

M3102

Services réseaux

**Introduction à la sécurité dans les
systèmes informatiques**

Introduction générale

Introduction générale

Aujourd'hui l'informatique est partout dans notre vie.

Grâce aux multiples services, les ordinateurs contiennent quantités de données, qui peuvent intéresser beaucoup de monde.

Informations que certains sont prêt à payer très cher :

- Informations bancaires,
- Informations personnelles,
- Documents divers.
- ...

Les ordinateurs sont, aussi, devenus indispensables, et l'on peut vivre difficilement sans eux mais toute panne est souvent dramatique pour l'entreprise.

→ Les équipements informatiques encourent de multiples risques. MAIS POURQUOI ??

Les failles

Les failles

Modèle Internet

Services (http – dns – ftp - ...)



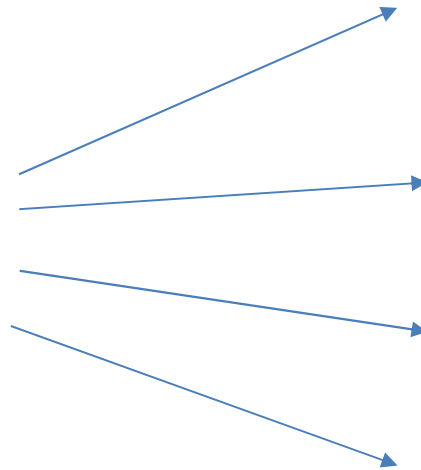
TCP - UDP



IP



Ethernet



Routage

DNS

DHCP

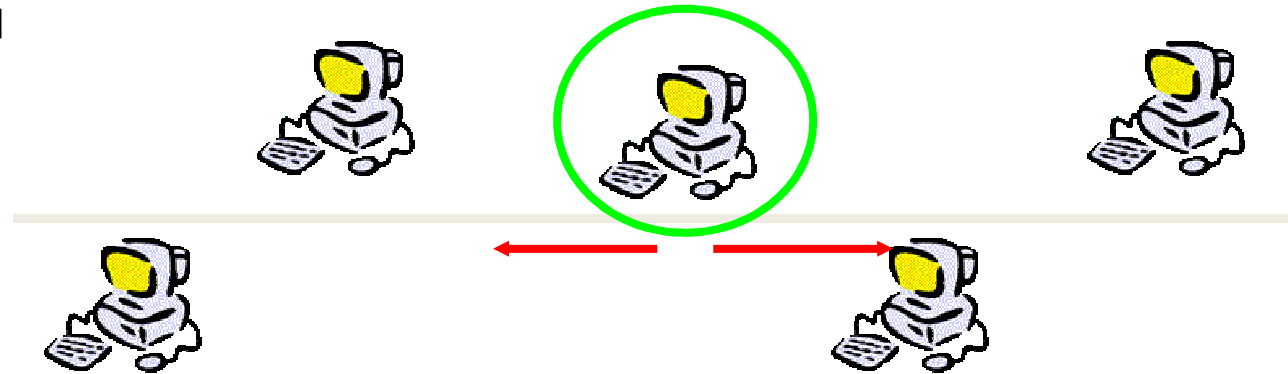
ARP

CSMA/CD

CSMA-CD

Transfert des données = diffusion générale

Le format des trames est public, n'importe qui peut interpréter leur contenu



Les protocoles ne cryptent pas les données échangées.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.67	226.178.217.5	UDP	87	Source port: 55024 Destination port: 21328
2	0.15592500	192.168.1.67	10.10.104.1	TCP	66	49726 > hp-pd1-datastr [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.19372300	109.3.48.154	192.168.1.67	ICMP	94	Destination unreachable (Port unreachable)
4	1.58643500	192.168.1.67	192.168.1.1	DNS	73	Standard query 0x0a9c A www.google.fr
5	1.62708600	192.168.1.1	192.168.1.67	DNS	89	Standard query response 0x0a9c A 173.194.67.94
6	1.63020200	192.168.1.67	173.194.67.94	TCP	66	49730 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	1.67755900	173.194.67.94	192.168.1.67	TCP	66	http > 49730 [SYN, ACK] Seq=0 Ack=1 win=42900 Len=0 MSS=1430 SACK_PERM=1 WS=64
8	1.67779300	192.168.1.67	173.194.67.94	TCP	54	49730 > http [ACK] Seq=1 Ack=1 win=65536 Len=0
9	1.67827300	192.168.1.67	173.194.67.94	HTTP	997	GET / HTTP/1.1
10	1.73155200	173.194.67.94	192.168.1.67	TCP	54	http > 49730 [ACK] Seq=1 Ack=944 Win=42304 Len=0
11	1.83167200	173.194.67.94	192.168.1.67	HTTP	555	HTTP/1.1 302 Found (text/html)
12	1.83886800	192.168.1.67	173.194.67.94	TCP	66	49731 > https [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

ARP

Objectif : fournir, à une machine donnée, l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IP

Pour éviter de répéter plusieurs fois cette opération lourde, les informations sont stockées dans un cache local.

```
C:\Users\image-port10-2011>arp -a

Interface : 192.168.1.67 --- 0xd
Adresse Internet      Adresse physique      Type
192.168.1.1           e0-a1-d7-2a-d6-bc     dynamique
192.168.1.255         ff-ff-ff-ff-ff-ff     statique
224.0.0.2             01-00-5e-00-00-02     statique
224.0.0.22            01-00-5e-00-00-16     statique
224.0.0.252           01-00-5e-00-00-fc     statique
226.178.217.5         01-00-5e-32-d9-05     statique
239.255.255.250       01-00-5e-7f-ff-fa     statique
255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

1 - Une machine envoie une fausse adresse MAC : **ARP-Poisoning**

2 – Le contenu de la mémoire cache peut être modifié intentionnellement : **ARP-Cache Poisoning** :

DHCP

Objectif : Distribuer les adresses IP aux machines.

Epuisement des ressources : Si un pirate génère un grand nombre de requêtes DHCP semblant venir d'un grand nombre de clients différents, le serveur épuisera vite son stock d'adresses. Les «vrais» clients ne pourront donc plus obtenir d'adresse IP : le trafic réseau sera paralysé.

Faux serveurs DHCP : Si un pirate a réussi à saturer un serveur DHCP par épuisement de ressources, il peut très bien en activer un autre à la place. Il pourra ainsi contrôler tout le trafic réseau.

DNS

Objectif : fournir à une machine l'adresse IP correspondant à nom de domaine

Pour éviter de répéter plusieurs fois cette opération lourde, les informations sont stockées dans un cache local.

scolariteparis.cnam.fr

Nom d'enregistrement. : sclariteparis.cnam.fr

Type d'enregistrement : 5

Durée de vie : 41329

Longueur de données . : 8

Section : Réponse

Enregistrement CNAME : klingon.cnam.fr

pop.1and1.fr

Nom d'enregistrement. : pop.1and1.fr

Type d'enregistrement : 1

Durée de vie : 1449

Longueur de données . : 4

Section : Réponse

Enregistrement (hôte) : 212.227.15.140

DNS

DNS - Limites

- 1 – Envoie d'une fausse réponse à une requête DNS avant le serveur DNS. De cette façon, le pirate peut rediriger vers lui le trafic à destination d'une machine qu'il l'intéresse

DNS-spoofing

- 2 - Un serveur DNS n'a que la table de correspondance des machines du réseau sur lequel il a autorité. Pour des machines distantes, il doit interroger d'autres serveurs DNS et garde en mémoire (dans un cache), le résultat des précédentes requêtes. L'objectif du pirate est d'empoisonner ce cache avec de fausses informations : **DNS cache poisoning**

- 3 – Blocage du serveur DNS

Routage IP

Objectif : Permettre à un paquet d'être acheminé vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur.

Le routage repose :

Sur des machines physiques : les routeurs

Sur des fonctions logiques : Tables de routage, logique de routage, format de trame normalisé.

Remarque : IP encapsule des données sans protection (chiffrage)

Routage IP

Déconfiguration IP : on peut supprimer les informations de configuration IP (adresse, masque) dans la machine.

Modification des tables de routage : la commande « route » modifie le contenu d'une table de routage.

Modification de la durée de vie des paquets.

Camouflage d'adresse IP : on utilise une machine intermédiaire qui fait les requêtes à la place d'une autre machine.

TCP

Objectif : Assure le transfert des données entre IP et les applications, fiabilise IP

Désynchronisation TCP : pendant un échange, l'attaquant envoie au client des paquets en y plaçant des mauvais numéros de séquences → le client croit qu'il a perdu la connexion et stoppera ses échanges . Puis l'attaquant envoie les bons numéros de séquences au serveur, il récupère la connexion pour lui.

Interruption d'un échange TCP : pendant un échange, on expédie un message contenant un 'Reset' .

Les services

Considérations générales (1)

Un service est accessible via une @IP et un n° Port

Le dialogue entre service et application cliente est normalisé
→ il est donc facile de les identifier.

Les services sont conçus pour répondre à toutes les requêtes.

Les services

Considérations générales (2)

- Les services fonctionnent sur le principe de la « confiance »

→ Les échanges entre services ne sont pas cryptés.

```
00 17 33 26 12 b0 9c b7 0d 2d 54 6a 08 00 45 00 ..3&.... -Tj..E.
02 a7 07 a7 40 00 80 06 15 a5 c0 a8 01 43 3f f5 .....@... .....C?.
d9 24 c1 62 00 50 99 56 36 e9 37 33 57 8e 50 18 $.b.P.V 6.73W.P.
41 3a 00 86 00 00 47 45 54 20 2f 3f 70 72 6f 64 A:....GE T /?prod
75 63 74 3d 66 69 72 65 66 6f 78 2d 31 38 2e 30 uct=fire fox-18.0
2e 31 2d 63 6f 6d 70 6c 65 74 65 26 6f 73 3d 77 .1-compl ete&os=w
69 6e 26 6c 61 6e 67 3d 66 72 20 48 54 54 50 2f in&lang= fr HTTP/
31 2e 31 0d 0a 48 6f 73 74 3a 20 64 6f 77 6e 6c 1.1..Hos t: downl
6f 61 64 2e 6d 6f 7a 69 6c 6c 61 2e 6f 72 67 0d oad.mozila.org.
0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a .User-Agent: Moz
69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (window
73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b s NT 6.1 ; WOW64;
20 72 76 3a 31 32 2e 30 29 20 47 65 63 6b 6f 2f rv:12.0 ) Gecko/
32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 20100101 Firefox
2f 31 32 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 /12.0..A ccept: t
65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 ext/html ,applica
74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 tion/xhtml+xml,a
```

Les services

Considérations générales (3)

- Des services très bavards

Les informations de votre système

Nous pouvons voir que votre ordinateur utilise le système d'exploitation :

Windows Seven

Votre navigateur est :

Mozilla Firefox

Votre écran a une resolution de :

720x1280 pixels

```
...-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
```

- Des serveurs trop bavards
Les bannières des serveurs web sont trop explicites.

