INTRODUCTION À LA SÉCURITÉ INFORMATIQUE SÉANCE 1

Marc-Olivier Killijian
UQAM, CNRS
INF4471 A21

PRÉSENTATIONS

- Etudes en France, postdoc en Irlande, carrière à Toulouse en France
- 2001-2019 - Directeur de Recherche CNRS, France
  Langages, Réseaux mobiles, Sûreté de fonctionnement, Protection de la vie privée, Sécurité informatique, Cryptographie homomorphe
- 2017: Directeur-adjoint du **G**roupement **D**e **R**echerche **Sécurité Informatique**
- 2020 : Prof UQAM
  Motivation : penser alternatif, créativité ...
    - Trouver des solutions originales, hors des sentiers battus
    - Imaginer les différentes façons de **1**/arriver à un objectif **2**/empêcher un évènement

MA RECHERCHE

- Sécurité informatique et cryptographie homomorphe
- Protection de la vie privée
  - Données de mobilité
  - Apprentissage
  - Génomique

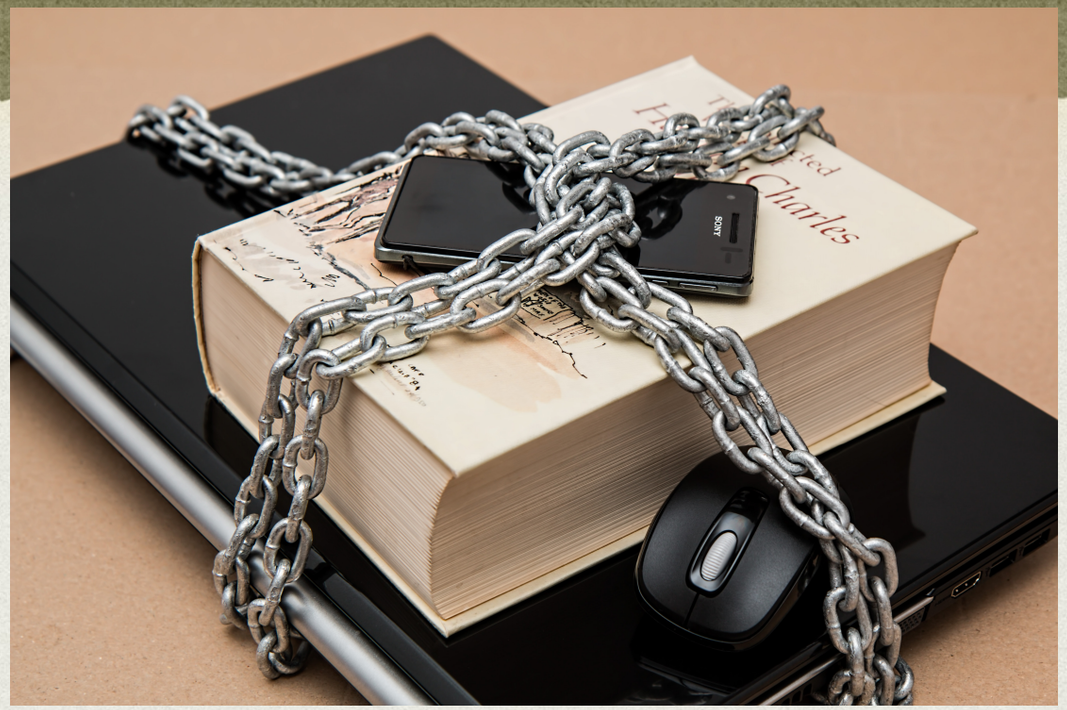
ME CONTACTER

- Questions **organisationnelles**
  - PK4740, mardi pm sur RDV Zoom sur RDV
  - killijian.marc-olivier.2@uqam.ca
- Questions concernant le **cours**
  - Moodle INF4471_604
  - Mattermost

VOUS ?

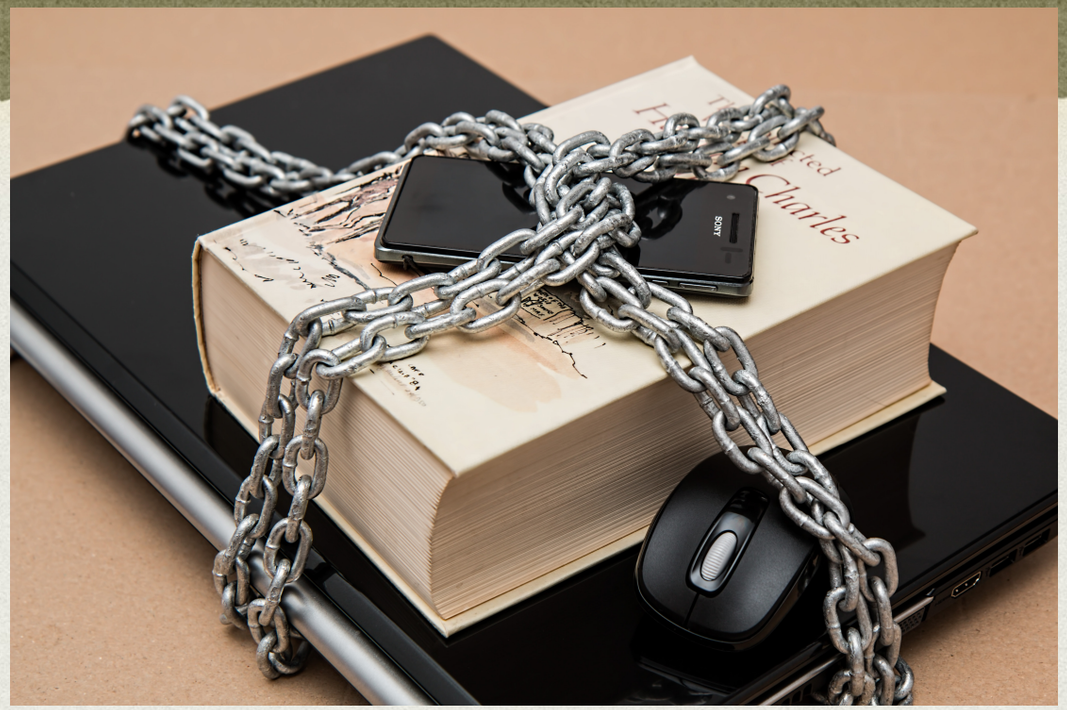
- ~~Tour de table rapide (~20-30s)~~
  Activité par groupe (10 min.)
  - Prénom, Nom, Age, Formation
  - D'où venez-vous ?
  - Pourquoi êtes vous ici
    - @UQAM : motivation professionelle
    - @INFO : intérêts ?
    - INF4471: pourquoi avoir pris ce cours, attendus ?
- Chaque groupe exprime les motivations synthétisées de ses membres

