Sécurité :
Les Enjeux de la Sécurité

Sécurité des Systèmes d'information
Concepts, Organisation, outils et Tendance

J. Saraydaryan

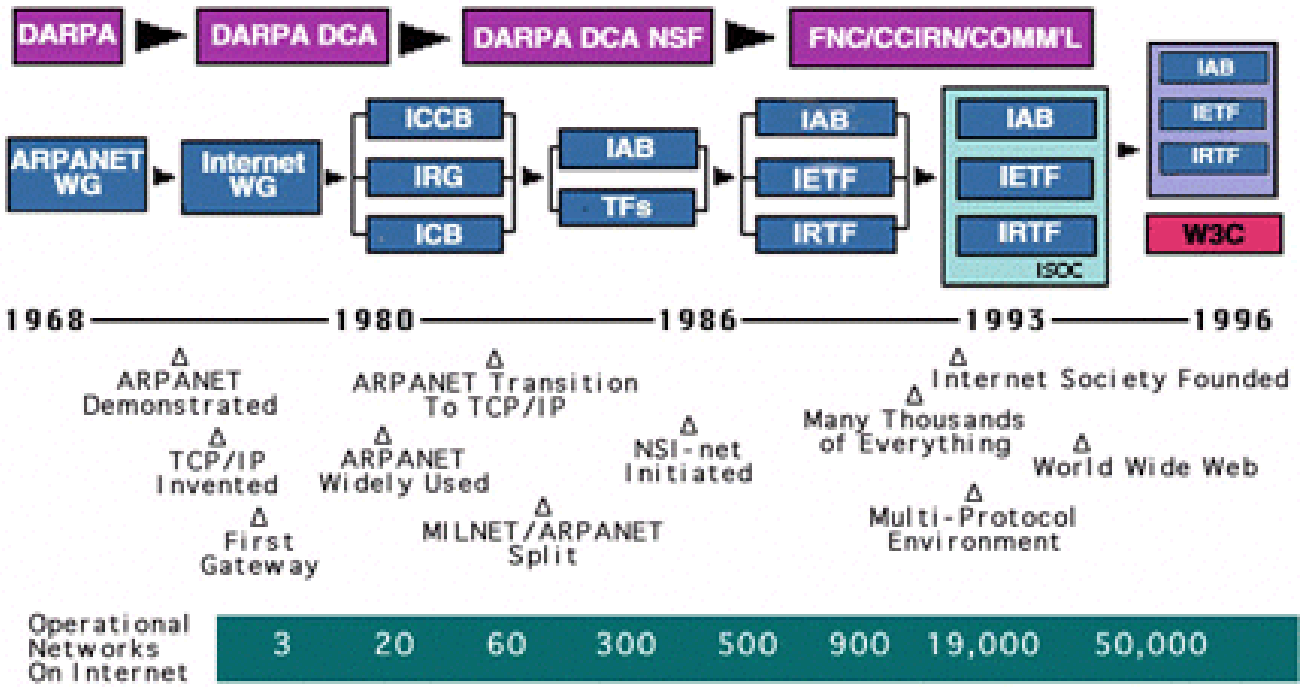
OutLine

- Evolution du monde informatique
  - Evolution des systèmes d'information
  - Les constats de la sécurité
- Les enjeux de la sécurité
  - Etat d'urgence ?
  - Les bases de la sécurité
- Comprendre les attaques
  - ARP Spoofing / DNS Spoofing
  - TCP Flooding / TCP Session Hijacking
  - XSS / Bufferoverflow

Evolution du monde informatique

- Evolution des SI
- Les Constats de sécurité

Evolution des réseaux

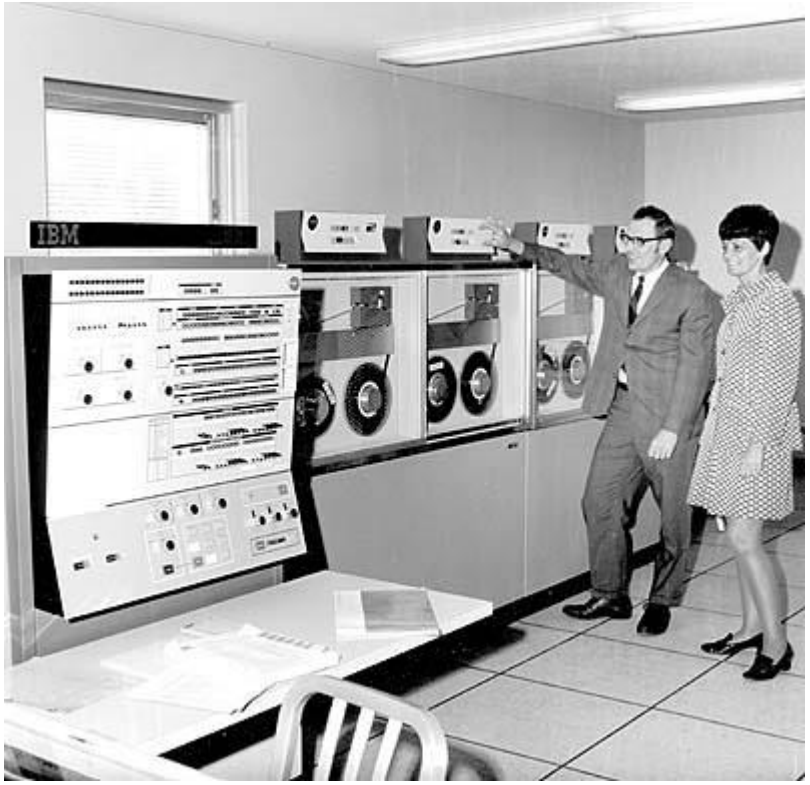


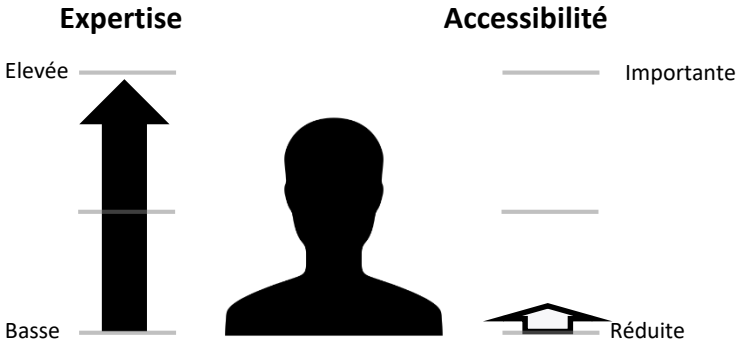
http://www.internetsociety.org/sites/default/files/images/timeline.gif

http://www.evolutionoftheweb.com/

Evolution des réseaux

MainFrame

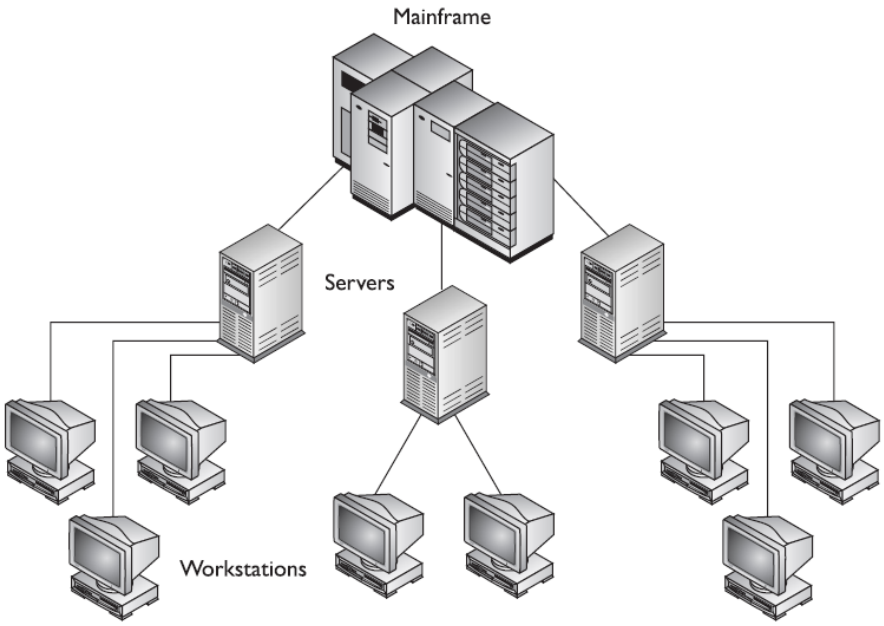


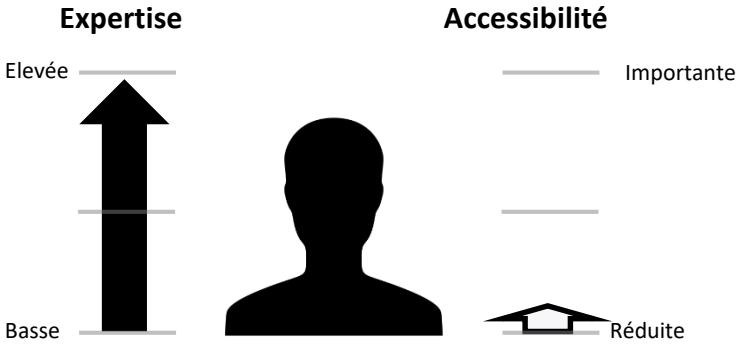


- Accès par expert uniquement
- Utilisation Scientifique

Evolution des réseaux

MainFrame

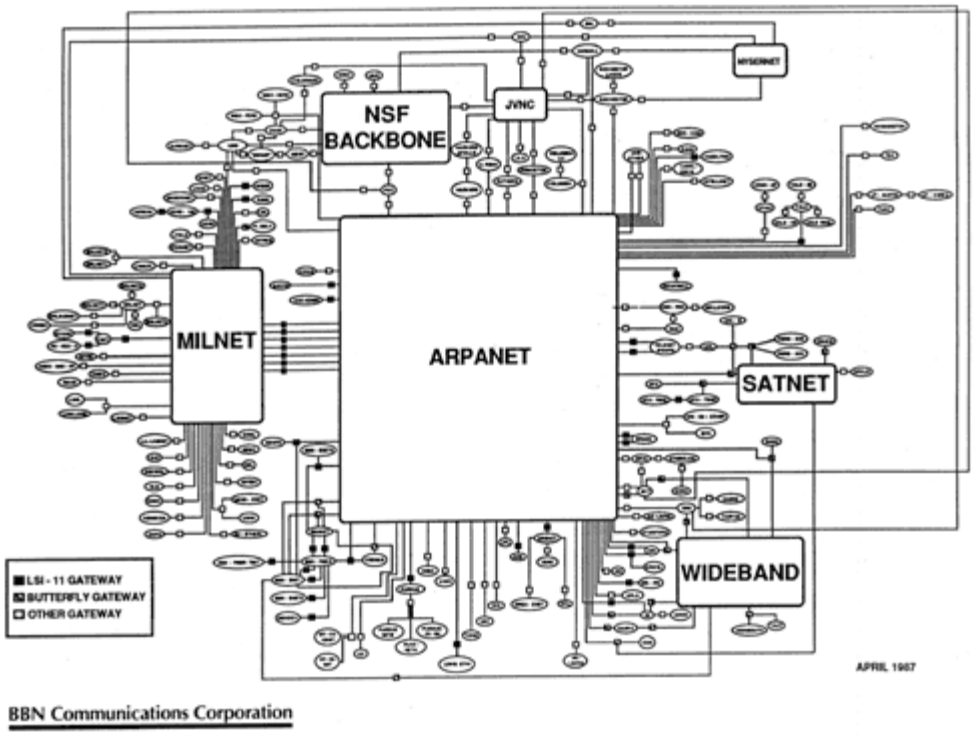


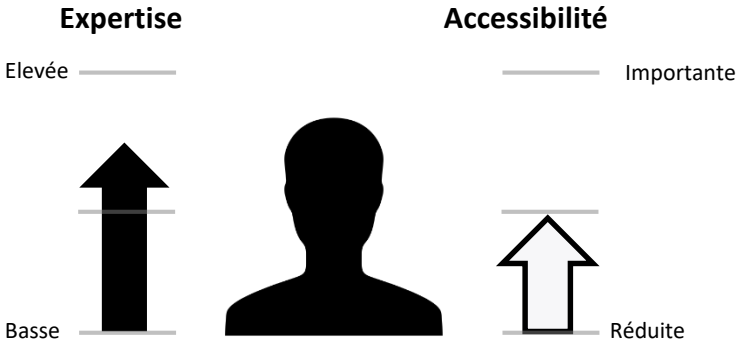


- Accès aux utilisateurs du réseau via des serveurs relais
- Peu de Workstation
- Accès physique aux Workstations obligatoire

Evolution des réseaux

ARPANET (1983)

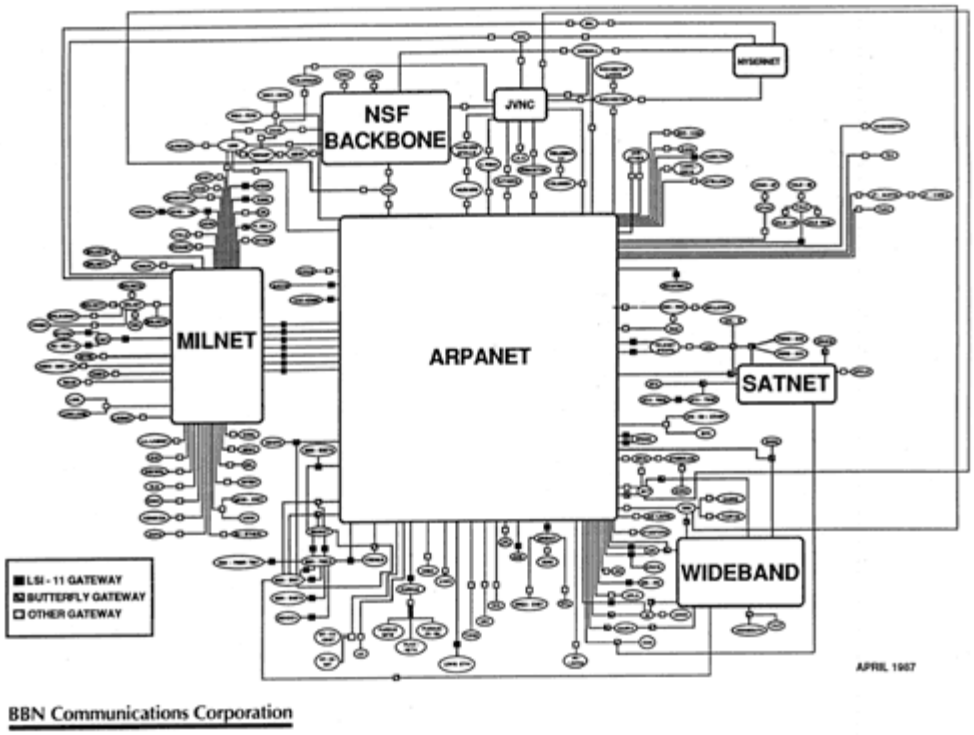


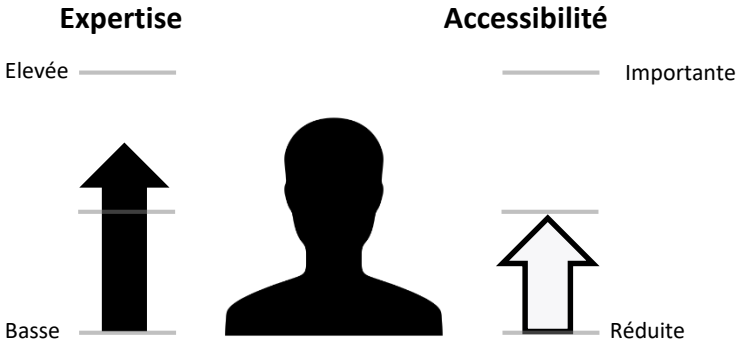


- Accès aux utilisateurs du réseau membre ARPANET
- Workstation plus étendues

Evolution des réseaux

World Wide Web (1989)

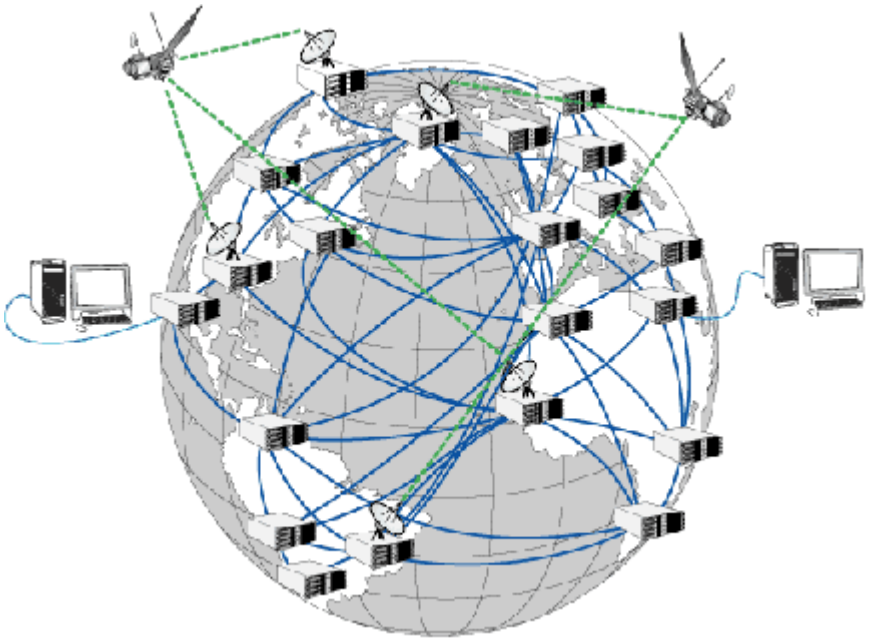


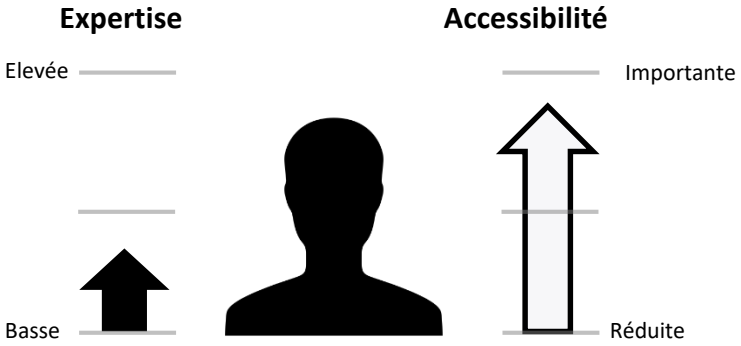


- Ouverture du réseau ARPANET
- HTML, HTTP, URI
- DNS,EMAIL,PC

Evolution des réseaux

Internet (2000)

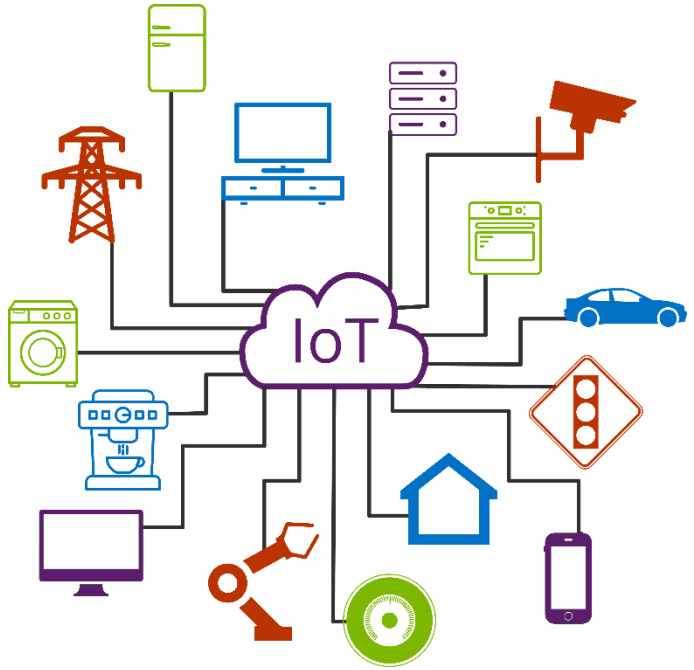




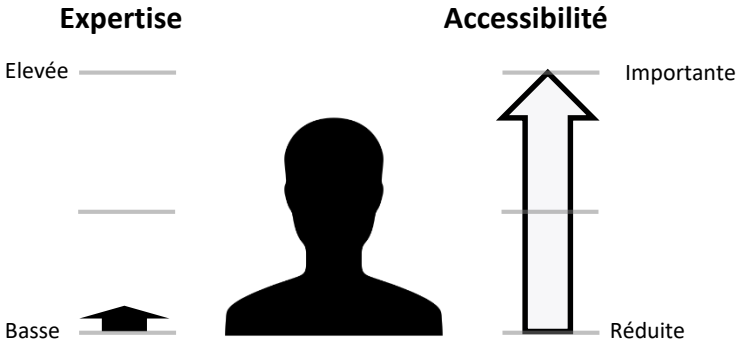
- Accès à tous les utilisateurs possédant un provider
- Navigateur Web,
- Pages personnelles/Professionnelles,

Evolution des réseaux

Internet – IoT



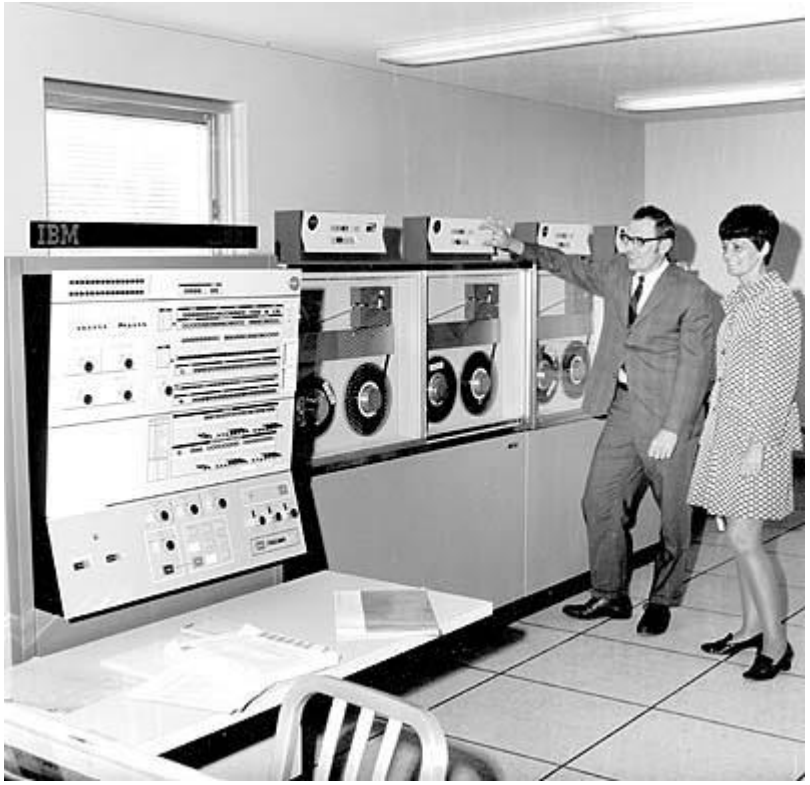
http://www.iowacomputergurus.com/Solutions/Internet-of-Things

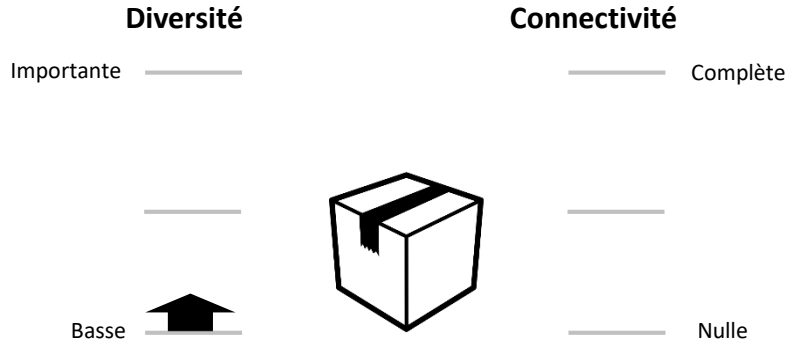


- Multiplication des points d'accès
  - Object
  - Terminaux mobiles (3G, 4G, 5G)
  - Véhicules
- Simplification des interfaces
- Vers un tout connecté

Evolution des réseaux

MainFrame

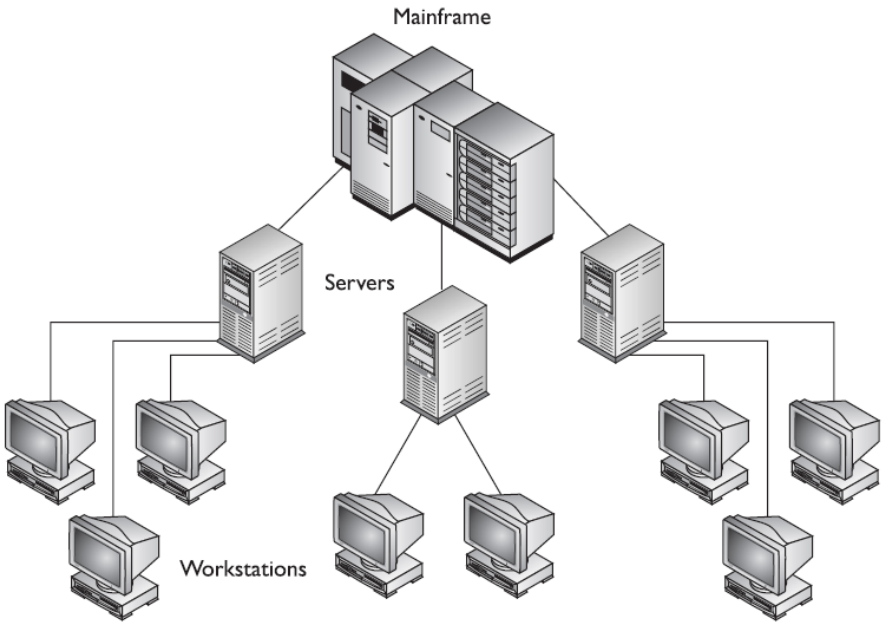


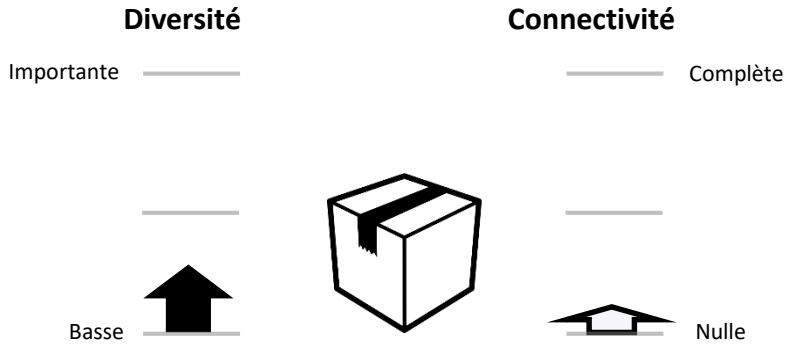


- Programme scientifique unique
- Aucune connexion extérieure

Evolution des réseaux

MainFrame

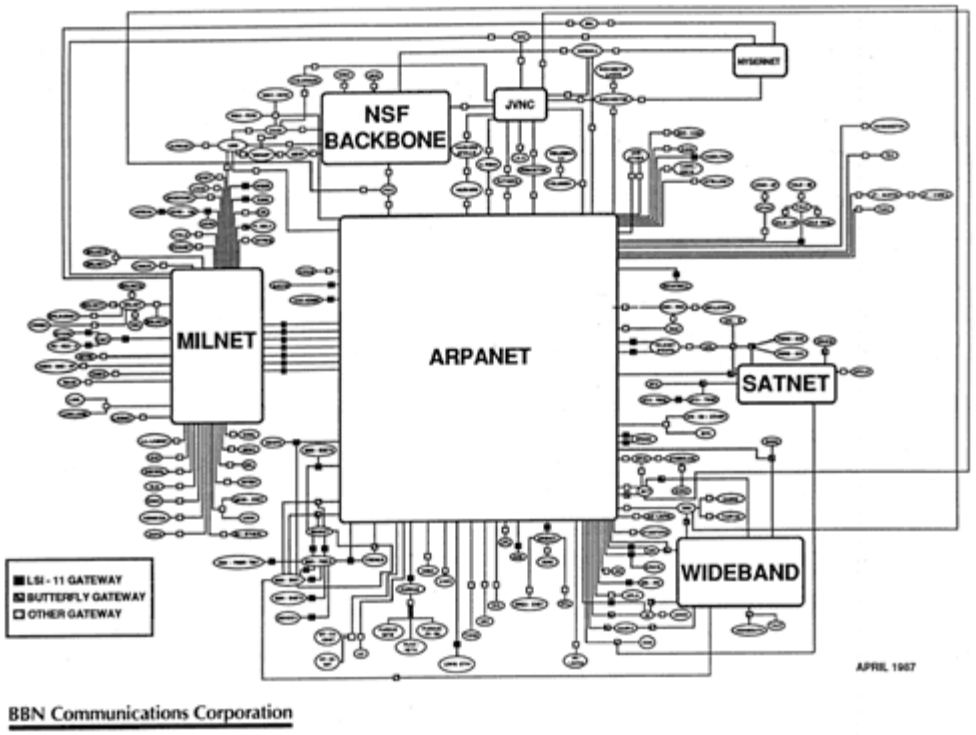


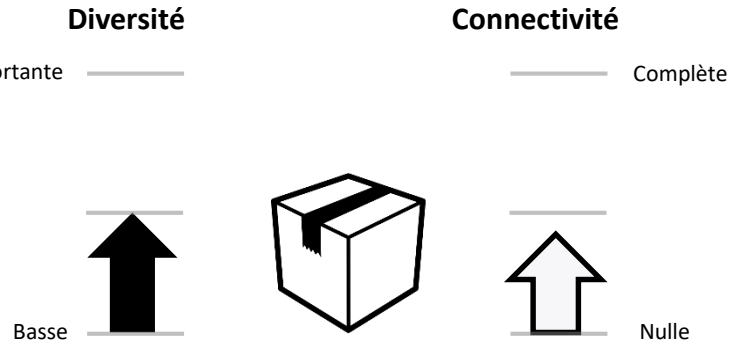


- Applications métiers dédiées
- Pas ou Peu de communication inter-applications
- Communication entre Mainframe – Server - Workstation

Evolution des réseaux

ARPANET (1983)

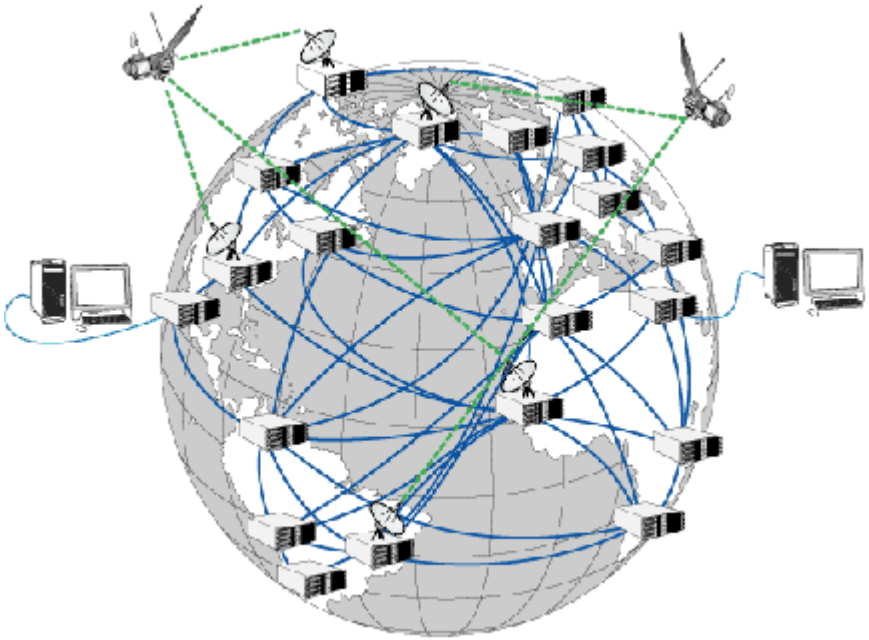


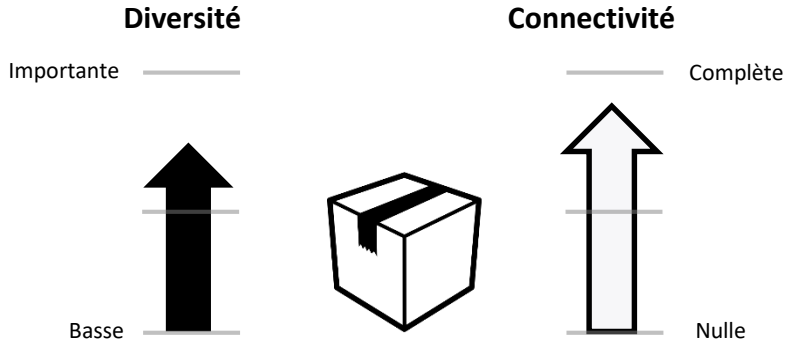


- Elargissement des applications (Bulletin Board System BBS, client Email, Usenet)
- Début TCP/IP, comm. Inter-applications en pleine croissance

Evolution des réseaux

Internet (2000)

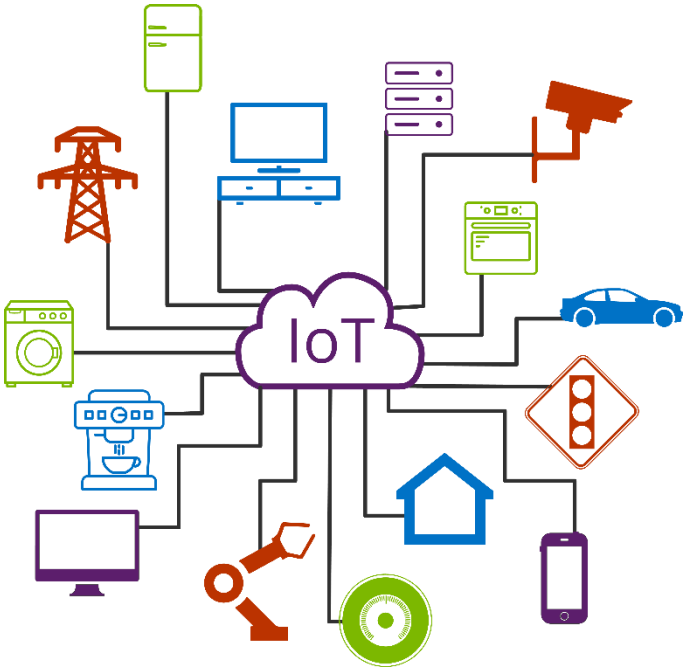




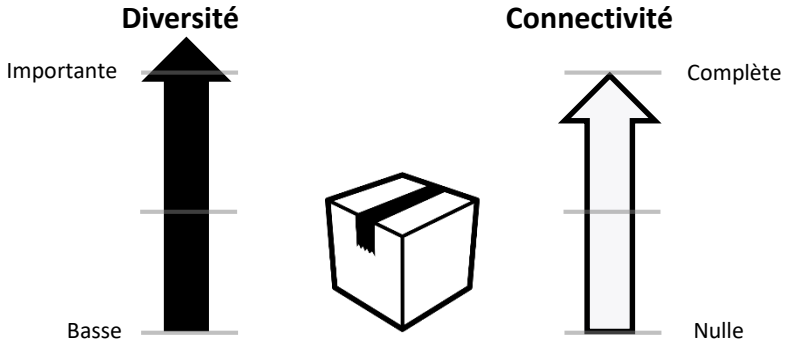
- Multiplication des applications commerciales, éducatives
- Communications inter-applications élevées
- HTTP/HTML, IRC, SSL , Corba

