INF30007

Séance 08 – Sécurité, sûreté

Automne 2023

Définitions

- Sécurité: « Absence ou faiblesse relative de risques d'accidents; mesures prises pour diminuer ces risques… »[1]

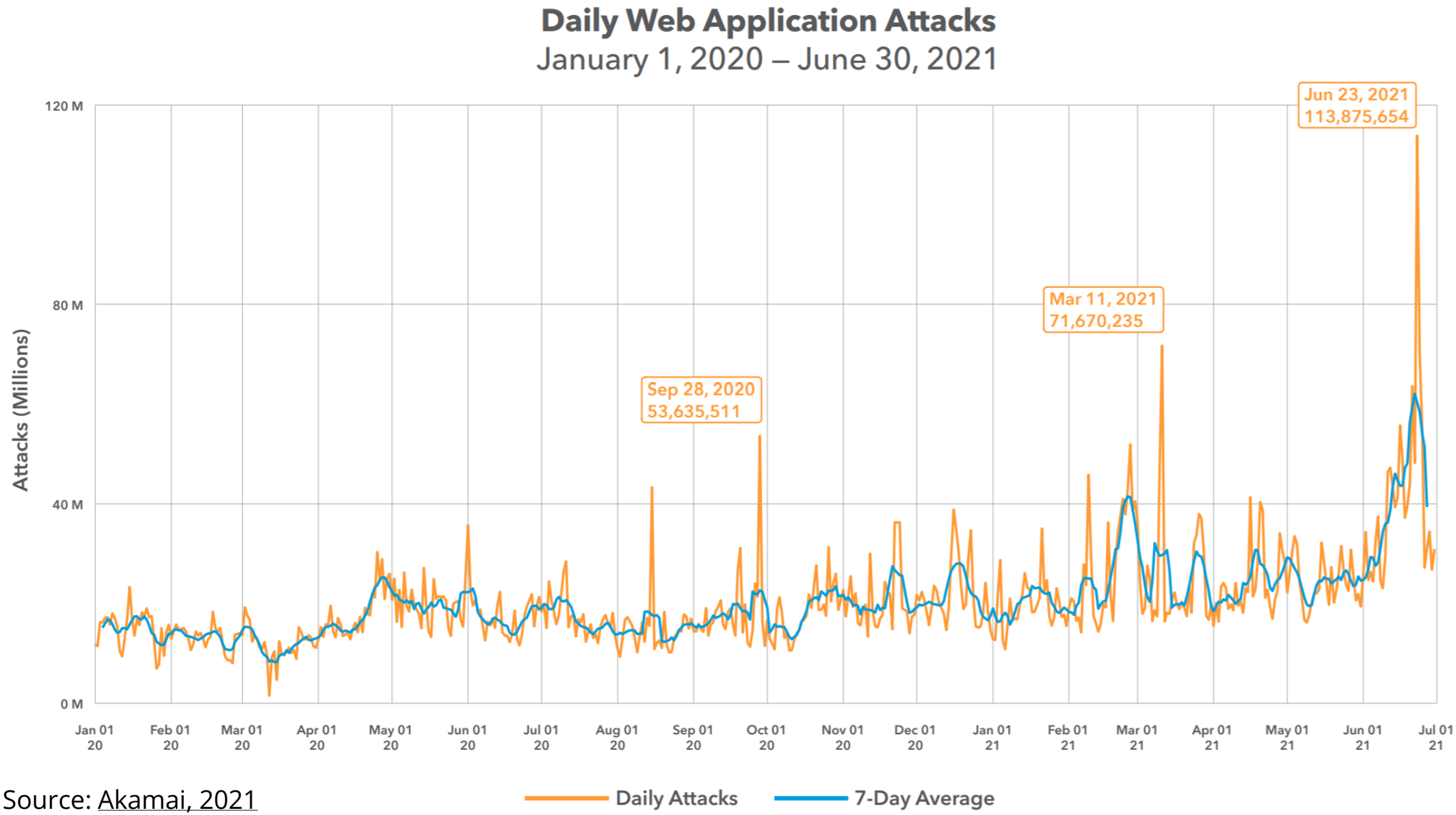
- Sûreté: « caractère de ce qui est sûr », c'est-à-dire qui ne pose pas de danger ou, selon le contexte, « fonctionne de manière fiable et conforme à son type »[1]

[1] Gouvernement du Canada, ministère de la J. (2009, janvier 22). *ministère de la Justice—Harmonisation*. https://www.justice.gc.ca/fra/pr-rp/sjc-csj/redact-legis/juril/no127.html