SÉCURITÉ À L'UQAM



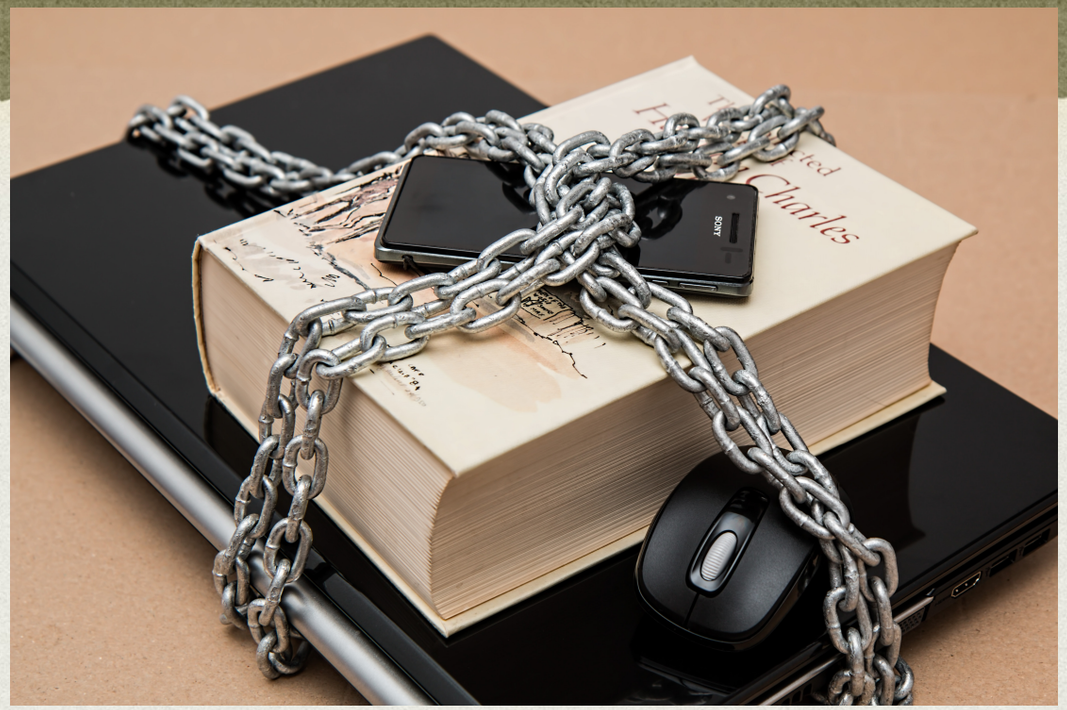
- INF4471 : **Introduction** à la sécurité informatique
- INF600C : Sécurité des logiciels et **exploitation** de vulnérabilités
- INF889A : Maîtrise, **Analyse** de programmes pour la sécurité logicielle
- INF8700 : Maîtrise, Sécurité des systèmes, données et **contrats**
- INF8750 : Maîtrise, **Sécurité** des systèmes informatiques, version avancée de INF4471
- EMB7025 : Maîtrise, Sûreté et sécurité des systèmes **embarqués**

SÉCURITÉ À L'UQAM



- INF4471 : **Introduction** à la sécurité informatique
- Cours d'intro à la sécurité info au bac !
  - ~~Devenir des experts~~

POURQUOI CE COURS?



- ~~Pourquoi s'intéresser à la sécu ?~~

- Pourquoi s'initier à la sécu ?
  - Tout le monde devrait avoir un cours d'**hygiène informatique** !
  - Tous les informaticiens doivent connaitre les **bonnes pratiques** !
  - Peut-être que vous y prendrez gout !

2 OBJECTIFS PRINCIPAUX

Hygiène informatique

Risques, problématiques et mécanismes de sécurité

5 OBJECTIFS GÉNÉRAUX

1. **Comprendre** l'ensemble des **problématiques** de la sécurité informatique
2. **Manipuler** de façon **sécuritaire** les outils informatiques
3. **Expliquer** les principaux **mécanismes** de sécurité
4. **Identifier** les **risques et menaces**, actuels et futurs
5. **Proposer** des **mesures de contrôle** appropriées

PLAN DE COURS

- S1: Avoir un **panorama global de la sécurité**, le vocabulaire, les enjeux, les besoins, les propriétés, les moyens d'y parvenir, etc.

- S2: **Fuites d'information et vie privée** - Identifier les canaux cachés, potentielles fuites d'information; comprendre les enjeux de la PvP, du contrôle de la dissémination des données; de mécanismes de protection des données.

- S3: **Géolocalisation, géopolitique et intelligence économique** - Enjeux économique, politiques et étatiques de la sécu; problématiques de la « Geo-vie-privée ».

- S4: **Fraude sur Internet** - les différents types de fraudes, leurs motivations et leurs contre-mesures + bonus et préambule à la crypto=arithmétique modulaire.

PLAN DE COURS

- S5: **Cryptographie symétrique** - Histoire de la crypto; DES, 3DES, AES, chiffrement par blocs ou par flux; théorie et pratique.

- S6: **Communications anonymes, darkweb et messageries sécurisées** - P2P, Darkweb, routage en oignon, TOR, chaine de blocs, Bitcoin; Messageries sécurisées, VPNs et accréditation anonymes.

- S7: **Présentations** par équipe de sujets « Sécurité », on y revient

- S8: **Malware et antivirus** - histoire et typologie des malwares; analyse de malware, pots de miel; systèmes de détection d'intrusion; antivirus; mises-à-jour.

- S9: **Crypto asymétrique** - propriétés de la crypto asymétrique; bases mathématiques (calculs entiers, PGCD, modules et exponentiation modulaire); RSA; chiffrement homomorphe.

PLAN DE COURS

- S10: **Courriel, pourriel, signatures électronique et gestion de clés** - Pourriel et détection; signatures électroniques, DSA, RSA; log-discret ; infrastructure de gestion de clé; certificats.

- S11: **Mots de passe et authentification** - Hachés, MD5, SHA-1, SHA-3, MAC et HMAC; Mots de passes, évaluation et conservation; Biométrie.

- S12: **Chiffrement de disque dur et forensique** - pourquoi, fonctionnement et comment chiffrer son disque dur; forensique, expertise judiciaire, réponse à incidents.

- S13-S14: **Sécurité réseau** - TCP/IP, attaques et protections réseau; protocoles, VPN, IPSec, SSH, SSL; réseaux sans-fil

MODALITÉS PÉDAGOGIQUES

- Différentes **activités obligatoires**
  - Cours, laboratoires, lectures, ballados, vidéos, etc.
  - **~100h de travail requis sur la session**
  - répartition **variable** de 5 à 8h/semaine
- Certaines activités **optionnelles**, parfois *in english*

COMMUNICATION

- **Mattermost** - toutes les questions d'intérêt général (contenu ou organisation du cours) - participation (Q&R) évaluée

- Courriel si plus personnel ou confidentiel
  killijian.marc-olivier.2@uqam.ca : cours
  bouderbala.merouane@courrier.uqam.ca : labos

- RDV si besoin

EVALUATIONS

1	Devoir 1	25 %	10 octobre
2	Présentation par équipes de 5	20 %	19 octobre
3	Devoir 2	25 %	14 novembre
4	Examen final	30 %	14 décembre

EVALUATIONS

- cf. plan de cours
- cf. entente d’évaluation
  - discussion 5min.
  - vote

DE QUOI ON PARLE?

La sécurité informatique d'hier à aujourd'hui

LA SÉCURITÉ INFORMATIQUE ?

LEDEVOIR

Un bogue informatique crée la confusion dans les primaires démocrates de l'Iowa

Photo: Alex Wong / Getty Images / Agence France-Presse Un bogue informatique dans l'application utilisée par le parti aurait provoqué un comptage partiel des voix.

Ivan Couronne - Agence France-Presse et Agnès Bun - Agence France-Presse
à Washington et à Manchester

4 février 2020

États-Unis

Le camp démocrate aux États-Unis était plongé dans l'embarras et l'incompréhension mardi après la première échéance des primaires présidentielles la veille dans l'Iowa, où aucun résultat officiel n'a encore pu être publié et où deux candidats revendiquent la victoire.

Le président Donald Trump a jubilé face au chaos du parti qui espère l'expulser de la Maison-Blanche en novembre, tweetant que le spectacle illustrait l'« incompétence » de ses adversaires. La semaine se profile bien pour lui, qui prononcera mardi soir son grand discours annuel au Congrès, et se dirige vers un acquittement mercredi au Sénat dans son procès en destitution.

LA SÉCURITÉ INFORMATIQUE ?

LEDEVOIR

Les systèmes informatiques du gouvernement fédéral menacent de s'effondrer

Photo: iStock M. Trudeau a été informé après les élections d'octobre que des systèmes et des logiciels cruciaux «sont en train de se détériorer et menacent de tomber en panne».

La Presse canadienne
à Ottawa
1 février 2020
Science

Les systèmes informatiques du gouvernement fédéral, essentiels aux versements à l'ensemble des prestataires, sont en piètre condition et menacent de s'effondrer, selon une note de synthèse transmise au premier ministre Justin Trudeau.

M. Trudeau a été informé après les élections d'octobre que des systèmes et des logiciels cruciaux « sont en train de se détériorer et menacent de tomber en panne ». Cette situation nécessite une

LES PLUS POPULAIRES

1 CHRONIQUE
Le pitbull

2 La montée de l'extrême droite plonge l'Allemagne dans une crise politique

3 Chercher le «fuck» (et le trouver partout)

LA SÉCURITÉ INFORMATIQUE ?

