à vérifier si des ports sont ouverts sur une ou plusieurs machines et ensuite de récupérer la réponse du service actif et de l'identifier via les informations contenues dans l'entête des réponses (Exemple : http 1.1)

```
...-Tj... 3&....E.  
..6S@... 9.?...$..  
.C.P.b73 W .V9hP.  
.....HT TP/1.1 3  
02 Found ..Server  
: Apache ..X-Back  
end-Serv er: boun  
cer10.we bapp.phx  
1.mozill a.com..C  
ache-Con trol: ma  
x-age=15 ..Conten  
t-Type: text/htm  
l; chars et=UTF-8  
..Date: Wed, 06  
Feb 2013 15:34:2
```

Balayage (ou scan)

Rappel : Les applications communiquent via les ports qui sont la plus part du temps figés.

20	FTP-DATA	File Transfer [Default Data]
21	FTP	File Transfer [Control]
25	SMTP	Simple Mail Transfer
53	DNS	Domain Name Server
80	HTTP	WWW

Ainsi le scan, consiste à vérifier si certains services dont on connaît des failles sont ouverts et ensuite à exploiter ces failles.

Balayage (ou scan)

On peut facilement créer un scan :

1 - Un exemple classique de scan et d'identification de service sous TCP en shell Linux:

```
port=1
while [ port < 65535 ]
do    telnet 127.0.0.1 $port
      let port=$port+1
done
```

Balayage (ou scan)

2 - Un exemple de scan en C:

```
#include <sys/socket.h>
#include <netinet/in.h>
#define SERV "127.0.0.1"
int port,sock;
struct sockaddr_in serv_addr;
struct hostent *serveur;
main()
{ port = 1;
  serveur = gethostbyname(SERV);
  if (!serveur){ fprintf(stderr, "Problème serveur \"%s\"\n",SERV);exit(1);}
  while (port<65535)
  { sock = socket(AF_INET, SOCK_STREAM, 0);
    serv_addr.sin_family = AF_INET;
    bcopy(serveur->h_addr, &serv_addr.sin_addr.s_addr,serveur->h_length);
    serv_addr.sin_port = htons(port);
    if (connect(sock,(struct sockaddr *)&serv_addr, sizeof(serv_addr)) < 0)
        {printf("Connexion impossible au port %d \n",port);}
        else {printf("Port %d ouvert\n",port);}
    port++ ;
  } close (sock);
}
```

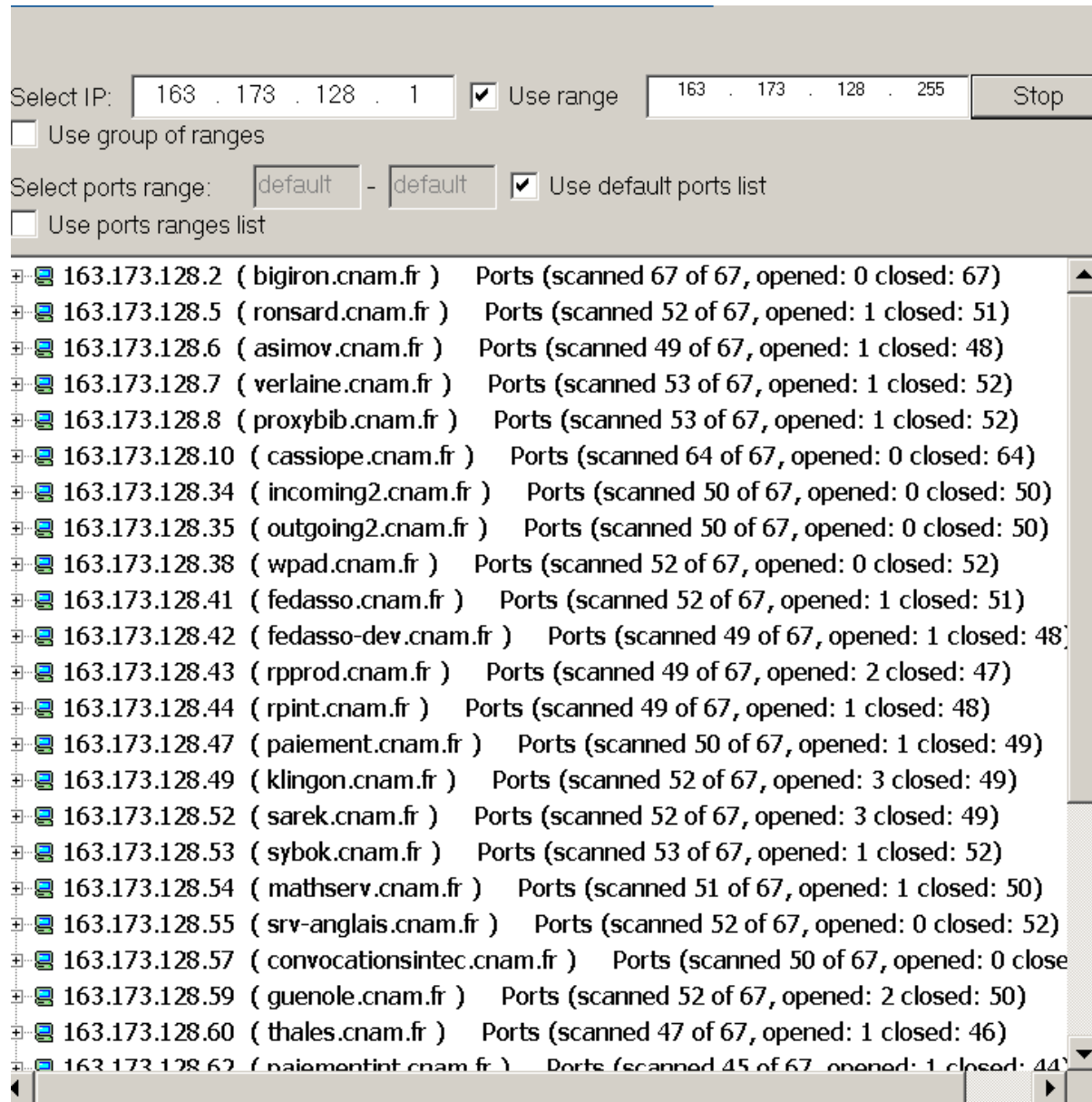
Balayage (ou scan)

On peut aussi utiliser un outil tout prêt:

Quelques outils :

- nmap (sous Linux) : scan des ports d'une machine
- telnet : envoie une requête à une service
- netcat : permet d'établir une connexion (TCP ou UDP) sur un port souhaité et d'y envoyer ou d'y recevoir des données
- amap : permet d'identifier les services

Balayage (ou scan)



Un exemple
de scan

Les risques

Balayage (ou scan)

Exemple pour FTP

Failles ftp

Web

Images

Vidéos

Actualités

Shopping

Plus ▼

Outils de recherche

Environ 62 100 résultats (0,25 secondes)

Les cookies assurent le bon fonctionnement de nos services. En utilisant ces derniers, vous acceptez l'utilisation des cookies.

OK

[En savoir plus](#)

SYSTEMe - Faille FTP - accueil

sysgb.fr/gd/Faille-FTP.htm ▼

Faille FTP. Hacker un site non protégé en entrant sur le compte ftp : Dans cette section, je vais vous apprendre à hacker un site par le port 21 (celui de FTP).

Balayage (ou scan)

Exemple pour FTP

Hacker un site non protégé en entrant sur le compte ftp :

Dans cette section, je vais vous apprendre à hacker un site par le port 21 (celui de FTP). Bon avant de commencer je dois vous dire que cette manière de hacker un site non protégé s'est pratiquement éteinte (peu de chance de réussite!) mais je la dévoile.

Tout d'abord, aller dans Démarrer - Exécuter et taper ftp-n

La méthode se déroule en 4 étapes :

open http://www.victim.com/ (victim.com est un exemple)

quote user ftp

quote cwd ~root

quote pass ftp

Lorsque j'ai écrit en rouge, c'est lorsque c'est ce qu'il ne faut pas avoir.


Taper open www.victim.com	Connected to www.assassin.com 220 websrv1 Microsoft FTP Service (Version 4.0)
Taper open www.victim.com	Connect 10061
quote user ftp	331 Anonymous acces allowed, send identify (e-mail name) as password
quote user ftp	331 Password required for ftp
quote cwd ~root	530 Please login with USER and PASS.
quote cwd ~root	Connexion closed by remote host
quote pass ftp	230 Anonymous user logged in.
quote pass ftp	530 User ftp cannot log in.

Voilà, normalement vous êtes connecté !!! Si vous voulez un peu toucher le site, regarder juste en dessous les Commandes Dos.

Copie d'écran du site : sysgb.fr/gd/Faille-FTP.htm

Balayage (ou scan)

Sujet: [Piratage](#)


Suivre via: 

Cybervandalisme, 25000 sites Web français attaqués

Sécurité : *L'offensive des activistes islamistes contre le Web français donne lieu à une réponse judiciaire commune, prévient le ministre de l'Intérieur.*



Par La rédaction de ZDNet.fr | Lundi 19 Janvier 2015

 Suivre @zdnetfr

Réactions 3

[plus +](#)

Les odieux attentats ayant frappé la France ont, on le sait, donné lieu à une autre bataille, sur le Web. Premiers à réagir, les Anonymous qui ont promis de venger les victimes de Charlie Hebdo avec l'opération #OpCharlieHebdo. [Cette offensive](#) des hacktivistes a évidemment provoqué une réaction de hackers de l'autre bord, soutenant les islamistes radicaux. Et ces derniers ont massivement attaqué de nombreux sites Web français (églises, municipalités, universités, hôpitaux...).

Les risques

Les menaces

3

Fouille

Parcours de fichiers sur une machine
donnée

Fouille

Une fois que l'on a repéré une application, on sait quelle enregistre temporairement des copies des données utilisées (Fichiers de travail) , afin de diminuer le temps d'accès (en lecture ou en écriture) .

→ Les zones de stockage se dénomment « CACHE » ou « fichiers cachés »

Par exemple, le navigateur conserve toutes les pages Web, images et autres fichiers sur votre PC.

Les risques

Fouille

Sous windows :

Base de registre (Regedit)

C:\Documents and Settings\user\Local Settings\Temporary Internet Files

C:\Documents and Settings\user\Local Settings\Historique

C:\Documents and Settings\user\Mes Documents\Mes Documents Récents

...

Sous Linux

/home/user/.kde/share/apps/...

/home/user/.kde/cache-localhost/http

/tmp

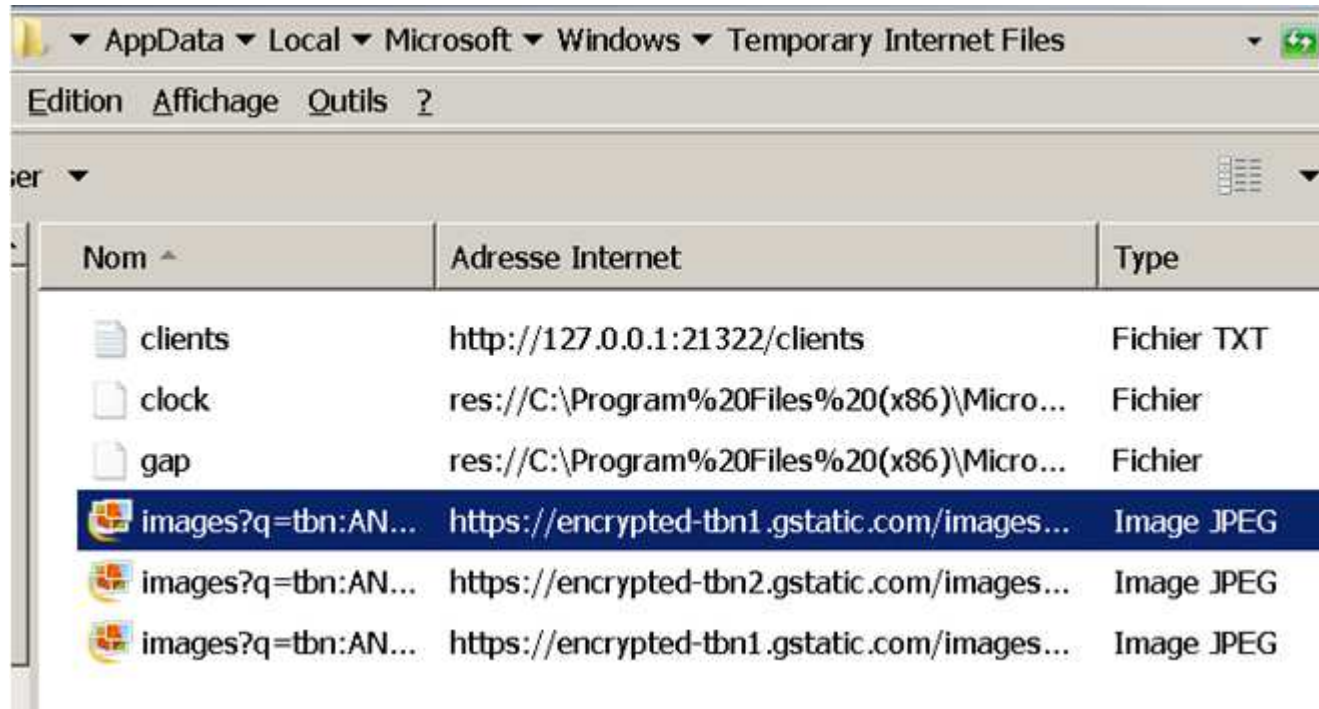
...

Fouille

Problème, c'est que ces zones sont :

- souvent situées dans des dossiers par défaut ;
- facilement accessibles ;

→ Donc, si on connaît les applications (détectées par le balayage), on connaît l'emplacement de ces fichiers de travail.



