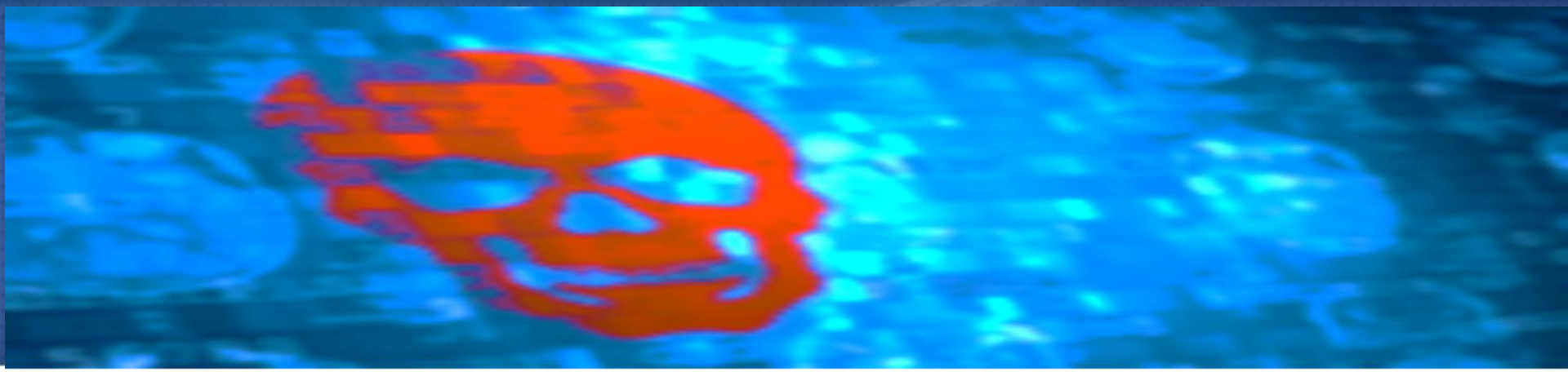
Mois de la sensibilisation en cybersécurité

Webinaire 1 – Le 2 octobre 2020

Risques et menaces émergents de 2020



Nadia Vigneault

CEH / CHFI

ISACA®
Section de Québec

Risques et menaces émergents de 2020

ISACA
Section de Québec

Qui suis-je ??

2019… Analyste en sécurité opérationnelle (compagnie secteur assurances et services financiers)

2016… Chargée de cours au Cegep Garneau au Programme AEC en Cyberenquête

2015 à 2019 Conseillère en sécurité de l'information à l'Université Laval

2010 à 2014 Analyste en sécurité chez LGS inc.

Diplômes :

- Science (BACC par cumule : certificat en informatique appliquée (UQAC), certificat en cyberenquête & certificat en cybersécurité des réseaux informatiques (Polytechnique)
- Science politique (BACC) de l'UQAC

Formations :

- Linux, OSINT, Investigation (forensics), etc.

Certifications :

- EC-Council (CEH, CHFI)

Conférencière :

- Enquêtes informatiques :
  - HackerSpace (2015 maintenant QuebecSec)
  - Hackfest (conférences 2015-2016 et journée de formation 2017)
- Cyber-attaques :
  - ISACA (2018), SeqCure (2019)

ISACA Section de Québec

Plan du webinaire

1. Préambule

2. Menaces 2020

3. Tendances 2021

ISACA
Section de Québec

Préambule

L'année 2020 n'aura pas été comme les autres...on va s'en souvenir longtemps! Pas parce qu'il y eu des tonnes de virus... mais à cause d'un virus humain dévastateur. Mais celui-ci n'a pas, par contre, infecté nos postes/serveurs informatiques comme l'ont fait encore cette année les rançongiciels! Ces menaces perpétuelles, ainsi que la compromission d'identifiants, la menace interne et la toute nouvelle donne cette année, le télétravail, ont été les menaces de 2020.

Que nous réserve 2021?

Des virus? Humains ou informatiques?

ISACA Section de Québec

Menaces 2020

Les pronostiques du début 2020 étaient quoi ?