LEDEVOIR

Le piratage informatique a coûté 45 milliards en 2018

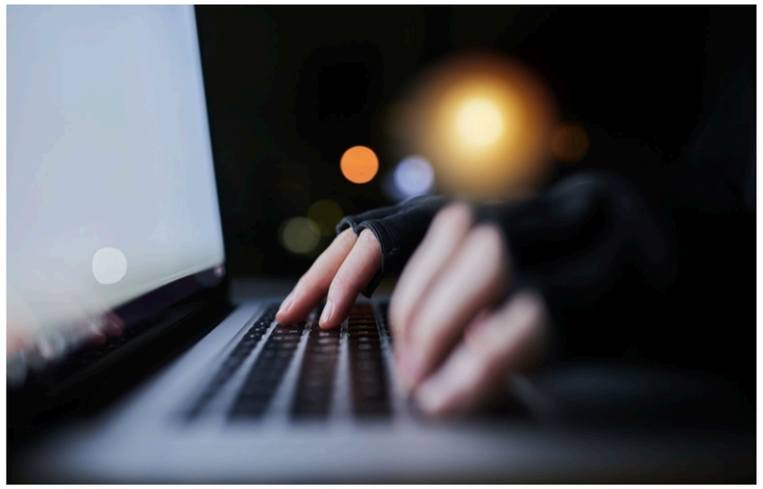


Photo: Getty Images L'Alliance pour la confiance en ligne a dénombré environ 6515 failles informatiques ayant exposé les données de cinq milliards de fichiers, ce qui est un peu moins qu'en 2017. Mais ces chiffres sont probablement inférieurs à la réalité.

Agence France-Presse
À Washington
10 juillet 2019
Économie

Entre logiciels malveillants et documents contenant un virus, les pirates informatiques ont mené environ deux millions d'attaques en 2018 ayant coûté mondialement plus de 45 milliards de dollars, d'après une étude américaine dévoilée mardi.

Selon l'Alliance pour la confiance en ligne de la société Internet, qui a compilé des données provenant du monde entier, les rançongiciels auraient coûté 8 milliards. Ces attaques consistent à s'emparer des

LA SÉCURITÉ INFORMATIQUE ?

Japan says defence data possibly breached

By Staff Writer
Feb 12 2020
2:00PM

0 Comments

RELATED ARTICLES

WA's P&N Bank hit by data breach

IT contractor faces new charges over LandMark White data breaches

NAB sheds new light

After cyber attacks on Mitsubishi Electric.

The Japanese defence ministry said late on Monday that sensitive data on defence equipment may have been breached as a result of cyber attacks on Mitsubishi Electric, a major supplier of the country's defence and infrastructure systems.

The company has told the ministry that potentially stolen data included requirements for defence equipment that the ministry specified for contract bidders in October 2018, the ministry said in a statement.

The ministry said it was still in the process of investigating the security impact of the potential leak. Mitsubishi Electric did not win the contract in the auction.

LA SÉCURITÉ INFORMATIQUE ?

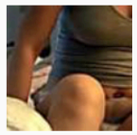
Personal data of all 6.5 million Israeli voters exposed by security flaw in app

By Oren Liebermann and Michael Schwartz, CNN

Updated 1:21 PM ET, Tue February 11, 2020

Trump announces Mideast plan alongside Israeli prime minister 01:51

MORE FROM CNN BUSINESS


The ad you didn't see during the Oscars

CEO forced out after calling Uber driver racial slur

Recommended by outbrain

Ajoutez le Wi-Fi Partout chez vous.

Location de 4 capsules
10 $/mois

Plus d'info

Bell

LA SÉCURITÉ INFORMATIQUE ?

Personal information hacked from Carson City online utility payment system

Carson City | February 11, 2020

Geoff Dornan
gdornan@nevadaappeal.com

82

Hackers managed last fall to access Carson City's water bill payment system on the city website, obtaining personal information including credit card data of some 2,000 customers

Une université américaine verse 457 000 dollars de rançon

Sécurité : *Les responsables de l'université ont restauré à partir des sauvegardes, mais ils ont dû payer le groupe de ransomware pour empêcher la divulgation des données des étudiants.*

Par Catalin Cimpanu | Modifié le vendredi 21 août 2020 à 12:23

Réaction 1 Partager 15 Tweeter Partager plus +

L'université de l'Utah a révélé hier qu'elle avait payé 457 059 dollars à un groupe de ransomware afin d'éviter que des pirates informatiques ne divulguent en ligne des informations sur ses étudiants.

publicité

Des rançons sur les données

Cet incident est le dernier en date d'une longue série d'attaques au ransomware, au cours desquelles des groupes

Extorsion

Alerte à la fraude!

21 août 2020 : Fraude du numéro d'assurance sociale (NAS)

Nous avons reçu des rapports sur une nouvelle tendance de fraude téléphonique qui consiste à faire croire aux victimes que leur numéro d'assurance sociale (NAS) a été bloqué, compromis ou suspendu. Demeurez vigilant!

Les fraudeurs se font passer pour des employés d'organismes gouvernementaux, notamment Service Canada, la GRC ou divers palais de justice et s'arrangent pour que le numéro de téléphone de ces organismes apparaisse sur votre afficheur. Ils demandent alors aux victimes de fournir leur NAS et d'autres renseignements personnels (date de naissance, nom, adresse, etc.). Les personnes qui s'exécutent risquent d'être victimes de fraude à l'identité.

31 juillet 2020 : Les communautés asiatiques au Canada sont la cible d'appels

Les communautés asiatiques au Canada sont la cible d'appels automatisés dans lesquels on prétend avoir un message urgent d'une entreprise de messagerie (comme DHL) ou d'un organisme d'application de la loi étranger (p. ex. la police de Beijing, les douanes de Shanghai). Ces appels peuvent être très menaçants et intimidants. Si vous recevez un de ces appels, raccrochez tout de suite et signalez l'incident à votre poste de police ou au Centre antifraude du Canada (CAFC).

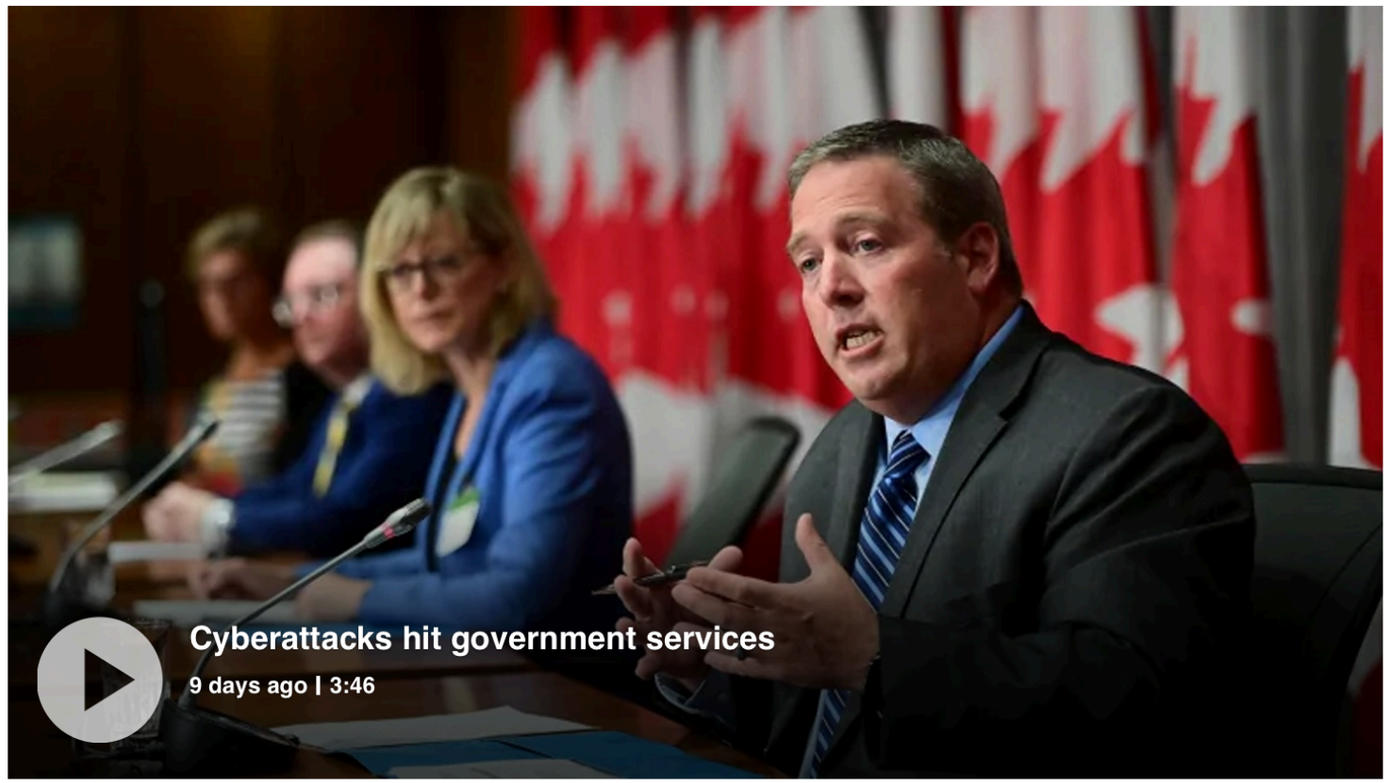
Les communautés asiatiques au Canada sont la cible d'appels automatisés.

