



# Comprendre la Sécurité

## Menaces – Nouveaux risques sur Internet

## Les Enjeux et les Composants

# Plan de l'exposé

- 1 Cybercriminalité : Menaces & Tendances
- 2 Sécurité des réseaux IP
- 3 TCP/IP – Composants de sécurité
- 4 Autres composants de sécurité



# 1 Cybercriminalité



# Sujets abordés

La sécurité : Pourquoi ?

Les acteurs en présence

Présentations d'études réalisées par divers organismes

Évolution de la mode des attaques sur l'Internet

Évolution du piratage et futur de la sécurité sur Internet la partie

Quelques mots sur Internet, origine et évolutions

Origine des failles, cycle de vie d'une vulnérabilité

Ecosystème, Risques et menaces : Ex. de sites Web hackés

Organigramme typique d'une attaque, outils

Quelques mots sur l'observation des menaces

# Définitions



ANSSI

Agence nationale  
de la sécurité  
des systèmes d'information



- CyberSécurité

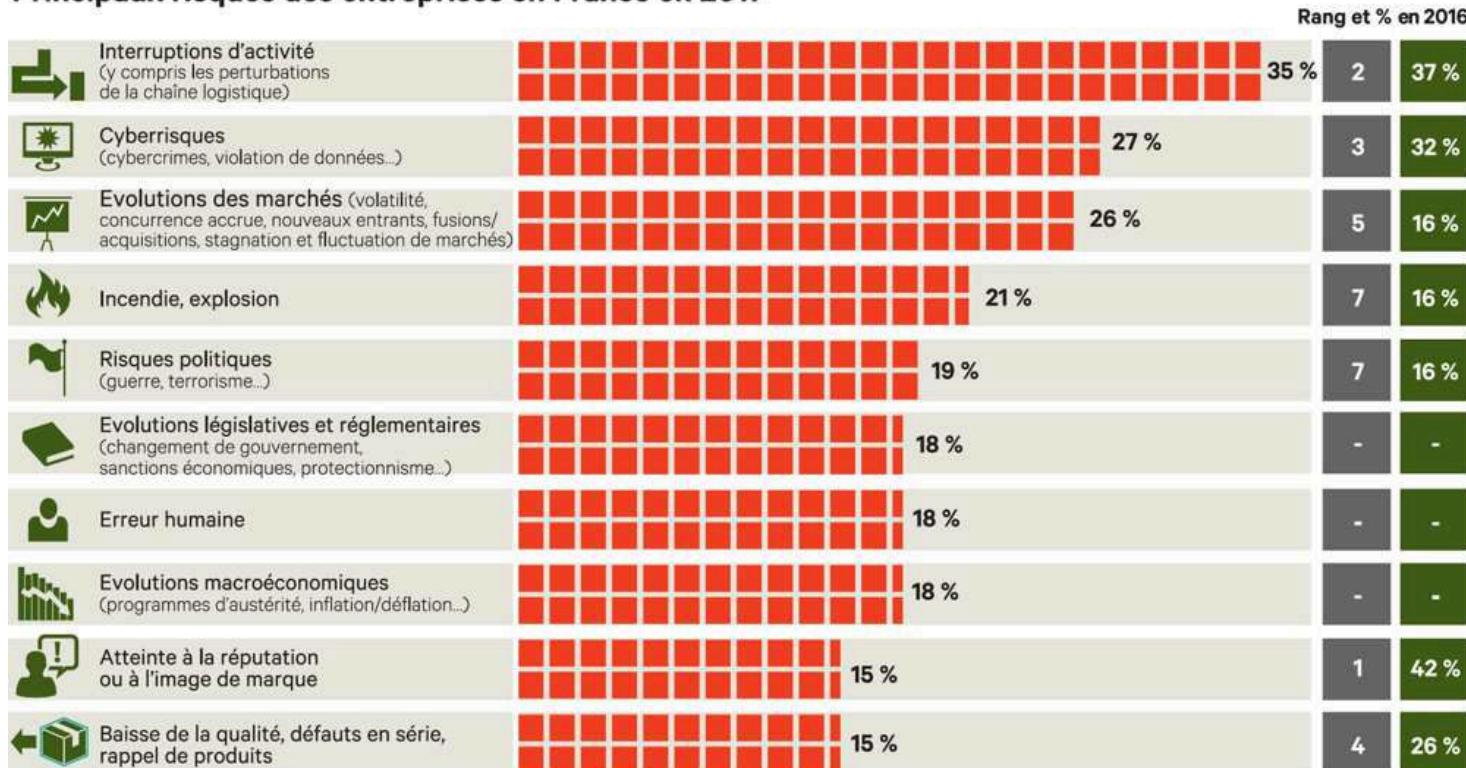
- Etat recherché pour un **système d'information** lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre **la disponibilité, l'intégrité ou la confidentialité** des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.
  - fait appel à des techniques de **sécurité des systèmes d'information** et s'appuie sur la lutte contre la cybercriminalité et sur la **mise en place d'une cyberdéfense**.

- CyberDéfense

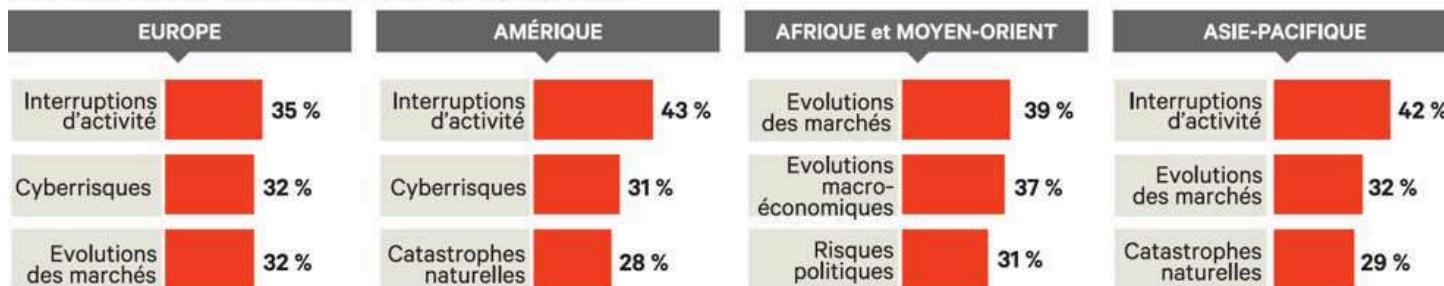
- Ensemble des mesures **techniques et non techniques** permettant la défense dans le cyberspace les systèmes d'information jugés essentiels.

# Cyberattaques, réputation : l'ère de l'aléatoire

## Principaux risques des entreprises en France en 2017



## Le Top 3 des risques par zone géographique



# The Cyclades computer network

- Projet expérimental français ayant pour but de créer un réseau global de télécommunication utilisant la commutation de paquets. Crée en 1971, conçu par Louis Pouzin, il fut abandonné en 1978. (Minitel, Transpac, CGE, Thomson,...)
- Ses concepts ont influencé les travaux de développement de l'Internet en inspirant sa suite de protocoles [TCP/IP]



▪ Louis Pouzin

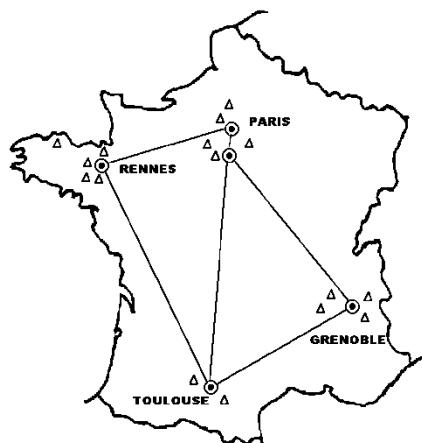


Fig. 1. CYCLADES topology

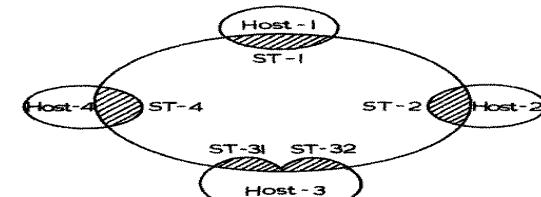


Fig. 2 CYCLADES Model

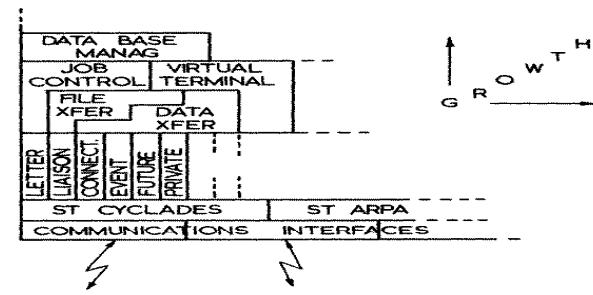


Fig. 3 CYCLADES Architecture

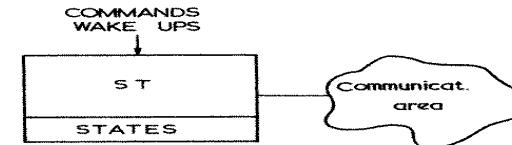
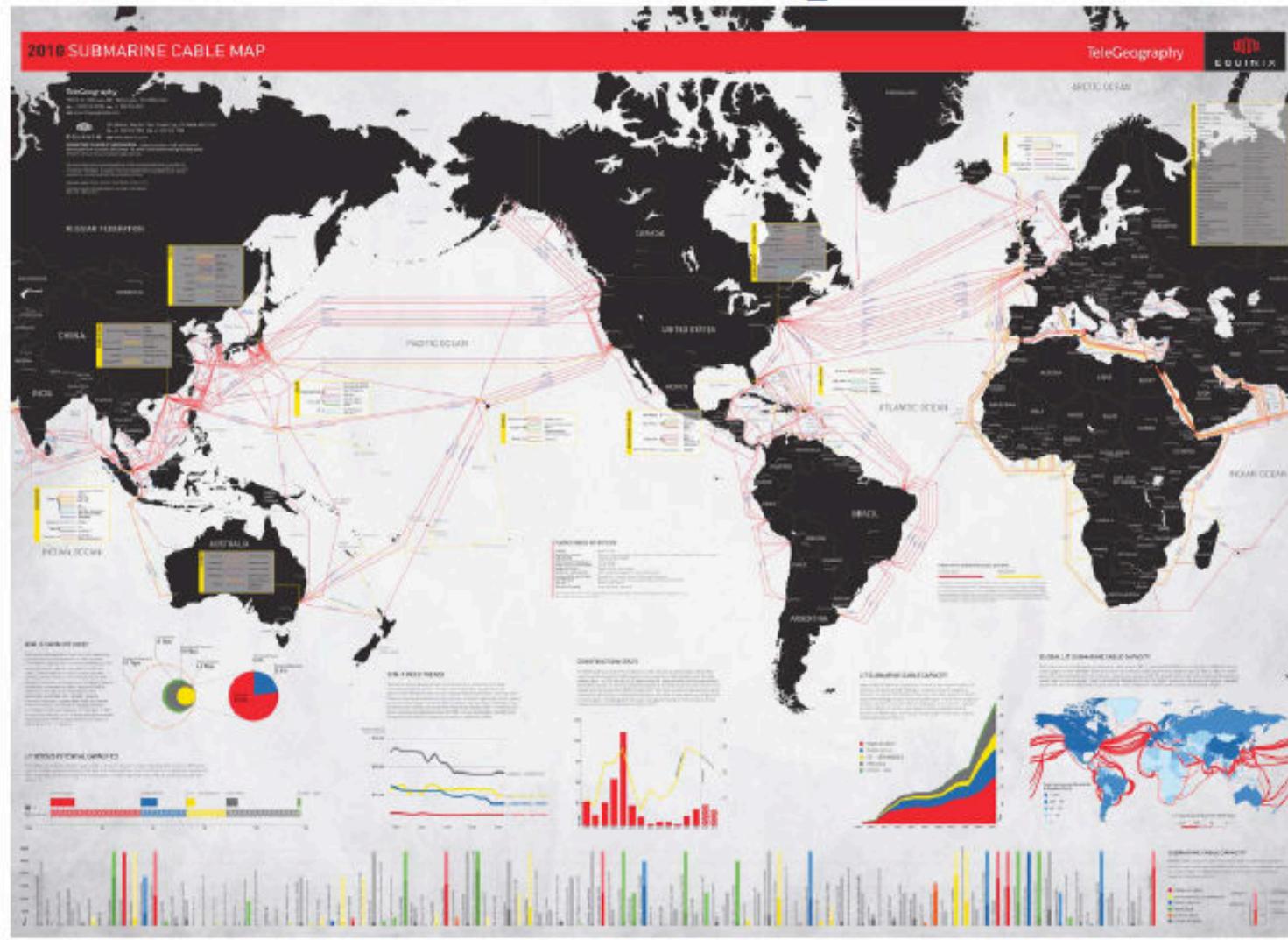


