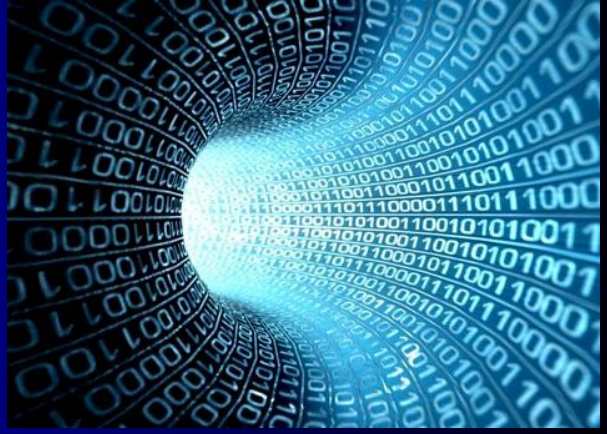
Région de Gendarmerie de Midi-Pyrénées

Internet et sécurité

Mars 2015

http://chrisharrison.net/projects/InternetMap/medium/worlddotblack.jpg

quelques citations pour débuter



« *A quoi sert Internet ? A part aller sur internet ?* » (Jacob Berger, 1999)

« *Le problème avec les citations sur internet, c'est qu'il est très difficile de savoir si elles sont authentiques* » (Napoléon Bonaparte)

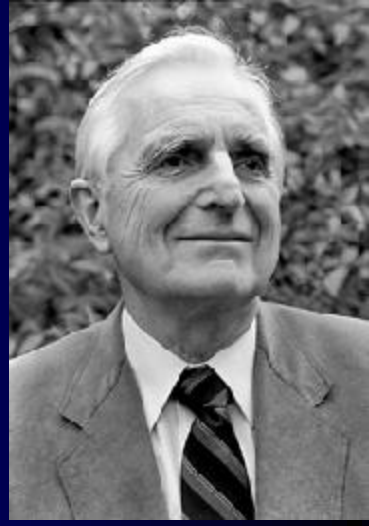
internet ?

Pour vous, qu’est-ce internet ?

- Le web ?
- Les réseaux sociaux ?
- Une bibliothèque mondiale ?
- Autre chose ?

http://www.dougengelbart.org/firsts/internet.html

internet ?

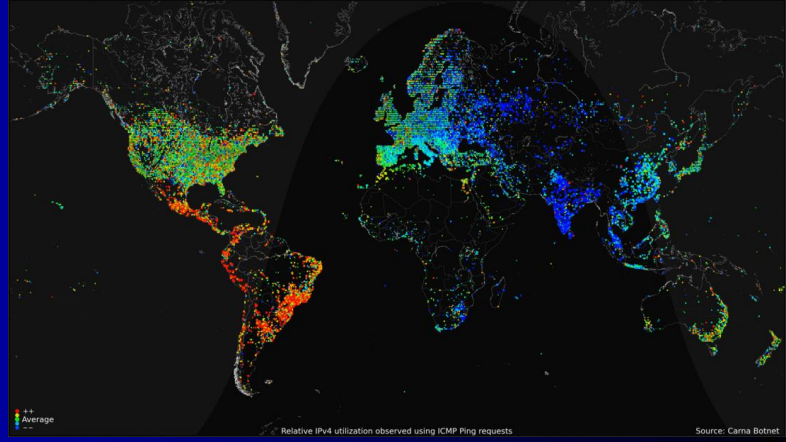


Un des pionniers : Douglas Engelbart (1925-2013)

- A l'intuition d'internet[1] dès les années 50 (son laboratoire (SRI) participe à la première liaison en 1969 avec l'UCLA)
- Démontre la première vidéoconférence (1968) « The Mother of All demos » [2]
- Invente la souris (1968)

[1]Augmented Human intellect:
http://www.dougengelbart.org/pubs/augment-3906.html
[2]The Mother of All demos,
http://www.dougengelbart.org/firsts/dougs-1968-demo.html

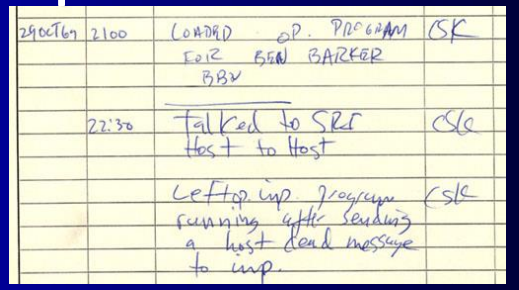
internet ?



http://motherboard.vice.com/blog/this-is-most-detailed-picture-internet-ever

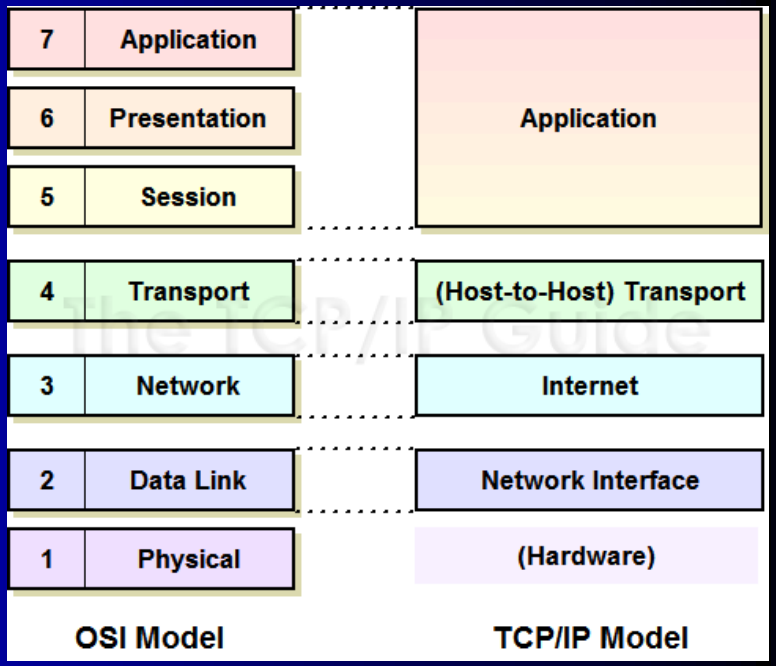
Internet est en fait un réseau de réseaux

On désigne par réseau ou plus précisément réseau téléinformatique un ensemble d'équipements comprenant, entre autres, des terminaux, des ordinateurs, des imprimantes, reliés entre eux par des liaisons de communication.



http://www.computerhistory.org/internet_history

internet ?



http://www.tcpipguide.com/free

internet … est un ensemble de protocoles (1969/1972)

- **IP** “Internet Protocol” (couche réseau)

  échange les données entre ordinateurs hôtes

- **TCP** “Transport Control Protocol” (couche transport)

  échange les données entre les applications

internet ?