Nom ^	Adresse Internet	Type
clients	http://127.0.0.1:21322/clients	Fichier TXT
clock	res://C:\Program%20Files%20(x86)\Micro...	Fichier
gap	res://C:\Program%20Files%20(x86)\Micro...	Fichier
images?q=tb1:AN...	https://encrypted-tbn1.gstatic.com/images...	Image JPEG
images?q=tb1:AN...	https://encrypted-tbn2.gstatic.com/images...	Image JPEG
images?q=tb1:AN...	https://encrypted-tbn1.gstatic.com/images...	Image JPEG

Les risques

Fouille

Information about the Network Cache Storage Service

☐ Private ☐ Anonymous AppID ☐ In Browser Element [Back to overview](#)

disk

Number of entries: 82
 Maximum storage size: 358400 KiB
 Storage in use: 1740 KiB
 Storage disk location: C:\Users\f\AppData\Local\Mozilla\Firefox\Profiles\lylu5545.default\cache2

Key	Data size
https://blocklist.addons.mozilla.org/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/36.0.1/Firefox/20150305021524/WINNT_x86-msvc/fr/release/Windows_NT%206.2/default/default/1/170/33/	20740 bytes
http://ciscobinary.openh264.org/openh264-win32-vl.3.zip	303940 bytes
https://services.addons.mozilla.org/fr/firefox/api/1.5/search/guid:wrc%40avast.com,%7B972ce4c6-7e08-4474-a285-3208198ce6fd%7D?src=firefox&appOS=WINNT&appVersion=36.0.1	103 bytes
https://services.addons.mozilla.org/fr/firefox/api/1.5/search/guid:wrc%40avast.com,%7B972ce4c6-7e08-4474-a285-3208198ce6fd%7D?src=firefox&appOS=WINNT&appVersion=33.1&tMain=999&tFirstPaint=3855&tSessionRestored=4485	103 bytes
https://dtex4kvbpovt.cloudfront.net/desktop/FR/fr.c94d7ae48dc130bbcdf7c9173b498ae4bbcb1b25.json	3742 bytes
https://blocklist.addons.mozilla.org/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/36.0.1/Firefox/20150305021524/WINNT_x86-msvc/fr/release/Windows_NT%206.2/default/default/1/170/33/	20740 bytes

Cache entry information

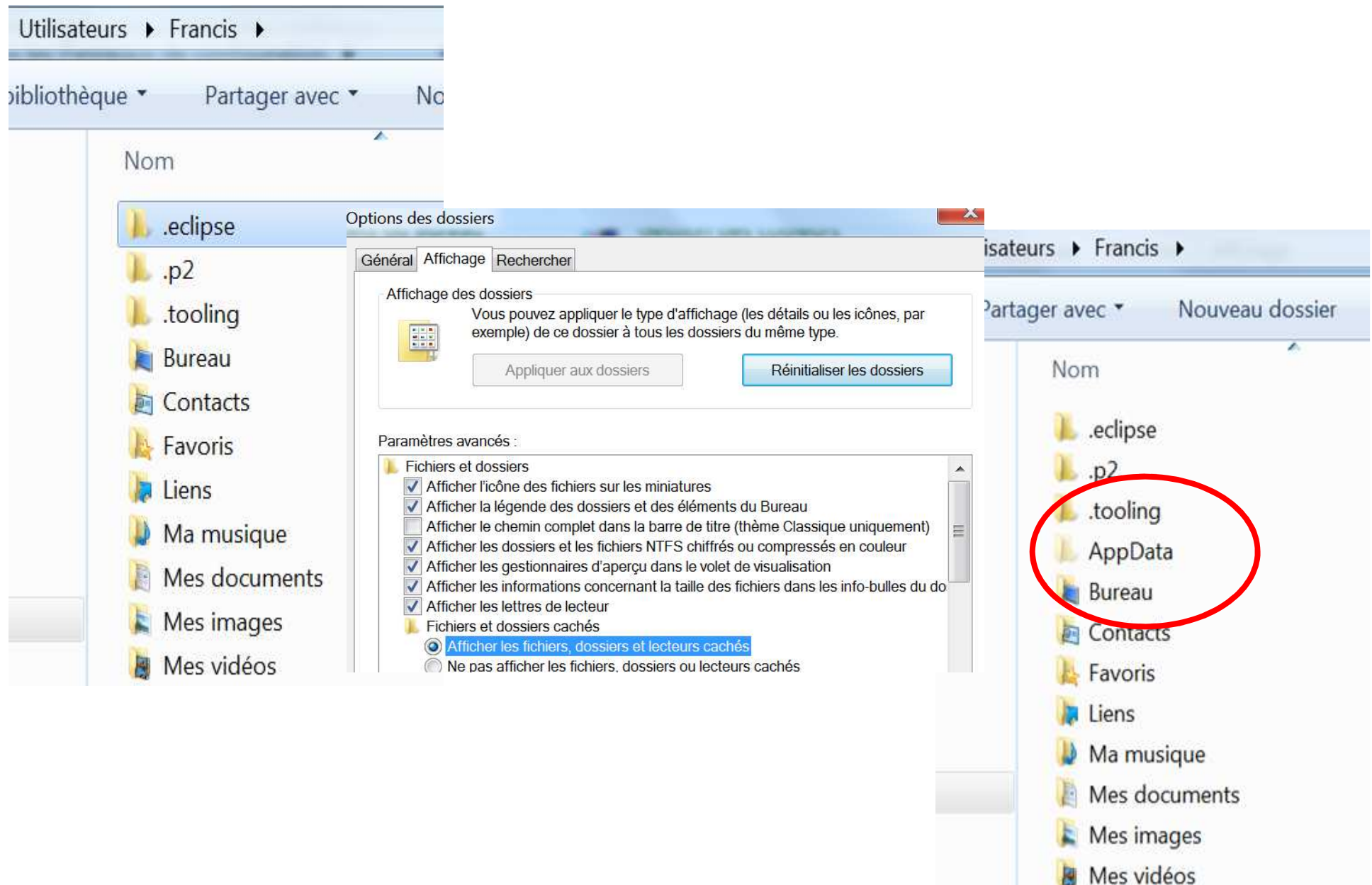
key: <http://ciscobinary.openh264.org/openh264-win32-vl.3.zip>
 fetch count: 3
 last fetched: 2015-03-13 07:43:06
 last modified: 2015-03-13 07:38:50
 expires: 2015-03-16 01:06:40
 Data size: 303940 B
 Security: This document does not have any security info associated with it.

request-method: GET
 response-head: HTTP/1.1 200 OK
 Last-Modified: Tue, 27 Jan 2015 18:54:24 GMT
 Etag: 5ad102414ed4e233ed17c5e67442db9d
 Origin: https://mycloud.rackspace.com
 Content-Length: 303940
 Accept-Ranges: bytes
 X-Timestamp: 1422384863.37510
 Content-Type: application/zip
 X-Trans-Id: txdd76a94be7d2478180140-0054c8fbc3dfwl
 Cache-Control: public, max-age=235691
 Expires: Mon, 16 Mar 2015 00:06:41 GMT
 Date: Fri, 13 Mar 2015 06:38:30 GMT

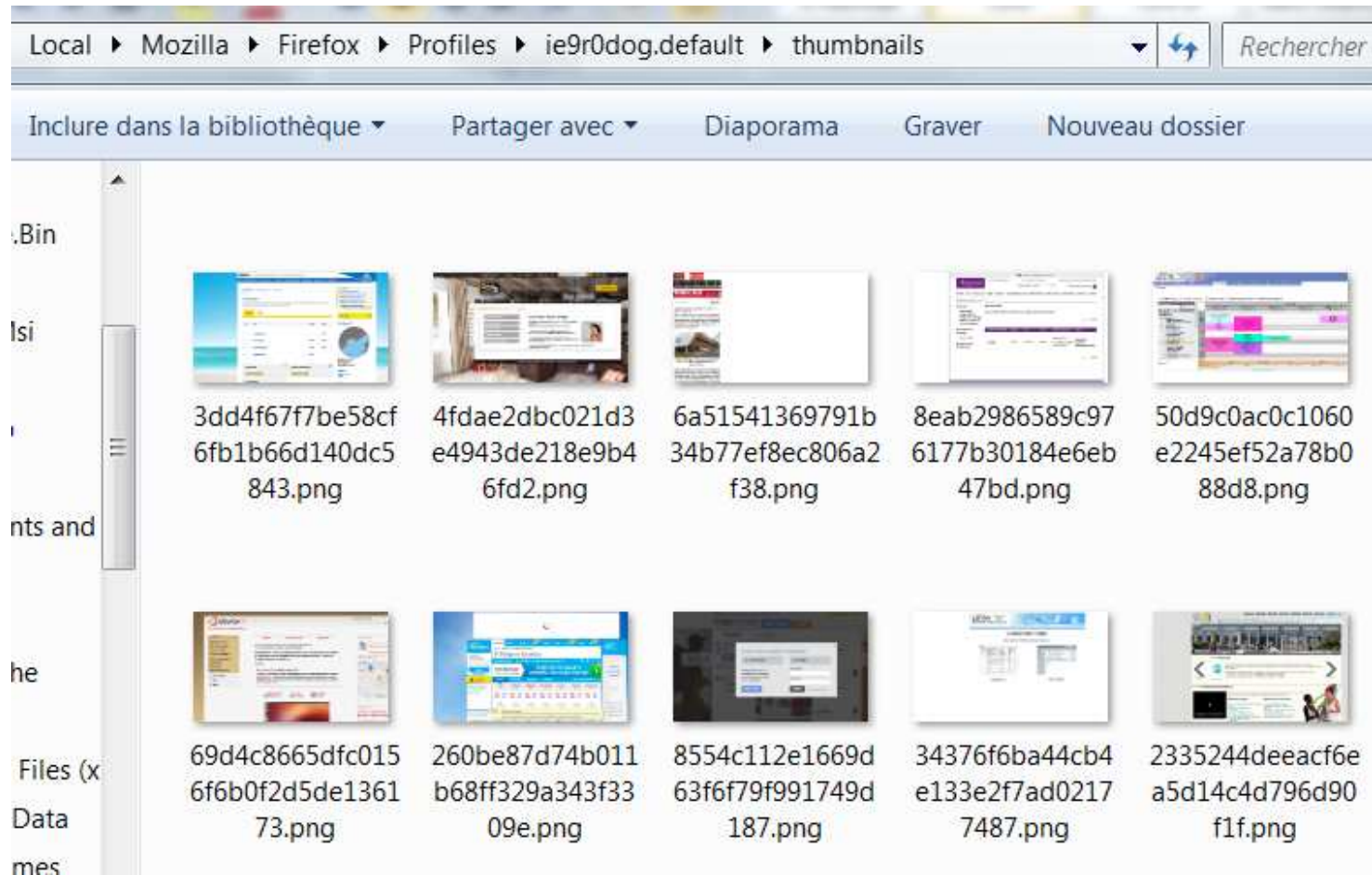
```
00000000: 50 4b 03 04 14 00 00 00 08 00 06 3f 2f 46 4d 2b PK.....?/FM+
00000010: fa 88 f1 a0 04 00 00 6e 09 00 0f 00 71 00 67 6d .....n....q.gm
00000020: 70 6f 70 65 6e 68 32 36 34 2e 64 6c 6c 53 44 5c popenh264.dllSD\
00000030: 00 98 00 00 00 00 08 00 b0 cb 72 76 63 64 60 69 .....rvcd`i
00000040: 10 61 60 60 50 61 80 00 07 20 66 64 02 33 59 15 .a`Pa... fd.3Y.
00000050: 80 84 02 90 cd c8 0a e1 8b 02 09 8e e3 4d a9 eb .....M..
00000060: 3c 5c 9d 5d d4 9e d7 80 d4 31 31 44 30 30 83 a5 <\.j.....11D00..
00000070: 45 18 fe 33 ca 33 30 32 42 d4 0a 81 29 09 88 18 E..3.302B...)...
00000080: 9a 79 20 db c0 e2 38 cc 7d 01 34 10 00 55 54 0d .y...8\4.UIT
```