Préface

Sauce: That Was Close via imgur

Sécurité



Source: Akamai, 2021

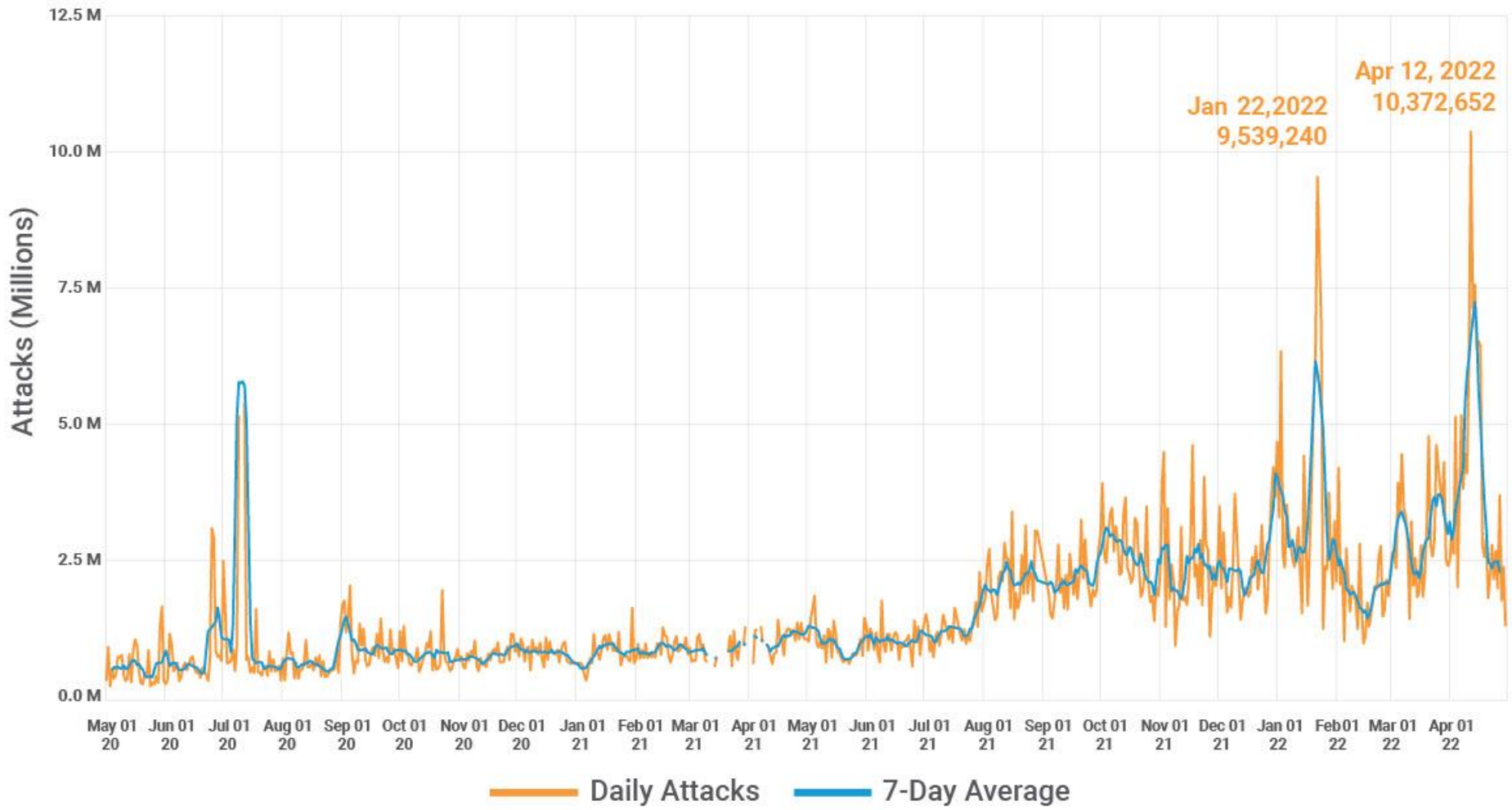


Fig. 1: Daily web application attacks targeting gaming

Source: [Akamai, 2022]

Contexte

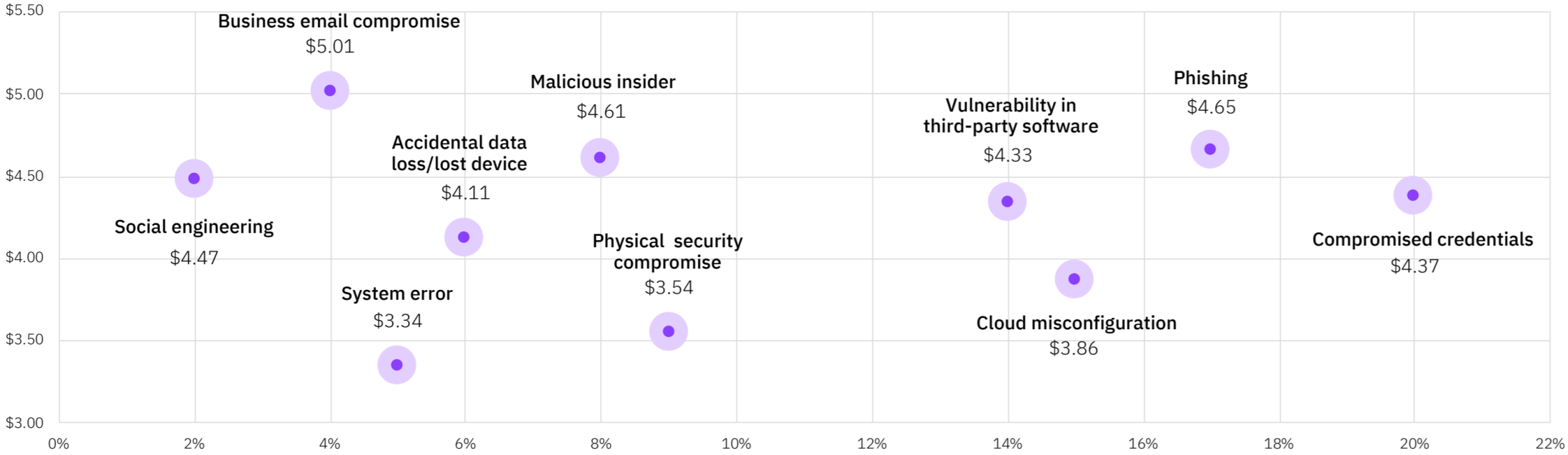
- Vulnérabilité: faiblesse exploitable
- Menace: dangerosité d’une vulnérabilité
- Risque: mesure du dommage causé si une menace se concrétise