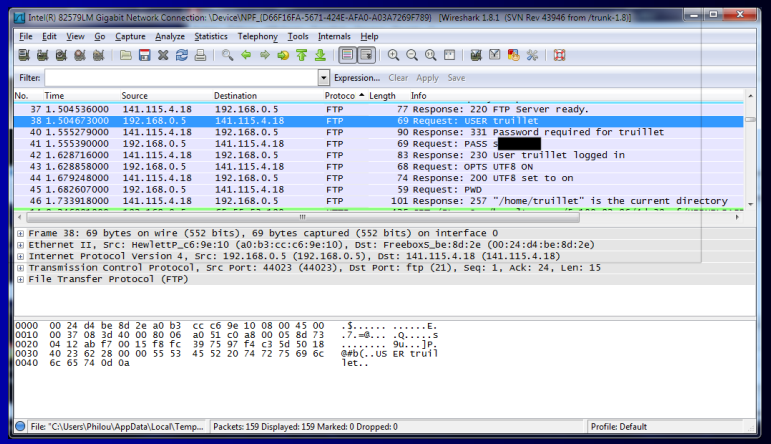
et **surtout** un ensemble de services !

- telnet, ssh
- ftp, sftp
- smtp, pop, imap
- p2p
- …
- et http, 

(le web) défini en 1990 au CERN

internet … sûr ?

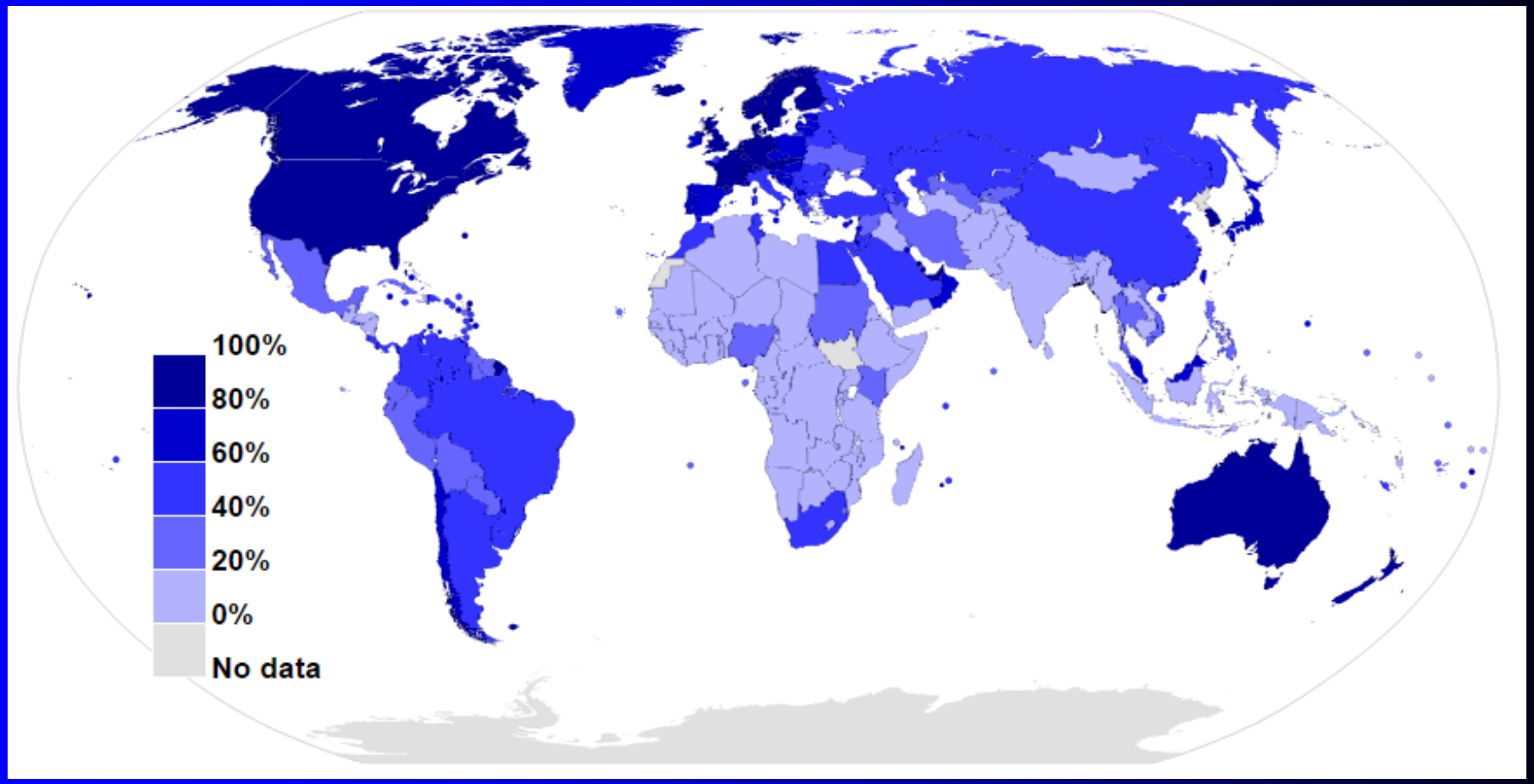
La manière de gérer le réseau est une des sources de faiblesse d'internet (certains mots de passe transitent « en clair » …)



http://www.wireshark.org

Une autre faiblesse réside (parfois) dans la mauvaise implémentation des piles de protocoles TCP/IP