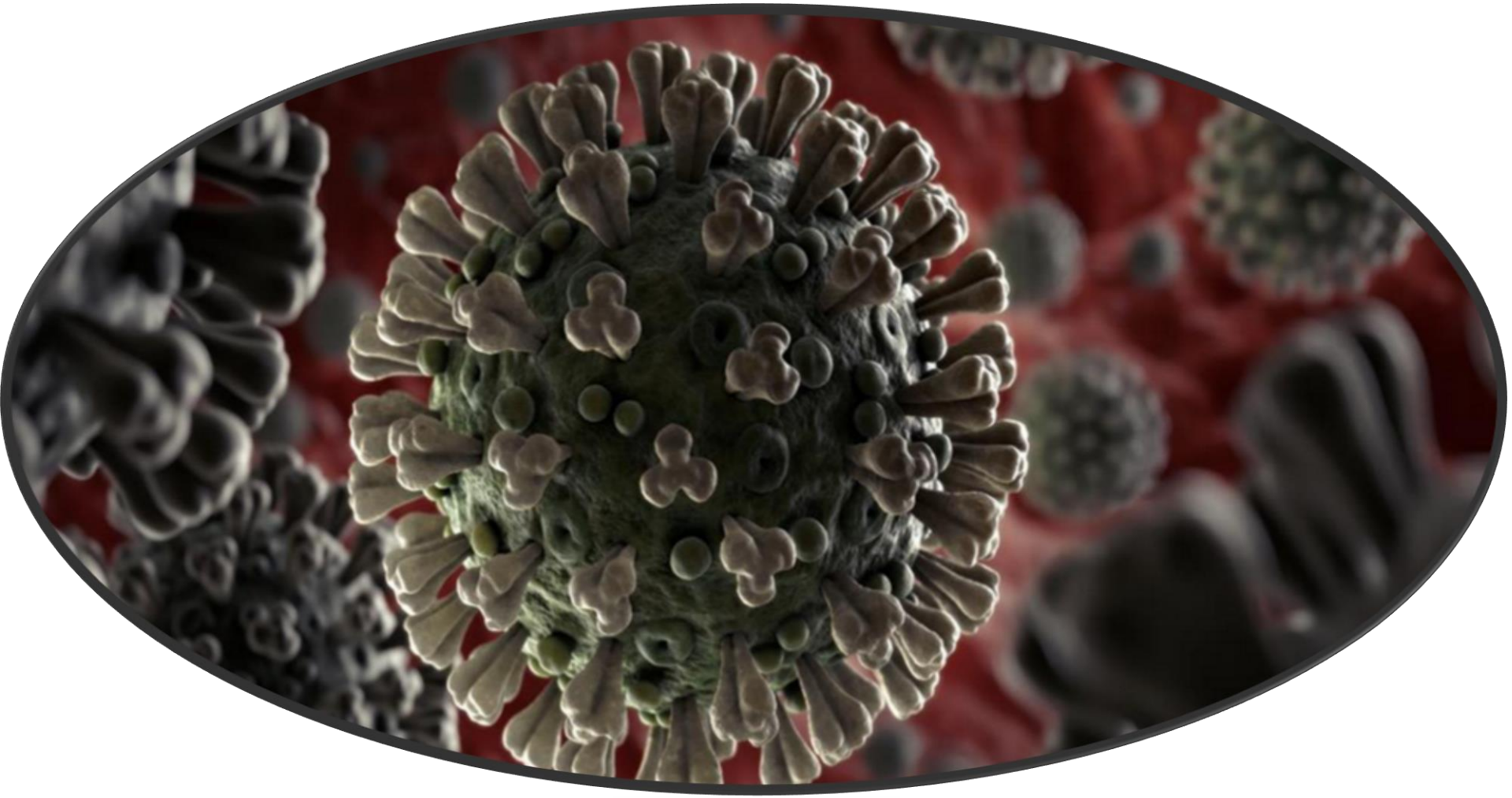
- Les outils de piratage de type “Intelligence Artificielle”;
- Une crise dans les “cyber talents” (manque de formation);
- La fraude, l’hameçonnage, les maliciels, les DoS, les mauvaises configurations dans le Cloud, les vulnérabilités dans les images Dockers;
- Les “Shadow IT”;
- Les attaques sur les plate-formes infonuagiques;
- Les rançongiciels;
- Etc…

https://builtin.com/cybersecurity/cybersecurity-trends

Webcast : 2020 Cyberthreats Landscape Proofpoint 28 janvier 2020

ISACA Section de Québec

Notre #1!