Politics

Cyberattacks targeting CRA, Canadians' COVID-19 benefits have been brought under control: officials

Total of 11,200 Canada Revenue Agency and GCKey accounts affected by series of attacks

Ryan Patrick Jones · CBC News · Posted: Aug 17, 2020 9:29 AM ET | Last Updated: August 18



Cyberattacks that compromised the personal information of thousands of Canadians and allowed hackers to fraudulently access government services such as the Canada Revenue Agency are now under control, officials say. The type of cyberattack at issue is called credential stuffing — which involves reusing previously hacked user names and passwords. 3:46

1031 comments

Fraudsters exploited a security vulnerability in the Government of Canada website and took advantage of login credentials exposed through previous hacks to conduct a series of cyberattacks that compromised the personal information of thousands of Canadians, federal officials say.

Politics

Cyberattacks targeting CRA, Canadians' COVID-19 benefits have been brought under control: officials

Des hauts fonctionnaires du Conseil du Trésor, de l'ARC et du Centre canadien pour la cybersécurité font le point lors d'une conférence de presse à 10 h. CBC News le diffuse en direct.

Les incidents sont un type d'attaque connu sous le nom de «bourrage d'informations d'identification», où les pirates obtiennent frauduleusement des noms d'utilisateur et des mots de passe pour des comptes sur d'autres sites Web, et tirent parti du fait que de nombreuses personnes utilisent le même mot de passe pour différents comptes.

La GRC a confirmé que sa Division nationale, qui enquête sur «les cas sensibles et très médiatisés qui menacent l'intégrité politique, économique et sociale du Canada», étudie activement les attaques. Le Commissariat à la protection de la vie privée du Canada surveille également la situation.

La fermeture des services en ligne de l'ARC signifie que quiconque tente de demander des prestations d'urgence COVID-19, telles que la prestation canadienne d'intervention d'urgence, la prestation étudiante d'urgence ou la subvention salariale fédérale pour les entreprises, ne pourra pas le faire jusqu'à nouvel ordre.

1031 comments

Fraudsters exploited a security vulnerability in the Government of Canada website and took advantage of login credentials exposed through previous hacks to conduct a series of cyberattacks that compromised the personal information of thousands of Canadians, federal officials say.

Politics

Cyberattacks targeting CRA, Canadians' COVID-19 benefits have been brought under control: officials

Des hauts fonctionnaires du Conseil du Trésor, de l'ARC et du Centre canadien pour la cybersécurité font le point lors d'une conférence de presse à 10 h. CBC News le diffuse en direct.

Les incidents sont un type d'attaque connu sous le nom de «bourrage d'informations d'identification», où les pirates obtiennent frauduleusement des noms d'utilisateur et des mots de passe pour des comptes sur d'autres sites Web, et tirent parti du fait que de nombreuses personnes utilisent le même mot de passe pour différents comptes.

Leçon #1 :On ne réutilise pas ses mots de passe !

La GRC a confirmé que sa Division nationale, qui enquête sur «les cas sensibles et très médiatisés qui menacent l'intégrité politique, économique et sociale du Canada», étudie activement les attaques. Le Commissariat à la protection de la vie privée du Canada surveille également la situation.

La fermeture des services en ligne de l'ARC signifie que quiconque tente de demander des prestations d'urgence COVID-19, telles que la prestation canadienne d'intervention d'urgence, la prestation étudiante d'urgence ou la subvention salariale fédérale pour les entreprises, ne pourra pas le faire jusqu'à nouvel ordre.

1031 comments

Fraudsters exploited a security vulnerability in the Government of Canada website and took advantage of login credentials exposed through previous hacks to conduct a series of cyberattacks that compromised the personal information of thousands of Canadians, federal officials say.

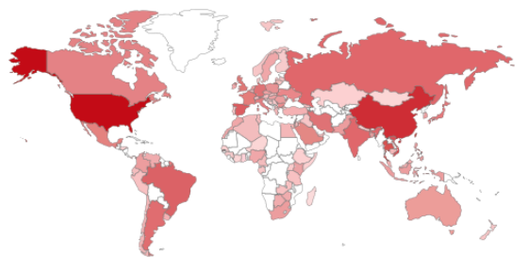
SHODAN "default password" Explore Pricing Enterprise Access

Exploits Maps Images

TOTAL RESULTS

47,223

TOP COUNTRIES



Taiwan	7,741
United States	7,353
China	4,070
Thailand	2,081
Viet Nam	1,953

TOP SERVICES

Telnet	13,184
HTTP (8080)	10,174
8081	3,665
8083	2,227
NAS Web Interfaces	1,568

TOP ORGANIZATIONS

Peicity Digital Cable Television.	6,290
Viettel Group	1,599
TOT	1,310
Mountain West Technologies Corporation	663
Natural Wireless, LLC	520

TOP OPERATING SYSTEMS

Linux 2.6.x	351
Linux 3.x	43
Windows 7 or 8	19
Linux 2.4.x	4
QTS	3

TOP PRODUCTS

Boa HTTPd	10,948
TP-LINK WR740N WAP http config	681
nginx	621
TP-LINK WR841N WAP http config	579

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

RELATED TAGS: router default password

120.89.98.235

Nepal Telecom
Added on 2020-01-09 19:34:34 GMT
Nepal

```
<html>

<head>
<script type="text/javascript">
function checkFormAndSubmit(form)
{
   if((form.elements[0].value == "") ||
         (form.elements[1].value == ""))
   {
      alert("ERROR: Either login/password field is empty");
      return false;
   }
   return true;
}
function loadFunc()
{
        li...
```

105.159.255.154

Maroc Telecom
Added on 2020-01-09 19:36:03 GMT
Morocco, Settat

```
-----------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15.
...
```

401 Unauthorized

150.117.147.14
AboveNet Communications Taiwan
Added on 2020-01-09 19:35:56 GMT
Taiwan

```
HTTP/1.0 401 Unauthorized
Date: Thu, 09 Jan 2020 19:36:05 GMT
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
Keep-Alive: timeout=10, max=1000
WWW-Authenticate: Basic realm=" Default  Name:admin  Password:1234 "
Content-Type: text/html
```

5.189.137.172

-
Contabo GmbH

COMMENT EN EST ON ARRIVÉS LÀ

Une brève histoire de la sécurité informatique

LA SÉCU N'EST PAS UN PROBLÈME RÉCENT !