internet ? des chiffres



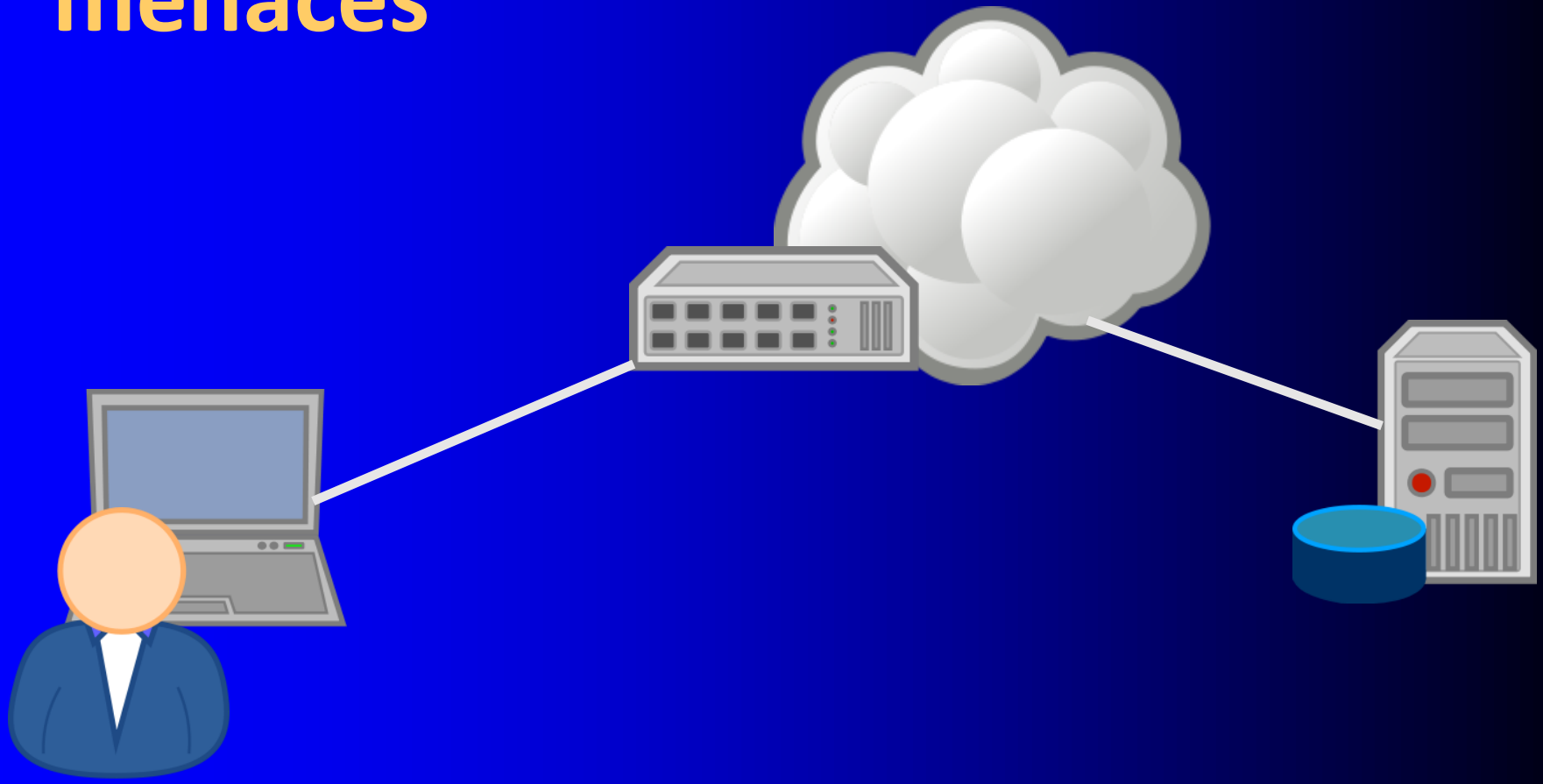
http://upload.wikimedia.org/wikipedia/commons/9/99/InternetPenetrationWorldMap.svg

internet : en conclusion

d'un outil pour les militaires (ARPANET) puis pour les chercheurs, le grand public s'est approprié « *internet* » …

La simplicité **d'usage** s'accompagne d'un certain nombre de « dangers » dans lesquels tombent un grand nombre d'internautes …

menaces



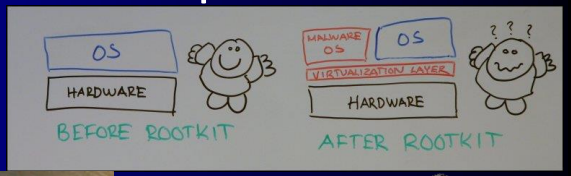
1 http://openclipart.org/detail/171417/laptop-by-cyberscooty-171417
2 http://openclipart.org/detail/171423/server---database-by-cyberscooty-171423
3 http://openclipart.org/detail/171432/user-1-by-cyberscooty-171432
4 http://openclipart.org/detail/152311/internet-cloud-by-b.gaultier
5 http://openclipart.org/detail/171420/switch-hub-by-cyberscooty-171420