```
GE T / HTTP /1.1..  
Host: www.google.fr.  
User-Agent: Mozilla/5.0 (Windows NT 6.1)  
Firefox/26.0..  
Accept: text/html,application/xhtml+xml|  
Accept-Language: fr,fr-fr;q=0.8,en-us;
```


Les services

Considérations générales (4)

- Des services qui mémorisent tout

Les services enregistrent des copies de données que vous utilisez (Fichiers de travail) , afin de diminuer le temps d'accès (en lecture ou en écriture) .

Problème, c'est que ces zones sont :

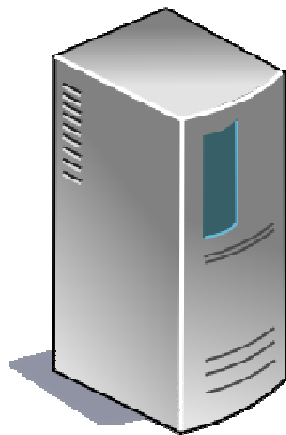
- souvent situées dans des dossiers par défaut ;
- facilement accessibles ;

Conséquences

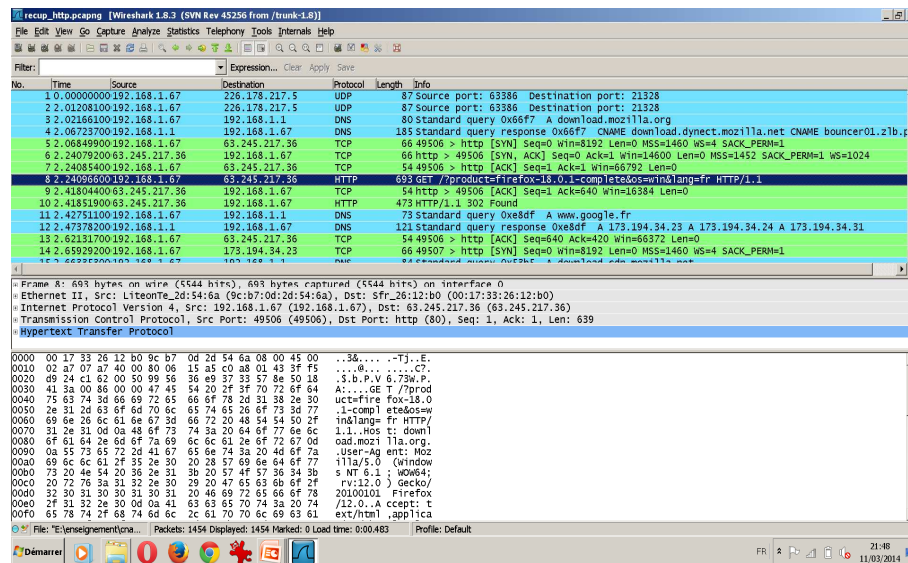
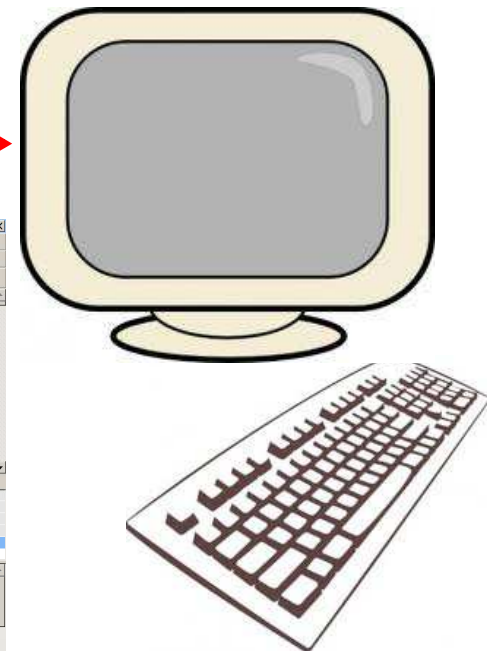
L'écoute

Internet à vu le jour dans les années 80. A cette époque la sécurité n'était pas une priorité. De nos jours, les mêmes techniques sont encore utilisées.

Ainsi, il est possible d'intercepter des informations qui circulent sur ce réseau.



Données



Le scan

Les applications communiquent via des adresses IP et des n° de ports, de plus elles sont programmées pour répondre à toutes les demandes.

The screenshot shows a network scanning application with a menu bar (Fichier, Opérations, Paramètres, Afficher, Aide) and a toolbar with icons for analysis, network, IP, and other functions. The main window displays a search range of 162.38.18.1 - 162.38.18.254 and a list of results. The selected device is MACBOOKPRO-C122.

Statut	Nom	IP	Fabricant
Actif	162.38.18.207	162.38.18.207	Apple, Inc.
Actif	162.38.18.217	162.38.18.217	Apple, Inc.
Actif	DESKTOP-O0BK56N	162.38.18.218	Intel Corpora
Actif	162.38.18.222	162.38.18.222	Apple, Inc.
Actif	162.38.18.225	162.38.18.225	
Actif	DESKTOP-IQ6VO7C	162.38.18.230	Intel Corpora
Actif	162.38.18.236	162.38.18.236	
Actif	162.38.18.238	162.38.18.238	
Actif	162.38.18.240	162.38.18.240	Hon Hai Prec
Actif	162.38.18.242	162.38.18.242	SAMSUNG E
Actif	MACBOOKPRO-C122	162.38.18.243	Apple, Inc.
Actif	162.38.18.247	162.38.18.247	
Actif	162.38.18.251	162.38.18.251	HUAWEI TEC
Actif	162.38.18.252	162.38.18.252	SAMSUNG E
Actif	162.38.18.253	162.38.18.253	Rivet Networ

MACBOOKPRO-C122	
Statut:	Actif
Système d'exploitation:	
IP:	162.38.18.243
MAC:	78:31:C5:6A:00:08
Fabricant:	Apple, Inc.
NetBIOS:	
Utilisateur:	
Type:	
Date:	
Commentaires:	

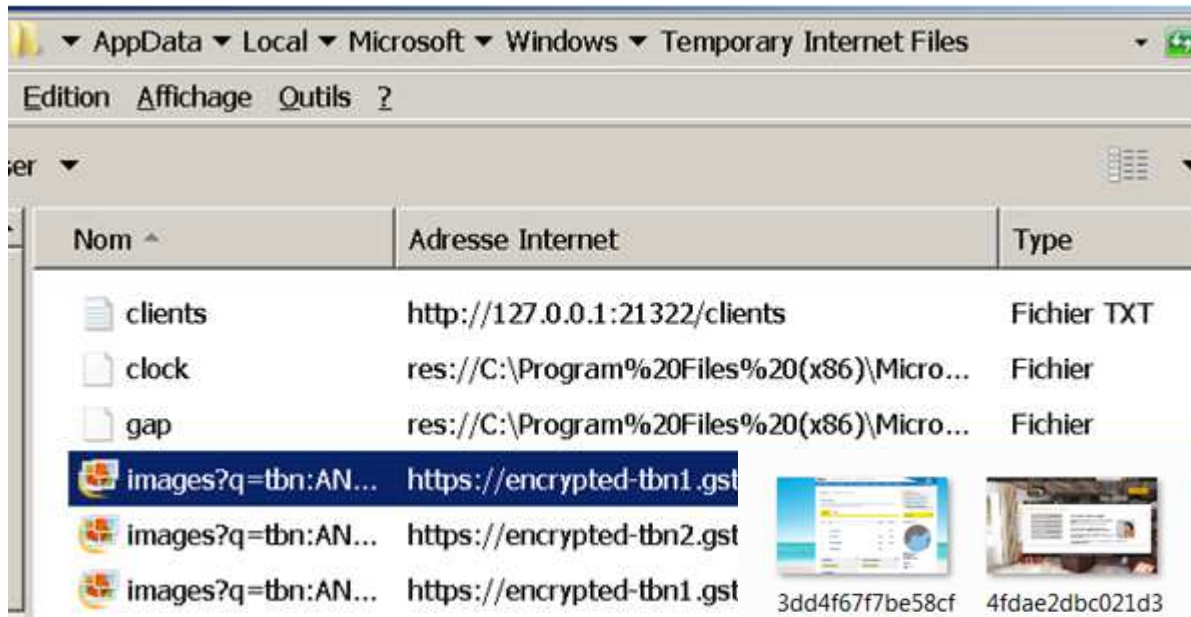
Service	
Port 88 (TCP)	Heimdal Kerberos se
Port 548 (TCP)	
Port 631 (TCP)	CUPS 2.2

Etant connecté sur un réseau, il est possible de voir qui est connecté : c'est le balayage ou scan.

Le scan permet de voir quelles applications sont actives sur les machines connectées.

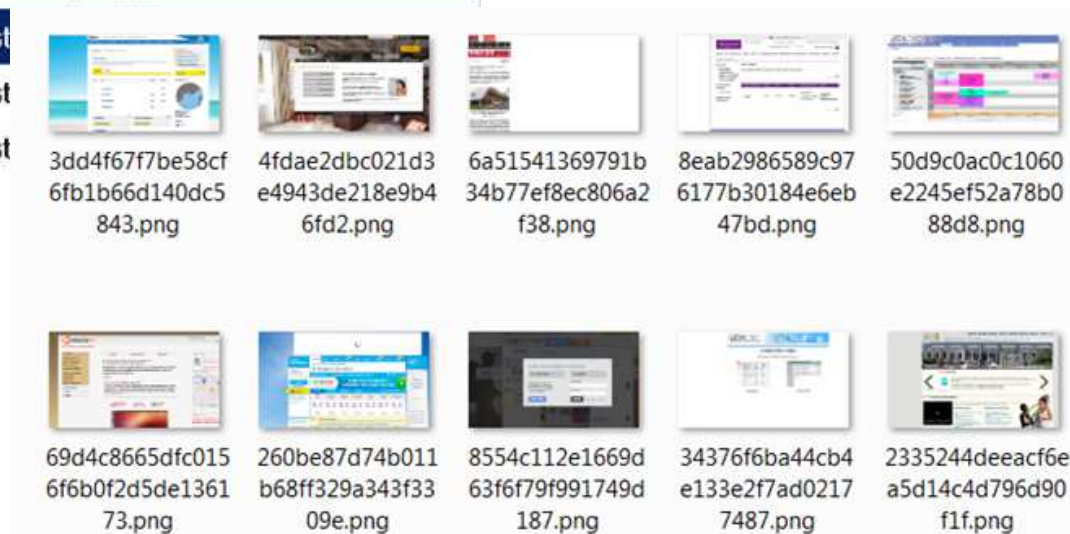
La fouille

Tous les systèmes gardent une grande quantité d'information, pour des raisons de performance : les fichiers temporaires, cookies ,



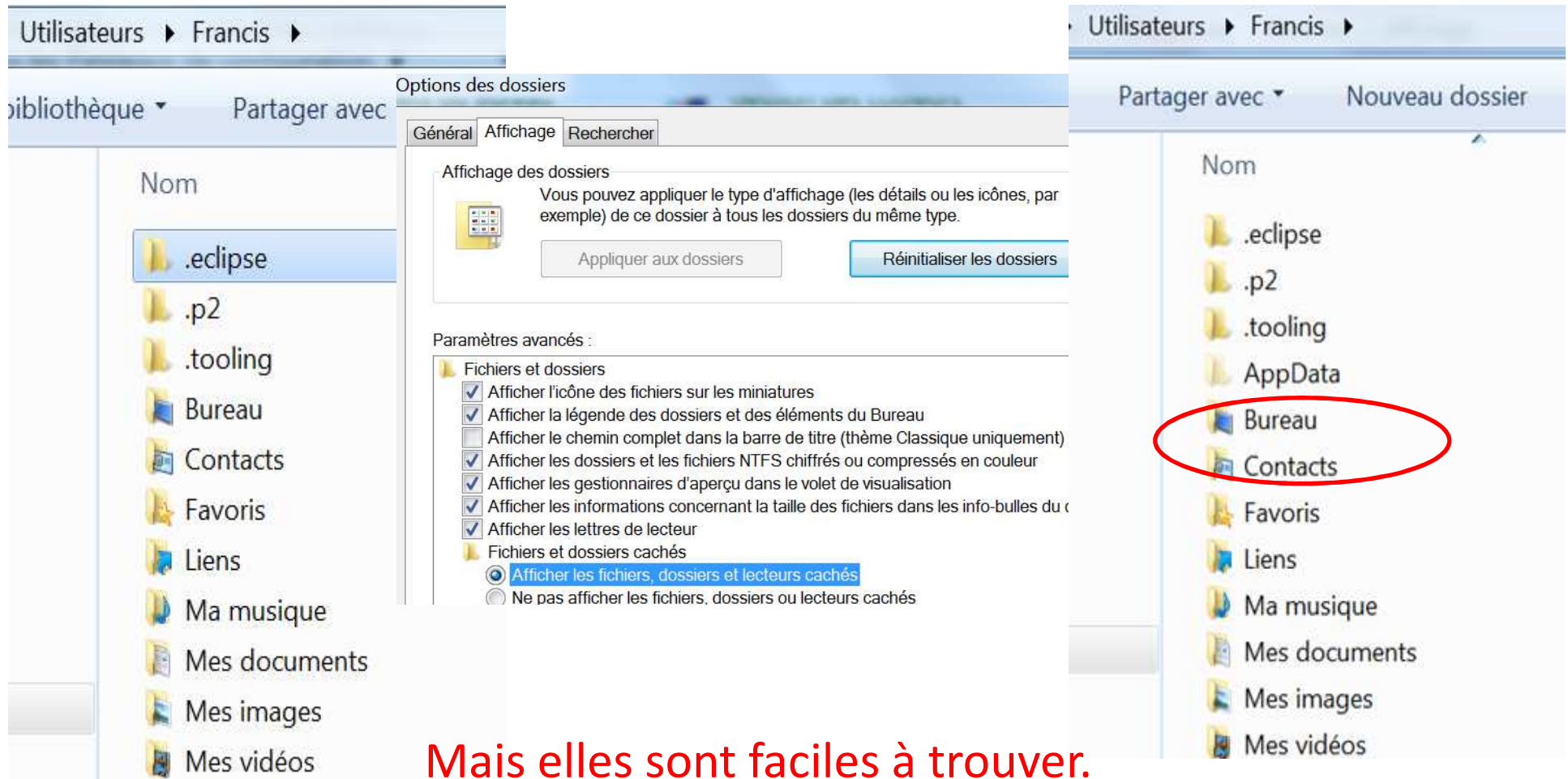
On y trouve les pages consultées sur internet ...

Mais aussi des informations plus confidentielles : login, mots de passe ...



La fouille

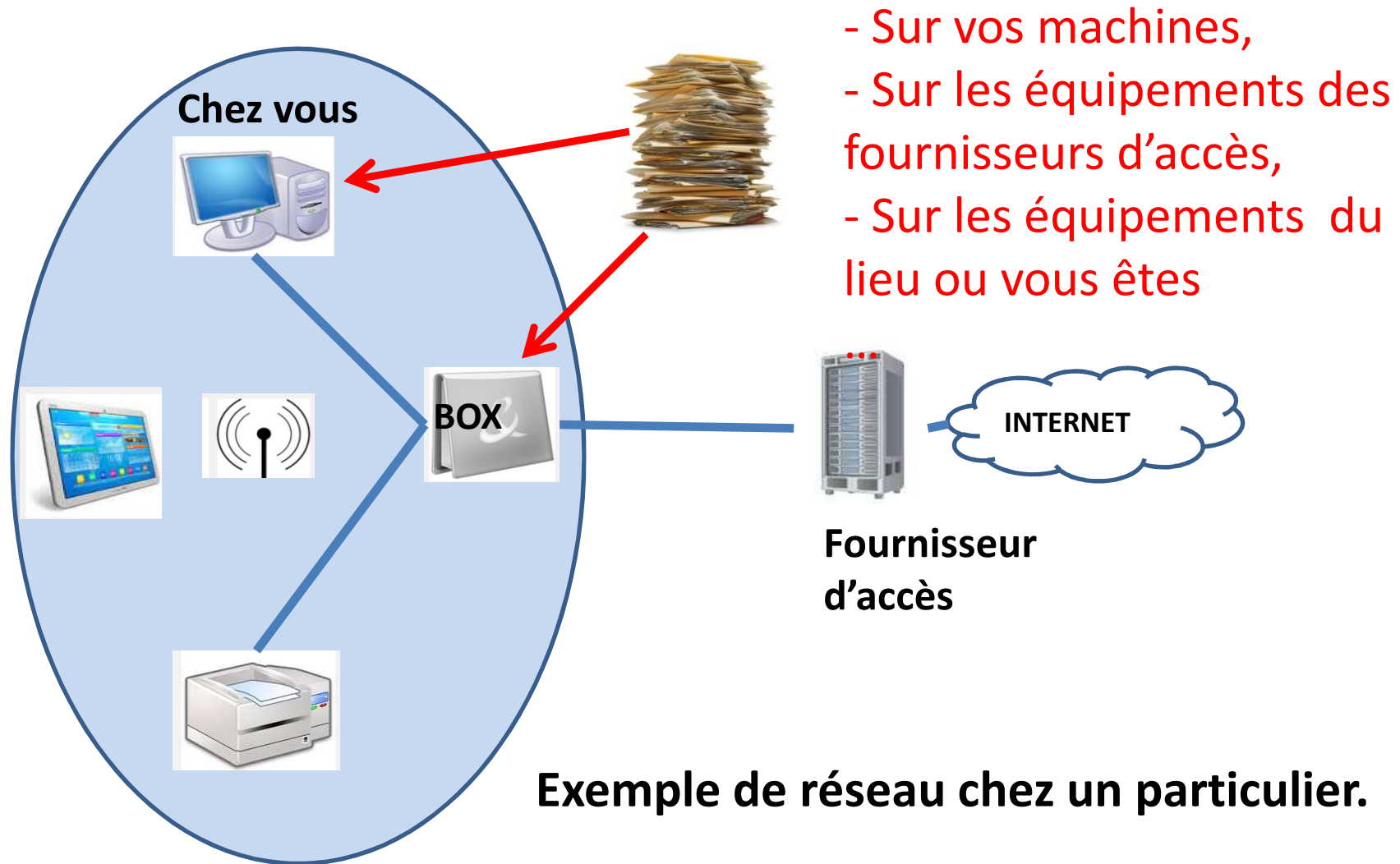
Ces données sont cachées, car non utiles aux utilisateurs.



Mais elles sont faciles à trouver.
Il suffit de demander à les voir !!

La fouille

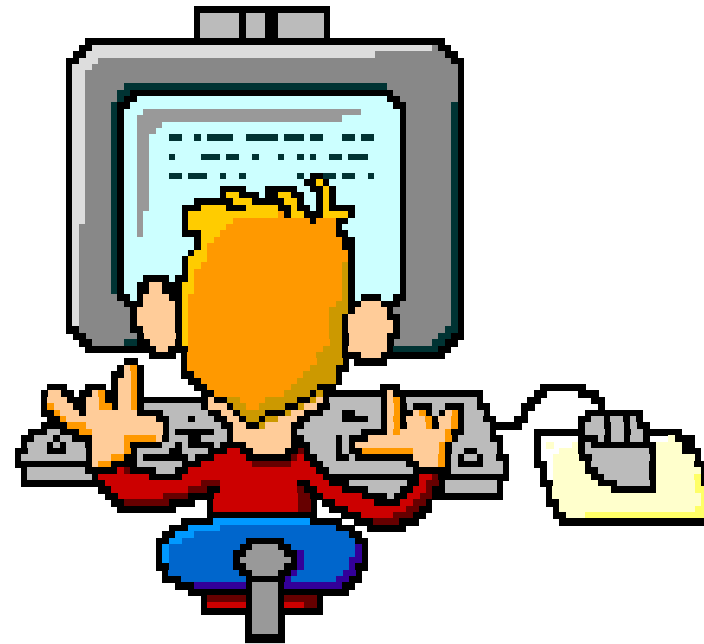
Où se trouvent ces fichiers cachés ?



Contexte actuel

La majorité des utilisateurs :

- utilisent Windows
- utilisent le Wi-Fi
- ouvrent des sessions en mode administrateur
- installent les applications par défaut
- protègent mal les accès à la machine
- n'ont aucune conscience des risques
- ...

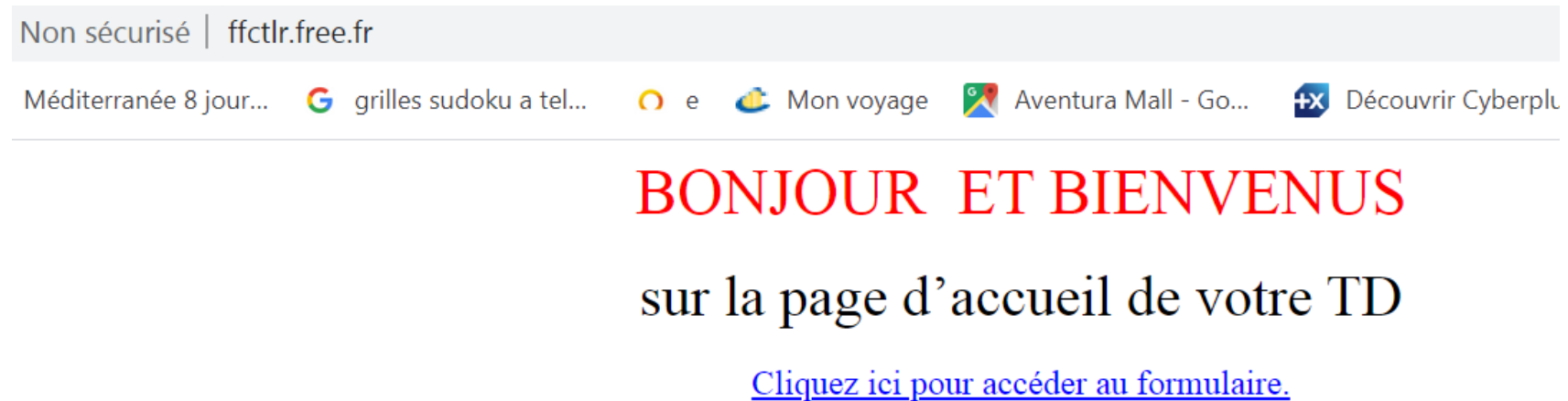


Examples

Cas d'écoute

Il est possible d'intercepter les informations qui sont échangées entre votre machine et une machine distante.

Un exemple de consultation d'une page sur un espace web de chez FREE.



Cas d'écoute

	Time	Source	Destination	Protocol	Length	Info
8	2.355165	212.27.63.105	192.168.1.36	TCP	66	80 → 52304 [SYN]
9	2.355261	192.168.1.36	212.27.63.105	TCP	54	52304 → 80 [ACK]
10	2.409549	212.27.63.105	192.168.1.36	TCP	54	80 → 52303 [ACK]
11	2.420920	212.27.63.105	192.168.1.36	HTTP	1004	HTTP/1.1 200 OK

\n

<p class=MsoNormal align=center style='text-align:center'><span\n
 style='font-size:22.0pt;mso-bidi-font-size:11.0pt;line-height:115%;color:red'>BONJOUR.
 style='mso-spacerun:yes'>\240 ET BIENVENUS<o:p></o:p></p>\n