Contenu des fichiers de travail de Mozilla

Fouille



Fouille



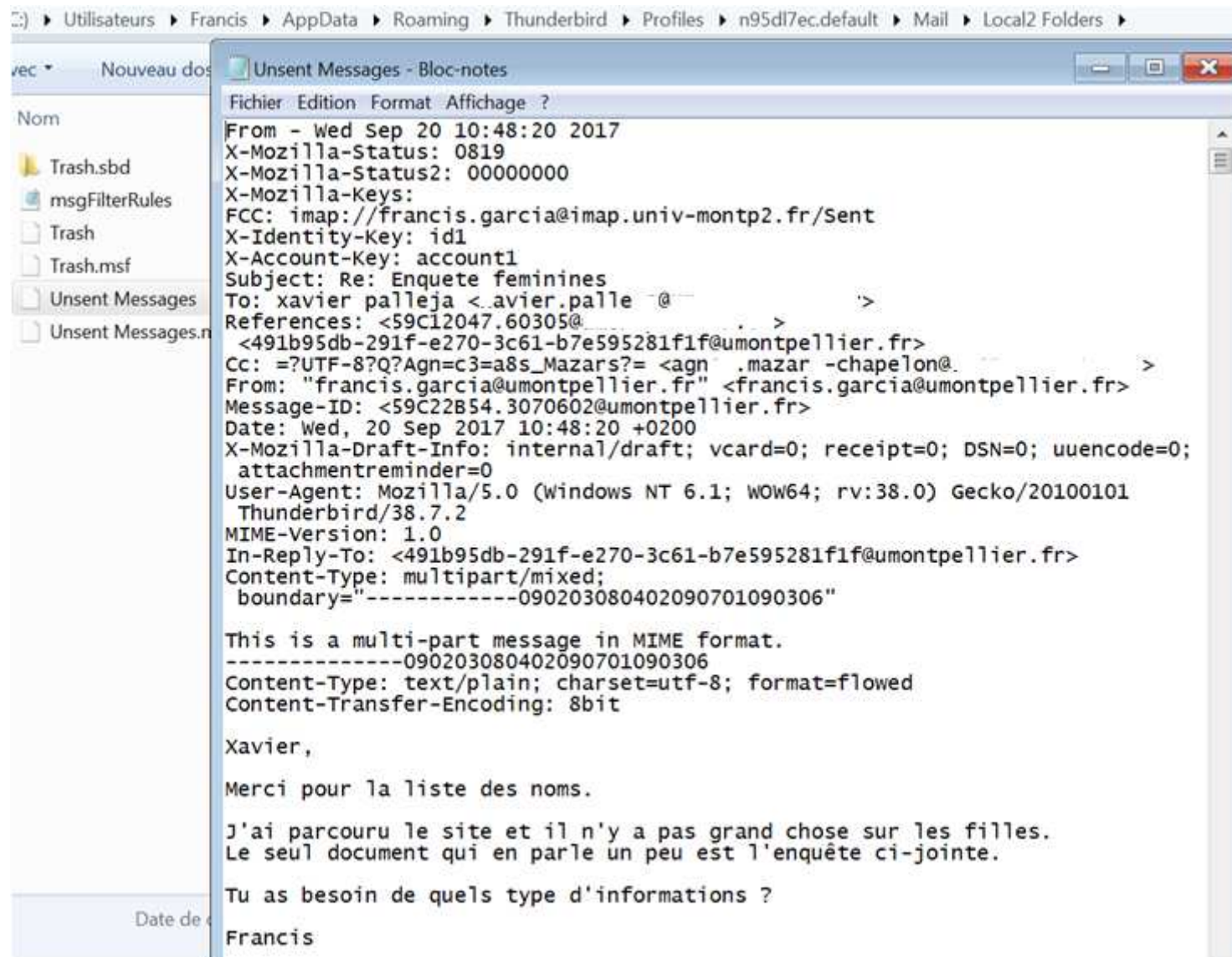
Fouille

Outlook.NK2 - Bloc-notes

Fichier Edition Format Affichage ?

pgs-dir@plugandgosolutions.com
gilles.lucato@plugandgosolutions.com
SMTP christian.ferrand@plugandgosolutions.com
SMTP ariegeoise.cycloclub@wanadoo.fr
L Benjamin Arnaud <shiryu34@...>
francis@laposte.net
SMTP:CAVADELIS@...
Ana Maria Gonzalez Box, t, eCn, Ana
garcia. @laposte.net, ig, garcia.lauren
it, N michel.burckart@plugandgosolutions.com
SMTP jerome.web SMTP jerome@...
SMTP nathalie@webcroisieres.com
SMTP OpVE <francis.garcia@univ-montp2.fr>
GUY DAURELLE SMTP guy.daurelle@...
L Francis garcia <gmail.com>
SMTP:CEDRIC@CHOOSIT.COM

Fouille



Messagerie Thunderbird

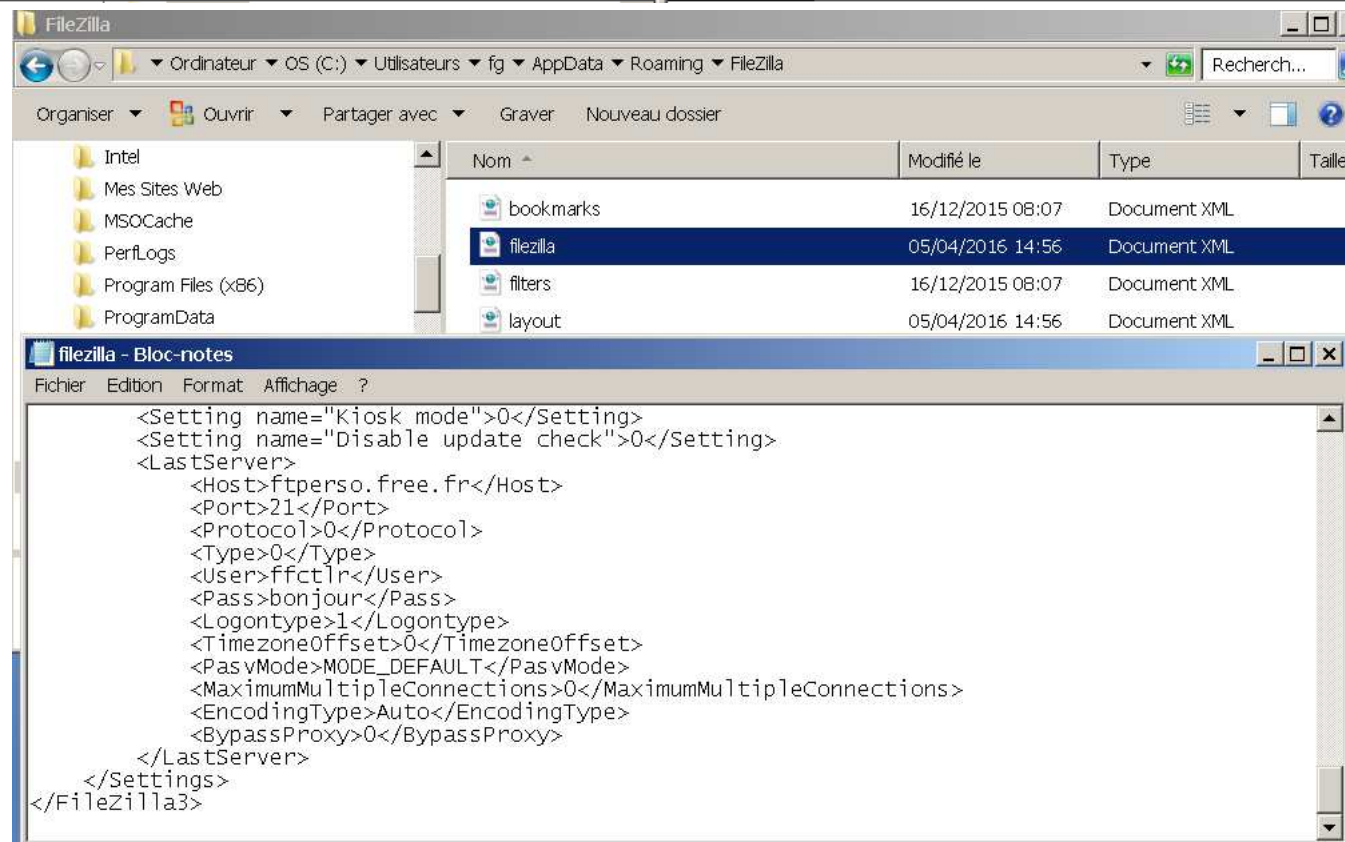
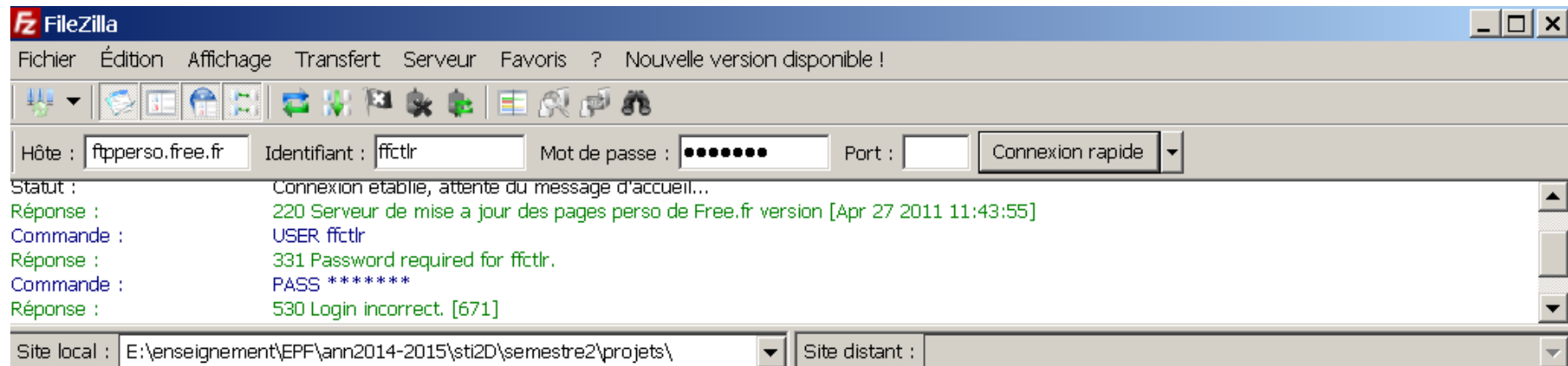
Fouille

Dans toutes ces données sont stockées une grande quantité d'informations sensibles comme des identifiants et mots de passe d'accès aux services.

Nom de la ressource	Nom d'utilisateur	Mot de passe
PORT-GARCIA64 (Dell Inc. Latitude E5520)		
FileZilla		
ftpperso.free.fr	ffctlr	ce2f*****
Outlook		
garcia.francis@laposte.net [POP3 Password]	garcia.francis@laposte.net	Z5nk*****
garcia_francis@sfr.fr [POP3 Password]	garcia_francis@sfr.fr	Z5nk*****
francis.garcia@plugandgosolutions.com [POP...]	francis.garcia@plugandgosolutio...	garc*****
Wireless SSID/Key		
WPA-PSK	SFR_0BE8	bes8*****nstrougg

Logiciel SIW

Fouille



Fouille

En fait, on trouve de tout dans ces fichiers de travail :

- Pages visitées,
- Images,
- Vidéos
- Nom des sites,
- Mots de passe,
- ...

Il est donc tentant d'introduire sur votre machine des logiciels dits « espions ou spywares » qui collectent et envoient des informations personnelles via Internet à des personnes malveillantes.

→ On parle « d'infection du système »

Les risques

Conséquences de la fouille - Les spywares

Des logiciels dits « logiciels espions ou spywares » collectent et envoient des informations personnelles via Internet à des bases de données qui sont utilisées pour envoyer de la publicité plus ou moins ciblée : c'est le « Spam ».

Ces logiciels sont souvent intégrés à d'autres logiciels que l'on télécharge ou fournis directement avec le système (exemple : Windows Media Player).

Conséquences de la fouille - Le spam

Le spam est une activité en pleine expansion.

Les raisons :

- Envoyer des millions de mail ne coûte presque rien
- L'expédition peut se faire de manière anonyme
- Les « spammeurs » sont rémunérés par les clients

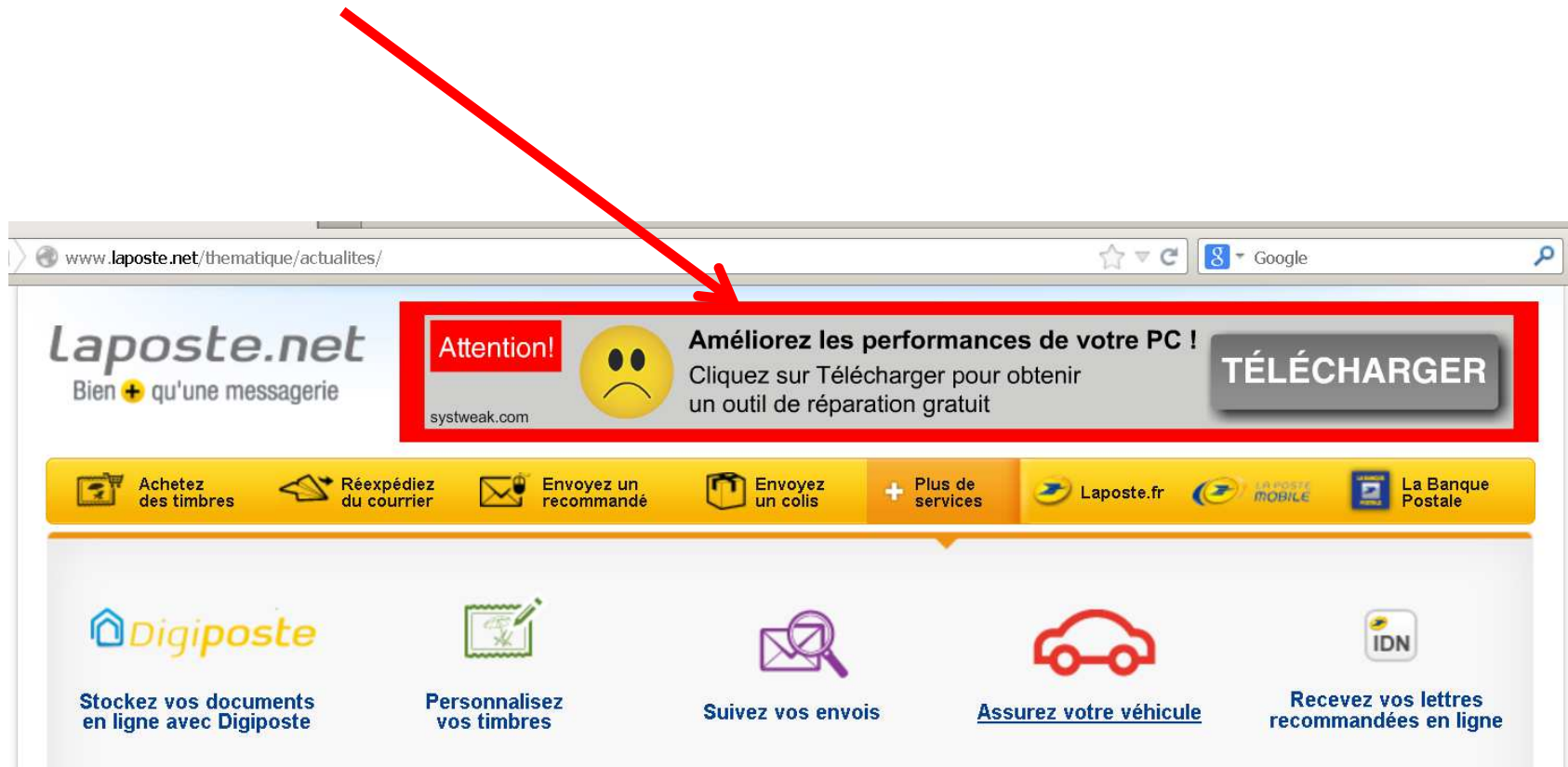
Le spam devient une vraie activité économique. Des sociétés se sont créées dans les pays où la législation tolère ce type d'activité.