- IXe siècle : analyse fréquentielle par Al-Kindi
- 1850: Cryptanalyse du code Vigenère par Babbage et Kasiski
- 1928-1945: cryptanalyse d'Enigma par une équipe Britannique dont A.Turing
- 1971: Creeper, considéré comme le premier ver
- 1976: Apogée du *phreaking* (piratage téléphonique), John Draper
- 1982: Elk Cloner, premier virus sur Apple II
- 80s : plus d'Internet, plus de problèmes (Kevin Mitnick, Poulsen, ver Morris)
- 1994 : Vladimir Levin attaque le dispositif de Citibank et vole 10.7M USD
- 2000: Premiers botnets (GTBot, Agobot, etc.)

QUI A ÉVOLUÉ RAPIDEMENT !

BREACH LEVEL INDEX

THE NUMBERS

"More and more organizations are accepting the fact that, despite their best efforts, security breaches are unavoidable."

RECORDS BREACHED IN THE FIRST HALF OF 2018

3,353,172,708

NUMBER OF BREACH INCIDENTS

944

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

20%

PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED

2.2%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

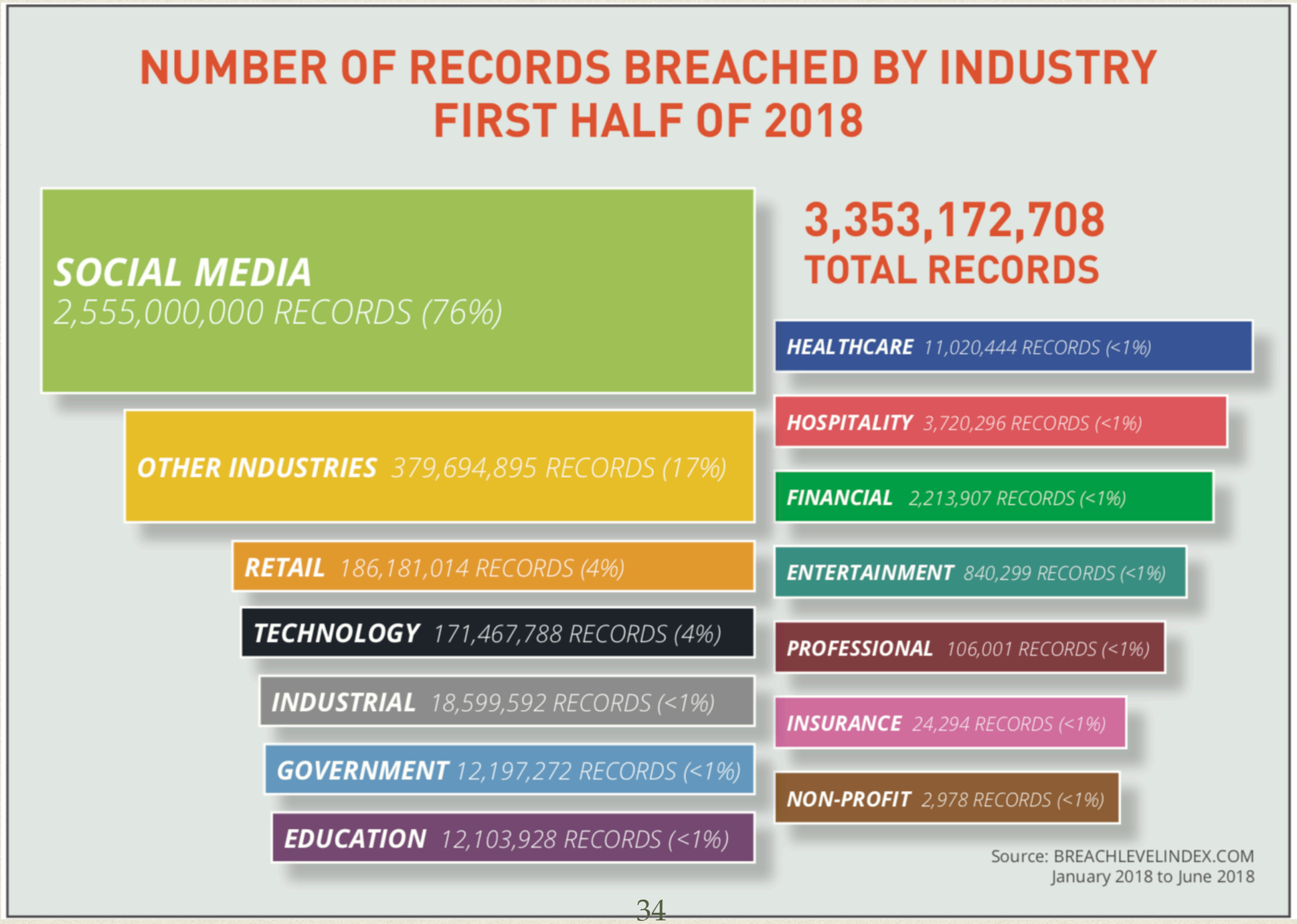
18,525,816 EVERY DAY

771,909 EVERY HOUR

12,865 EVERY MINUTE

214 EVERY SECOND

FUITES DE DONNÉES



Desjardins

ÉVOLUTION VERS LE CYBERCRIME

- C’est plus une **économie** qu’un **business** qui reprend les clés du capitalisme contemporain
  - Startups, info-nuagique, supermarchés d’outils à la Amazon
  - Des monnaies numériques
  - Des agents spécialisés: producteurs, fournisseurs, vendeurs, consommateurs
- Les biens échangés sont divers et variés
  - Numéros de carte de crédit, « likes », points de cartes de fidélité, login/passwords, recettes de soda et autres secrets d’affaire, données personnelles, outils technologiques d’état
- Des spécialisations géographiques avec des pays exportateurs des pays importateurs
- Professionnalisation grandissante : centres de formation, consultants en CV, recommandations personnelles références

CYBERCRIME

- Un « marché » de **1500 Milliards** de US$ en 2018

Crime	Annual Revenues*
Illicit, illegal online markets	$860 billion
Trade secret, IP theft	$500 billion
Data trading**	$160 billion
Crimeware, CaaS (Cybercrime-as-a-Service)	$1.6 billion
Ransomware***	$1 billion

*totals are approximate
**Revenues derived from trading in stolen data, such as: credit and debit card information banking log-in details, loyalty schemes and so on
***Revenues derived from extortions based on encrypting data and demanding payments

Table 1: Annual Cybercrime Revenue Estimates

Source: Bromium - Into the Web of Profit

LA SÉCURITÉ INFORMATIQUE C’EST QUOI ?

ON PARLE DE QUOI ?

- Sécurité informatique
- Cyber-sécurité
- Cyber
- Sécurité

L'INSÉCURITÉ INFORMATIQUE

- La sécurité informatique c'est le contraire de l'insécurité
  - Pourquoi et comment protéger ses ressources « informatiques » (données, systèmes, services)
  - On est « sécure » de ou contre quelque-chose (hackers, criminels, attaquant, etc.) (Schneier on security 2010)
- La sécurité info. (*security*) ce n'est pas la sécurité (*safety*)
  - **Sécurité-safety** = absence de conséquences catastrophiques sur les utilisateurs ou l'environnement
    - ex: 737Max (gros moteurs-avion instable-fix. logiciel-capteurs défaillants-pas de redondance-**GROS FAIL**)
  - **Sécurité-security** = confidentialité, intégrité, disponibilité (*Laprie et al. 2004*)