Fig. 4 Transfer station model

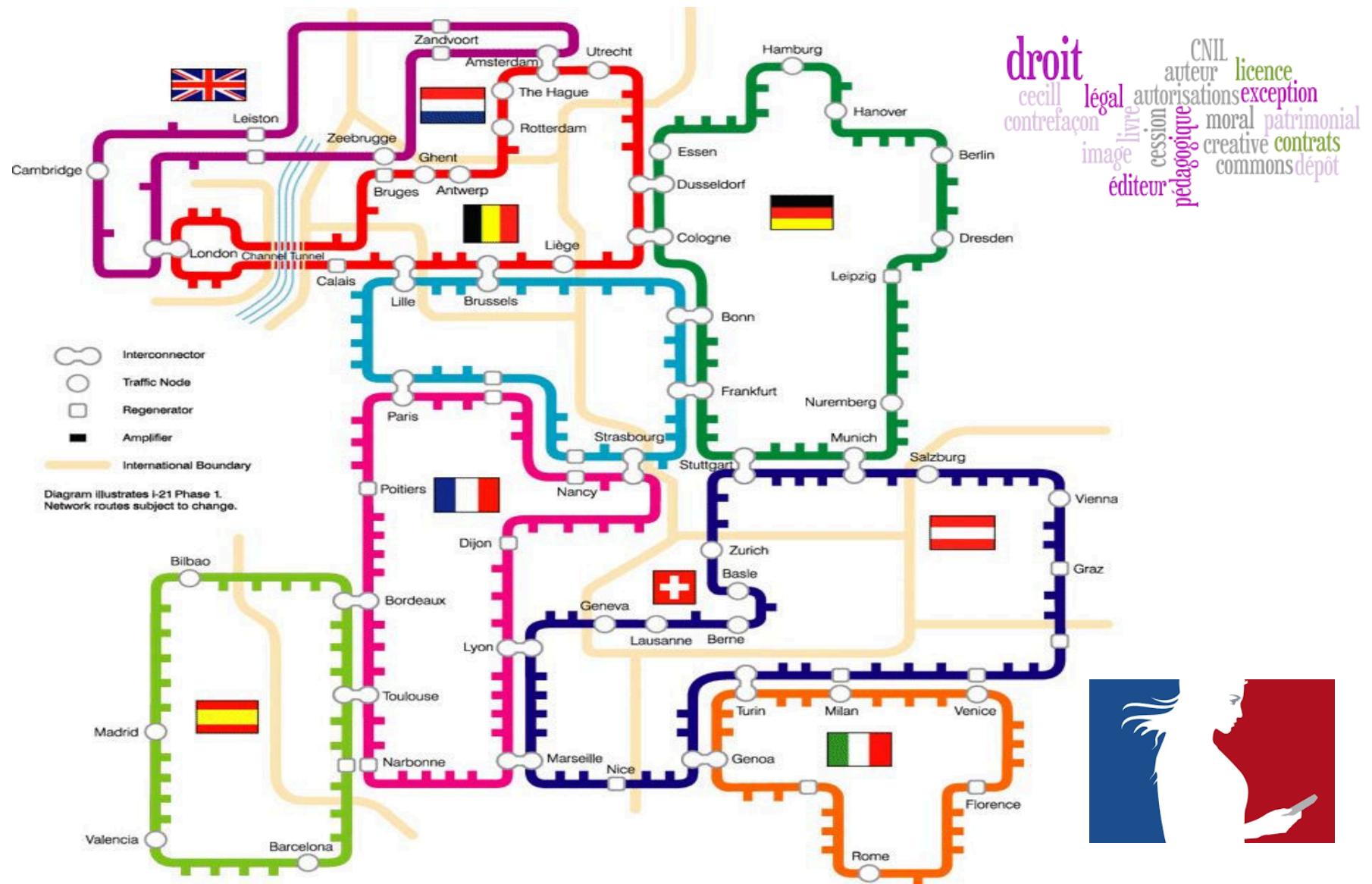


Fig. 5 Transfer station components

# Un grand espace disponible ...



# Internet : la résilience et droit

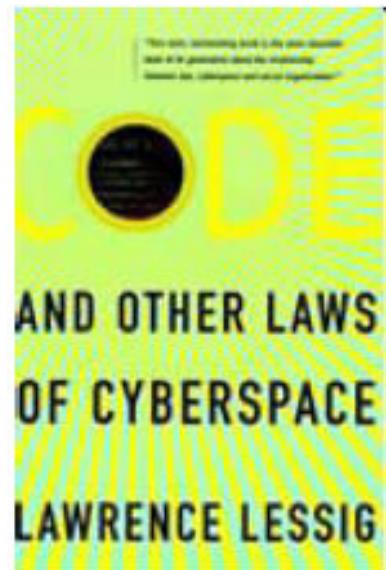


# ...pourtant si fragile



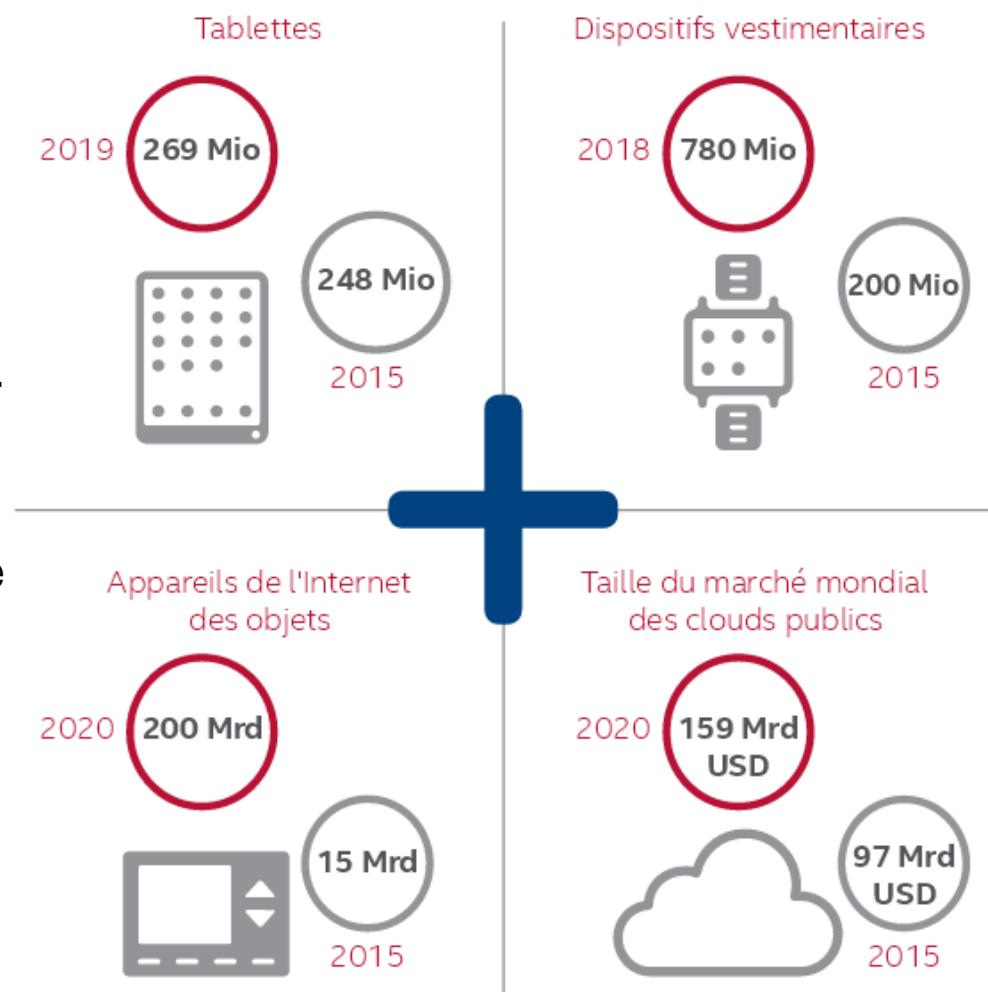
PROJET DE LOI DE

## PROGRAMMATION MILITAIRE 2014 / 2019



## Nouveaux types de terminaux

- Les nouveaux gadgets arrivent vite à maturité
- Un public de plus en plus nombreux sur les segments des applications grand public, industrielles et métier.
- Certains de ces appareils de pointe connectés à l'Internet des objets (IoT) disposent de suffisamment d'utilisateurs pour susciter l'intérêt des **cyberpirates**, et d'autres suivrons.



Source : McAfee Labs, 2015

# Le connectée en chiffres avec l'IoT

- 2015-20 estimation de **2 Md** d'appareils intelligents en France (GFK – déc 2015)



**27%** de toutes les données seront générées par les objets connectés en **2020**. <sup>(2)</sup>



**7 100 milliards** de dollars c'est le marché mondial des solutions IoT en **2020**. <sup>(1)</sup>

**15%** de tous les « objets » seront connectés en **2020**. <sup>(2)</sup>

**3 fois** plus rapide

La croissance des dépenses d'IoT est 3 fois plus rapide que sur les marchés TIC classiques. <sup>(2)</sup>

**50 milliards** d'« objets » seront connectés à Internet en **2020**. <sup>(3)</sup>

**20 milliards** de dollars En trois ans, le marché de la RFID a été multiplié par 4. <sup>(4)</sup>

— La protection des données sera le défi majeur —



**80%** des appareils connectés à Internet présentent de potentielles failles de sécurité. <sup>(10)</sup>

Sources

(1) IDC - The Internet of Things Moves Beyond the Buzz - 2014

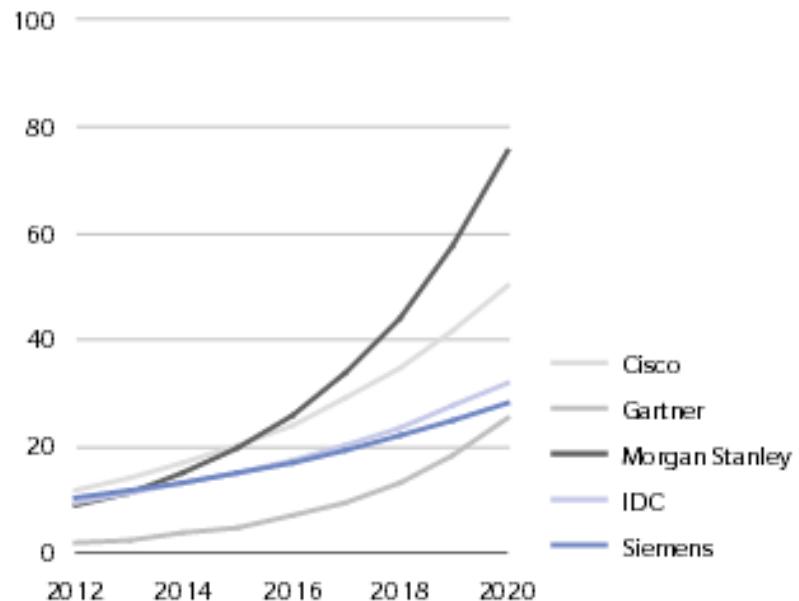
(2) IDC - The Digital Universe of Opportunity - 2014