```

0210 2d 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 2e 30 70 -font-size:11.0p
0220 74 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 31 t;line-height:11
0230 35 25 3b 63 6f 6c 6f 72 3a 72 65 64 27 3e 42 4f 5%;color:red'>BO
0240 4e 4a 4f 55 52 3c 73 70 61 6e 0a 73 74 79 6c 65 NJOUR<span style
0250 3d 27 6d 73 6f 2d 73 70 61 63 65 72 75 6e 3a 79 ='mso-spacerun:y
0260 65 73 27 3e a0 20 3c 2f 73 70 61 6e 3e 45 54 20 es'> </span>ET
0270 42 49 45 4e 56 45 4e 55 53 3c 6f 3a 70 3e 3c 2f BIENVENU S<o:p></
0280 6f 3a 70 3e 3c 2f 73 70 61 6e 3e 3c 2f 70 3e 0a o:p></span></p>
0290 0a 3c 70 20 63 6c 61 73 73 3d 4d 73 6f 4e 6f 72 <p class=MsoNor
02a0 6d 61 6c 20 61 6c 69 67 6e 3d 63 65 6e 74 65 72 mal align=center
02b0 20 73 74 79 6c 65 3d 27 74 65 78 74 2d 61 6c 69 style='text-ali
02c0 67 6e 3a 63 65 6e 74 65 72 27 3e 3c 73 70 61 6e gn:center'><span
02d0 0a 73 74 79 6c 65 3d 27 66 6f 6e 74 2d 73 69 7a style='font-siz
02e0 65 3a 32 30 2e 30 70 74 3b 6d 73 6f 2d 62 69 64 e:20.0pt;mso-bid
02f0 69 2d 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 2e 30 i-font-size:11.0
0300 70 74 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 pt;line-height:1
0310 31 35 25 27 3e 73 75 72 20 6c 61 20 70 61 67 65 15%'>sur la page
0320 0a 64 92 61 63 63 75 65 69 6c 20 64 65 20 76 6f d'accueil de vo
0330 74 72 65 20 54 44 3c 6f 3a 70 3e 3c 2f 6f 3a 70 tre TD<o:p></o:p
0340 3e 3c 2f 73 70 61 6e 3e 3c 2f 70 3e 0a 0a 3c 70 ></span> </p>
0350 20 63 6c 61 73 73 3d 4d 73 6f 4e 6f 72 6d 61 6c class=MsoNormal
0360 20 61 6c 69 67 6e 3d 63 65 6e 74 65 72 70 73 74 align=center et
  
```

**Des outils gratuits,
 que l'on trouve
 facilement,
 peuvent voir ce qui
 circule sur le net et
 que personne ne
 voit ou ne
 comprend.**

Cas d'écoute

