INTERNET : UN NOUVEAU FAR-WEST ?

Janvier 2021

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

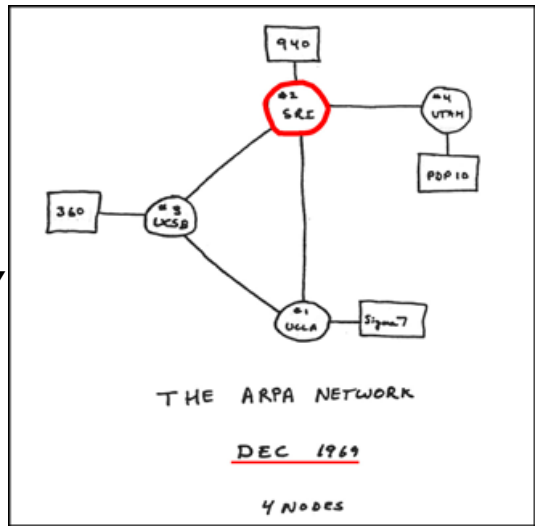
UN CONSTAT

La première réalité d'Internet est **qu'il n'y a plus de frontières : le monde est un village !**

UN SECOND CONSTAT

INTERNET ?

https://www.youtube.com/watch?v=_7ZtlSeGyCY

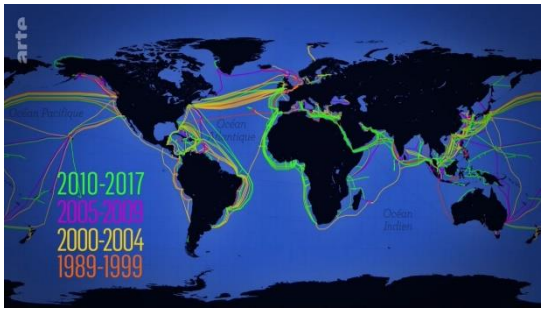


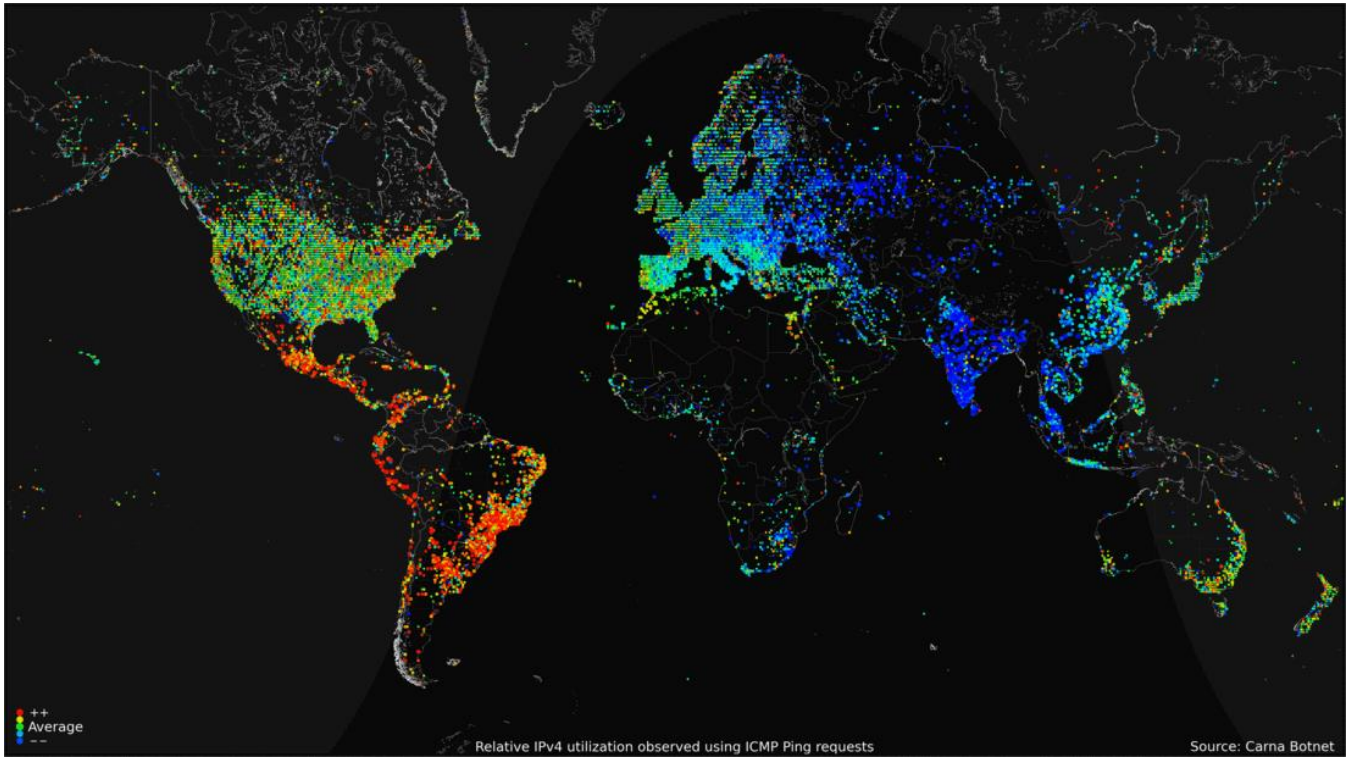
Un des pionniers : Douglas Engelbart (1925-2013)

- A l'intuition d'internet[1] dès les années 1950 (son laboratoire –SRI- participe à la première liaison en 1969 avec l'UCLA)
- Démontre la première vidéoconférence (1968) « *The Mother of All demos* »[2] (Le 1er Skype)
- 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

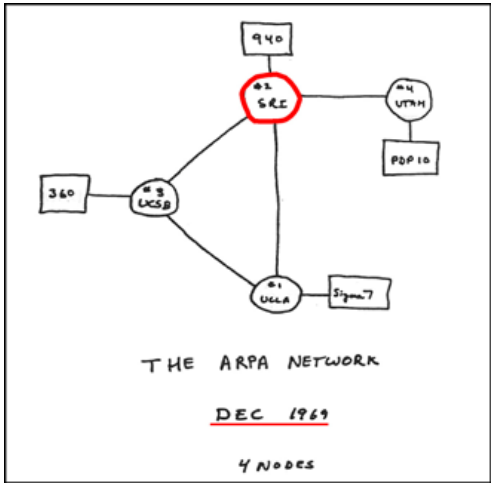
INTERNET ?

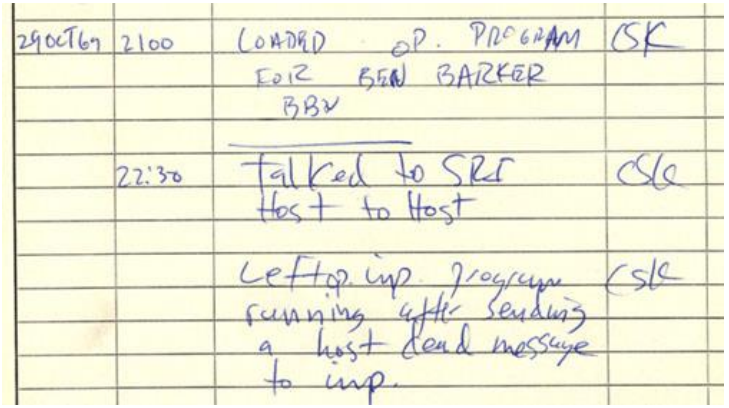




http://motherboard.vice.com/blog/this-is-most-detailed-picture-internet-ever

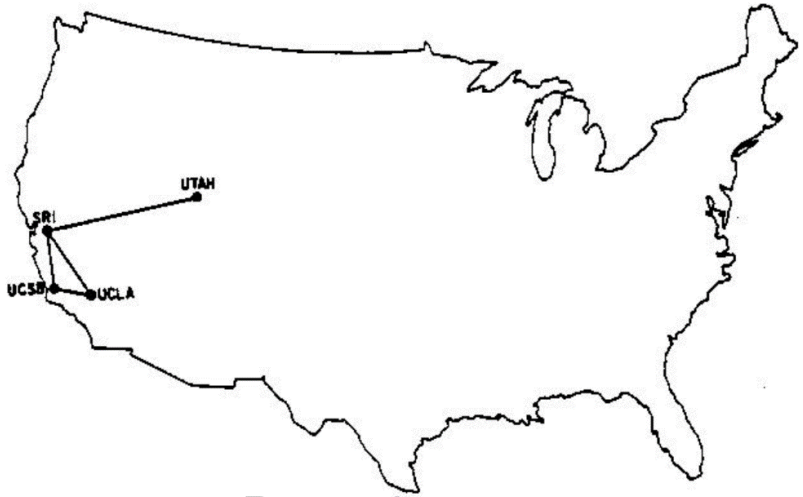
Internet est … un réseau de réseaux (Vous en avez un <u>morceau</u> à la maison !)



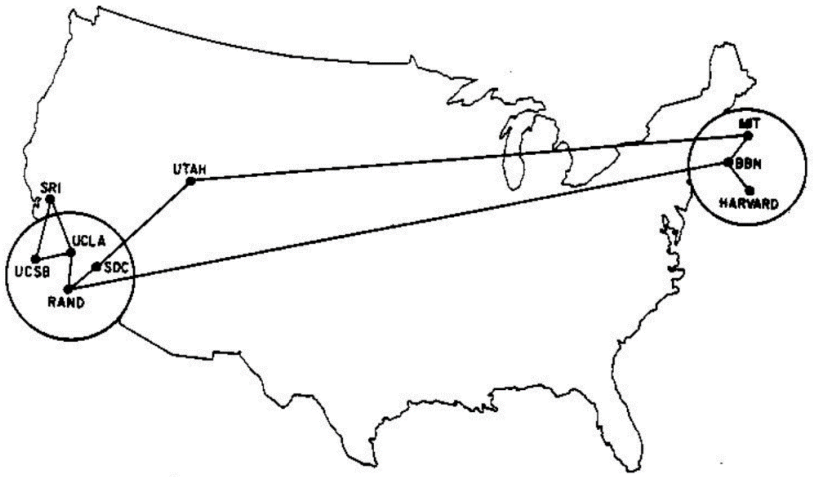


http://www.computerhistory.org/internet_history

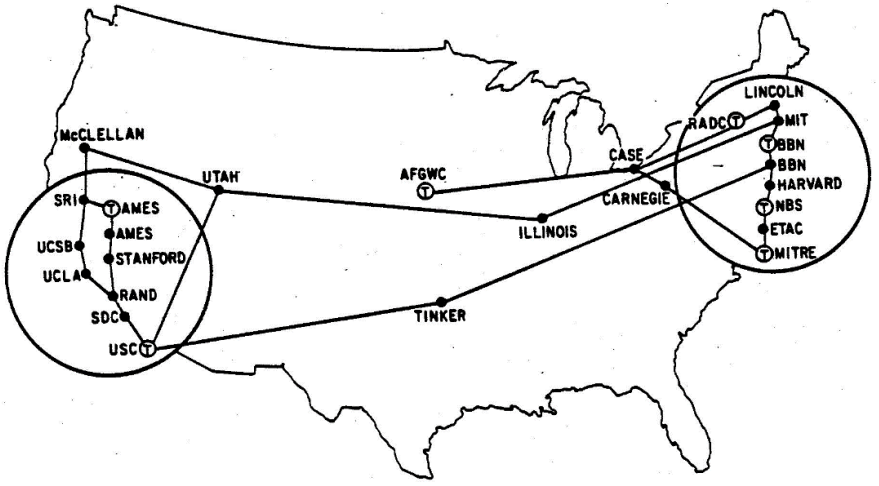
INTERNET ?