menaces

- sur les serveurs

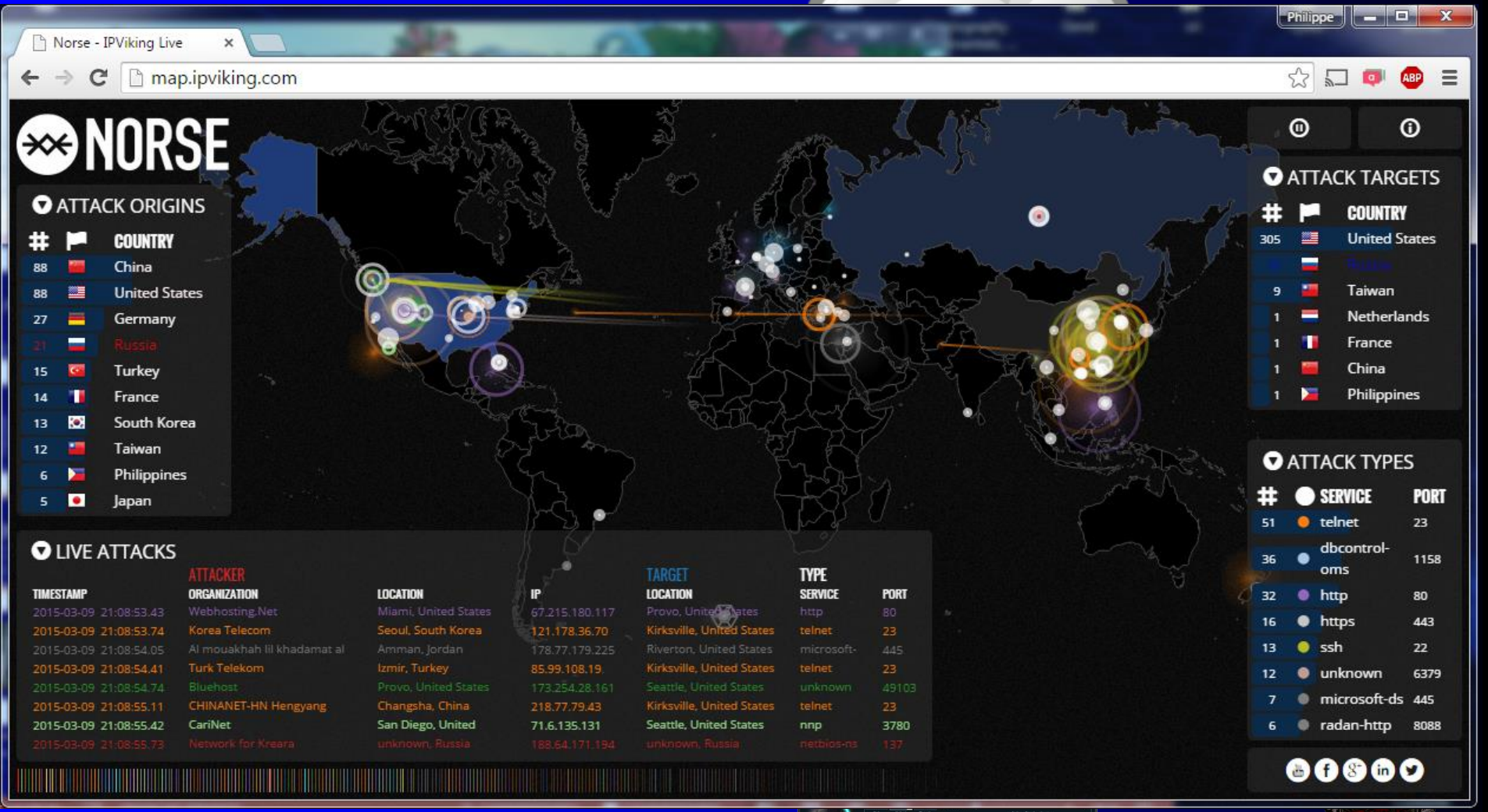
- Le « pirate » prend la main sur tout ou partie de la machine qui délivre des services
  - Ex: par intrusion (cassage de mots de passe, injection SQL, …)

- Il compromet des services
  - Ex : modification de pages web, ...
- Et/ou ouvre « des portes dérobées » pour revenir plus tard
  - Ex : usage de rootkits, …
  - Attaque de type « cheval de Troie »



http://www.f-secure.com/weblog/archives/archive-032006.html
http://hackaday.com/2011/06/28/teensy-avrs-used-in-penetration-testing/

menaces



http://sourceforge.net/projects/loic
http://map.ipviking.comhttp://map.ipviking.com/

http://nakedsecurity.sophos.com/2012/11/21/prince-william-photos-password/

quelques « dangers »

Les dangers sont donc … multiformes !

- spams
- virus, trojan, …
- keylogger
- phishing
- scamming
- « arnaques »
- ingénierie sociale …

quelques « dangers » : spams

« pourriels »

Les spammeurs cherchent … des adresses méls valides !

La plupart du temps, les FAI proposent des outils de détection et d'élimination des spams

Évitez de laisser traîner votre adresse sur internet

https://www.youtube.com/watch?v=anwy2MPT5RE

quelques « dangers » : virus

Logiciels malveillants conçus pour se propager …

- Premières « traces » en 1986 avec « Brain » qui se propage par disquette

- Caractéristiques
  - Chiffrement
  - Polymorphisme ou métamorphisme
  - furtivité

http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Cryptolocker-une-prise-d-otages-en-2.0

Le réseau de la ville attaqué par le virus «Rançongiciel»

Article exclusif
réservé aux abonnés Voir l'offre Digital

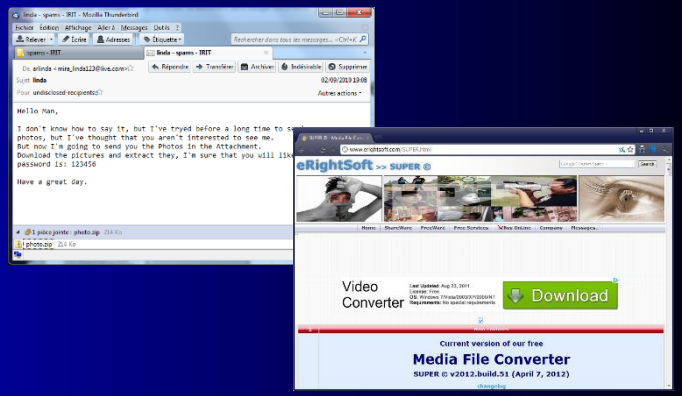
Votre crédit de bienvenue en cours : 20 **articles**

Publié le 13/03/2015 à 03:53, Mis à jour le 13/03/2015 à 06:56

Sciences / High tech - Informatique

quelques « dangers » : virus

L'objectif n'est plus totalement de « détruire » mais « d'utiliser » le système hôte comme *botnet*



- Relai de *spams*
- Opérations de *phishing*
- Infection de nouvelles machines
- Attaques groupées (*DDos*)
- Vol d'informations
- Exploitation la puissance de calcul pour casser des mots de passe, …
- …

quelques « dangers » : virus

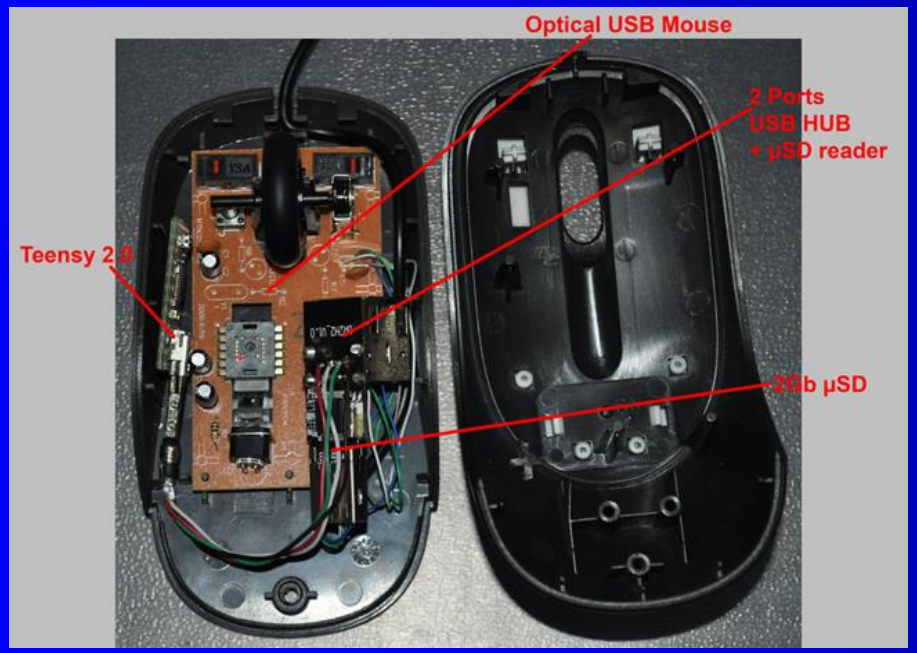
Comment s'en protéger ?