(3) Cisco - The Internet of Things - Cisco Visualization

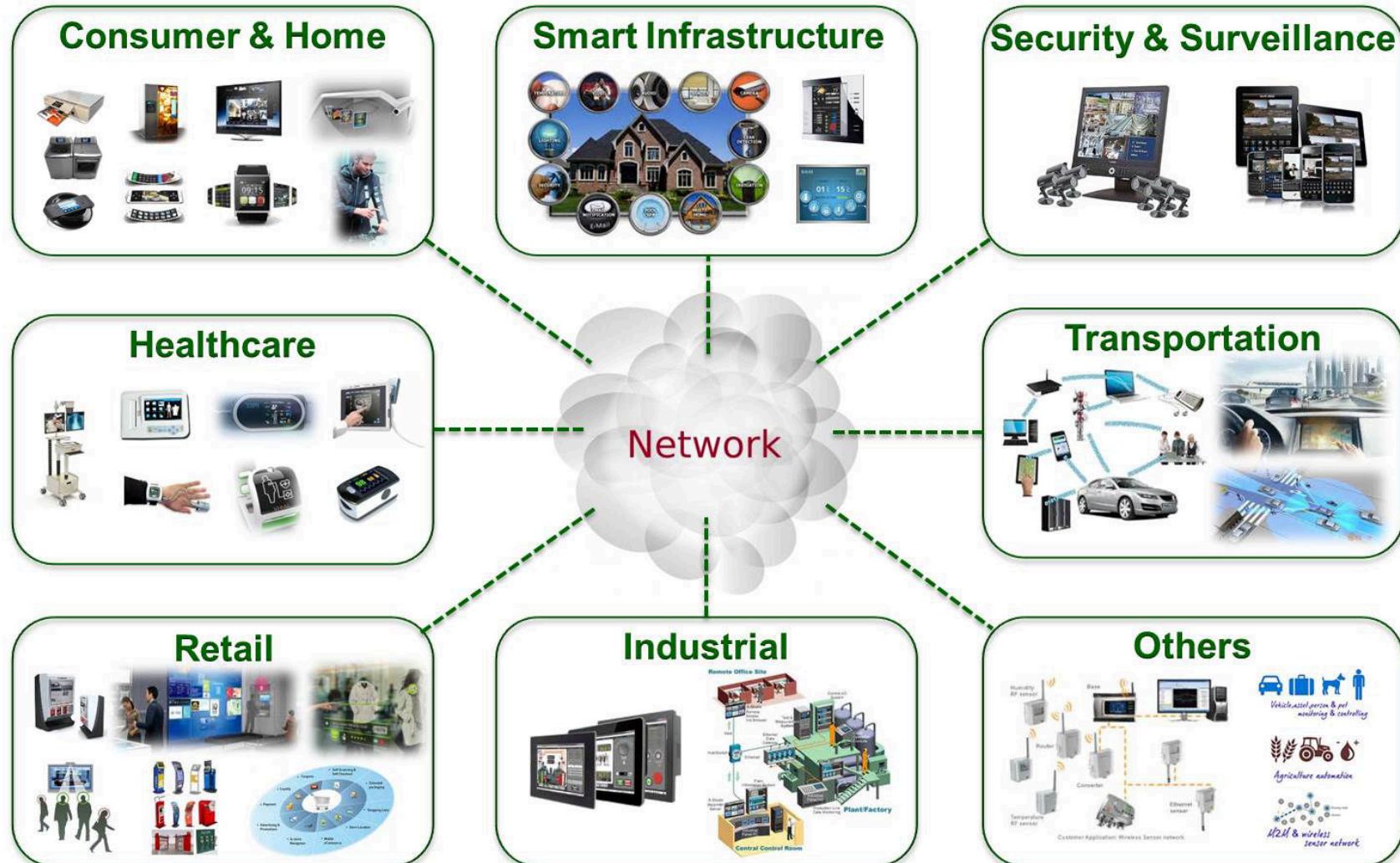
(4) SOGETI - Things Internet of Business Opportunities - 2013

(10) HP - Internet of Things Research Study 2014

NOMBRE D'OBJETS CONNECTÉS EN MILLIARDS (2012-2020)



# IoT : Répartition des services en 2020



Vivante and the Vivante logo are trademarks of Vivante Corporation. All other product, image or service names in this presentation are the property of their respective owners. © 2013 Vivante Corporation

# A quoi doit-on s'attendre en 2018 ?

- Augmentation de l'implication de la technologie dans les délits
  - Facilitation de la recherche d'objets vulnérables et de l'exploitation des failles
  - Possibilité d'atteindre physiquement une entreprise, une habitation, une personne
- Les jouets connectés : Barbie et Vtech(et bientôt BB8 ?)



- Le domicile connecté :télévision, babymonitor, serrure, prise électrique et réfrigérateur



- pompes à insuline, fusils de sniper, avion ?



# Evolution 2.0 ?



**OWASP**

The Open Web Application Security Project

Communauté en ligne travaillant sur la sécurité des applications [Web](#) - 2001



[Page](#) [Discussion](#)

[Read](#) [View source](#) [View history](#) [Search](#)

## OWASP Internet of Things Top Ten Project

[Main](#) [OWASP Internet of Things Top 10 for 2014](#) [Talks](#) [In the News](#) [Community](#) [Manufacturers](#) [Developers](#) [Consumers](#)

[Project Details](#)



The OWASP Internet of Things Top 10 - 2014 is as follows:

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

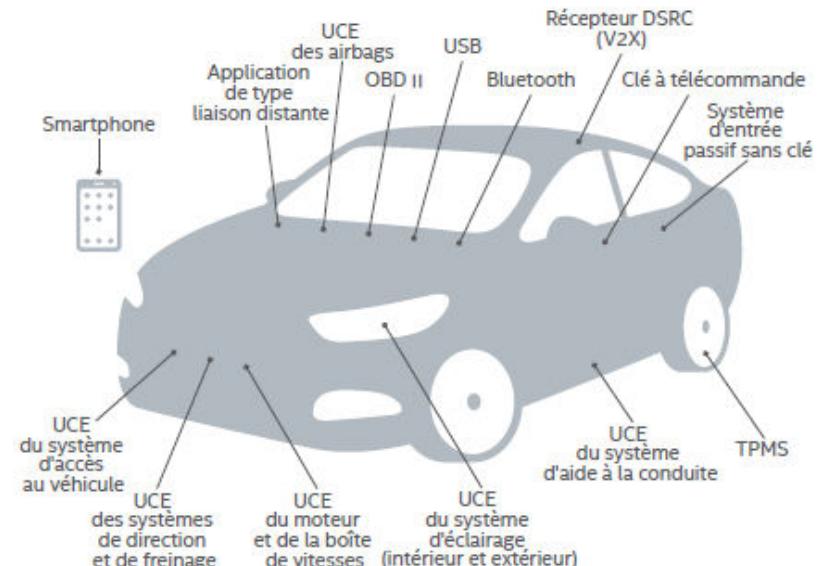
[Home](#)  
[About OWASP](#)  
[Acknowledgements](#)  
[Advertising](#)  
[AppSec Events](#)  
[Books](#)  
[Brand Resources](#)  
[Chapters](#)  
[Donate to OWASP](#)  
[Downloads](#)  
[Funding](#)  
[Governance](#)  
[Initiatives](#)  
[Mailing Lists](#)  
[Membership](#)  
[Merchandise](#)  
[News](#)  
[Community portal](#)  
[Presentations](#)  
[Press](#)  
[Projects](#)  
[Video](#)  
[Volunteer](#)

▼ [Reference](#)  
[Activities](#)  
[Attacks](#)

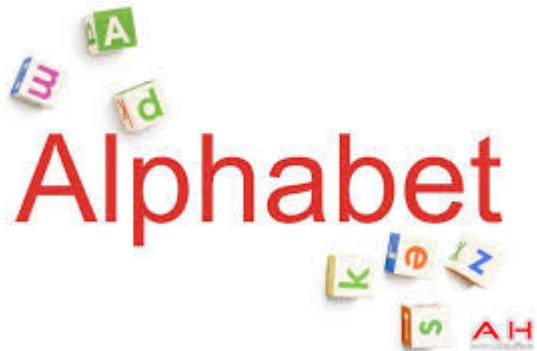
# Le hack de la voiture

- BMW fonction de déverrouillage à distance via le smartphone
- Analyse de sécurité des systèmes embarqués automobiles (QNX)
- La connexion fonctionne également au travers du module 3G/4G qui est intégré et **activé** par défaut
- Procédure, connexion entre le terminal mobile et les serveurs de BMW non **chiffré** et sans aucune **authentification**
- Correctif sur + deux millions de voitures (ConnectedDrive) du firmware en OTA
  - BMW, mais aussi Mini, et Rolls-Royce
- Conférence **Black Hat 2015**, les détails techniques du piratage de la Jeep Cherokee de Chrysler
- Prendre le contrôle à distance de la voiture:

Activer les essuies-glace, monter le volume radio, mais aussi actionner les freins, tourner le volant, couper le moteur



## Les cyberacteurs : hier et aujourd'hui



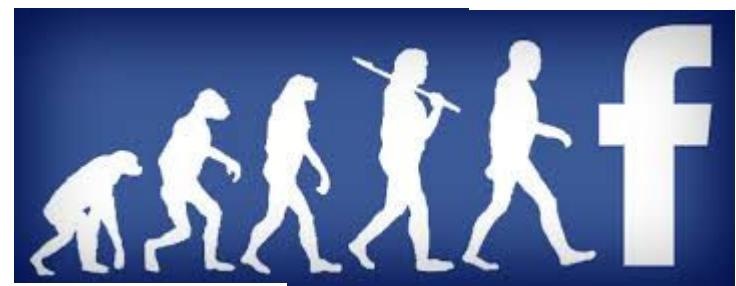
U B E R

**LE FIGARO.fr**

Le géant chinois qui fait trembler la planète télécoms

Haïk Cheiki (8 langages)  
20/06/2018 | Mis à jour : 10:11 | Commentaires : 27

A small image showing two women in red uniforms standing in front of a large red and white Huawei logo.