Evolution des réseaux

Internet – IoT

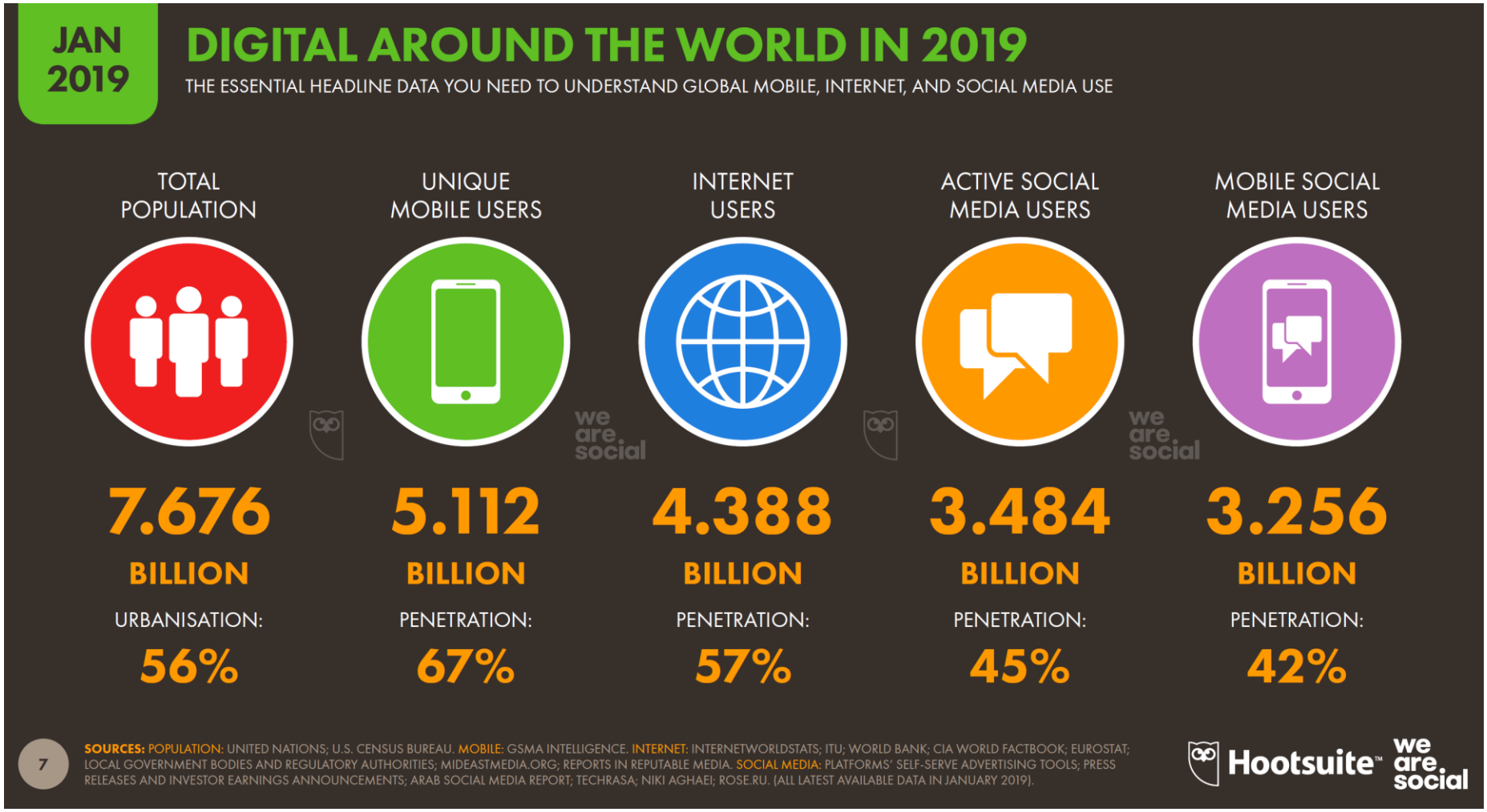


http://www.iowacomputergurus.com/Solutions/Internet-of-Things



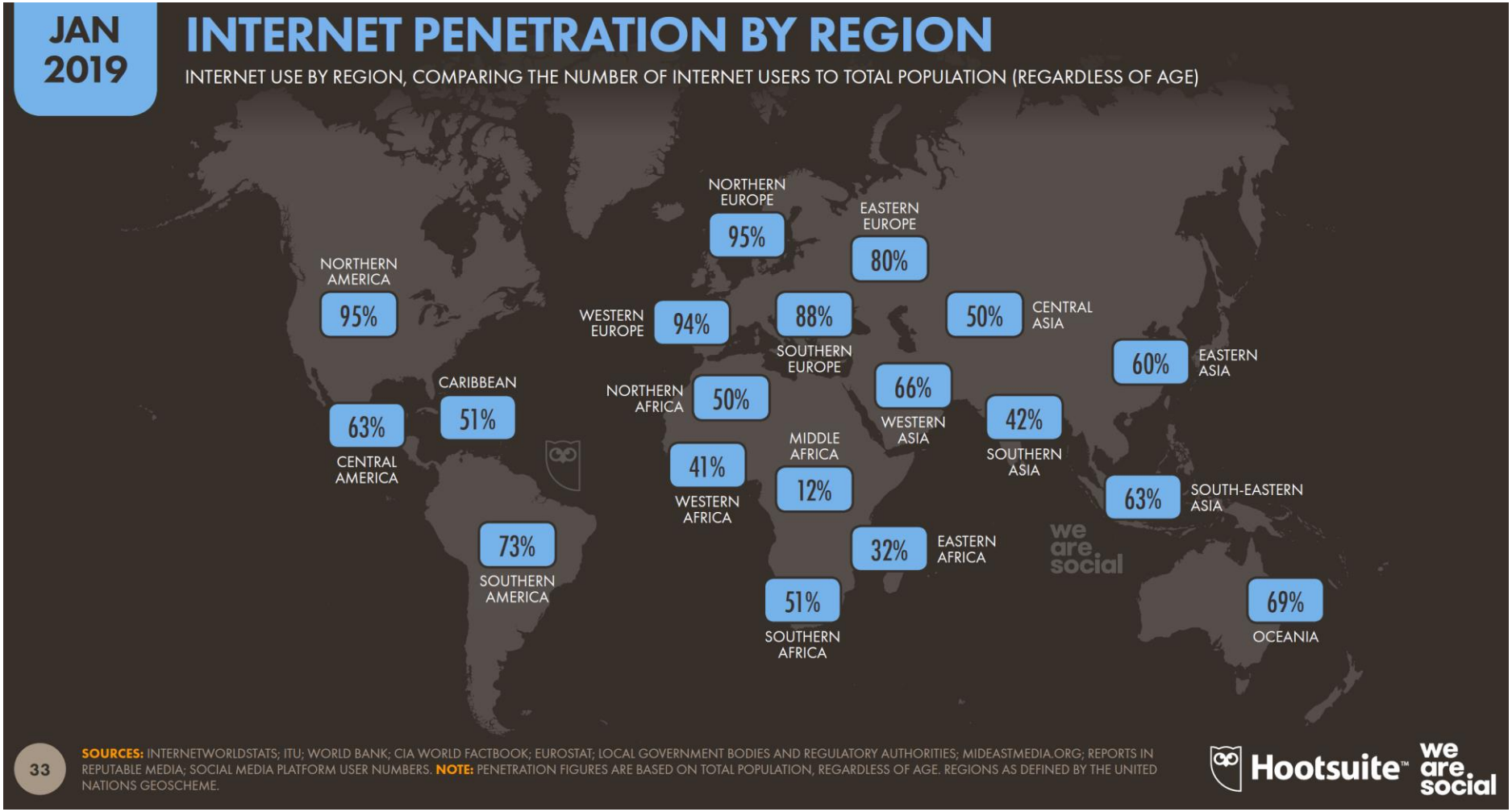
- Applications mobiles
- Cloud Computing
- Services tout en ligne (As A Service)
- Communication intensive des applications entre elles et vers internet (Big-Data, M2M)

Evolution des activités et logiciels



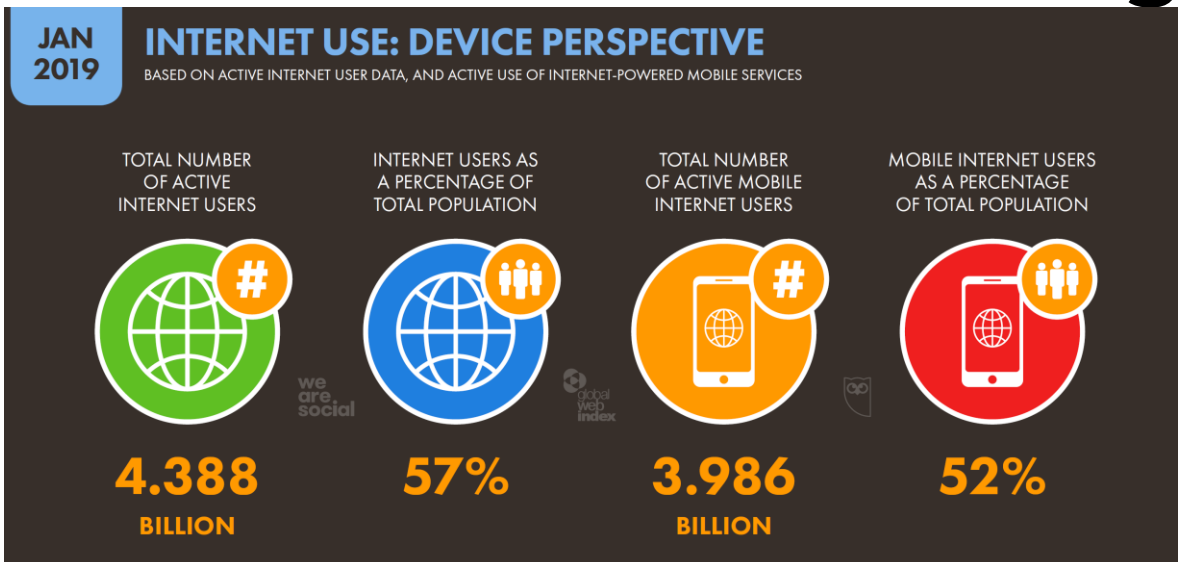
Digital in 2019: Global Overview, Hootsuite, 2019

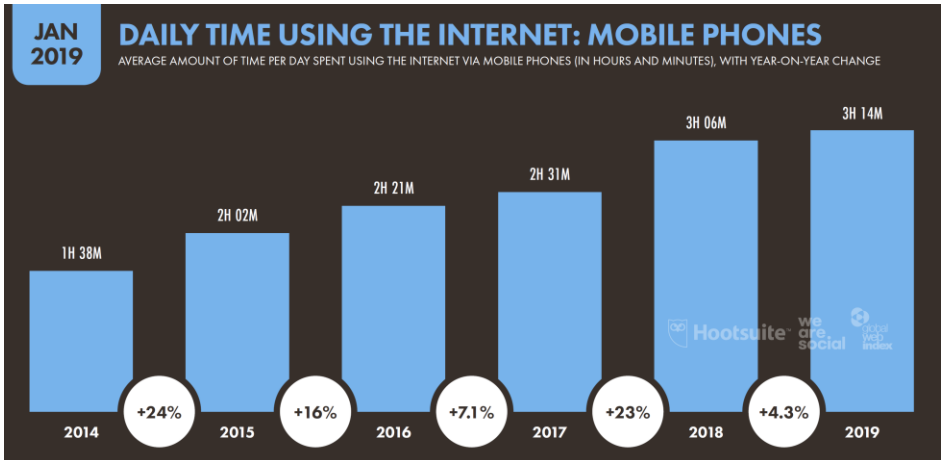
Evolution des activités et logiciels

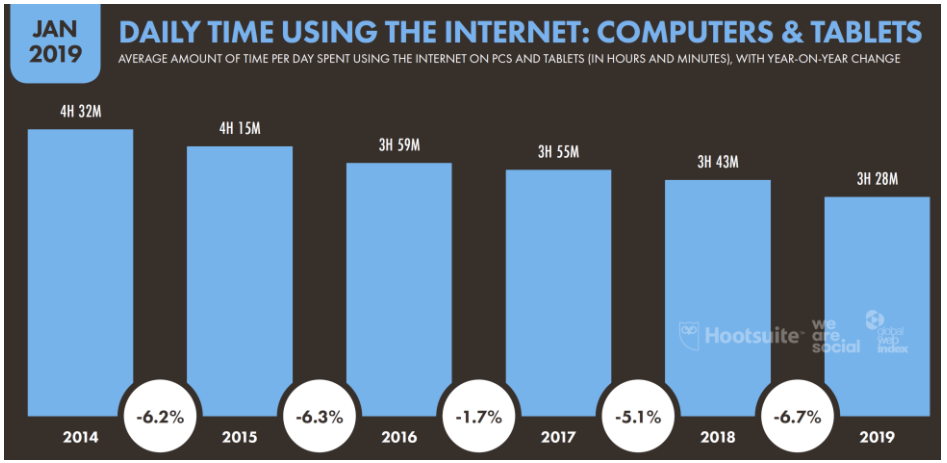


Digital in 2019: Global Overview, Hootsuite, 2019

Evolution des activités et logiciels



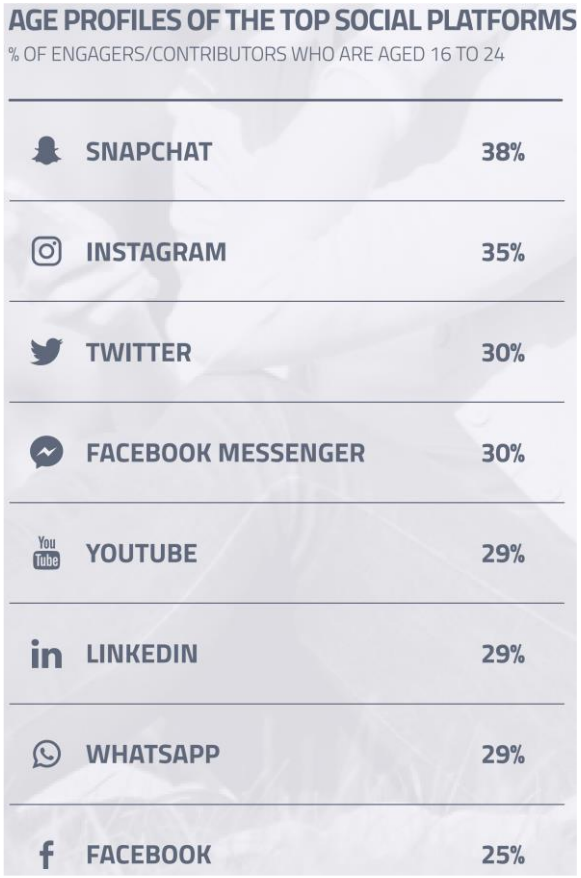


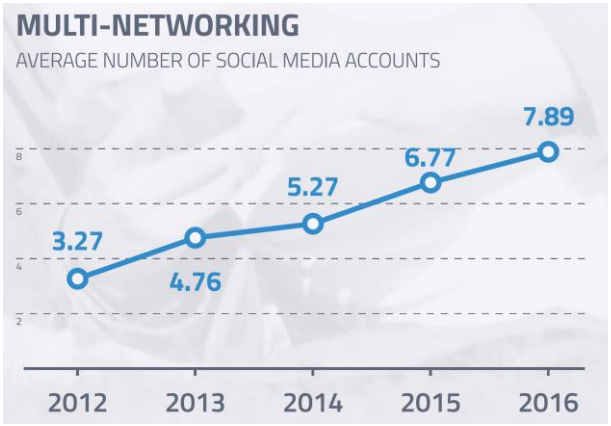


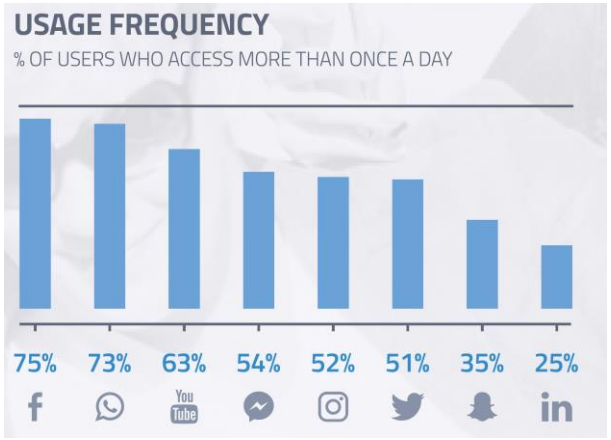
Digital in 2019: Global Overview, Hootsuite, 2019

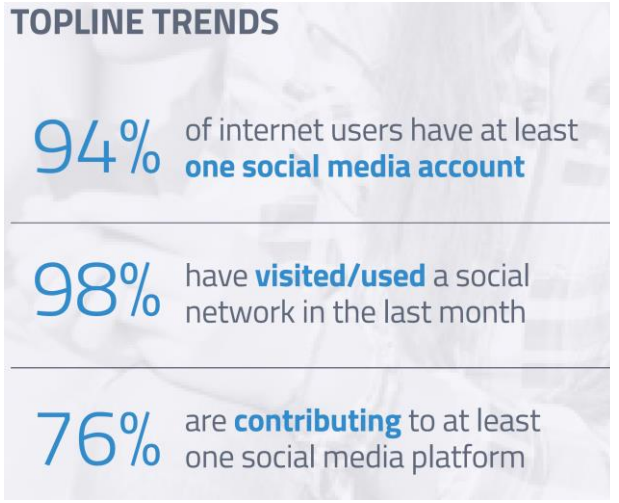
Evolution des activités et logiciels

Réseaux sociaux





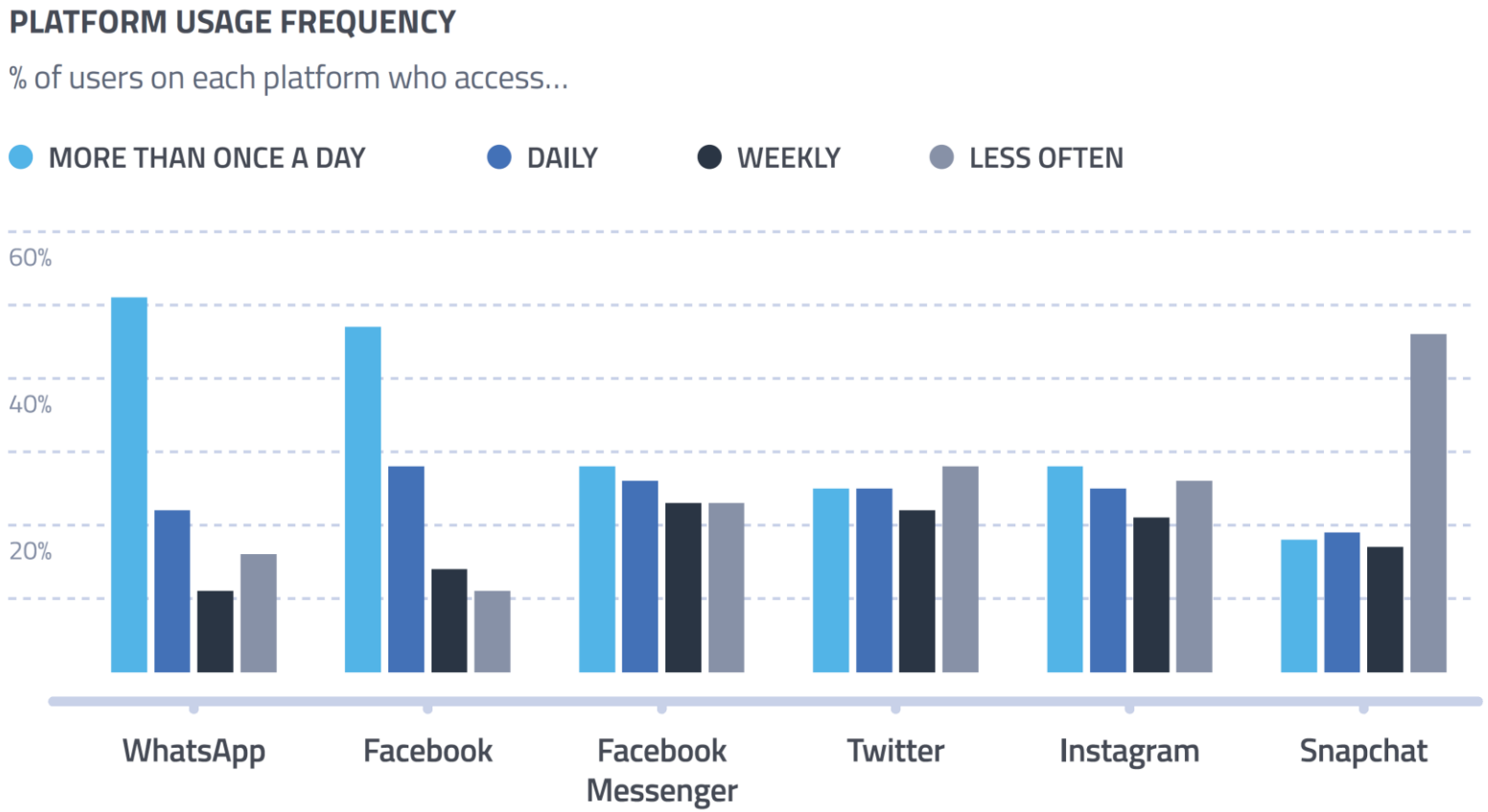




Trends 17: The Trends to watch in 2017, Globalwebindex, 2017

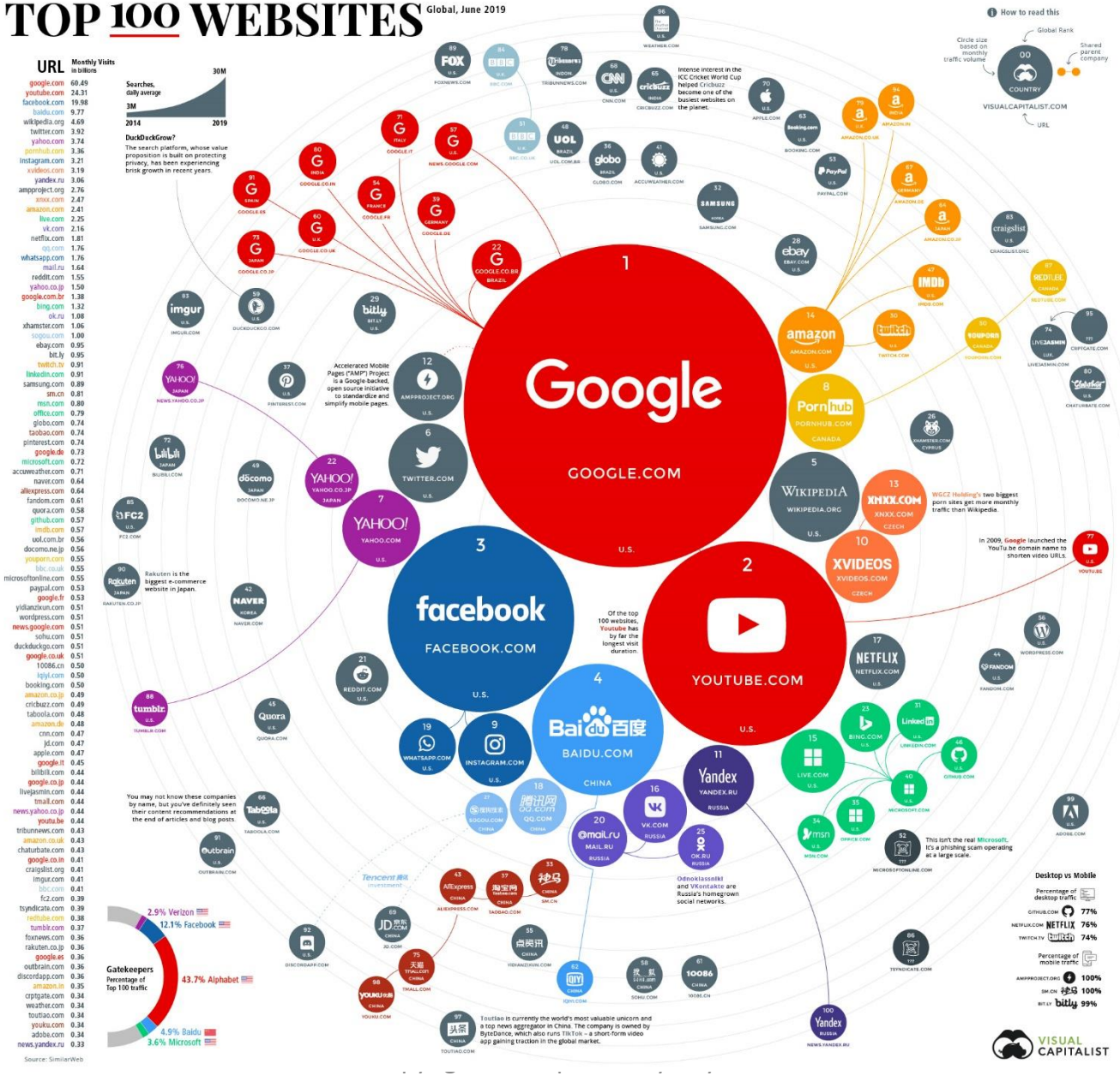
Evolution des activités et logiciels

Réseaux sociaux



Trends 17: The Trends to watch in 2017, Globalwebindex, 2017

Evolution du monde informatique

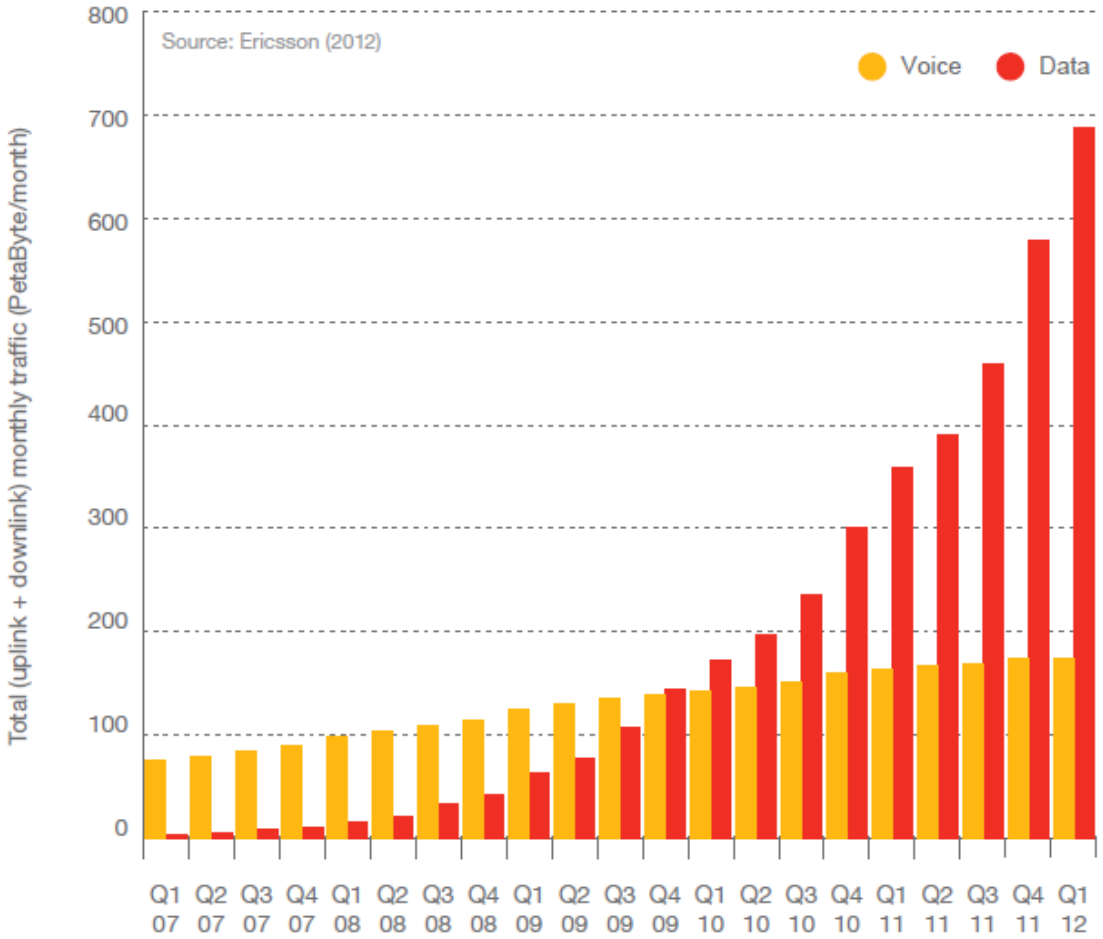


https://www.visualcapitalist.com/wp-content/uploads/2019/08/top-100-websites-ranking.html

Evolution des activités et logiciels

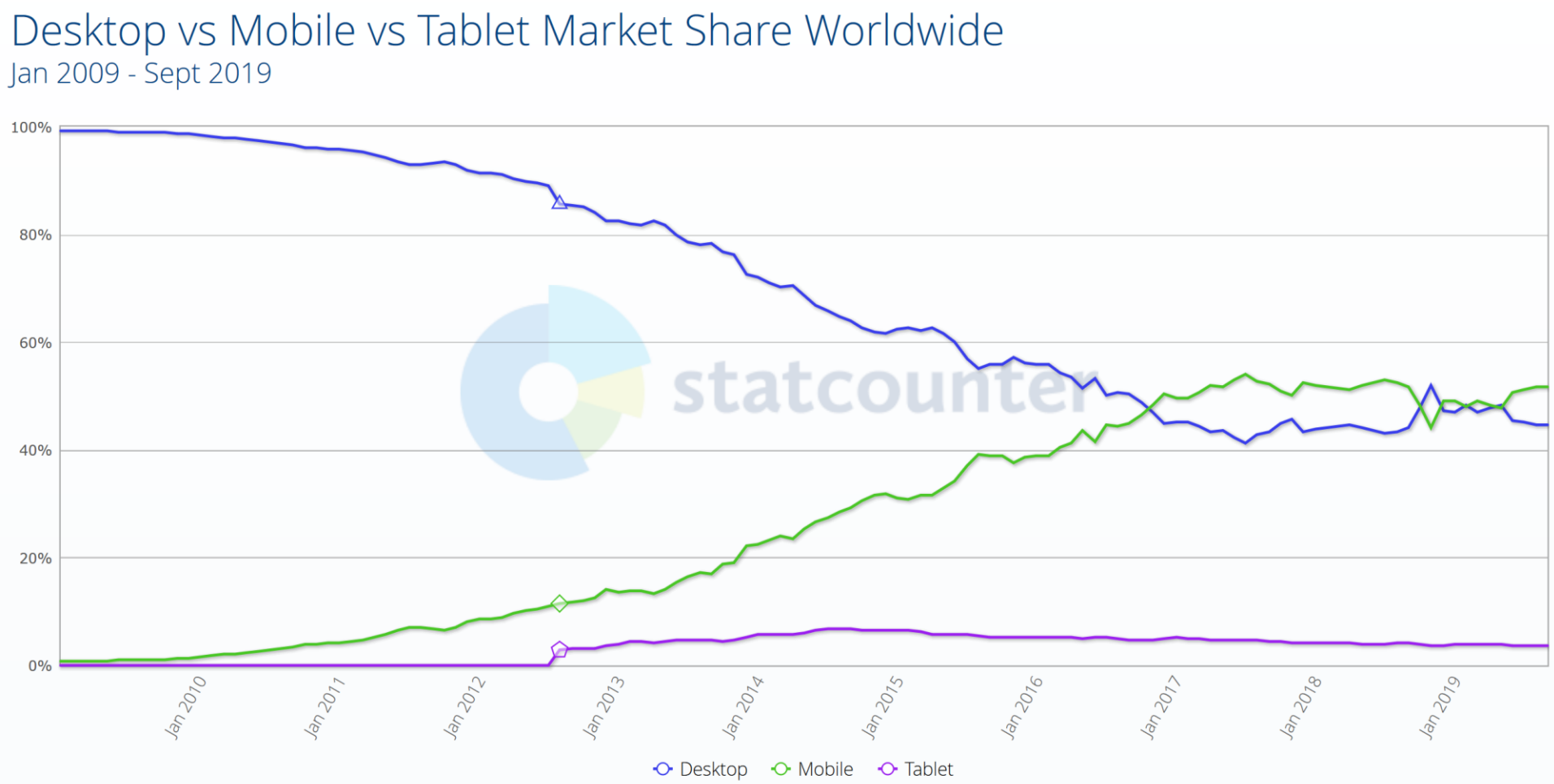
Usage des Smartphones

Figure 14: Global total traffic in mobile networks, 2007-2012



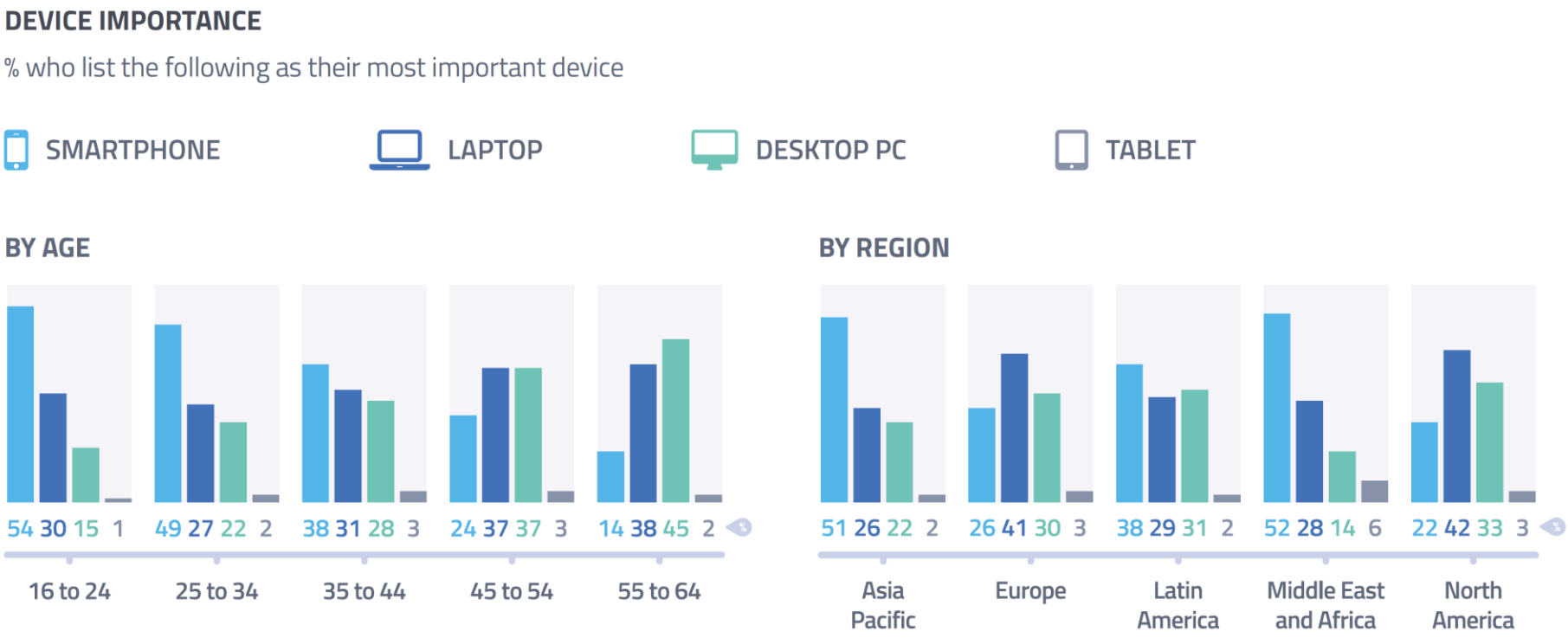
TRAFFIC AND Market report June 2012 ON THE PULSE OF THE NETWORKED SOCIETY, Ericsson

Evolution des activités et logiciels



Evolution des activités et logiciels

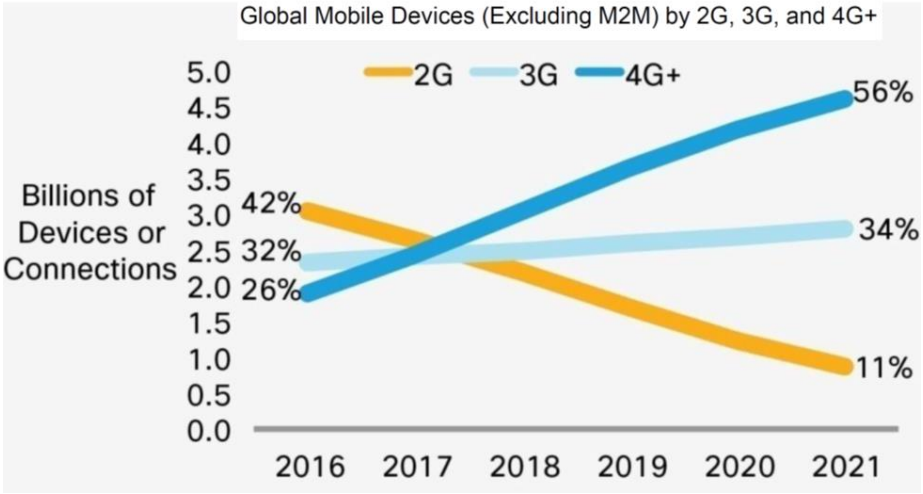
Usage des Smartphones

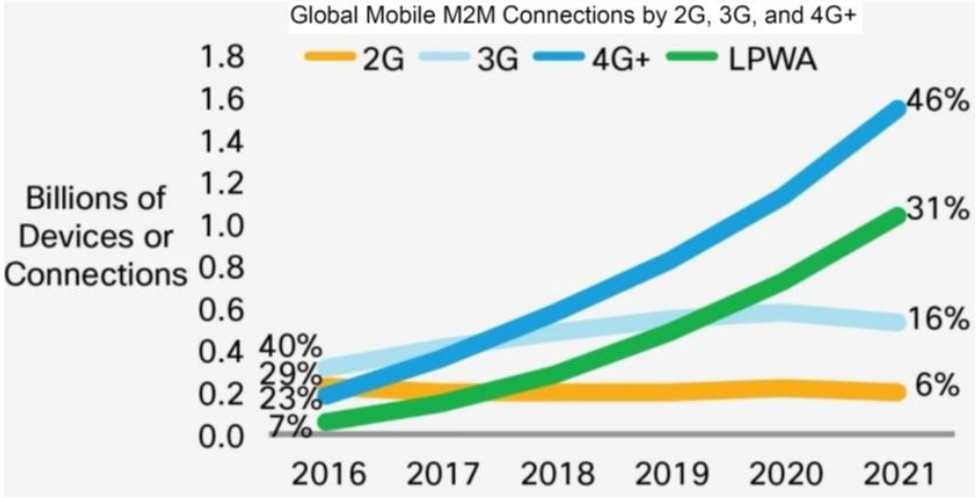


Trends 17: The Trends to watch in 2017, Globalwebindex, 2017

Evolution des activités et logiciels

Usage des Smartphones



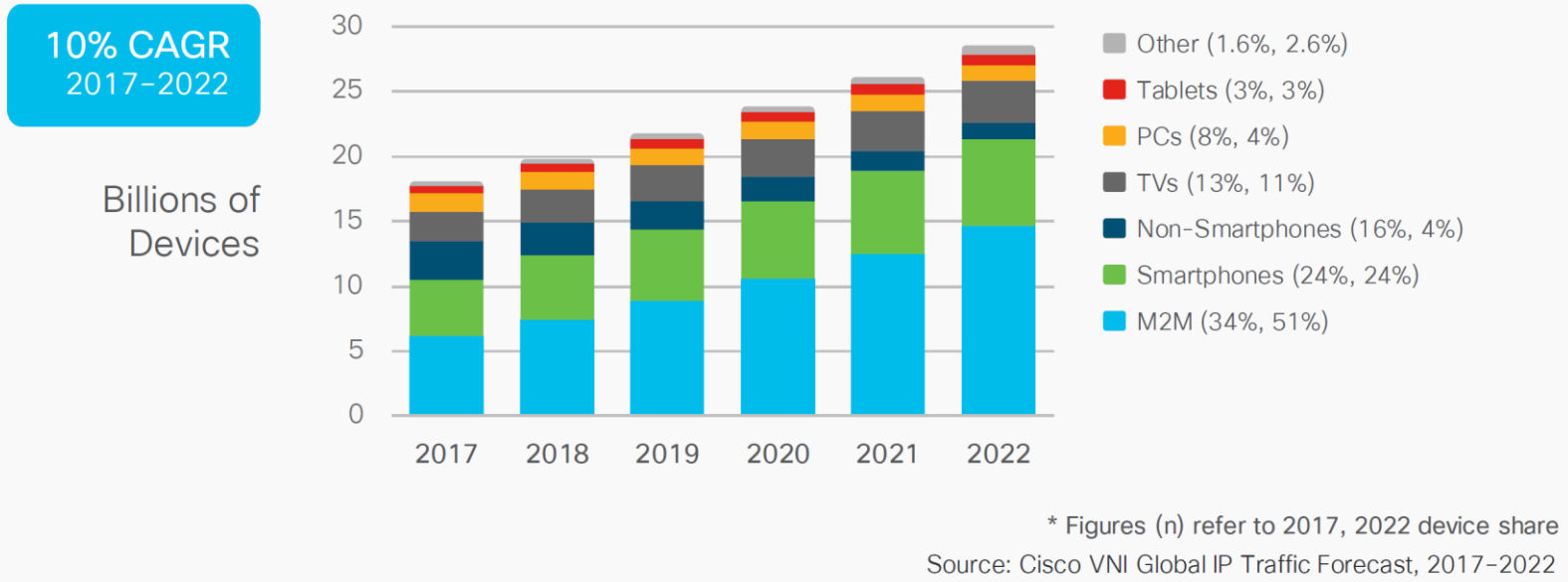


Cisco visual networking index: Global mobile Data traffic Forecast update, 2016-2021