- **« faire attention »** à ce que l'on reçoit, ce que l'on télécharge
- **faire les mises à jour** de votre OS, logiciels
- **utiliser des logiciels antivirus**

quelques « dangers » : trojan

Littéralement, « cheval de Troie » (comme la légende …)

- Sous couvert de logiciels ou de matériels « sûrs », ouvrent des portes dérobées sur votre ordinateur

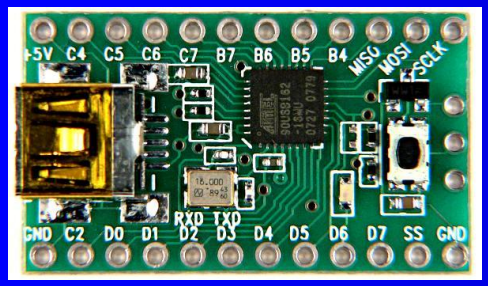


Ex : http://pentest.netragard.com/2011/06/24/netragards-hacker-interface-device-hid/

http://www.nes.fr/securitylab/?p=374

quelques « dangers » : trojan

Une démonstration



http://www.pjrc.com/teensy

TeensyHack | Arduino 1.0

File Edit Sketch Tools Help

TeensyHack §

```
/*The following is Astro's code using the PHUKD libs from
Irongeek http://www.irongeek.com/downloads/phukdlib0.2.zip
to do some Keyboard stuff with Teensy only for educational purposes.
Use at your own risk !
To learn more about Teensyduino see: http://www.pjrc.com/teensy/teensyduino.html  http://www.ardui
void setup() {}

void loop ()
{
  delay(5000); //Wait 5 secs to settle down
  Keyboard.set_modifier(MODIFIERKEY_CTRL);
  Keyboard.send_now();
  Keyboard.set_key1(KEY_ESC);
  Keyboard.send_now();
  Keyboard.set_modifier(0);
  Keyboard.set_key1(0);
  Keyboard.send_now();
  Keyboard.print("powershell");
  //Keyboard.print("powershell -Command '$disk = wmic logicaldisk list brief | select-string -patt
  Keyboard.set_key1(KEY_ENTER);
  Keyboard.send_now();
  Keyboard.set_key1(0);
  Keyboard.send_now();

  delay(5000); //Need some time on some machines to open powershell
  Keyboard.print("$disk = wmic logicaldisk list brief | select-string -pattern mydisk | out-string
```

Done uploading.

```
Attemping to safely remove USB Disk...
Attemping to safely remove USB Disk...
Unable to safely remove USB Disk
error sending reboot command
```

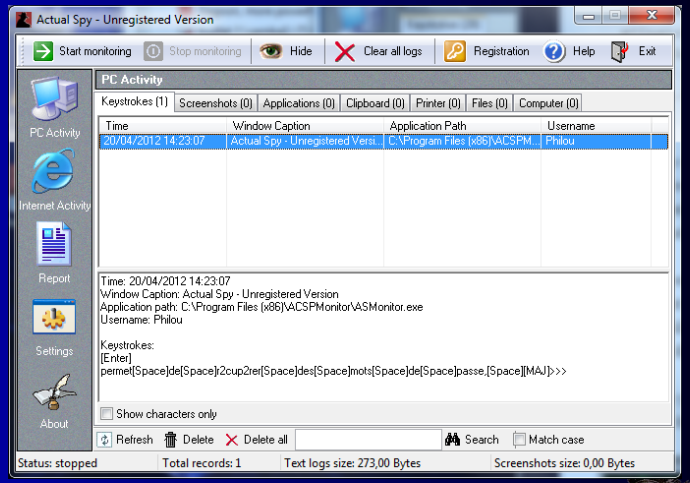
37 Teensy 2.0 on (USB Port)

http://arduino.cc

quelques « dangers » : keylogger

Logiciel ou matériel « espion » (spyware), enregistre les frappes sur le clavier, parfois les déplacements souris … et les stocke ou les envoie à un tiers …

Permet de récupérer des mots de passe, …



http://www.it-connect.fr/keysweeper-un-keylogger-pour-clavier-sans-fil-microsoft/