# Motivations et profils

---



**LUCRATIVE**  
Cybergangs  
Cybermercenaires  
Officines



**LUDIQUE**  
Adolescent désœuvré



**POLITIQUE**  
Hacktivistes  
Cyberpatriotes  
Cyberterroristes



**TECHNIQUE**  
Hacker



**MILITAIRE**  
Unités spécialisées



**PATHOS**  
Employé mécontent

# Opérations malveillantes

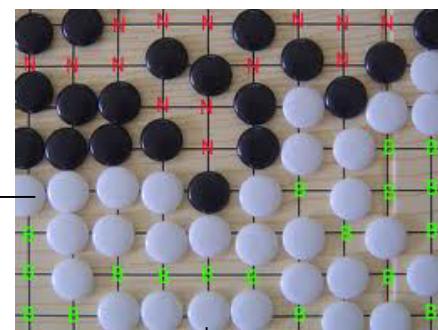
Espionnage



Agit-prop



Invasion



Sabotage

Fraude massive



Saturation

# Web profond - 90% du World Wide Web



- « DarkNet », « Deepnet », « Web invisible », ou le « Web caché », Internet non indexé
- Utilisation de bases de données dynamiques, ils sont dépourvues de liens hypertextes
- Google = +1 million de serveurs pour sans cesse crawler le web

# Les niveaux du web

## ❑ NIVEAU 0 : Le web commun

- Tout ce que vous pouvez trouver en utilisant un moteur de recherche comme Google.
- Ex de sites : Facebook, Google, Youtube, Twitter... Il se trouve en quelques secondes via l'ensemble des moteurs de recherche du globe

## ❑ NIVEAU 1 : Le web de surface

- le Web Surface est tout ce qu'un moteur de recherche peut trouver, il est toujours accessible avec un navigateur normal, ». Lui aussi est simple d'accès, mais on y croise des choses plus « underground » il peut contenir des sites sombres.
- Ex de sites : Reddit, Digg, jetable.org ... ou tout simplement des bases de données SQL

## ❑ NIVEAU 2 : Le « Bergie Web »

- le lien entre le « Web » et le « darkweb ». On y croisa par exemple The Pirate Bay Toujours, indexés, les sites du niveau 2 sont bien plus « underground » et contiennent des contenus légèrement malsains pour certains.
- Ex de sites : FTP, 4chan, sites gore, sites de « jailbait » (fausse pédopornographie)...(findbostonbombers)

## ❑ NIVEAU 3 : Le web profond

- tout ce qu'un moteur de recherche ne peut pas accéder, à partir d'ici les choses sérieuses commencent. Pour accéder à cette partie du web, vous devez avoir un proxy ou TOR. C'est le début du web profond : dans lequel se trouvent **plusieurs autres sous-niveaux**, ceux des markets et autosshops du Black Market (Alphabay, SilkRoad...).
- Ex : Pédopornographie « légère », hacking, informations secrètes...



[https://rationawiki.org/w/index.php?title=Dark\\_web&oldid=100000](https://rationawiki.org/w/index.php?title=Dark_web&oldid=100000)

# Les moteurs de recherches du web profond

- Exemple de Moteurs de recherche **DeepWeb** [accessible mais non indexée] :
  - La WWW Virtual Library <http://vlib.org/>
  - Yippy : <http://yippy.com/>
  - Surf wax : <http://lookahead.surfwax.com/>
  - IceRocket : <http://www.icerocket.com/>
  - Stumpedia : <http://www.stumpedia.com/>
  - Freebase : <https://www.firebaseio.com/>
  - TechDeepWeb : <http://techdeepweb.com/index.html>
- Exemple de Moteurs de recherche **DarkWeb** [utilisent l'Internet public, mais qui nécessitent des logiciels, des configurations ou des autorisations spécifiques à l'accès] :
  - .onion / pseudo TLD - caché anonyme via Tor, adresses ne sont pas des noms DNS réels, et ne sont pas dans la racine DNS Internet, mais avec le logiciel de proxy approprié installé, les programmes Internet tels que les navigateurs Web peuvent accéder à des sites avec des adresses .onion en envoyant la demande par l'intermédiaire du réseau de serveurs Tor.
  - Onion.City : <http://onion.link> (enabling search and global access to Tor's onionistes)
  - Not Evil : <https://hss3uro2hsxfogfq.onion.to/>
  - Memex Web profond Search Engine
- Métamoteurs : <http://c.asselin.free.fr/atmo/Metamoteurs.htm>

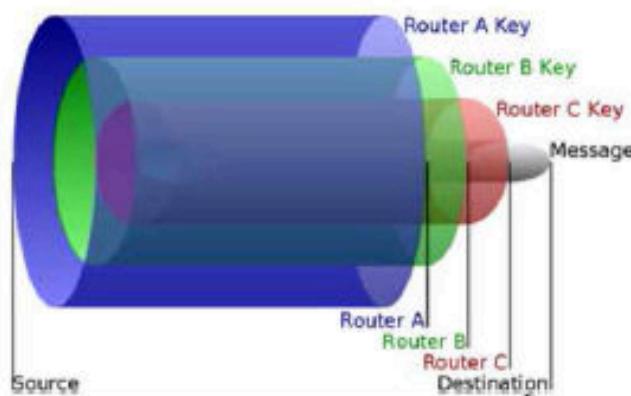


# Réseaux anonymes et réseaux publics



Share anonymously with your friends.  
Speak freely.

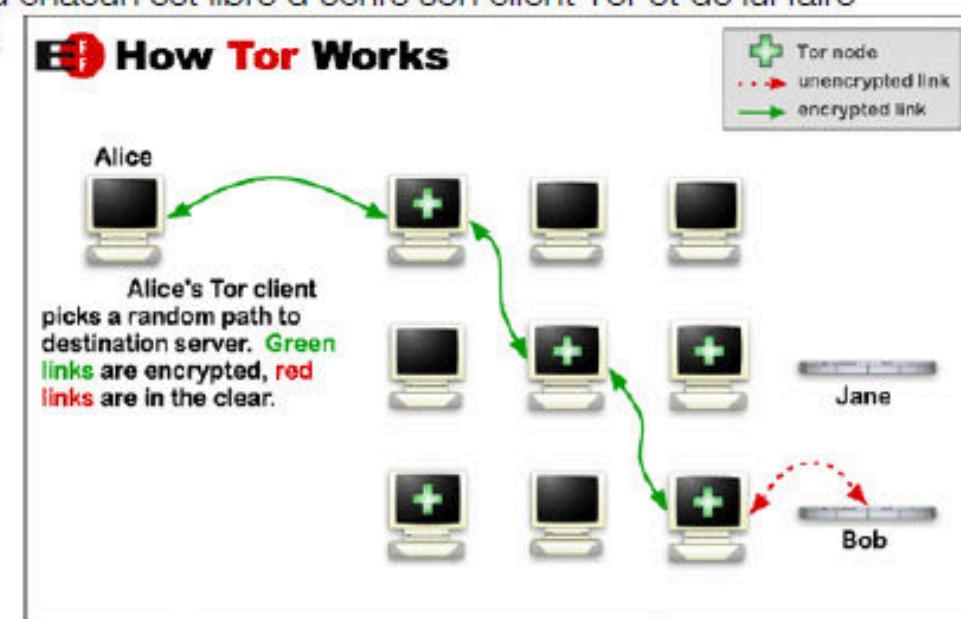
- Pour se déplacer sur le web parallèle, il n'est pas question de recourir aux **outils de recherche classiques**
- Ces derniers, normés, standardisés, n'indexent pas les contenus illicites et quand bien même ils le feraient, ils **conservent dans leurs logs et historiques**, l'ensemble des traces laissées par les requêtes des internautes
- Pour échanger, commercer, s'organiser et naviguer dans le web profond et réaliser des transactions sur le blackmarket, les Cybercriminels se sont dotés d'**outils spécifiques** et de **structures techniques** dédiées
  - **Les forums** du blackmarket fonctionnent comme les sites de petites annonces du Clear Web
  - **Proxy et VPN anonymes**, Deux techniques sont principalement utilisées pour masquer l'adresse IP de leur machine, VPN anonymes leur sont généralement privilégiées
  - **Tor** : le réseau décentralisé Tor répond lui aussi au besoin d'anonymisation recherché par les cybercriminels
  - **Serveurs bulletproof** : proposent des hébergements **sans prendre en considération le type de données** qui seront stockées ou l'usage qui en sera fait



## ToR : The Onion Router



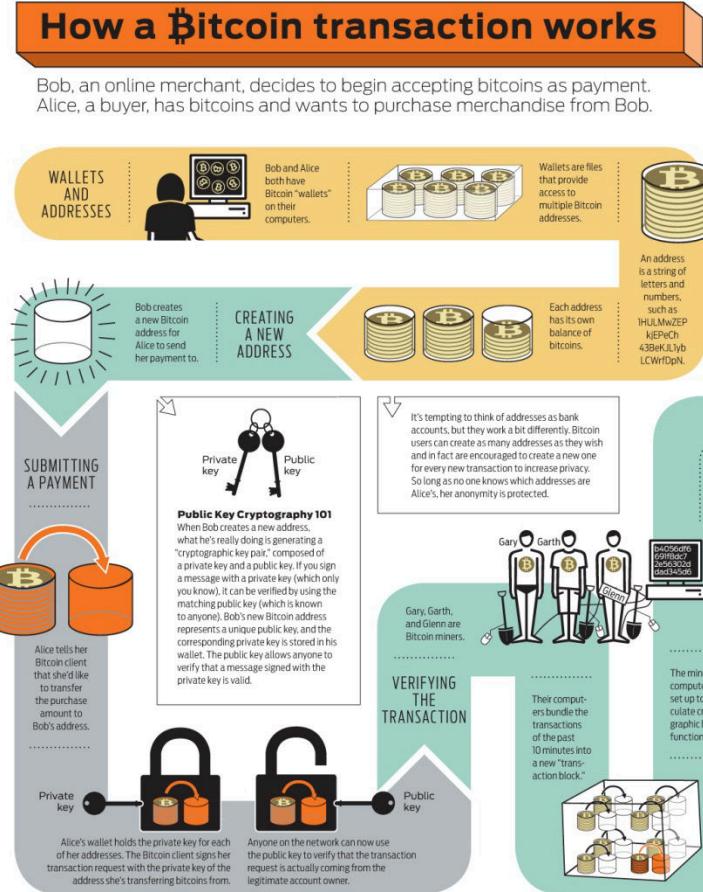
- Un client de navigation anonyme, qui permet à ses utilisateurs de naviguer sur Internet de manière anonyme en séparant identification et routage, dissimulant ainsi l'activité du réseau de surveillance. Les sites sur le Web profond ne peuvent être accessibles que via le client Tor.
- La première idée était de passer de proxy en proxy, sur une chaîne suffisamment longue et distribuée pour dissuader quiconque de remonter les logs jusqu'à la source réelle
- Un circuit est une chaîne de relais Tor, il suffit de sélectionner l'option relayer le trafic pour le réseau Tor, de choisir les options de bande passante et de politique de sortie dans Vidalia, dans la mesure où chacun est libre d'écrire son client Tor et de lui faire appliquer les règles qu'il désire.
- En outre, certains paramètres, tels que la sélection de relais « non stables », peuvent être positionnés par l'utilisateur, comme précisé dans le document de spécifications.



- Les directory servers sont indubitablement le talon d'Achille de Tor. « Hardcodée », la liste exhaustive est restreinte et accessible dans le fichier src/or/config.c.

# Bitcoin [21 millions]

Date	cours en euros <sup>12</sup>
7 février 2011	4,15 €
9 août 2011	5,36 €
25 novembre 2011	1,83 €
10 décembre 2011	2,30 €
25 janvier 2012	4,34 €
3 août 2012	8,51 €
15 janvier 2013	10,97 €
21 mars 2013	50,78 €
3 avril 2013	109,91 €
9 avril 2013	200,00 €
13 avril 2013	66,00 €
24 avril 2013	109,79 €
19 juillet 2013	69,28 €
22 octobre 2013	146,00 €
8 novembre 2013	259,00 €
15 novembre 2013	331,34 €
18 novembre 2013	547,00 €
4 décembre 2013	860,00 €
8 décembre 2013	498,00 €
12 décembre 2013	659,17 €
18 décembre 2013	355,00 €
3 janvier 2014	640,00 €
13 février 2015	218 €
13 mars 2015	272 à 279 €
24 avril 2015	215 €
17 juillet 2015	263 €
19 novembre 2015	315 €



Bitcoin : une monnaie électronique distribuée (crypto-monnaie). Elle permet le transfert d'unités bitcoins à travers le réseau Internet. Les bitcoins ainsi échangés ont vocation à être utilisés en tant que devise monétaire et comme moyen de paiement.