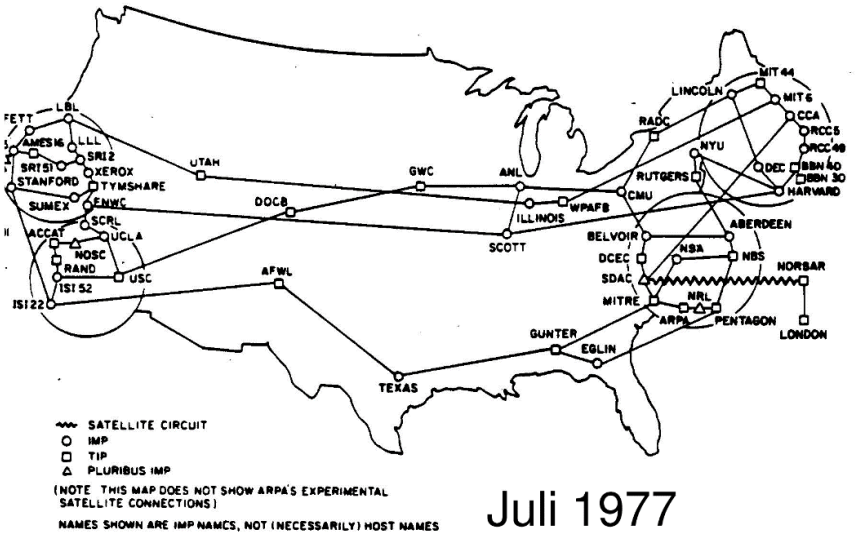
Dezember 1969



Juni 1970

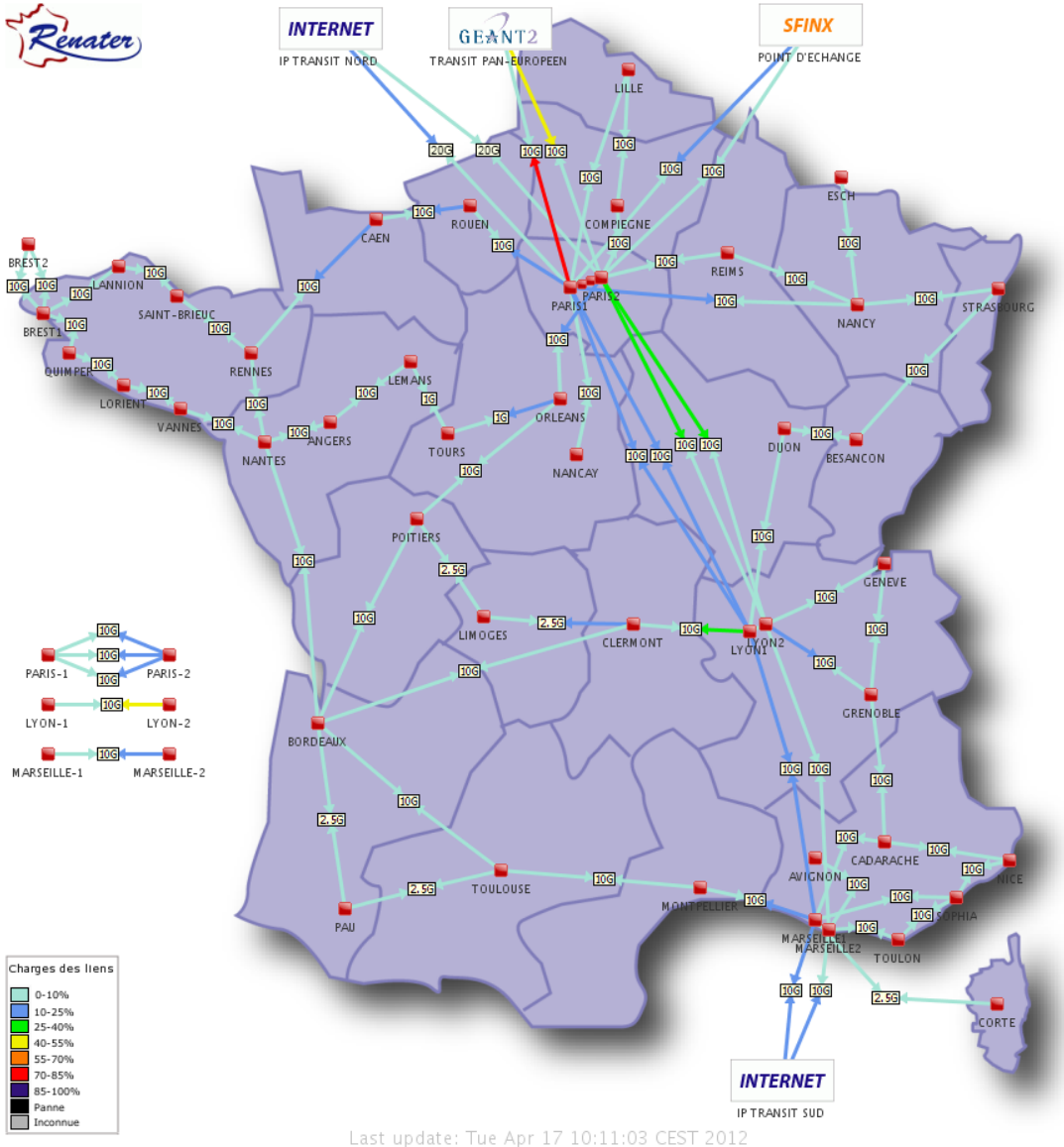


März 1972

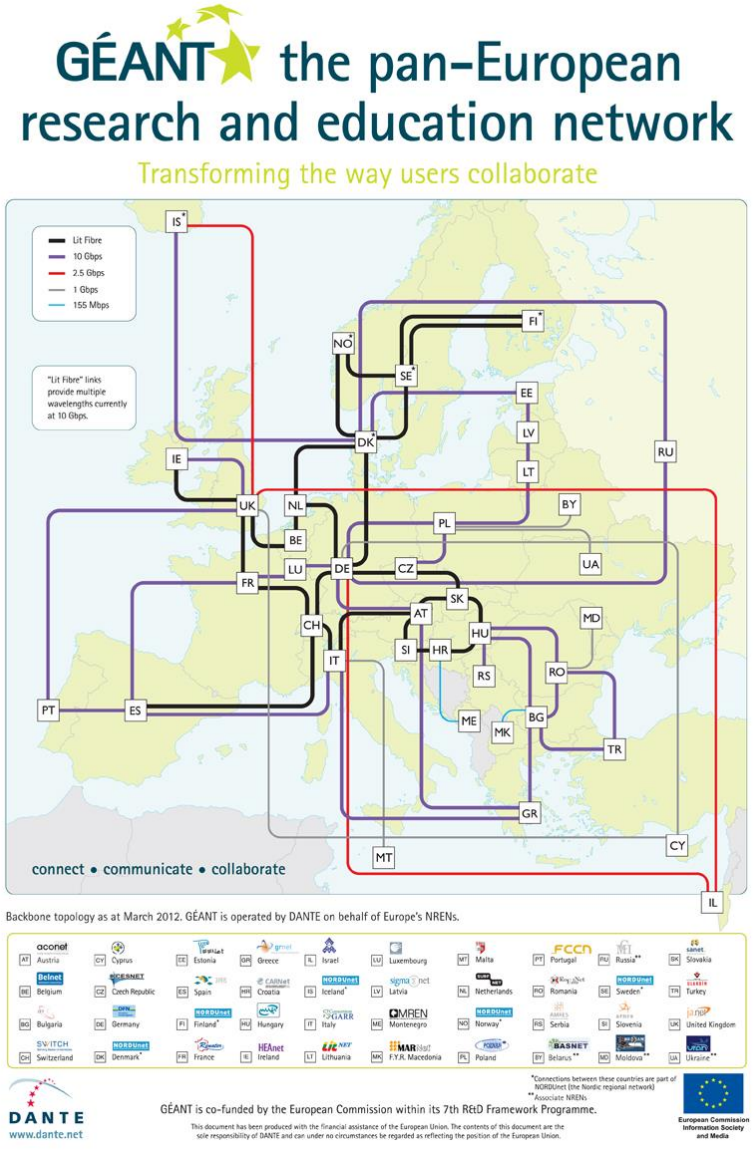


Juli 1977

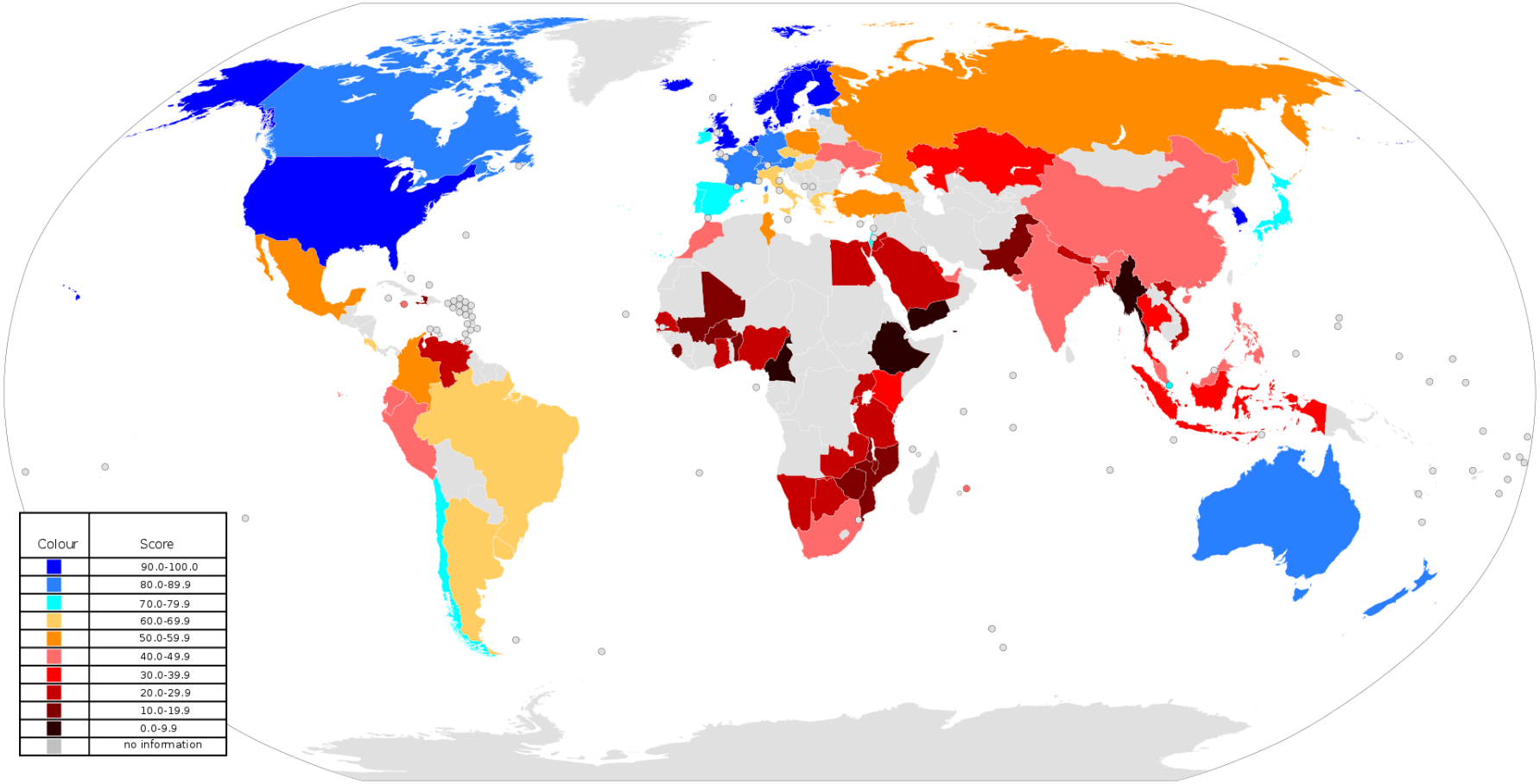
INTERNET ?