L'INSÉCURITÉ TOUT COURT

- **La *security* ce n'est pas le contraire de la *safety* !**

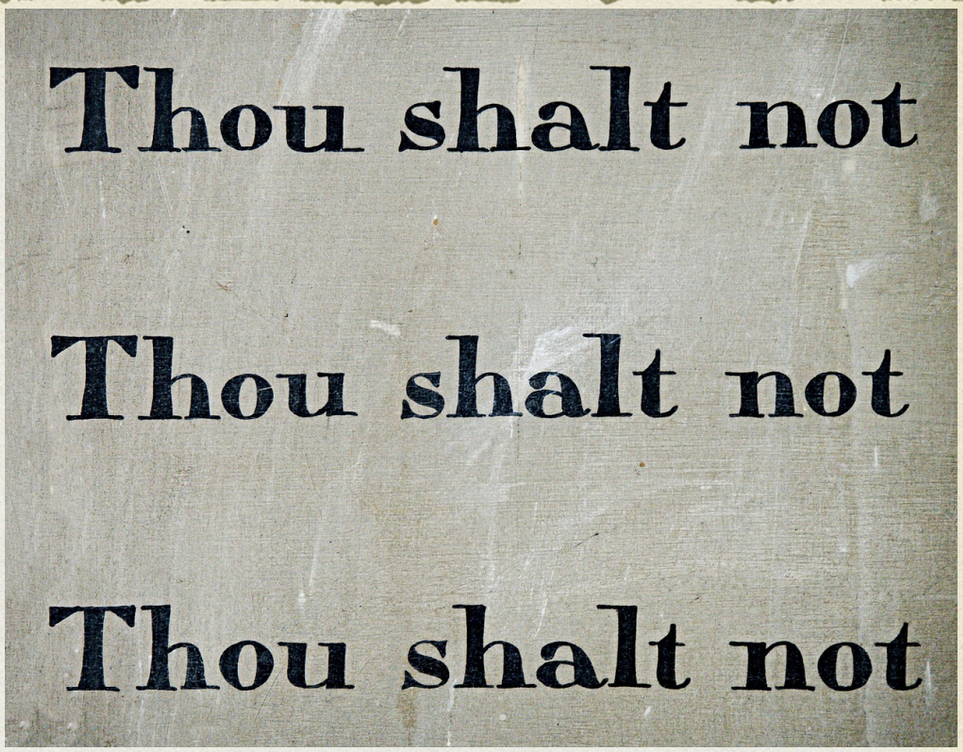
cf. page web Attaques Fantômes contre pilotage automatique

10 COMMANDEMENTS

1. De **bons** mots de passe (cf. travaux de Nicolas Cristin)
   20000 mots dans un dictionnaire ~2^{14}
   capacité de calcul d'un ordinateur ~2^{34} op/sec.
   pas de réutilisation -> gestionnaire de mdp
   ex. une Phr4s32P4ss3NOT-PossibleA2VINER et des mots de passe autogénérés
   att: les politiques qui consistent à changer régulièrement de mdp ne sont plus à la mode
   NE PAS utiliser d'outils en ligne pour tester la difficulté de ses mots de passe !

2. Système et logiciels **à jour**
   Coût d'entretien
   Migration vers de nouvelles solutions (ex. plus de support Win7 depuis le 14jan2020)

3. Sauvegarder **régulièrement** (et **diversifié**) ses données
   Principe de base rarement appliqué
   Protection contre : rançon, pannes, virus, vols, etc.

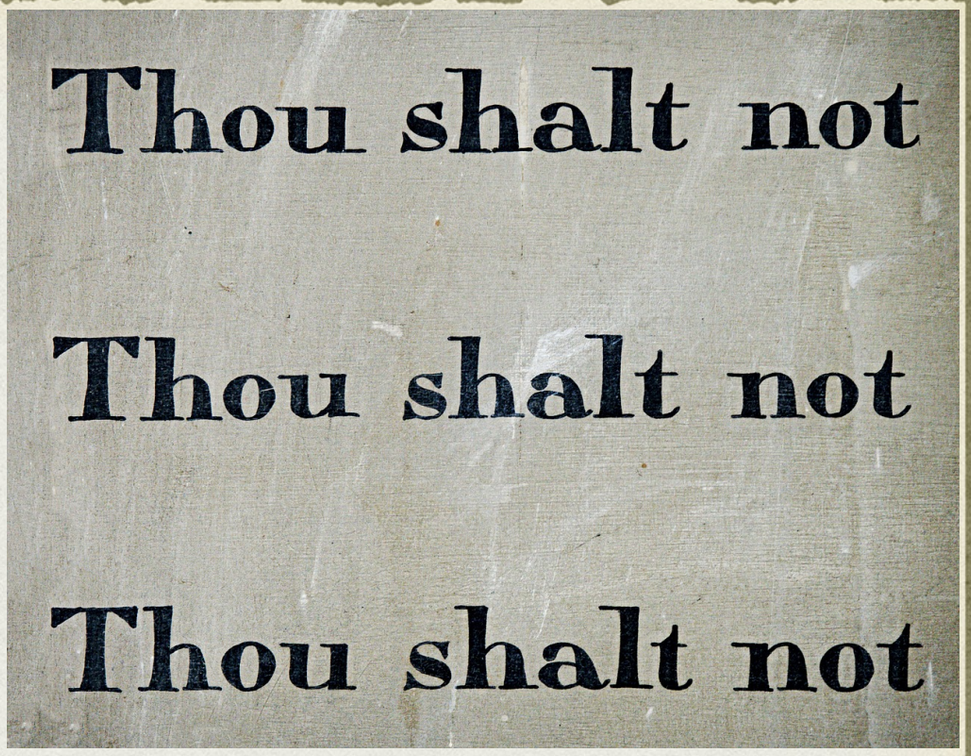


Source: ANSSI (Agence Nationale - Française- pour la Sécurité des Systèmes Informatiques)
eq. Centre de la sécurité des communications CST Canadien

10 COMMANDEMENTS (2)

4. **Désactiver ActiveX et Javascript** (et Flash!)
   Parmi les principaux vecteurs d'entrée des *logiciels malveillants*
   Difficile à désactiver ? Utiliser une machine virtuelle.

5. Ne **pas cliquer trop vite sur des liens**/fichiers attachés
   Surtout dans les courriels. Surtout sous Windows.
   Toujours vérifier le (contenu du) lien. Court, bon site, pas redirigé
   ex: www.desjardins.ça ou www.desjardin.com ou ...



6. Pas de compte admin pour naviguer sur Internet
7. Pas de photo compromettantes sur le net
8. Ne pas relayer de chaine de courriel
9. Ne pas faire confiance au nom de l'émetteur de courriel
10. Attention aux pièces jointes

Source: ANSSI (Agence Nationale - Française- pour la Sécurité des Systèmes Informatiques)

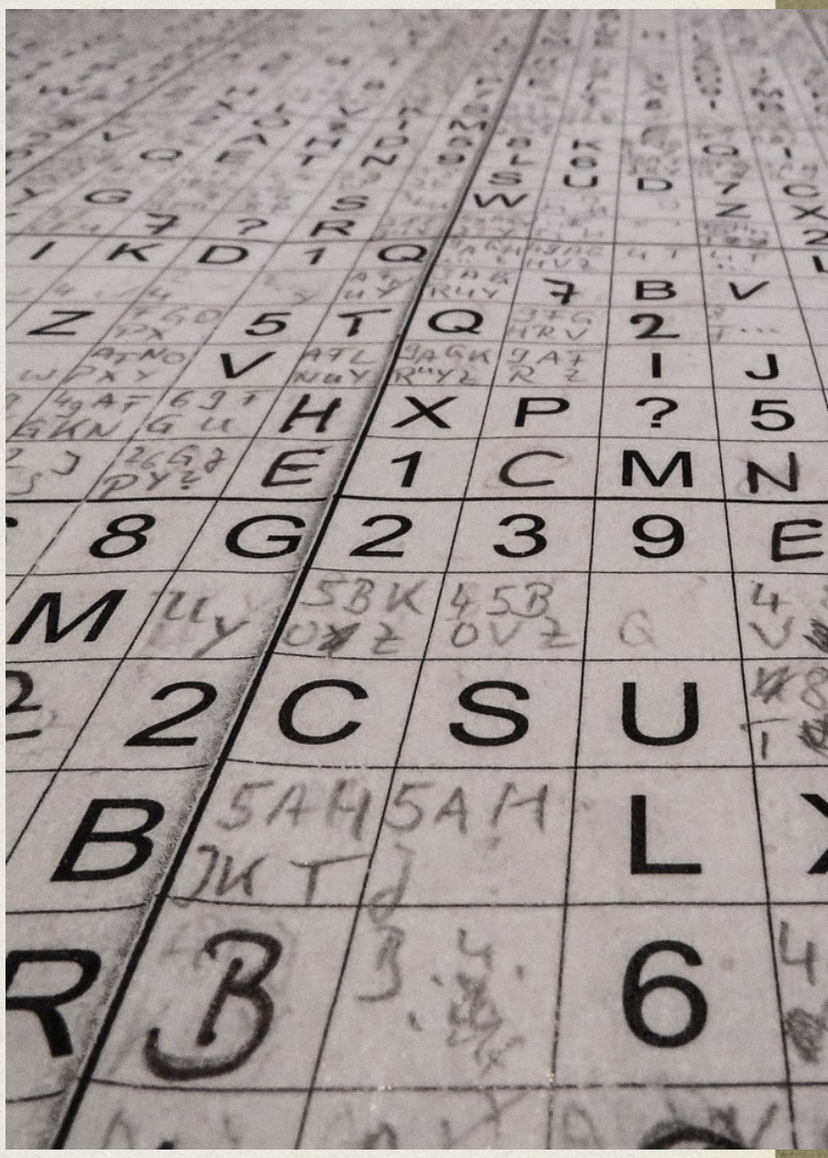
LA DIFFICULTÉ DE LA SÉCURITÉ INFORMATIQUE

- **Infaillibilité**
  pour de nombreuses attaques, l'attaquant n'a besoin que de réussir **1 seule fois**