Conçu en 2009 par un développeur non identifié utilisant le pseudonyme Satoshi Nakamoto,

Comprendre la Sécurité – dec 2018 - © Xa - diffusion contrôlée

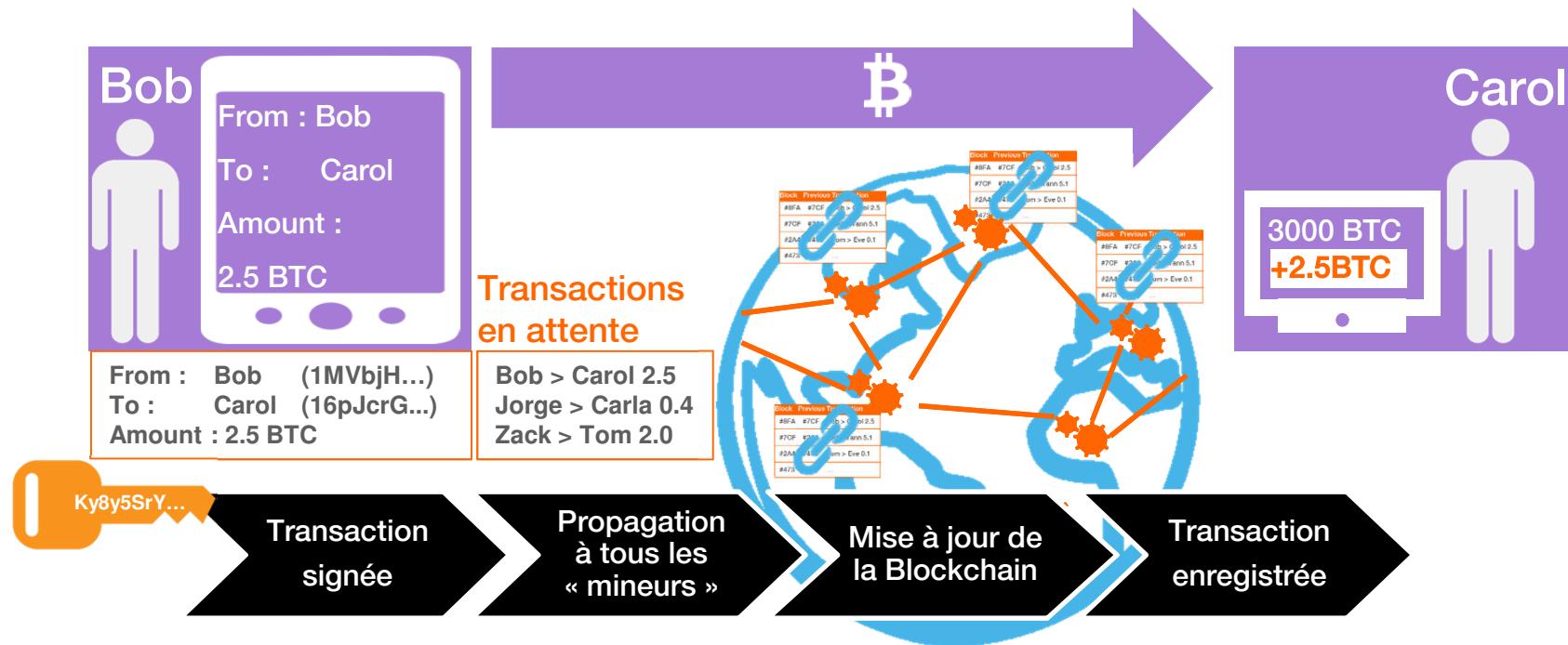


<http://www.bitcoinfr.com/fonctionnement/>

EUR +2.87%  
8795 €  
CAD 13710\$



# Comment ça marche?



**Blockchain : registre public de toutes les transactions passées**

- chacun peut vérifier les transactions depuis le début
- personne ne peut modifier une transaction passée

Block	Previous Transaction
#8FA	#7CF Bob > Carol 2.5
#7CF	#2A4 Ted > Yann 5.1
#2A4	#473 Tom > Eve 0.1
#473	...

**Les mineurs : système distribué peer to peer**

- garantissant le contenu des transactions (authentification, non falsification des registres, pas de « doubles paiements » possibles)
- en établissant un consensus sans autorité centrale
- et sans être détournable par une minorité coordonnée



## Des mineurs « professionnels » en pools

- Le maintien du registre est assuré par des volontaires, les mineurs
- Rajouter un bloc de nouvelles transactions au registre (blockchain) nécessite de résoudre un problème difficile
- En cas de bifurcation (fork), la blockchain la plus longue est considérée comme valide
  - 1er Août 2017 : la taille des blocs peut atteindre 8 Mo contre 1 Mo auparavant.
- Chaque transaction est propagée au réseau (mécanismes peer-to-peer)
- Elle n'est validée qu'une fois rajoutée au registre
  - Qui maintient le registre? Comment assurer son unicité? : **1CPU = 1 voix -> Proof of Work**
  - 2017 : Antminer S9 = 1 bitcoin / an
  - W : 4,30 € / h = 1570 € / an
  - Blockchain : 657k bitcoin/an = 1,760 TWh = 1 réacteur EPR
- Caractéristique d'une Blockchain**
  - Autogestion: aucune autorité de confiance
  - Ouverture: liberté d'échanger, de miner, etc
  - Transparence: le registre est public
- Avantages d'une Blockchain**
  - Sécurisation sans confiance mutuelle
  - Participation libre et sans identification
  - Transparence
  - Pas d'autorité
- Limites des blockchains**
  - structurellement plus coûteux qu'un système centralisé
  - Sécurité: dépend de la puissance de calcul des mineurs
  - Taille: chaque transaction augmente la taille de la blockchain
  - Anonymat: ces systèmes ne sont pas intrinsèquement anonymes /pseudo
  - Décentralisation: les mineurs se regroupent en « pools » contrôlant l'essentiel de la blockchain : fin 2014: les deux pools produisent plus de 50 % des blocs
- Gouvernance**
  - Mise à jour très complexe: chaque changement doit faire l'unanimité => **fork**
  - Incitation des utilisateurs court-termes à profiter des forks
  - Quasi-impuissance face aux vols et piratages



### ANTMINER S9

\$1,750.00  
฿0.24718

1 ADD TO CART

Free shipping worldwide



Description	Specifications	Payment	Warranty	Reviews
Power	Supply unit is not included. You will need an ATX PSU.			
Hash Rate	13TH/s & 13.5TH/s, depending on batch. Variation of ±5% is expected			
Power Consumption	1.274W +10% (for 13TH/s batch) & 1.323W +10% (for 13.5TH/s batch) (at the wall, with Bitmain's APW3 PSU, 93% efficiency, 25°C ambient temp)			

# Le système de monnaies virtuelles

- Ces monnaies n'ont a priori jamais été pensées pour contrevenir à la légalité, elles présentent toutes les caractéristiques susceptibles de **faciliter les transactions illégales**. Elles peuvent servir à tous types d'échanges (légaux et illégaux) en se substituant à des services de paiement régulés.
- En théorie, la création d'un compte permettant d'utiliser un système de monnaie virtuelle **implique que l'authenticité de l'utilisateur** soit vérifiée et qu'il justifie de son identité avec des documents officiels.



**WebMoney** : solution a vu le jour en 1998 en Russie. Elle revendique aujourd'hui 28 millions d'utilisateurs dans le monde

# “Depp Web Marketplaces”

## DARKWEBNEWS

The Ultimate Dark Web Resource

ACCESS DARKWEB

DARKNET MARKET LIST

DEEP WEB LINKS

ANONYMITY TOOLS

DEEP WEB ANONYMITY BITCOIN DARKNET MARKETS HELP &amp; ADVICE MARKETS COMPARISON DICTIONARY

Silk Road is a darknet marketplace featuring a wide range of products across numerous categories. Some visible categories include Electronics, Clothing, Furniture, and Pharmaceuticals. The site uses Bitcoin as its primary payment method, indicated by the prominent PayPal logo.

BlackMarket Reloaded is another darknet marketplace. It displays a grid of product cards, each with an image, a title, and a price. The interface includes a sidebar with categories like Drugs, Electronics, and Services, and a central search bar.

- Silk Road créée en Février 2011, mais fermé par le FBI en Oct 2013
- La route de la soie est un marché noir en ligne qui ne peut être accessible via le client de navigation TOR. Beaucoup de vendeurs sur le site se spécialisent dans le commerce de drogues illicites, achat/vente en Bitcoins, une monnaie numérique peer-to-peer.
- Les marchandises étaient disponibles dans plus de 200 catégories,
- Des concurrents qui sont toujours actifs.

## 5 Biggest Markets

Up / Online Dream Market - 95.8% ↗

Up / Online Silk Road 3 - 87.55% ↗

Down / Offline Valhalla - 96.46% ↗

Up / Online Tochka - 89.77% ↗

Up / Online WallStreet Market - 89.39% ↗

## Smaller Markets

Down / Offline Acropolis Market - 99.24% ↗

Down / Offline Alphabay (ALT) - 91.77% ↗

Down / Offline Apple Market - 91.74% ↗

Down / Offline Berlusconi Market - 77.67%

Up / Online BitBlender - 98.48%

Up / Online BitCloak - 95.11% ↗

Down / Offline BlockChain info - 86.02%

Up / Online CGMC - 98%

Up / Online CharlieUK - 89.26%

# Passports – Cartes d'Identité

**FakeID®**

Main | News | Services | Samples | FAQ | Order | Contacts

**Pricing**

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italy	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	600 Euro	700 Euro	700 Euro	800 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

For some countries we have an unique option to register passports in official government department databases. To get more details please contact with our manager: [documents.service@safe-mail.net](mailto:documents.service@safe-mail.net)

Additional services	Price for one unit
Documents duplicating	extra 100 Euro
Visa/stamps affixion	extra 25-110 Euro

Prices on specific services like producing passports and documents for countries not listed above, duplicates, stamps, diplomatic passports and others should be discussed with our operator and may be variable.



# Cartes de Crédits – Monnaies - Armes

Please enter the amount you wish to purchase below and fill in the form.  
(BTC value updates periodically via BTPAY)

USA VISA CREDIT CARD BALANCE \$2,000  
Accepted at ATM worldwide  
\$500 daily withdraw limit  
\$90 (0.4001 BTC)  
amount 0

USA VISA CREDIT CARD BALANCE \$5,000  
Accepted at ATM worldwide  
\$1,000 daily withdraw limit  
\$170 (0.7557 BTC)  
amount 0

EU VISA CREDIT CARD BALANCE €5,000  
Accepted at ATM worldwide  
€1,000 daily withdraw limit  
\$210 (0.9335 BTC)  
amount 0

HQER - High Quality Euro Replicas / Counterfeits

Products Info Login Register

### Counterfeit 50 Euro Bills

Our notes are produced of cotton based paper. They pass the pen test without problems. UV is incorporated, so they pass the UV test as well. They have all necessary security features to be spent at most retailers.  
FREE EXPRESS SHIPPING! We are shipping from france!