```
7a 65 3a 31 31 2e 30 70 -font-si ze:11.0p
65 69 67 68 74 3a 31 31 t;line-h eight:11
3a 72 65 64 27 3e 42 4f 5%;color :red'>BO
61 6e 0a 73 74 79 6c 65 NJOUR<sp an·style
61 63 65 72 75 6e 3a 79 ='mso-sp acerun:y
73 70 61 6e 3e 45 54 20 es'>· </ span>ET
53 3c 6f 3a 70 3e 3c 2f BIENVENU S<o:p></
61 6e 3e 3c 2f 70 3e 0a o:p></sp an></p>·
73 3d 4d 73 6f 4e 6f 72 ·<p clas s=MsoNor
6e 3d 63 65 6e 74 65 72 mal alig n=center
74 65 78 74 2d 61 6c 69 style=' text-ali
72 27 3e 3c 73 70 61 6e gn:cente r'><span
66 6f 6e 74 2d 73 69 7a ·style=' font-siz
3b 6d 73 6f 2d 62 69 64 e:20.0pt ;mso-bid
69 7a 65 3a 31 31 2e 30 i-font-s ize:11.0
68 65 69 67 68 74 3a 31 pt;line- height:1
20 6c 61 20 70 61 67 65 15%'>sur la page
69 6c 20 64 65 20 76 6f d·accue il de vo
3a 70 3e 3c 2f 6f 3a 70 tre TD<o :p></o:p>
```

BONJOUR ET BIENVENUS

sur la page d'accueil de votre TD

[Cliquez ici pour accéder au formulaire.](#)

Mais avec un minimum de connaissances, il est possible de comprendre le contenu de cette suite de caractères ...

Cas d'écoute

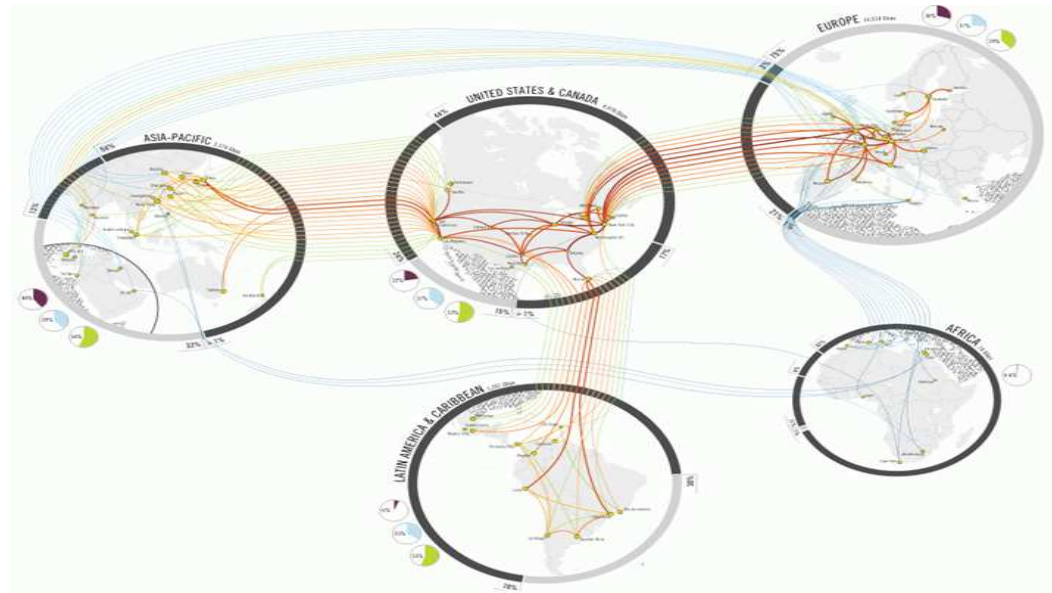
A quel endroit peut-on intercepter vos informations ?

1 – Sur votre machine

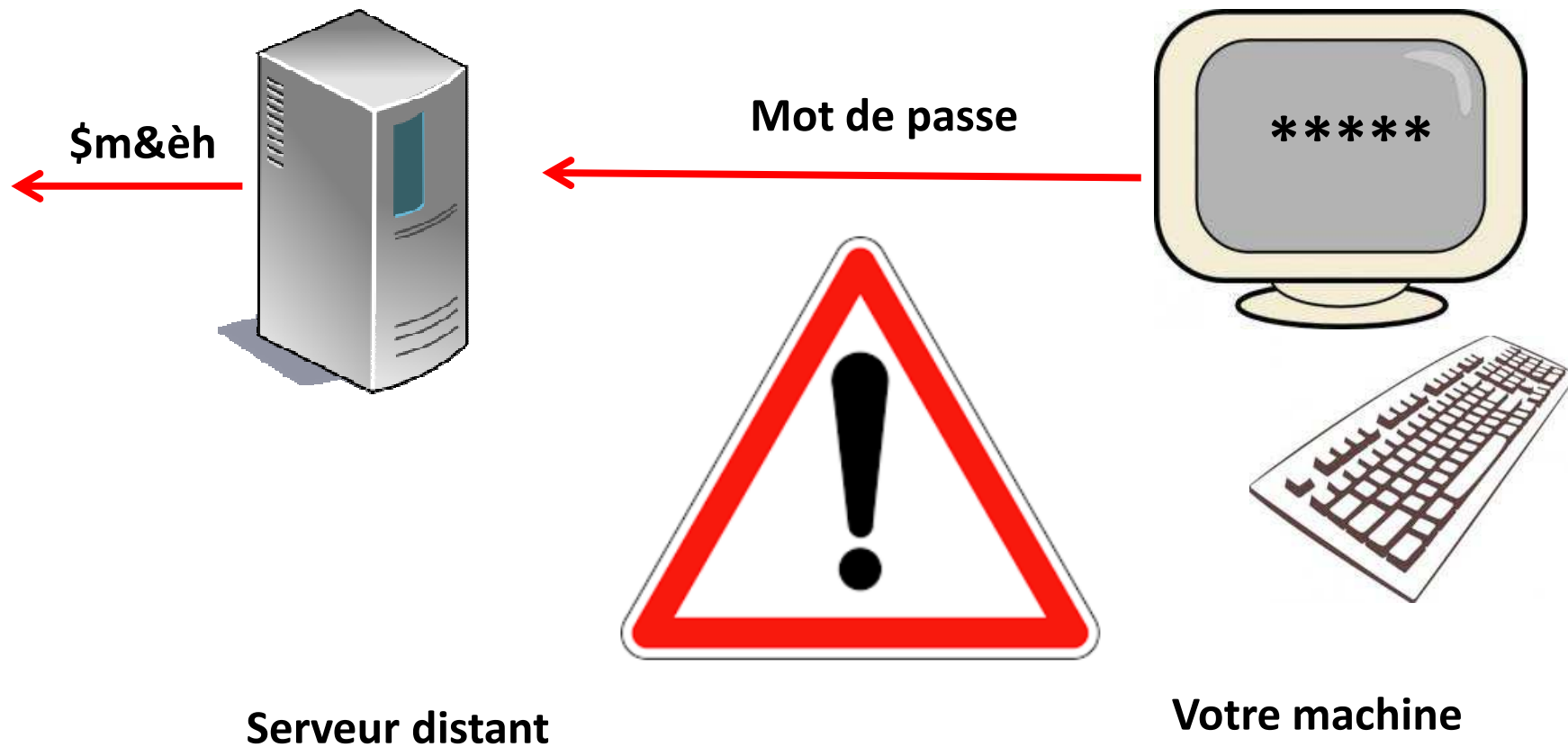
2 – Dans le réseau ou vous trouvez (IUT, McDo, ...)

Et si le serveur se trouve loin :

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



Cas d'écoute



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

Cas d'écoute

Méditerranée 8 jour... G grilles sudoku a tel... e Mon voyage Aventura Mall - Go... Décou

Portail Freebox Bas débit Webmail Mon Compte Pages

free Accueil Internet Téléphone Télévision B

Rechercher avec Google tout le wel

Pour vous connecter, veuillez saisir les informations suivantes:

Login:

Mot de passe:

Ok

Attention:

- Cette interface ne permet pas le téléchargement (download)
- Votre navigateur doit accepter les cookies pour utiliser cette interface
- **!!Cette interface est en phase de tests!!!**

Un exemple : connexion à un serveur FTP de chez **free**

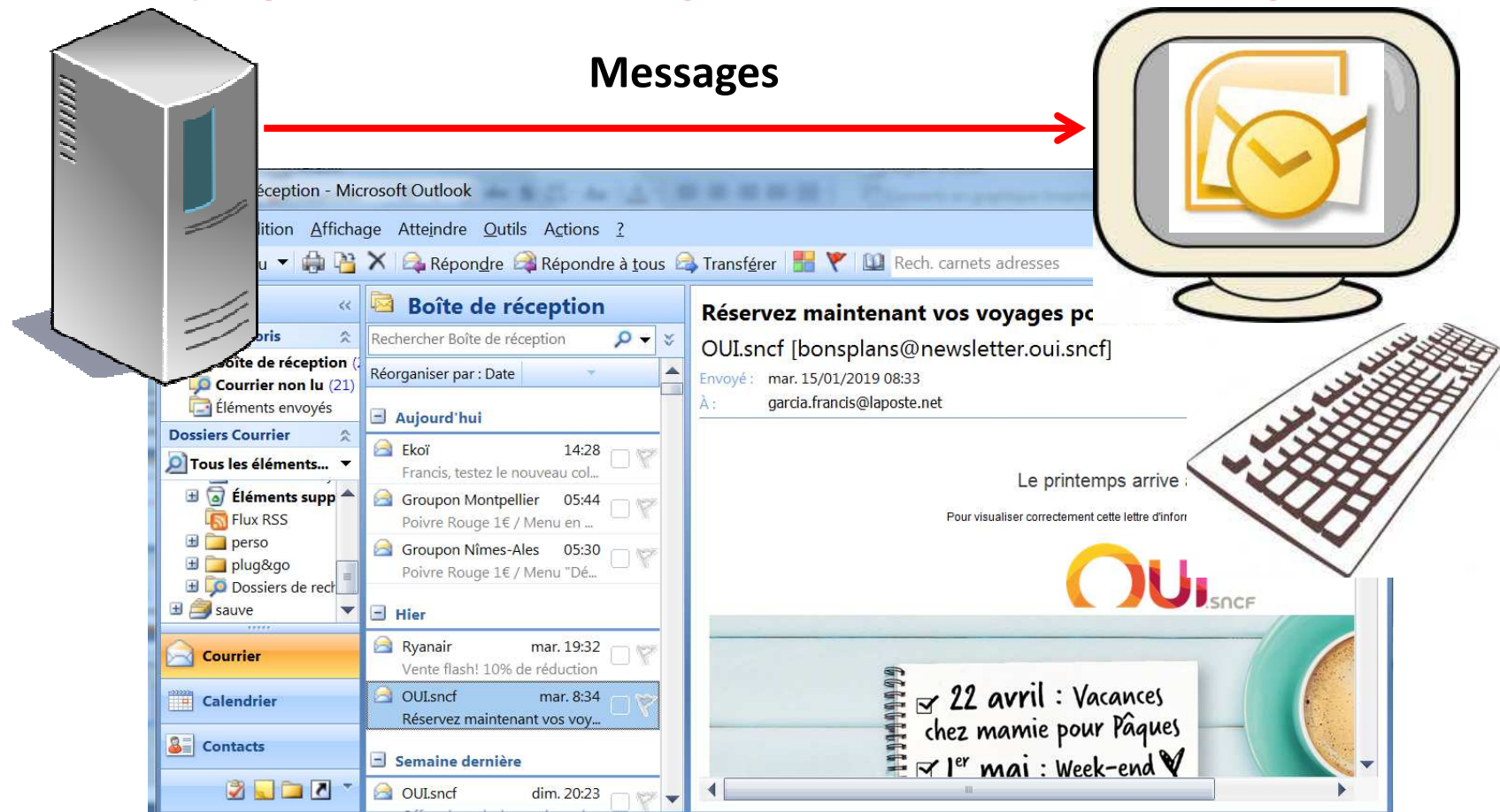
Cas d'écoute

16	2.311737	212.27.63.3	192.168.1.36	TCP	54 80 → 52077
17	2.312698	192.168.1.36	212.27.63.3	HTTP	1172 POST /index
<p>▶ Frame 17: 1172 bytes on wire (9376 bits), 1172 bytes captured (9376 bits) on interface</p> <p>▶ Ethernet II, Src: IntelCor_fc:5e:2c (e4:b3:18:fc:5e:2c), Dst: Sfr_94:0b:e8 (30:7e:cb:94)</p> <p>▶ Internet Protocol Version 4, Src: 192.168.1.36, Dst: 212.27.63.3</p> <p>▶ Transmission Control Protocol, Src Port: 52096, Dst Port: 80, Seq: 1, Ack: 1, Len: 1118</p>					
0320	74 25 32 30 70 72 6f 76	69 64 65 64 29 3b 20 5f	t%20prov ided); _		
0330	5f 75 74 6d 61 3d 31 37	32 37 36 34 36 36 30 2e	_utma=17 2764660.		
0340	31 35 32 34 34 38 39 30	34 31 2e 31 35 37 33 37	15244890 41.15737		
0350	32 34 36 39 30 2e 31 35	37 33 37 32 34 36 39 30	24690.15 73724690		
0360	2e 31 35 37 33 37 32 34	36 39 30 2e 31 3b 20 43	.1573724 690.1; C		
0370	47 49 53 45 53 53 49 44	3d 30 65 35 34 31 31 31	GISESSID =0e54111		
0380	32 31 62 30 32 36 35 33	64 39 33 64 32 39 32 32	21b02653 d93d2922		
0390	30 63 65 61 33 65 37 64	62 0d 0a 0d 0a 2d 2d 2d	0cea3e7d b.....		
03a0	2d 2d 2d 57 65 62 4b 69	74 46 6f 72 6d 42 6f 75	---WebKi tFormBou		
03b0	6e 64 61 72 79 73 55 30	4c 53 75 55 62 61 33 41	ndarysU0 LSuUba3A		
03c0	32 4e 79 79 61 0d 0a 43	6f 6e 74 65 6e 74 2d 44	2Nyya·C ontent-D		
03d0	69 73 70 6f 73 69 74 69	6f 6e 3a 20 66 6f 72 6d	ispositi on: form		
03e0	2d 64 61 74 61 3b 20 6e	61 6d 65 3d 22 6c 6f 67	-data; n ame="log		
03f0	69 6e 22 0d 0a 0d 0a 46	2e 47 41 52 43 49 41 0d	in"... F.GARCIA		
0400	0a 2d 2d 2d 2d 2d 57	65 62 4b 69 74 46 6f 72	-----W ebKitFor		
0410	6d 42 6f 75 6e 64 61 72	79 73 55 30 4c 53 75 55	mBoundar ysU0LSuU		