Vulnérabilités

- Logicielles
- Matérielles
- Humaines

Average total cost and frequency of data breaches by initial attack vector

Measured in US$ millions

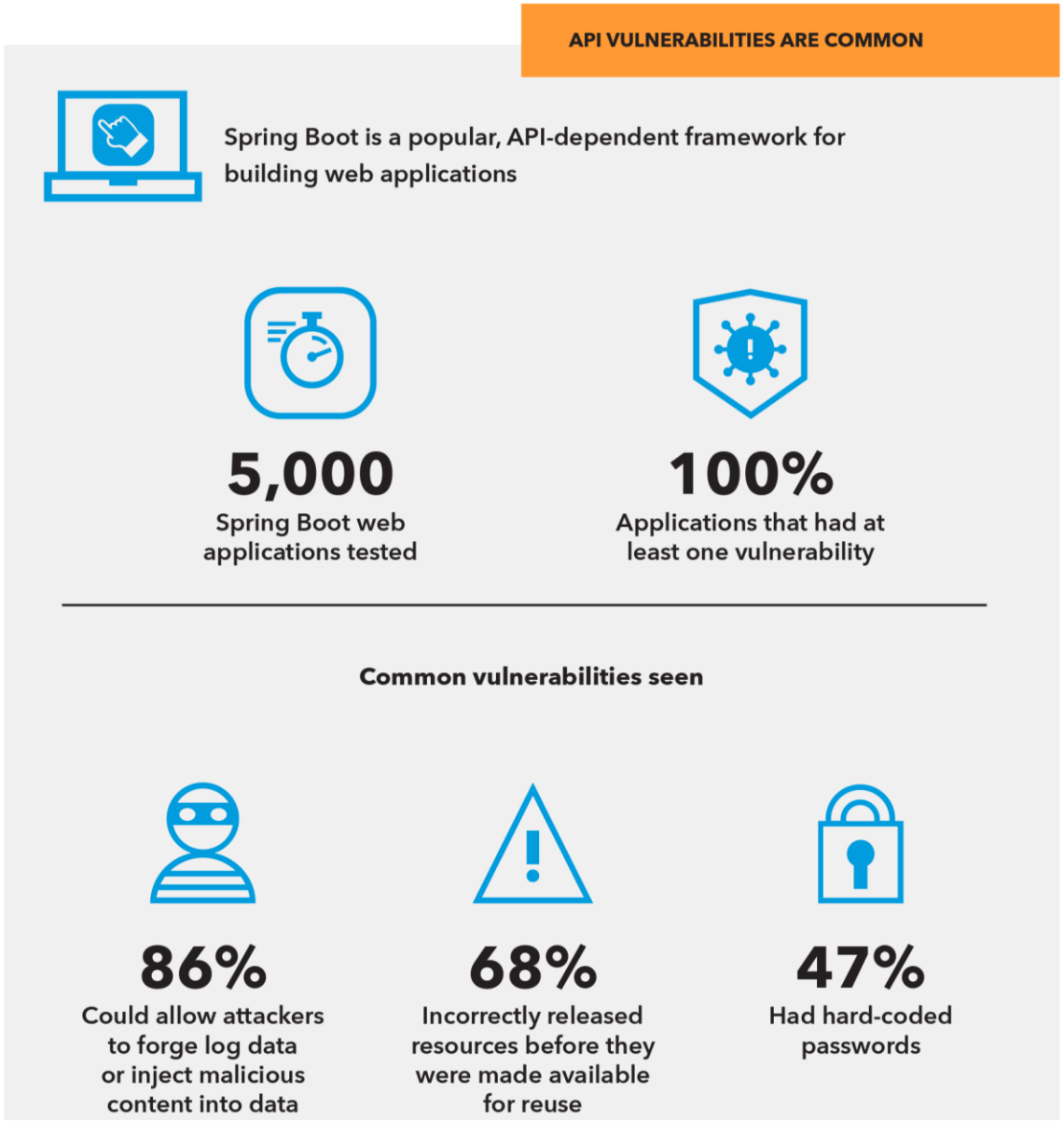


Source: Cost of Data Breach Report 2021 | IBM Security, 2021

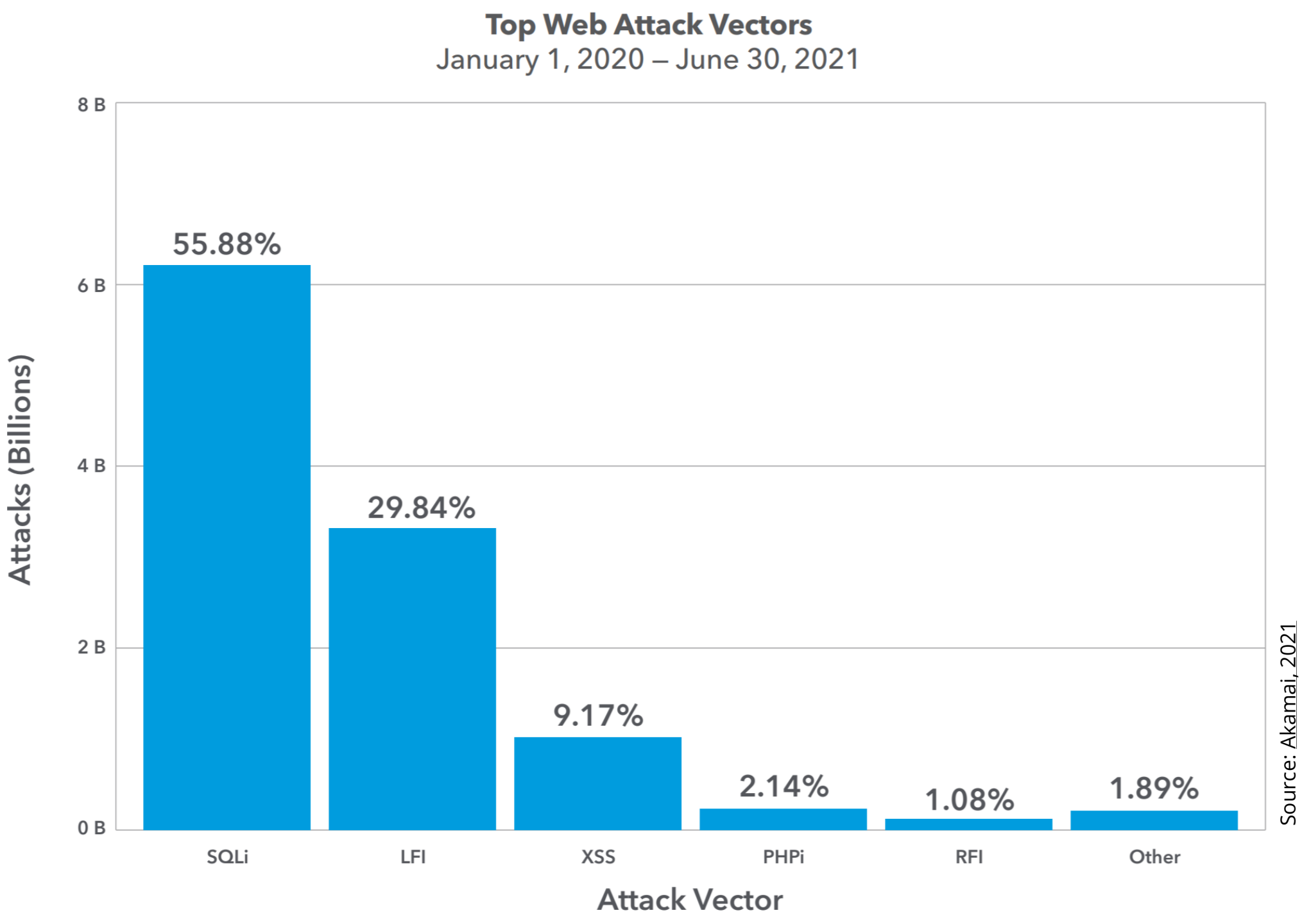
OWASP - Les 10 principales vulnérabilités liés à la sécurité des applications Web