Last update: Tue Apr 17 10:11:03 CEST 2012

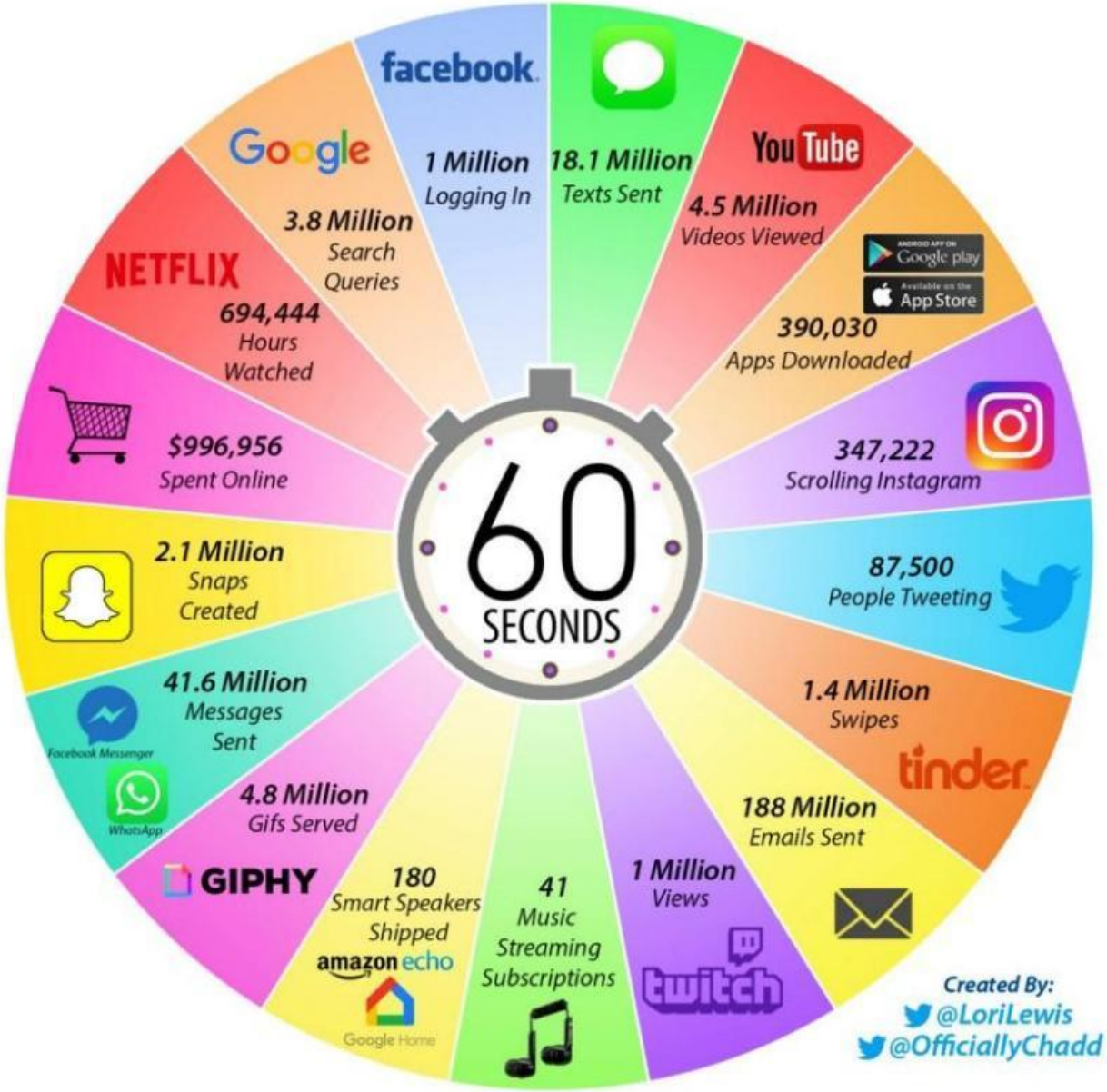


INTERNET ? DES CHIFFRES (2014)



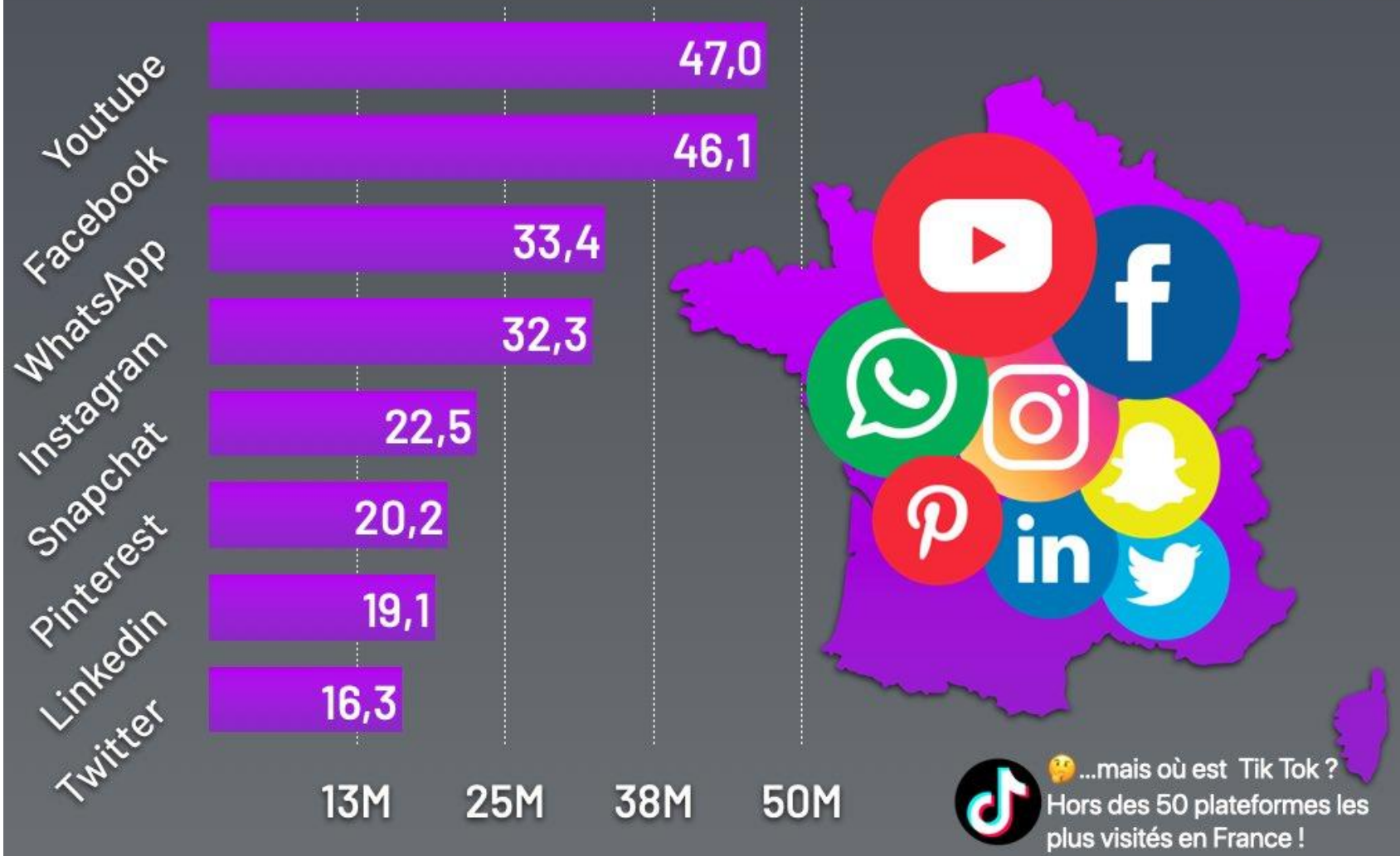
https://en.wikipedia.org/wiki/File:InternetPenetrationWorldMap.svg

2019 This Is What Happens In An Internet Minute



Classement Médias Sociaux en France - Novembre 2020

Mediametrie

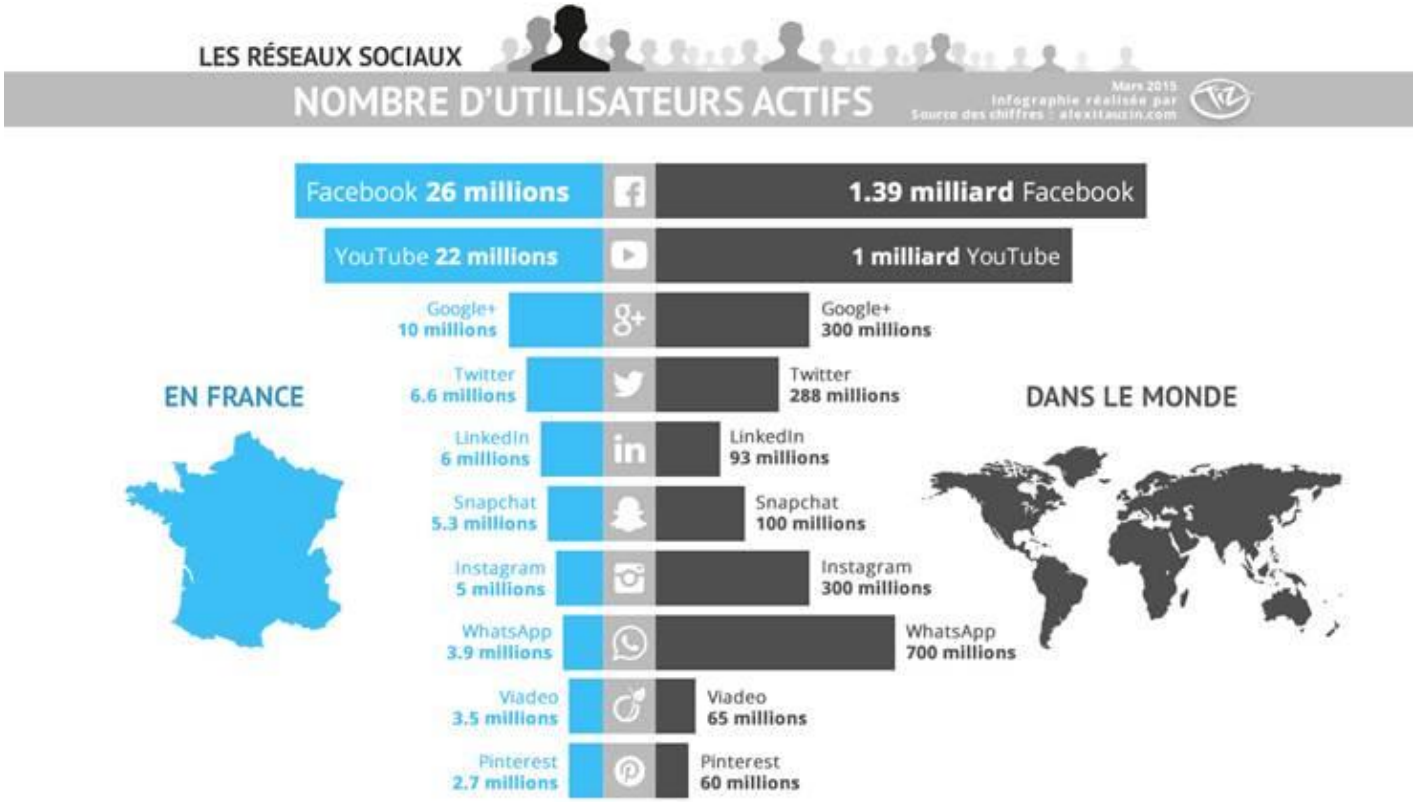


🤔...mais où est Tik Tok ?
Hors des 50 plateformes les plus visités en France !