Ce phénomène risque de perdurer ...

Conséquences de la fouille - Le Publiciel

Outils de capture d'information :

- Publiciel (adware) pour l'affichage de bannières publicitaires



Les menaces

4

Infections :
Virus et autres ...

Infections (Virus, bombes logiques, troyens, vers)

Cette méthode consiste à inclure un programme d'apparence anodin dans un fichier. Celui-ci, une fois lancé peut exécuter n'importe quelle action sur le système.

Il existe deux grandes familles d'infection :

- Les programmes simples
- Les programmes auto-reproducteurs

Infections (Virus, bombes logiques, troyens, vers)

Les programmes simples

Ces programmes contiennent une fonctionnalité malveillante qui se déclenche lors de leur exécution. Il n'y a pas de propagation, ces programmes doivent être introduits dans l'ordinateur (cd, usb, fichiers attachés,...) .

Bombes logiques : Programme qui contient une fonction destructrice cachée et qui se déclenche en différé.

Troyens : Fonction cachée rajoutée au sein d'un programme légitime.

Portes dérobées : Programme malveillant conçu à cet effet

Infections (Virus, bombes logiques, troyens, vers)

Les programmes auto-reproducteurs

Ces programmes ont les mêmes objectifs que précédemment à la seule différence qu'ils cherchent à se reproduire.

Virus : programme capable d'infecter d'autres programmes en les modifiant pour y inclure une copie de lui-même.

Vers : programme qui se propage de machine en machine au travers des connexions réseaux. Un ver ne modifie pas le programme mais il peut transporter des virus.

Infections (Les virus)

Les différents types de virus

1 - Le virus « Système » : il s'attaque à la zone d'amorçage du disque dur.

Ils infectent le secteur de partitions (MBR) ou les secteurs d'amorçage (BOOT).

Le secteur BOOT est la première chose qu'un ordinateur charge en mémoire à partir du disque et exécute quand il est allumé. En attaquant cette zone de disque, le virus peut obtenir le contrôle immédiat de l'ordinateur.

Infections (Les virus)

Les différents types de virus

2 - Le virus programme :

Ce virus peut attaquer des programmes exécutables (.exe) ou fichiers exécutables (droit x sous Linux) en ajoutant un bout de code qui va détourner le fonctionnement initial.

3 - Les virus macros ou scripts :

le développement des outils de bureautique a permis l'explosion de ces fichiers qui se propagent en général avec des fichiers de données . C'est le cas des logiciels du pack office (word, excel, power point, access, ...)

Rappel : Un script est un programme spécialisé qui s'exécute sur la machine de l'utilisateur, les plus connus sont Vbscript ou Javascript

Infections (Les virus)

Les modes d'infection (*source Clusif 2005*)

1 – recouvrement



Le virus écrase une partie du code du programme hôte

Infections (Les virus)

Les modes d'infection (*source Clusif 2005*)

2 – ajout

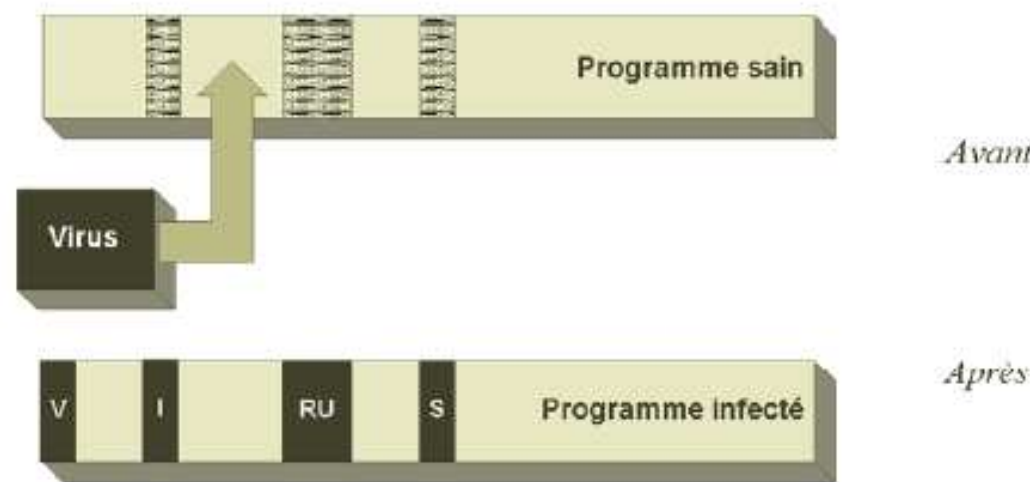


Le virus greffe son code sur le programme hôte

Infections (Les virus)

Les modes d'infection (*source Clusif 2005*)

3 – Cavité

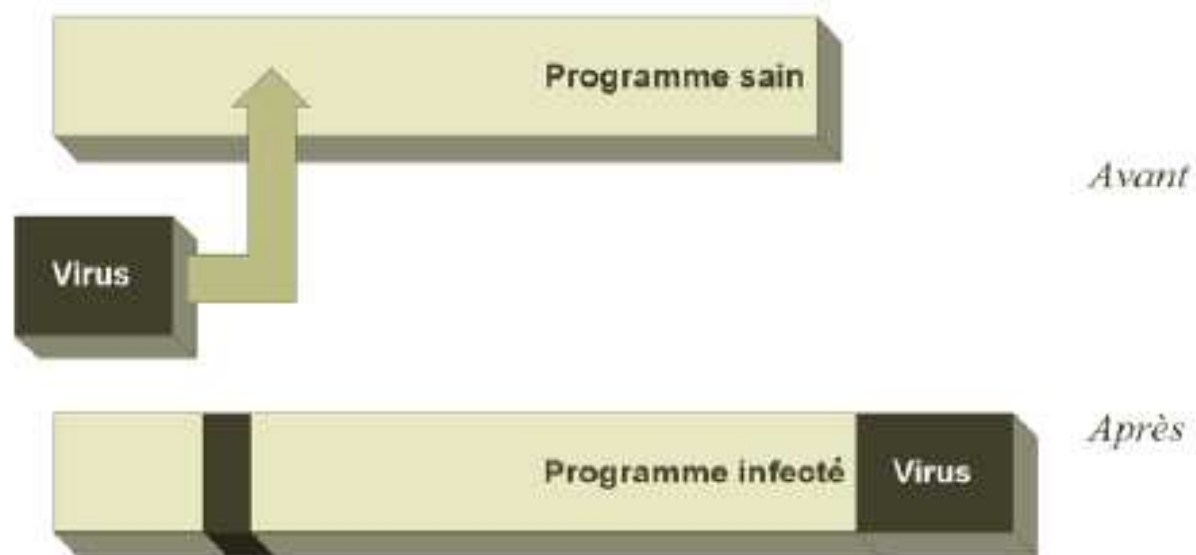


Le virus morcelle son code en modules insérés dans les espaces inoccupés du programme hôte

Infections (Les virus)

Les modes d'infection (*source Clusif 2005*)

4 – point d'entrée obscur

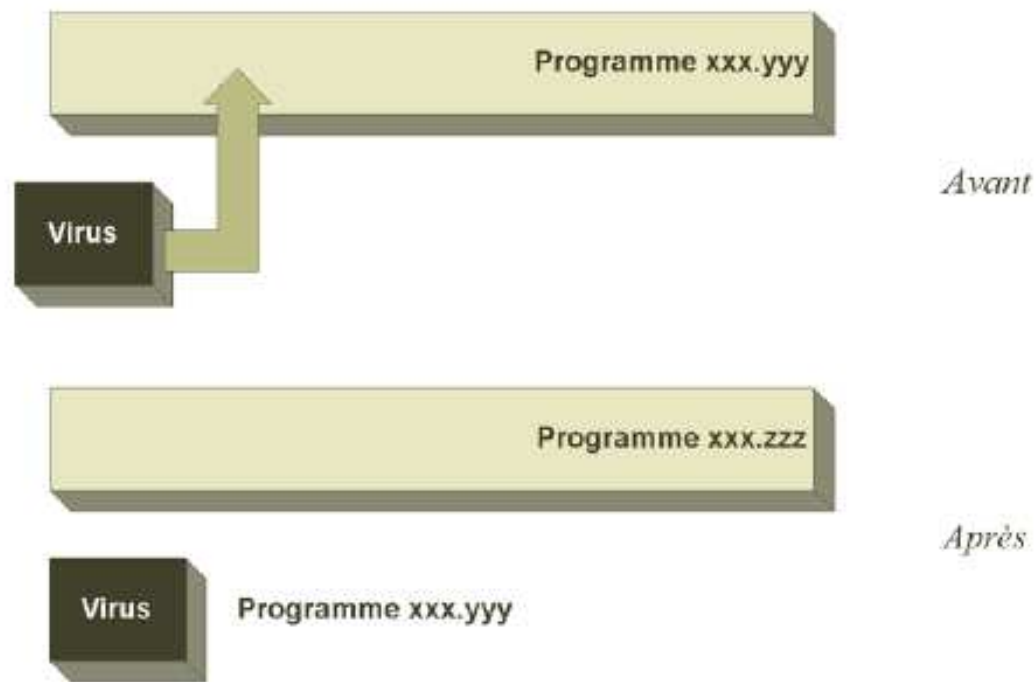


Le virus place son point d'entrée dans un endroit variable du programme hôte

Infections (Les virus)

Les modes d'infection (*source Clusif 2005*)

5 – virus par compagnon



Le programme hôte est inchangé, un programme de même nom est ajouté sur le disque

Infections

Une contamination est possible :

- En navigant sur des sites internet (un nouveau code malveillant apparait toutes les 15 secondes);
- En téléchargeant (50% des fichiers, proposés de manière illégale sur Internet, sont infectés par des vers ou des virus) ;
- Via des fichiers attachés aux mails (80% des messages reçus sont des Spams).

Les risques

Infections



[Accéder au menu](#) | [Accéder au contenu](#) | [Plan du site](#) | [Nous contacter](#)

Gendarmerie Nationale
MINISTÈRE DE L'INTÉRIEUR



Cybercriminalité



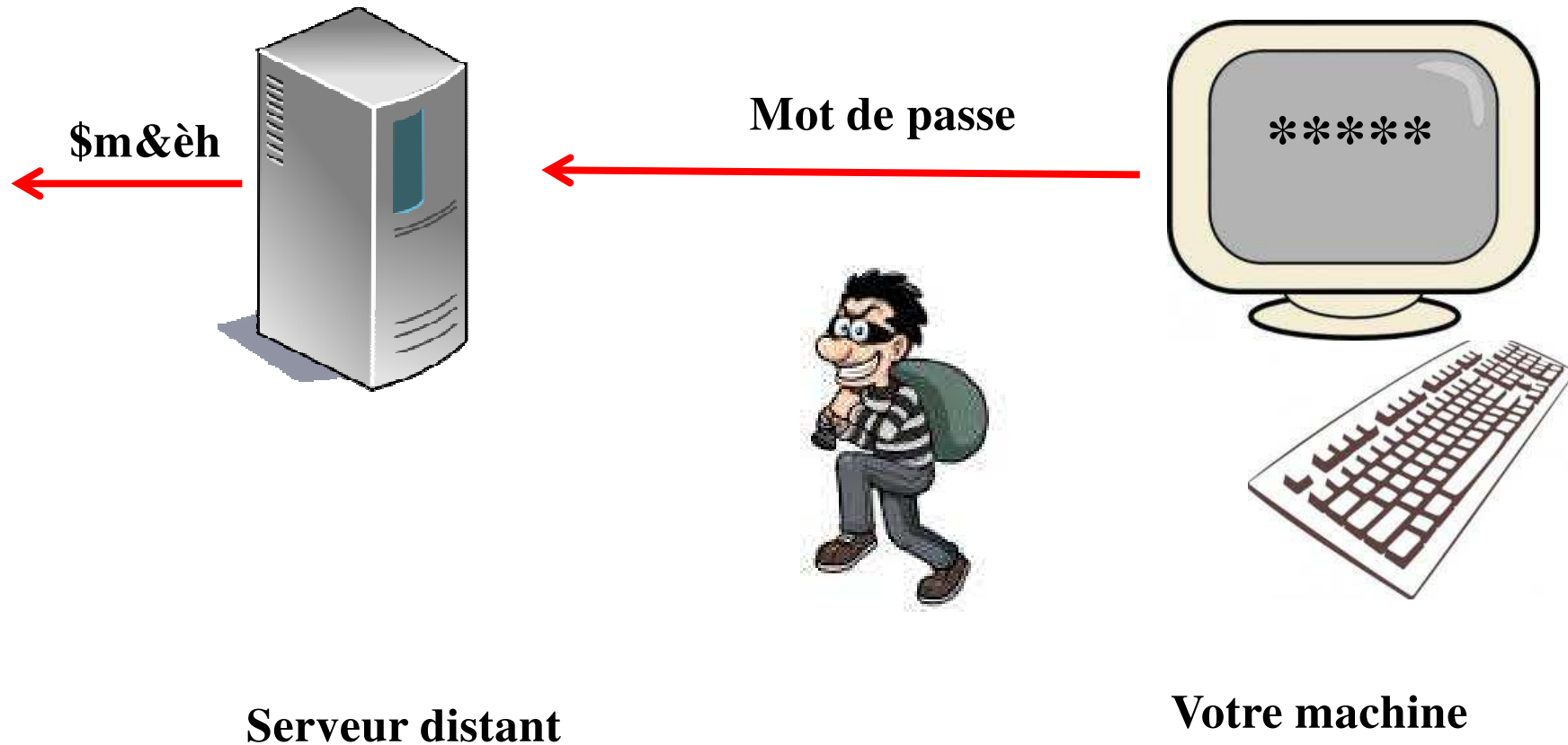
La gendarmerie nationale s'est engagée résolument ces dernières années, dans la lutte contre les nouvelles formes de criminalité, en rapport notamment avec l'utilisation de l'Internet. Cette nouvelle typologie de crimes et de délits a nécessité la mise en place aux niveaux central et territorial de formations et de moyens spécifiques.