1. Contrôle d'accès défaillant
2. Défaillances cryptographiques
3. Injection
4. Conception non sécurisée
5. Mauvaise configuration de la sécurité
6. Composants vulnérables et obsolètes
7. Défauts d'identification et d'authentification
8. Défauts d'intégrité des logiciels et des données
9. Défauts de journalisation et de surveillance de la sécurité
10. Falsification de requêtes côté serveur

Vulnérabilités dans les API



(Source: *Akamai State of the Internet / Infographic | API*, 2021)


Top Web Attack Vectors
January 1, 2020 – June 30, 2021
8 B
6 B
4 B
2 B
0 B
Attacks (Billions)
55.88%
29.84%
9.17%
2.14%
1.08%
1.89%
SQLi
LFI
XSS
PHPi
RFI
Other
Attack Vector
Source: Akamai, 2021

MITRE 2022 Common Weakness Enumeration (CWE™)
Top 25 Most Dangerous Software Weaknesses (CWE Top 25)

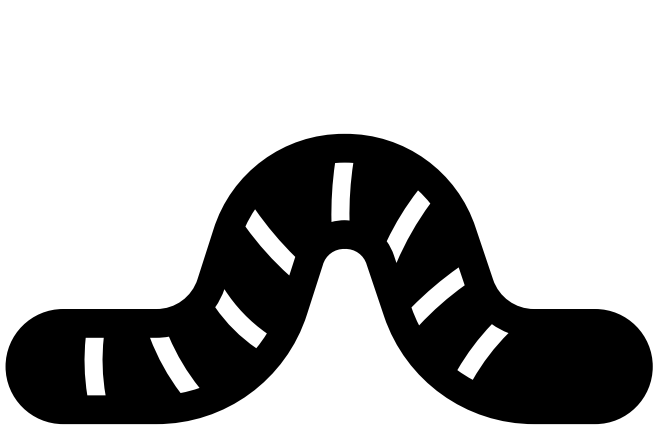
Rank	ID	Name
[1]	CWE-787	Out-of-bounds Write
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[3]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[4]	CWE-20	Improper Input Validation
[5]	CWE-125	Out-of-bounds Read
[6]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[7]	CWE-416	Use After Free
[8]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[9]	CWE-352	Cross-Site Request Forgery (CSRF)
[10]	CWE-434	Unrestricted Upload of File with Dangerous Type
[11]	CWE-476	NULL Pointer Dereference
[12]	CWE-502	Deserialization of Untrusted Data
[13]	CWE-190	Integer Overflow or Wraparound
[14]	CWE-287	Improper Authentication
[15]	CWE-798	Use of Hard-coded Credentials
[16]	CWE-862	Missing Authorization
[17]	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
[18]	CWE-306	Missing Authentication for Critical Function
[19]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
[20]	CWE-276	Incorrect Default Permissions
[21]	CWE-918	Server-Side Request Forgery (SSRF)
[22]	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
[23]	CWE-400	Uncontrolled Resource Consumption
[24]	CWE-611	Improper Restriction of XML External Entity Reference
[25]	CWE-94	Improper Control of Generation of Code ('Code Injection')

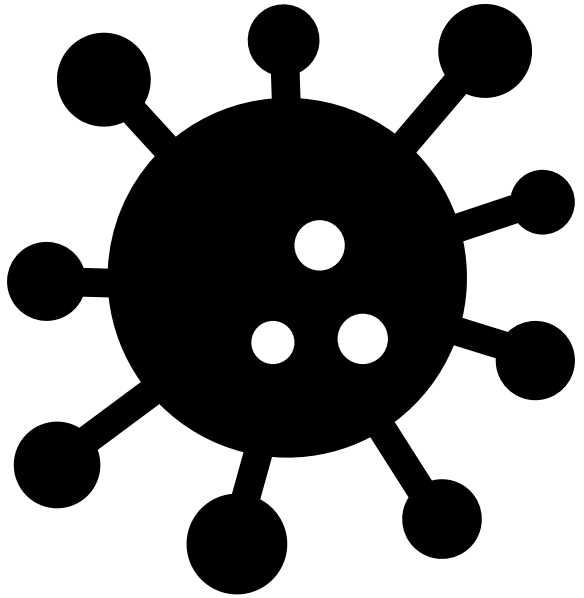
MITRE 2021 Common Weakness Enumeration (CWE™) The 2021 CWE Most Important Hardware Weaknesses

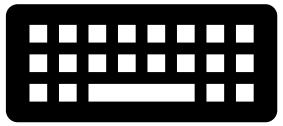
CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
CWE-1231	Improper Prevention of Lock Bit Modification
CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
CWE-1274	Improper Access Control for Volatile Memory Containing Boot Code
CWE-1277	Firmware Not Updateable
CWE-1300	Improper Protection of Physical Side Channels

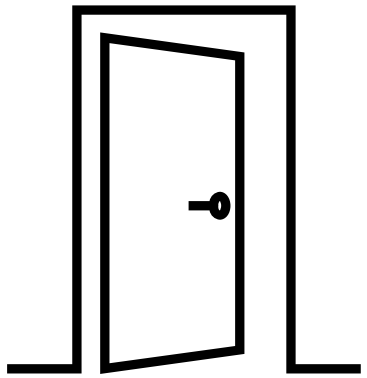
Menaces - logicielles

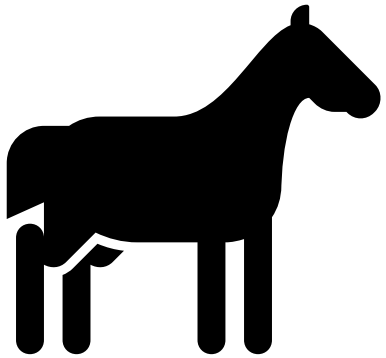
- Virus
- Vers
- Logiciels traqueurs
- Enregistreurs de frappe
- Rançongiciels
- Cheval de Troie
- Backdoor
- Réseau zombie
- Logiciels espions,