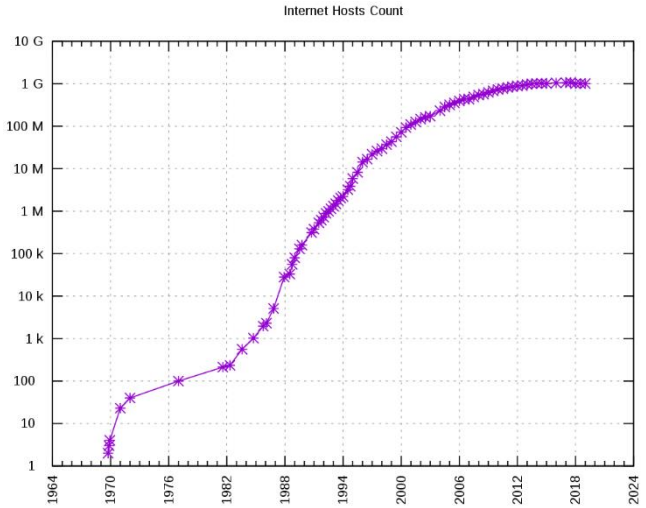
Komboo

Nombre de visiteurs uniques par mois

INTERNET ? DES CHIFFRES



INTERNET ? DES CHIFFRES



https://en.wikipedia.org/wiki/Global_Internet_usage#/media/File:Internet_Hosts_Count_log.svg

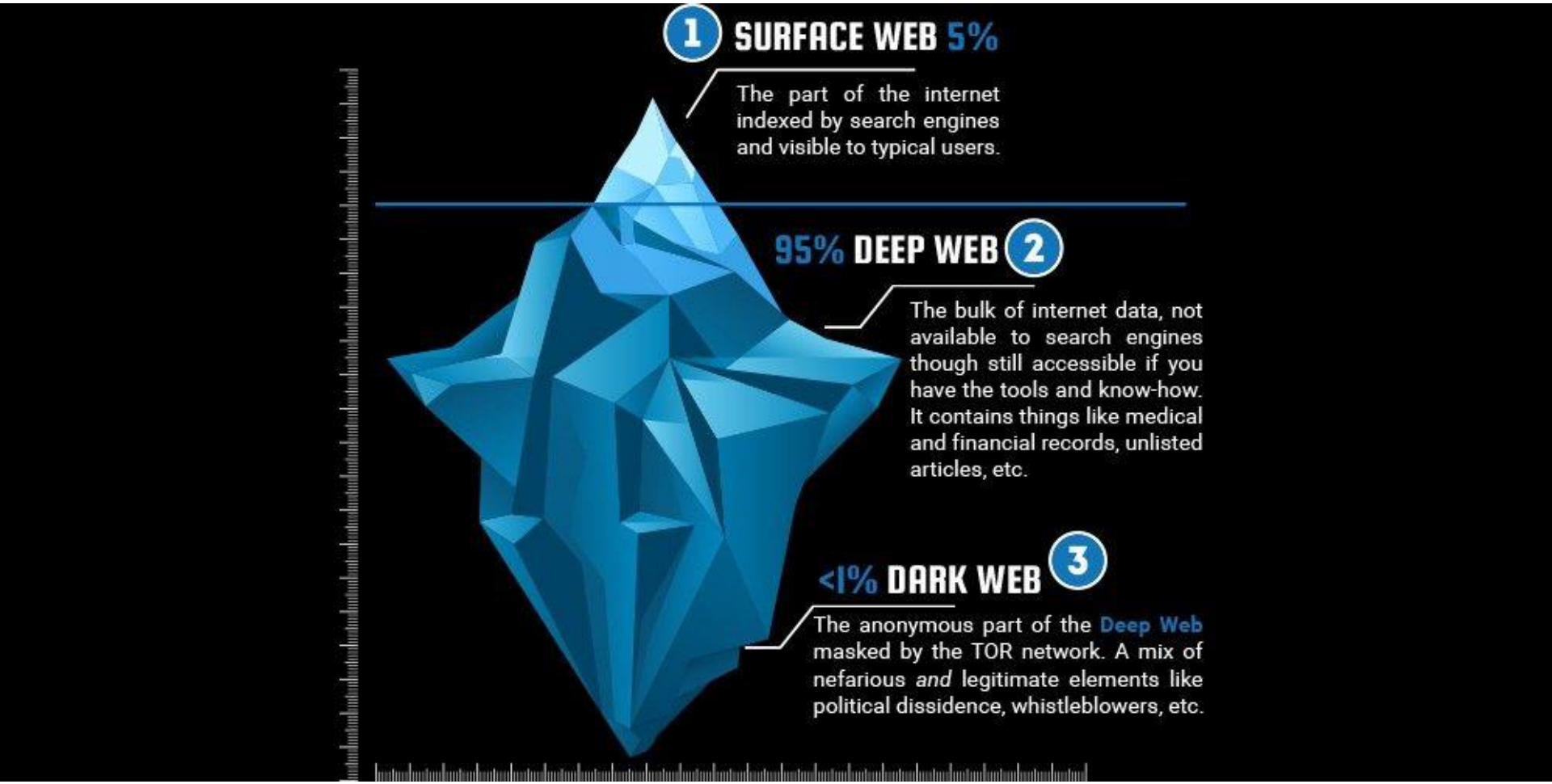
3,43 milliards d'internautes

- 144 milliards d'emails envoyés par jour (2/3 sont des spams)

1 site internet sur 500 est infecté par un virus ou un malware

- Google bloque 10 000 sites /jour

INTERNET ?


1
SURFACE WEB 5%
The part of the internet indexed by search engines and visible to typical users.
95% DEEP WEB
2
The bulk of internet data, not available to search engines though still accessible if you have the tools and know-how. It contains things like medical and financial records, unlisted articles, etc.
<1% DARK WEB
3
The anonymous part of the Deep Web masked by the TOR network. A mix of nefarious and legitimate elements like political dissidence, whistleblowers, etc.

"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

INTERNET … ET ARNAQUES

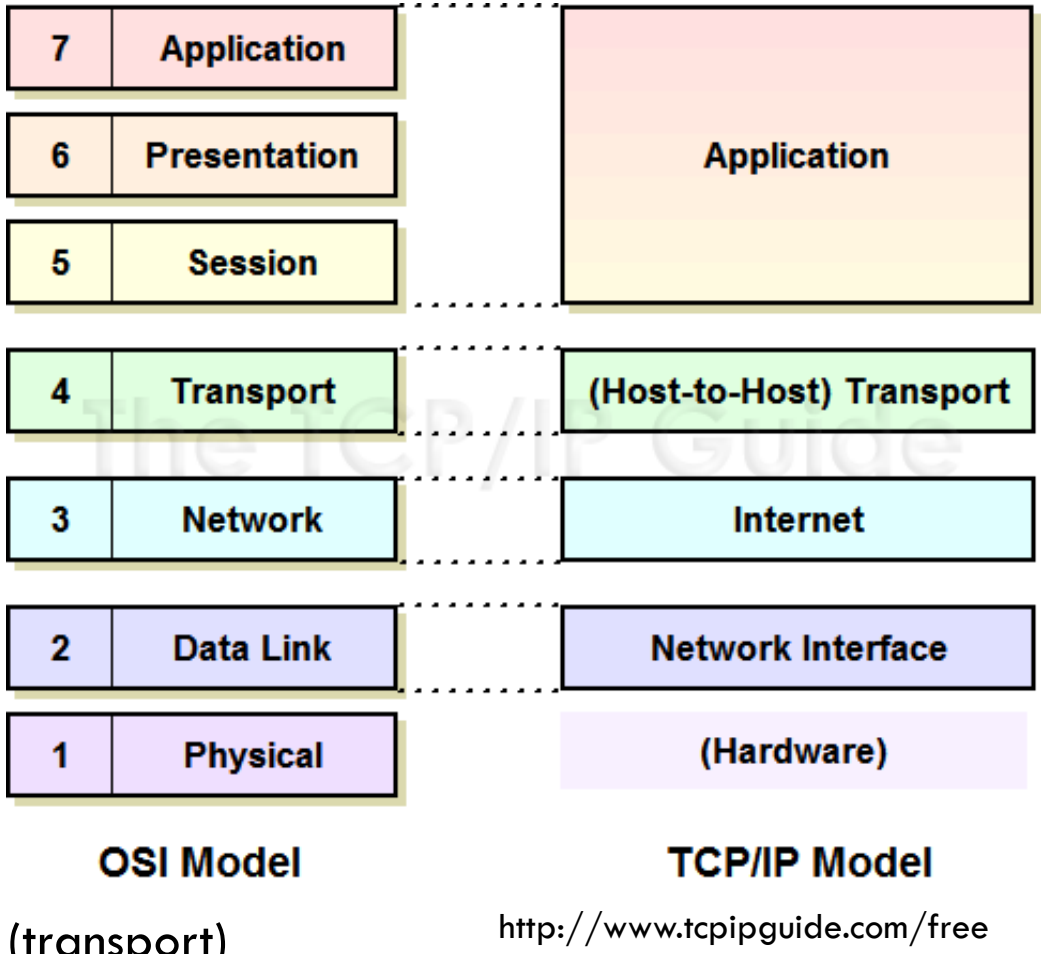
Le(s) danger(s) réside(nt) d'abord dans la

CONFIANCE

INTERNET … ET ARNAQUES

- **Confiance** dans les **réseaux** utilisés (infrastructure)
- **Confiance** dans les **machines** (PC, smartphones, …)
- **Confiance** dans les **personnes** derrière les machines

INTERNET ?



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

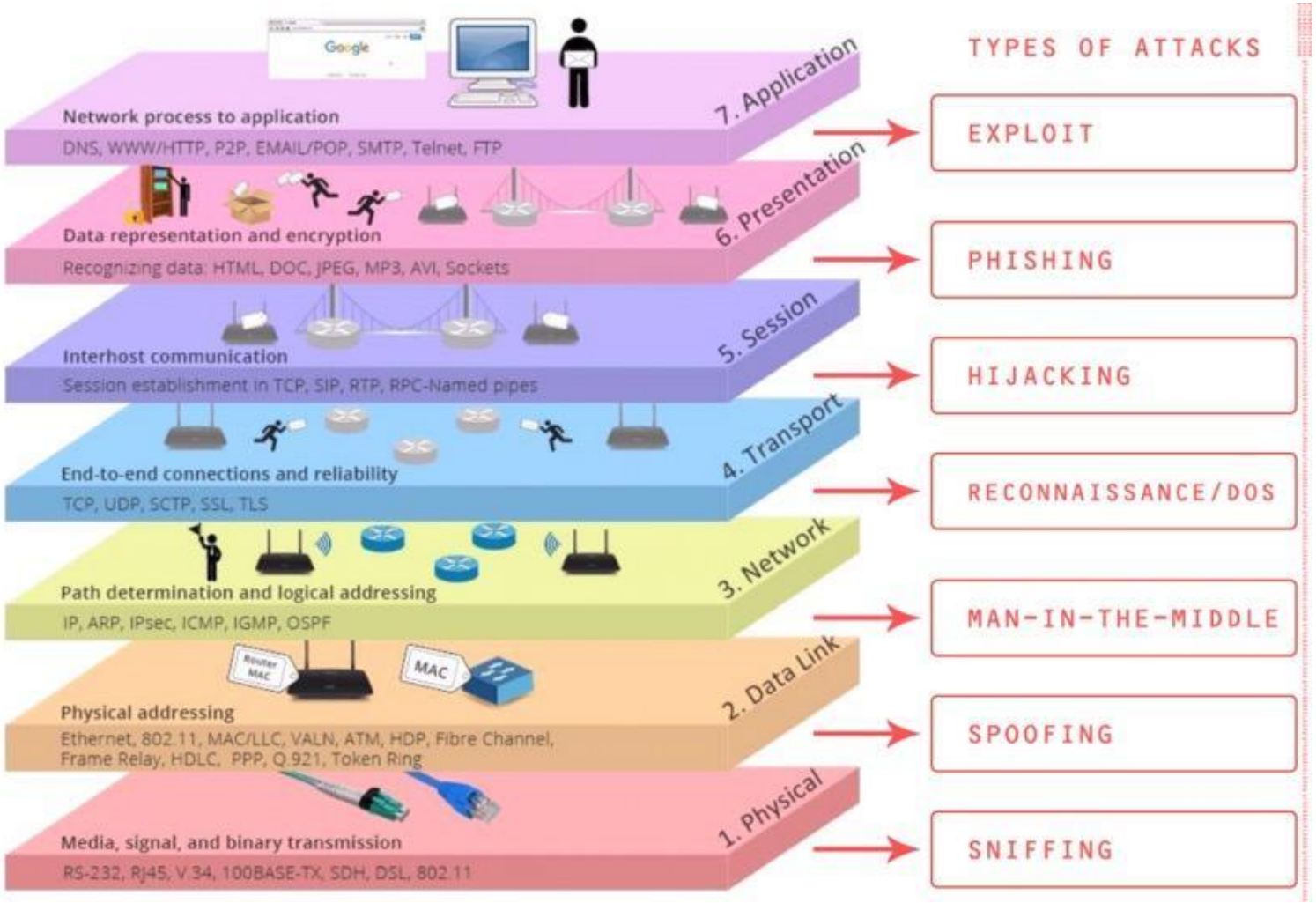
IP "Internet Protocol" (réseau)