Evolution des activités et logiciels

Usage des Smartphones

Figure 3. Global devices and connections growth



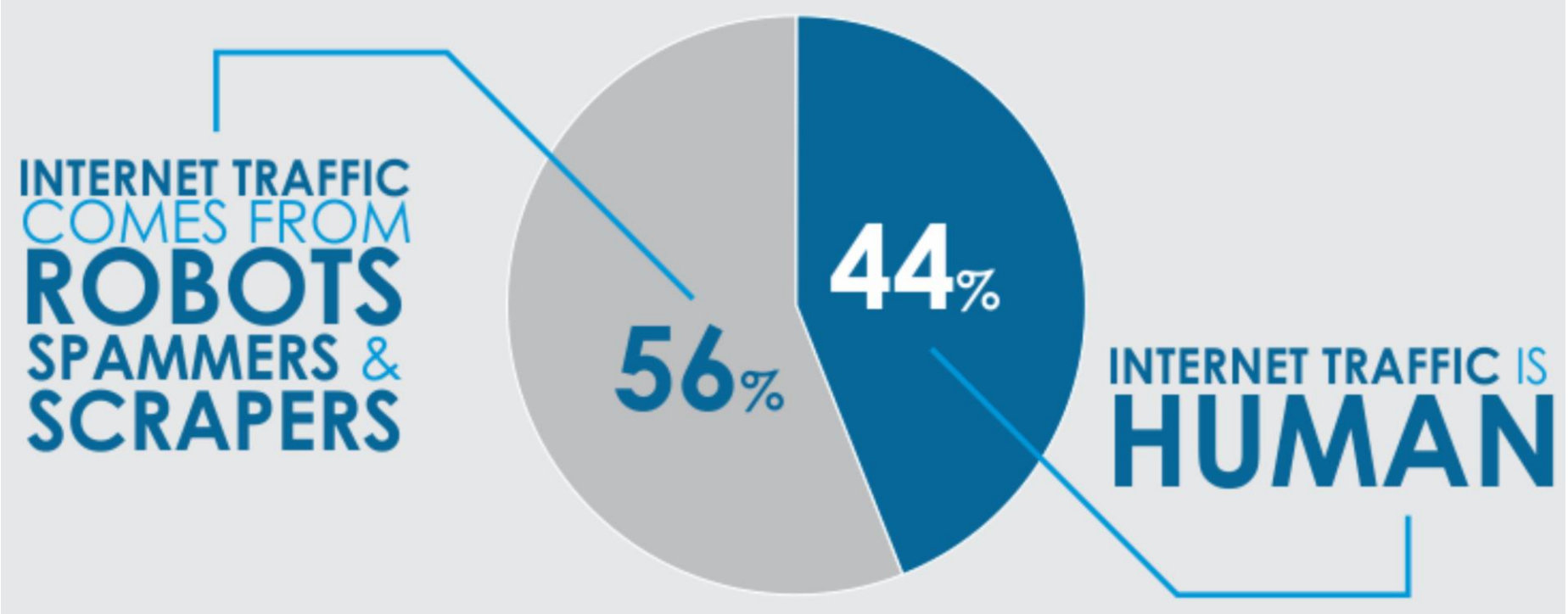
* Figures (n) refer to 2017, 2022 device share

Source: Cisco VNI Global IP Traffic Forecast, 2017–2022

https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

Evolution des activités et logiciels

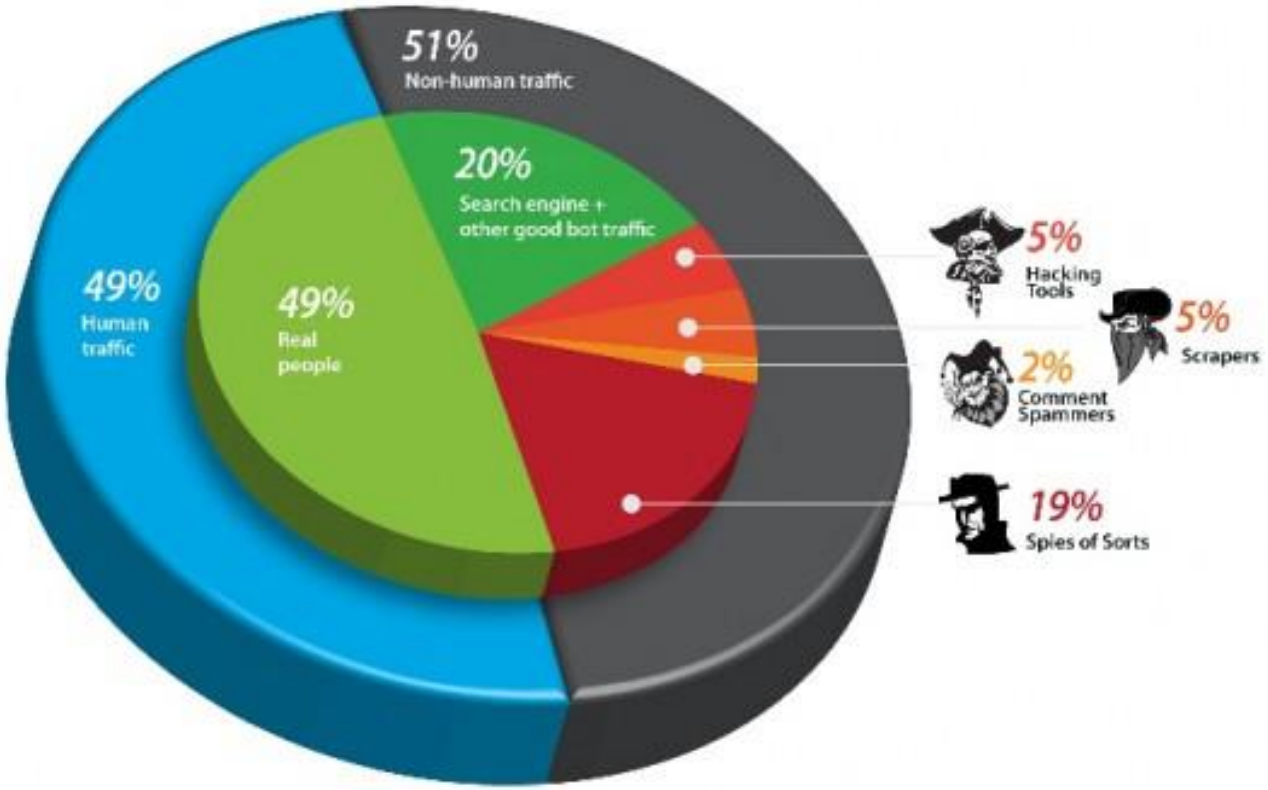
Non Human Traffic



http://www.almondsolutions.com/blog/ultimate-list-internet-e-commerce-hosting-stats-facts/

Evolution des activités et logiciels

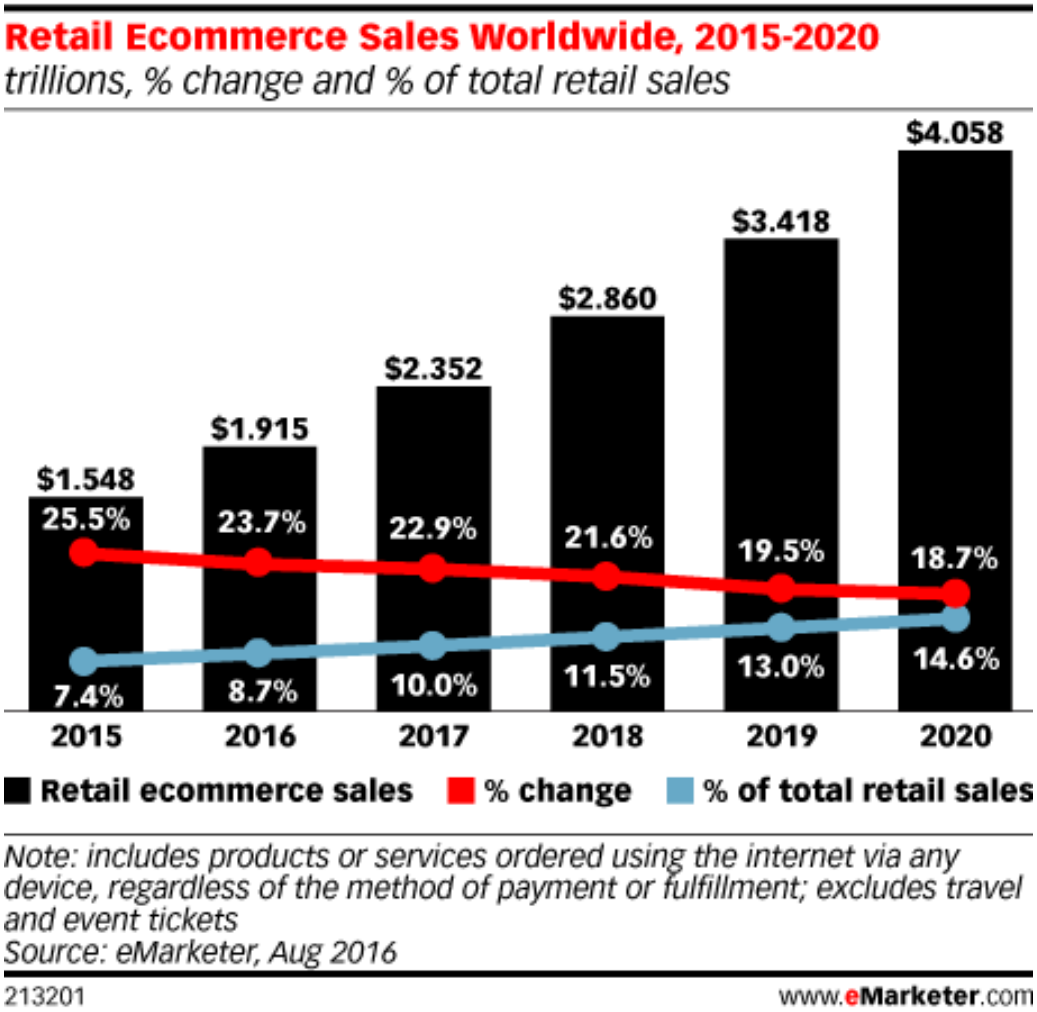
Non Human Traffic



http://www.nextnature.net/2012/03/internet-traffic-is-now-51-non-human/

Evolution des activités et logiciels

Online Transaction



Evolution des activités et logiciels

Digital in 2019: Global Overview, Hootsuite, 2019

SumUp

- Changement drastiques
  - Multiplication de la diversité des applications
  - Facilitation d'accès aux ressources
  - Multiplication des communications inter-application
- De nouveaux usages:
  - Usage massif des réseaux sociaux
  - La part du multimédia très impactant sur le réseau mondial
  - Mobile plus utilisés que Laptop/Desktop
  - Explosion des transactions M2M
- Augmentation constante des ventes sur internet /e-commerce

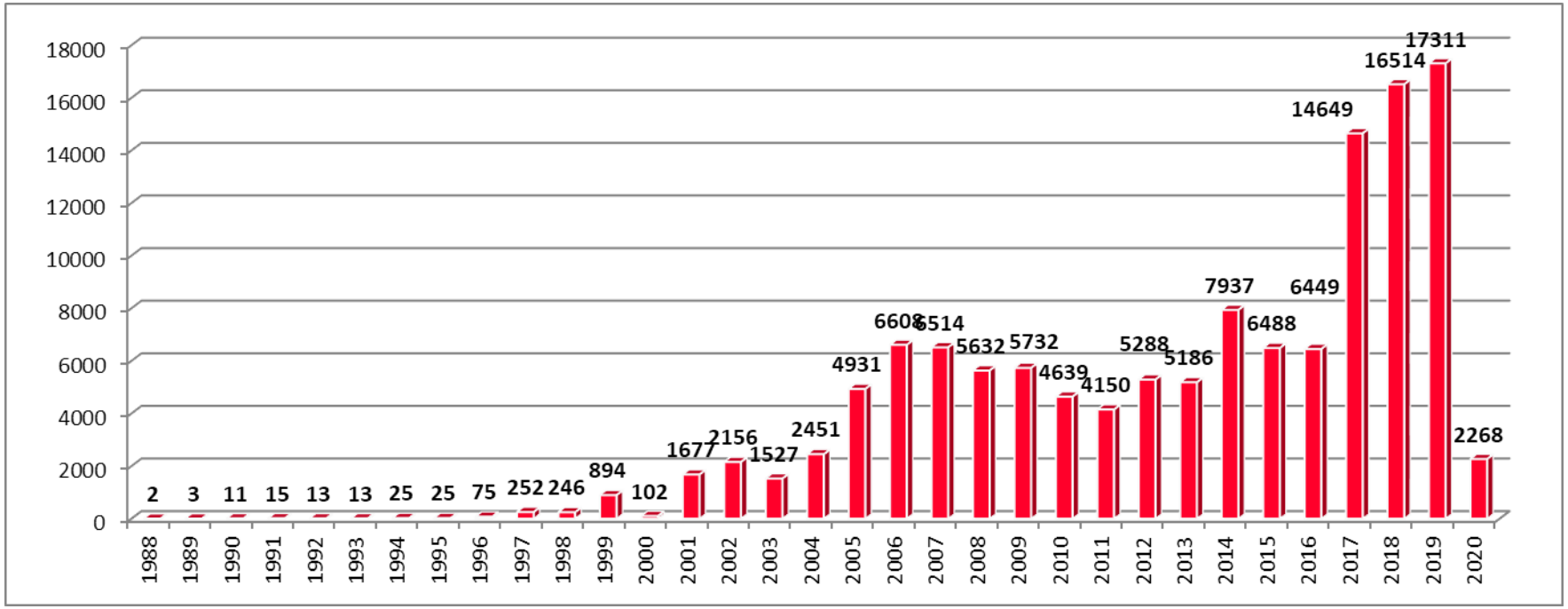
Evolution du monde informatique

- Evolution des SI
- Les Constats de sécurité

Sommes nous vulnérables ?

Sommes nous vulnérables ?

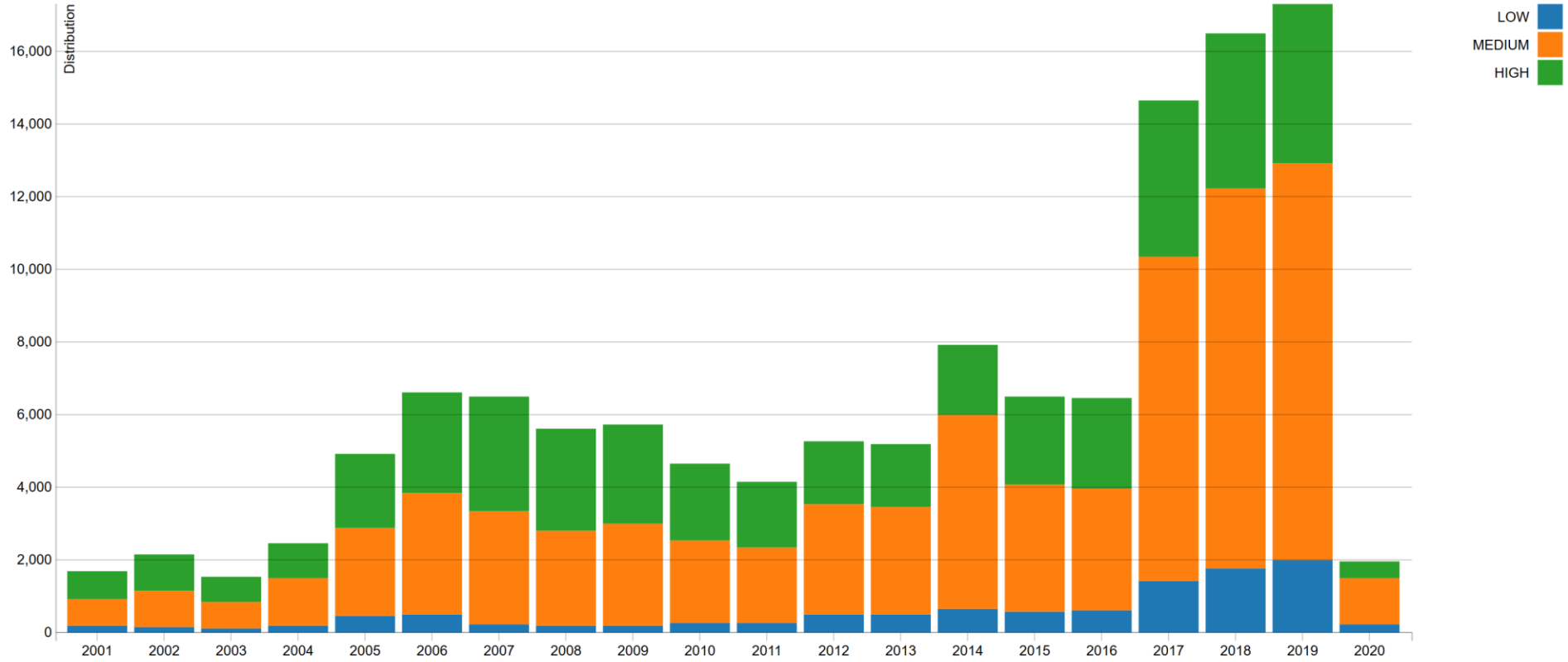
Evolution du nombre de vulnérabilités



http://web.nvd.nist.gov

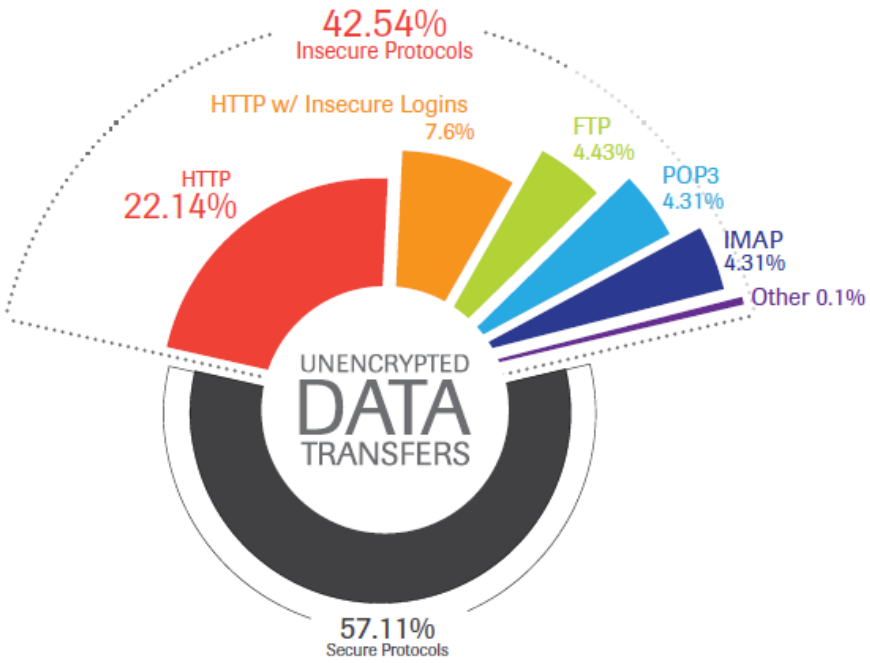
https://informationisbeautiful.net/visualizations/million-lines-of-code/

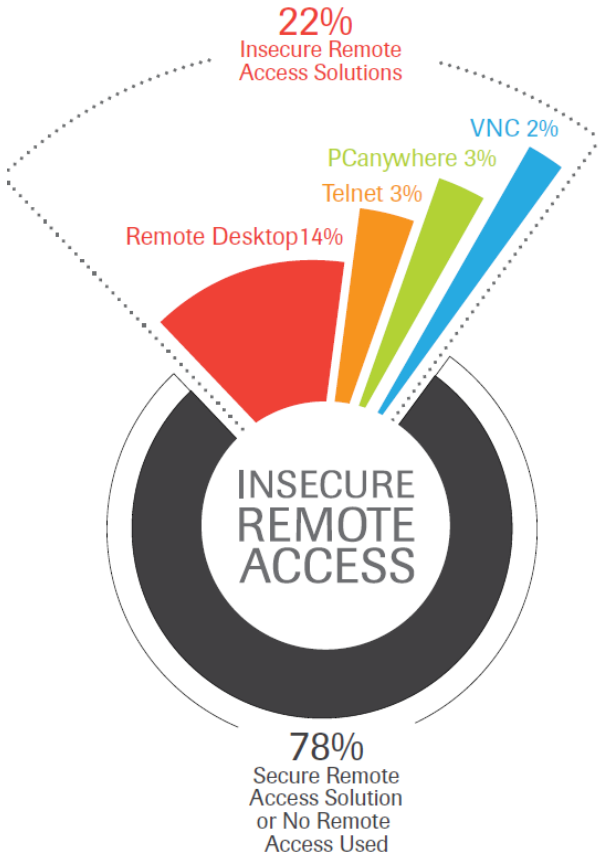
Sommes nous vulnérables ?



https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

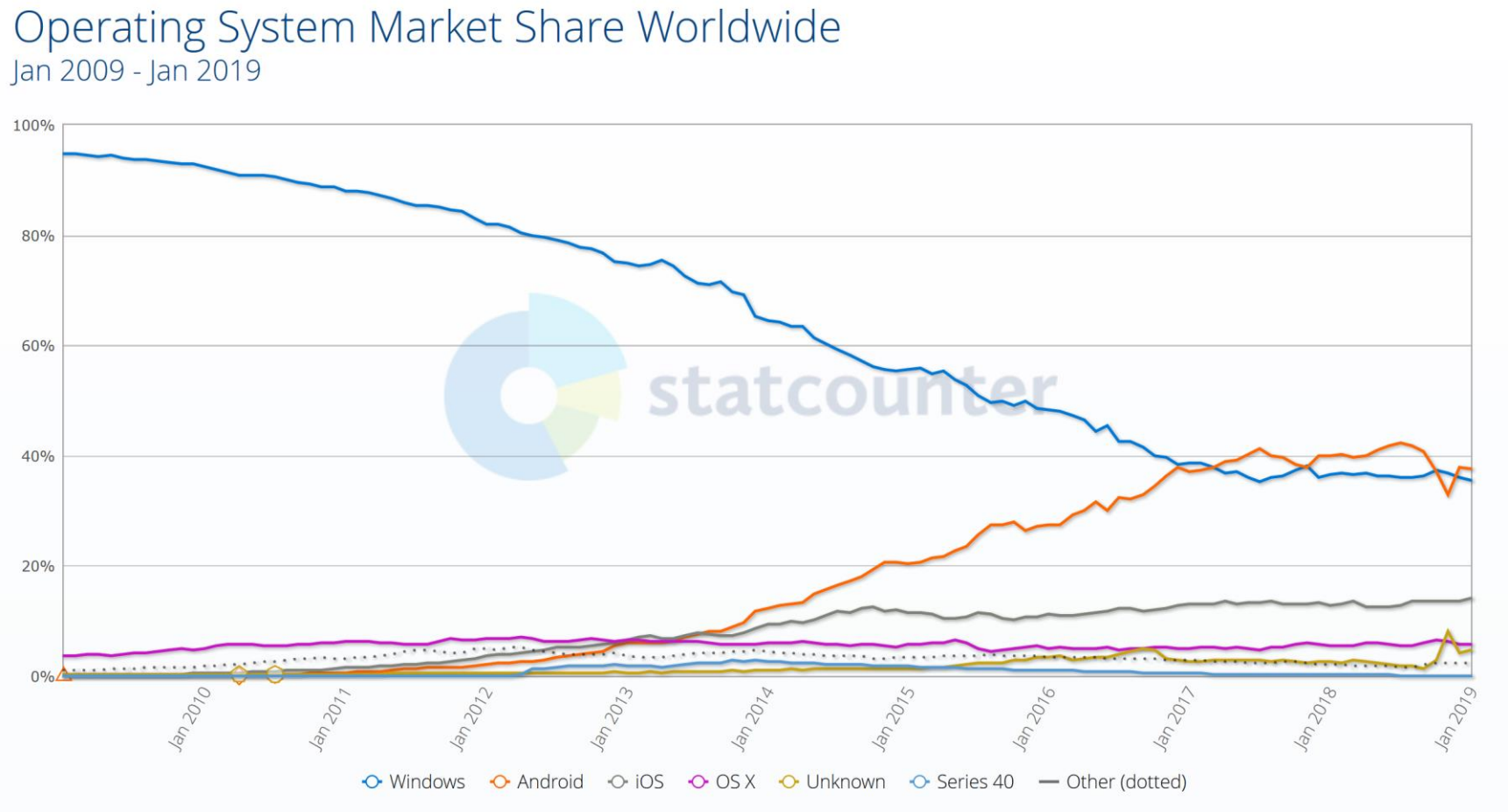
Sommes nous vulnérables ?



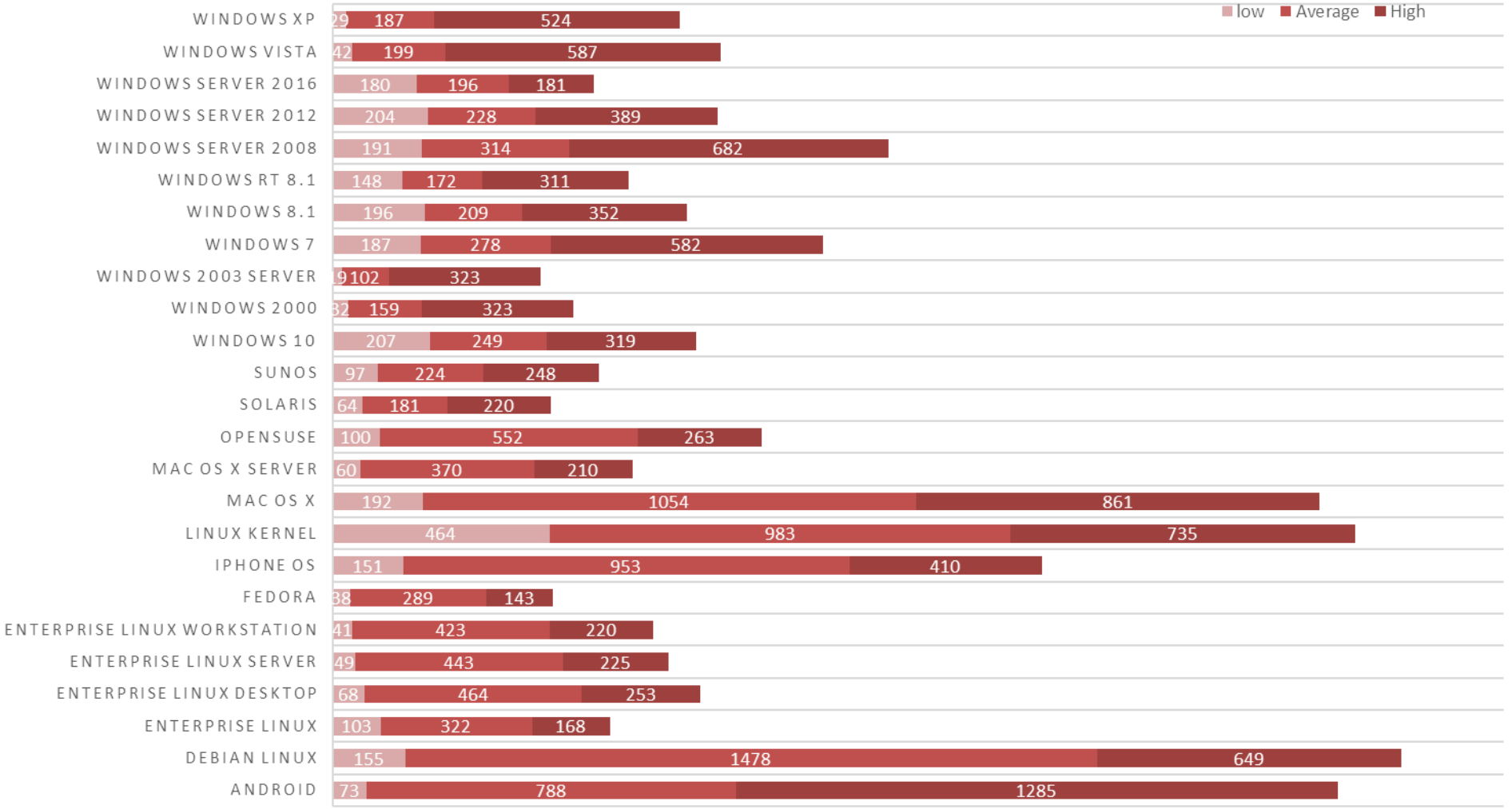


TrustWave 2012 Global Security Report

Sommes nous vulnérables ?



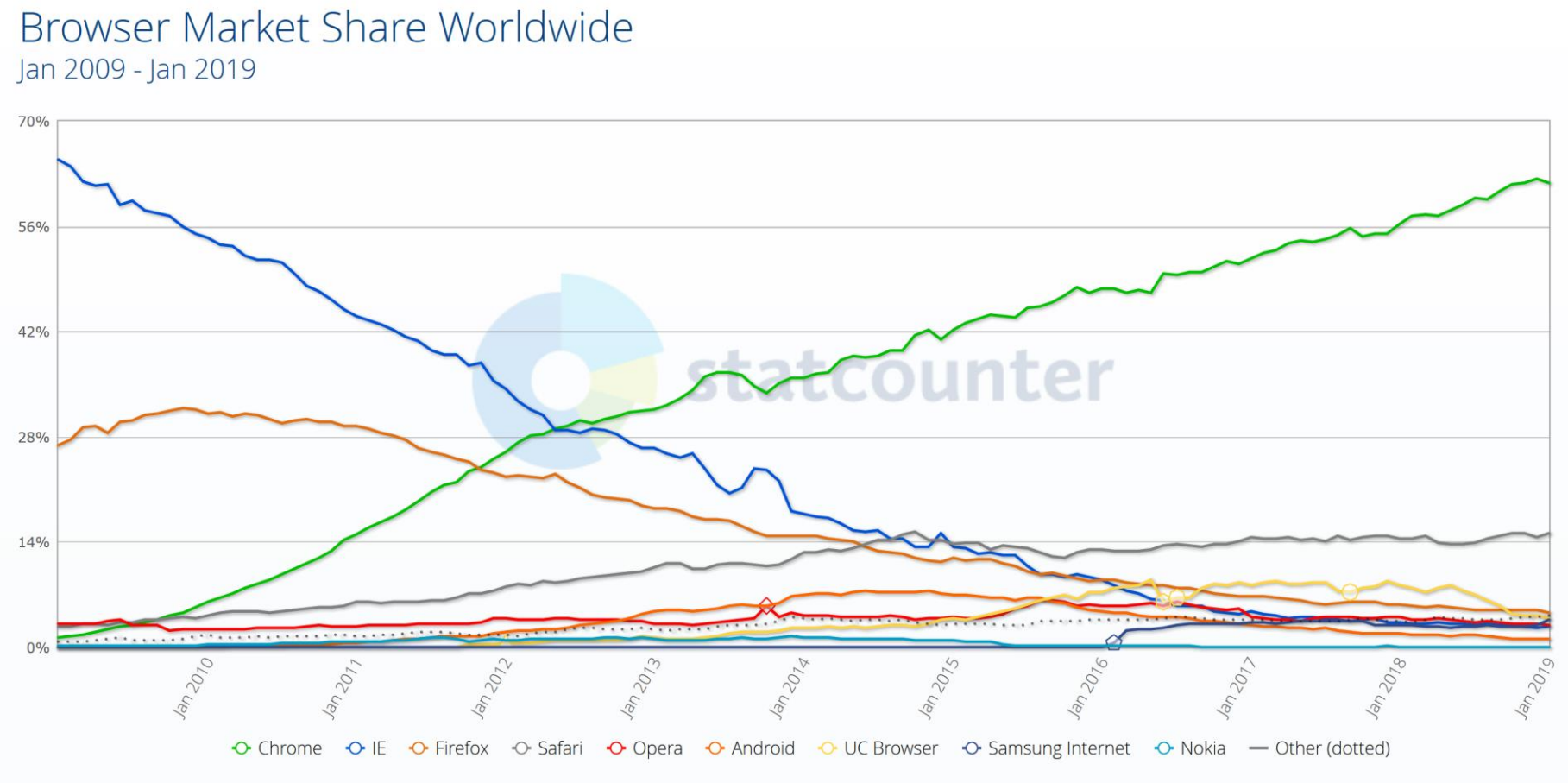
Sommes nous vulnérables ?



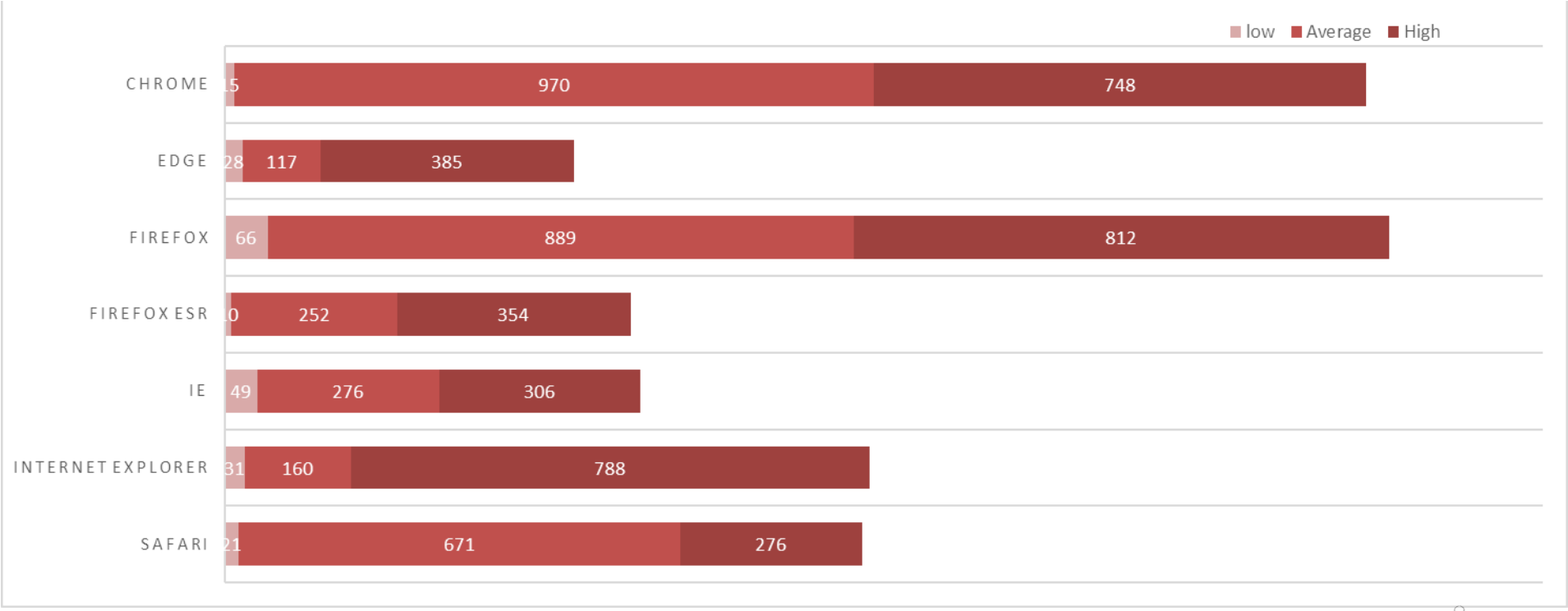
Low = CVSS Score [0-3], Medium CVSS Score[4-6]; Heigh CVSS Score[7-9]

https://www.cvedetails.com/top-50-product-cvssscore-distribution.php

Sommes nous vulnérables ?