Menaces - matérielles

- Intercepteur d'IMSI
- Faux points d’accès
- Backdoor/matériel compromis

New Line Cinema (2002)

Menaces – facteur humain

- « L’erreur humaine est à l’origine de 95% des problèmes de sécurité/sureté informatique » (Forum Économique Mondial, 2022)
- « […] plus des trois quarts (76 %) des employés québécois pensent que la responsabilité de la protection des données de l’entreprise incombe au service informatique » (Terranova Security, 2022)

Menaces – facteur humain

- Pirates informatiques
- Ingénierie sociale
- Hameçonnage
- Harponnage
- Typosquattage
- Espionnage par-dessus l'épaule

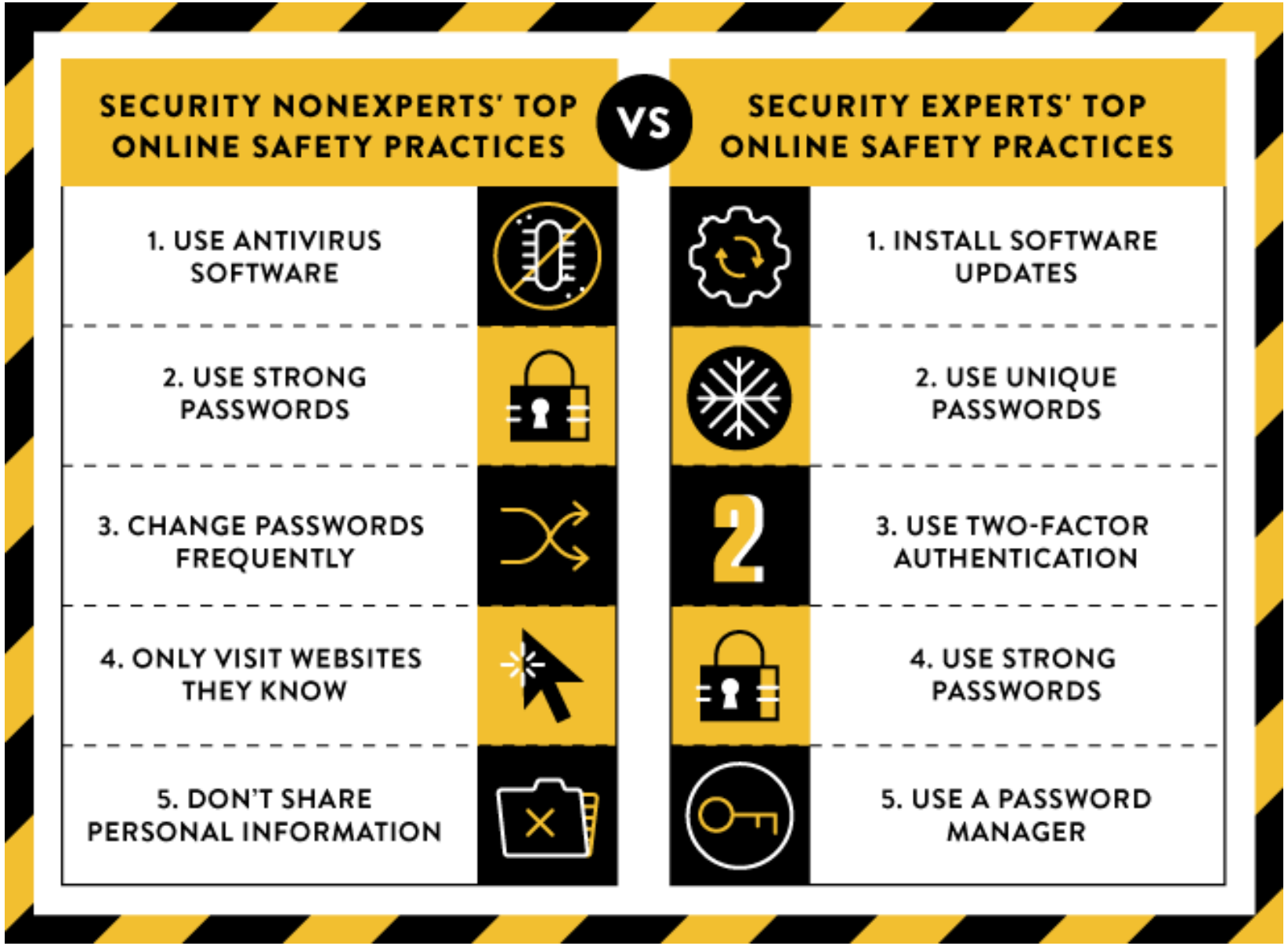
Risques

- Vol d’identité
- Pertes financières/matérielles
- Pertes de vie[1]
- Paralysie de certains secteurs de la société[2]

[1] Eddy & Perlroth, 2020; *German Hospital Hacked, Patient Taken to Another City Dies | SecurityWeek.Com*, s. d.
[2] Le Monde, 2021, Kelly & Resnick-ault, 2021, « Colonial Hackers Stole Data Thursday Ahead of Shutdown », 2021