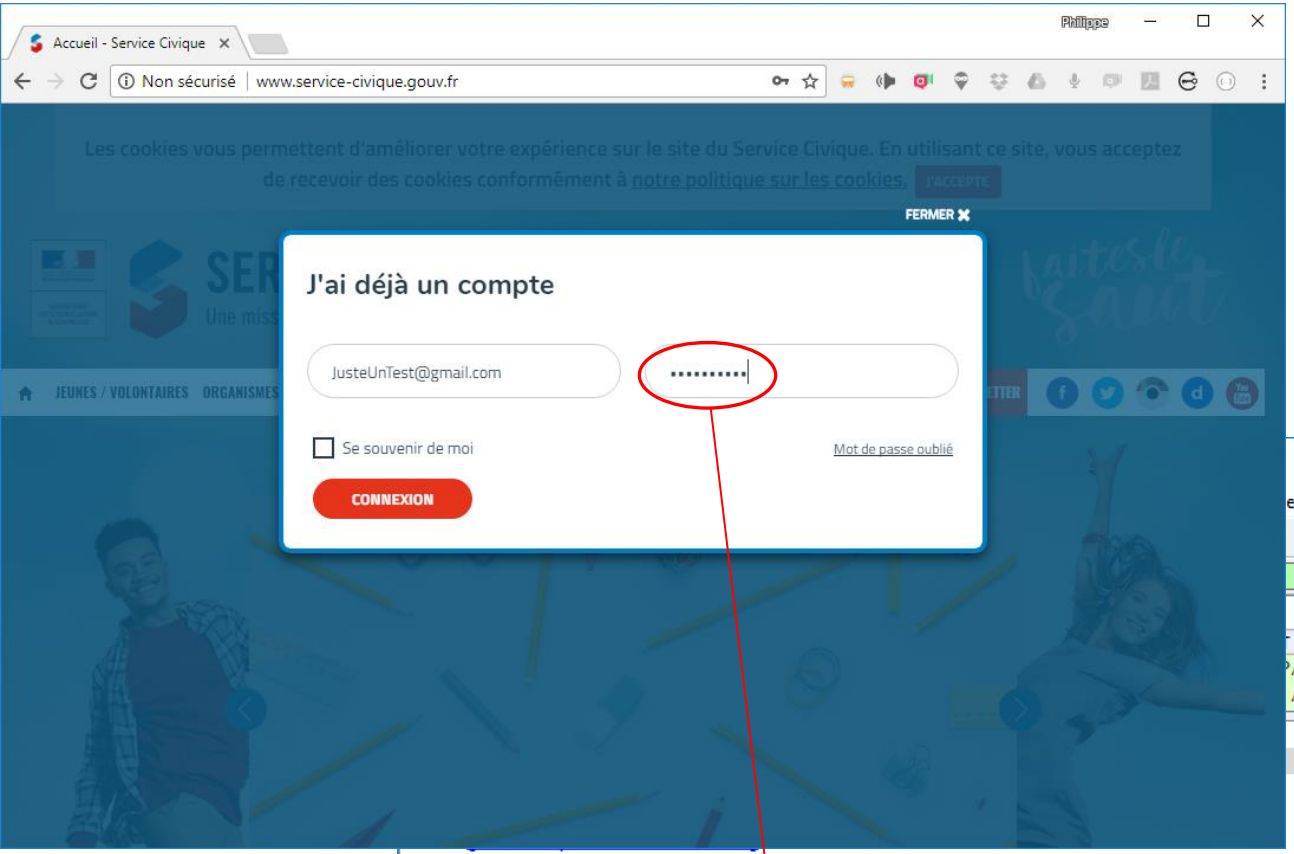
TCP "Transport Control Protocol" (transport)

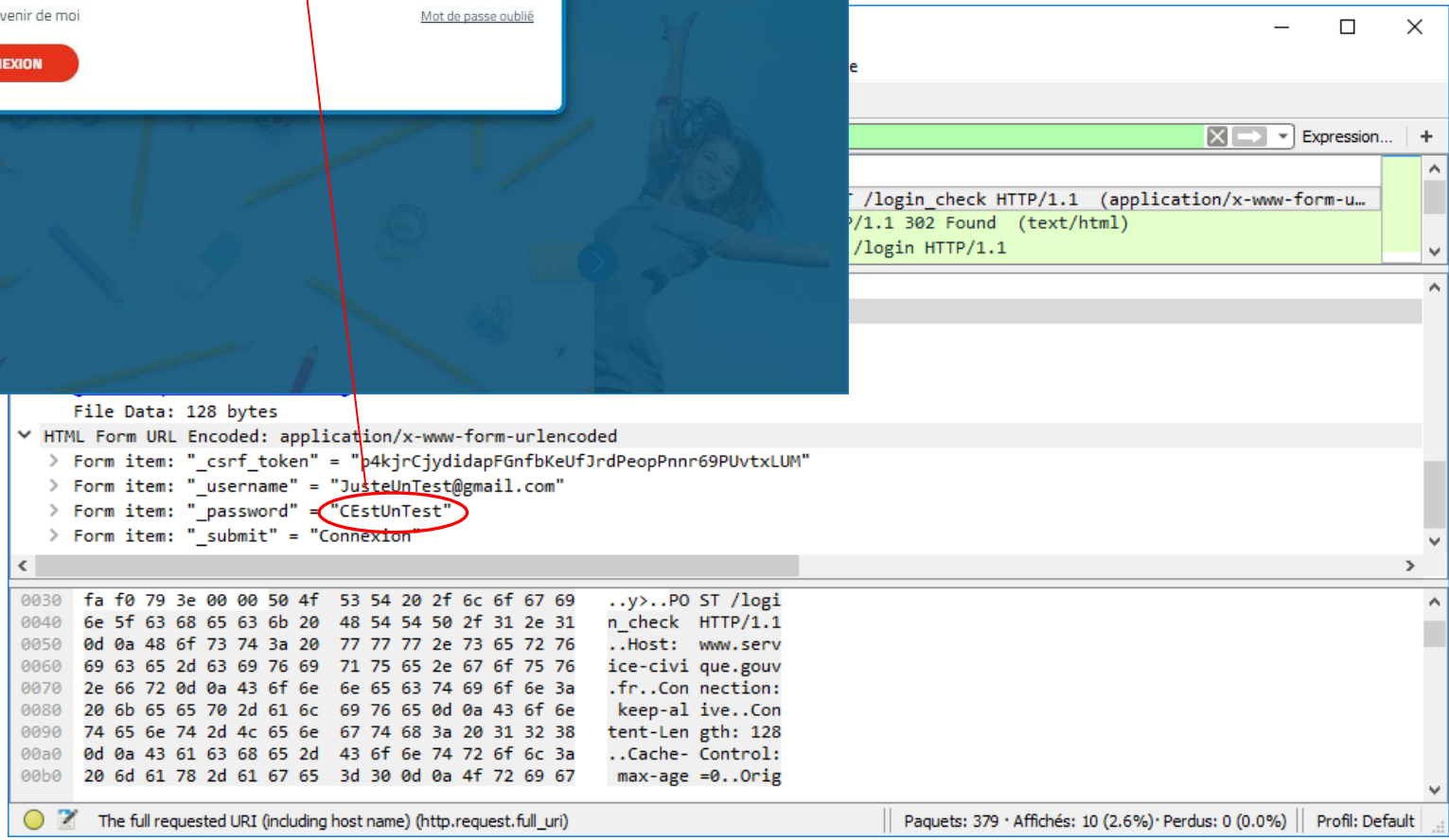
http://www.tcpipguide.com/free

internet n'a **PAS** été pensé pour la sécurité mais pour <u>le partage des données</u>

INTERNET ?


TYPES OF ATTACKS
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
EXPLOIT
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
PHISHING
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
HIJACKING
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
RECONNAISSANCE/DOS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
MAN-IN-THE-MIDDLE
2. Data Link
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring
SPOOFING
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
SNIFFING


Accueil - Service Civique
Philippe
Non sécurisé | www.service-civique.gouv.fr
Les cookies vous permettent d'améliorer votre expérience sur le site du Service Civique. En utilisant ce site, vous acceptez de recevoir des cookies conformément à notre politique sur les cookies.
J'ACCEPTE
FERMER
J'ai déjà un compte
JusteUnTest@gmail.com
Se souvenir de moi
Mot de passe oublié
CONNEXION
JEUNES / VOLONTAIRES
ORGANISMES


Expression...
/login_check HTTP/1.1 (application/x-www-form-u…
/1.1 302 Found (text/html)
/login HTTP/1.1
File Data: 128 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "_csrf_token" = "p4kjrCjydidapFGnfbKeUfJrdPeopPnnr69PUvtxLUM"
Form item: "_username" = "JusteUnTest@gmail.com"
Form item: "_password" = "CEstUnTest"
Form item: "_submit" = "Connexion"
0030 fa f0 79 3e 00 00 50 4f 53 54 20 2f 6c 6f 67 69 ..y>..PO ST /logi
0040 6e 5f 63 68 65 63 6b 20 48 54 54 50 2f 31 2e 31 n_check HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 73 65 72 76 ..Host: www.serv
0060 69 63 65 2d 63 69 76 69 71 75 65 2e 67 6f 75 76 ice-civi que.gouv
0070 2e 66 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a .fr..Con nection:
0080 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e keep-al ive..Con
0090 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 32 38 tent-Len gth: 128
00a0 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a ..Cache- Control:
00b0 20 6d 61 78 2d 61 67 65 3d 30 0d 0a 4f 72 69 67 max-age =0..Orig
The full requested URI (including host name) (http.request.full_uri)
Paquets: 379 · Affichés: 10 (2.6%) · Perdus: 0 (0.0%)
Profil: Default

ÇA A L'AIR SIMPLE …

Beaucoup d'attaques sont liées à internet (devenu **LE** réseau mondial qui relie **TOUT** – les gens, les transports, …)

Les utilisateurs sont souvent le point de départ … ou l'objectif final !

Pourquoi ?