Product	Price	Quantity
25 x 50 Euro Bills	1.128 B	1 X <a href="#">Buy now</a>
60 x 50 Euro Bills	2.256 B	1 X <a href="#">Buy now</a>
120 x 50 Euro Bills	4.286 B	1 X <a href="#">Buy now</a>

Desert Eagle IMI, Kal.44

New and unused!

Product	Price	Quantity
Desert Eagle IMI, Kal.44	1250 EUR = 12.059 B	1 X <a href="#">Buy now</a>
Ammo, 50 Rounds	45 EUR = 0.434 B	1 X <a href="#">Buy now</a>

# Infos & Forums : reddit.com/r/DarkNetMarkets

- Faites vos recherches avant d'utiliser un marché caché sur Reddit

The screenshot shows the DarkNetMarkets subreddit homepage. In the top navigation bar, the link [/r/bitcoin](#) is circled in red. A red arrow points from this link to a smaller screenshot of the [r/bitcoin](#) subreddit page.

**DarkNetMarkets**  
Market Superlist [/r/DarkNetMarketsNoobs](#) Harm Reduction

/r/Deepz [/r/bitcoin](#) /r/DNMParensale /r/DRMUK /r/DarkNetMarkets /r/DarkNetMarketsDC /r/DarkNetMarketsWD /r/DarkMarketsBrazil /r/DRMTurkey /r/DRMDE /r/DRMIndia /r/DNM\_Memes

Daily OpSec-Tip: Do not forget to [donate to the Tor Project](#). Their tireless work is the reason why we are even able to enjoy freedom. Do not [source or direct deal](#) on reddit. Please read the [rules](#) before posting or commenting.

populaire nouveau en progression controversé le meilleur doré wiki Want to join? Se connecter ou s'enregistrer in seconds. | [français](#)

7 Trade Monero for CASH - Register now on Liberalcoins, the most private exchange  
promu par liberalcoins  
2 commentaires partager signaler

Please subscribe from the sidebar if you would like to submit or download posts.

31 PSA / Article [Use this one weird trick to double your Tor-donations](#)  
soumis il y a 5 jours par wombat2combat - announcement  
19 commentaires partager signaler

1 Tinfoil Tuesday  
[Tinfoil Hat Tuesday!](#)  
soumis il y a 3 heures par AutoModerator (M) - announcement  
5 commentaires partager signaler

40 PSA / Article [FYI: "No Logs" VPN Provider Shared Logs with FBI](#)  
soumis il y a 7 heures par ChadButlerJCK  
11 commentaires partager signaler

7 PSA / Article [Block I.P Leak Tor](#)  
soumis il y a 3 heures par ritalin7711

recherche  nom d'utilisateur  mot de passe  mémoriser

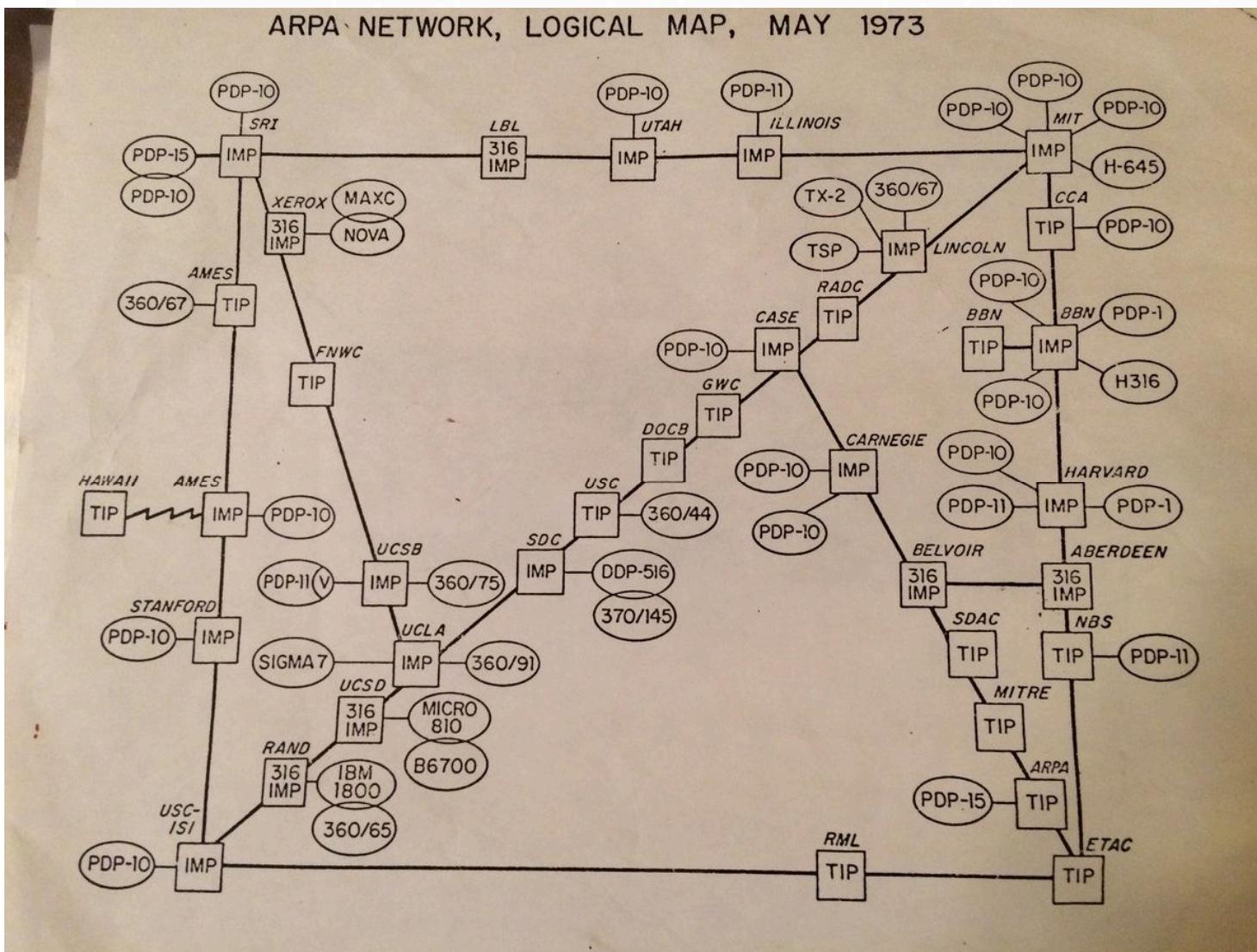
**r/bitcoin** populaire nouveauté

12 DMarket is cross-game trading platform based on blockchain for presale! (dmarket.io)  
promu par TamanShud89  
1 promu signaler

/r/Bitcoin FAQ - Newcomers please read

DarkNetMarkets [s'abonner](#)  
160 142 lecteurs

# Origine d'Internet 1/2



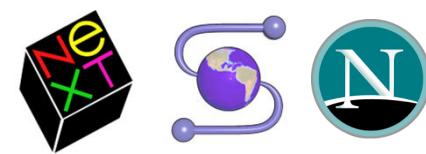
Source : <http://www.fieldmuseum.org>

## Origine d'Internet 2/2

- Projet ARPANET en 1969 : US Department of Defense (DoD)
  - Advanced Research Projects Agency Network
  - Objectif : Rendre fiable un ensemble de système informatique
    - Résistance aux attaques... réseau, routage...
- Faits marquants du réseau Arpanet
  - 1971 : Quelques ordinateurs (23) échangent des informations de recherche
  - 1972 : présentation officiel du projet ARPANET à l'International Conference on Computer Communications.
  - 1974 : TCP/IP pour uniformiser le réseau
  - Le 1<sup>er</sup> janvier 1983, ARPANET adopte le TCP/IP qui sera la base d'Internet
  - 1986 : Premier incident de sécurité rendu public, possibilité de vol de fichiers des ordinateurs du gouvernement
  - 1988 : le premier vers, « Morris Worm ». Autour de 10% des stations US contaminées en quelques heures. Création du CERT (Computer Emergency Response Team) par le DARPA (Defense Advanced Research Project Agency)
  - 1989 : ARPA devient officiellement Internet www [12 mars/ Tim Berners-Lee – www project] réseau de recherche du CERN de 100 000 stations
  - 1990 : HTTP, HTML, URL, 1<sup>er</sup> Navigateur « Nexus »
  - 1993 : NCSA Mosaic, Xwindows, Mac, Windows - Populaire
  - 1995 : Netscape et I.E



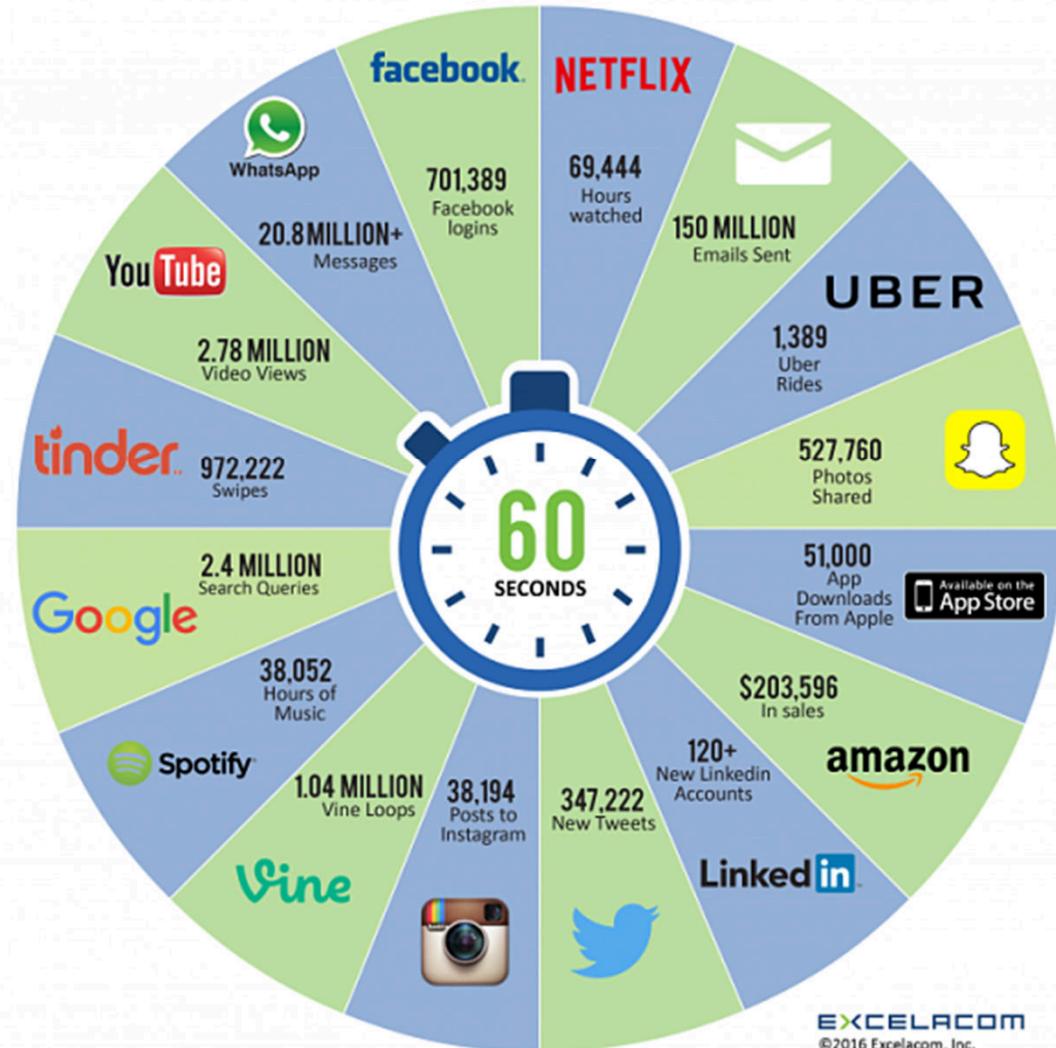
<https://fr.wikipedia.org/wiki/ARPANET>



## Une tranche de 60 secondes d'Internet

- 69 444 heures de films sont regardées sur Netflix
- 150 millions d'emails sont envoyés
- 1 389 demandes de courses sont traitées par Uber
- 527 760 photos sont partagées sur Snapchat
- 51 000 applications sont téléchargées sur Apple App Store
- 203 596 dollars de chiffres d'affaire sont réalisés par Amazon
- 120 nouveaux comptes sont créés sur LinkedIn
- 347 222 Tweets sont publiés sur Twitter
- 38 194 posts sont partagés sur Instagram
- 1,04 million de boucles de vidéos de Vine sont regardées
- 38 052 heures de musique sont écoutées sur Spotify
- 2,4 millions de recherches sont effectuées sur Google
- 972 222 swipes (réponses négatives et positives) sont réalisées sur Tinder
- 2,78 millions de vidéos sont vues sur YouTube
- 20,8 millions de messages sont envoyés via WhatsApp
- 701 389 connexions sont effectuées sur Facebook