- **Ubiquité**
  Postes: actualiser et migrer SEs et apps
  Infrastructure réseau: actualiser (matériel, firmware, SEs, configurations) et surveiller (débits, flux)
  Utilisateurs: actualiser (rôles, départs/arrivées, droits), sensibiliser, surveiller (mdp, accès)
  Logiciels métiers, logiciels de sécurité, etc.

- **Tout savoir**
  Faire de la veille sur tout ces points
  Avoir tout prévu (ou plutôt que personne ne pense à quelque-chose que l'on n'a pas prévu)

- **Energie infinie**
  Les attaquants ont une portée planétaire (pas d'horaire)
  … sont nombreux
  … n'ont rien d'autre à faire
  … sont teigneux et passionnés



SÉCURITÉ EN PROFONDEUR

- Ex. hors informatique **Accès à un site sensible**
  Un accueil avec *contrôle d'identité*
  et on doit porter un *badge* visible dans l'enceinte
  et on doit être *accompagné*
  et il faut *badger* à différents endroits
  et on doit *repasser* par le poste de contrôle en sortie

- Ex. entre deux
  On forme l'utilisateur X pour qu'il ne se fasse *pas voler* son laptop **et** il y a un *mot de passe au boot* **et** le *disque est chiffré* **et** X ne peut pas avoir de données *trop confidentielles*

- Ex. réseau
  Routeur *filtrant* **et** système de *détection d'intrusion* **et** serveurs sensibles dans un *réseau séparé* **et** système de *journalisation* et ...

- ZeroTrust : besoin de s'authentifier à tous les échelons du système

SE PRÉPARER AU PIRE

- Si **la dernière barrière tombe** ?
  - Puis-je revenir en arrière (sauvegardes) ?
  - Puis-je tout couper ?
  - Qui dois-je prévenir ?
  - Quel protocole pour revenir à une situation normale ?
- Et dans ce cas
  - Quelle est l'**étendue des dégâts** ?
  - Combien de temps avant **recouvrement** ?
  - Comment couvrir ses **pertes** ?

UN PEU DE TERMINOLOGIE -> GLOSSAIRE

- **Propriétés** de sécurité : C.+I.+A.+Traçabilité
- **Participants** : entités légitimes qui sont impliquées dans l'exécution d'un protocole (A-lice et B-ob)
- **Adversaire** : entité malveillante (pas malicieuse) qui essaye de porter atteinte à une des propriétés (E-ve)
- **Algorithme** : procédure effectuée localement par un participant
- **Protocole** : procédure effectuée conjointement par les participants, dont les rôles respectifs sont clairement identifiés

TYPOLOGIE DES ATTAQUES

- **Espionnage** : capture d'infos
- **Modification** : altération d'information
- **Rejeu** d'un message capturé
- **Réflection** : rejeu d'un défi qui nous était destiné
- **Déni de service** : empêcher les participants de compléter le protocole
- **Typage** : remplacer un champs par une autre valeur
- **Cryptanalyse** : profiter d'une faiblesse cryptographique pour déchiffrer (sans clé)
- **Manipulation de certificat** : choix ou altération d'un certificat dédié à l'authentification
- **Interactions de protocole** : exploitation d'une même clé utilisée dans différents protocoles

VULNÉRABILITÉ, MENACE, ATTAQUE

- **Menace** : n'importe quel évènement négatif (d'origine malveillante ou non) qui *peut* arriver à un actif ; violation d'une ou plusieurs propriétés de sécurité

- **Vulnérabilité** : une faiblesse, ou une faille, qui rend une menace possible si elle est *exploitée*

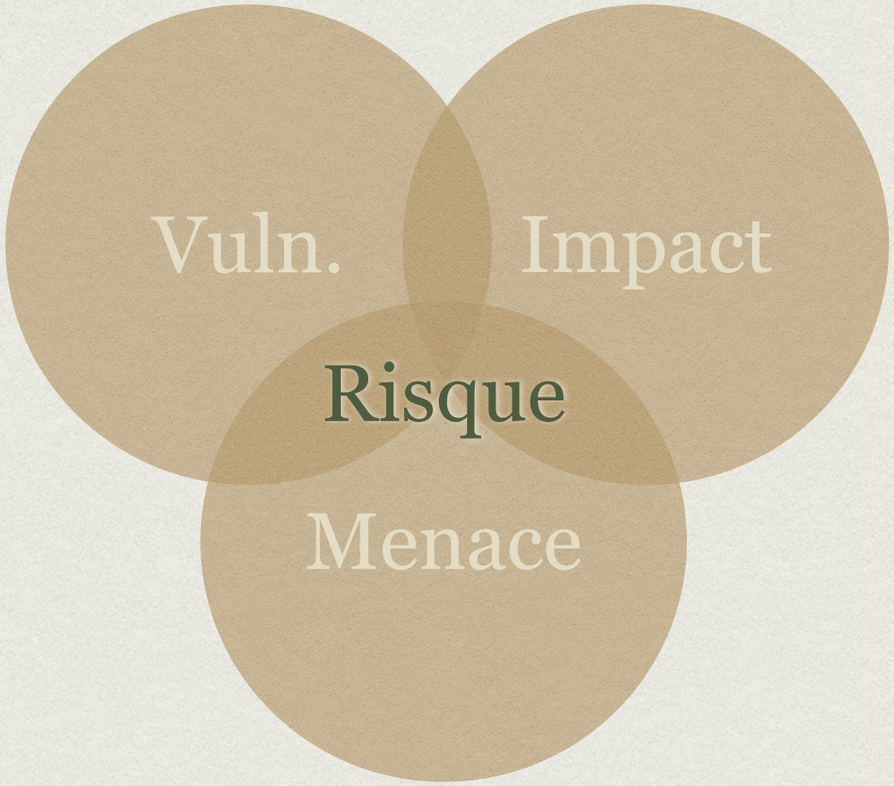
- **Attaque** : action *intentionnelle* qui exploite une *vulnérabilité* ou met en oeuvre une *menace*

- **Intrusion** : violation effective de la politique de sécurité, fait suite à une ou plusieurs *attaques* réussies

GOUVERNANCE

- **Gestion du risque**
  Identifier les biens
  Identifier les sources de menaces
  Evaluer la vulnérabilité face aux menaces
  Evaluer le risque (valeur/dangerosité)
  Identifier des solutions et les prioritiser
  Auditer et recommencer

- **Identifier des solutions ?**
  Politiques de sécurité
  Organisation (responsables, protocoles, etc.)
  Plans de recouvrement
  Gestion des incidents
  Aspects humains (formation)