- Pour vous nuire (diffamer, nuire à votre commerce)

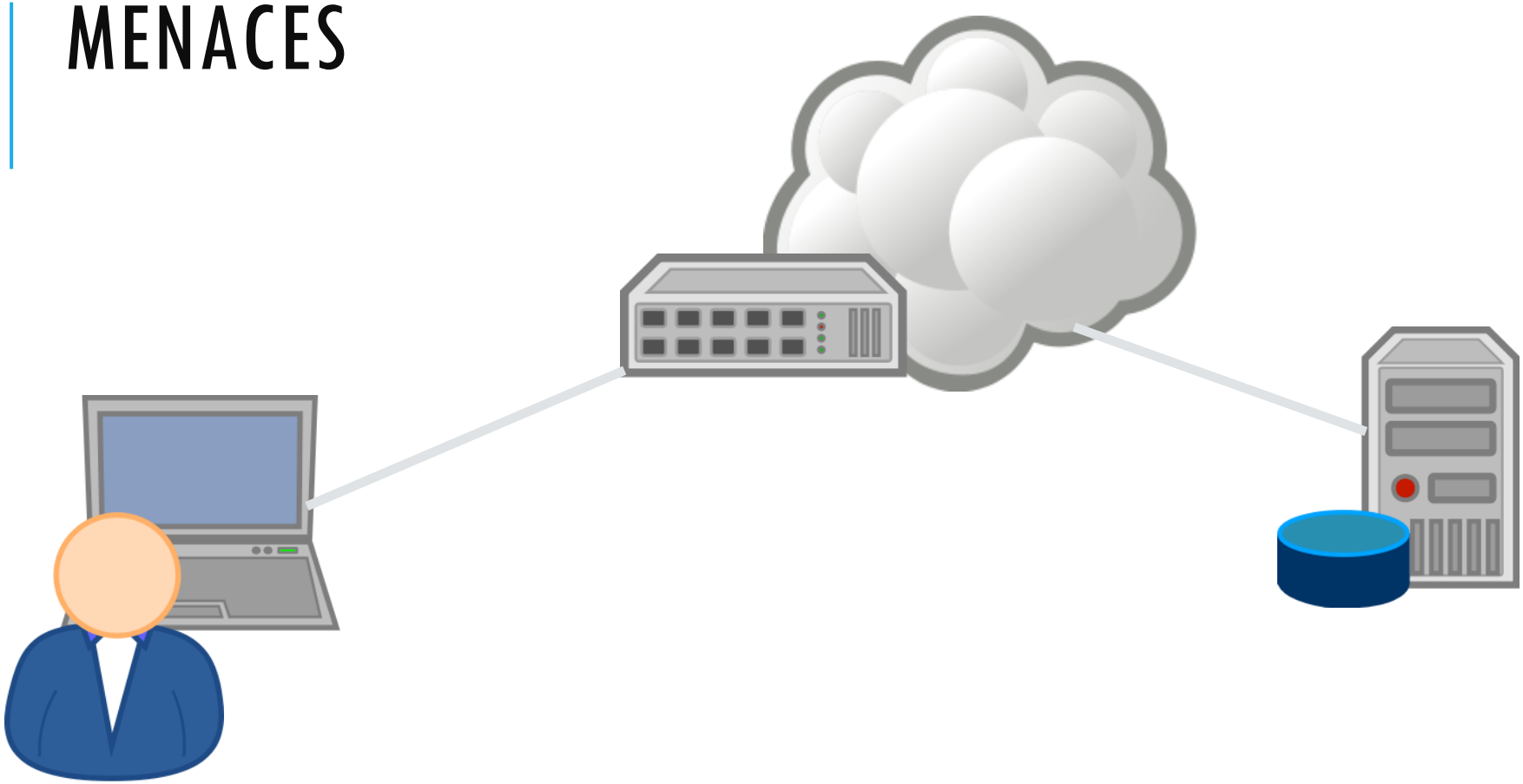
- Voler votre argent !

D'OÙ VIENNENT LES PROBLÈMES ?

Beaucoup de « **fantasmes** »

La plupart des attaques sont simples et sont effectuées par des « *script kiddies* » (des gens qui ne connaissent pas grand-chose à l'informatique voire des enfants)

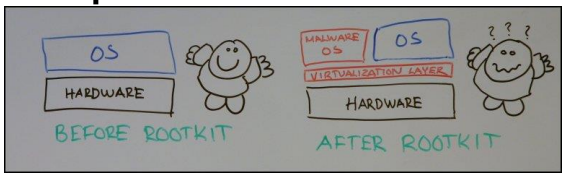
MENACES



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

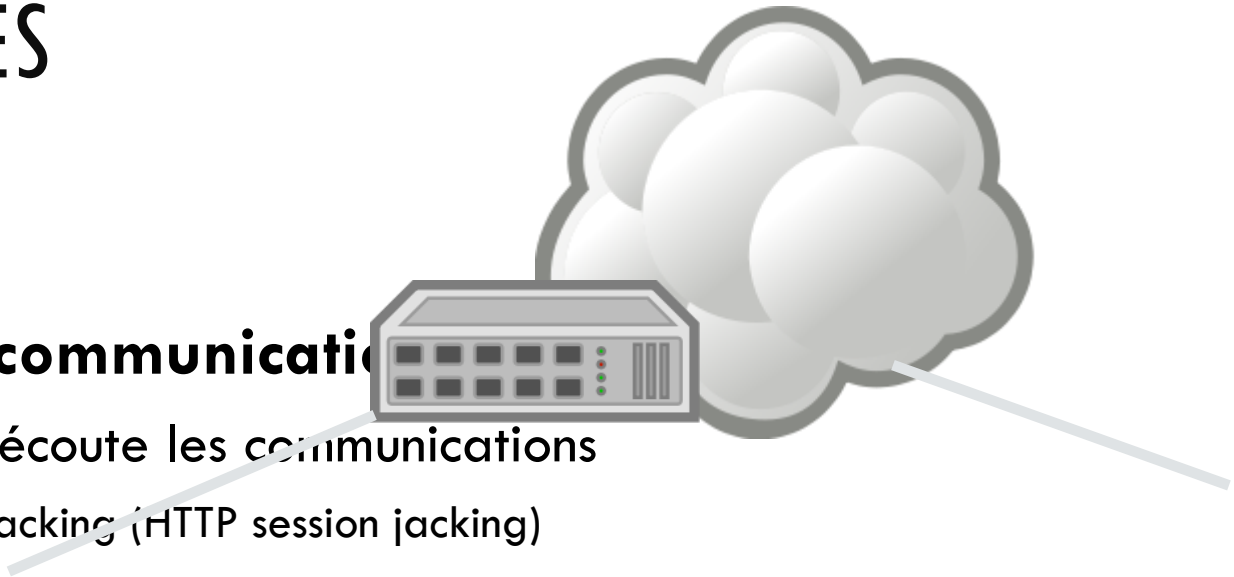
MENACES

- **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, bootkits, …
    - Attaque de type « cheval de Troie »
    - Ou via les « objets IoT » (Ex. de 未来)

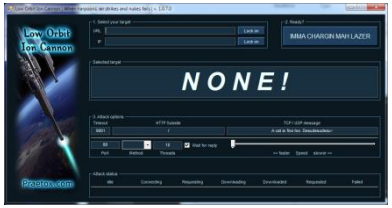


http://www.f-secure.com/weblog/archives/archive-032006.html
http://hackaday.com/2011/06/28/teensy-avrs-used-in-penetration-testing/

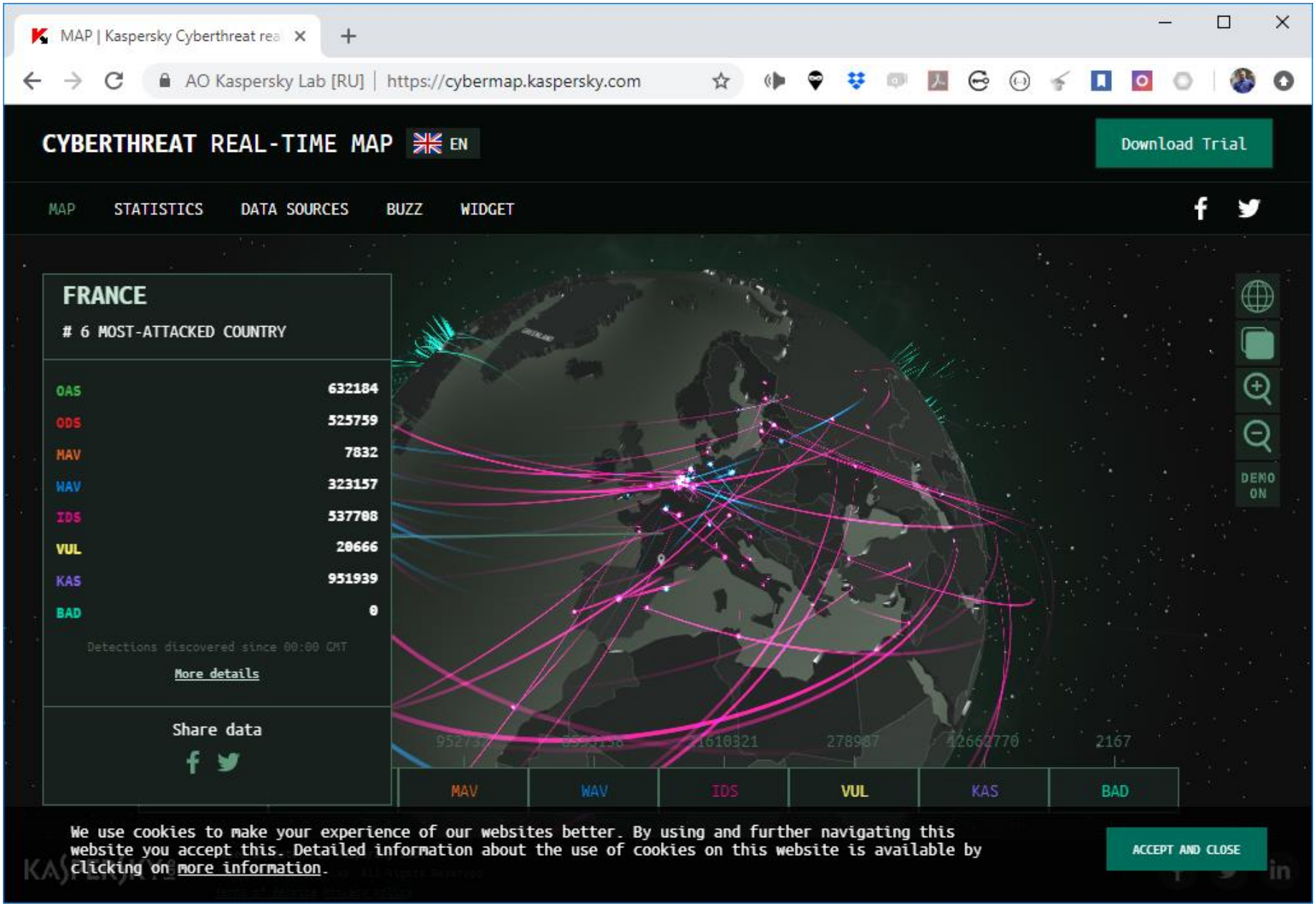
MENACES



- **sur la communicati**
  - Le pirate écoute les communications
    - Ex : sidejacking (HTTP session jacking)
  - Détourne les communications en se faisant passer pour un autre
    - Ex : Fake hotspot, ARP Poisoning, …
  - « Attaque » des serveurs en le saturant de demandes
    - Ex : Déni de Service Distribué (DDoS)



http://sourceforge.net/projects/loic
https://map.httpcs.com/


MAP | Kaspersky Cyberthreat rea
AO Kaspersky Lab [RU] | https://cybermap.kaspersky.com
CYBERTHREAT REAL-TIME MAP
EN
Download Trial
MAP
STATISTICS
DATA SOURCES
BUZZ
WIDGET
FRANCE
6 MOST-ATTACKED COUNTRY
OAS 632184
ODS 525759
MAV 7832
WAV 323157
IDS 537708
VUL 20666
KAS 951939
BAD 0
Detections discovered since 00:00 GMT
More details
Share data
DEMO ON
MAV
WAV
IDS
VUL
KAS
BAD
We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.
ACCEPT AND CLOSE

MENACES

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

EXTRAITS . . .