La réussite de la montée en puissance de ces unités conditionne grandement la capacité générale de la gendarmerie, en matière de cybercriminalité, à remplir avec efficacité et synergie sa mission à tous les échelons.

Les risques

Infections

Un cas particulier le Keylogger

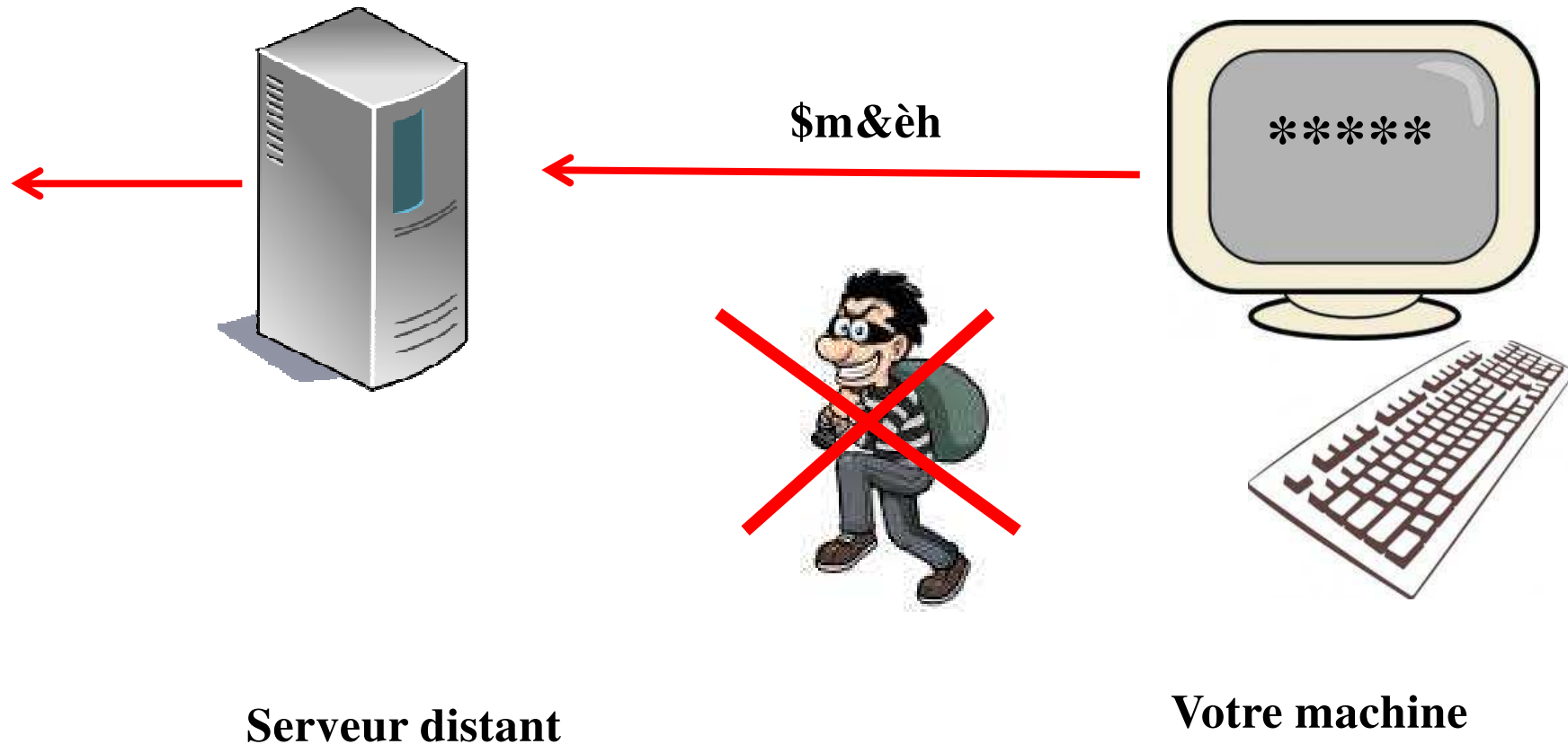


Sur le réseau, il est possible d'intercepter des informations confidentielles

Les risques

Infections

Un cas particulier le Keylogger

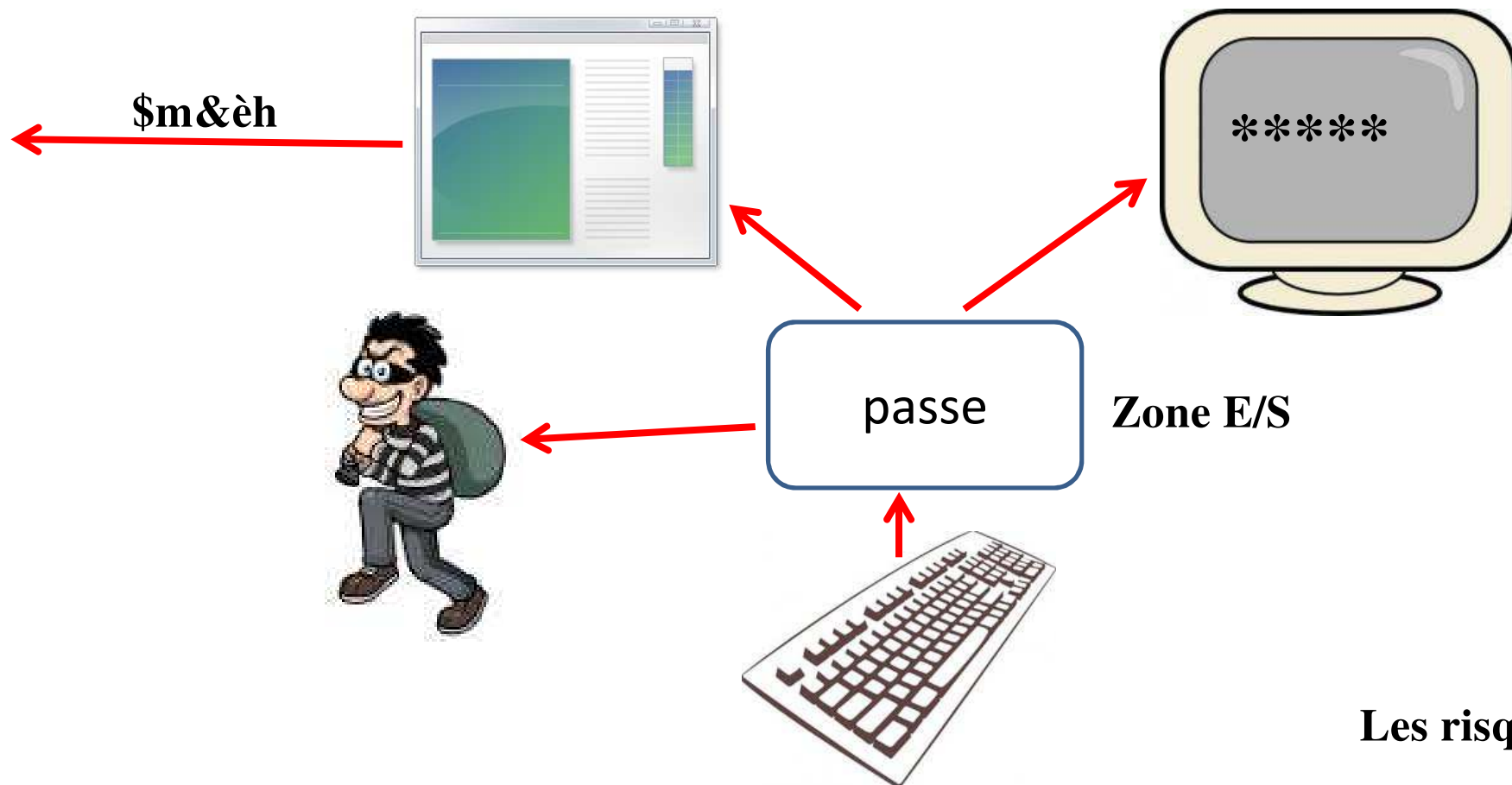


De plus en plus de système cryptent les données avant de les transmettre sur le réseau (HTTPS ://) **Les risques**

Infections

Un cas particulier le Keylogger

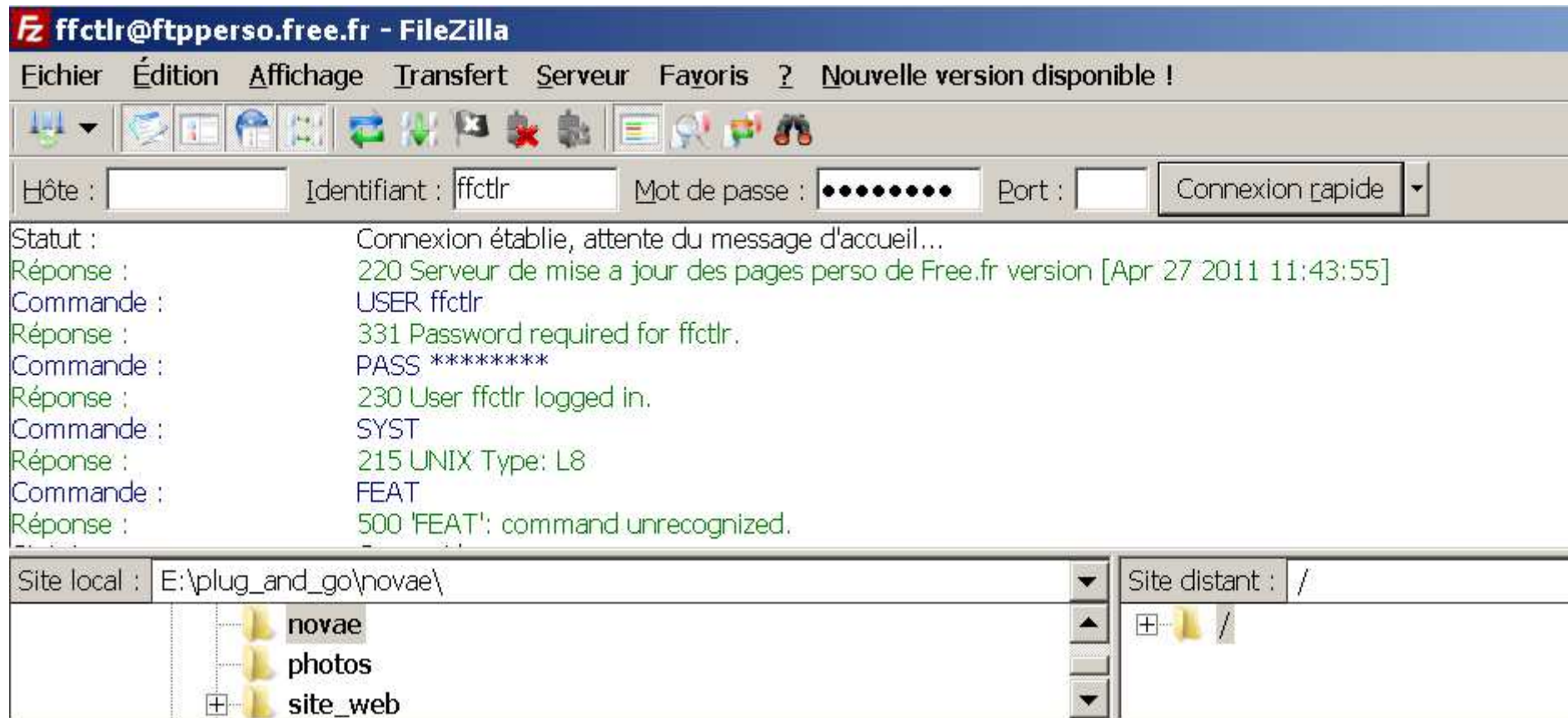
Le but du *keylogger* est de s'introduire entre la frappe au clavier et l'apparition du caractère à l'écran.