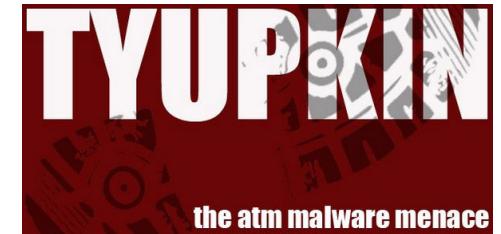
## What happens in an 2016 INTERNET MINUTE?



## Attaques ciblées



# Cyber attaques notables en 2014



TARGET



snapchat



orange™



Aol.

JPMorganChase



kmart

SONY

Dec | Jan | Feb | Mar | Apr | May | Jun | July | Aug | Sept | Oct | Nov



HEARTBLEED



## TYUPKIN – Carbanak

- TYUPKIN : Local par accès physique
- 50 ATMs touchés en Russie
- Fabricant ATM : NCR fonctionnant sous Windows 32 bits
- Malware installé via un CD de boot

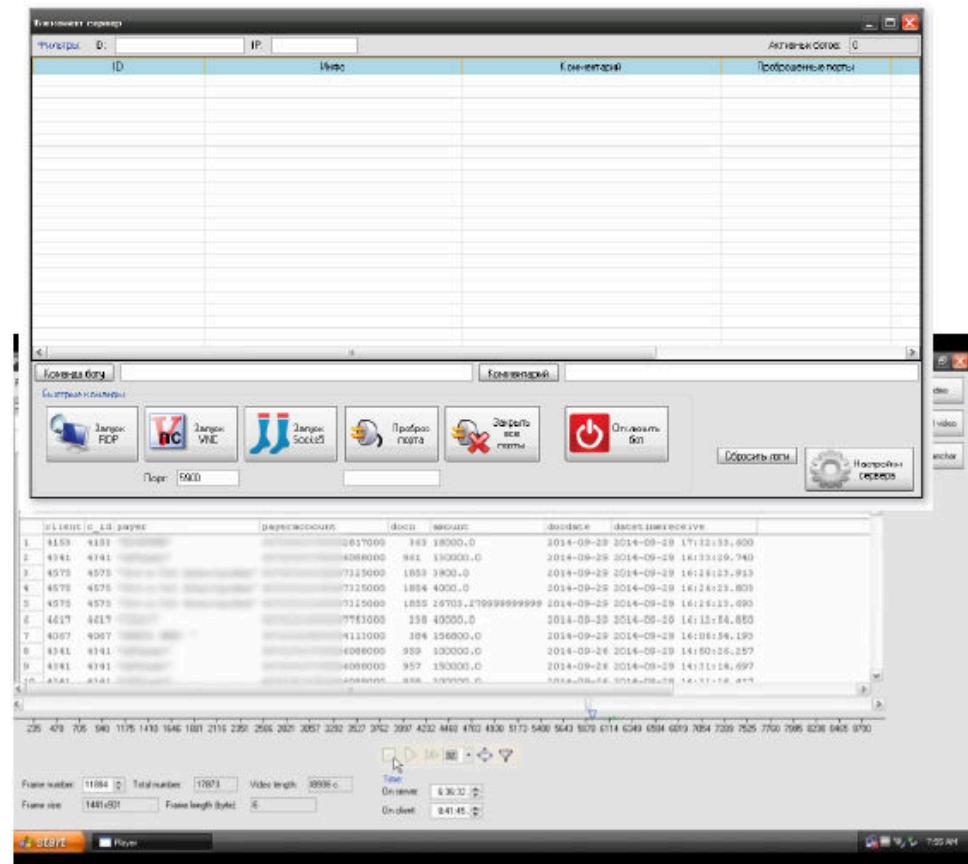
```
C:\windows\system32\ulssm.exe  
%ALLUSERSPROFILE%\Start Menu\Programs\Startup\AptraDebug.lnk
```

- Fonctionnement :
  - Actif entre 1h et 5h du matin
  - Utilisation d'un code pour accéder à l'ATM
  - Menu permettant de choisir le bac de billet
  - Récupération de 40 billets
    - 111111 – affichage de la fenêtre de menu du malware
    - 333333 – suppression à l'aide d'un fichier batch
    - 5555555 – extension de l'activation de 01:00 AM à 10:00 AM
    - 000000 – fermeture du menu
    - Utilisation d'un code de session « challenge/response »



# CARBANAK : à distance par méthode d'infection 1/2

- 100 banques touchées (Russie, USA, Allemagne, Chine et Ukraine)
- Des pirates situés en Russie et en Chine
- 1 Milliard \$ volés
- Entre 2,5 et 10 Millions \$ par cible
- Durée des opérations entre 2 et 4 mois
- Etude de la banque
- Contrôle à distance
- Enregistreurs de frappes
- Outils de capture d'écran
- Etude pas à pas des outils financiers
- Formation en ligne ou transfert de compétence



## CARBANAK : Etude de la banque 2/2

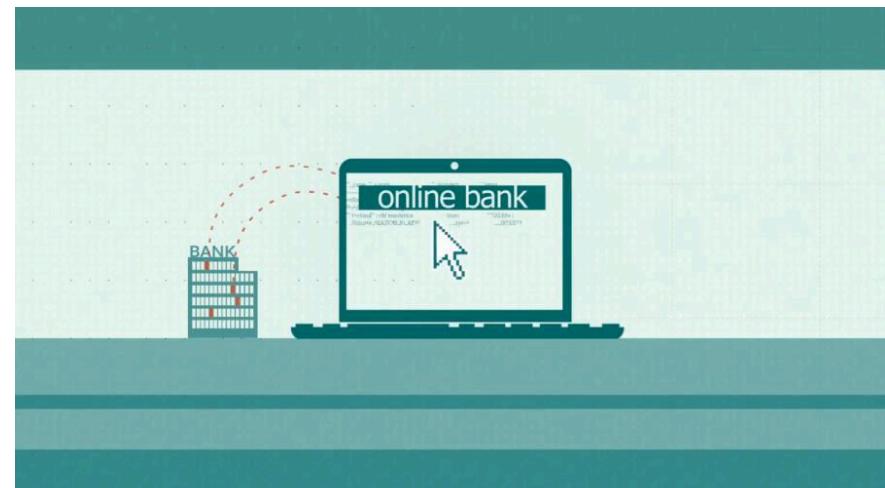
- Utilisation du spear phishing – malware basé sur le trojan Carberp
- Exploitation de vulnérabilités Microsoft Office
- Installation d'une Backdoor (basée sur Carberp)
- Recherche des cibles avec accès aux systèmes critiques financiers
- Transfert d'argent via le réseau SWIFT
- Manipulation des BD :
  - Création de faux comptes bancaires
  - Utilisation de l'équilibrage des comptes
- Commande à distance des DAB

Good Day!  
I send you our contact details  
The amount of deposit 32 million rubles and 00 kopecks, for a period of 366 days,% year---end contribution term  
Sincerely, Sergey Kuznetsov;  
+ 7 (953) 3413178  
f205f@mail.ru

Exploits utilisés:  
Microsoft Office (CVE- 2012-0158), CVE-2013-3906) et Microsoft Word (CVE- 2014-1761).

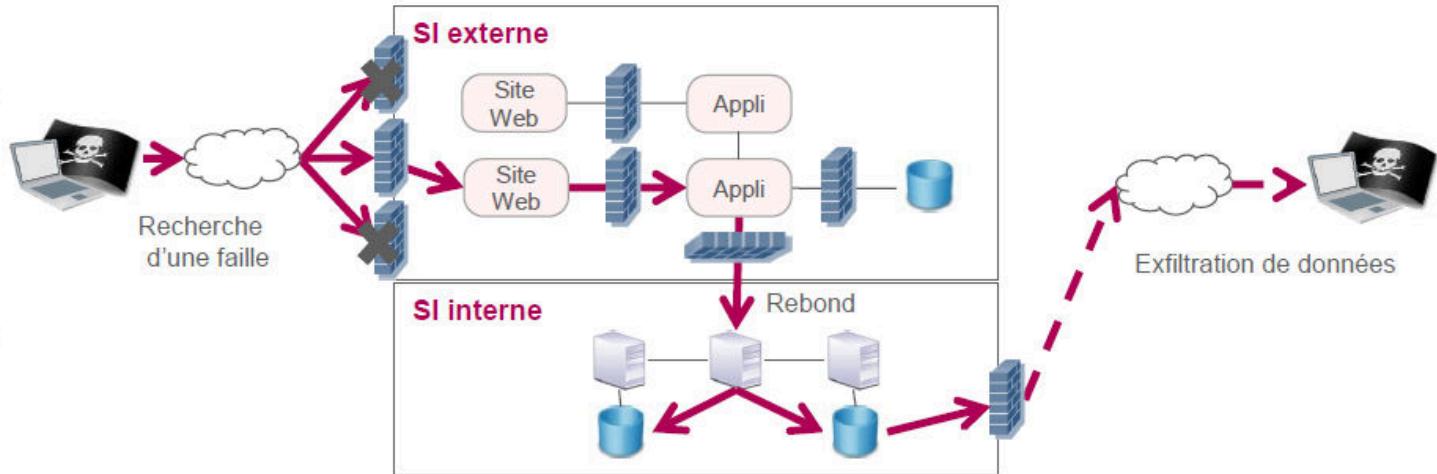
Copie %system32%\com avec le nom "svchost.exe" + création service "`<ServiceName>Sys`".bin créé dans %COMMON\_APPDATA%\Mozilla Récupération configuration proxy registre Windows ou config Firefox