https://www.who.int/news-room/detail/06-02-2020-who-to-accelerate-research-and-innovation-for-new-coronavirus

ISACA Section de Québec

Menaces 2020

Au ¾ de 2020, les menaces auront été celles-ci :

1.1- Prolifération des attaques avec la thématique de la pandémie, du virus covid-19…

Webcast de Tenable le 27 mars 2020:
40% d'augmentation des cyber-attaques (hameçonnage…)

https://us-cert.cisa.gov/ncas/alerts/aa20-099a

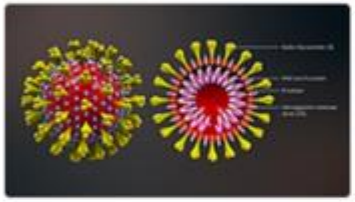
https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

Webcast : Understanding and address the cybersecurity impacts of COVID-19 Tenable 27 mars 2020

ISACA Section de Québec

https://www.darkowl.com/blog-content/coronavirus-on-the-darknet

Home Poisons -Viruses Coronavirus – COVID-19



Coronavirus – COVID-19

$1,000.00

I was infected with Coronavirus – COVID-19!!!

I sell my infected blood and saliva.

I do this to provide for my family

Product categories

Advertising

COVID-19 Everything you need to know

JD • John DeFranco <[redacted]>

To: • [redacted]

How to Protect your friends from nCov 2019 FAQ

There are more than 75,000 infected COVID-19 cases all around the world!

COVID-19-FAQ - uploaded with iCloud Drive.

Regards,
John DeFranco

https://www.forbes.com/sites/thomasbrewster/2020/03/12/coronavirus-scam-alert-watch-out-for-these-risky-covid-19-websites-and-emails/#

Ответить Ответить всем Переслать Больше

От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

https://insideepic.com/posts/company-news/be-careful-of-covid-19-phishing-emails/

Menaces 2020

Fake Online Coronavirus Map Delivers Well-known Malware
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV
Date: March 10, 2020

https://it.brown.edu/alerts/read/malicious-website-disquised-covid-19-live-map

ISACA Section de Québec

Menaces 2020

Impacts ?

Hameçonnage (courriel avec fichier infecté et/ou lien vers un site web infecté)

Risques ?

- $$ chiffrement de données
- vol d’informations sensibles
- etc.

ISACA Section de Québec

Menaces 2020

1.2- Un nombre élevé de noms de domaine ont été acheté par les fraudeurs pour perpétrer ces attaques.

by **Jonathan Greig** in **Security**
on May 4, 2020, 12:00 PM PST

More than 86,600 new domains related to the pandemic are considered "risky" or "malicious," according to a new report.

https://www.techrepublic.com/article/nearly-2000-malicious-covid-19-themed-domains-created-every-day/