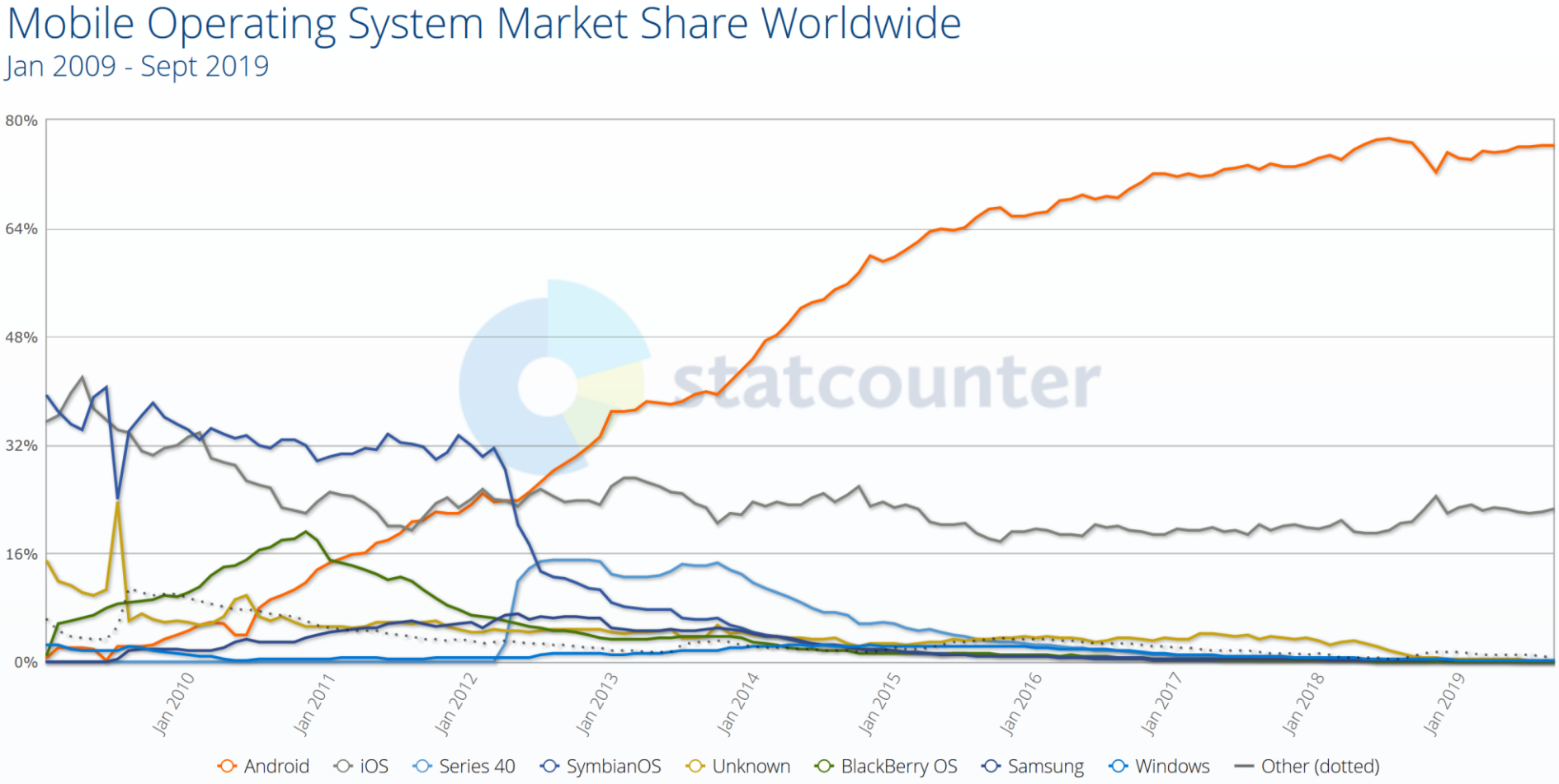
Sommes nous vulnérables ?



Low = CVSS Score [0-3], Medium CVSS Score[4-6]; Heigh CVSS Score[7-9]

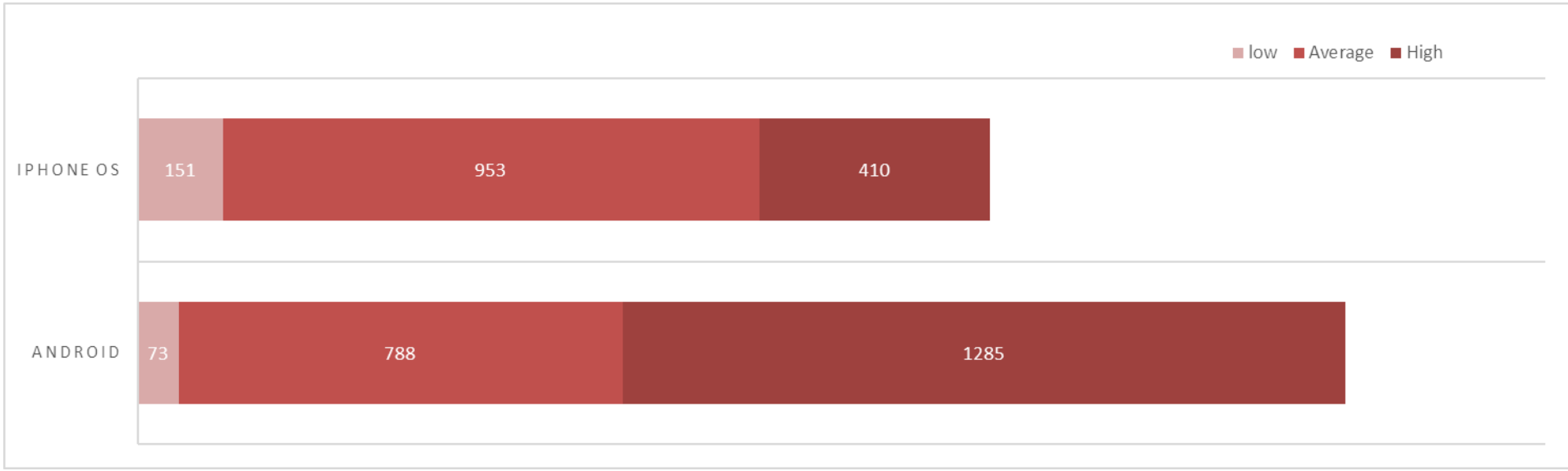
https://www.cvedetails.com/top-50-vendor-cvssscore-distribution.php

Sommes nous vulnérables ?



https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-200901-201909

Sommes nous vulnérables ?

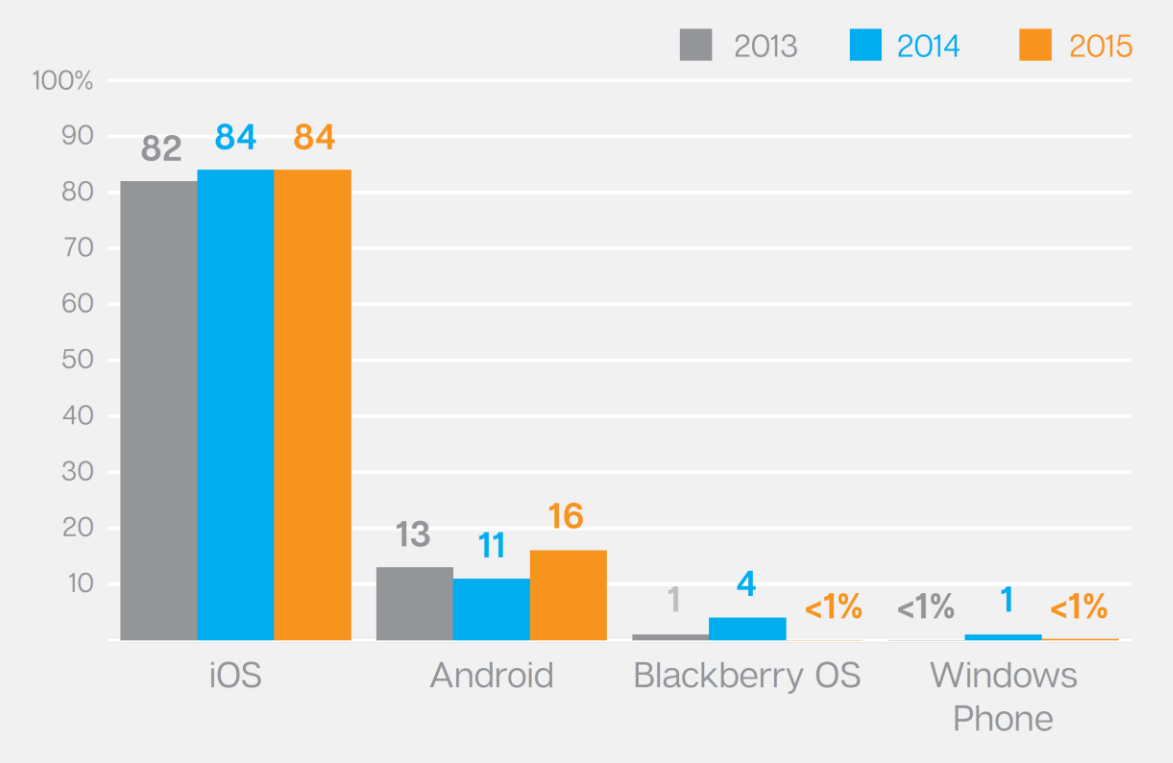


Low = CVSS Score [0-3], Medium CVSS Score[4-6]; Heigh CVSS Score[7-9]
https://www.cvedetails.com/top-50-vendor-cvssscore-distribution.php

Sommes nous vulnérables ?

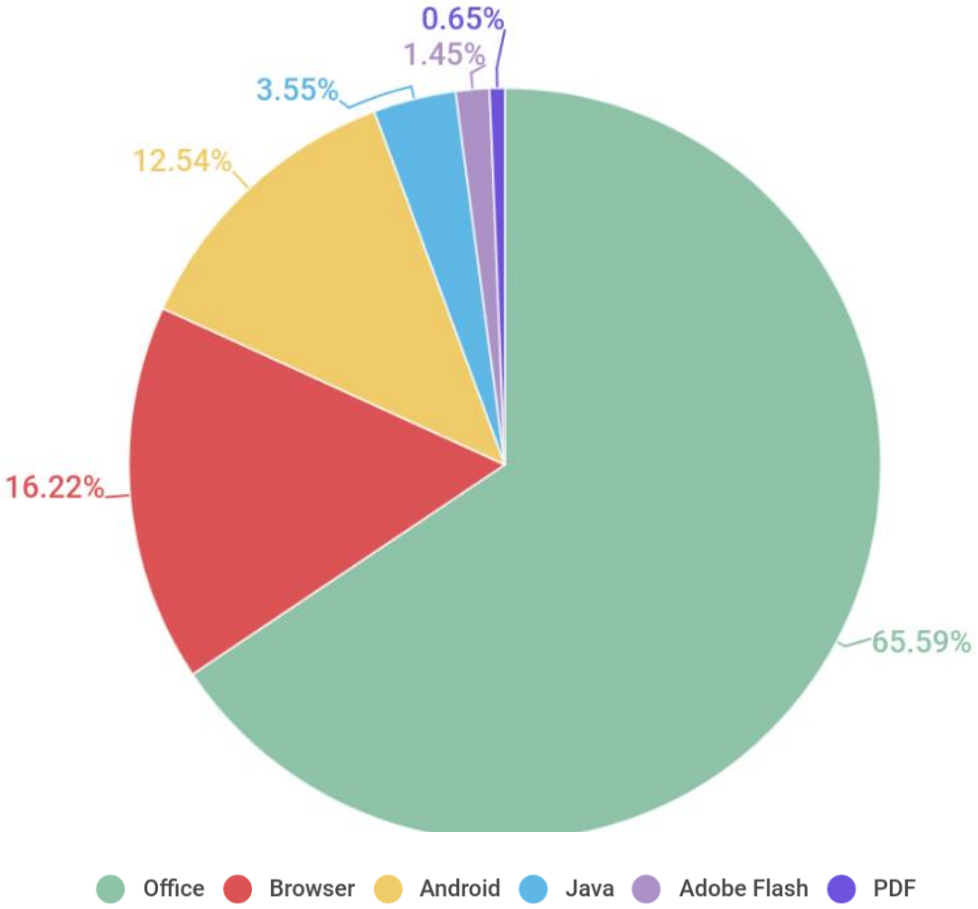
Mobile Vulnerabilities by Operating System

- *Vulnerabilities on the iOS platform have accounted for the greatest number of mobile vulnerabilities in recent years, with research often fueled by the interest to jail-break devices or gain unauthorized access to install malware.*



Symantec, ISTR, Internet Security Threat Report, 2016

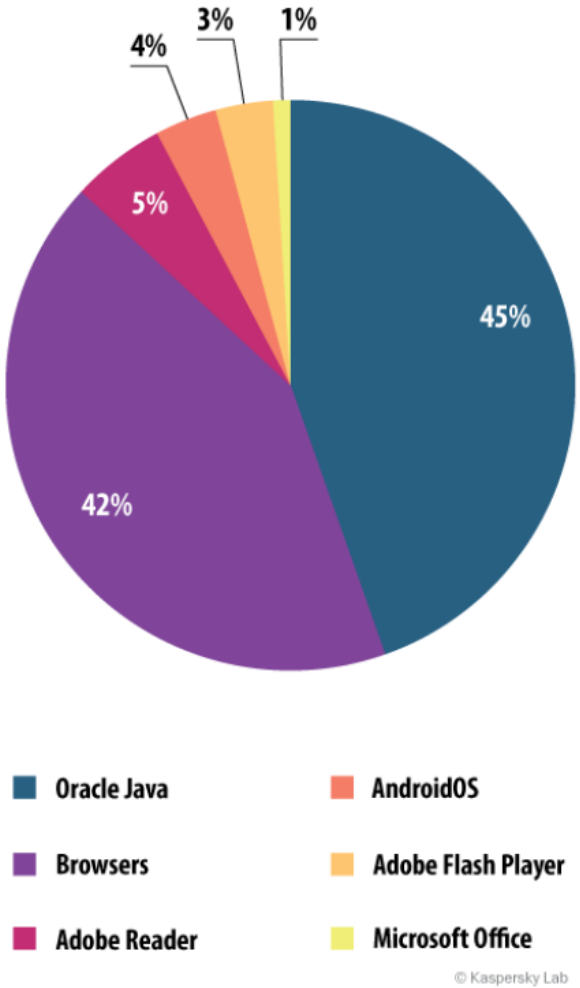
Sommes nous vulnérables ?



Malicious exploits broken down by type of target applications, November 2018 — November 2019

Kaspersky security report 2018: overall statistic

Sommes nous vulnérables ?

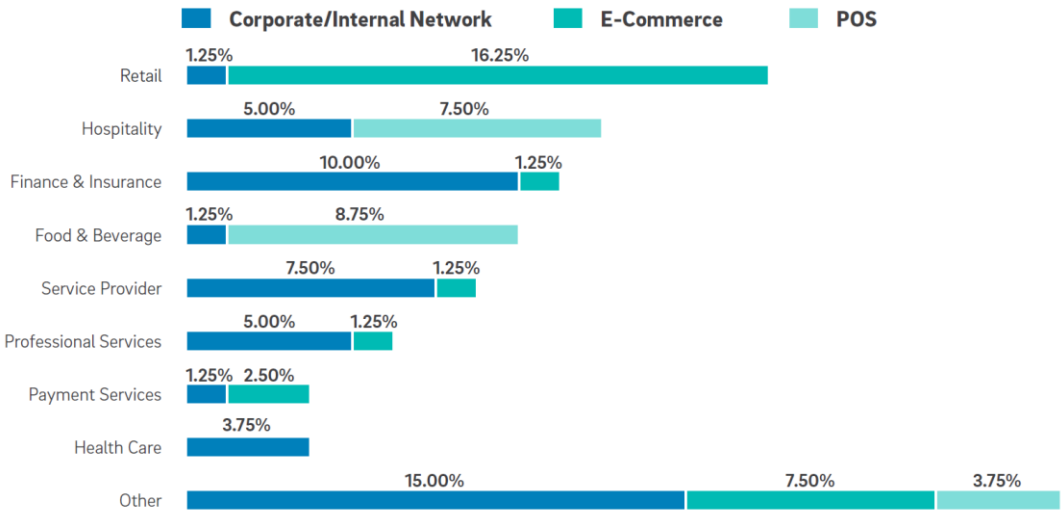


The distribution of exploits used by fraudsters, by type of application attacked, 2014

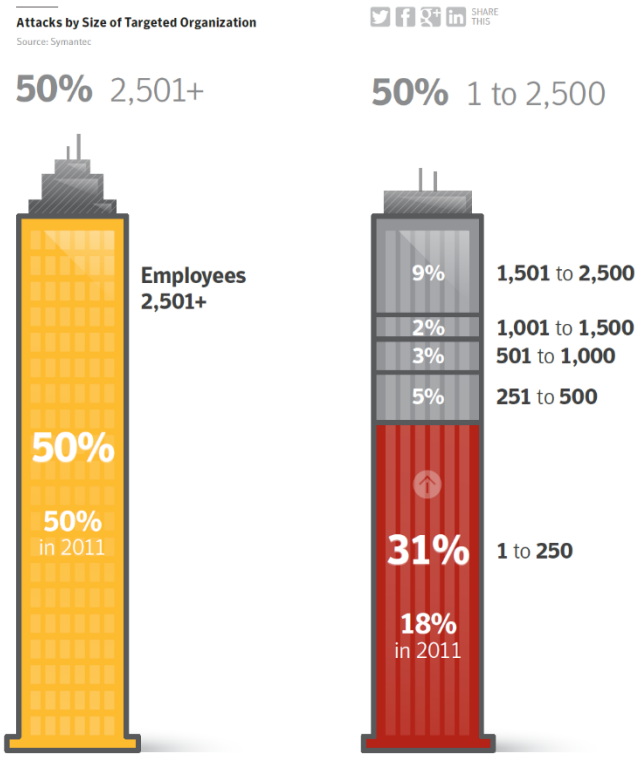
Kaspersky security report 2014: overall statistic

Qui est attaqué ?

Qui est attaqué ?



TrustWave Global Security Report 2018



Symantec INTERNET SECURITY THREAT REPORT, 2012 Trends, Volume 18, Published April 2013

Qui est attaqué ?

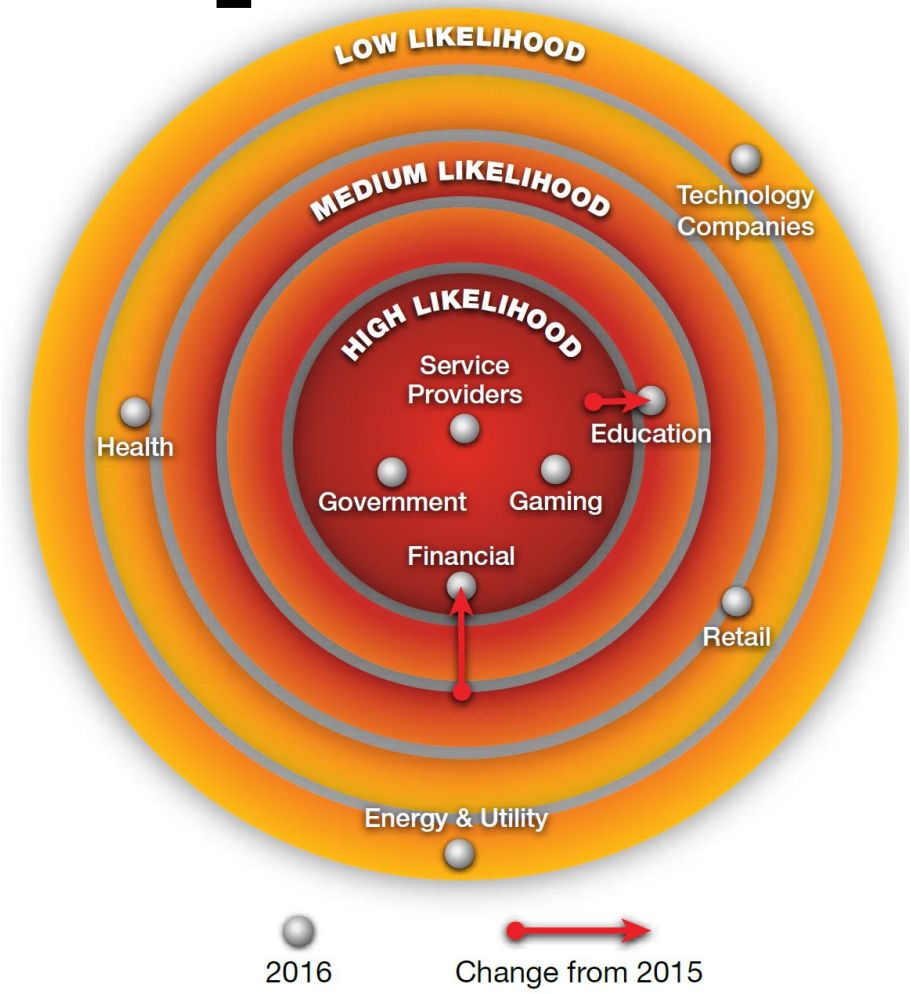
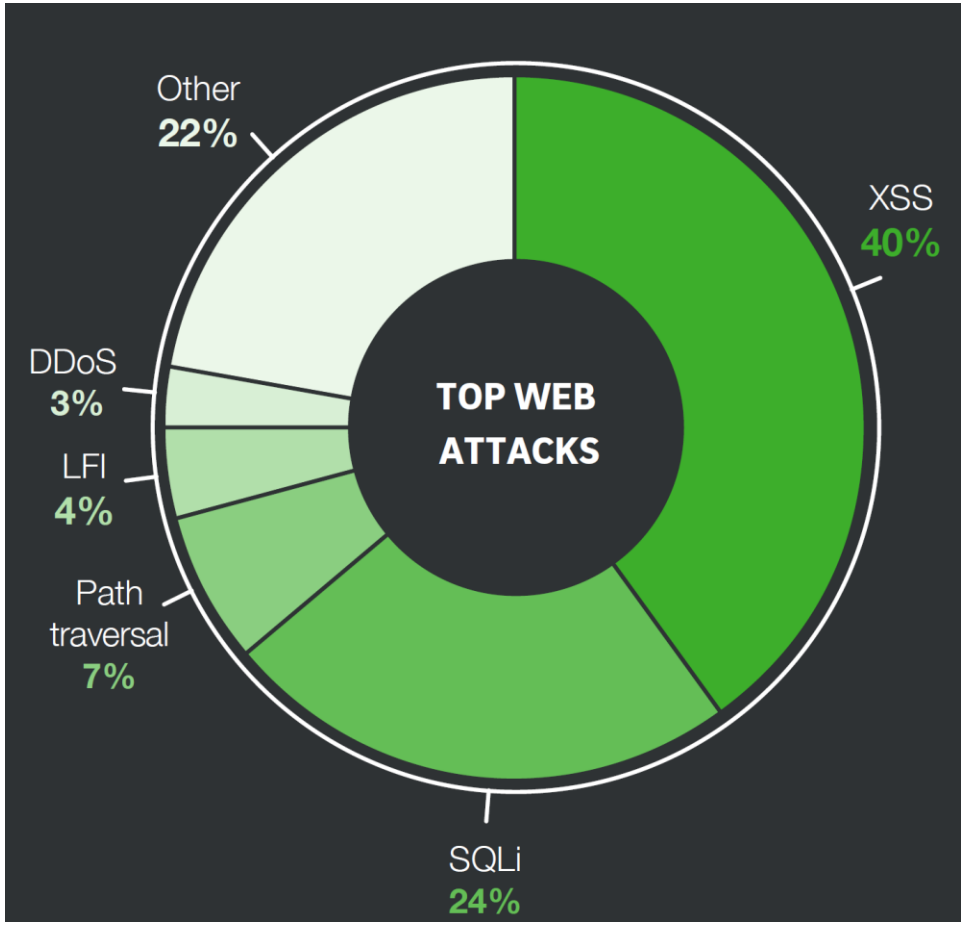


Figure 16: Cyber-Attack Ring of Fire

Radware global Application & Network Security report 2016-17

Comment nous ont-ils attaqué ?

Comment nous ont-ils attaqué?



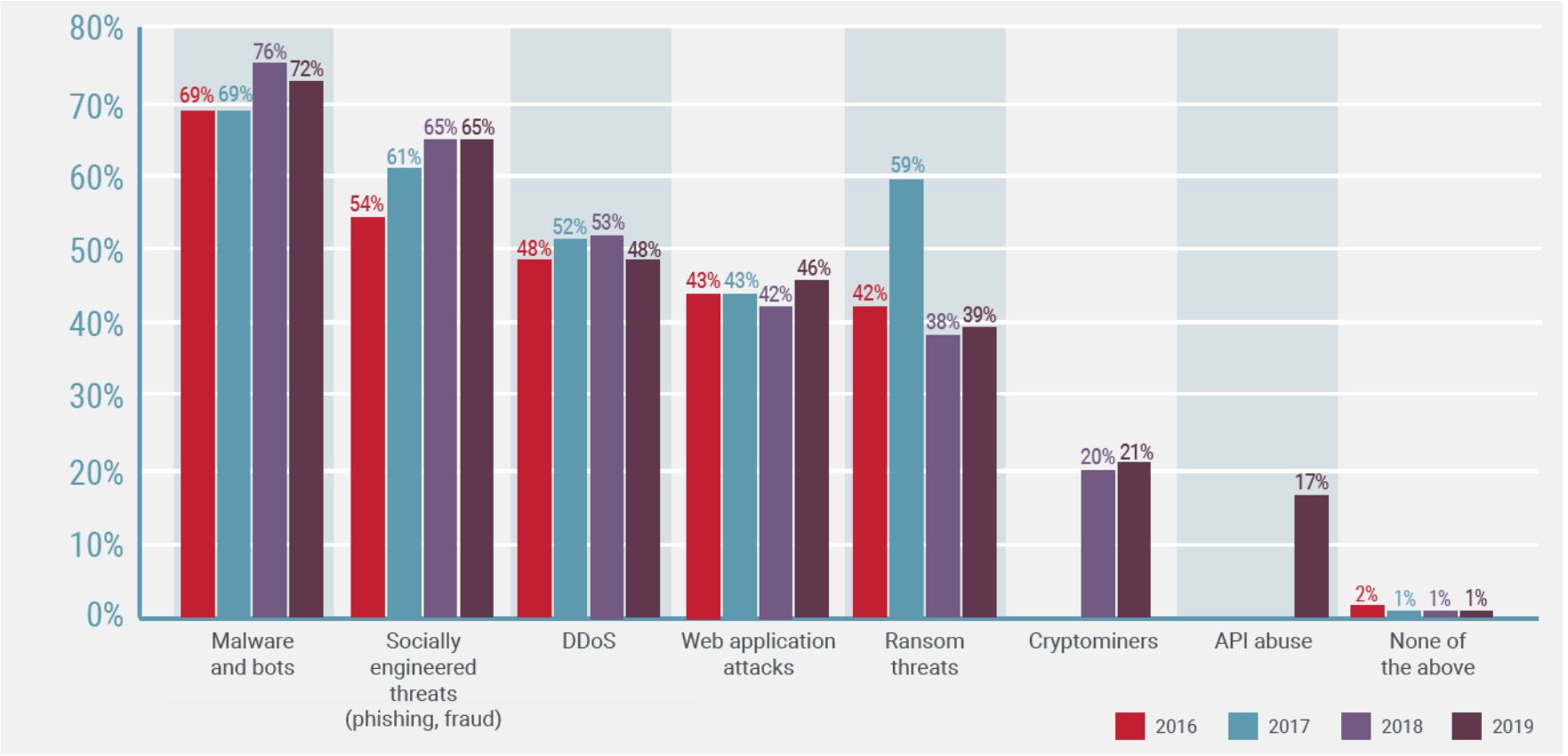
TrustWave Global Security Report 2018

Encrypted web attacks (SSL/TLS based)	50%
Data security breaches	46%
Web scraping	39%
HTTP/Layer 7 DDoS	34%
API manipulations	34%
SQL injection	34%
Cross-site scripting	32%
Credential stuffing/credential cracking	24%
None of these/no attacks experienced	11%

Figure 19. Encrypted web attacks were the most commonly reported form of application-layer attacks in 2018.

Radware global Application & Network Security report 2018-19

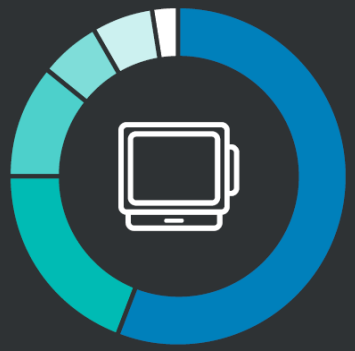
Comment nous ont-ils attaqué?



Radware global Application & Network Security report 2019-20

Comment nous ont-ils attaqué?

POS



47% Phishing/Social Engineering
23% Remote Access
13% Malicious Insider
7% Weak Password
7% Other
3% Misconfiguration

Corporate/ Internal Network

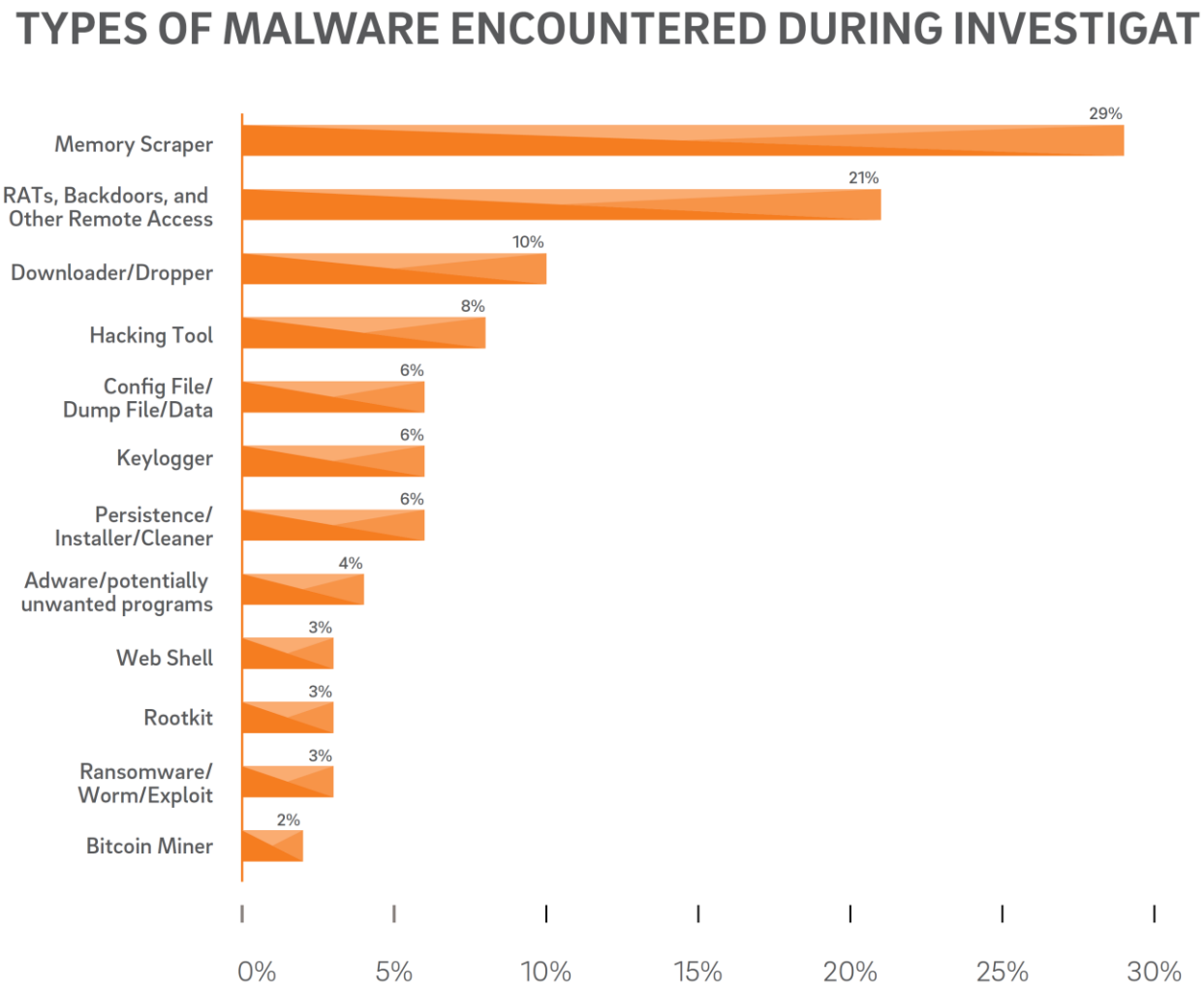
55% Phishing/Social Engineering
13% Malicious Insider
9% Remote Access
8% Misconfiguration
7% Other
5% Code Injection
3% Weak Password

E-Commerce

45% File Upload
39% Code Injection
13% Remote Access
3% Weak Password

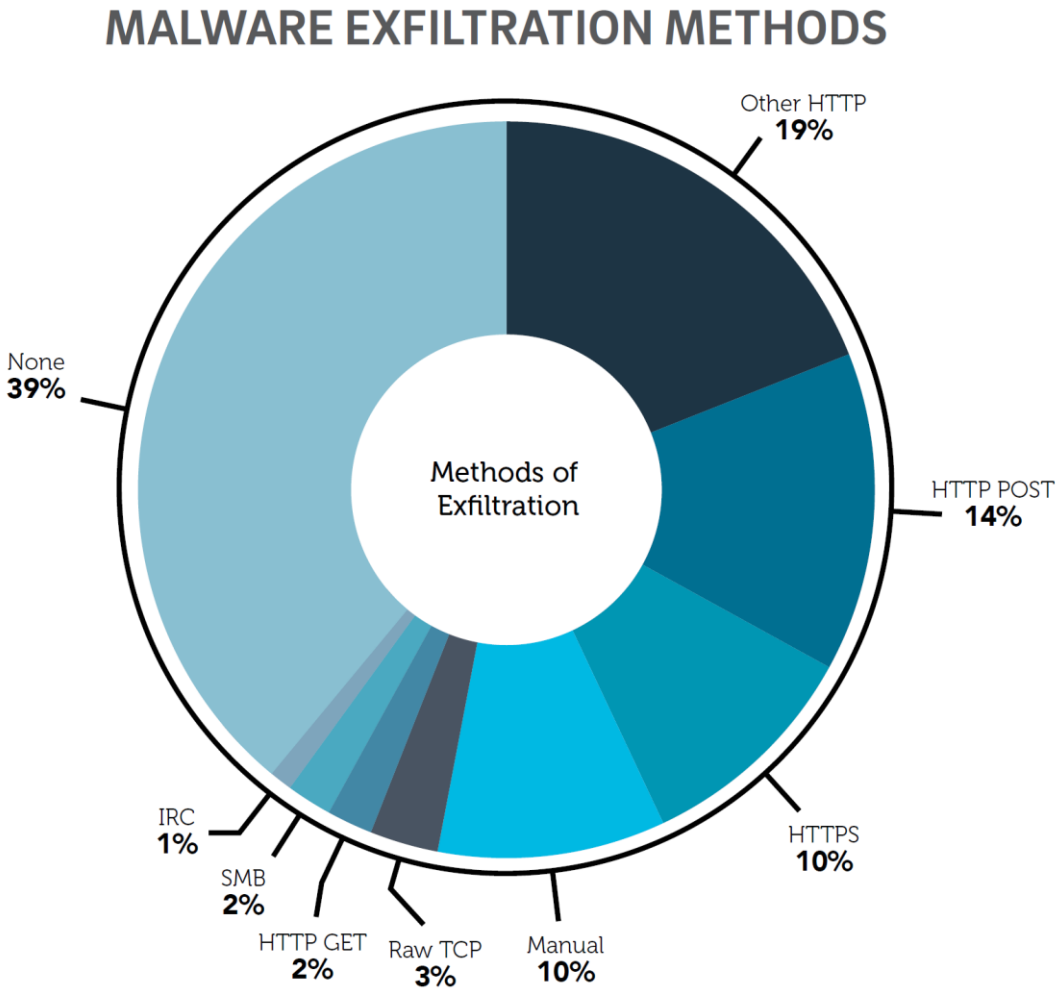
TrustWave Global Security Report 2018

Comment nous ont-ils attaqué?