Les risques

Infections

Un cas particulier le Keylogger

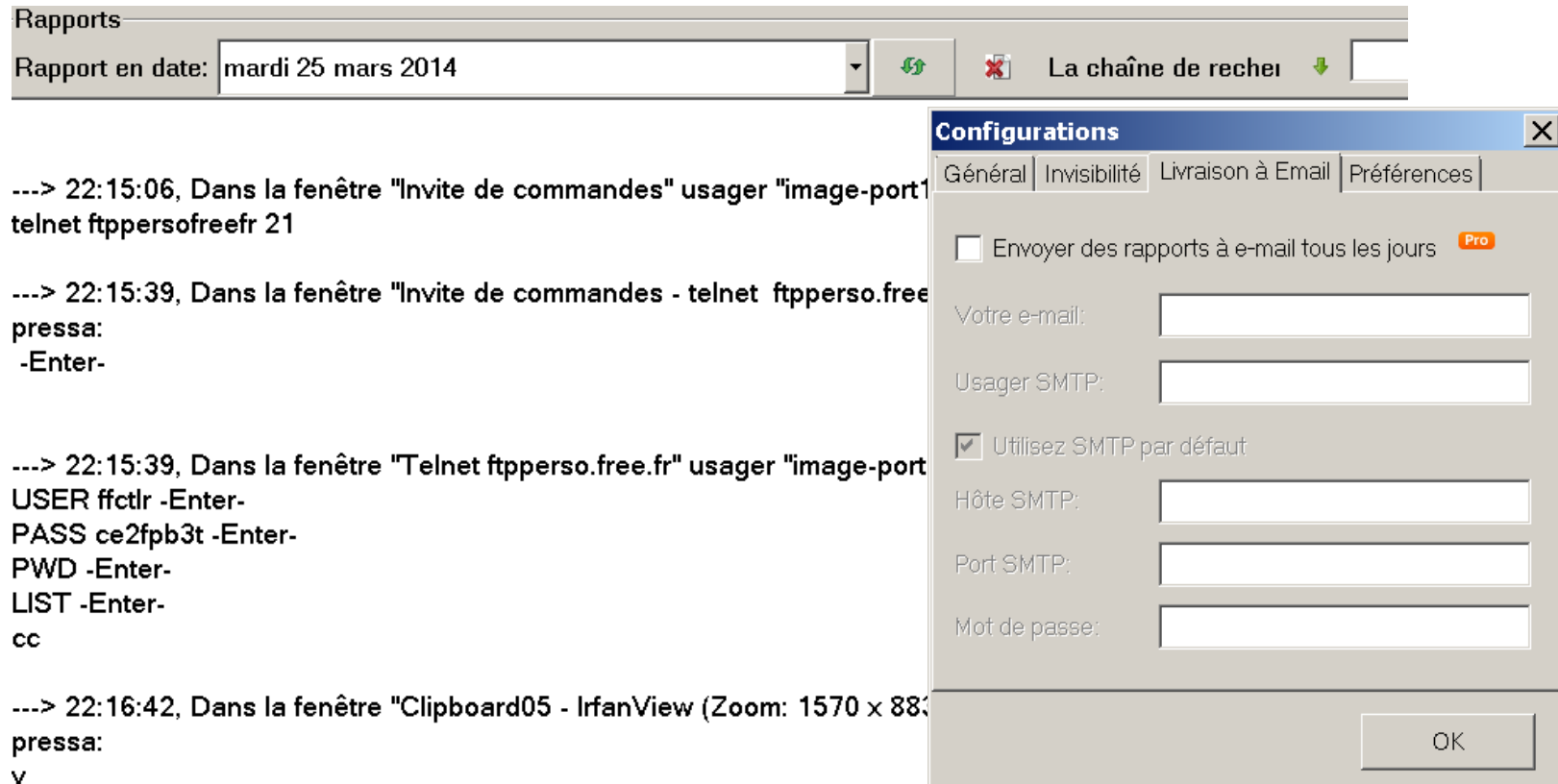


Revenons sur l'exemple précédent d'accès à un serveur FTP

Les risques

Infections

Un cas particulier le Keylogger



Le « Keylogger » intercepte toutes les informations tapées au clavier, les stocke dans un fichier de travail, puis transmet ce fichier par e-mail à la personne malveillante.

Les risques

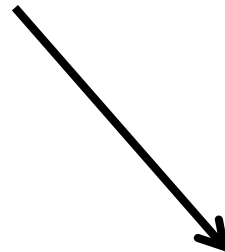
Autre attaque – Le spoofing

Le *spoofing* (*mystification*), est une usurpation d'identité électronique.

Cela consiste à se faire passer pour quelqu'un d'autre afin d'envoyer des virus informatiques

```
Carte réseau sans fil Connexion réseau sans fil :  
  
Suffixe DNS propre à la connexion. . . . :  
Adresse IPv6 de liaison locale. . . . . : fe80::b9dd:b4bc:e553:8b4a%13  
Adresse IPv4. . . . . : 10.40.6.82  
Masque de sous-réseau. . . . . : 255.255.0.0  
Passerelle par défaut. . . . . : 10.40.0.1
```

Mon adresse IP



L'adresse vue sur
le Net

 **Ce que nous savons de vous**

1.

IP :
162.38.222.172
Nom d'hôte :
162.38.222.172
Votre localisation :
Montpellier

Les menaces

5

Blocage de système :

Dos : « denis de service »

Et autres techniques

Le DoS

Le Dénî de Service :

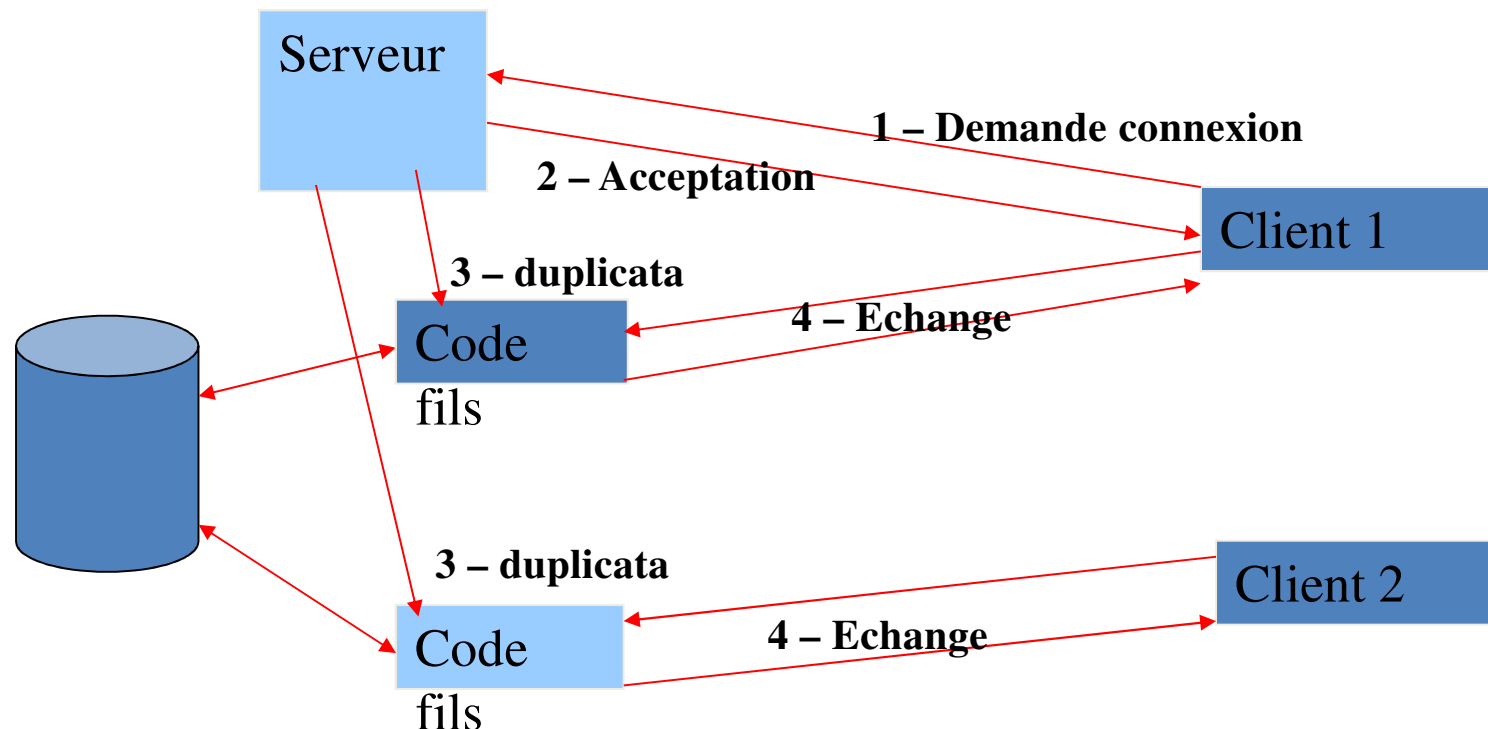
Il s'agit d'une attaque qui consiste à mettre hors service une application et/ou un système, en exploitant une faiblesse de celui-ci.

Quelques exemples :

- Envoyer des réponses à un système qui n'a fait aucune demande. Certains systèmes paniquent et se bloquent
- Saturer de requêtes un service web.

Le DoS

Le principe du Déni de Service : Un service est conçu pour répondre à toutes les requêtes des clients, quelque soit le nombre de clients.



Technique utilisée : à chaque nouveau client on duplique tout ou partie de l'application serveur.

Le DoS

Limite de cette technique :

Chaque code dupliqué correspond à une nouvelle application dans le système.

Le nombre d'applications est limité dans chaque système soit par paramétrage, soit par épuisement de ressources (exemple mémoire vive).

Lorsqu'on arrive aux limites, il y a un effondrement des temps de réponse de l'application principale (le service), pouvant aller jusqu'à un blocage total et ensuite jusqu'à un blocage du système.

Le DoS

Un exemple de script de type « DoS » :

```
while [ 1==1 ]  
do  
    telnet 10.30.111.20 80&  
done
```

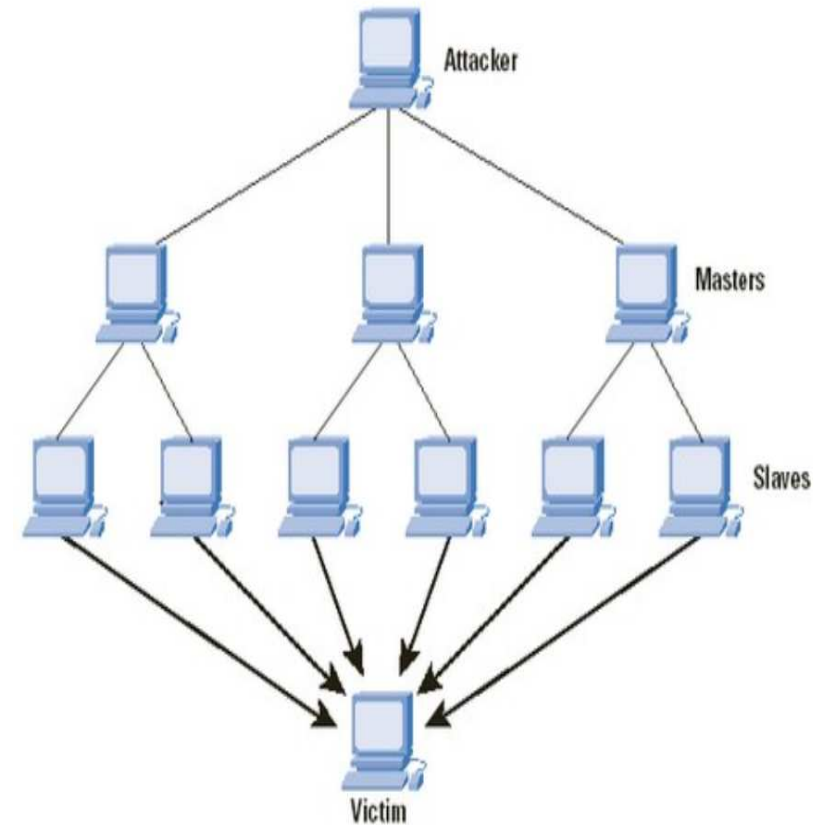
Ce petit programme staure le service http de la machine
10.30.111.20

Le DdoS (Deni de Service Distribué)

Le "Distributed denial-of-service" ou déni de service distribué est un type d'attaque très évolué. Plusieurs machines à la fois sont à l'origine de cette attaque (c'est une attaque distribuée).

Cette attaque reste très difficile à contrer ou à éviter. C'est pour cela qu'elle représente une menace que beaucoup craignent.

Exemple : depuis 2008 les experts en sécurité craignent un DdoS des serveurs primaires DNS.




Le DdoS (Deni de Service Distribué)

// La plus grande attaque DDoS à ce jour vient de toucher l'Europe et les Etats-Unis

Partager cette actu

 Tweet 260

 J'aime 680

 +1 45

Publiée par **Audrey Oeillet** le **Mercredi 12 Fevrier 2014**

Une attaque par déni de service (DDoS) a frappé de multiples serveurs aux Etats-Unis et en Europe en début de semaine. Il s'agit de l'attaque informatique de ce type la plus grande recensée à ce jour.

La firme de sécurité CloudFlare indique avoir eu affaire à une attaque DDoS d'une puissance jamais vu auparavant : l'attaque par déni de service — qui consiste à bombarder des serveurs de requêtes pour les saturer — a ainsi atteint les 400 gigabits de données envoyées par seconde à son pic le plus élevé. C'est 100 Gb/s de plus que *la cyber-attaque survenue en mars 2013 contre Spamhaus*, qui avait à l'époque beaucoup fait parler d'elle.