quelques « dangers » : phishing

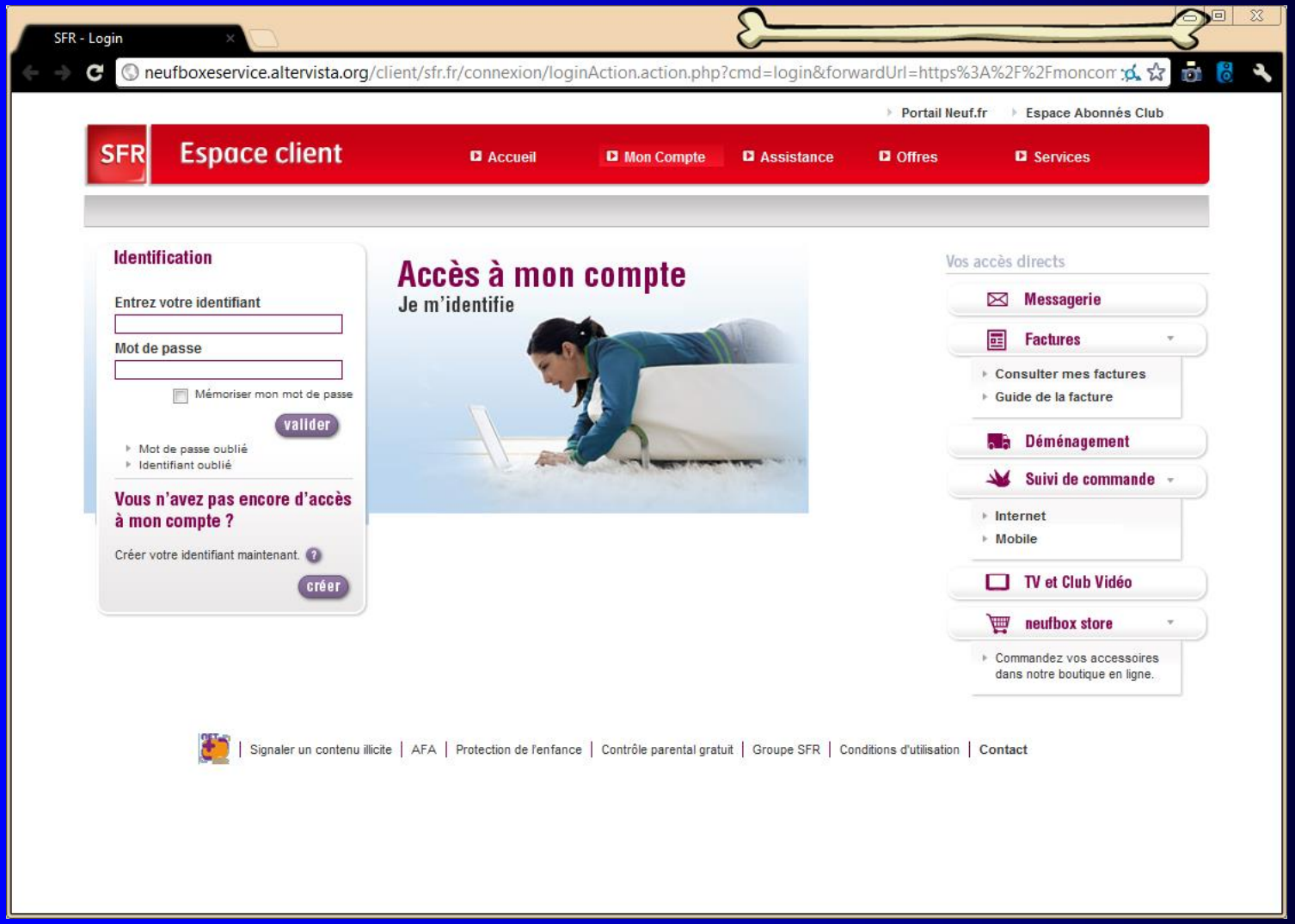
Littéralement, « hameçonnage », permet de perpétrer une usurpation d'identité (et pas que numérique !)

La technique consiste à faire croire que l'on s'adresse à un tiers de confiance

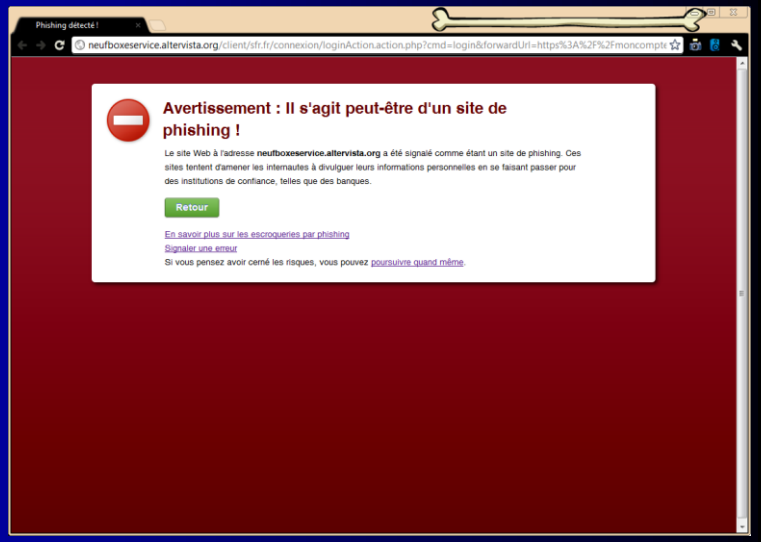
Repose sur l'ingénierie sociale

Peut se faire par courrier électronique, sites web frauduleux, …

quelques « dangers » : phishing



quelques « dangers » : phishing

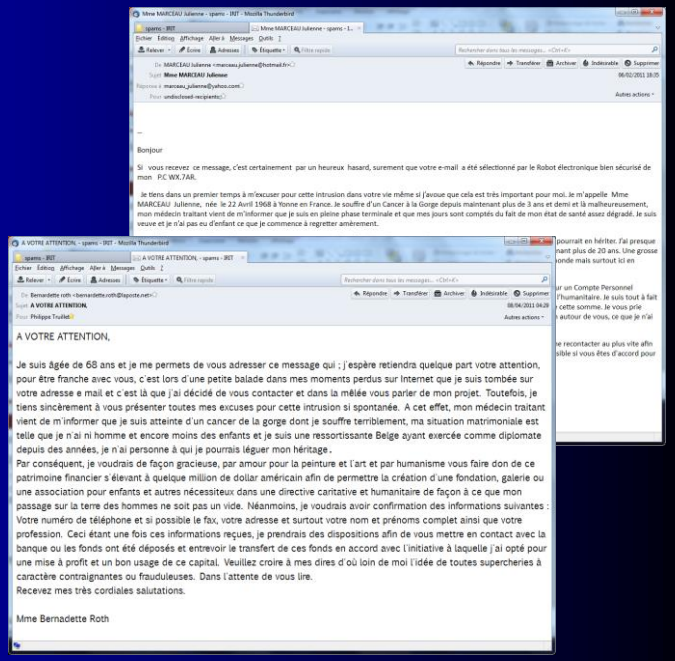


Comment s'en protéger ?

- **Être vigilant !**
- **Savoir détecter les potentiels problèmes et « lire »**

quelques « dangers » : scamming

dit « *arnaque à la nigériane* »
(ou fraude 419)
(http://www.securityvibes.fr/menaces-alertes/
fraude-nigeriane-20-000-de-gain-par-victime-en-moyenne)



Repose aussi sur la naïveté et la cupidité
(ancêtre lointain de l'arnaque : les lettres de Jérusalem, fin XVIIIè siècle)

quelques « dangers » : scamming

Comment s'en protéger ?