0420	62 61 33 41 32 4e 79 79	61 0d 0a 43 6f 6e 74 65	ba3A2Nyy a·Conte		
0430	6e 74 2d 44 69 73 70 6f	73 69 74 69 6f 6e 3a 20	nt-Dispo sition:		
0440	66 6f 72 6d 2d 64 61 74	61 3b 20 6e 61 6d 65 3d	form-dat a; name=		
0450	22 70 61 73 73 77 64 22	0d 0a 0d 0a 6d 6f 74 64	"passwd" ··· motd		
0460	65 70 61 73 73 65 0d 0a	2d 2d 2d 2d 2d 57 65	epasse · -----We		
0470	62 4b 69 74 46 6f 72 6d	42 6f 75 6e 64 61 72 79	bKitForm Boundary		
0480	73 55 30 4c 53 75 55 62	61 33 41 32 4e 79 79 61	sU0LSuUb a3A2Nyya		
0490	2d 2d 0d 0a		----		

Un exemple :
connexion à un
serveur FTP

Cas d'écoute

On peut intercepter n'importe quel type d'information :
pages web, messages, données téléchargées, ...



Exemple : interception d'une connexion à la messagerie

Cas d'écoute

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 220y0d4
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 01 74 05 04 20 70 72 05 06 74 01 02 0C quoced p r m eab
 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 J ul=.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 r 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=.










On peut observer les échanges d'informations entre votre machine et la messagerie.

Le contenu des messages.

Exemple : interception d'une connexion à la messagerie

Cas de scan (ou balayage)

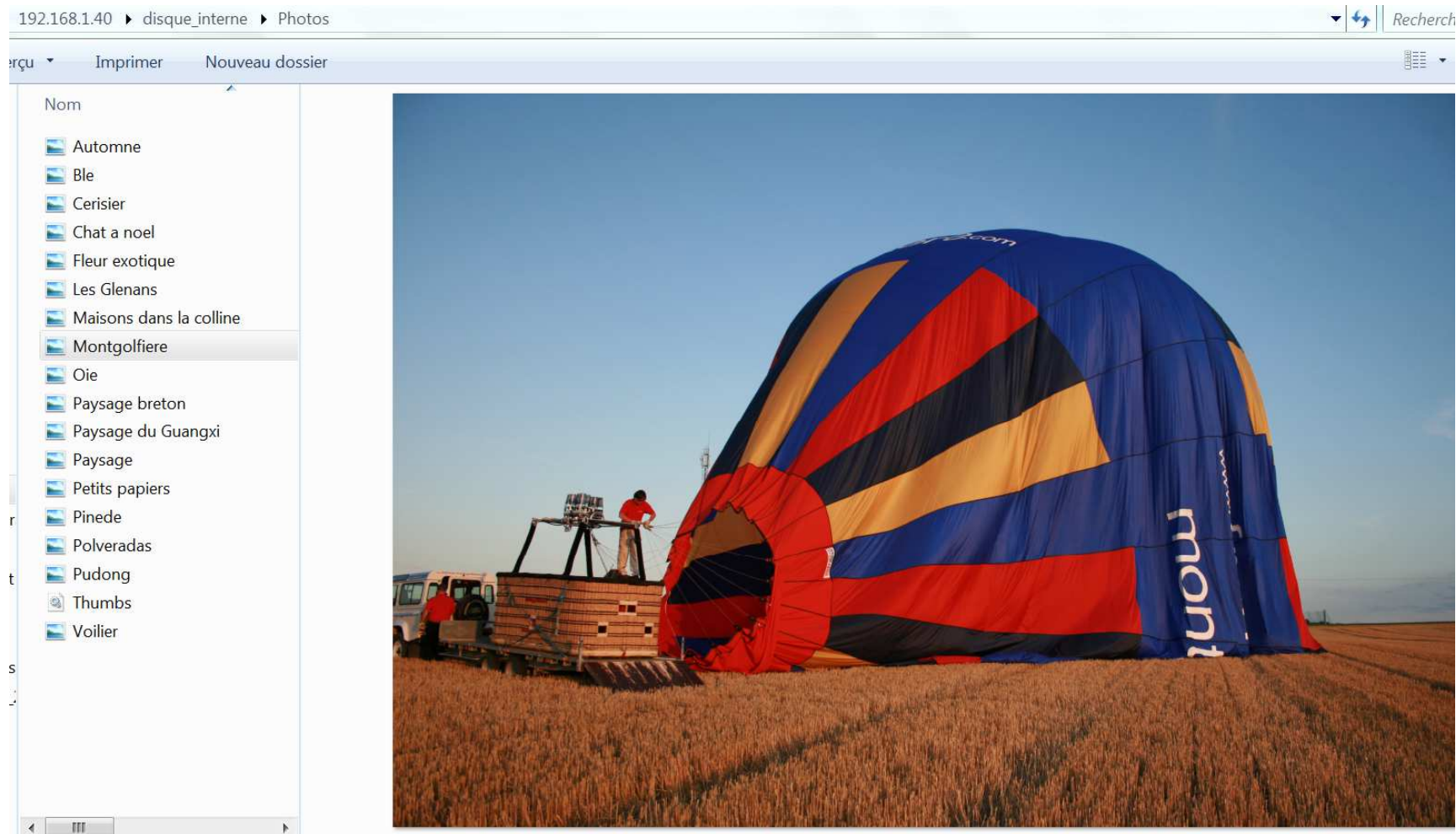
Le balayage va permettre de voir qui est connecté à un réseau

192.168.1.0-192.168.1.254		
Liste des résultats Favoris		
Statut	Nom	IP
▲ 	box  HTTP, Box - Accueil (Server)	192.168.1.1
	HUAWEI_MediaPad_T3_10	192.168.1.29
▲ 	Garcia-PC.univ-perp.fr  HTTP, Apache httpd 2.2.6	192.168.1.36
▲ 	NEUFTVSTB_MA_A018  DISQUE_INTERNE  PERIPHERIQUES  PLAYLIST	192.168.1.40

Exemple de scan sur le réseau d'un foyer ...

Cas de scan (ou balayage)

Puis quand on a repéré une machine , ici le décodeur TV,
on peut visualiser son contenu



Cas de scan (ou balayage)

On peut aussi voir s'il y a des failles dans l'application et les exploiter

Liste des résultats Favoris

Statut	Nom	IP
▶	servliste.ac-montpellier.fr	19
▶	wsus.ac-montpellier.fr	19
▶	infocentre-stat.ac-montpellier.fr	19
▶	ocean.ac-montpellier.fr	19
▶	sti.ac-montpellier.fr	19
▶	ftp.ac-montpellier.fr	19
▶	intranet-pp.ac-montpellier.fr	19
▶	duer-dev.ac-montpellier.fr	19
▶	bv.ac-montpellier.fr	19
▶	zephirlogs.ac-montpellier.fr	19
▶	intraia34.ac-montpellier.fr	19
▶	extranet.ac-montpellier.fr	19
▶	id.ac-montpellier.fr	19
▶	libre.ac-montpellier.fr	19
▶	be1d-echanges.ac-montpellier.fr	19
▶	ecare.ac-montpellier.fr	19
▶	riddo.ac-montpellier.fr	19
▶	nuxeo.ac-montpellier.fr	19
▶	gdm134.ac-montpellier.fr	19
▶	mathematiques.ac-montpellier.fr	19
▶	salle-visio-dsi.ac-montpellier.fr	19
▶	visio-cevennes.ac-montpellier.fr	19

FTP (ftp)

ftp.ac-montpellier.fr

Statut: Acti
Système d'exploitation:
IP: 195
MAC:
Fabricant:
NetBIOS:
Utilisateur:
Type:
Date:
Commentaires:

Service	Détails
FTP	ftp

Faillles ftp

Web Images Vidéos Actualités Shopping P

Environ 62 100 résultats (0,25 secondes)

SYSTEMe - Faille FTP - accueil
sysgb.fr/gd/Faille-FTP.htm

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

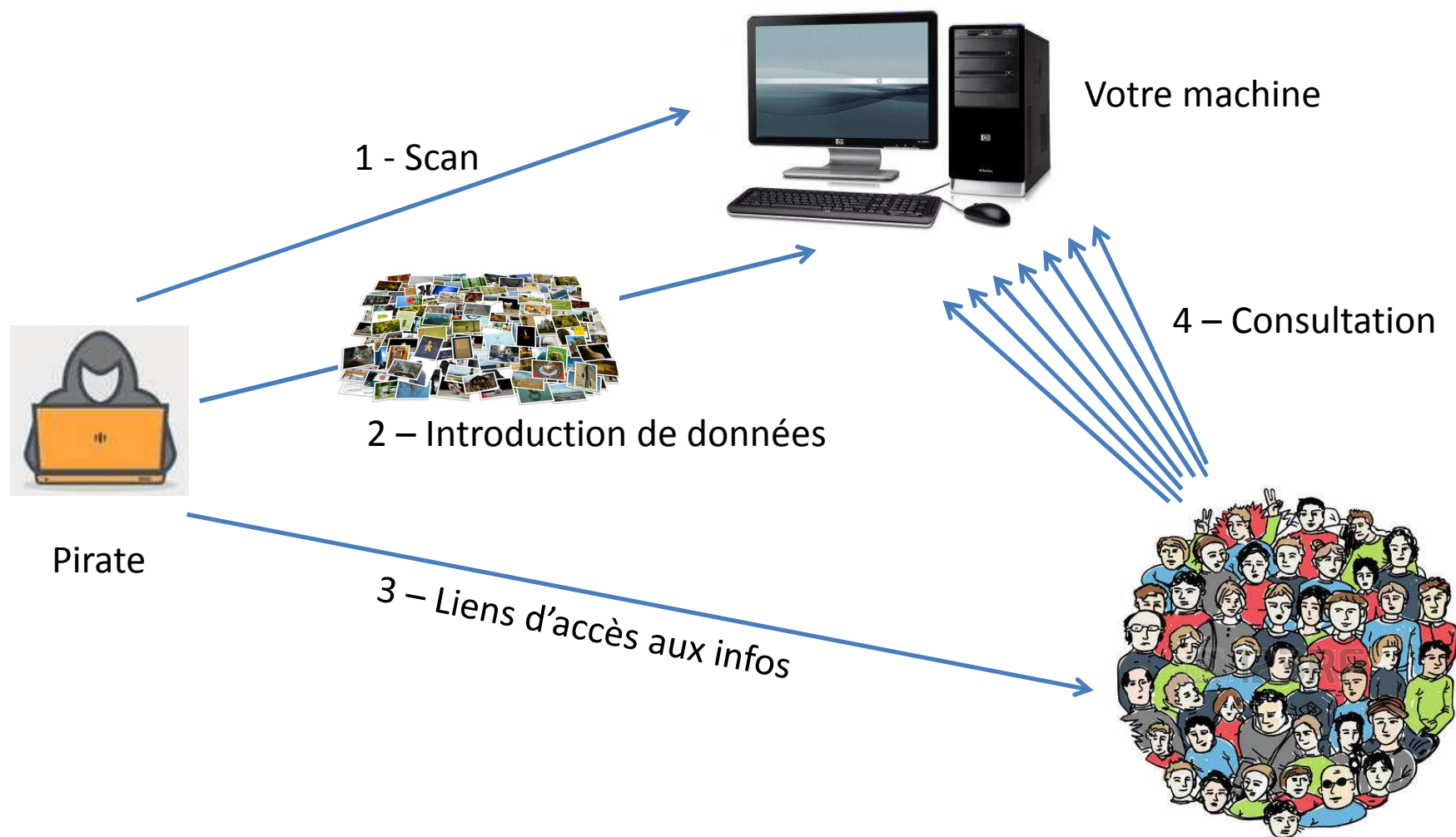
Hacker un site non protégé en entrant sur le compte ftp :

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

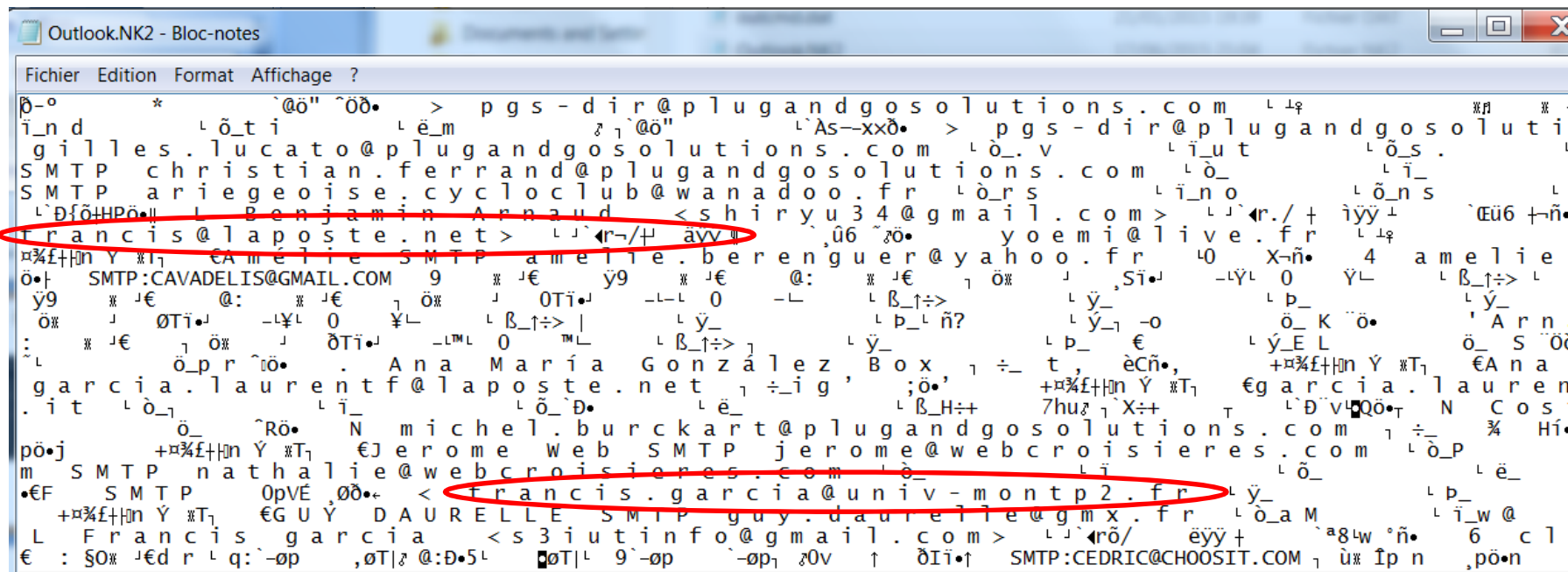
Cas de scan (ou balayage)

Exemple d'utilisation de faille FTP



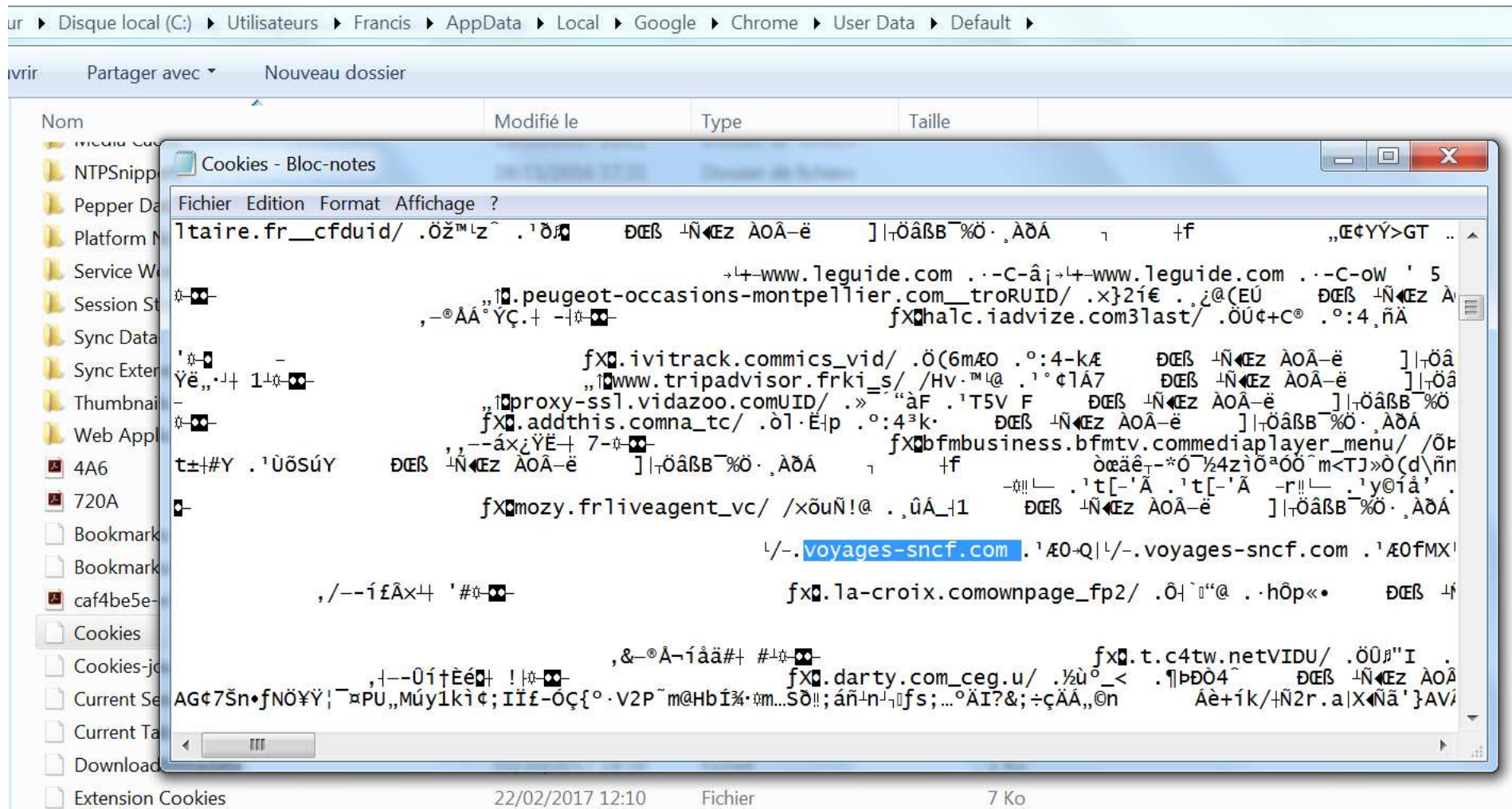
Cas de fouille

Il est tentant de vouloir accéder aux informations présentes dans les espaces cachés. **On pourra ainsi fouiller pour trouver des choses intéressantes.**



Exemple : Fichier de travail OUTLOOK

Cas de fouille



Les cookies

Cas de fouille