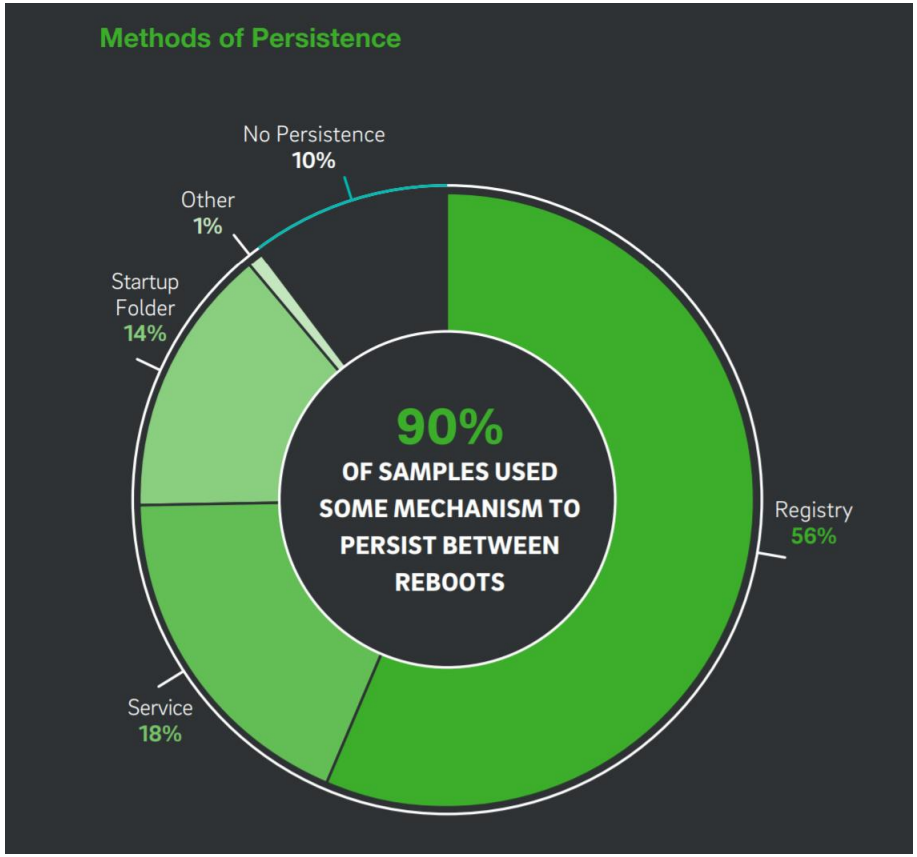
TrustWave Global Security Report 2016

Comment nous ont-ils attaqué?



TrustWave Global Security Report 2019

Comment nous ont-ils attaqué?



TrustWave Global Security Report 2018

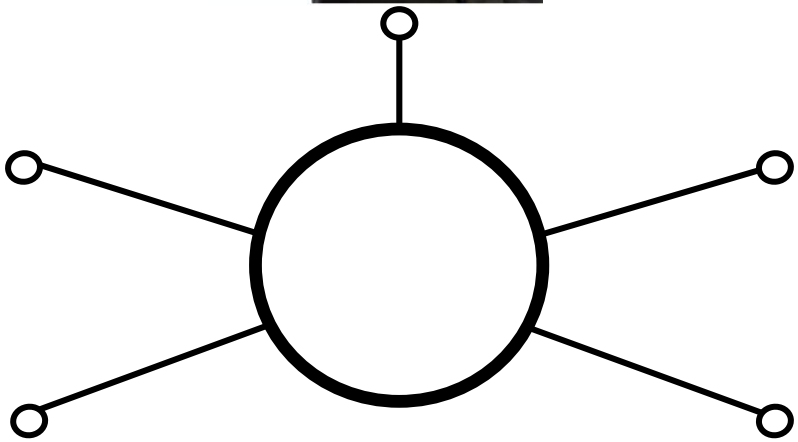
Qui Nous Menace ?

Qui Nous Menace ?

Internal

Coder, old guard hackers

Newbie/Toolkit



Professional criminals,
Cyber-terrorists

Cyberpunk

Qui Nous Menace ?

Newbie/Toolkit

- Peu expérimentés
- Utilisent les outils disponibles (coder, old guard hackers)
- **Objectif:** attaquent par loisir sans intention de nuire

Qui Nous Menace ?

Cyberpunk

- Plus expérimentés
- **Objectif:** Actions malicieuses pour leur propre compte (défacement de site, vol de cartes de crédit)

Qui Nous Menace ?

Internal

- Employés mécontents
- Utilisent ses privilèges existants
- **Objectif:** Attaquer leur entreprise

Qui Nous Menace ?

Coder, old guard hackers

- Très grande expertise
- Passionnés, réalisent des outils d'attaques
- **Objectif:** Sans intention de nuire, prouesse technique, reconnaissance dans leur groupe

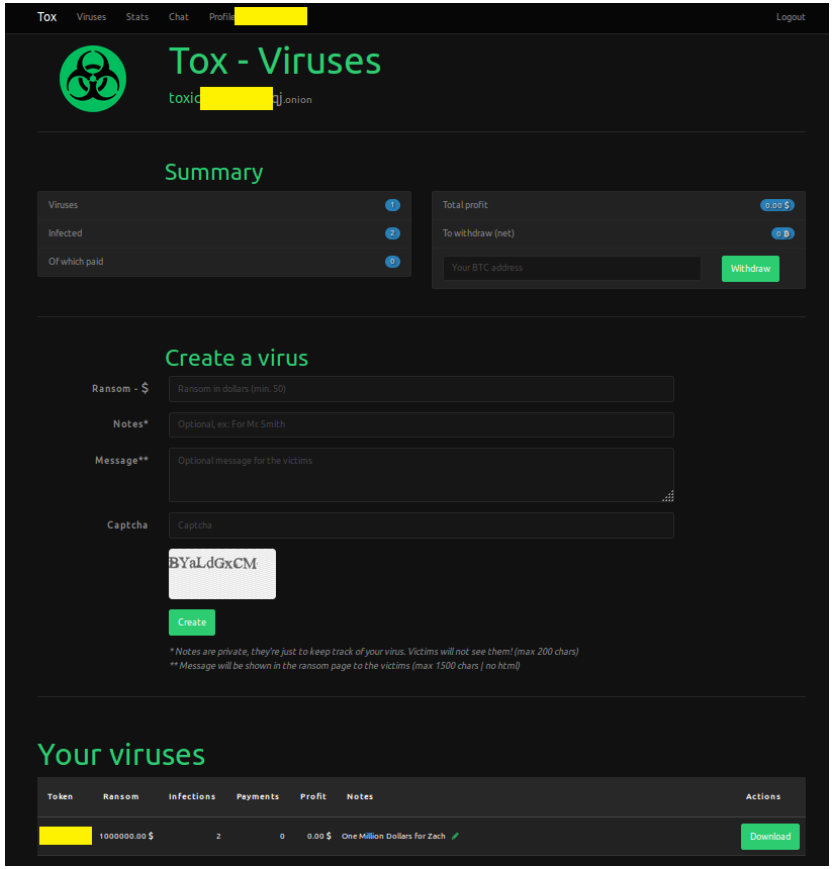
Qui Nous Menace ?

Professional criminals,
Cyber-terrorists

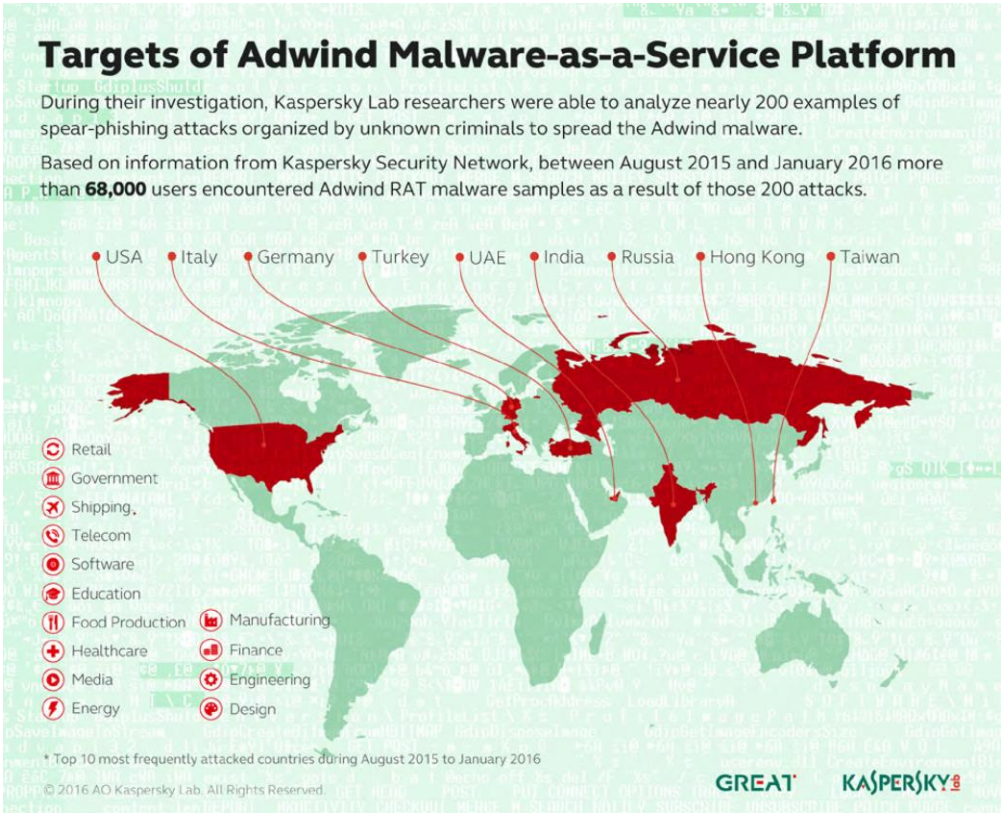
- Grande expertise
- Forte organisation
- Organisation criminelle à grande échelle
- **Objectif:**
  - **Vols, espionnage, dénis de service**
  - **Alimentent une véritable économie souterraine**

Qui Nous Menace ?

Ransomeware As A Service (RAAS)



Malware As A Service (MAAS)

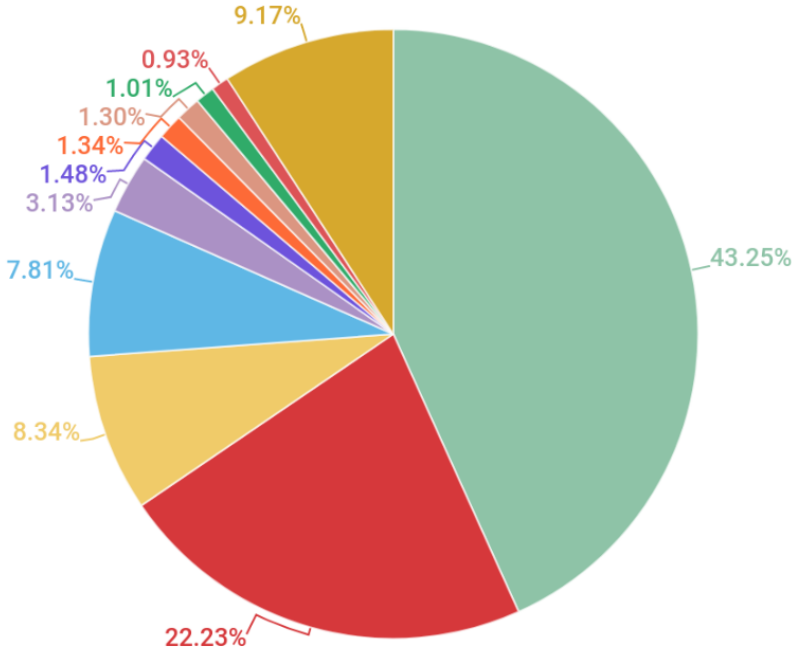


Kaspersky Security Bulletin 2016

Qui Nous Menace ?

Kaspersky Security Bulletin 2016

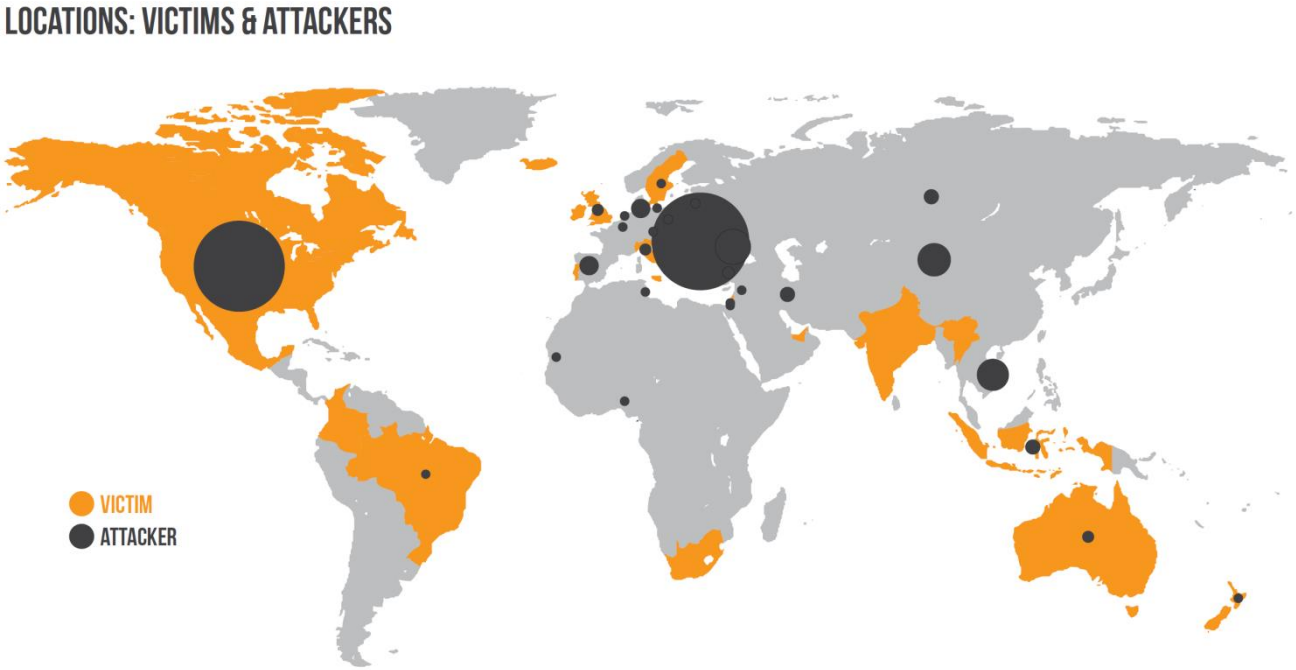
Qui Nous Menace ?



Distribution of web attack sources by country, November 2018 – October 2019

Kaspersky Security Bulletin: Overall Statistics for 2019

Qui Nous Menace ?



> 450
DATA BREACHES

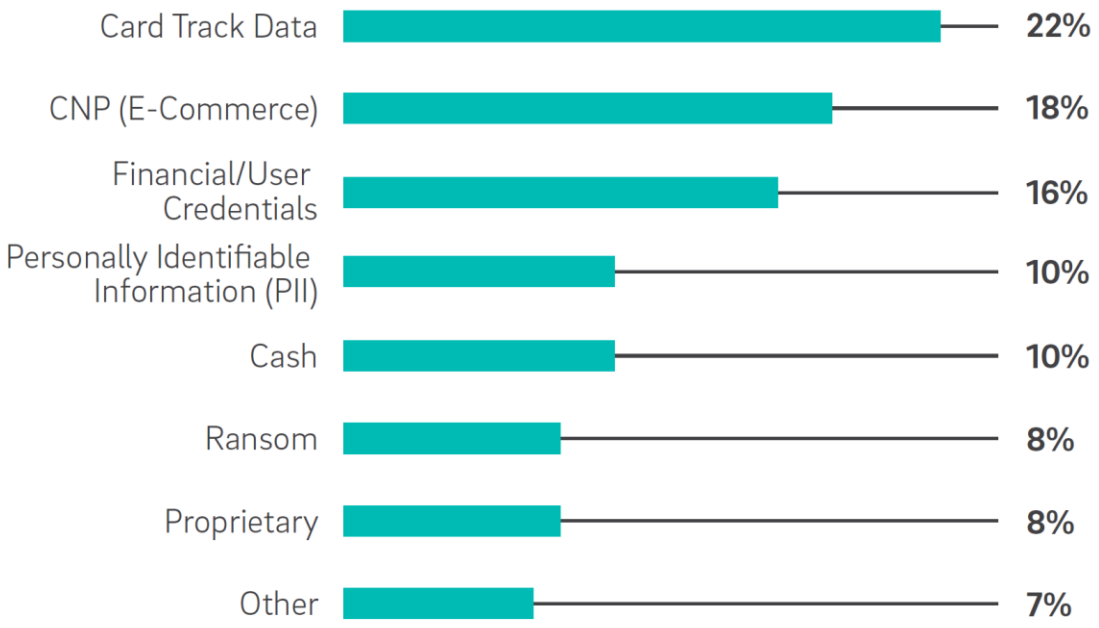
19
COUNTRIES

TOP VICTIM LOCATIONS:		TOP ATTACKER LOCATIONS:	
UNITED STATES	73.0%	ROMANIA	33.4%
AUSTRALIA	7.0%	UNITED STATES	29.0%
CANADA	3.0%	UNKNOWN	14.8%
UNITED KINGDOM	2.0%	UKRAINE	4.4%
BRAZIL	1.2%	CHINA	3.9%

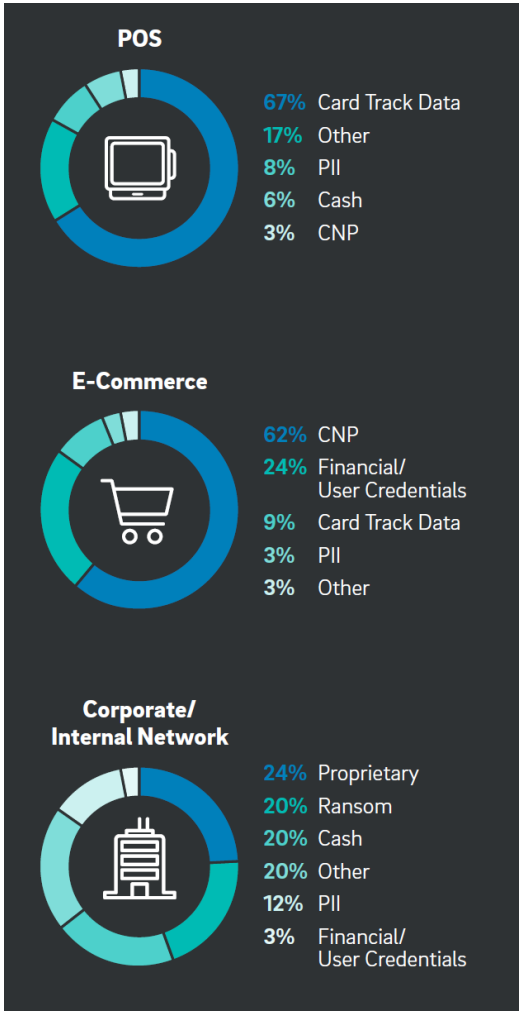
TrustWave 2013 Global Security Report

Que nous prennent-ils ?

Qui Nous prennent-ils ?

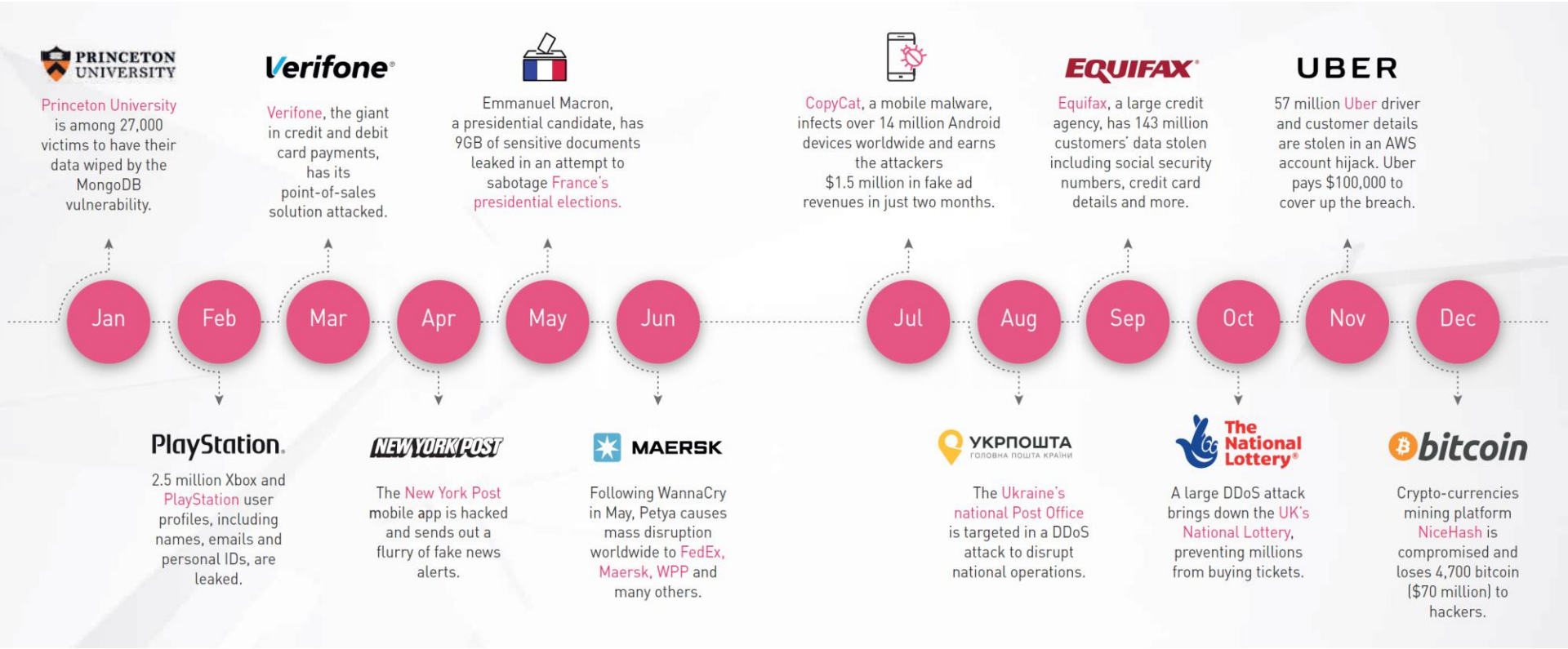


TrustWave Global Security Report 2018



TrustWave Global Security Report 2018

Qui Nous prennent-ils ?

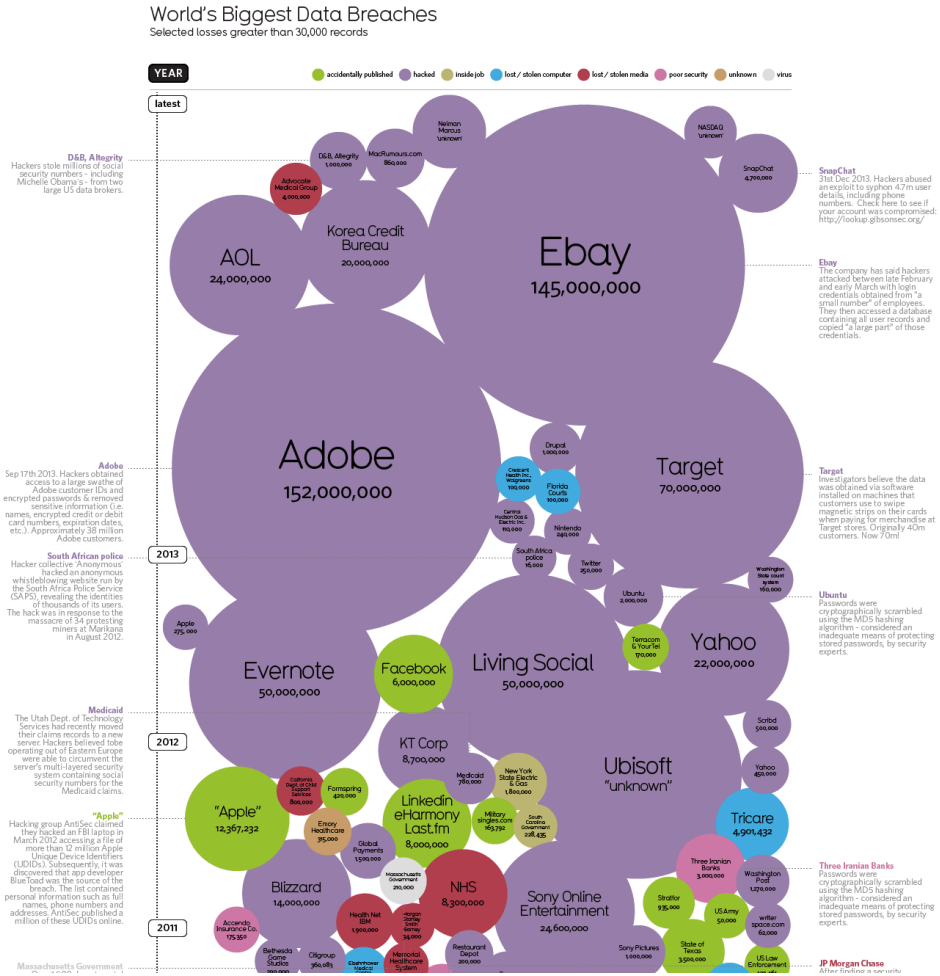


Major Cyber Attack of 2017

CheckPoint Security Report 2018

CPE LYON

Qui Nous prennent-ils ?



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-static/

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Qui Nous prennent-ils ?

Motives for cyberattacks by region

	Total	REGION			
		USA/Canada	APAC	EMEA	CALA
Financial/ransom	59%	70%	52%	59%	30%
Insider threat	29%	26%	28%	31%	39%
Political/hacktivism/social	28%	30%	23%	38%	20%
Cyberwar/geopolitical conflict related	27%	36%	27%	20%	7%
Competition/espionage	25%	23%	22%	34%	26%
Angry users	20%	21%	12%	23%	30%
Motive unknown/other	27%	28%	27%	27%	26%
Have not experienced any cyberattacks	1%	0%	2%	1%	2%

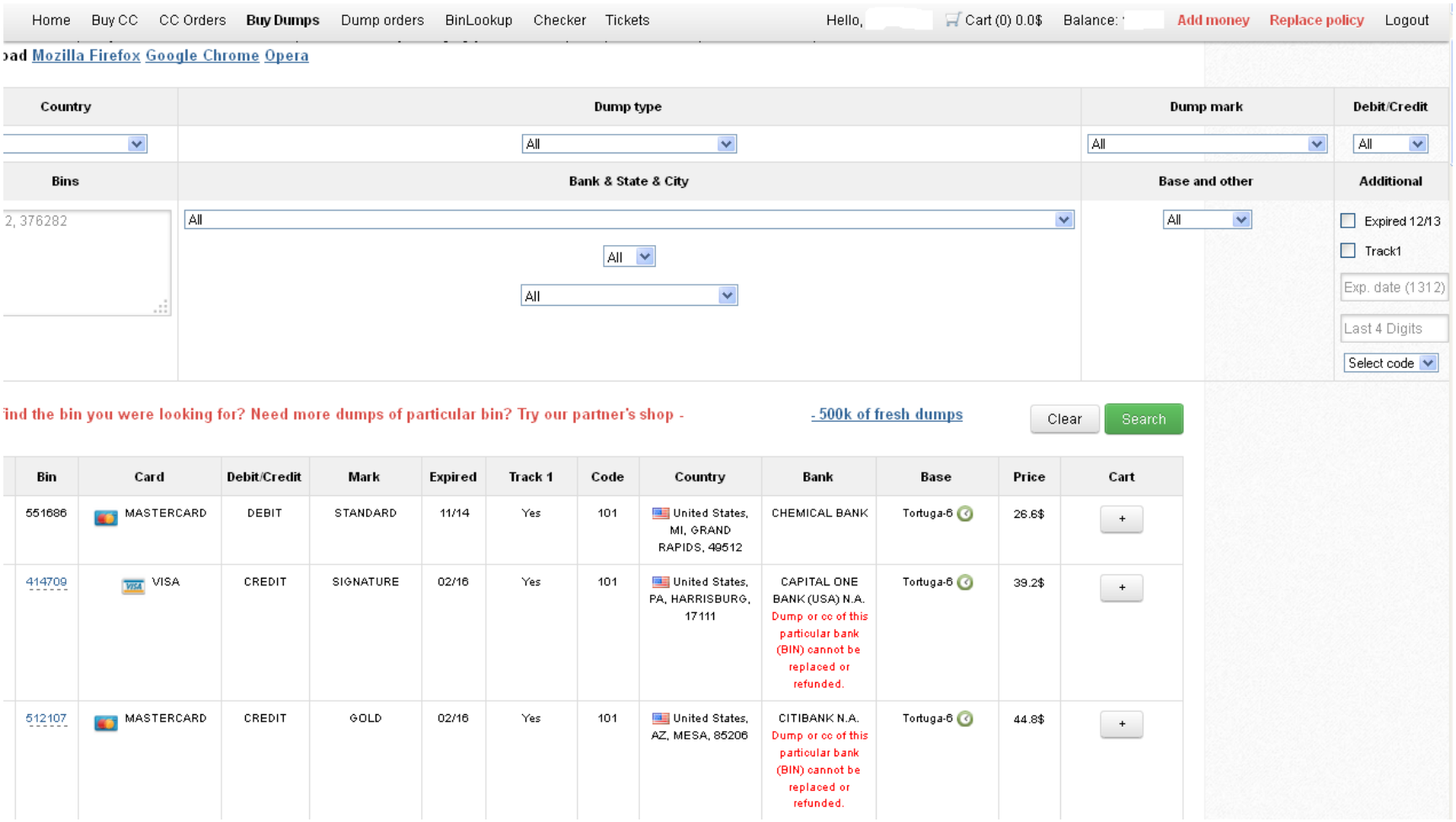
Radware global Application & Network Security report 2019-20

Qui Nous prennent-ils ?

Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	$0.50–$5
2	Bank Accounts	21%	$30–$400
3	Email Passwords	8%	$1–$350
4	Mailers	8%	$8–$10
5	Email Addresses	6%	$2/MB–$4/MB
6	Proxies	6%	$0.50–$3
7	Full Identity	6%	$10–$150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5–$7
10	Compromised UNIX® Shells	2%	$2–$10

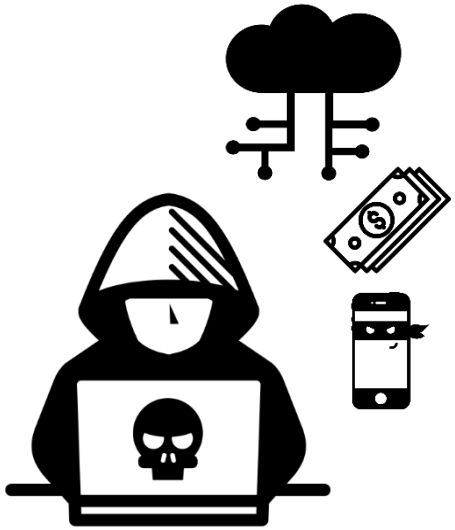
Source: Symantec Corporation

Qui Nous prennent-ils ?



http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

SumUp



- Augmentation de la connectivité et des applications

  → Augmentation du nombre de vulnérabilité

- Evolution de l'usage des Systèmes d'information, augmentation transaction financières, connexion de données sensibles

  → Augmentation des menaces

SumUp

Figure 12: What is your major obstacle when it comes to countering cyber-attacks?

Radware global Application & Network Security report 2016-17

OutLine

- Evolution du monde informatique
  - Evolution des systèmes d'information
  - Les constats de la sécurité
- Les enjeux de la sécurité
  - Etat d'urgence ?
  - Les bases de la sécurité
- Comprendre les attaques
  - ARP Spoofing / DNS Spoofing
  - TCP Flooding / TCP Session Hijacking
  - XSS / Bufferoverflow

Les enjeux de la sécurité

- Etat d'urgence ?
- Les Bases de la sécurité

Un état d'urgence ?

- Menaces présentent avérées et prouvées
- Sécurisé coûte de l'argent et du temps → engagement modéré des décideurs
- Attentisme des organisations/compagnies face à la menace
- Silence radio lors d'attaques
  - Pourquoi?
    - Perte de confiance des utilisateurs/partenaires
    - Peur d'une escalade d'exploitation de la brèche de sécurité.

→ Etude de la faille de sécurité tardive,

→ Continuité des transactions (escalade)

→ Niveau de menace difficilement quantifiable

Un état d'urgence ?

Information Warefare

Démentir
Exploiter
Corrompre
Détruire

Les information et les fonctions de son ennemi tout en se protégeant soit même contre ces actions

Un état d'urgence ?