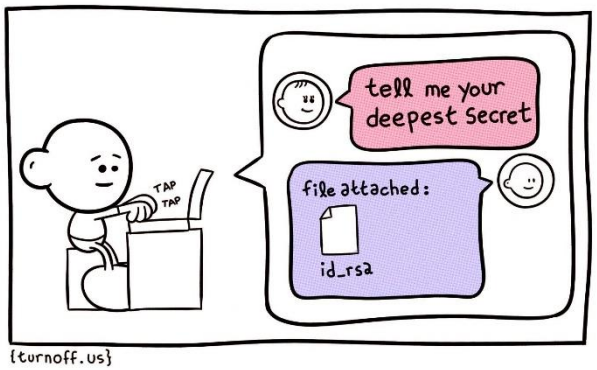
---**Question** : **Décrivez nous brièvement l'infrastructure réseau du laboratoire et le fonctionnement de l'adressage des Ips publiques au sein de celui ci ?**
---Réponse : Le CNRS a un réseau de classe B, ce qui signifie qu'il bénéficie d'une plage d'adresses Ips 157.136.0.0/16, soit plus de 65000 adresses Ips publiques routables sur Internet. Dans ce cadre, le laboratoire bénéficie de 2000 adresses Ips publiques sur la plage 157.136.63.0/24.---
---Le serveur virtuel utilise une de ces adresses Ips publiques du laboratoire.
---Concernant les logs, tout est centralisé à la délégation régionale.---
---**Question** : **Pouvez vous nous détailler les fonctions de ce serveur ?**.---
---Réponse : Ce serveur virtuel est principalement dédié au jeu multijoueur *Call of Duty*. Il s'agit d'un serveur que j'ai personnellement installé pour jouer aux heures de pauses avec mes collègues. Ce serveur était ouvert sur Internet pour permettre d'accueillir d'autres joueurs.---
---Ce serveur avait également des fonctions de récupération de données et quelques logiciels étaient installés.---
---Concernant *Call of Duty*, plusieurs instances étaient en fonction simultanément pour permettre de jouer à différents « *modes* » du jeu.
---Sur ce serveur, il y avait également plusieurs autres serveurs de jeux : *Quake 3* mais qui ne tournait pas, *Minecraft*, *Unreal Tournament 2003*…
---**Question** : **Quelles sont les caractéristiques techniques de ce serveur virtuel ?** ---
---Réponse : Le serveur virtuel est un Windows Server 2008 R2. Il tournait sous *Vmware* et était sur ma machine hôte *Windows 7*. Physiquement ce serveur était dans mon bureau et j'en avais l'administration exclusive.---
---A l'origine, j'ai monté ce serveur virtuel chez moi que j'ai importé par la suite pour l'implémenter au bureau.---
---L'accès sur cette machine se fait via le compte « *w2k8r2* » avec le mot de passe associé « *azerty* ». Il s'agit d'un compte administrateur.---
---**Question** : **Avez vous constaté un fonctionnement anormal de celui ci en particulier au courant du mois d'octobre ?**.---
---Réponse : J'ai effectivement constaté au cours du mois d'octobre qu'il y

SCSP
SEASONED CYBER SECURITY PROFESSIONALS

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

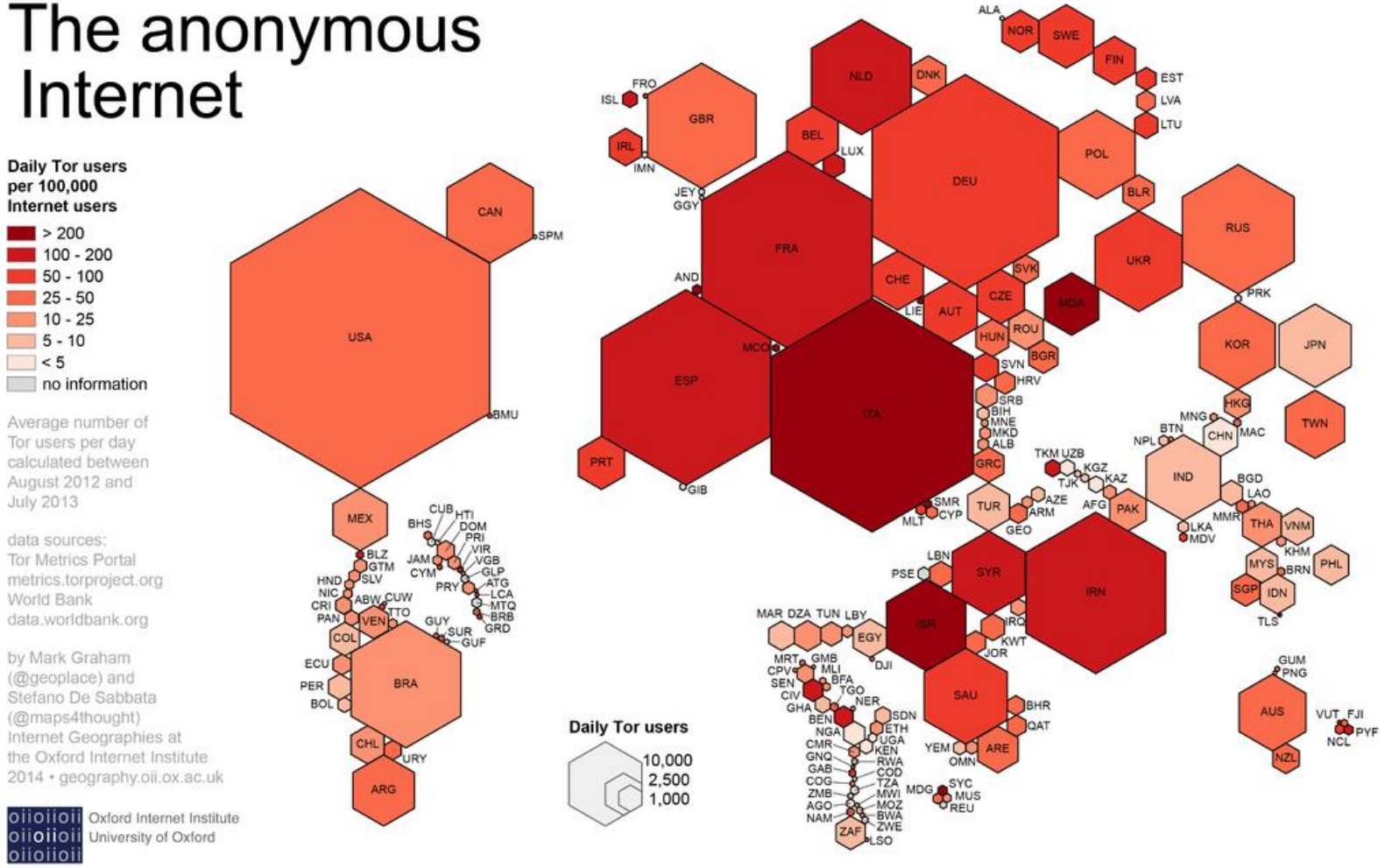
EN RÉSUMÉ …



- Des menaces diverses et finalement peu issue de la technologie
- **L'usage** est au cœur des problèmes
- Comprendre « *comment ça marche* » limite aussi les problèmes !

TOR

The anonymous Internet



TOR ET NOUVEAU MARCHÉ

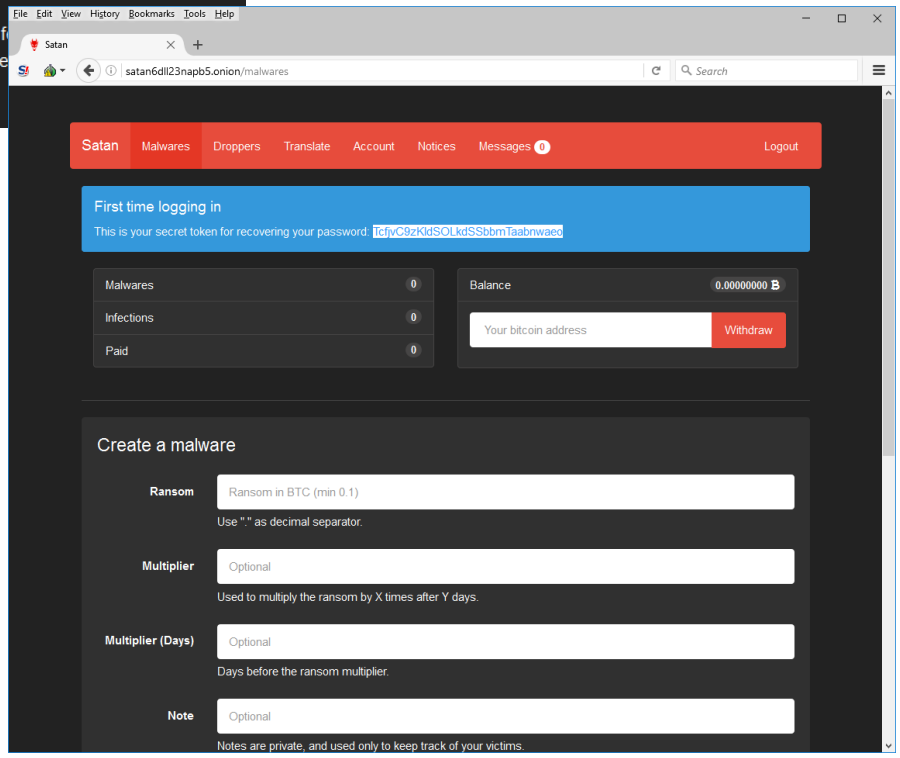
What is Satan?

Apart from the mythological creature, Satan is a ransomware, a malicious software that once opened in a Windows system, encrypts all the files, and demands a ransom for the decryption tools.

How to make money with Satan?

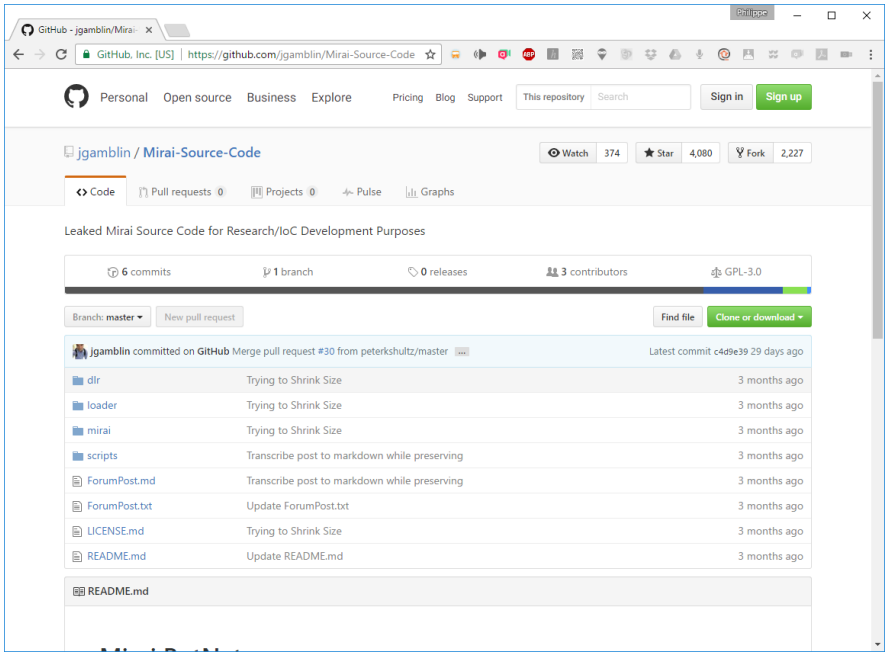
First of all, you'll need to sign up. Once you've sign up, you'll have to log in to your account, create a new virus and download it. Once you've downloaded your newly created virus, you're ready to start infecting people.