On peut même trouver des 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	ffctrl	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

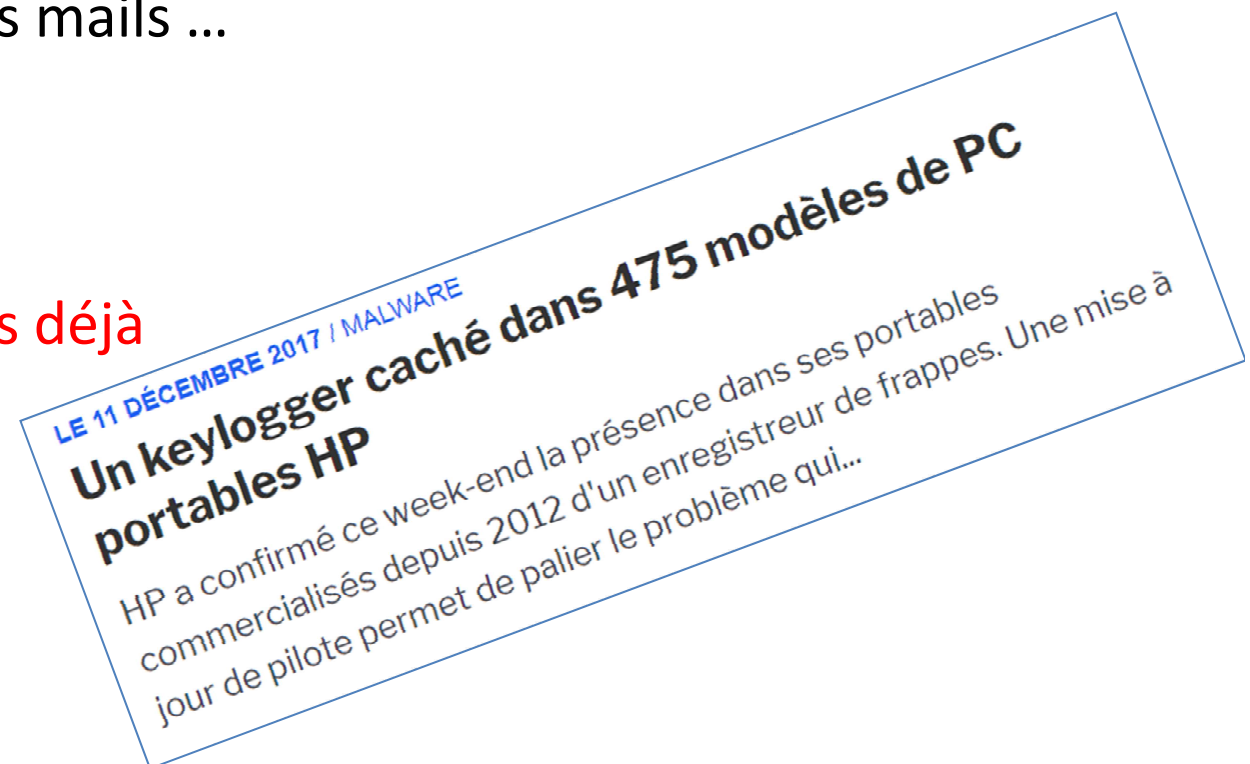
Logiciel SIW

Cas de fouille

La fouille est possible via des logiciels espions (Spyware) qui s'installent sur votre machines via :

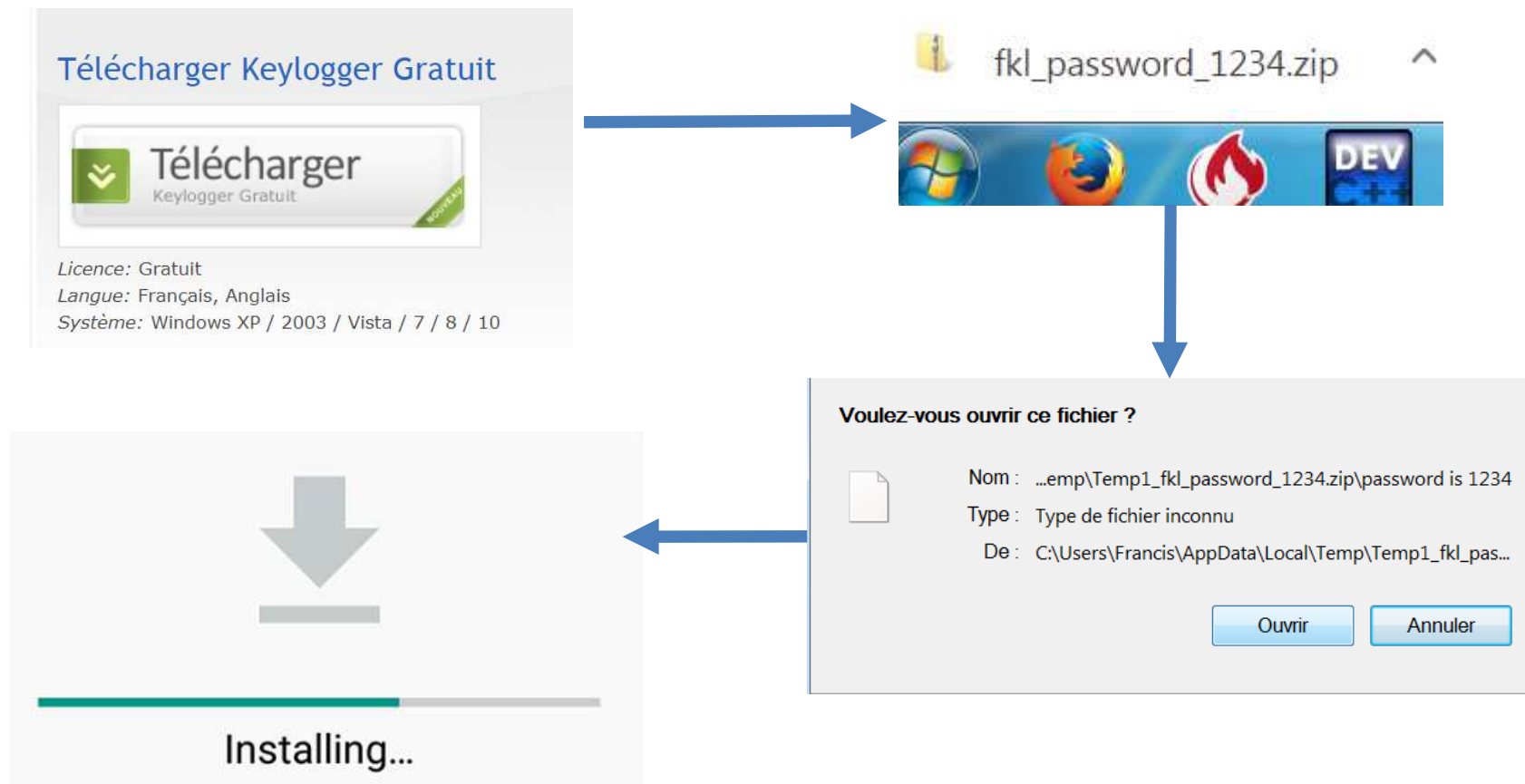
- Clé USB;
- Téléchargement d'application;
- Pièces jointes dans les mails ...

Ou par des applications déjà
présentes sur votre
machine à l'achat :
Des keyloggers.



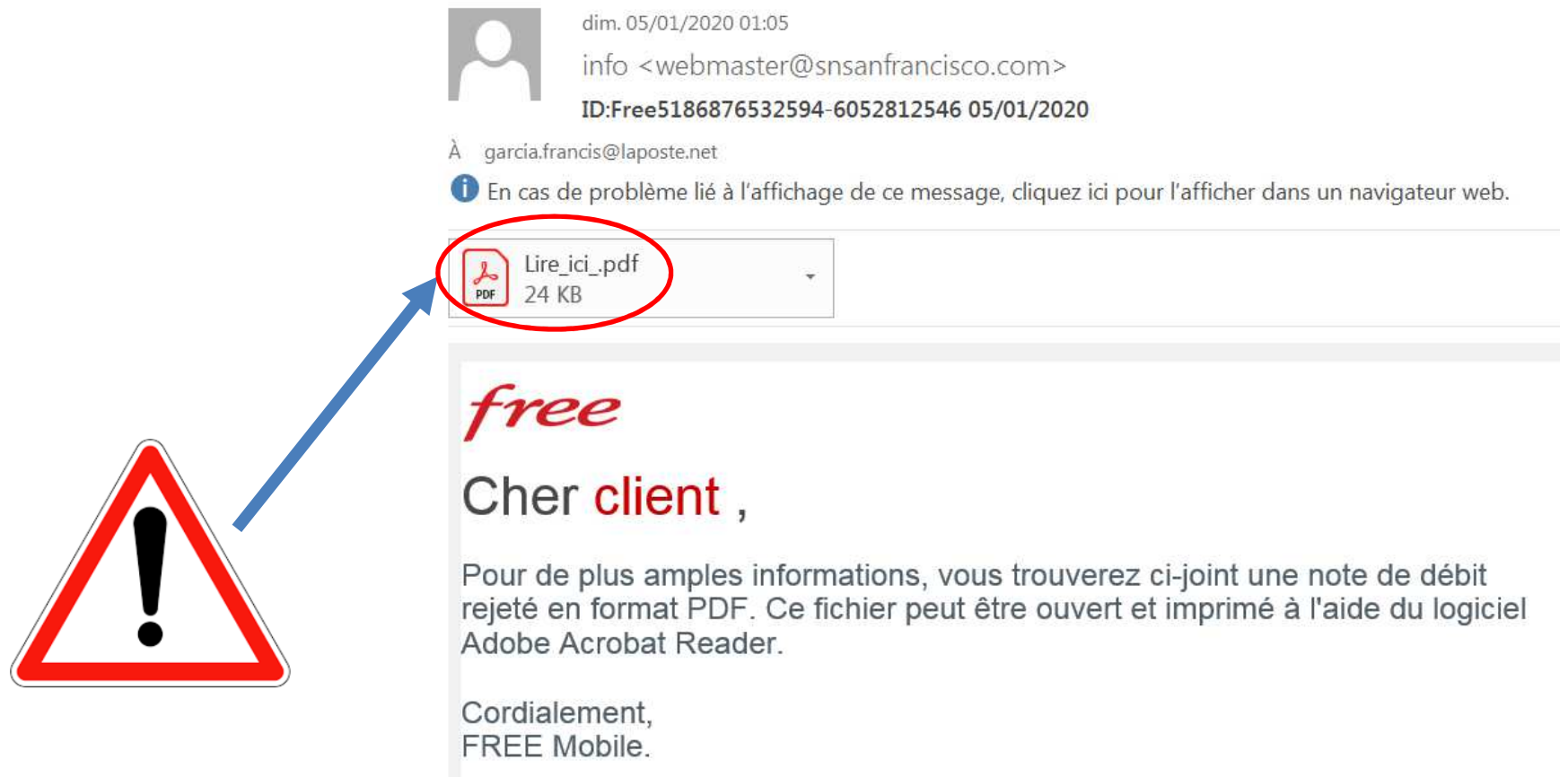
Cas de fouille

Les logiciels « espions » sont souvent contenus dans les fichiers téléchargés, mais on ne les voit pas ...



Cas de fouille

Les logiciels « espions » sont aussi contenus dans les pièces jointes des mails ...



Autres cas, le phishing

Objectif

Gagner la confiance d'utilisateurs légitimes pour en abuser, ou faire en sorte qu'ils révèlent les secrets de leur système (Codes d'accès, numéros de compte, ...)

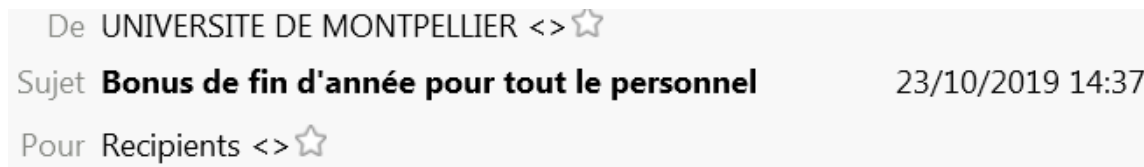


Méthode

Diriger la victime vers des faux sites (qui ressemblent à des vrais).

Autres cas, le phishing

La technique consiste à envoyer des mails à des millions d'adresses récupérées (ou achetées) ou à des adresses ciblées.

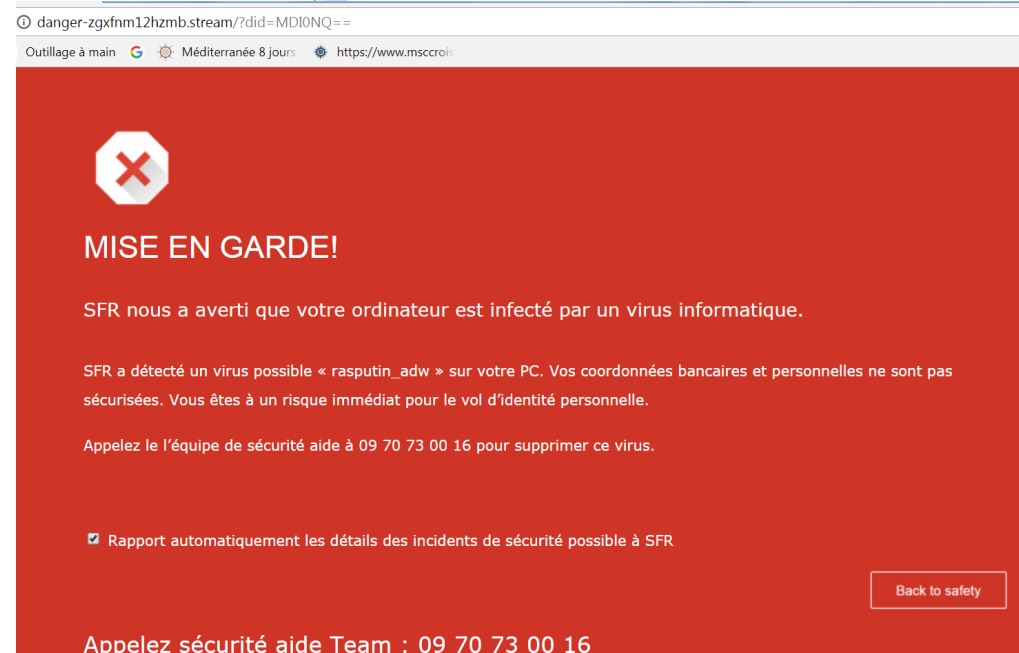


Nous avons le plaisir de vous informer que l'Université distribuera des primes de fin d'année à tout le personnel académique et non académique.

[voir les primes](#)

Cordialement
UNIVERSITÉ DE MONTPELLIER


Dans la masse il a toujours
quelqu'un qui va cliquer
sur le lien...



Cas d'école

Cas d'école

Sujet: [Piratage](#)


Suivre via: 

Cybervandallisme, 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 @zdnnetfr

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...).

2020 – Meow : le virus qui supprime les données avec une touche d'humour

La dernière cyberattaque marquante en date est survenue en juillet 2020. Il s'agit de Meow, un logiciel qui s'attaque aux serveurs mal sécurisés. Elle n'aurait pas d'autre mission que de nuire aux entreprises. Au total, des milliers de bases de données ont été touchées, avec comme victime majoritaire la société UFO qui édite un VPN (virtual private network).

12/12/2020

2017 – WannaCry et NotPetya : les logiciels malveillants qui ont fait trembler Internet

Mai 2017. Le logiciel de rançon (ou rançongiciel) WannaCry frappe le monde, et touche près de 300 000 ordinateurs dans plus de 150 pays. Cette attaque est considérée comme la plus grosse cyberattaque avec rançon de l'histoire d'Internet. En France, on peut citer des entreprises comme Auchan ou SNCF qui ont subi les conséquences de NotPetya.

AWS victime de la plus grande attaque DDoS de l'histoire

Une attaque avec un volume de 2,3 téraoctets par seconde

Par Benjamin Terrasson - @BenTerrasson
Publié le 19 juin 2020 à 12h07



AWS Shield est l'entreprise chargée d'atténuer les attaques subies par les services de cloud d'Amazon, AWS. Selon [son rapport du premier trimestre 2020](#) Amazon aurait été victime de la plus grande attaque DDoS jamais enregistrée la semaine du 17 février.

Sécurité informatique

48

Cas d'école

ACCUEIL / TECHNOLOGIES

Une cyberattaque tous les trois jours dans les hôpitaux : "Il est temps pour les Etats d'agir"

🕒 07h52, le 26 mai 2020, modifié à 09h20, le 26 mai 2020

AA

CYBERATTQUES DANS LE MONDE
JURIDIQUE : LE CAS DES ATTAQUES PAR
« EMOTET ».

SÉCURITÉ INFORMATIQUE

Rançongiciels : la liste des collectivités victimes s'allongent, comme une litanie

Publié le 08/10/2020 • Par [Alexandre Léchenet](#) • dans : [France](#)