Menaces 2020

```
Date, Query, Match
2020-03-09, covid, *.cdccovid19.com
2020-03-09, covid, *.cookingincovidtimes.com
2020-03-09, covid, *.corona-covid19.de
2020-03-09, covid, *.coronavirus-covid-19-dashboard.online
2020-03-09, covid, *.coronaviruscovid19preparedness.com
2020-03-09, covid, *.covid-19-wuhan.com
2020-03-09, covid, *.covid-19clinics.com
2020-03-09, covid, *.covid-19diagnostics.com
2020-03-09, covid, *.covid-19help.info
2020-03-09, covid, *.covid-19labs.com
2020-03-09, covid, *.covid-19labtest.co.uk
2020-03-09, covid, *.covid-19selftestkit.com
2020-03-09, covid, *.covid-19uk.com
2020-03-09, covid, *.covid-2019.de
2020-03-09, covid, *.covid-cov-19.com
2020-03-09, covid, *.covid-cov-19.net
2020-03-09, covid, *.covid-cov-19.us
2020-03-09, covid, *.covid-impfschutz.de
2020-03-09, covid, *.covid-lawyer.com
2020-03-09, covid, *.covid-lawyers.com
2020-03-09, covid, *.covid-legal.com
2020-03-09, covid, *.covid-x.de
2020-03-09, covid, *.covid.chat
2020-03-09, covid, *.covid.com.pl
2020-03-09, covid, *.covid.org.uk
2020-03-09, covid, *.covid.sk
2020-03-09, covid, *.covid19-hack.tech
2020-03-09, covid, *.covid19-safety.com
2020-03-09, covid, *.covid19.nl
2020-03-09, covid, *.covid19africa.com
2020-03-09, covid, *.covid19alerts.org
2020-03-09, covid, *.covid19antiviral.com
2020-03-09, covid, *.covid19application.com
2020-03-09, covid, *.covid19cr.com
2020-03-09, covid, *.covid19crowd.com
2020-03-09, covid, *.covid19delivery.com
2020-03-09, covid, *.covid19diagnostics.com
2020-03-09, covid, *.covid19drone.com
2020-03-09, covid, *.covid19dronedelivery.com
2020-03-09, covid, *.covid19economics.com
2020-03-09, covid, *.covid19finance.com
```

“RiskIQ is making matches against 'covid', 'coronav', 'vaccine', 'pandemic', and 'virus' from its Newly Observed Host (NOH) feed available to the public. No reputation filters or enrichment have been done on the results. This data is delivered "AS-IS".**”**

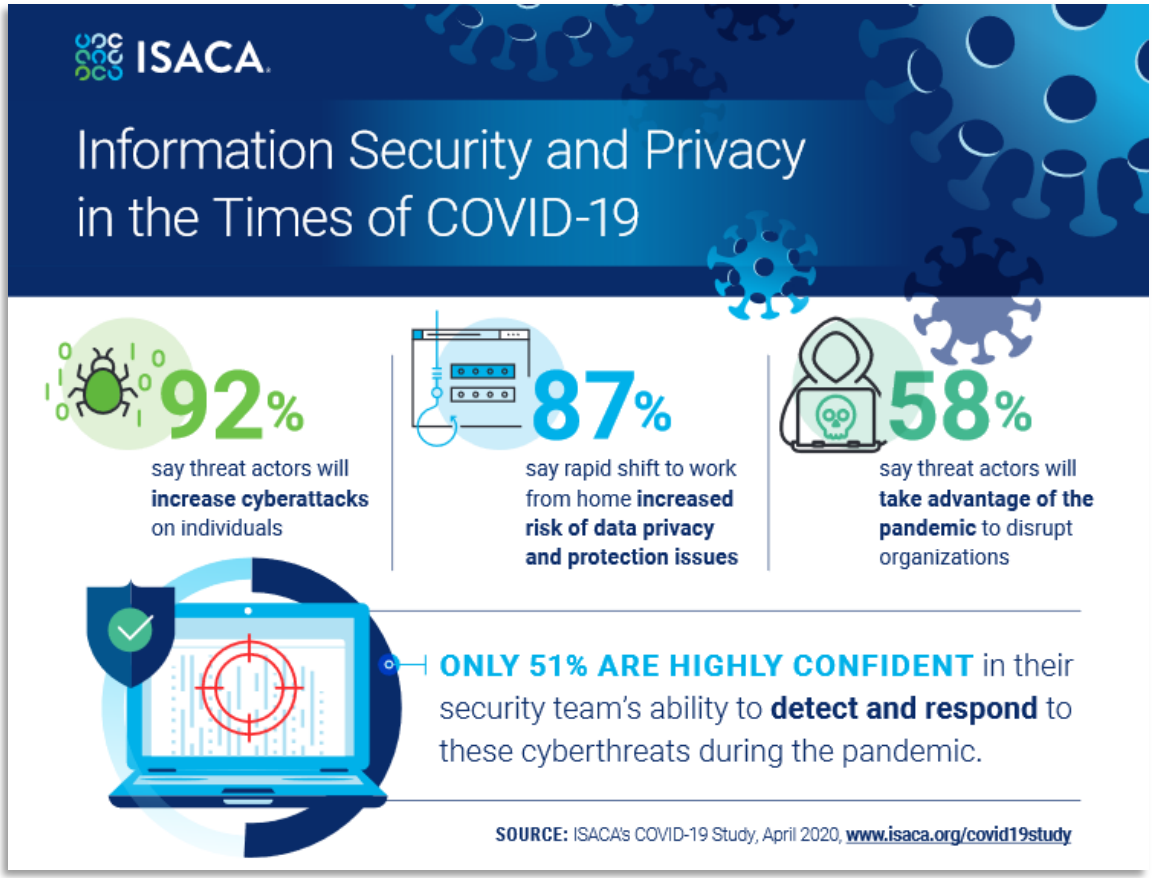
80% hébergés chez Amazon (AWS)
15% hébergés chez Google cloud
5% hébergés sur Azure