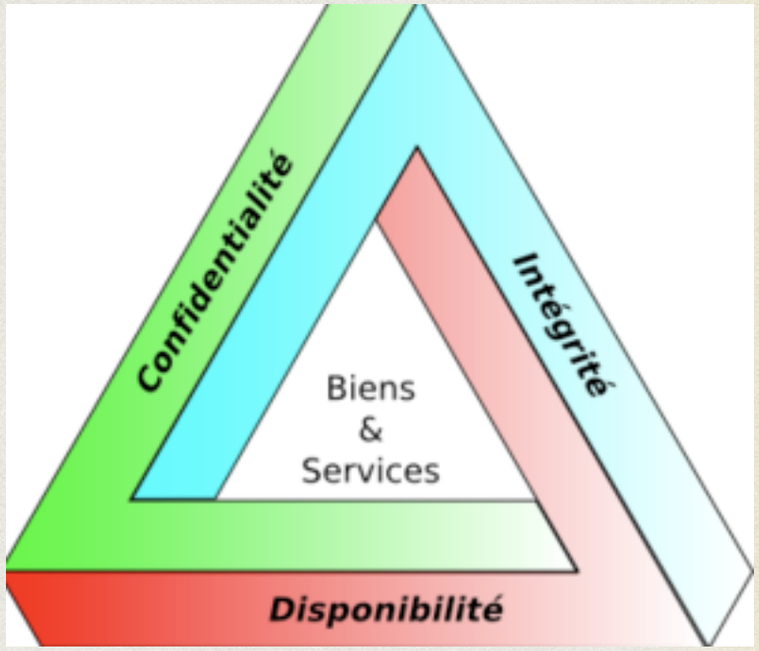


POUR ALLER PLUS LOIN

- La sécurité pour les ~~nuls~~ dirigeants d'entreprise
  - livre blanc OSSIR/CLUSIF
  - une idée sur tous les sujets en qqs pages : email, cloud, espionnage, etc.
- Les associations d'utilisateurs (de SSI, d'entreprises)
  - Clusif: panorama des menaces, RGPD, etc.
- Les agences gouvernementales
  - Centre Canadien pour la Cybersécurité : guide entreprises, etc.
  - ANSSI - guides, pratiques, formations, labels, logiciels et OS « blindés »

PROPRIÉTÉS DE SÉCURITÉ

- **Confidentialité**: ne pas être accessible aux personnes non-autorisées
- **Intégrité**: ne pas être modifiable par des personnes non-autorisées
- **Disponibilité**: être accessible aux personnes autorisées
- C.I.A. (Dispo=Availability)



PROPRIÉTÉS DE SÉCURITÉ

- **Confiden**[illegible] ccessible aux personne[illegible]s

  Craquer un mot de passe

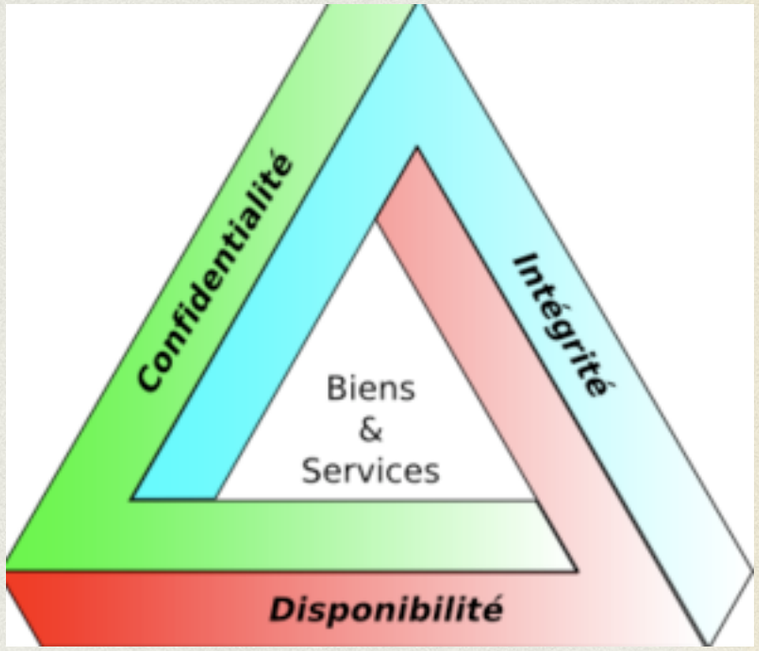
- **Intégrité**: n[illegible]fiable par des person[illegible]

  « Défacer » un site web

- **Disponibil**[illegible]le aux personnes [illegible]

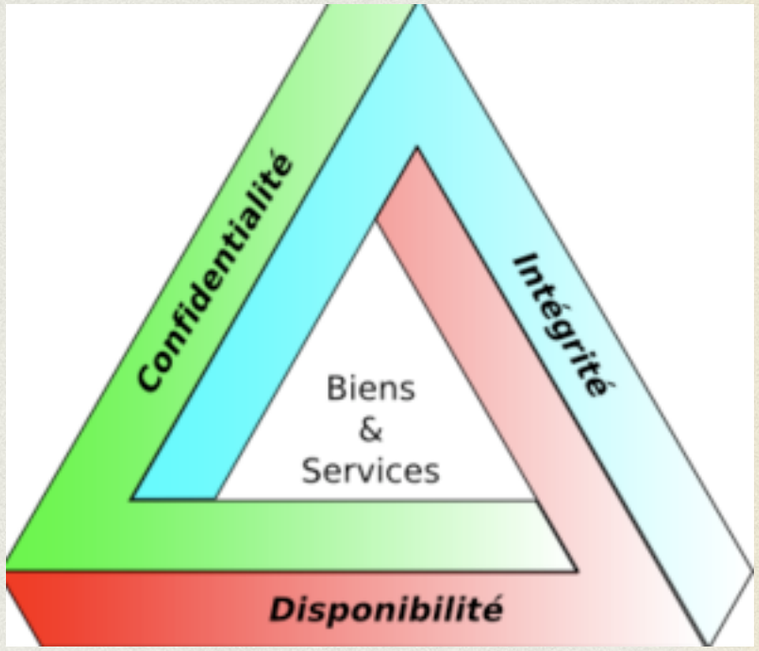
  Déni de service

- C.I.A. (Dispo=Availability)



MÉCANISMES DE SÉCURITÉ

- **Authentification**: vérifier une identité
- **Autorisation**: appliquer une politique d'accès à des ressources
- **Traçabilité**: mise en place de logs permettant de savoir ce qui a été consommé ou fait
- **Auditabilité**: généralement post-mortem (analyse forensique), bénéficie grandement de la traçabilité
- A.A.A.(A) : Authentication, Autorisation, Accounting (and Auditing)



MENACES

- **Objectifs classiques**
  - Ecoute (simple ou élaborée)
  - Contournement de moyens d'authentification/ autorisation
  - Déni de service (attaque physique, réseau, vers)
- **Types d'attaquants**
  - **Internes** (un ou plusieurs utilisateurs) ou **externes**
  - *Principalement* ***internes*** **: 80%** d'après Jim Carr « Thwarting Insider Attacks »
  - «

POURQUOI EST-IL IMPORTANT DE MODÉLISER L'ADVERSAIRE

- **Rappel**: *On est « sécure » de ou contre quelque-chose (hackers, criminels, attaquant, etc.)*
  (Schneier on security 2010)

- Savoir **contre qui**/quoi on veut se protéger

  - Mécanismes mis en place pour **protéger une propriété contre un type d'attaque**

  - La sécurité absolue est utopique ou « **le risque 0 n'existe pas** »

  - en fonction des couts/bénéfices on se **protège contre certains attaquants**

- Mais attention, un adversaire plus puissant, des hypothèses mal calibrées et la **sécurité mise en place ne tiendra plus**

- **La sécurité inviolable n'existe pas, on cherche a rendre la vie difficile à l'adversaire**

ACTIVITÉS OPTIONNELLES DE LA SEMAINE

- Ballado NoLimitSecu sur la formation en cyber-sécurité
- Série documentaire (en langue anglaise) sur la surveillance généralisée : https://uqam.kanopy.com/video/surveillance-state
  - 24 épisodes de 30 min. la plupart des épisodes en lien (vulgarisé) avec certaines séances du cours
- (ENG) Plus sur les vulnérabilités, menaces, attaques
- livre blanc OSSIR/CLUSIF

MERCI

- **Questions ?**
  - **Maintenant** et chaque mardi
  - **Mattermost**
  - **Courriel**