Des données dérobées à la ville de Mitry-Mory ont été publiées en ligne mardi 6 octobre. Les annonces de collectivités touchées par les rançongiciels se multiplient, les pirates informatiques ayant su tirer profit de la crise sanitaire.

Plusieurs entreprises françaises visées par une cyberattaque de type « fraude au président »

12/12/2020

Publié le 6 octobre 2020 à 14h01

« La digitalisation de la profession d'avocat ne retire rien à la prépondérance de l'aspect humain du métier, bien au contraire. Dans le contexte numérique, valorisons davantage ce facteur humain, en sensibilisant l'avocat aux règles d'hygiène numérique, nécessaires à la protection de ses principes essentiels.

Cyberattaque : « Il y a une explosion de la grande criminalité », rapporte le directeur de l'Anssi

Auditionné au Sénat, le directeur général de l'agence nationale de la sécurité des systèmes d'information rend compte de la multiplication des attaques ciblées. Des inquiétudes ont aussi été formulées sur les conséquences du télétravail susceptible d'ouvrir de brèches dans les systèmes d'information.

LE 04 NOV 2020

Par [Hélène Berkaoui](#)

🕒 5mn

En 2020, le niveau de sécurité des mots de passe est toujours aussi alarmant

Sécurité informatique

Publié le 23 novembre 2020 à 15h13

49

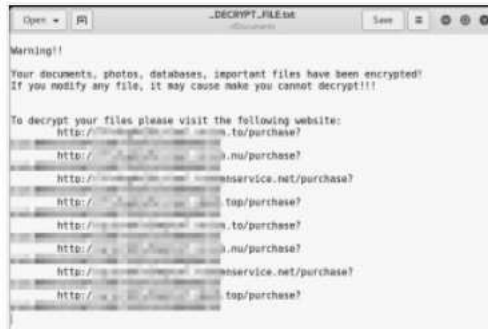
Cas d'école



LE 02 NOVEMBRE 2018 / MALWARE

L'Iran frappé par un malware plus violent que Stuxnet

Une variante du ver Stuxnet plus sophistiquée et dangereuse a ciblé l'infrastructure réseau de l'Iran. L'agence de la défense civile de ce pays ne s'est pas étendue sur...



LE 19 JUIN 2018 / MALWARE

Les systèmes Linux aussi terrorisés par les malwares

Les bots, backdoors, trojans et autres applications malveillantes qui attaquent le système d'exploitation Linux sont rares. Mais lorsqu'ils apparaissent, mieux vaut ne pas les...

TSMC contraint de fermer des usines à cause d'un virus

Sécurité : Le fabricant de semi-conducteurs, qui travaille notamment pour Nvidia, a été obligé de stopper plusieurs usines dont les outils de production ont été infectés par un virus informatique.

Un ver mystérieux cible les machines à rayons X et les scanners IRM

Technologie : Le groupe de hacker Orangeworm choisit soigneusement les victimes de ses attaques très ciblées.

Les risques (un résumé)

Les risques

En résumé, les principaux risques viennent de :

→ SYSTÈME (Installations par défaut, mauvaises configurations, erreurs de programmation, manque de protections,...)

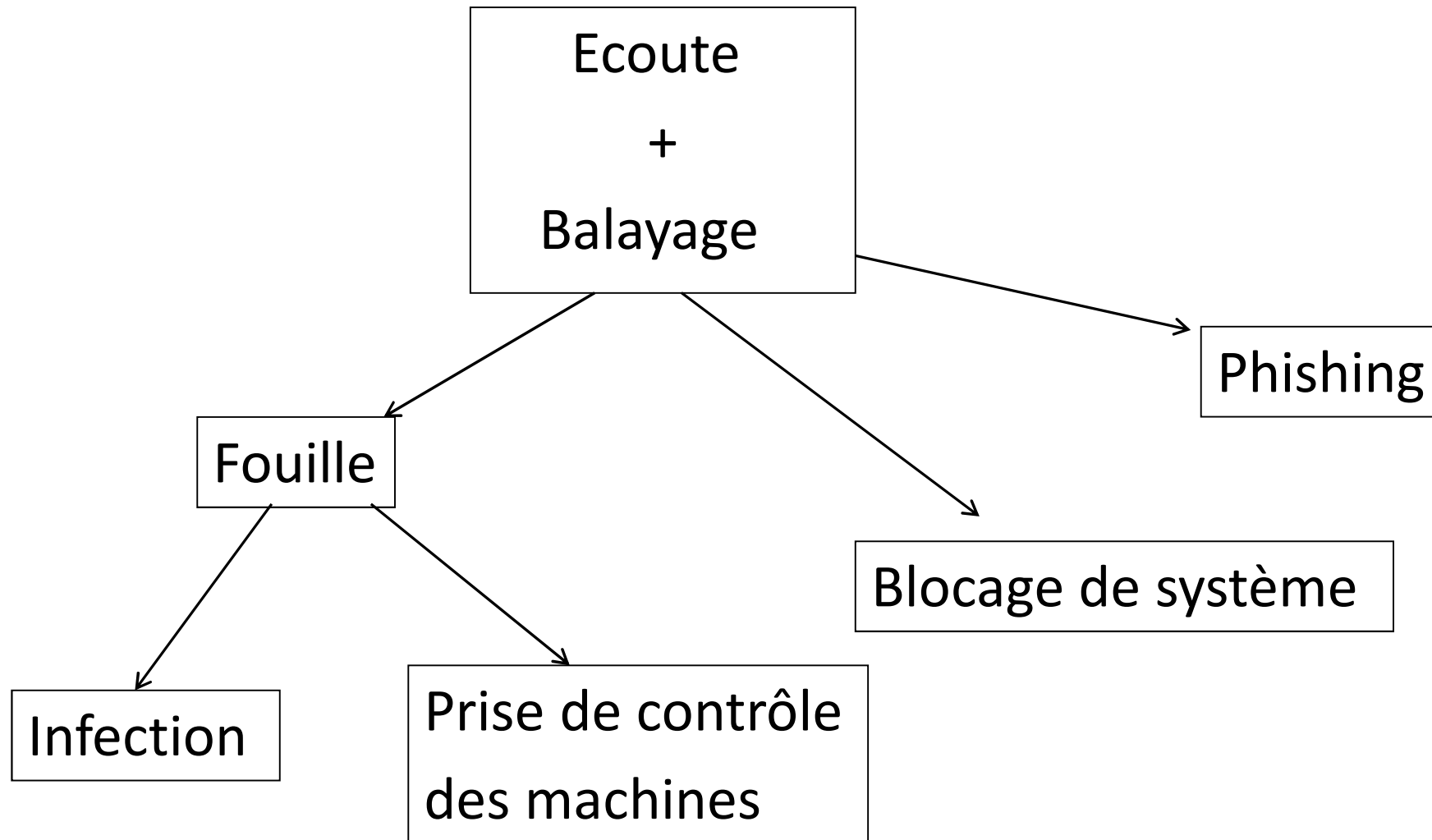
→ RESEAU (Manque de fiabilité, virus, complexité, ...)

Mais aussi :

→ HUMAIN (Absence de consignes, manque de formation, négligence , erreur de manip, ...)

→ ORGANISATION (Manque de protections, pannes diverses, ...)

Les menaces ou scénarios d'attaques



La protection

La défense

Principales technologies de défense

- 1 – Protection physique des équipements
- 2 – Protection contre les intrusions (Firewalls , anti-virus, Anti – spyware, Anti Spam, Suppression des fichiers de travail)
- 3 – Sauvegarde des données
- 4 – Cryptage des données
- ...
- 5 - Bonnes pratiques ...

Protection contre les intrusions

Le pare-feu

Objectif : filtrer les trames entre le réseau externe et le réseau interne.

Un firewall intervient au niveau des couches 3 et 4 de l'OSI en filtrant les données des paquets IP et/ou TCP :

- types de paquets (TCP, UDP, ...)
- adresse IP d'origine
- adresse IP de destination
- le port de destination (TCP, UDP, ...)
- . . .

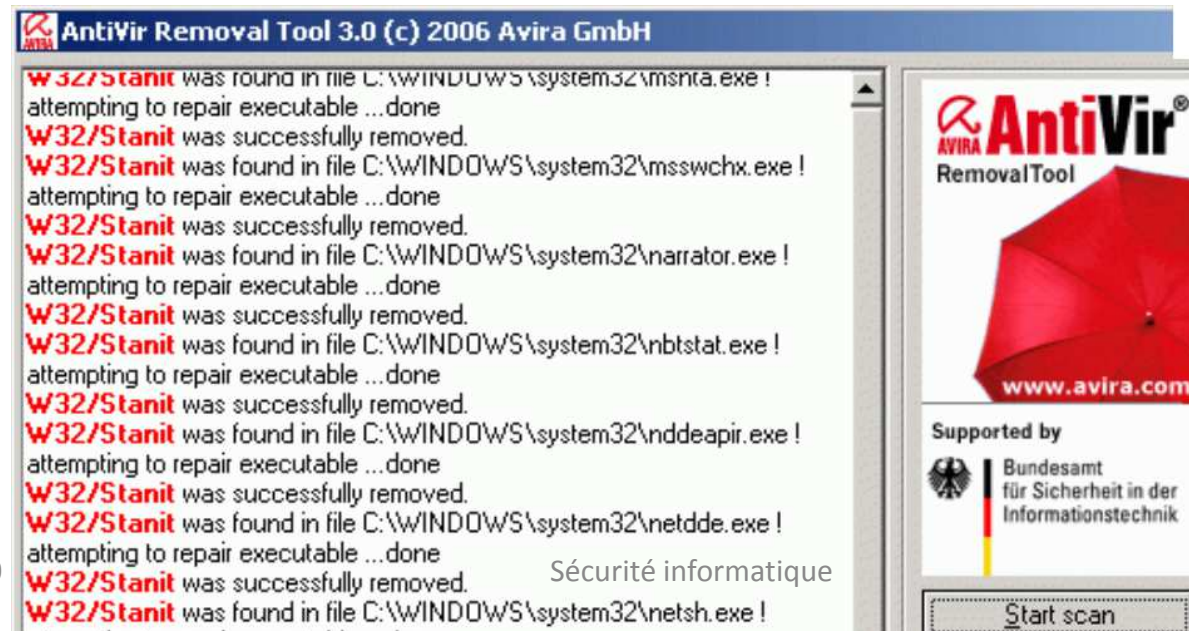
Protection contre les intrusions

Anti-Virus

Objectif : détecter et mettre hors d'état de nuire les virus

Il existe trois grandes techniques de détection :

- La signature ;
- L'analyse heuristique .



12/12/2020

Sécurité informatique

Protection contre les intrusions