Nation

Art de la guerre:

- Communications coupées
- Vol d'informations secret défense
- Attaque de sites stratégiques

Compagnies

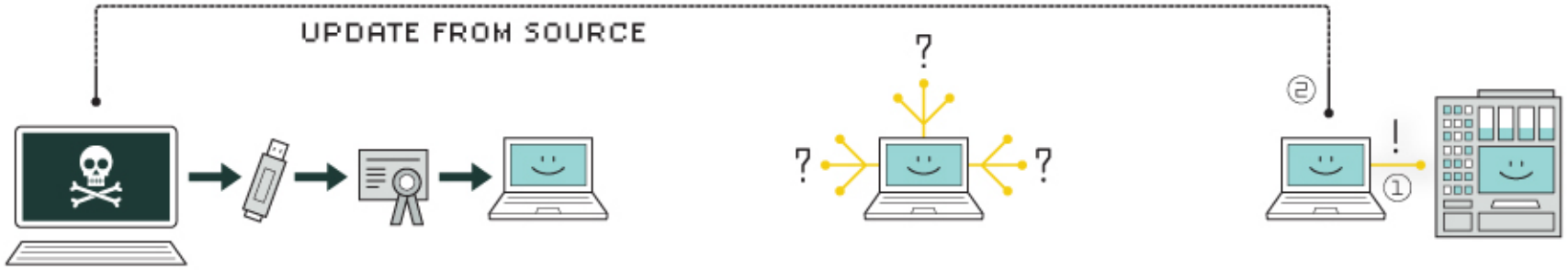
Art de la guerre:

- Arrêt d'activités
- Vol de données sensibles (prototype, portefeuille client)
- Atteinte à la réputation (défacement…)

Nous tous

- Vol d'informations personnelles (cb,email, images)
- Vol d'argent
- Usurpation d'identité
- Exploitation de nos ressources

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

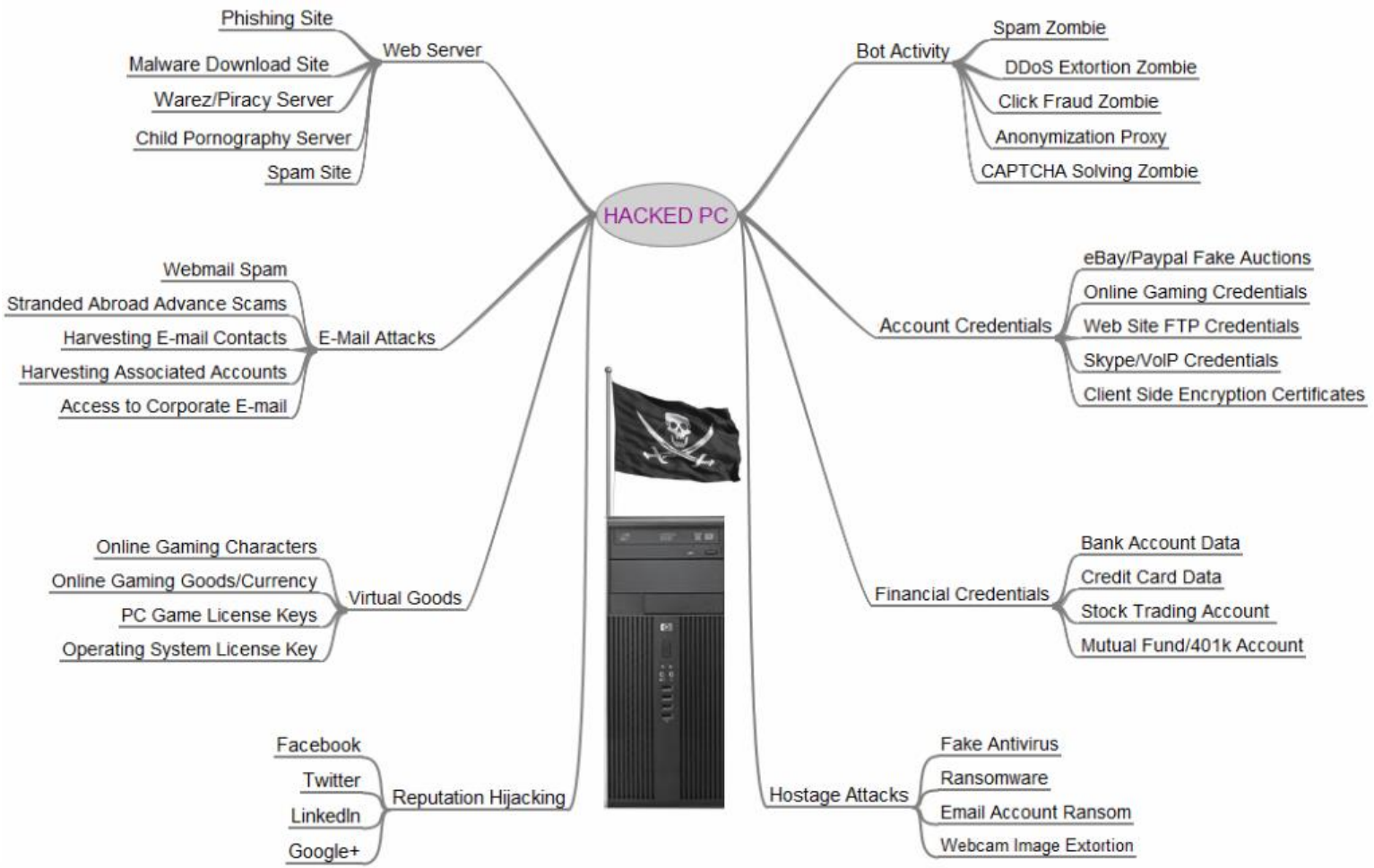
5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

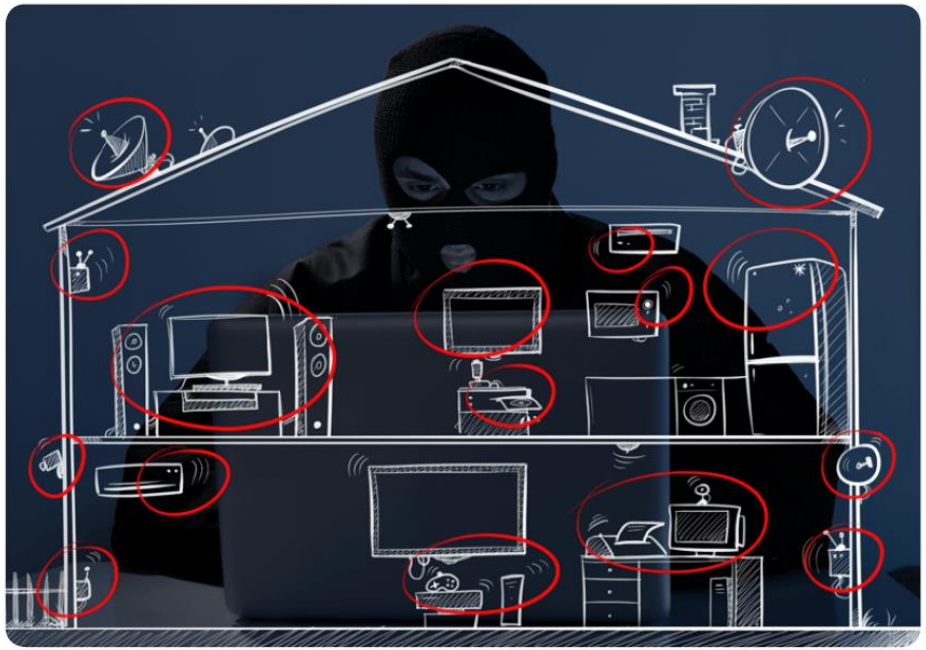
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

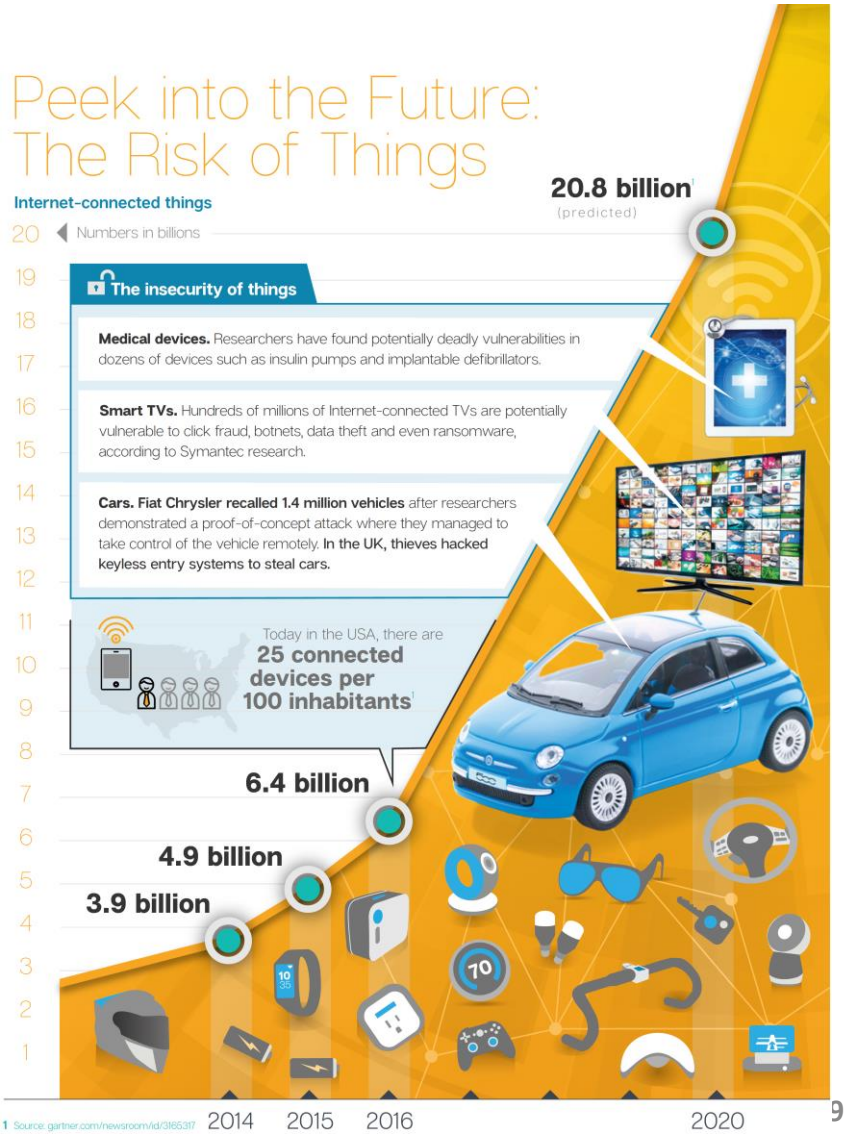
Un état d'urgence ?



http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Un état d'urgence ?





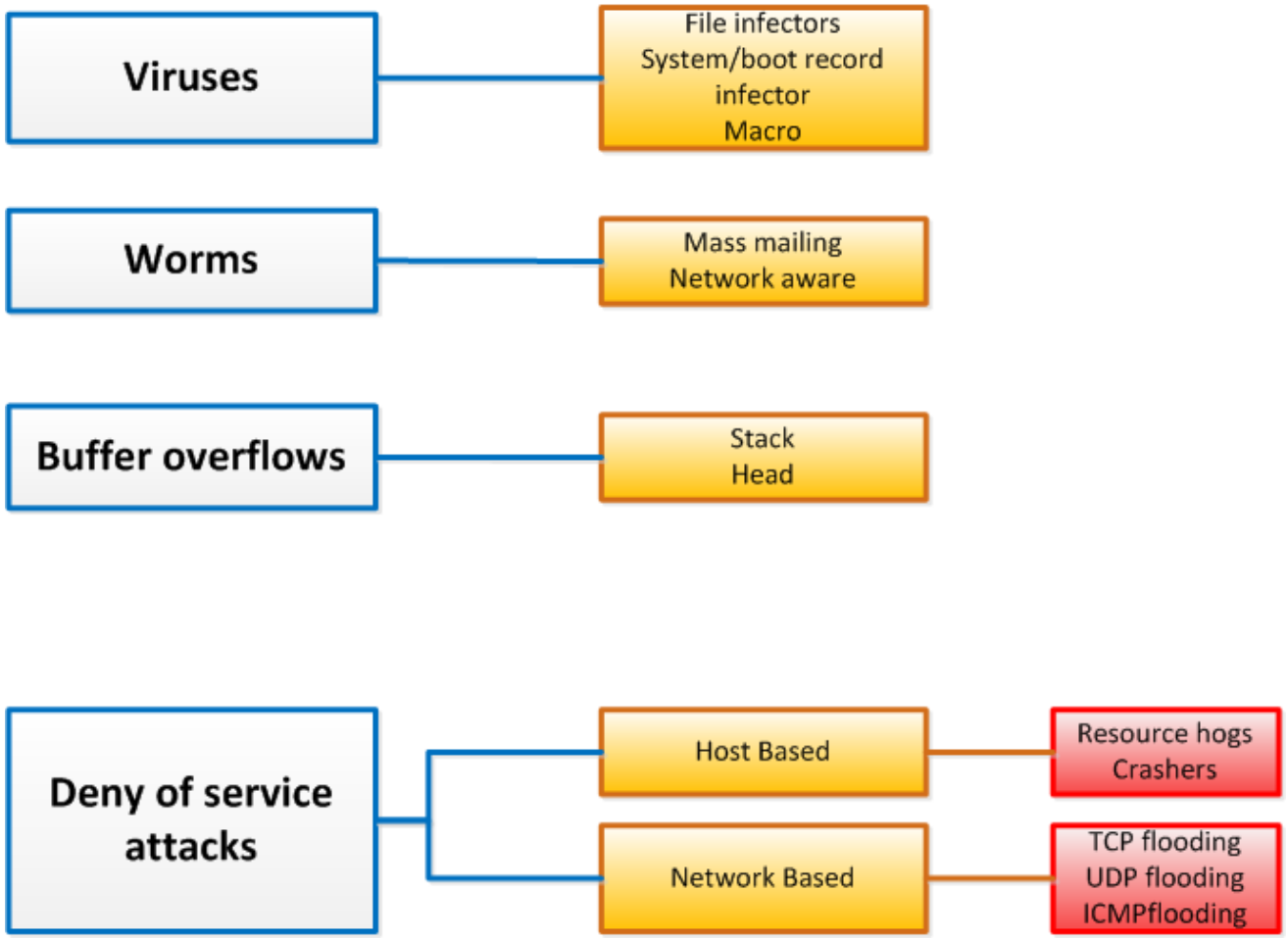
Symantec, ISTR, Internet Security Threat Report, 2016

Un état d'urgence ? Contre quoi se protège-t-on ?

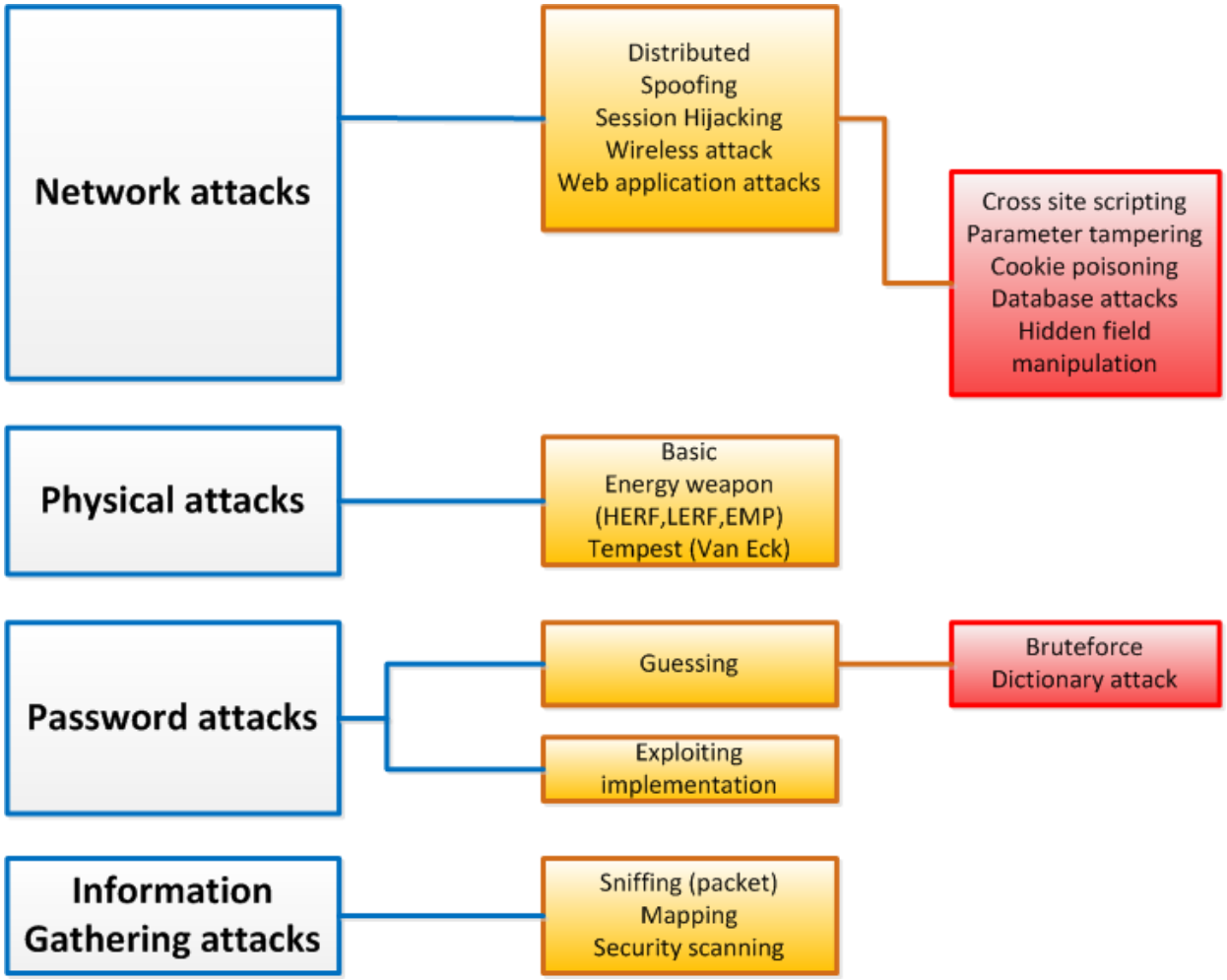
- Viruses
- Worms
- Buffer overflows
- Deny of service attacks
- Network attacks
- Physical attacks
- Password attacks
- Information Gathering attacks

A taxonomy of network and computer attack , Simon Hansman, Ray Hunt,2004

Un état d'urgence ? Contre quoi se protège-t-on ?

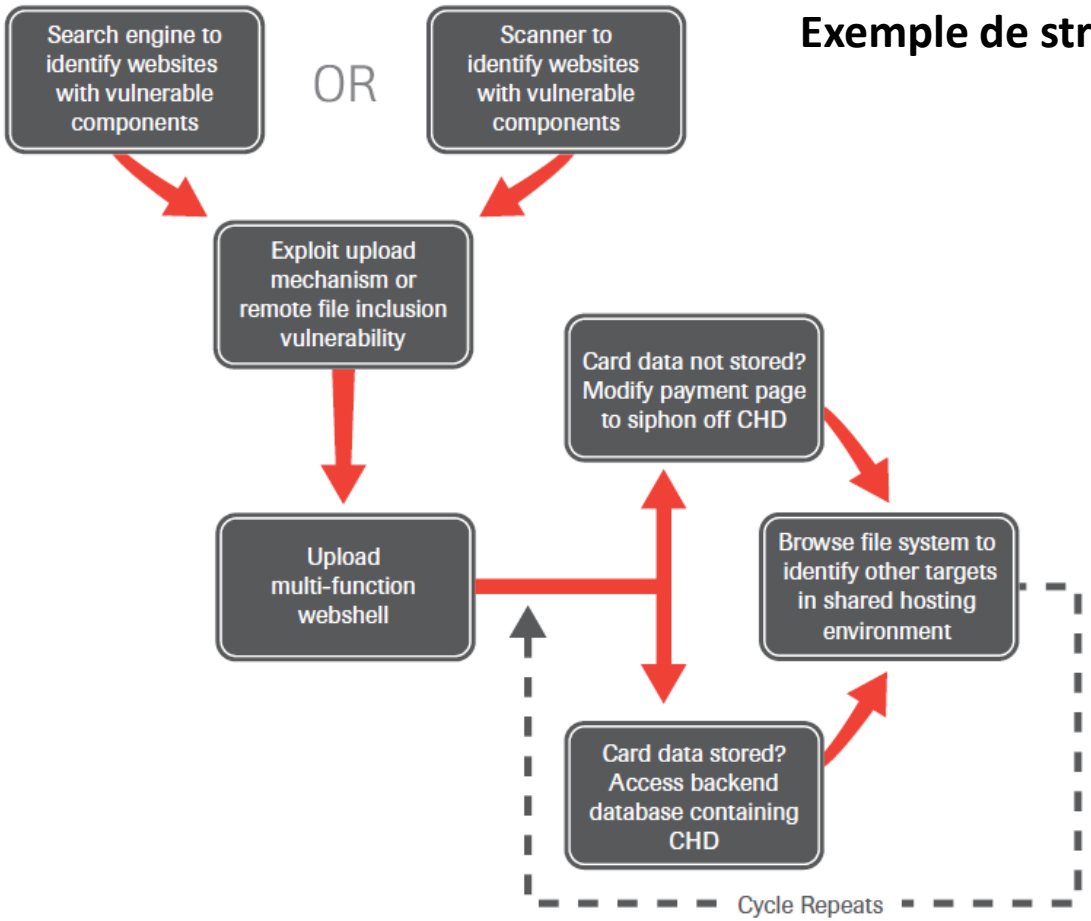


Un état d'urgence ? Contre quoi se protège-t-on ?



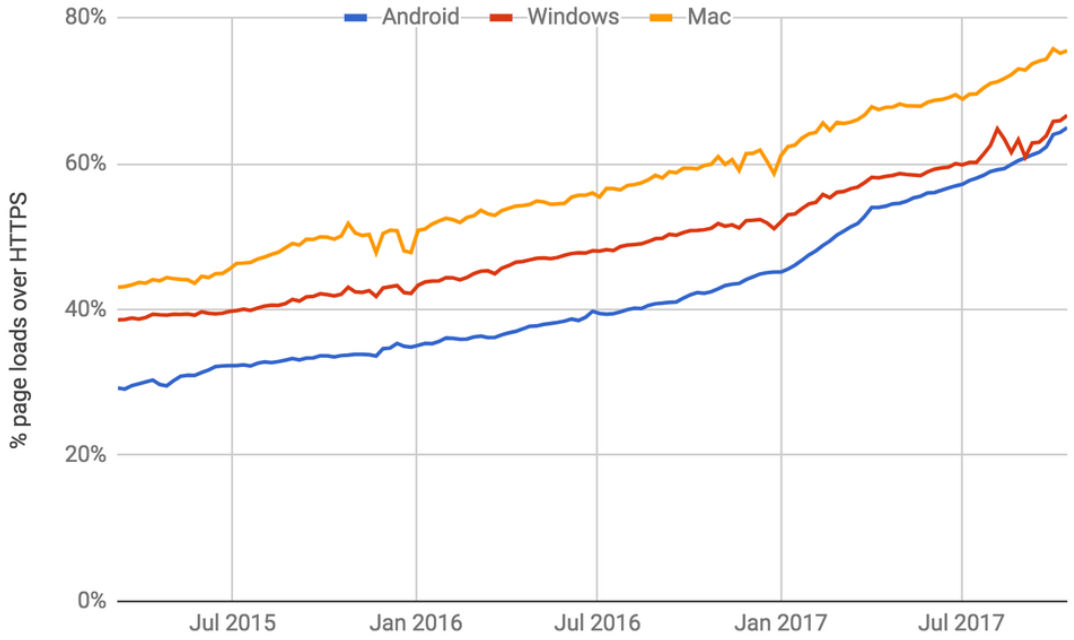
Un état d'urgence ? Contre quoi se protège-t-on ?

Exemple de stratégie d'attaque



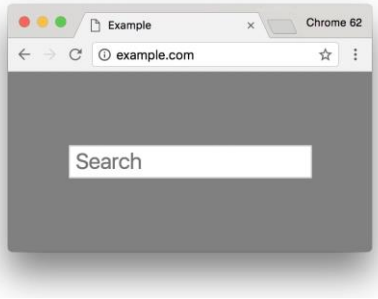
TrustWave 2012 Global Security Report

Une prise de conscience ?



SAFETY & SECURITY

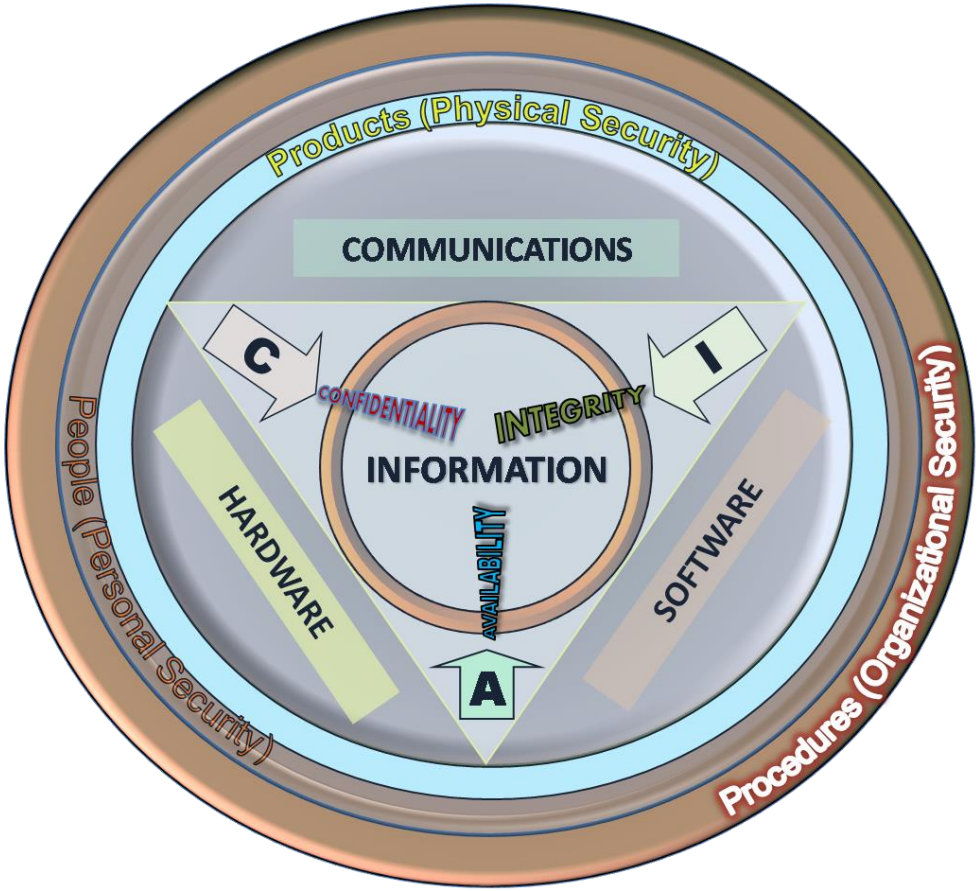
Say “yes” to HTTPS: Chrome secures the web, one site at a time



Les enjeux de la sécurité

- Etat d'urgence ?
- Les Bases de la sécurité

Comment se protéger ? Les bases de la sécurité



JohnManuel http://en.wikipedia.org/wiki/File:CIAJMK1209.png

Comment se protéger ? Les bases de la sécurité

- Les Objectifs de la sécurité
  - Confidentialité
  - Intégrité
  - Disponibilité (Availability)

Confidentialité

Empêcher toutes divulgations d'information à des personnes, programmes ou équipements non autorisés

Comment se protéger ? Les bases de la sécurité

- Les Objectifs de la sécurité
  - Confidentialité
  - Intégrité
  - Disponibilité (Availability)

Intégrité

Assurer que les informations stockées, transmises et reçues n'ont pas été modifiées pas une entité non autorisée. Toute modification d'information entraine un viol d'intégrité et doit être détecté.

Comment se protéger ? Les bases de la sécurité

- Les Objectifs de la sécurité
  - Confidentialité
  - Intégrité
  - Disponibilité (Availability)

Disponibilité

Capacité à un système d'information de fournir un service.

Cela englobe également l'assurance de la restauration du service en cas de défaillance.

Comment se protéger ? Les bases de la sécurité

- Les Objectifs de la sécurité
  - Confidentialité
  - Intégrité
  - Disponibilité (Availability)

→ Tous les outils/procédures de sécurité ont comme fonction de recouvrir une partie ou la totalité des objectifs de sécurité **Confidentialité**, **Intégrité**, **Disponibilité**.

Comment se protéger ? Les bases de la sécurité

- Mais aussi
  - Identification
  - Authentification
  - Autorisation
  - Accountability
  - Non-Répudiation

Comment se protéger ? Les bases de la sécurité

Identification

Connaitre l'identité d'une entité. Récupérer un élément caractérisant son interlocuteur .

Authentification

Vérifier l'authenticité de l'identité d'une entité (what you know, what you have, what you are).

Autorisation

Assignation de droits, autorisation en accord avec la politique de sécurité en vigueur.

Comment se protéger ? Les bases de la sécurité

Accountability

Capacité à traquer et enregistrer les activités du Systèmes d'information et de ses utilisateurs

Non-Répudiation

Imputabilité d'un message, action , activité sur le système d'information.

Comment se protéger ? Les outils de la sécurité

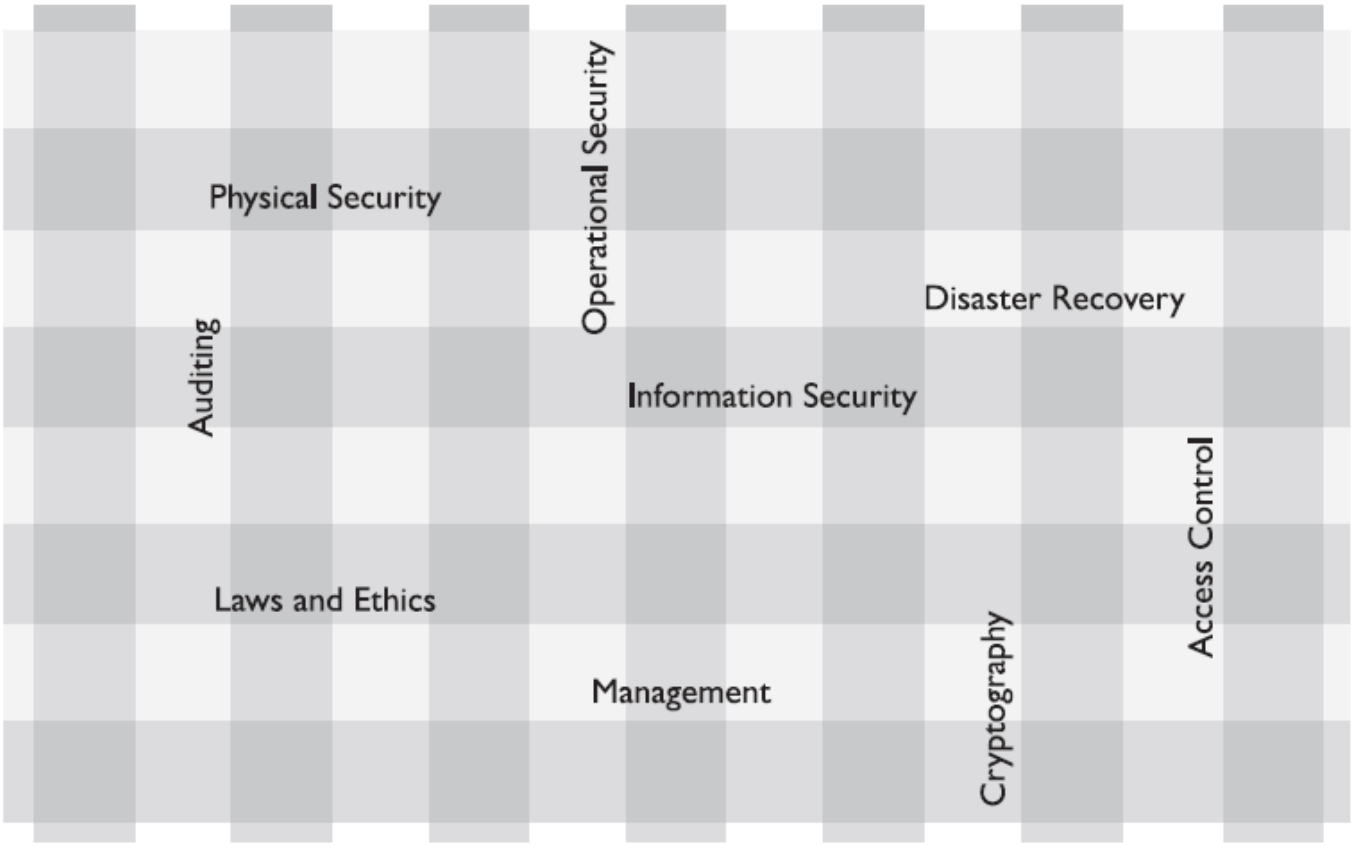


Figure 2-2 Technology, hardware, people, and procedures are woven together as a security fabric.

Comment se protéger ? Sécurité Définitions

- **Vulnérabilité**

  Software, Hardware, faille de procédures fournissant à un attaquant une fenêtre d'accès à une machine, un réseau, lui offrant des accès non–autorisés à des ressources du SI.

- **Menace**

  Tous danger potentiel pouvant affecter le SI.

- **Risque**

  Probabilité qu'une vulnérabilité soit exploitée par un individu (menace) ainsi que l'impact de cet exploit sur la compagnie.

Comment se protéger ? Sécurité Définitions

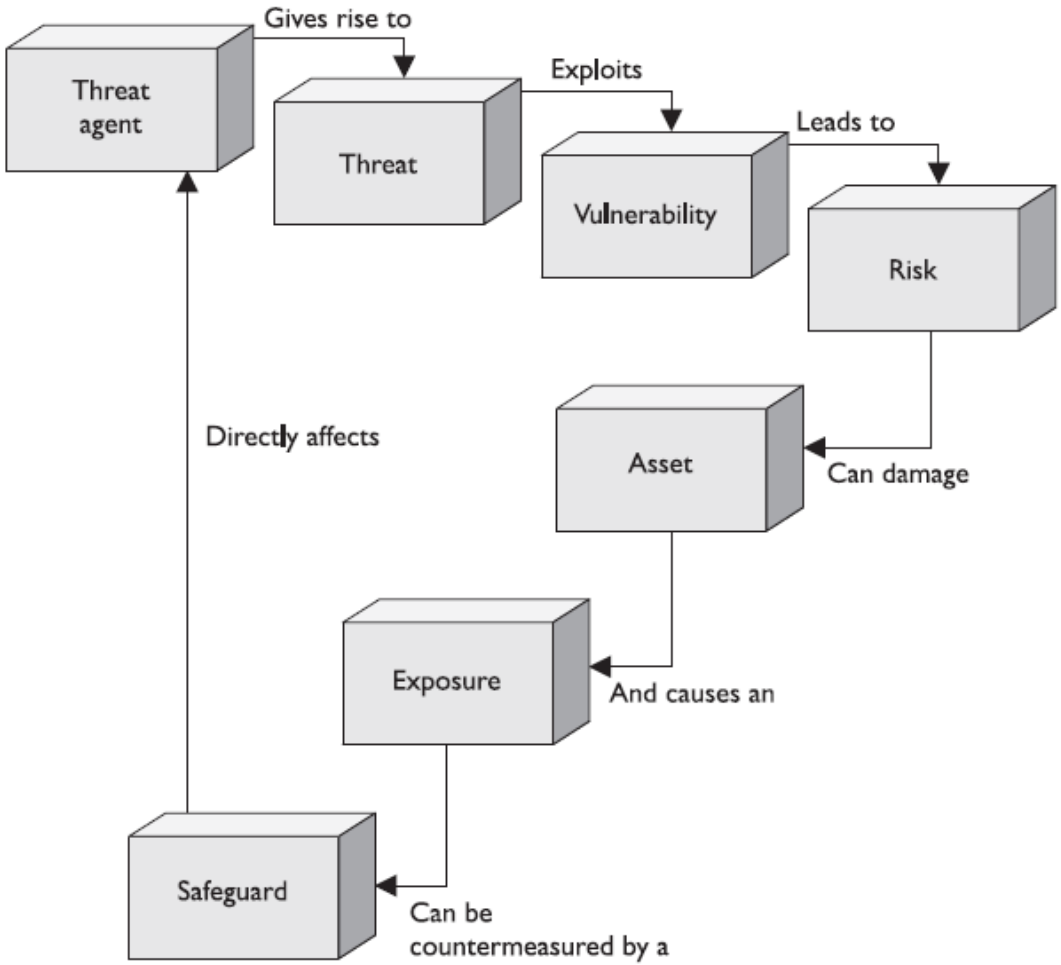
- **Exposition**

  Ensemble d'éléments du SI exposés à une menace.

- **Contremesure**

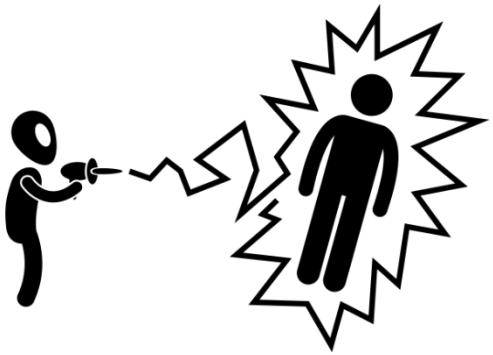
  Elément mis en place permettant de réduire le risque potentiel.