- **Signaler les méls comme indésirables …**
- **Détruire les méls dès réception**
- **Ne PAS répondre !**

quelques « dangers » : arnaques

Les malfrats profitent de sites « *bien connus* » comme eBay, leboncoin.fr vendez, achetez, près de chez vous ...

ils peuvent être vendeurs ou acheteurs !

quelques « dangers » : arnaques

Comment s'en protéger ? Encore une fois, en restant méfiant notamment lorsque :

- Vous recevez des opportunités d'investissement présentées comme exceptionnelles.
- On vous présente des bonnes affaires pour les équipements électroniques, véhicules ou autres.

quelques « dangers » : ingénierie sociale

Attaques les plus efficaces ! (+75%)

C’est une attaque de persuasion … et il n’y a pas besoin d’avoir de connaissances techniques …

- Sessions restées ouvertes
- Discussions …

Code carte bleue : 1204 (à cacher)

Actualité > Grand Sud > Tarn > Castres

Un collégien aurait trafiqué ses notes par internet

Publié le 12/03/2015 à 03:55, Mis à jour le 12/03/2015 à 07:34

Faits divers - Castres (81)

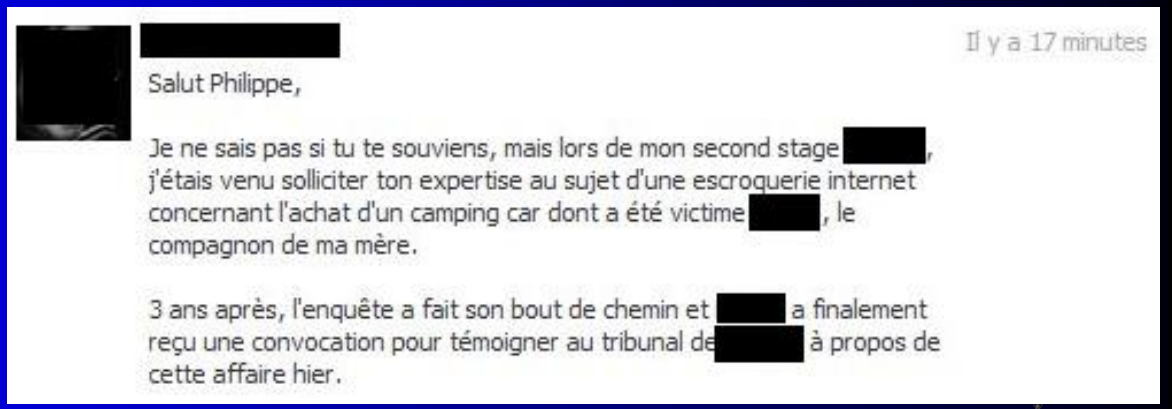
Un adolescent se serait fait passer pour le principal de son collège pour récupérer, par e-mail auprès du rectorat, des codes d'accès au système informatique de l'établissement afin d'augmenter ses notes.

quelques « dangers » : bilan

Faible préjudice par victime (1 000 à 3 000 €) mais qui rapporte gros ! (estimé à plus de 5 M € depuis 2004)

Auteurs souvent étrangers

Difficulté à enquêter et retrouver les auteurs (mais ça arrive !)


[redacted] Il y a 17 minutes

Salut Philippe,

Je ne sais pas si tu te souviens, mais lors de mon second stage [redacted], j'étais venu solliciter ton expertise au sujet d'une escroquerie internet concernant l'achat d'un camping car dont a été victime [redacted], le compagnon de ma mère.

3 ans après, l'enquête a fait son bout de chemin et [redacted] a finalement reçu une convocation pour témoigner au tribunal de [redacted] à propos de cette affaire hier.

quelques « dangers » : bilan

Un seul mot d'ordre : VIGILANCE !

Ne pas hésiter à signaler les méls et sites suspects →

- **https://www.internet-signalement.gouv.fr**
- **https://www.signal-spam.fr**

tous cybercriminels ?

La cybercriminalité, c'est **l'ensemble des infractions pénales** (définies par le Code Pénal) qui se commettent sur le **réseau Internet**

En explicitant, **la cybercriminalité** peut se définir comme **l'ensemble des exactions commises par un moyen lié aux nouvelles technologies**, principalement Internet, permettant l'intrusion par des réseaux filaires, hertziens ou satellites, de voler, détourner, paralyser, désinformer, contrefaire, modifier, détruire des données, s'en procurer et échanger des contenus illégaux

tous cybercriminels ?

Le cybercrime génèrerait plus d'argent que la drogue !

- Une des cinq plus grandes menaces pour l'économie mondiale d'après l'OCDE
- Les attaques génèreraient plus de 1 000 milliards de US$ par an
- Ont coûté en moyenne 2,2 M US$ aux entreprises visées en 2010 (+ 16% par rapport à 2009)
- Entre le 1er janvier et 31 mars 2010, MacAfee a découvert 8 600 nouveaux sites malveillants par jour

…

http://www.silicon.fr/la-cybercriminalite-rapporte-plus-que-la-drogue-55193.html

tous cybercriminels ?

En quoi suis-je complice ?

Exemple pour les sites de streaming et téléchargement direct

- Revenus captés par ces sites de l'ordre de 52 à 71 M € (entre 2010 et 2011) relativement aux 177 M € du marché légal

Table 3 : Classement des principaux services de référencement de contenus en streaming en France selon leur trafic (classement Alexa en nombre de visiteurs uniques)

	Marque	Films	Séries	Animés	Total	Classement Alexa (France)
1.	DPstream	14 179	2 304	1 663	18 146	54
2.	Streamiz	35 527	0	0	35 527	99
3.	Allo Show TV	29 614	855	0	30 469	203
4.	Streamania	16 578	1 953	1 566	20 097	963
5.	Cinemay	8 024	196	0	8 220	1 329
6.	StreamXD	6 255	431	265	6 951	1 843
7.	Filmze	812	0	0	812	1 988
8.	StreamLibre	7 132	51	0	7 183	2 299
9.	Lookiz	14 698	2198	1251	18 147	2 453
10.	Film 2 Streaming	45 655	0	0	45 655	2 475
11.	FilmsStreaming.com	1 591	0	0	1 591	2 739
12.	123serie	0	1150	0	1 150	3 031
13.	Streamov	17 785	0	0	17 785	3 036
14.	Streamovie.tv	1 186	0	10	1 196	3 083
15.	Movienostop	4 360	980	360	5 700	3 164
16.	Allo Streaming	62 611	42	4240	66 893	3 525
17.	StreamingDivx	3 672	0	0	3 672	3 542
18.	Streambot	8 697	0	468	9 165	16 923
19.	Films Live	7 874	0	0	7 874	17 653
20.	Streaming-az.com	1 872	0	0	1 872	22 142
21.	DyCine.com	7 715	120	0	7 835	46 184
22.	CineSoir	39 270	1944	2160	43 374	54 544
23.	Films Streaming	1 240	0	0	1 240	62 510
24.	Electrociné	38 984	n.a.	n.a.	38 984	n.a.
25.	Easy streaming	96	0	0	96	n.a.