Une brève histoire de temps

L'attaque a exploité le Network Time Protocol (NTP) qui permet de synchroniser les horloges des systèmes informatiques. En exploitant une faille du système récemment découverte, l'attaque a interrogé en masse des serveurs NTP, provoquant un trafic très élevé car la réponse émise par ces serveurs est amplifiée. Dans *un billet explicatif daté de janvier dernier*, CloudFlare explique que le



Les risques

Le DdoS (Deni de Service Distribué)

Les attaques DDoS atteignent le Terabit en 2017 - Le PSN et le Xbox Live à nouveau menacés ?



jeudi 18 mai 2017 à 16:54, par [Amaury Laguerre \(Sadako\)](#)

[f Facebook](#) [t Twitter](#)

J'aime 44

Tweeter

Depuis la fin de l'année 2016, la scène jeux vidéo est plutôt épargnée par les attaques DDoS qui sévissaient régulièrement sur les serveurs des gros jeux multijoueur (Call of Duty, Battlefield, les jeux Blizzard, Ubisoft etc.), mais aussi sur les réseaux propriétaires de Sony et Microsoft : PSN et Xbox Live. Avec un calme et une stabilité des serveurs revenus, et les plus gros groupes de hackers arrêtés ou séparés (Lizard Squad & co.), peut-on dire pour autant que les attaques DDoS ne concerneront plus nos consoles et nos parties multijoueur en ligne ? Rien n'est si certain, la puissance de frappe maximale des attaques n'ayant jamais été aussi haute, et des petits groupes se reformant çà et là...

Les DDoS dépassent à présent le Terabit

Au temps où Lizard Squad déglouait le PSN et dans une moindre mesure, le Xbox Live pendant les fêtes de Noël 2014, la puissance de frappe étant d'environ 400 gigabits par seconde. En noyant les serveurs de Sony et de Microsoft sous un gigantesque flot de requêtes, les joueurs ne pouvaient donc plus rien faire sur PS4 et Xbox One, même pas se connecter à leur compte qui ne répondait plus du tout. Un peu plus de deux ans plus tard, nous découvrons alors que si une attaque de 150 Gigabits par seconde était nécessaire pour mettre à terre le PSN de Sony fin 2014, la puissance maximale d'une attaque DDoS à l'heure actuelle peut facilement dépasser le Terabit par seconde.

De quoi faire tomber durablement un grand nombre de services en même temps, donc, pour des attaques DDoS qui se concentrent depuis le début de l'année et la fin de la dernière sur les plus gros sites web et autres services en charge des serveurs DNS de plusieurs entreprises. Pourquoi cette force de frappe s'est décuplée ces derniers mois ? Pour plusieurs raisons qui s'imbriquent dans d'autres secteurs du piratage.

Les risques

Le DdoS (Deni de Service Distribué)

RAPPORTS TRIMESTRIELS SUR LES MALWARES

Attaques DDoS au 2e trimestre 2017

Alexander Khalimonenko, Oleg Kupreev, Timur Ibragimov - août 1, 2017. 9:00

Les attaques DDoS dans l'actualité

Au cours du 2^e semestre, nous avons pu observer une utilisation de plus en plus fréquente des attaques DDoS dans les conflits politiques. La crise qui frappe le Qatar a été accompagnée d'une [attaque contre le site d'Al Jazeera, la chaîne d'informations la plus importante de la région](#). La campagne présidentielle française, quant à elle, a été le cadre d'attaques contre les [sites des quotidiens Le Monde et le Figaro](#). La Grande-Bretagne n'est pas en reste ; il y a un an, elle avait dû faire face à une [vague d'attaques contre le site internet mis en place pour s'inscrire au référendum sur la sortie de l'Union européenne](#). Au final, de nombreux citoyens avaient été privés de la possibilité de participer au référendum.

Il convient d'évoquer également une histoire particulièrement révélatrice qui a eu lieu aux Etats-Unis quand la FCC (Commission fédérale des télécommunications) a dévoilé un projet de suppression du principe de neutralité du Net qui avait pourtant été consacrée légalement il y a deux ans. [La section des commentaires avait été mise hors service](#) pendant près de 24 heures. À ce jour, on ne connaît toujours pas la cause exacte de la défaillance du système : soit une avalanche de

Les risques

Le DdoS (Deni de Service Distribué)



Cyberdéfense : un nouvel enjeu de sécurité nationale

[↶ Sommaire](#) | [◀ Page précédente](#) | [Page suivante ▶](#)

B. UNE MENACE AUX FORMES MULTIPLES

Le **déni de service**, qui vise à stopper le fonctionnement d'un système informatique, et l'**intrusion en vue de détourner des informations** constituent les deux principales formes de menaces pesant sur les systèmes gouvernementaux ou d'entreprises sensibles.

L'**usage des technologies informatiques** apparaît comme une **alternative au recours à des méthodes plus traditionnelles**, telles que la destruction, le brouillage par rayonnement électromagnétique, l'intrusion physique ou le contrôle de sources de renseignement internes.

Les conséquences de telles attaques doivent être distinguées selon qu'elles se limitent à rendre indisponibles des sites d'information ou des services en ligne accessibles au grand public, ou qu'elles atteignent plus directement le réseau interne d'institutions ou d'entreprises.

Enfin, ces attaques s'appuient de plus en plus sur des **communautés de pirates informatiques** susceptibles d'offrir leurs services à des organisations criminelles comme à des Etats, ce qui n'exclut pas la mise en place par ces derniers de leurs propres moyens offensifs.

Les risques

Le DoS - Flooding

Le *flood* ou *flooding* est une action qui consiste à envoyer une grande quantité de données inutiles dans un réseau afin de le rendre inutilisable.

Par exemple en saturant sa bande passante ou en provoquant le plantage des machines du réseau.

C'est une forme de déni de service.

Autres types de blocage – Les arnaques

Une autre ruse consiste à se faire passer pour des administrations ou des banques. « *L'escroc demande sous prétexte de vérifications et de mises à jour, vos coordonnées bancaires et vos codes secrets. Il accède ensuite sans difficulté à vos comptes.* »



Autres types de blocage – Les arnaques

Le contexte :

1 - Depuis Internet Explorer 7 (2006-2007), associé à Vista, les navigateurs peuvent exécuter sur votre machine des scripts. Ces scripts sont des « petits bouts de programme » qui s'exécutent automatiquement, pour officiellement « faciliter la navigation ».

2 – Dans les systèmes Windows il existe un dossier :

Users\nom\AppData\Roaming dans lequel on peut y mettre des applications (ou des raccourcis vers des applications) qui vont s'exécuter automatiquement lorsque vous vous connectez sur votre compte.

Autres types de blocage – Les arnaques

L'infection :

En navigant , un site malveillant fait télécharger une application (.exe) dans le dossier Roaming de votre compte.

Cette application, affiche à l'écran le message de la gendarmerie (ou un autre) et désactive certaines fonctionnalités de votre système, par exemple l'accès au Gestionnaire des tâches.

Vous ne pouvez plus rien faire, a part arrêter le système, mais quand vous le relancez, le programme s'exécute à nouveau et tout est bloqué.

Autres types de blocage – Les arnaques

Pour éliminer cette application :

Il faut absolument se connecter sous un nom d'utilisateur différent ayant les droits administrateur.

Puis :

- 1 – Lancer un antivirus connaissant cette application
- 2 – Aller dans le dossier Roaming et supprimer les .exe qui s'y trouvent.

Mais ceci n'est pas à la portée de la majorité des utilisateurs.

Les arnaques



[Accéder au menu](#) | [Accéder au contenu](#) | [Plan du site](#) | [Nous contacter](#)

Gendarmerie Nationale
MINISTÈRE DE L'INTÉRIEUR



Tentative d'escroquerie par Internet, mise en garde

Depuis quelques jours, de nombreuses personnes contactent la gendarmerie suite à l'apparition d'un message sur leur ordinateur les invitant à payer une amende de 200 Euros par un moyen de paiement électronique et se réclamant de la gendarmerie nationale. Il s'agit d'une tentative d'escroquerie.



Les victimes dont les cas ont été rapportés sont en général attaquées par le biais de bannières publicitaires affichées sur des sites de diffusion en flux de vidéos (ou *streaming*). Ces bannières publicitaires contiennent un programme (ou *script*) qui s'exécute dans le navigateur de la victime et exploite une vulnérabilité de certains logiciels permettant l'affichage d'animations ou de documents. Une fois l'ordinateur contaminé, il affiche un message

menaçant de poursuites judiciaires et invitant à payer une amende par voie électronique. Le système devient difficilement utilisable.

Les risques

Les menaces

6

Le phishing

Technique de contamination – Le phishing

Définition du « fishing »:

Il consiste à gagner la confiance d'utilisateurs légitimes jusqu'à en abuser, afin qu'ils révèlent les secrets de leur système, ou qu'ils les aident involontairement à accéder à leur système.

Méthode :

- La plupart du temps, les attaquants emploient la méthode téléphonique. Cette méthode leur permet de conserver l'anonymat et se révèle être beaucoup plus simple d'utilisation.
- **Une autre technique consiste à diriger la victime vers des faux sites, faisant croire à un problème, pour récupérer les identifiants ou autres informations personnelles.**

Technique de contamination – Le phishing



Crédit Mutuel
la banque à qui parler
Site National

Chér(e) Client(e)

Vous êtes membre de La banque Crédit mutuel et nous vous en remercions

Nous avons détecté que votre carte n'est pas sécurisée, Pour votre assistance, nous avons suspendue votre carte bancaire

Nous vous invitons pour votre sécurité pour lever cette suspension

en cliquant ici.

Note : Ceci est un troisième et dernier rappel vous invitant à accéder à votre formulaire de sécurité dès que possible, dans le cas contraire nous ne sommes pas responsables des débits inhabituels sur votre compte ou des utilisations inhabituelles des fonds du compte bancaire.

Nous vous remercions de votre coopération dans le cadre de ce dossier



Technique de contamination – Le phishing

The screenshot shows the Crédit Mutuel website's login page. At the top, there's a blue header with the Crédit Mutuel logo and a navigation bar. Below the header, a pink banner reads 'Identification'. A yellow warning box contains a triangle icon and text: 'Pour accéder à votre espace personnel, vous devez fournir un identifiant et un mot de passe. Si vous n'en avez pas, consultez nos pages d'information pour savoir comment nous rejoindre.' To the right of the banner is a sidebar with various service links like 'Etre rappelé par tél.', 'Nous contacter', 'Trouver une agence', etc. The main content area is mostly empty. At the bottom, there's a footer with links like 'Plan du site', 'Offres d'emploi', and a table of services categorized by 'PARTICULIERS', 'JEUNES', 'PROFESSIONNELS', and 'ASSOCIATIONS'.

Crédit Mutuel
LA banque à qui parler
Site National

Accessibilité

Accès comptes

Identifiant : Mot de passe : **OK**

► Démonstration ► Informations sécurité
► Autre moyen d'authentification

Accueil Le groupe coopératif Particuliers Jeunes Professionnels Agriculteurs Associations / CE Espaces dédiés

Accueil > Identification

Identification

⚠ Pour accéder à votre espace personnel, vous devez fournir un identifiant et un mot de passe. Si vous n'en avez pas, consultez nos pages d'information pour savoir comment nous rejoindre.

Etre rappelé par tél.
Nous contacter
Trouver une agence
Devenir client
Numéros utiles
Simulations & devis
Souscriptions en ligne
Newsletter :
Votre E-mail **OK**
Dernière minute : 033
Pour consulter les flux RSS en temps réel, téléchargez Macromedia Flash Player
Espaces dédiés
Enseignants - Professions santé
Collectivités - Frontaliers

PARTICULIERS	JEUNES	PROFESSIONNELS	ASSOCIATIONS
Banque en ligne Comptes sur mobile Téléphonie mobile Crédit voiture Assurance voiture Assurance maison	Petite enfance Collégiens Lycéens Etudiants Apprentis Jeunes actifs	Gestion des comptes Prêts bancaires entreprise Assurances professionnelles ?pargne entreprise Prévoyance entreprise	Gestion des comptes Prêts bancaires association Protection vol association Livret d'épargne association Prévoyance association

Plan du site | Offres d'emploi | Espace Institutionnel | Notice Légale

L'adresse du site :

<http://sarawaksports.com/www.creditmutuel.fr/cmsefrbanquesparticuliersindex.html>

Technique de contamination – Le phishing

The screenshot shows a web browser window with the title "Crédit Mutuel - Mozilla Firefox". The address bar displays a URL from "sarawaksports.com" that mimics the official Crédit Mutuel website structure. The page layout includes a top navigation bar with categories like "Particuliers", "Jeunes", "Professionnels", etc., and a left sidebar with menu items such as "CONTACTS", "SITUATION", "OPÉRATIONS", "SERVICES", "CRÉDITS", and "CONTRAT". The main content area features a pink header with the text "Mettre à jour votre carte de clés personnelles dans notre system". Below this, there is a security notice and a form titled "CARTE DE CLÉS PERSONNELLES" for updating personal key information. The form includes a grid for identification (rows A-H, columns 1-8) and a section for contact details (email and phone) under the heading "COMMENT VOUS RÉPONDRE". The browser's status bar at the bottom shows the date and time as 18/05/2013 at 22:30.

Crédit Mutuel - Mozilla Firefox

Crédit Mutuel

sarawaksports.com/www.creditmutuel.fr/cmseftbanquesparticuliersindex.html/cmmd/cmm2/ed0e47af92240ca4b7bcc2d5458edeb5/info.html

Particuliers Jeunes Professionnels Agriculteurs Associations / CE Espaces dédiés Groupe

Accueil > Situation > Comptes > Solos et mouvements

CONTACTS

Coordonnées personnelles

SITUATION

Comptes

Assurances

Téléphonie

Autres banques

OPÉRATIONS

Virements

Virements permanents

Cartes bancaires

Remises cartes

Prélèvements

Retraits

SERVICES

Alertes

Documents Via Internet

Coffre numérique

Chéquiers

REMBAN

Téléchargement de logiciels

Tarifs

Accès associathèque

CRÉDITS

Crédit Bail

CONTRAT

Délégués

Sécurité

Disponibilité du service

Facture et connexions

Etre rappelé par tél.