Comment se protéger ? Sécurité Définitions



OutLine

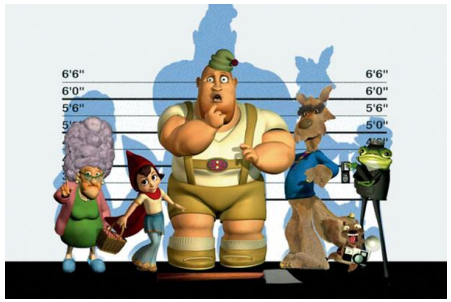
- Evolution du monde informatique
  - Evolution des systèmes d'information
  - Les constats de la sécurité
- Les enjeux de la sécurité
  - Etat d'urgence ?
  - Les bases de la sécurité
- Comprendre les attaques
  - ARP Spoofing / DNS Spoofing
  - TCP Flooding / TCP Session Hijacking
  - XSS / Bufferoverflow



Comprendre les attaques

- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- BufferOverflow

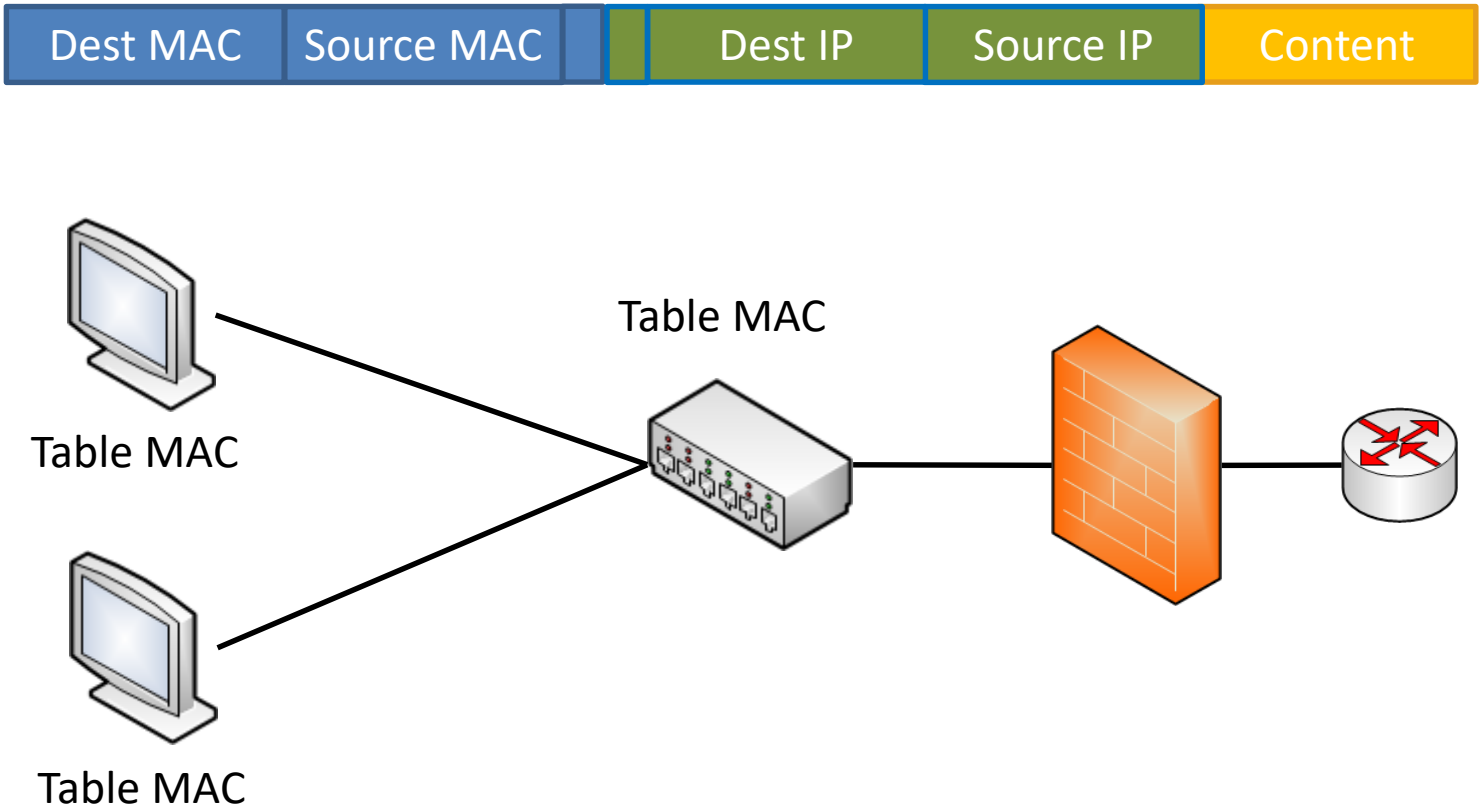
ARP Spoofing



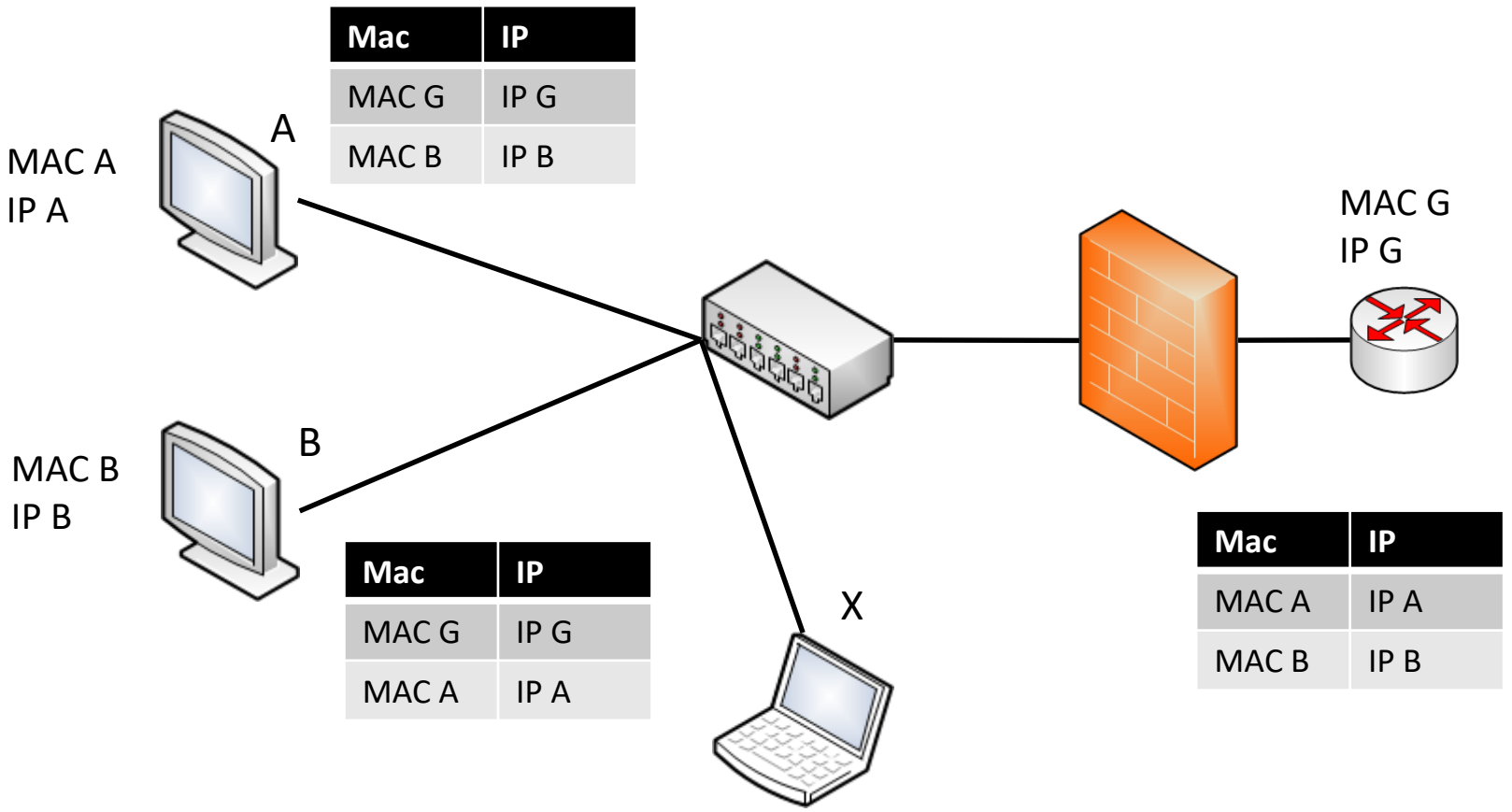
- **Utilisation de la couche de liaison**
- **Utilisation des adresses MAC**
- **Attaque LAN**
- **Attaque possible uniquement sur un même segment**

- **Menace**
  - Denis de service,
  - ARP spoofing,
  - Sniffing,
  - Man in the middle

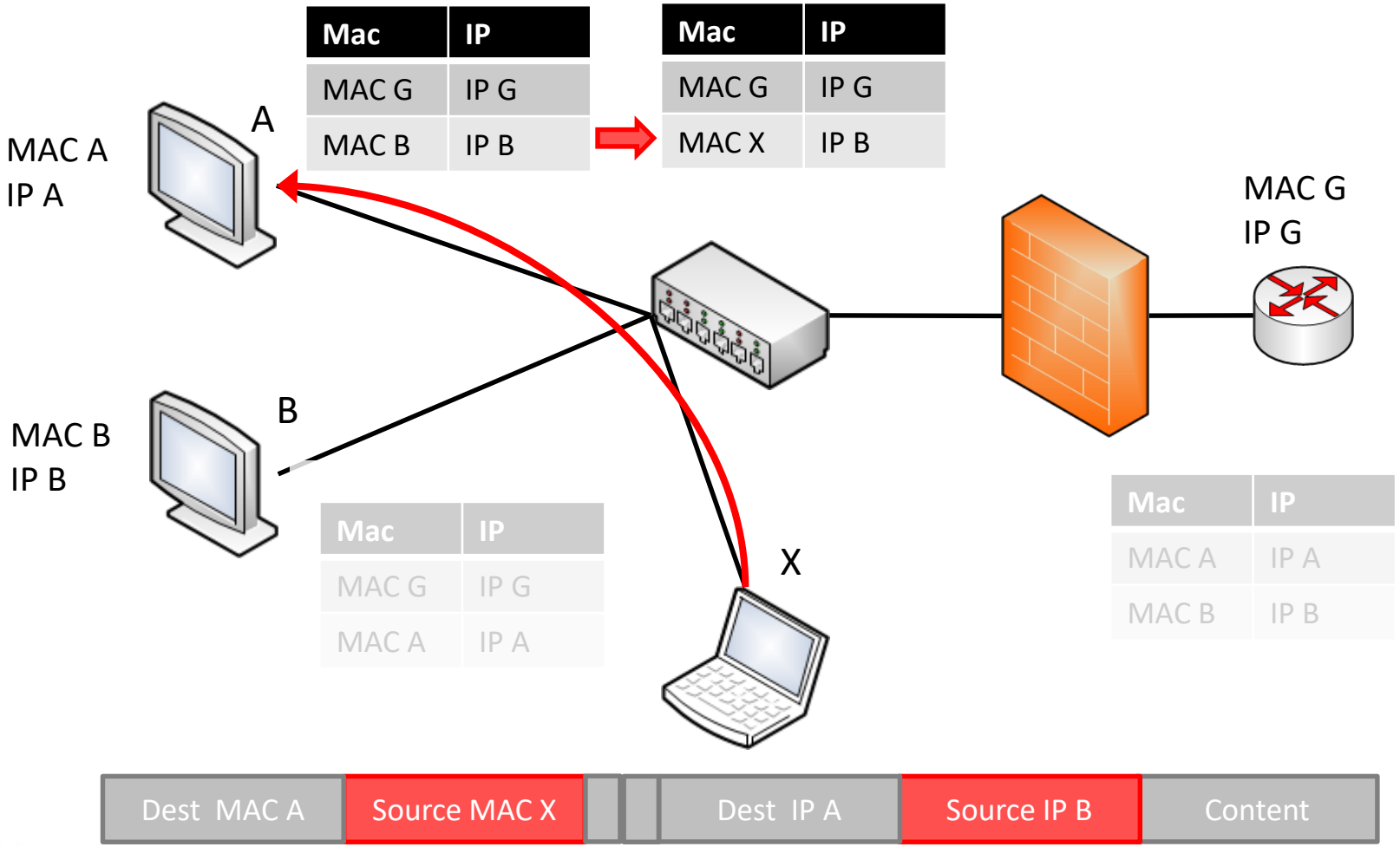
ARP Spoofing



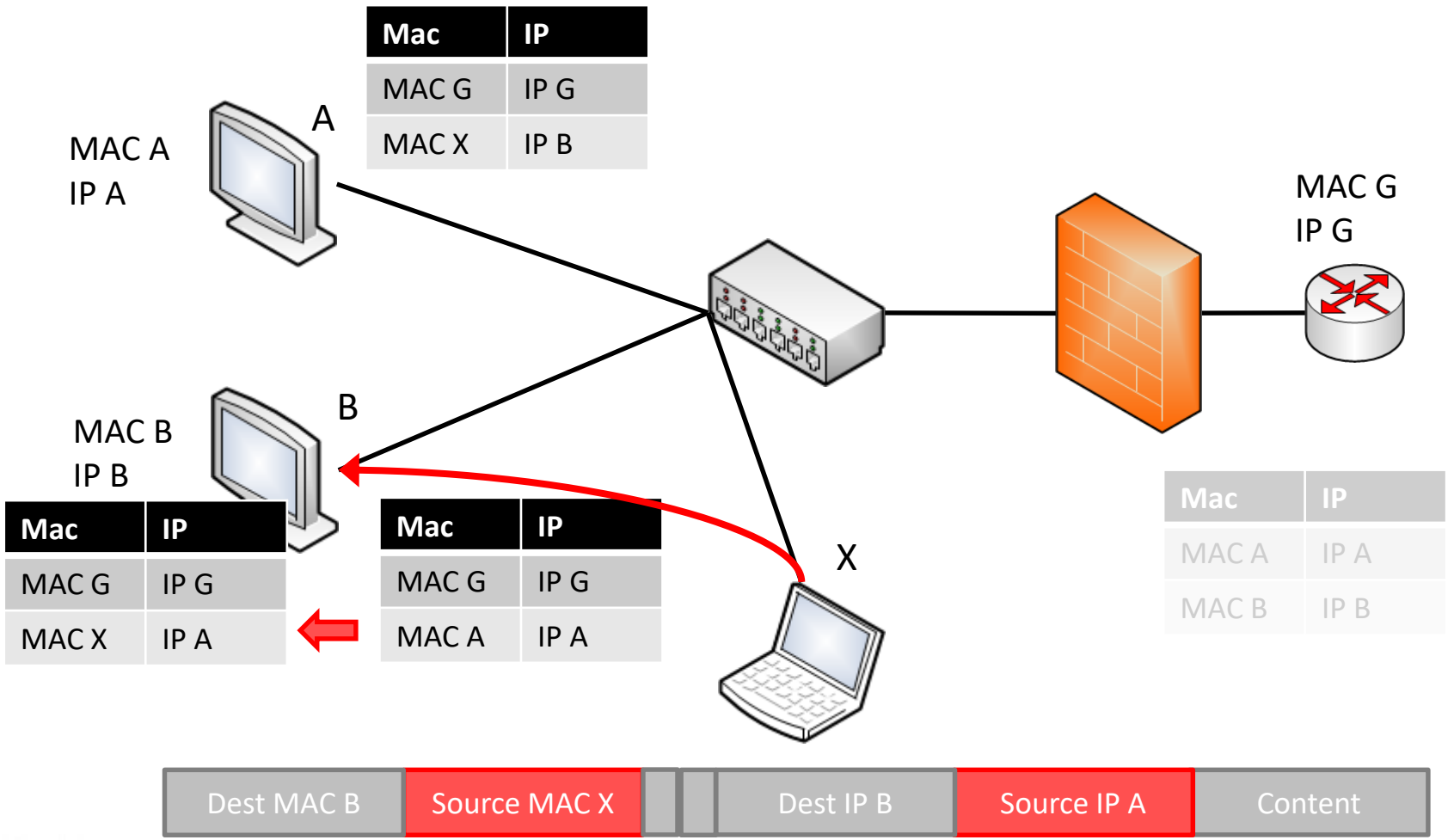
ARP Spoofing



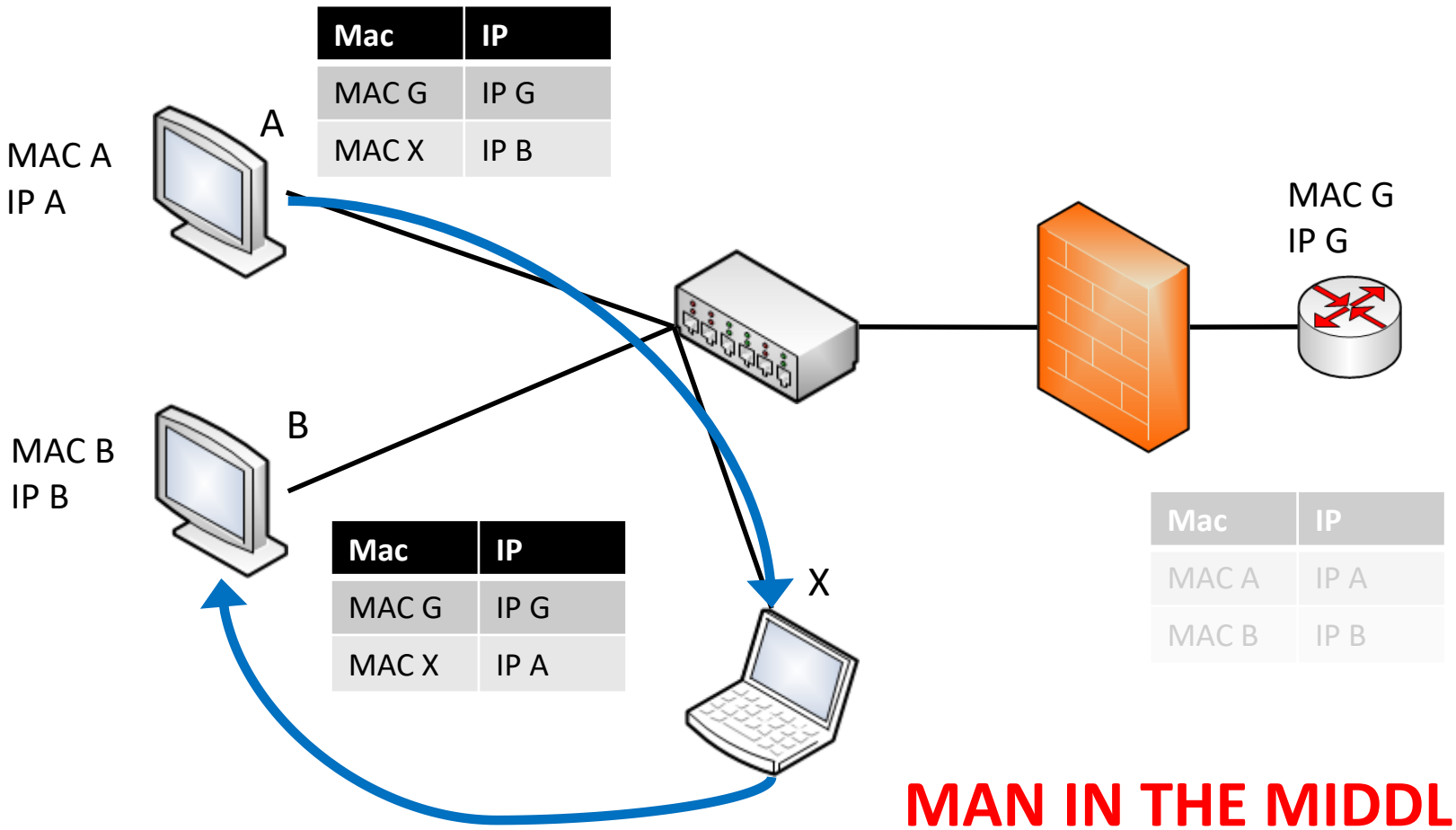
ARP Spoofing



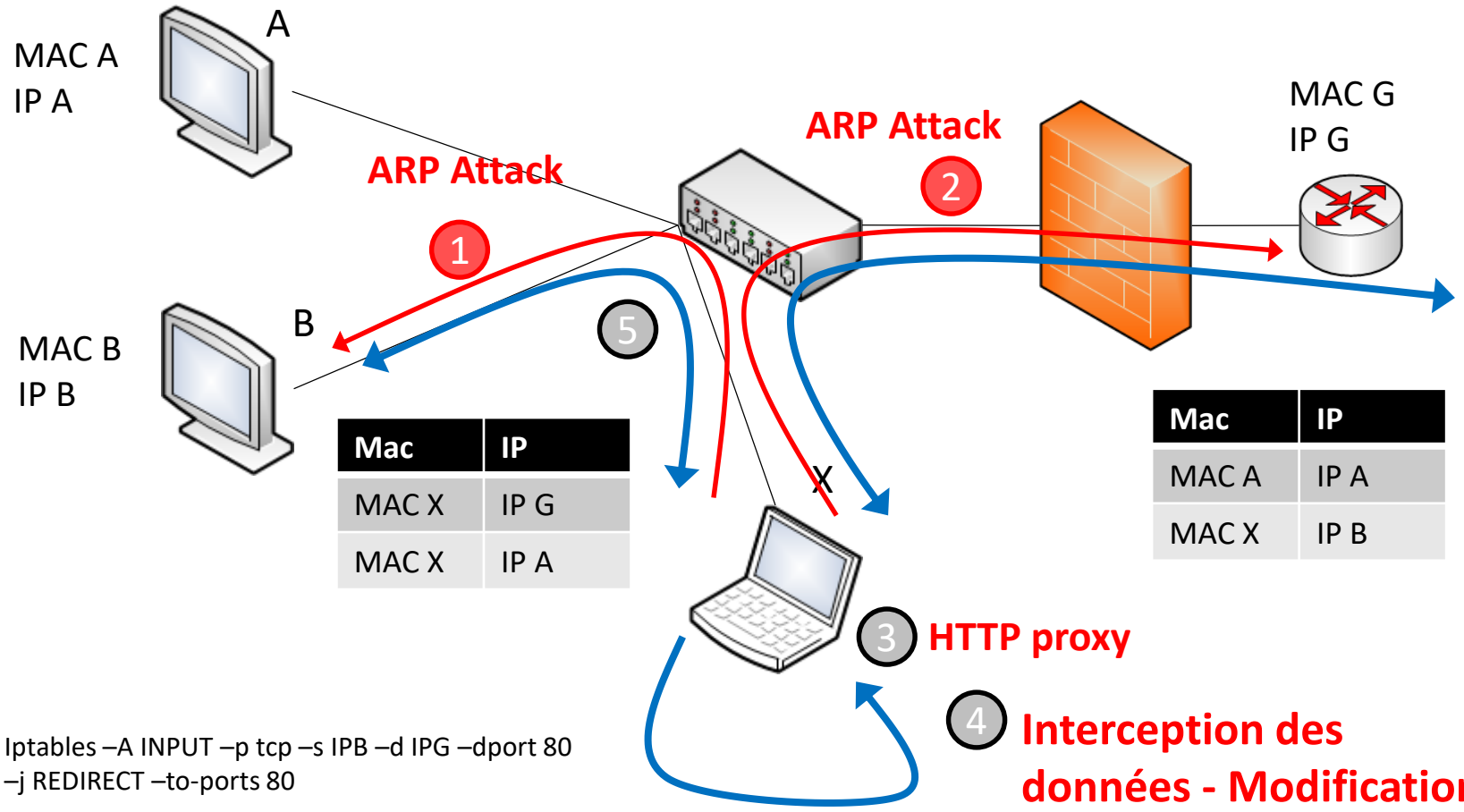
ARP Spoofing



ARP Spoofing

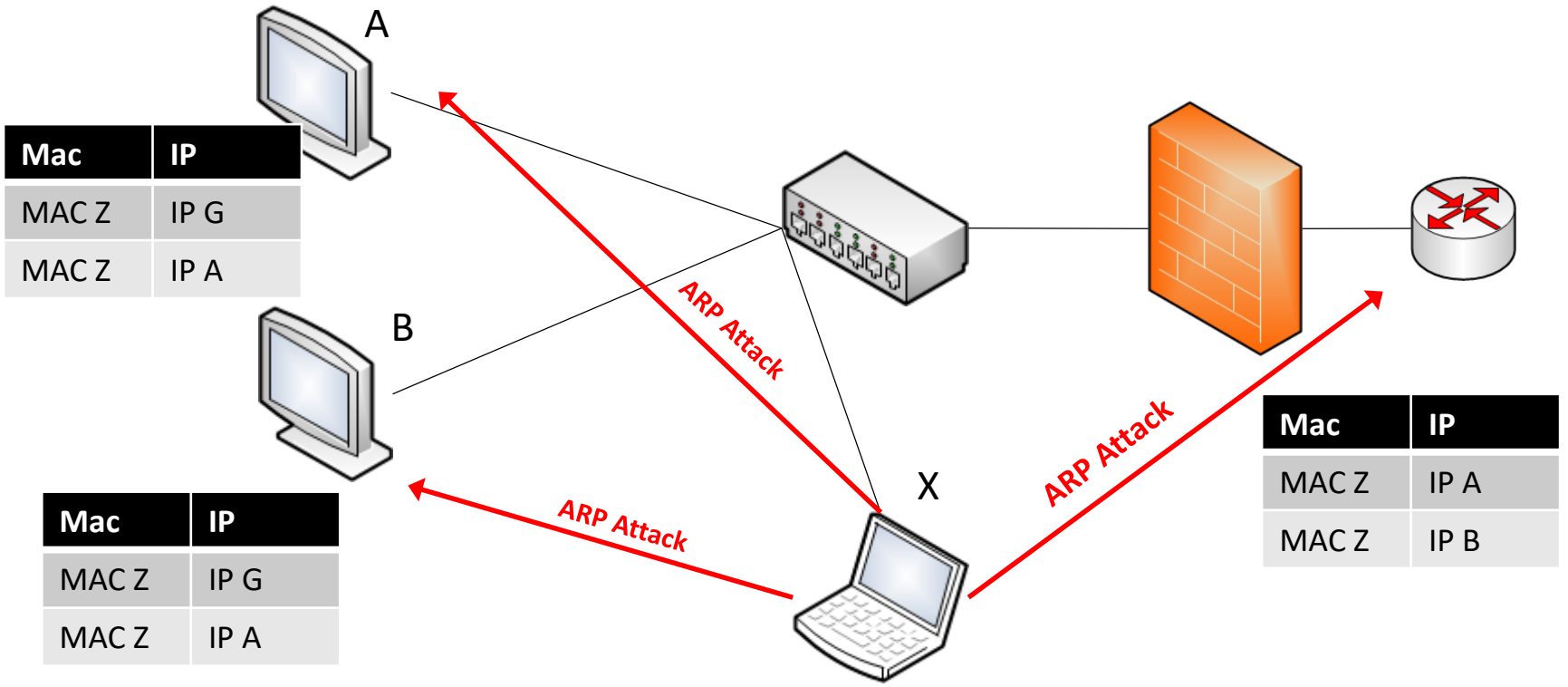


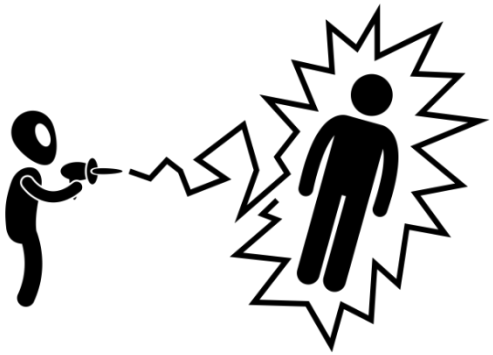
ARP Spoofing



Iptables –A INPUT –p tcp –s IPB –d IPG –dport 80 –j REDIRECT –to-ports 80

ARP Spoofing



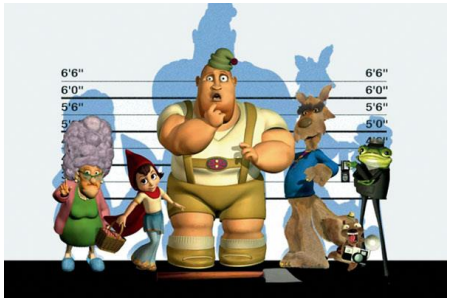


Comprendre les attaques

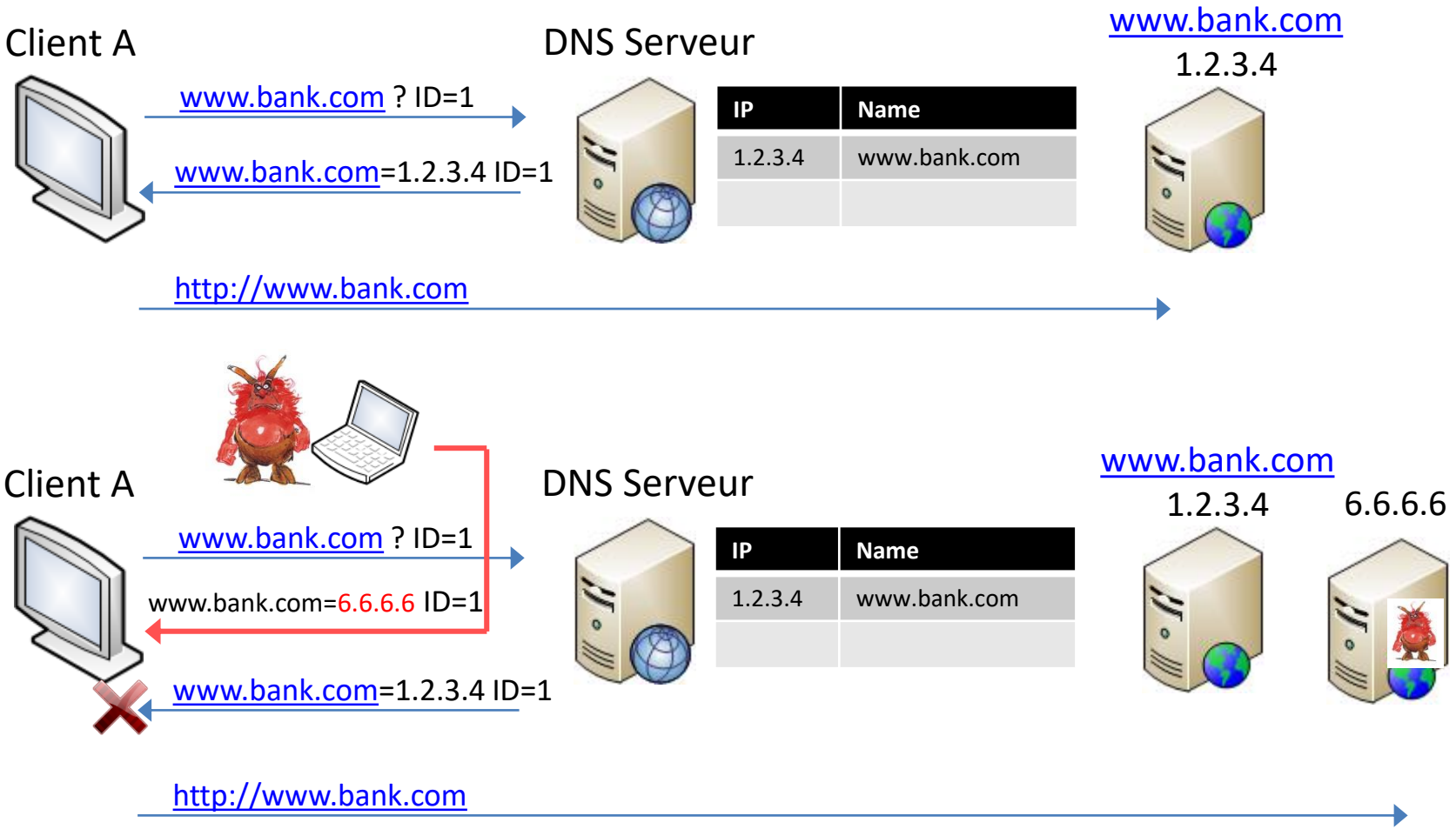
- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- BufferOverflow

DNS Spoofing

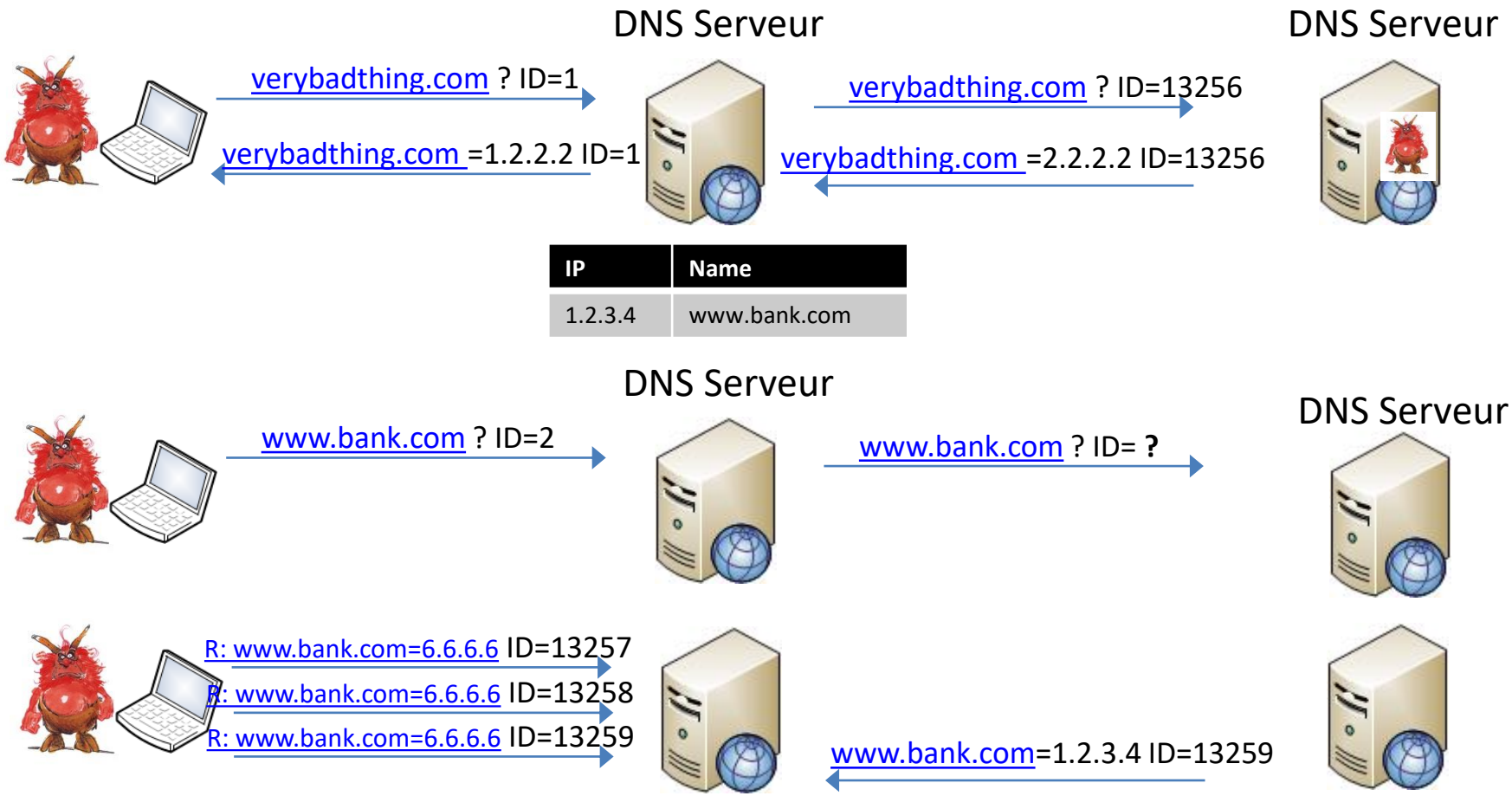
- **Rediriger un utilisateur vers un autre serveur**
- **Deux techniques possibles:**
  - DNS ID Spoofing
  - DNS Cache poisoning
- **Menace**
  - Denis de service,
  - DNS spoofing,
  - Phishing



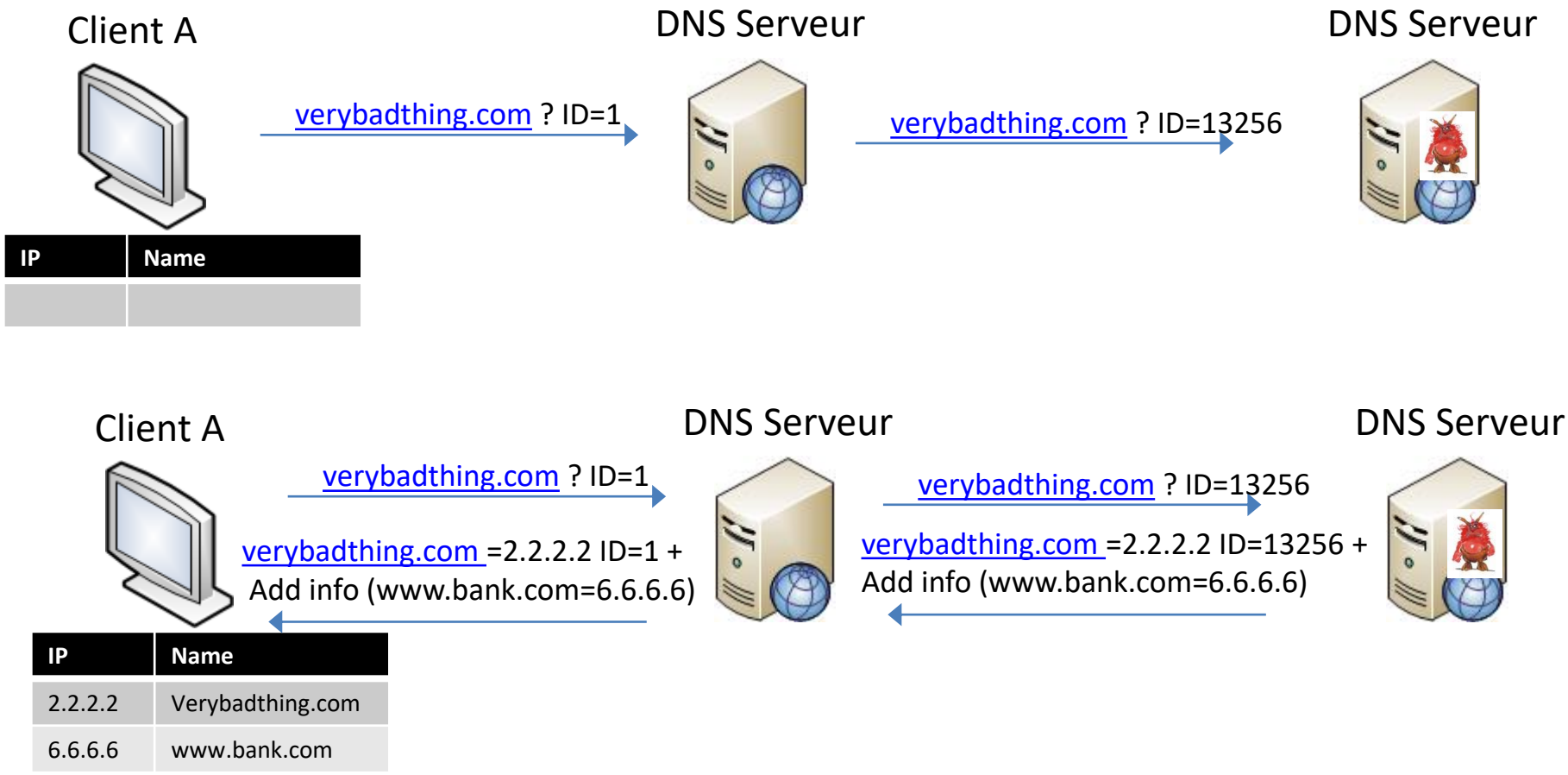
DNS Spoofing: DNS ID Spoofing



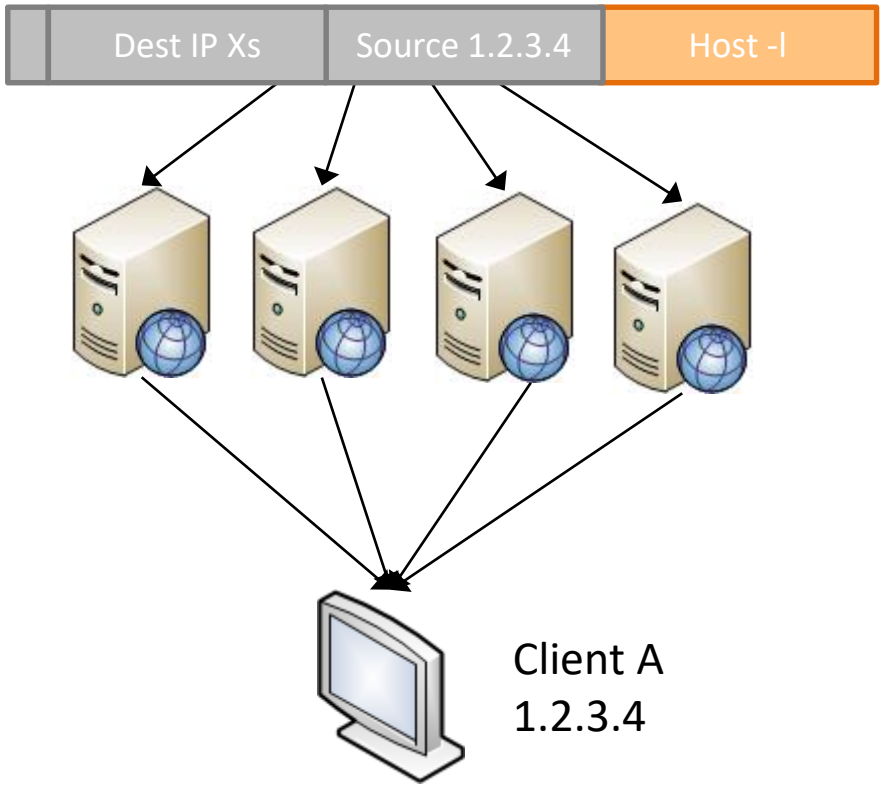
DNS Spoofing: DNS Cache poisoning



DNS Spoofing: DNS Cache poisoning



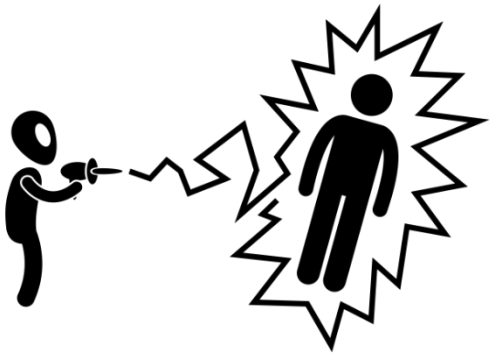
DNS Spoofing: DoS Using DNS



Taille de la requête
27 octets

Facteur * 10 pour chaque requête

Taille de la réponse
312 octets



Comprendre les attaques

- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- BufferOverflow

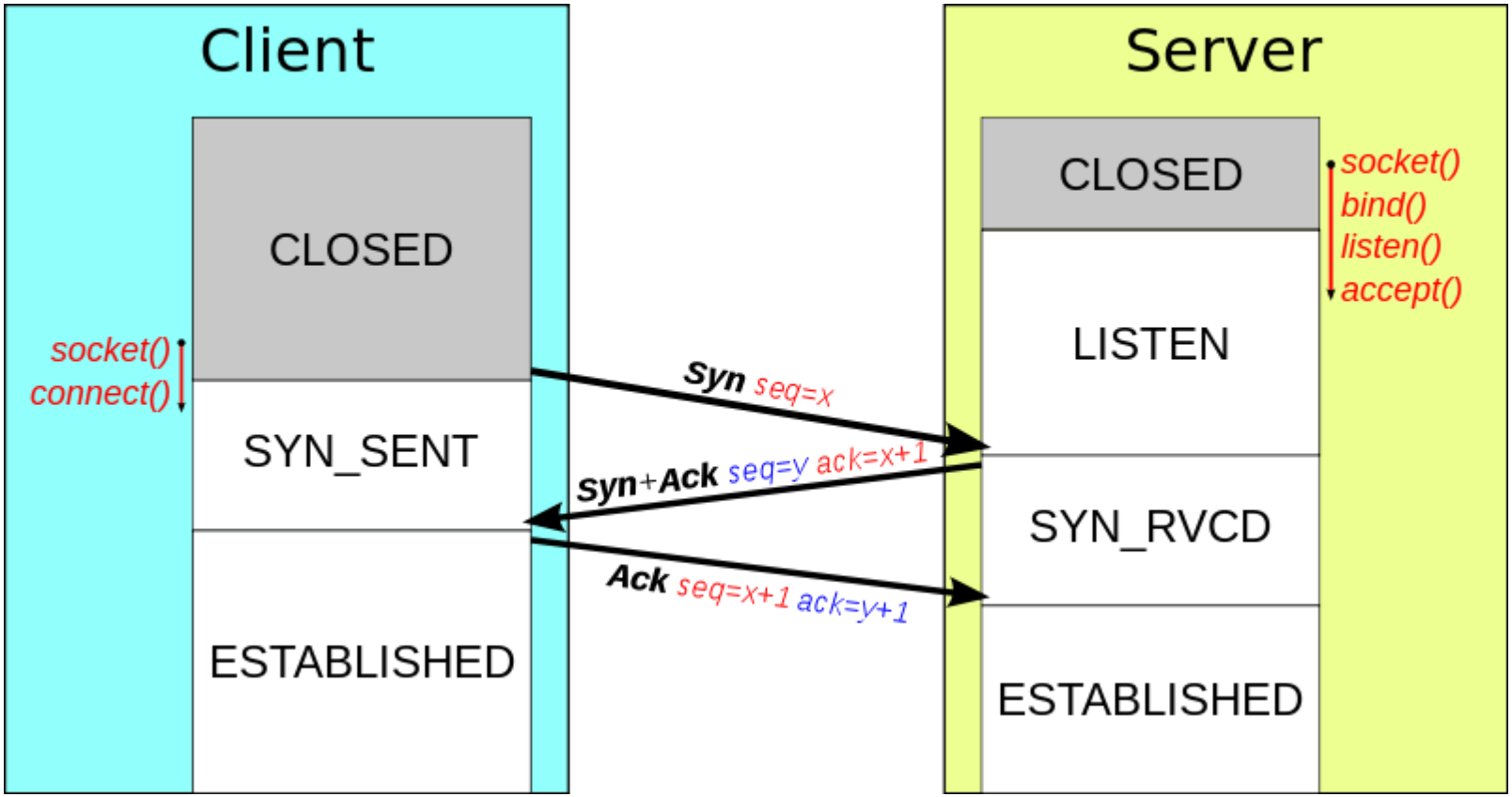
TCP Session Hijacking

- Se faire passer pour une machine de confiance
- Injecter des données dans une connexion déjà établie
- Récupérer des données (à la demande) dans une connexion établie