RAT: Ammyy Admin, Backdoor SSH, Metasploit, PsExec or Mimikatz

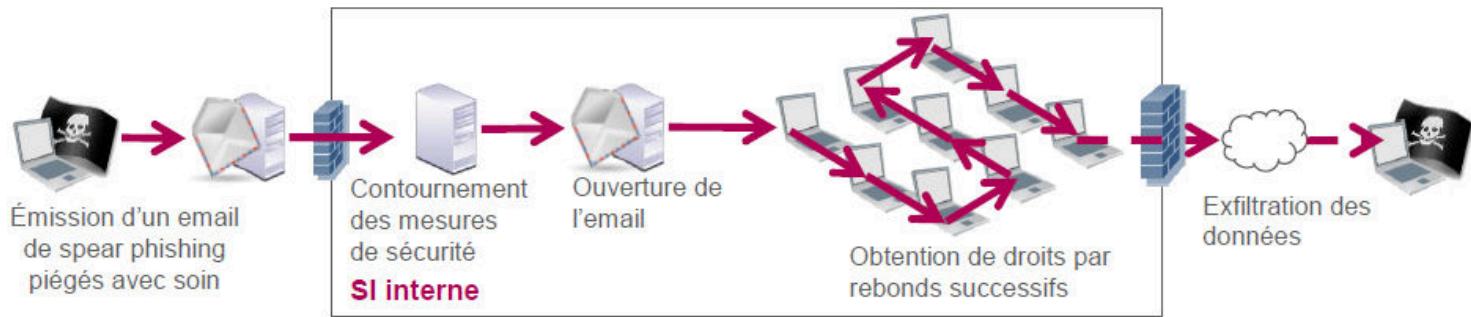


# Les canaux d'entrée les plus rencontrés...

## Attaque technique par canal web

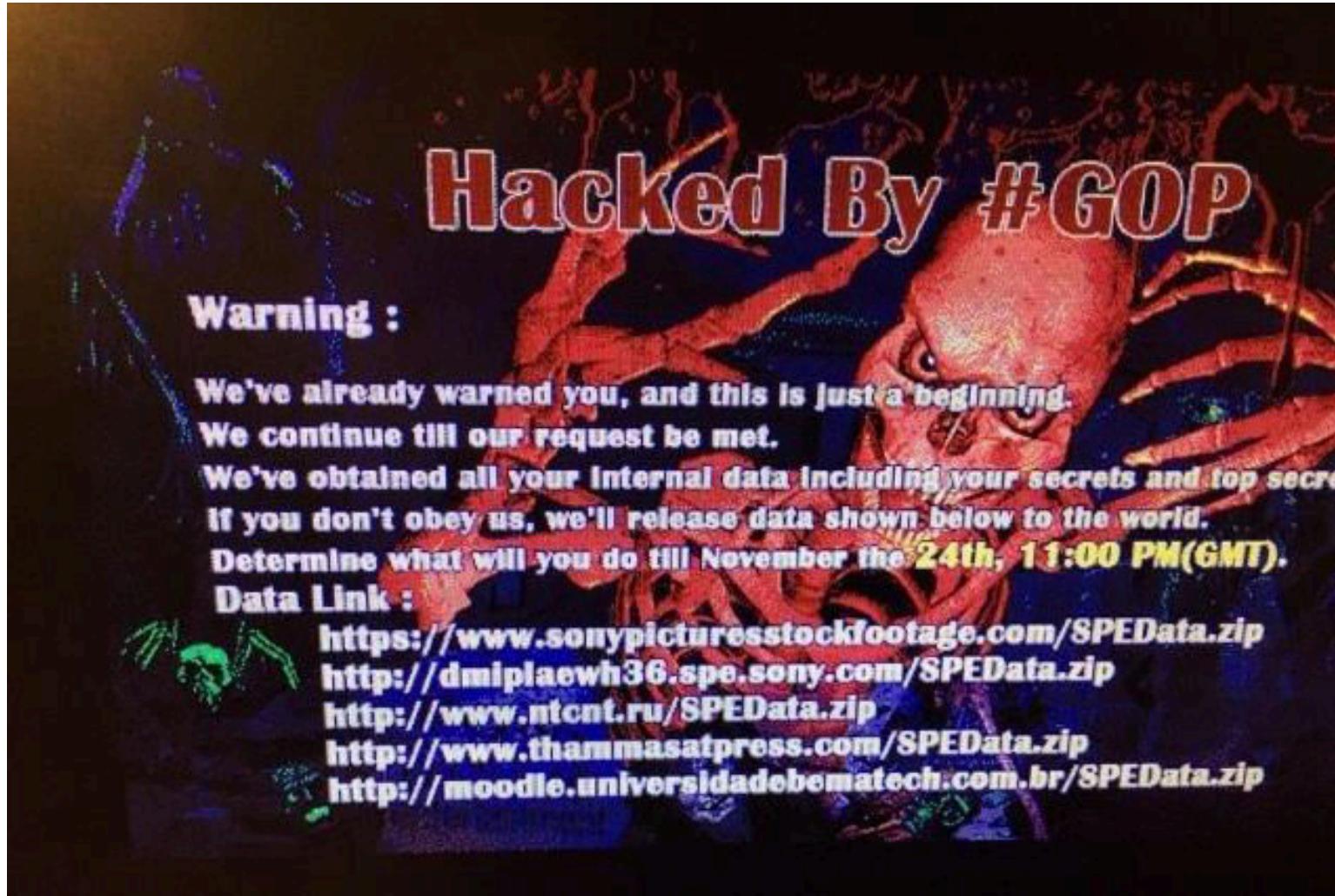


## Ingénierie sociale par messagerie (spear phishing)



Mais beaucoup d'autres moyens peuvent être mis en œuvre...

# Le cas Sony Pictures : Rançon ciblée



« Guardian of Peace »

# Sony : Les éléments déclencheurs

+/- Février 2014 : intrusion initiale dans le SI de Sony par un moyen encore inconnu et extraction de plus de 110 To de données

21/11/2014 : demande de rançon

22-23/11/14 : Déploiement d'un outil d'attaque destructeur (Destoyer)

24/11 – Lancement de l'attaque : effacement des postes de travail Windows et de 75% des serveurs

From Frank David <dfrank1973.david@gmail.com>  
Subject: Notice to Sony Pictures Entertainment Inc.  
To: michael\_lynton@spa.sony.com, amy\_pascal@spa.sony.com, doug\_belgrad@spa.sony.co  
  
We've got great damage by Sony Pictures.  
The compensation for it, monetary compensation we want.  
Pay the damage, or Sony Pictures will be bombarded as a whole.  
You know us very well. We never wait long.  
You'd better behave wisely.  
From God'sApostls



A source inside Sony Pictures, speaking to Deadline, said "We are down, completely paralysed."

BUSINESS INSIDER INTELLIGENCE EVENTS

Tech Finance Politics Strategy Life Entertainment All

Staff At Sony Pictures Are Being Forced To Use Pens And Paper After A Massive Hack

JAMES COOK NOV 28, 2014, 10:09 AM 3,900 ▶ 1

FACEBOOK LINKEDIN TWITTER GOOGLE+ PRINT EMAIL

# Sony : des impacts en 3D



# Les différents scénarios de l'origine de l'attaque cyberguerre est au programme

- Le 19/12/2014 Barack Obama lors d'une conférence de presse évoque le cas de piratage de SONY et pointe la Corée du Nord
- Le 20/12/2014 Pyongyang rejette l'accusation américaine à propos de la cyberattaque contre Sony Pictures



En parallèle le 25 décembre, «The Interview» sort en salle et en ligne, il rapporte en 6 jours 17,8 M\$ (face à un budget de 44 M\$)



- Et depuis le groupe GOP a disparu... mais le débat de l'attribution ne faiblit pas !
- Les impacts et l'effet des sanctions seront évalués en 2015...

# Gestion de risques : HACKMAGEDDON

Information Security Timelines and Statistics

SUBMIT AN ATTACK

Ref	Date	Author	Target	Description	Attack	Target Category	Attack Category	Country
1	Feb 1			The hacking group NullCrew AKA @NullCrew_FT8 claims to have successfully hacked Bell Canada (bell.ca). As a consequence 40,000 credentials are leaked.	SQI	Industry: Telco	CC	CA
2	Feb 1		 	The Syrian Electronic Army is back and leaks some internal emails from the Internal PayPal UK website. Also users visiting the UK, France and India sites are redirected.	Account Hijacking	Industry: E-Commerce	H	US
3	Feb 1			of Russia's Federal Customs Service (eng.customs.ru) is defaced by members of Team M0nkrus.	Defacement	Government	H	RU
4	Feb 1	?		The Twitter account of Carlo Ancelotti (@MrAncelotti), the manager of the Spanish football team Real Madrid, has been hacked.	Account Hijacking	Single Individual	CC	IT
5	Feb 2			Anonymouse defaced the website of the Ateneo Integrated Student Information System (AISIS).	Defacement	Education	H	PH
6	Feb 3	?		Orange confirms that hackers accessed the personal data of three percent of Orange's customers in France (corresponding to about 800,000 users), using the 'My Account' section of orange.fr. The attack took	Unknown	Industry: Telco	CC	FR

## Cyber Attacks Timeline

List the (Main) Cyber Attacks on a Monthly Base

H Hacktivism  
 CC Cyber Crime  
 CE Cyber Espionage  
 CW Cyber War

## Threat Evolution

e.g. *The Sapphire Worm or “Slammer”*

- Infections doubled every 8.5 seconds
- Infected 75,000 hosts in first 11 minutes
- Caused network outages, cancelled airline flights and created ATM failures

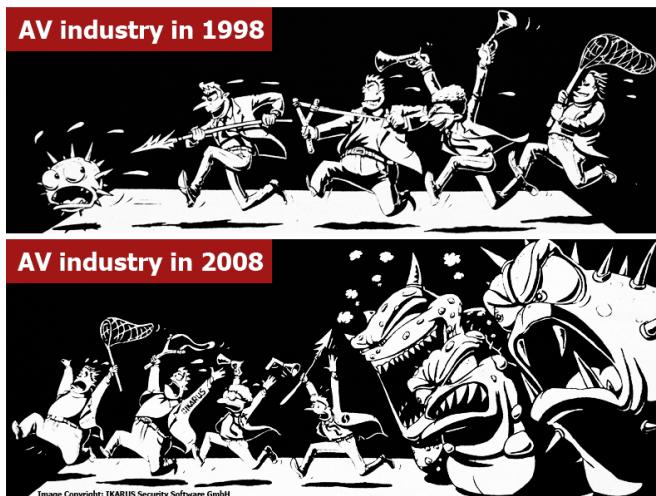
At peak,  
scanned 55 million hosts per second



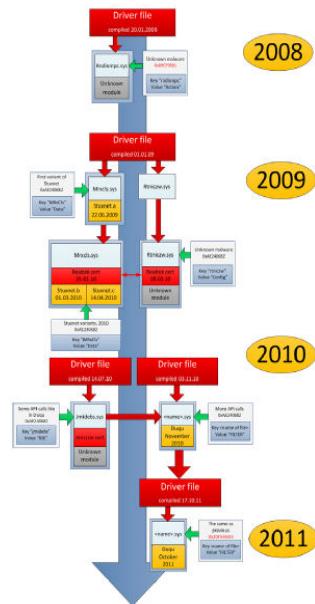
## Point commun entre ces sociétés



- Elles ont toutes subi une attaque ciblant à la base un poste de travail...
- Elles avaient toutes un antivirus !
- Les antivirus sont incapables de reconnaître une menace inconnue



# STUXNET : découvert en 2010



Découvert en juin 2010

- Technicité très élevée
- Charge active ciblant des PLC
- Simulateur de normalité SCADA
- Plusieurs zero-day exploitées
- Emploi de certificats dérobés
- Forte furtivité

D'après le New York Times (juin 2012) :

- Opération conjointe Etats-Unis / Israël
- Conçue pour saboter l'installation nucléaire de Natanz
- Développée et conduite sur des années
- Code déployé via clé USB par agents ou utilisateurs piégés
- A atteint ses objectifs (retarder le programme nuc. iranien)



# Open SSL : découvert en 2014 <- 03/2012

- Open source = code source ouvert
- Service et infrastructure critique
- Boîte à outils de cryptographie SSL-TLS
- Confidentialité des échanges
- Sites web, serveurs, smartphones
- 80% des applications assemblées en code open source
- Limite des usages