https://covid-public-domains.s3-us-west-1.amazonaws.com/list.txt

ISACA Section de Québec

Interlude : ISACA ☺

Sondage au sujet de la covid-19 par ISACA



https://www.isaca.org/go/covid19-study

ISACA Section de Québec

Menaces 2020

2- Un nombre élevé d'exploitation de vulnérabilités des applications de vidéo-conférence (Zoom, MS Teams, etc.).

Pourquoi ????

Nous sommes des millions à travailler de chez-soi en télétravail!

"It's important to appear professional, even when working fom home."

https://www.cartoonstock.com/directory/t/teleworking.asp

Menaces 2020

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

NVD
Go to for:
CVSS Scores
CPE Info

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 142417

HOME > CVE > SEARCH RESULTS

Search Results

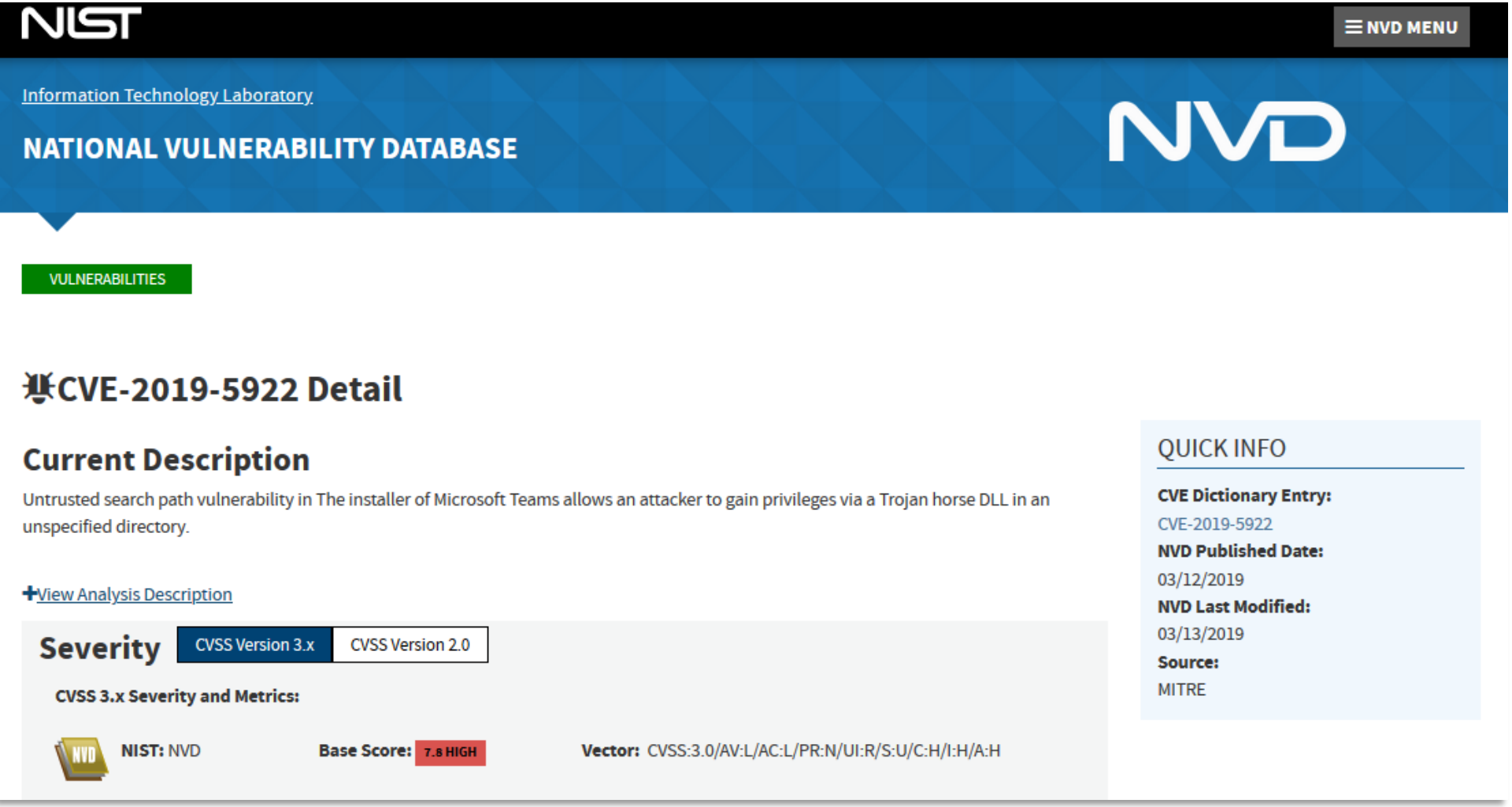
There are **60** CVE entries that match your search.