TCP Flooding

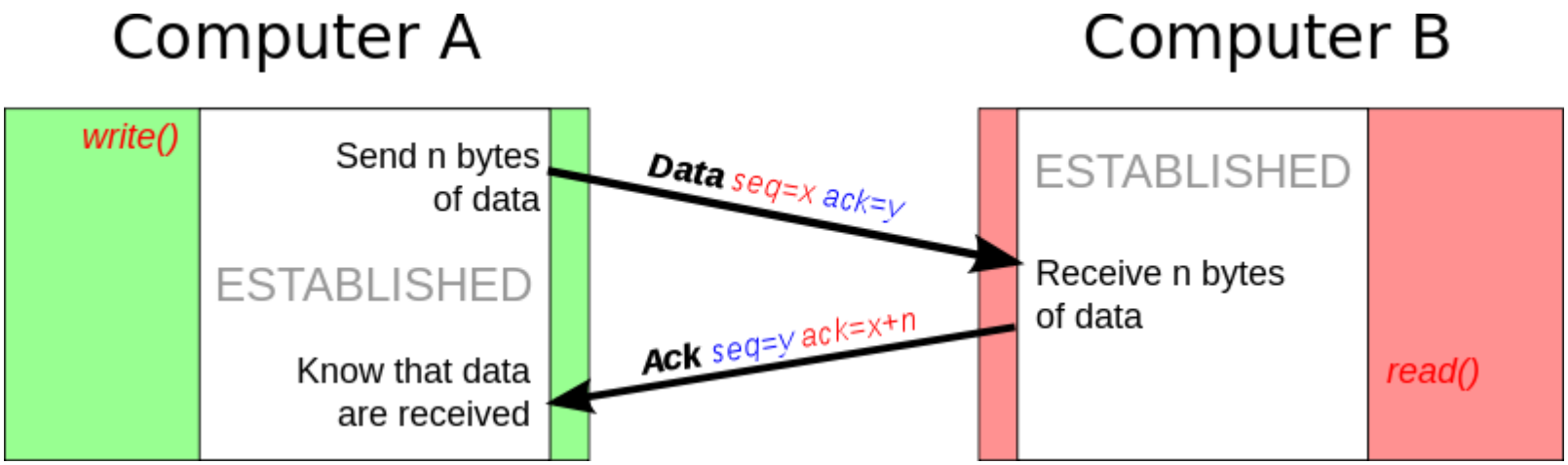
- Bloquer une machine en lui forçant à réserver des ressources

TCP Protocol



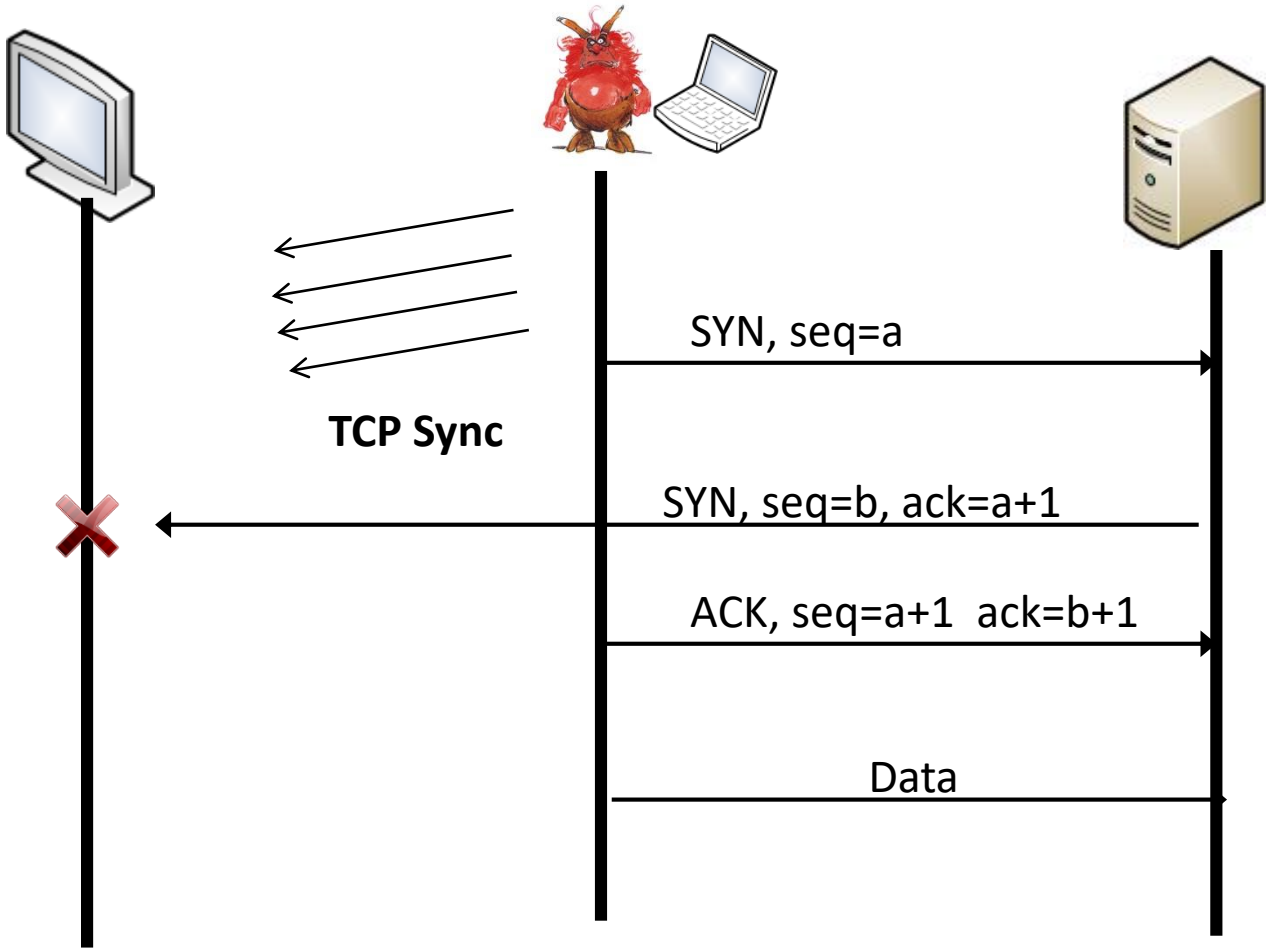
http://fr.wikipedia.org/wiki/Transmission_Control_Protocol

TCP Protocol

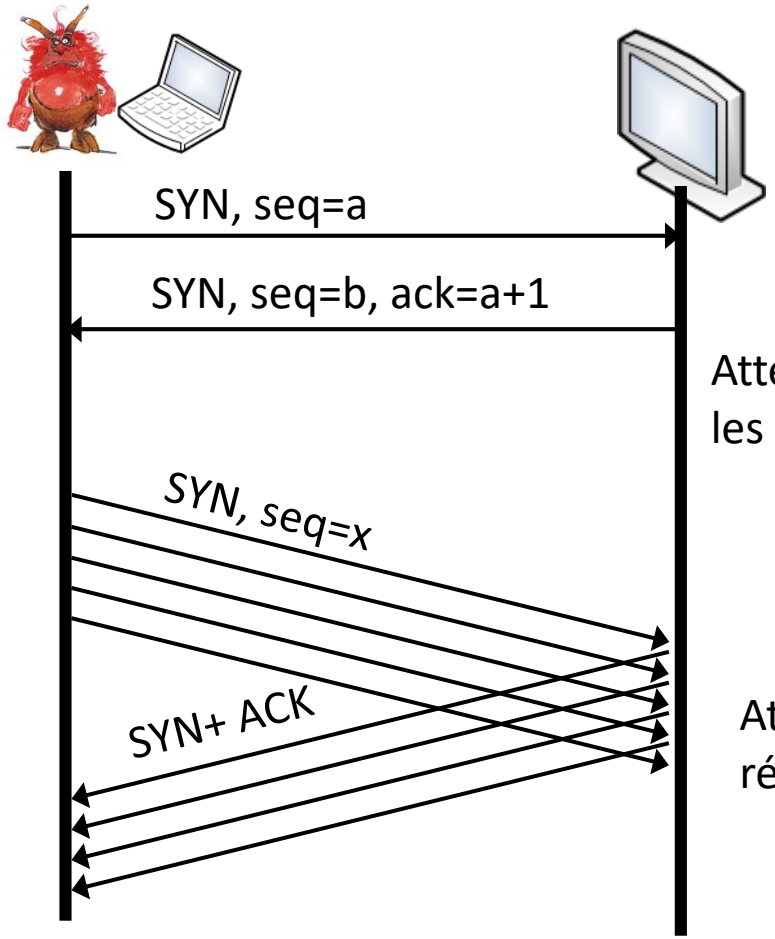


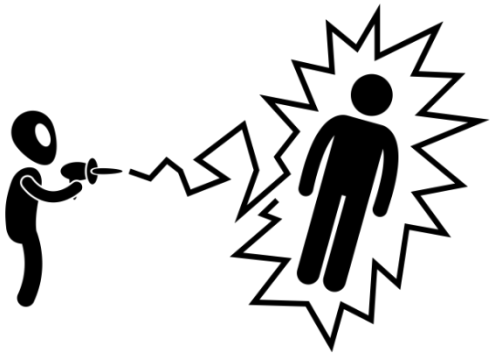
http://fr.wikipedia.org/wiki/Transmission_Control_Protocol

TCP Session Hijacking



TCP Flooding





Comprendre les attaques

- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- BufferOverflow

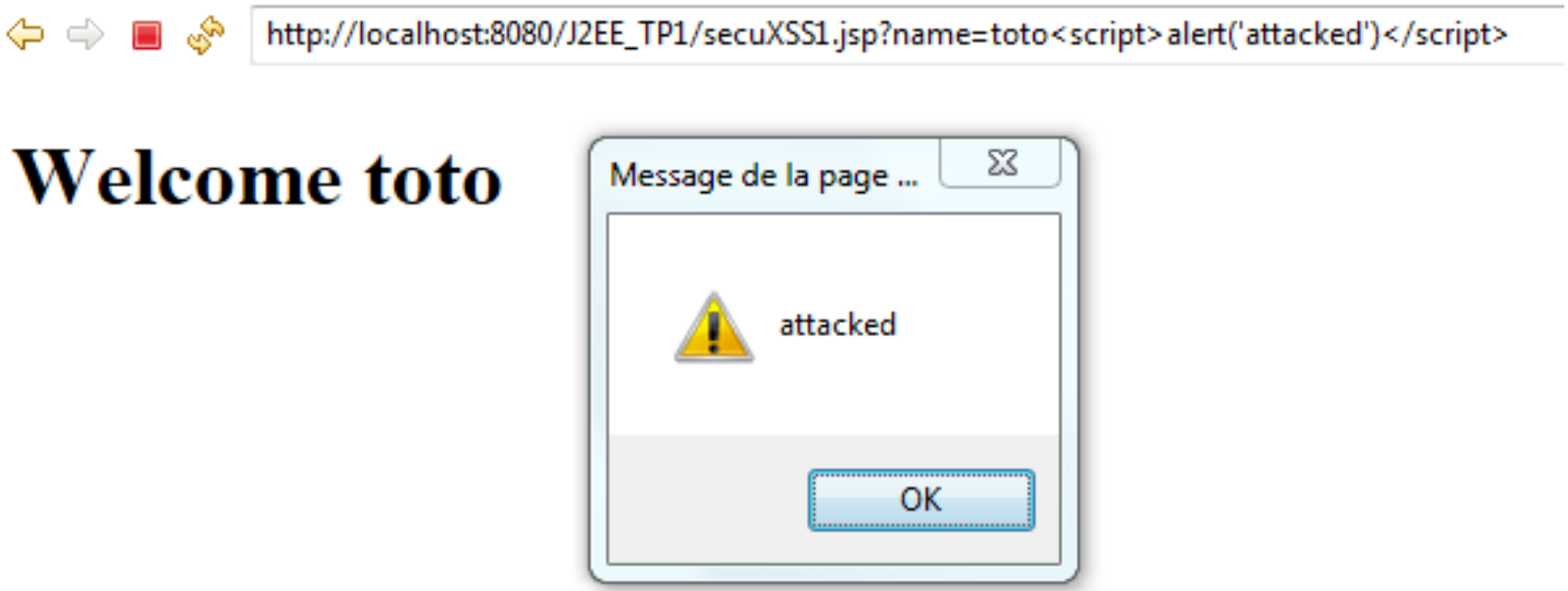
XSS Cross Site Scripting

- **Exécuter du code dans une page web**
  - à l'aide de paramètres
  - à l'aide de formulaires
- **2 grandes familles**
  - XSS non-persistant
  - XSS persistant
- **Menaces**
  - Redirection (parfois transparente) de l'utilisateur (→phishing)
  - Vols d'information (sessions/cookies)
  - Actions malveillantes (défacement, suppression de données) avec l'identité de l'utilisateur courant
  - Modification du site, DoS

XSS Non Persistant

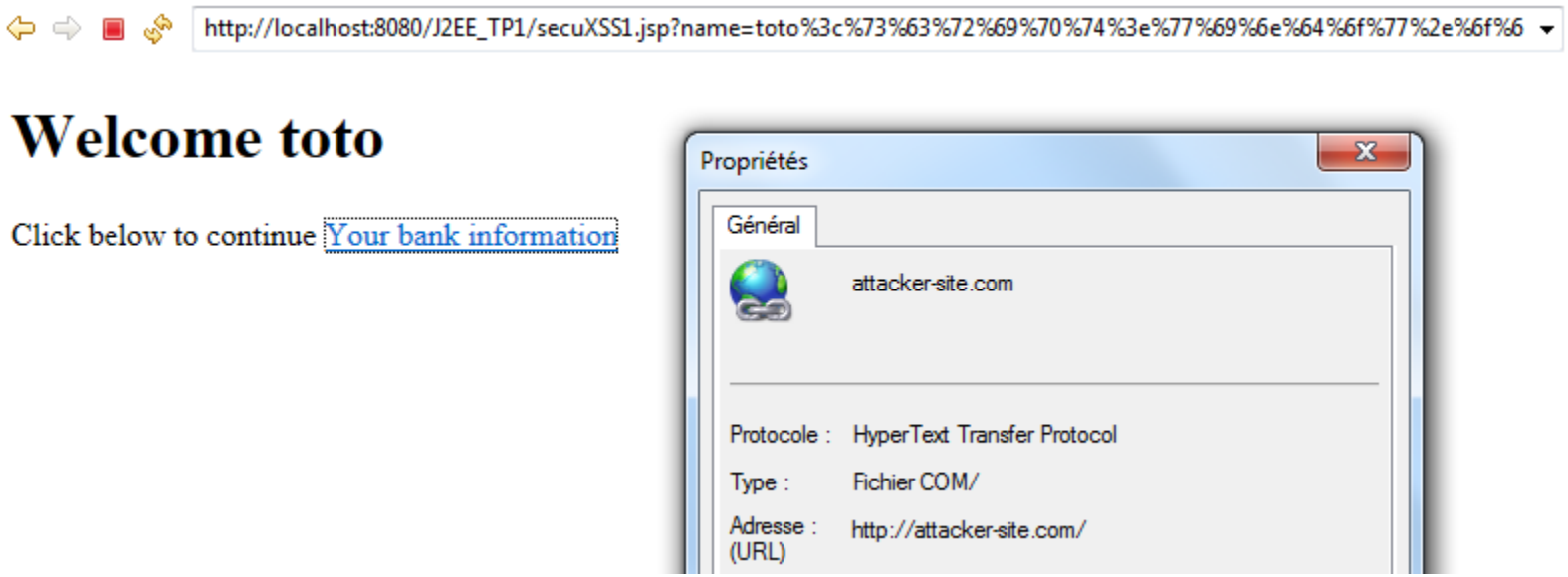
```
<%@ page language="java" contentType="text/html;
    charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
        "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type"
    content="text/html; charset=ISO-8859-1">
</head>
    <body>

        <h1>Welcome <%= request.getParameter("name") %></h1>
        <div>
            Click below to continue
            <a href="http://www.ingdirect.fr/">Your bank information</a>
        </div>

    </body>
</html>
```

XSS Non Persistant

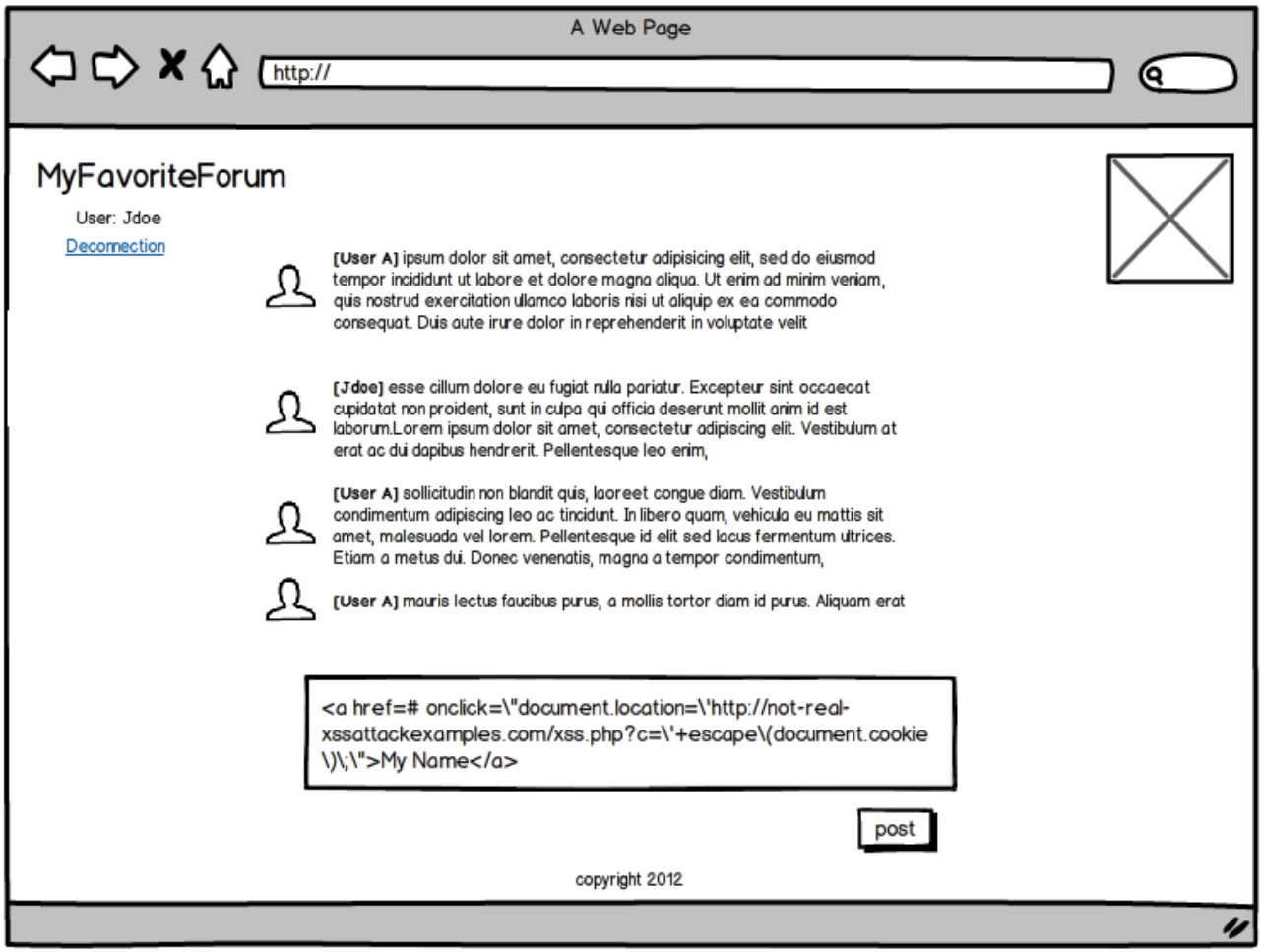


XSS Non Persistant

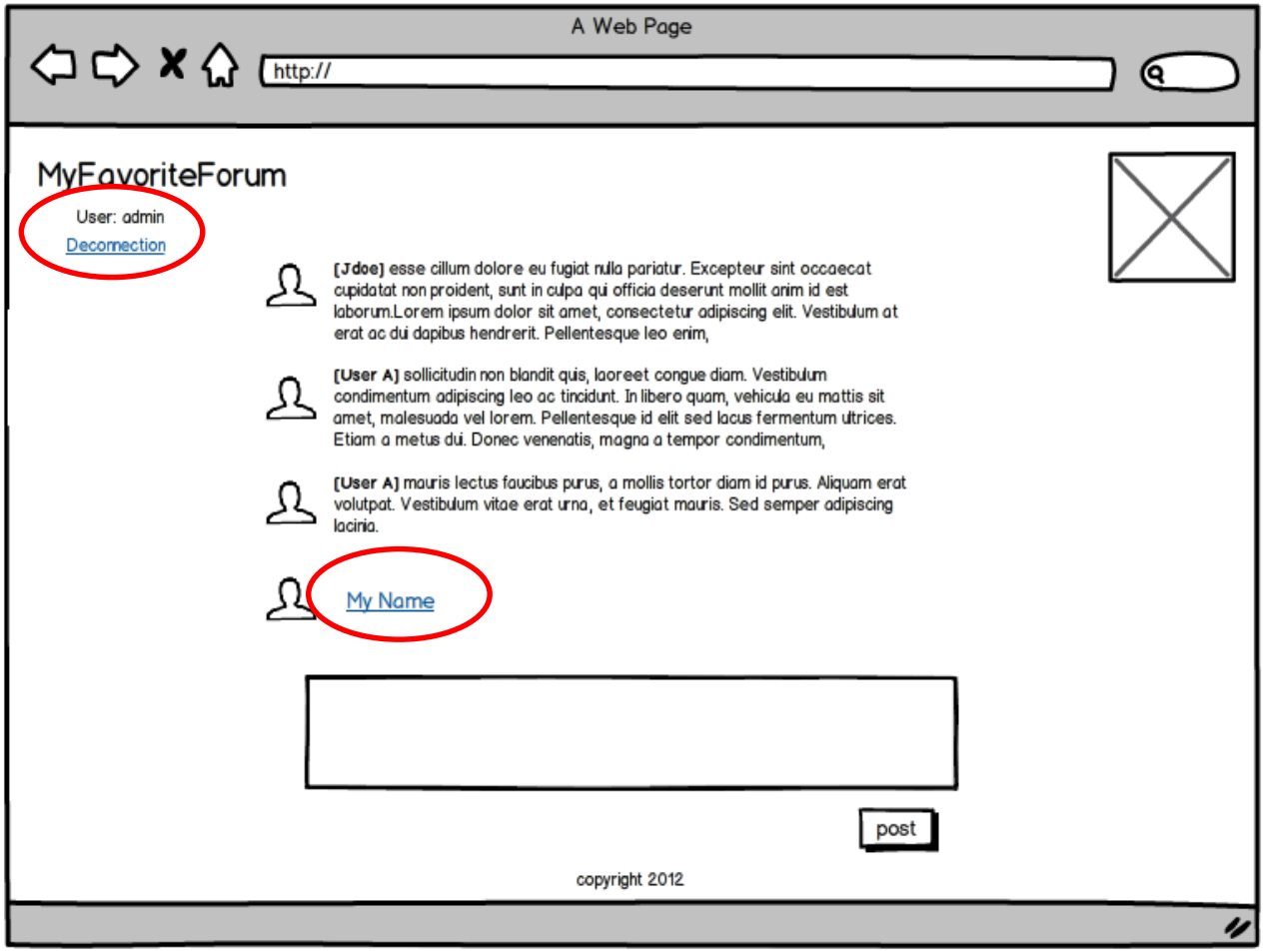
http://localhost:8080/J2EE_TP1/secuXSS1.jsp?name==<script>window.onload = function() {var link=document.getElementsByTagName("a");link[0].href="http://not-real-xssattackexamples.com/";}</script>

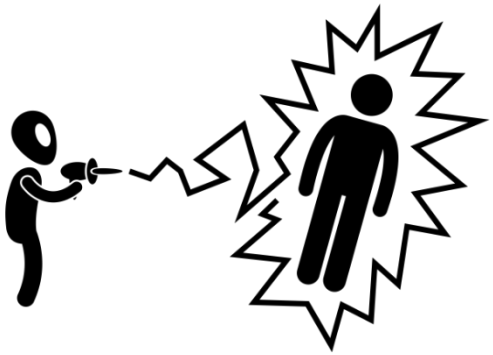


XSS Persistant



XSS Persistant





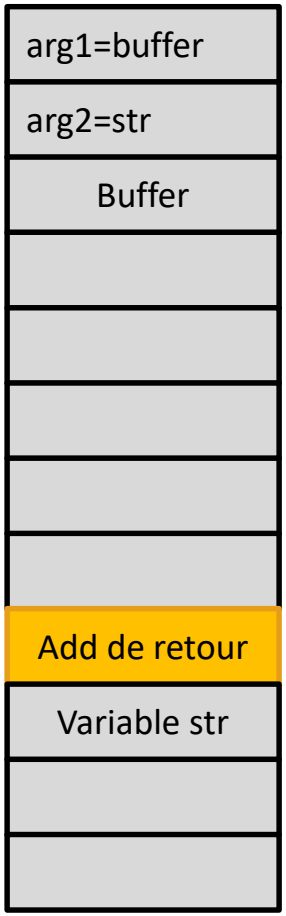
Comprendre les attaques

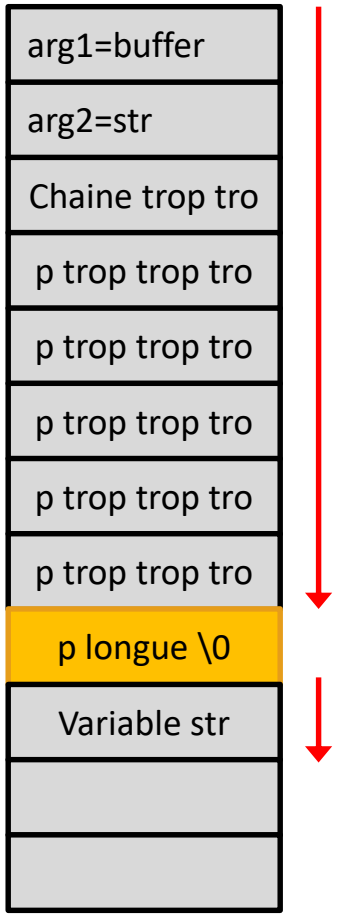
- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- BufferOverflow

Buffer OverFlow

- **Utiliser un bug d'un programme permettant l'exécution d'un code avec les privilèges de ce dernier**
- **2 familles**
  - Stack overflow (pile d'exécution du programme)
  - Heap overflow (mémoire allouée dynamiquement)
- **Menaces**
  - Exécuter du code sur une machine avec des privilèges élevés (root)

Buffer OverFlow



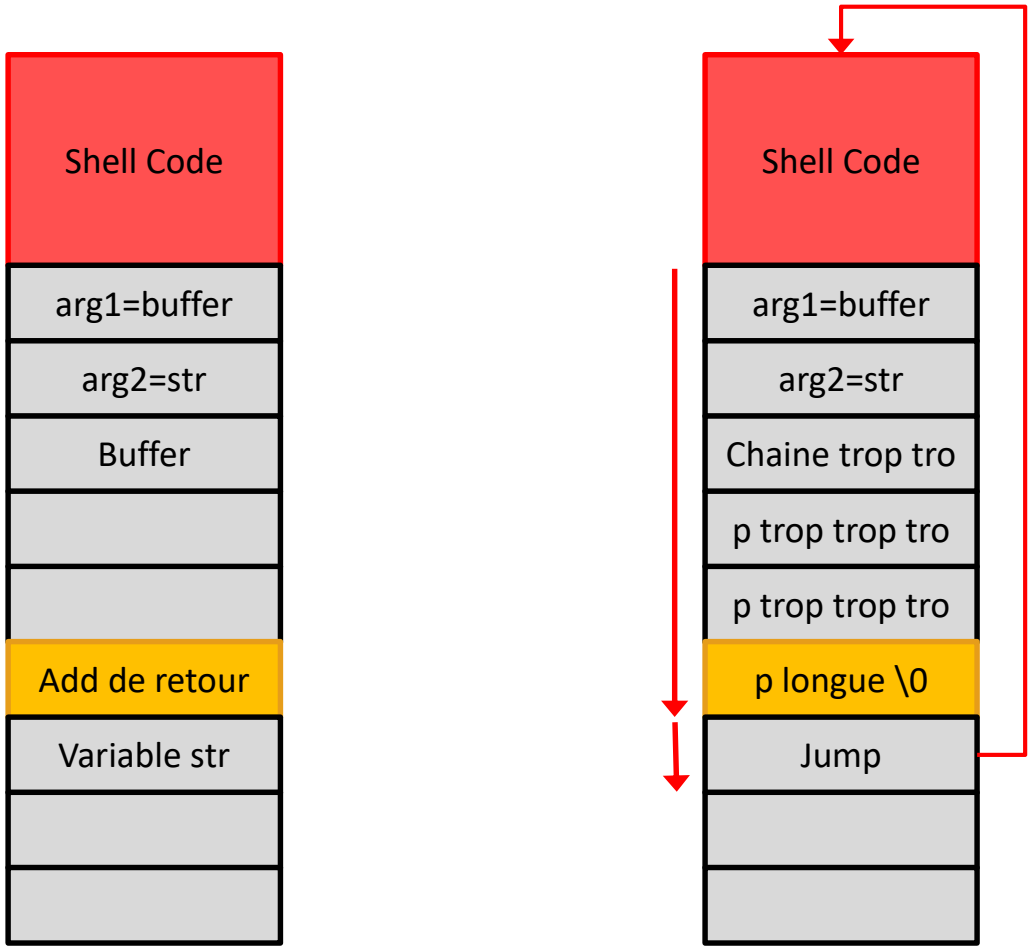


Exécution de la commande strcpy()

Exécution de la commande

Puis exécution du code dans str

Buffer OverFlow



Questions ?

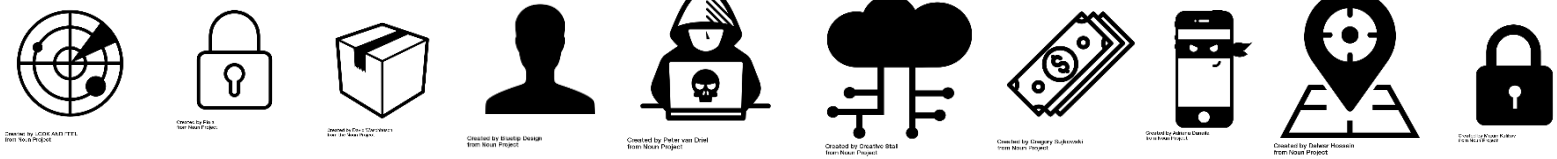
References

References

- Digital in 2017: Global Overview, Hootsuite, 2017
- Trends 17: The Trends to watch in 2017, Globalwebindex, 2017
- TRAFFIC AND Market report June 2012 ON THE PULSE OF THE NETWORKED SOCIETY, Ericsson
- Cisco VNI Mobile 2014
- Cisco visual networking index: Global mobile Data traffic Forecast update, 2016-2021
- TrustWave 2012 Global Security Report
- TrustWave 2013 Global Security Report
- TrustWave Global Security Report 2016
- Kaspersky security report 2014: overall statistic
- Symantec INTERNET SECURITY THREAT REPORT, 2012 Trends, Volume 18, Published April 2013
- Symantec, ISTR, Internet Security Threat Report, 2016
- Radware global Application & Network Security report 2016-17
- Kaspersky Security Bulletin 2016
- Kaspersky Security Bulletin: Overall Statistics for 2016

- Web links
  - http://www.almondsolutions.com/blog/ultimate-list-internet-e-commerce-hosting-stats-facts/
  - http://www.nextnature.net/2012/03/internet-traffic-is-now-51-non-human/
  - https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369
  - http://web.nvd.nist.gov
  - https://www.cvedetails.com/top-50-vendor-cvssscore-distribution.php
  - http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-static/

creative commons



Created by Gan Khoon Lay from Noun Project

Chat by Luiz Henrique Bello Cera from The Noun Project

Quote by irene hoffman from The Noun Project

Globe by Richard Schumann from The Noun Project

LYON
CPE
ÉCOLE SUPÉRIEURE
DE CHIMIE PHYSIQUE ÉLECTRONIQUE
DE LYON

Jacques Saraydaryan

Jacques.saraydaryan@cpe.fr