Source : IDATE, le 11/01/2012

http://hadopi.fr/sites/default/files/page/pdf/Rapport_IDATE.pdf
2014 – Out-of-Cycle Review of Notorious Market, USA Trade Representative – March, 5th 2015

tous cybercriminels : bilan

Des actes anodins en apparence peuvent avoir des conséquences dramatiques pour tout un chacun …

Nous sommes responsables de nos actions !

Sécurité ?

“Le seul système informatique vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés. Même dans ces conditions, je ne parierais pas ma vie dessus.”

Pr .Eugene Spafford
Purdue University

Sécurité

- Protéger sa vie privée
- Communiquer ?!

- Etre vigilant !

Sécurité - vie privée

Informations personnelles

Droit à l'image

Traces sur le net

Sécurité - vie privée

Pourquoi protéger ses informations ?

- Les données personnelles intéressent beaucoup les sites web ! (→ publicité ciblée)
- Tout ce qui est posté « ne vous appartient plus » …

Les informations à éviter de partager

- Localisation réelle, date de naissance, photos, … sauf si vous êtes réellement conscient de ce que vous faites ☺

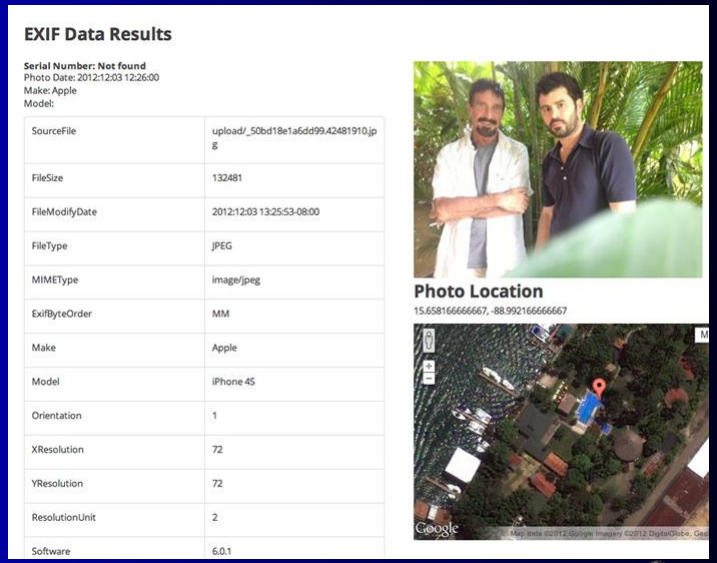
Sécurité - vie privée

Publier des photos de soi ?

- Peut-être mais pourquoi ? Pour qui ?

Nous laissons des traces …

- Historique de navigation
- Cookies
- Données EXIF (photos)
- …



EXIF Data Results

Serial Number: Not found
Photo Date: 2012:12:03 12:26:00
Make: Apple
Model:

SourceFile	upload/_50bd18e1a6dd99.42481910.jpg
FileSize	132481
FileModifyDate	2012:12:03 13:25:53-08:00
FileType	JPEG
MIMEType	image/jpeg
ExifByteOrder	MM
Make	Apple
Model	iPhone 4S
Orientation	1
XResolution	72
YResolution	72
ResolutionUnit	2
Software	6.0.1

http://www.mobileprivacy.org/2012/12/vice-com-publishes-exclusive-with-john-mcafee-reveals-location-in-iphone-metadata-exif/

Sécurité – communiquer

Blogs / informations

Chats – messageries instantanées / Forums

Sécurité – communiquer

Manipulation de données

- D'un prof (mars 2012)
  - Petite expérience amusante sur l'usage du numérique en lettres

http://www.laviemoderne.net/lames-de-fond/009-comment-j-ai-pourri-le-web.html

- Mais aussi des élèves (avril 2012)
  - Un élève modifie wikipédia pour maquiller sa triche

http://tempsreel.nouvelobs.com/societe/20120417.OBS6389/un-eleve-modifie-wikipedia-pour-maquiller-sa-triche.html

Sécurité – communiquer

Chats/Forums : permettent de discuter rapidement

Il est facile de se faire passer pour quelqu'un d'autre …

http://clione.skyrock.com/3053959583-Gens-de-la-vraie-vie-toi-et-moi-et-leurs-avatars-toi-et-moi.html

un point sur le « web 2.0 »

Les réseaux sociaux, c'est le partage (voir et être vu) !

- Partage de vidéos
- Partage de podcasts
- Partage de photos et de diaporamas
- Partage de CV, mise en relation
  - Réseaux publics
  - Réseaux professionnels
- Partage de bookmarks
- Partage d'informations et de savoir Wikipédia

un point sur le « web 2.0 »

“Le Web 2.0 pourrait être vu comme un réseau social mondial où chaque site participant est acteur du réseau et contribue à rendre acteurs les internautes”

Les réseaux sociaux ont des caractéristiques communes :

- un profil utilisateur
- une recherche parmi les utilisateurs
- une offre de mise en communication entre utilisateurs,
- une incitation à donner de l’information.

un point sur le « web 2.0 »

En tant qu'individu

- Se créer un profil uniforme (si nécessaire minimaliste) et maintenu à jour sur les différentes plateformes de réseaux sociaux
- Réfléchir avant d'y inscrire un profil trop complet
- Se souvenir de l'aspect temporel de l'information (indélébilité)

un point sur le « web 2.0 »

Des soucis …

- « mémoire » du web
  - À cause de cette image (sur MySpace)
    Stacy Snyder a perdu son travail à l'université de Millersville (PA- USA) [plainte rejetée en 2008]

Selon une étude de Microsoft, **75% des recruteurs** collectent de l'information sur les candiats sur le web (moteurs de recherche, réseaux sociaux, sites de partage, blogs, …)

70% disent qu'ils ont rejeté des candidats à cause des informations trouvées en ligne (notamment photos et discussions) !

https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=1&pagewanted=all

conclusion

La sécurité, c'est d'abord et surtout la vigilance !

- Être conscient de nos actes
- Être conscient des conséquences

Internet est un formidable outil qui nous ouvre le monde entier : tirons-en le meilleur !

contact

Site web / mél

http://www.irit.fr/~Philippe.Truillet

Philippe.Truillet@univ-tlse3.fr

Réseaux sociaux

Philippe Truillet (Profil Professionnel)

Philippe.Truillet.Pro