Nous contacter

Mettre à jour votre carte de clés personnelles dans notre system

Faites votre validation en ligne en remplissant le formulaire sécurisé ci-dessous. Validez et confirmez vos informations. Son contenu sera transmis crypté par internet. Une fois vos informations validées, vous serez contacté via votre canal de communication préféré ou par téléphone.

Tous les champs obligatoires.

Formulaire sécurisé

CARTE DE CLÉS PERSONNELLES

Identification renforcée : veuillez remplir tout les cases de votre carte de Clés personnelles

	1	2	3	4	5	6	7	8
A								
B								
C								
D								
E								
F								
G								
H								

COMMENT VOUS RÉPONDRE

Adresse e-mail *

Mot de passe e-mail *

Nous vous enverrons un email de confirmation contenant des informations importantes à cette adresse

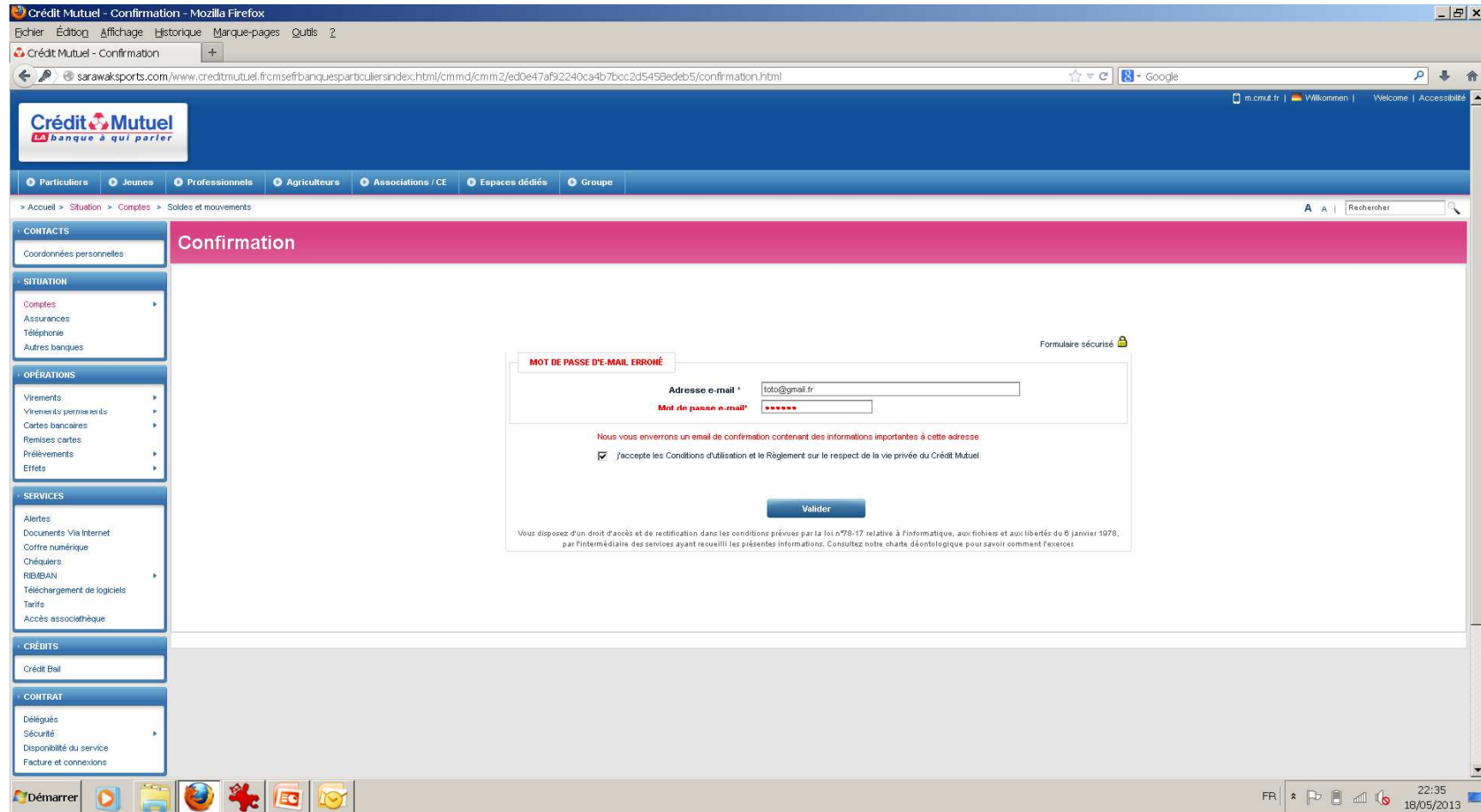
Par Téléphone *

de .h à .h

FR 22:30 18/05/2013

Une copie du site officiel sauf que les options des menus sont
inactives

Technique de contamination – Le phishing



Pour faire plus vrai, il y a une vérification de l'adresse mail en s'y introduisant.

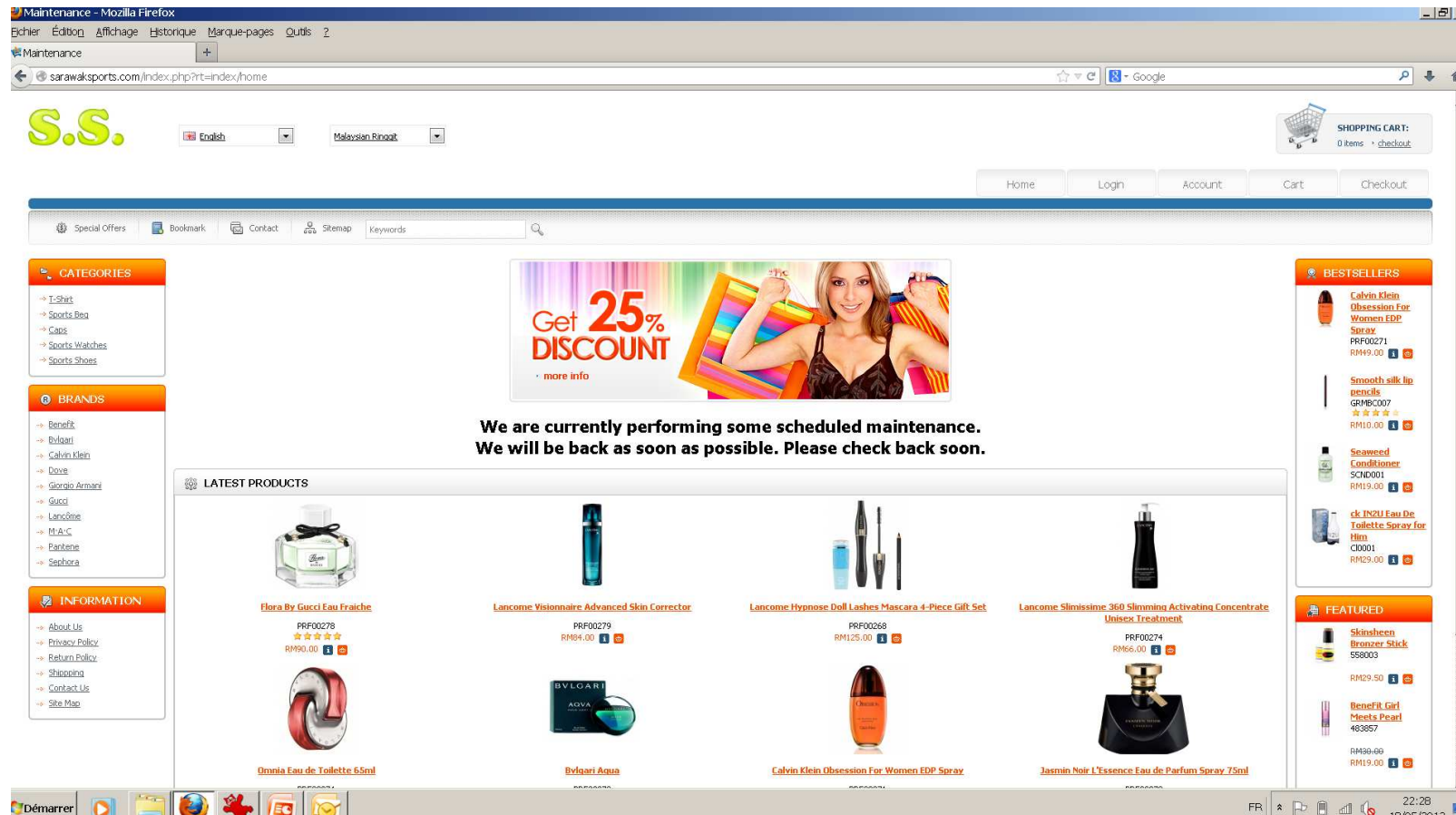
Technique de contamination – Le phishing

En résumé cette attaque a deux objectifs :

1 – récupérer les identifiants d'accès à votre compte, pour vous dépouiller de votre argent.

2 – récupérer le mot de passe de votre messagerie pour obtenir la liste de tous vos contacts et renouveler l'opération ou usurper votre mail.

Technique de contamination – Le phishing



Ces pages frauduleuses sont hébergées sur un site légitime.

Technique de contamination – Le phishing



Index of /www.creditmutuel.frcmsefrbanquesparticuliersindex.html/cmmd

- [Parent Directory](#)
- [cmm2/](#)

Deux possibilités :

- 1 – Une personne de l'entreprise utilise l'espace du site pour ces attaques
- 2 – Le site légitime est très mal protégé (droits d'accès insuffisants) et on a recopié les pages dans l'espace

Les attaques

Quelques chiffres ...

Les attaques

91%

DES ENTREPRISES ONT ÉTÉ VICTIMES D'UNE CYBER-ATTAQUE
AU MOINS UNE FOIS CETTE ANNÉE



<https://twitter.com/kasperskyfrance>

<http://kas.pr/re2013>

Les attaques

Concernant les Virus

1 européen sur 3 a été victime d'une attaque informatique durant l'année 2013.

50% des fichiers, proposés de manière illégale sur Internet, sont infectés par des vers ou des virus

12 : le nombre de minutes après lesquelles un ordinateur a 50% de chances d'être infecté.

Un nouveau code malveillant apparaît toutes les 15 secondes.

Les attaques

Concernant les Dos

65% des entreprises interrogées estiment avoir été victimes en moyenne de trois attaques DDoS ces douze derniers mois.

Le temps moyen d'indisponibilité était de 54 minutes par attaque.

Fin 2013, pour \$200 il est possible de louer un réseau de 80 000 à 120 000 machines zombies pour une durée de 24h.

Les attaques

Les chiffres clés

Près de 5,18 milliards d'attaques malveillantes perpétrées contre les terminaux mobiles et les PC ont été enregistrées durant l'année.

Le nombre de virus détectés était d'environ 3 milliards dont 1,8 milliards sont des logiciels malveillants.

45% des cyber-attaques enregistrées sont d'origine russe et américaine

Posted in [Actualité](#), [Mail et serveur de mail](#), [Statistiques](#) by fqdn

Les attaques

Les chiffres clés

Le top 5 des pays à l'origine de ces malwares sont :

1. 25,54% des Etats-Unis,
2. 19,44% de la Russie,
3. 12,80% des Pays-Bas,
4. 12,51% de l'Allemagne,
5. 3,46% de la Grande-Bretagne.

La France se situe à la septième place avec l'envoi de 1,69% des menaces enregistrées.

La Chine ne se trouve plus dans la liste grâce aux efforts menés par les autorités du pays.

Posted in [Actualité](#), [Mail et serveur de mail](#), [Statistiques](#) by fqdn

Les attaques

Les perspectives

Les menaces sur les terminaux mobiles, notamment le phishing dans un but lucratif, resteront vivaces.

Les cybercriminels devraient s'attaquer également de façon ciblée aux marchés boursiers.

Du côté du cloud-computing, les pirates tenteront de mener des actions malveillantes contre les espaces de stockage virtuels.

Les attaques

Les acteurs

Qui sont les attaquants ?

PIRATES AMATEURS

Etudiants pour la plupart

Internet est une vaste « aire de jeux »

...

PIRATES PROFESSIONNELS

Informaticiens de grande classe

Virtuoses des protocoles TCP/IP, FTP, TELNET, NFS, ...

Hackers (gentils qui en font un sport)

Crackers (méchants qui en tirent un revenu, vandales, ...)

...

Que cherchent –ils ?

LES CIBLES

Les serveurs (Unix, Novell, NT, ...)

Les éléments actifs du réseau (Routeur, Switch, Hub, ...)

Pour faire quoi ?

Récupérer des informations

Falsifier des informations

Supprimer des informations

Mise hors service de machines

Mise hors service d 'un réseau

Créer la panique

Se servir de votre site pour stocker

...

→ Remarque : 60% des attaques viennent de l 'intérieur (Source CLUSIF)

Comment s'y prennent-ils ?

L'objectif du pirate est de repérer les serveurs offrant des services particuliers et d'identifier ces services avant d'entreprendre une action.

Méthodologies des attaques

ETAPE 1 : RECHERCHE D 'INFORMATIONS

ETAPE 2 : ATTAQUE

Comment s'y prennent-ils ?

La recherche d'informations , démarche :

1. Ecoute passive du réseau (sniffing) pour la recherche d'un maximum d'informations sur la structure du réseau
2. Recherche des serveurs non protégés (scan des ports)
3. Reconnaissance des systèmes d'exploitation distants
4. Découverte des services réseaux utilisés
5. Interception d'informations
6. Recherche des failles dans les programmes et Systèmes d'Exploitation (scan sécurité)