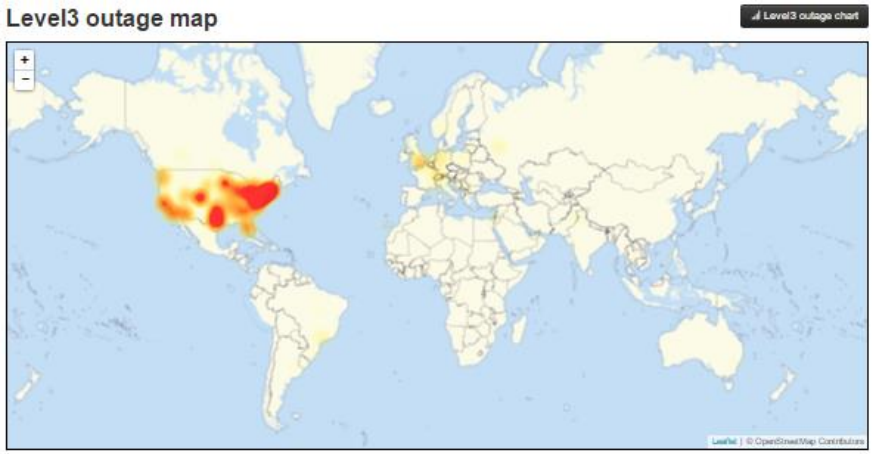
Now, the most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will keep a 30% f
specified a 1 BTC ransom, you will get 0.7 BTC and we will get 0.3 BTC. The fee will become lower depending on the
payments you have.



MIRAI BOTNET - 未来

https://github.com/jgamblin/Mirai-Source-Code

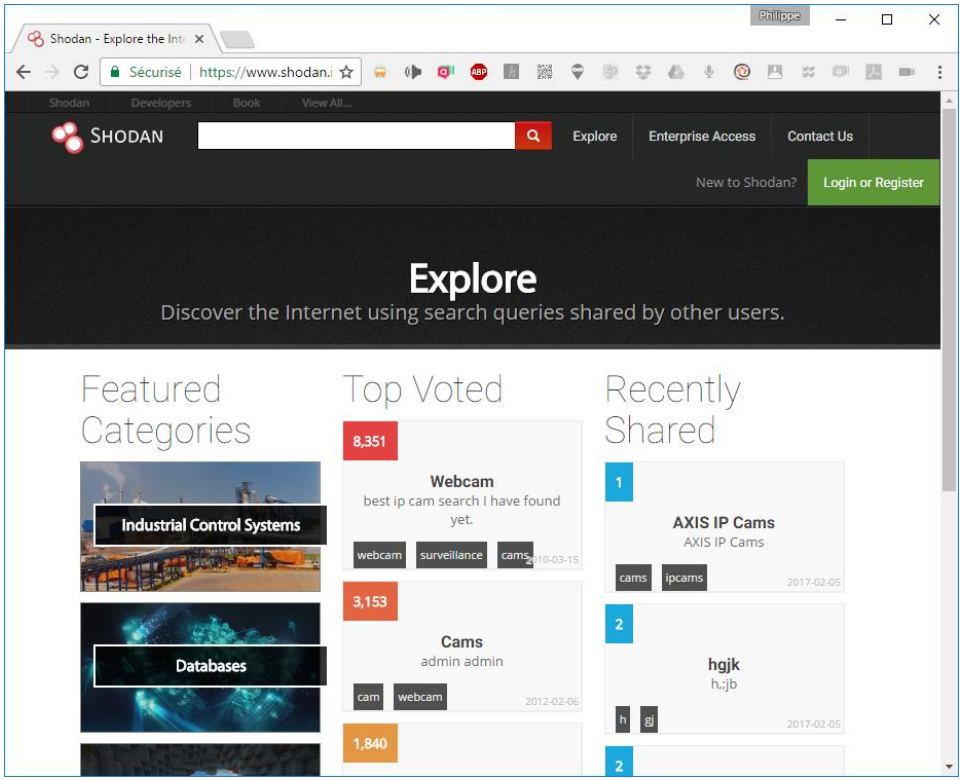


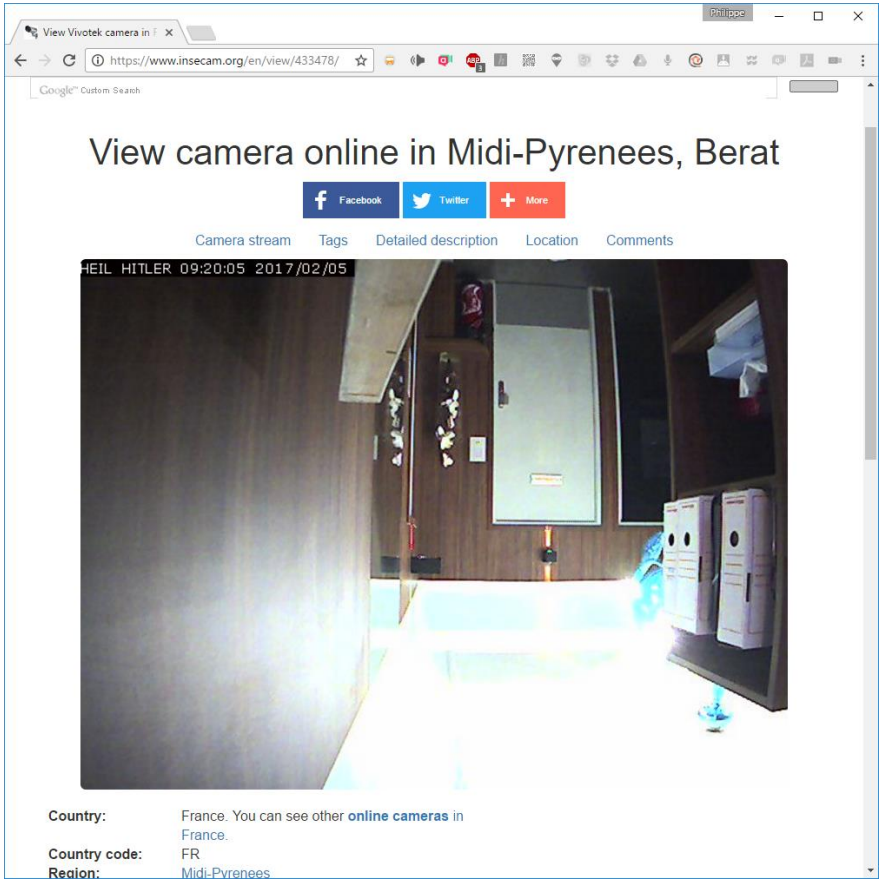


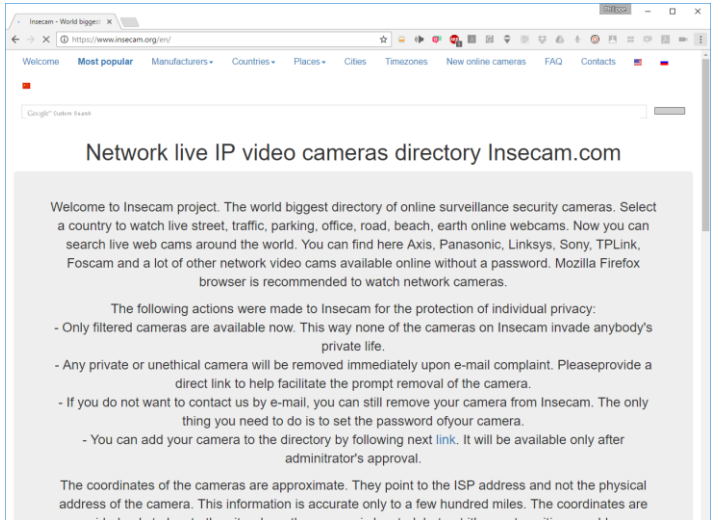
MOTEURS D'OBJETS

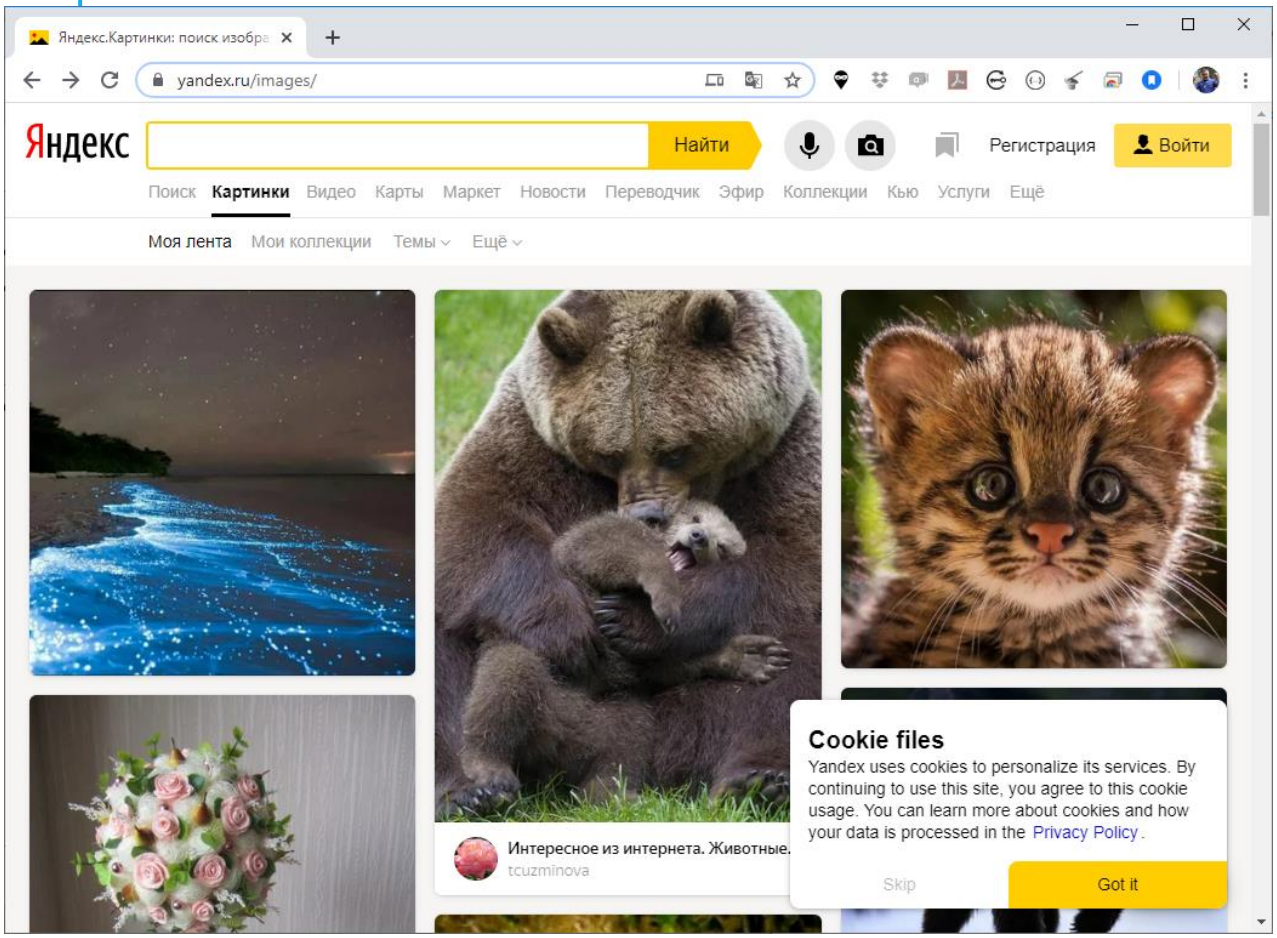
https://www.insecam.org

https://www.shodan.io









https://yandex.ru/images/