(quelques) Mesures de sécurité professionnelles

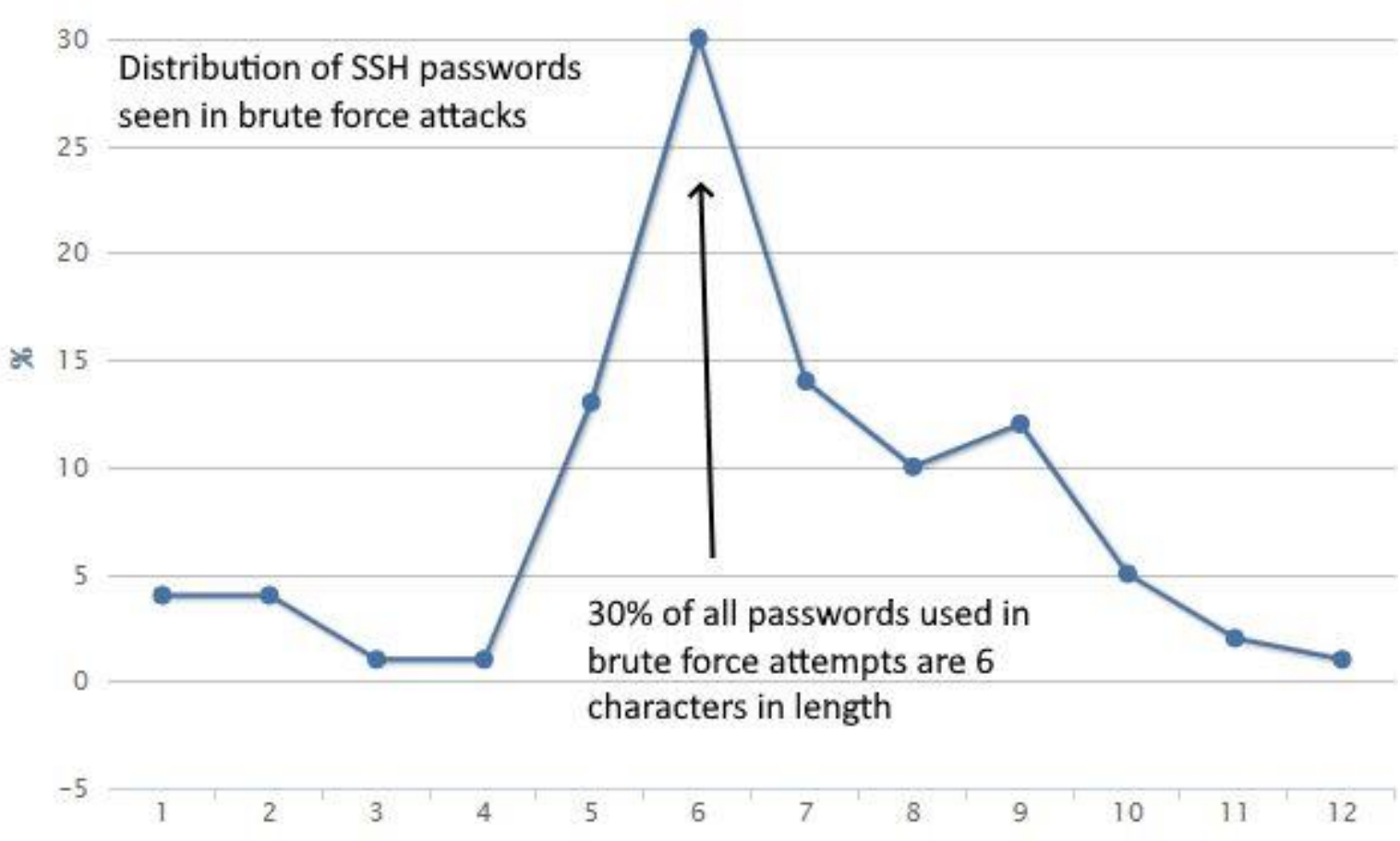
- Veille médiatique
- Maintenance
- Dispositifs pour utilisation professionnelle exclusive
- ~~Configuration par défaut~~
- Modèle Zero Trust



Source : Google Security Blog (2015)

Statistiques intéressantes mots de passe

- Attaques par force brute
- Sur 25 millions d'attaques:
  - 39% contenaient au moins un chiffre
  - 7% contenaient un caractère spécial
  - 0% incluent un espace



Source: Ross Bevington (2021)

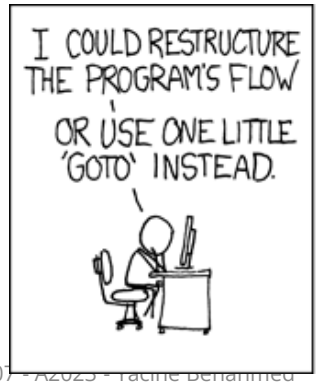
Sûreté

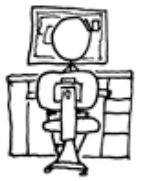
- Frustrations
- Cyberintimidation
- Développement incontrôlable et logiciels incompréhensibles…
- Dispositifs médicaux
- Désastres industriels
- Véhicules autonomes
- L’environnement


imgflip.com

Source: https://healthstreet.program.ufl.edu/2017/12/19/january-is-national-stalking-awareness-month/