Name	Description
CVE-2020-9767	A vulnerability related to Dynamic-link Library (“DLL”) loading in the Zoom Sharing Service would allow an attacker who had local access to a machine on which the service was running with elevated privileges to elevate their system privileges as well through use of a malicious DLL. Zoom addressed this issue, which only applies to Windows users, in the 5.0.4 client release.
CVE-2020-6110	An exploitable partial path traversal vulnerability exists in the way Zoom Client version 4.6.10 processes messages including shared code snippets. A specially crafted chat message can cause an arbitrary binary planting which could be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to trigger this vulnerability. For the most severe effect, target user interaction is required.
CVE-2020-6109	An exploitable path traversal vulnerability exists in the Zoom client, version 4.6.10 processes messages including animated GIFs. A specially crafted chat message can cause an arbitrary file write, which could potentially be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to exploit this vulnerability.
CVE-2020-11877	** DISPUTED ** airhost.exe in Zoom Client for Meetings 4.6.11 uses 3423423432325249 as the Initialization Vector (IV) for AES-256 CBC encryption. NOTE: the vendor states that this IV is used only within unreachable code.
CVE-2020-11876	** DISPUTED ** airhost.exe in Zoom Client for Meetings 4.6.11 uses the SHA-256 hash of 0123425234234fsdfsdr3242 for initialization of an OpenSSL EVP AES-256 CBC context. NOTE: the vendor states that this initialization only occurs within unreachable code.
CVE-2020-11500	Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key.
CVE-2020-11470	Zoom Client for Meetings through 4.6.8 on macOS has the disable-library-validation entitlement, which allows a local process (with the user's privileges) to obtain unprompted microphone and camera access by loading a crafted library and thereby inheriting Zoom Client's microphone and camera access.
CVE-2020-11469	Zoom Client for Meetings through 4.6.8 on macOS copies runwithroot to a user-writable temporary directory during installation, which allows a local process (with the user's privileges) to obtain root access by replacing runwithroot.
CVE-2020-11443	The Zoom IT installer for Windows (ZoomInstallerFull.msi) prior to version 4.6.10 deletes files located in %APPDATA%\Zoom before installing an updated version of the client. Standard users are able to write to this directory, and can write links to other directories on the machine. As the installer runs with SYSTEM privileges and follows these links, a user can cause the installer to delete files that otherwise cannot be deleted by the user.
CVE-2019-18822	A privilege escalation vulnerability in ZOOM Call Recording 6.3.1 allows its user account (i.e., the account under which the program runs - by default, the callrec account) to elevate privileges to root by abusing the callrec-rs@.service. The callrec-rs@.service starts the /opt/callrec/bin/rs binary with root privileges, and this binary is owned by callrec. It can be replaced by a Trojan horse.
CVE-2019-18223	ZOOM International Call Recording 6.3.1 suffers from multiple authenticated stored XSS vulnerabilities via the phoneNumber field in the (1) User Edit or (2) User Add form, (3) name field in the Role Add form, (4) name or number field in the Edit Group form, (5) tagKey or tagValue field in the Recording Rules Configuration, or (6) txt_69735:/VemailAddress/value or txt_75767:/VemailFrom/value field in callrec/config.
CVE-2019-16273	DTEN D5 and D7 before 1.3.4 devices allow unauthenticated root shell access through Android Debug Bridge (adb), leading to arbitrary code execution and system administration. Also, this provides a covert ability to capture screen data from the Zoom Client on Windows by executing commands on the Android OS.
CVE-2019-13567	The Zoom Client before 4.4.53932.0709 on macOS allows remote code execution, a different vulnerability than CVE-2019-13450. If the ZoomOpener daemon (aka the hidden web server) is running, but the Zoom Client is not installed or can't be opened, an attacker can remotely execute code with a maliciously crafted launch URL. NOTE: ZoomOpener is removed by the Apple Malware Removal Tool (MRT) if this tool is enabled and has the 2019-07-10 MRTConfigData.
CVE-2019-13450	In the Zoom Client through 4.4.4 and RingCentral 7.0.136380.0312 on macOS, remote attackers can force a user to join a video call with the video camera active. This occurs because any web site can interact