Suppression des fichiers de travail

La suppression des fichiers de travail (ou cache) va permettre de faire disparaître presque toutes les traces d'activité du système :

- Noms des sites visités
- Pages consultées
- Derniers fichiers utilisés
- Login
- Mots de passe
- ...

Sauvegarde des données

Suite à une attaque, un crash système, une défaillance matérielle, seule une sauvegarde permet de restaurer entièrement le système dans son état originel

Encore faut-il qu'elles soient bien faites !

Faire de bonnes sauvegardes consiste à :

- Bien paramétrer son outil,
- L'utiliser de manière correcte,
- Protéger ses sauvegardes.

→ Il est nécessaire de s'imposer quelques règles élémentaires

Sauvegarde des données – Quelques règles

1 – Ne pas tout sauvegarder à chaque fois : Tout n'est pas important à sauvegarder à chaque instant, comme par exemple le système et les applications.

2 – Ne pas oublier de données dans la sauvegarde : Par exemple la messagerie

3 - Faire des sauvegardes régulières : Il faut faire des sauvegardes quotidiennes des données de travail ou du moins à chaque fois que des modifications ont été faites.

4 – Protéger les sauvegardes : Les sauvegardes qui sont conservées à proximité de la machine représentent un risque en cas de vol, d'incendie, inondations, ...

Cryptage des données

Objectif : rendre les données incompréhensibles

Le chiffrement (ou cryptage) s'appuie sur des clés spécifiques que l'on utilise pour le cryptage et pour le décryptage.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed non risus. Suspendisse lectus tortor, dignissim sit amet, adipiscing nec, ultricies sed, dolor. Cras elementum ultrices diam. Maecenas ligula massa, varius a, semper congue, euismod non, mi. Proin porttitor, orci nec nonummy molestie, enim est eleifend mi, non fermentum diam nisl sit amet erat. Duis semper. Duis arcu massa, scelerisque vitae, consequat in, pretium a, enim. Pellentesque congue. Ut in risus volutpat libero pharetra tempor. Cras vestibulum bibendum augue. Praesent egestas leo in pede. Praesent blandit odio eu enim. Pellentesque sed dui ut augue blandit sodales. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae.

KM0tPNalqTIJir00inLyG16g7y44RXYd8hQWRAUMjzn9i3Knj7DLAYDITsfd2JLoR3
Q1U304BFQQvu6gKVk9UmMlX3BEkVrs7mY7drxWjUS9pQvKrs92qcXrZrklhyZ0tY
cMgHWwXL18Cfn2PdZxJlZKAQqKBfemFluOEZ9B22qbZ1URqK2PAghvUHRrjNclHD1y
PTXalbm6p5qCzEeReGZt4rgkH6s3VBJS9ET2YpAuEBKfDbOjeguyptCz34gHxbkiBo
x43yJyV2LfxruKu7bDBjQ8NGUd1TQmfVzJZP7I4SzsGZXR5iXdLFI77WZ2s7HCXZg4
YcdecJBCBJSn69CJPftZ7X1U5oqtOafReixTbjXVYyoH3riS9G8zrW5ktROrLVfVz5
Rso95rAHerlnYvBH67gAAwyHiINwBoCBERNV9sFnipOma9DI0jgFJhwIqtjZ3D2CxM
j9ejLMXEp7KHODrsjvAiccnfwwEhjKDBMwyGd4fc01G7JRFwRJ0ooftrQye4KUblp3
j0NMQesAzaZjMxJ7Qmis16tlWe9AbVhF3JPegdD6zFWkwyC9ZDodeNtRsJpUzIrZb
kFdy9dKNGkuduPeQmSvq567NYSdx3MDidGzDMkMKnSYJkZuTENDXIUZouvDjNBBmx9
XnuMC7pB59LuLwlqm9AmV9KEqImWB27E571bzx80NcLnenF1UyCeWzOdhteZzKoTJo

En résumé

Une sécurité à 100% n'existe pas !!!

Malgré toutes les solutions, la meilleure protection est
un comportement averti

Il est nécessaire de sensibiliser/former les utilisateurs
aux bonnes pratiques.

Une protection efficace

Les bonnes pratiques

- ✓ Refuser la mémorisation des mots de passe,
- ✓ Changer de mot de passe régulièrement,
- ✓ Protéger l'ordinateur des virus,
- ✓ Vérifier la source des emails,
- ✓ Ne pas ouvrir les messages indésirables et non sollicités,
- ✓ Ne pas surfer sur des sites sensibles,
- ✓ S'assurer que le site sur lequel utilisé est fiable et sécurisé (l'adresse Internet commence par https au lieu de http)

Et dans le doute ... s'abstenir.

Merci de votre attention

Prenez bien soin de vous
et de vos machines.