Logiciels incompréhensibles

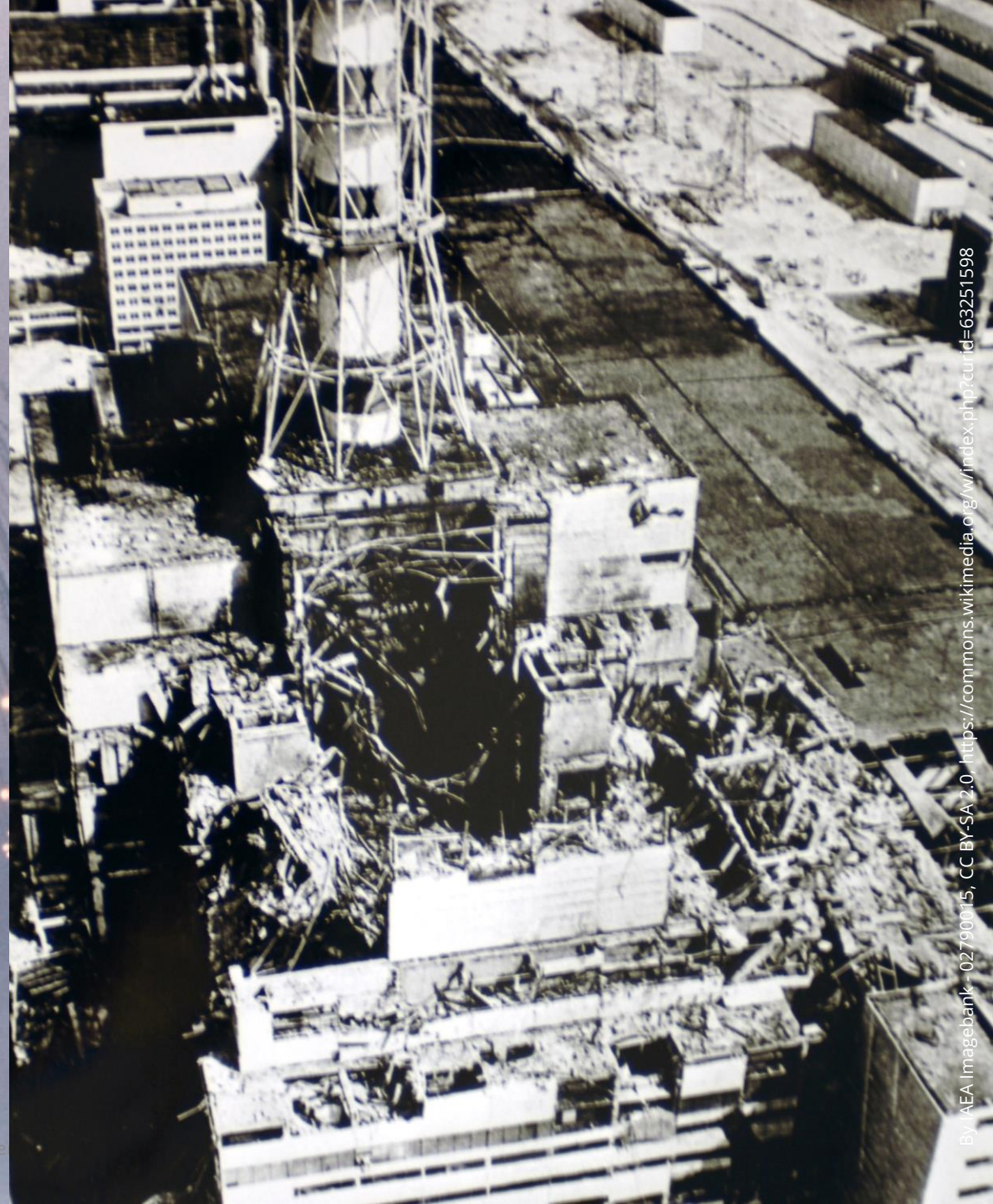


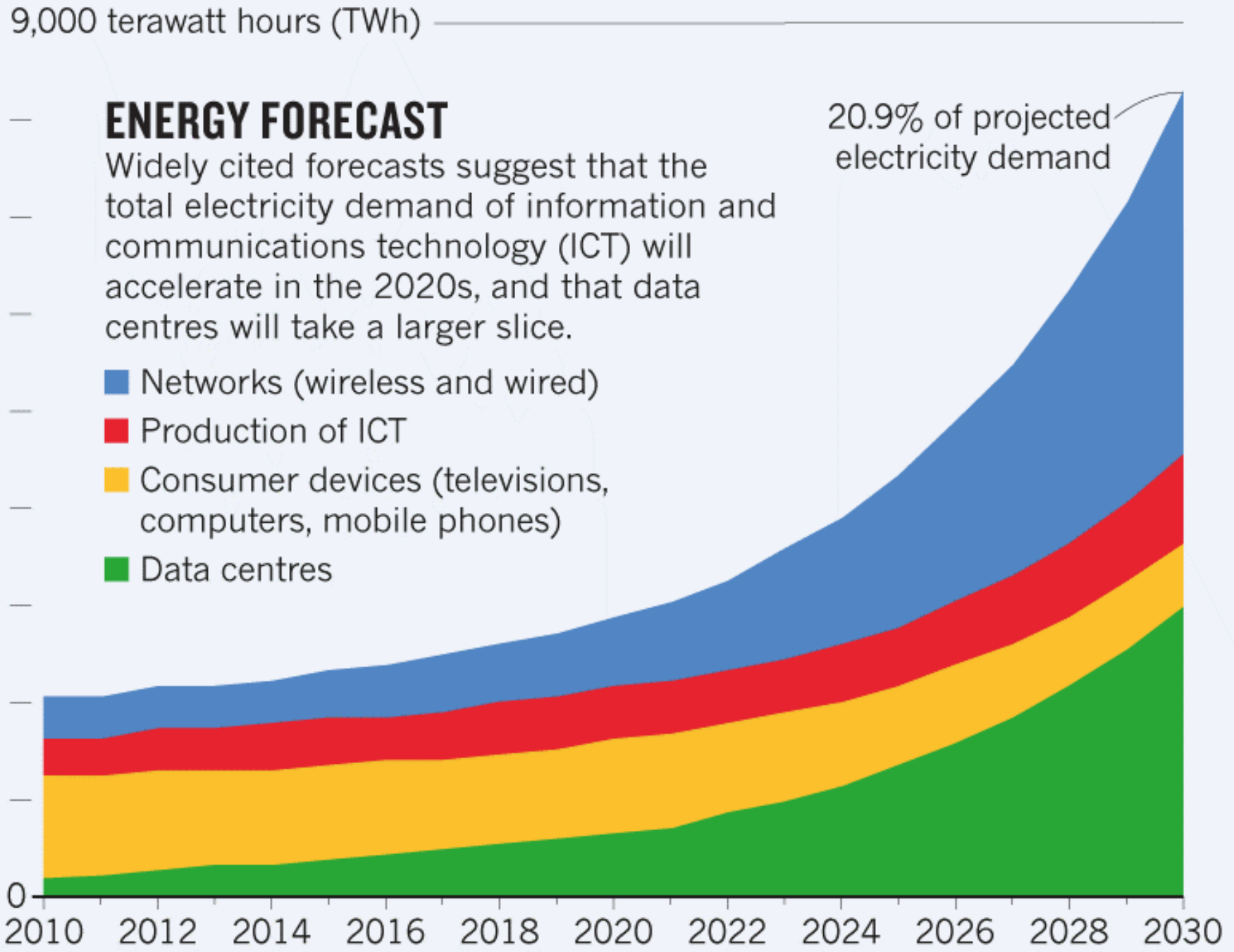


Appareils mécidaux

Illustration par Rob Donnelly

Désastres industriels





Source: Jones (2018)

Références

- Akamai. (2021). *API: The Attack Surface that Connects Us All*. *7*(4), 21.
- Céline Castets-Renard, Émilie Guiraud, & Jacinthe Avril-Gagnon. (2020). *Cadre juridique applicable à l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public au Québec et au Canada.pdf*. 'Observatoire international sur les impacts sociétaux de l'IA et du numérique (. https://www.docdroid.net/YIDTjrr/cadre-juridique-applicable-a-lutilisation-de-la-reconnaissance-faciale-par-les-forces-de-police-dans-lespace-public-au-quebec-et-au-canada-pdf
- *Chilean bank shuts down all branches following ransomware attack | ZDNet*. (s. d.). Consulté 9 septembre 2020, à l'adresse https://www.zdnet.com/article/chilean-bank-shuts-down-all-branches-following-ransomware-attack/
- Cimpanu, C. (s. d.). *Google removes Android app that was used to spy on Belarusian protesters*. ZDNet. Consulté 9 septembre 2020, à l'adresse https://www.zdnet.com/article/google-removes-android-app-that-was-used-to-spy-on-belarusian-protesters/
- Colonial Hackers Stole Data Thursday Ahead of Shutdown. (2021, mai 9). *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown
- *Cost of a Data Breach Report 2021.pdf*. (s. d.). Consulté 1 novembre 2021, à l'adresse https://www.ibm.com/downloads/cas/OJDVQGRY
- CWE. (2021, octobre 27). *CWE - CWE Most Important Hardware Weaknesses*. https://cwe.mitre.org/scoring/lists/2021_CWE_MIHW.html
- *Cybersécurité : Comment se protéger, son entreprise et ses clients en respectant les bonnes pratiques et exigences légales*. (s. d.). Laboratoire de cyberjustice. Consulté 25 août 2020, à l'adresse https://www.cyberjustice.ca/2020/06/19/cybersecurite-comment-se-proteger-son-entreprise-et-ses-clients-en-respectant-les-bonnes-pratiques-et-exigences-legales/
- *Cyberwar, Surveillance and Security*. (s. d.). EdX. Consulté 11 août 2020, à l'adresse https://www.edx.org/course/cyberwar-surveillance-and-security
- Eddy, M., & Perlroth, N. (2020, septembre 18). Cyber Attack Suspected in German Woman's Death. *The New York Times*. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html
- *European Police Malware Could Harvest GPS, Messages, Passwords, More—Slashdot*. (s. d.). Consulté 22 septembre 2020, à l'adresse https://yro.slashdot.org/story/20/09/15/1517203/european-police-malware-could-harvest-gps-messages-passwords-more
- *German Hospital Hacked, Patient Taken to Another City Dies | SecurityWeek.Com*. (s. d.). Consulté 22 septembre 2020, à l'adresse https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
- *GitLab scans its customers' source code, finds it's as fragile as you'd expect*. (s. d.). Consulté 7 octobre 2020, à l'adresse https://www.theregister.com/2020/10/06/gitlab_scans_customer_code_finds/
- Gouvernement du Canada, ministère de la J. (2009, janvier 22). *ministère de la Justice—Harmonisation*. https://www.justice.gc.ca/fra/pr-rp/sjc-csj/redact-legis/juril/no127.html
- *Hackers Attack Every 39 Seconds*. (s. d.). Consulté 3 novembre 2021, à l'adresse https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
- Howard Solomon. (2021, octobre 29). *Attacks on APIs are under-detected and under-reported, says Akamai report*. IT World Canada News. https://www.itworldcanada.com/article/attacks-on-apis-are-under-detected-and-under-reported-says-akamai-report/463391
- IBM Security. (2021). *Cost of a Data Breach Report 2021* (p. 73).
- Kelly, S., & Resnick-ault, J. (2021, juin 9). One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators. *Reuters*. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
- Le Monde. (2021, mai 19). Etats-Unis : Les oléoducs Colonial Pipeline ont versé une rançon de 4,4 millions de dollars à des hackeurs. *Le Monde.fr*. https://www.lemonde.fr/international/article/2021/05/19/etats-unis-les-oleoducs-colonial-pipeline-ont-verse-une-rancon-de-4-4-millions-de-dollars-a-des-hackeurs_6080761_3210.html
- MITRE. (2021, juillet 26). *CWE - 2021 CWE Top 25 Most Dangerous Software Weaknesses*. Common Weakness Enumeration. https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html
- New research : Comparing how security experts and non-experts stay safe online. (2015, juillet 23). *Google Online Security Blog*. https://security.googleblog.com/2015/07/new-research-comparing-how-security.html
- OWASP. (2021). *OWASP Top Ten Web Application Security Risks*. OWASP. https://owasp.org/www-project-top-ten/
- *Patient Dies After Hospital Hit By Ransomware Attack—Slashdot*. (s. d.). Consulté 22 septembre 2020, à l'adresse https://tech.slashdot.org/story/20/09/17/144257/patient-dies-after-hospital-hit-by-ransomware-attack
- *Security Breach Examples and Practices to Avoid Them*. (s. d.). Consulté 15 septembre 2020, à l'adresse https://its.ucsc.edu/security/breaches.html
- *State of the Internet / Infographic | API : The Attack Surface That Connects Us All*. (2021, octobre). https://www.akamai.com/resources/infographic/soti-security-api-the-attack-surface-that-connects-us-all-infographic
- What Are The Common Types Of Network Vulnerabilities? (2020, septembre 23). *PurpleSec*. https://purplesec.us/common-network-vulnerabilities/
- *While encryption will deter data breaches, it comes with its own baggage—And keys*. (2019, juillet 22). SC Media. https://www.scmagazine.com/home/security-news/sc-security-ops-center/encryption-everywhere/
- *(88) Post | LinkedIn*. (s. d.). Consulté 24 novembre 2021, à l'adresse https://www.linkedin.com/posts/ross-bevington-854440152_i-analysed-the-credentials-entered-from-over-activity-6842405845427359744-VF_S/
- Jones, N. (2018). How to stop data centres from gobbling up the world's electricity. *Nature*, *561*(7722), 163-166. https://doi.org/10/gd58cv