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=zoom
Démo : https://www.youtube.com/watch?v=sEatCUbL_U4

ISACA Section de Québec

Menaces 2020



https://nvd.nist.gov/vuln/detail/CVE-2019-5922
Démo : https://www.cbronline.com/news/microsoft-teams-vulnerability

ISACA Section de Québec

Menaces 2020

3- Un grand nombre des vulnérabilités exploitées en 2020 datent de plusieurs années! Les quatre plus exploitées sont :

- **CVE-2019-19781**
- **CVE-2019-11510**
- **CVE-2012-0158**
- **CVE-2018-8453**

https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

Menaces 2020

CVE-2019-19781

CVSS : **9.8 CVSS – Critique**

Produits : Citrix App Delivery Controller, Citrix Gateway, Citrix SD-WAN WANOP

Acteurs : États commanditaires / groupes cybercriminels

Détection de rançongiciels : **Sodinokibi/Revil**, Ragnarok, DopplePaymer, Maze, CLOP, Nephilim…

https://www.secureworks.com/research/revil-sodinokibi-ransomware

Menaces 2020

CVE-2019-11510

CVSS : **10 CVSS – Critique**

Produits : Pulse Connect Secure

Acteurs : États commanditaires / groupes cybercriminels

Détection de rançongiciels : Sodinokibi/Revil, **Black Kingdom**…

https://www.bleepingcomputer.com/news/security/black-kingdom-ransomware-hacks-networks-with-pulse-vpn-flaws/

Menaces 2020

CVE-2012-0158

CVSS : **9.3 – Haute**

Produits : Microsoft Office, SQL Server, BizTalk…

Acteurs : États commanditaires / groupes cybercriminels

Détection de rançongiciels : **EDA2**, Rasom…

https://www.2-spyware.com/remove-eda2-ransomware-virus.html

Menaces 2020

CVE-2018-8453

CVSS : **7.8 – Haute**

Produits : Microsoft Windows Win32k

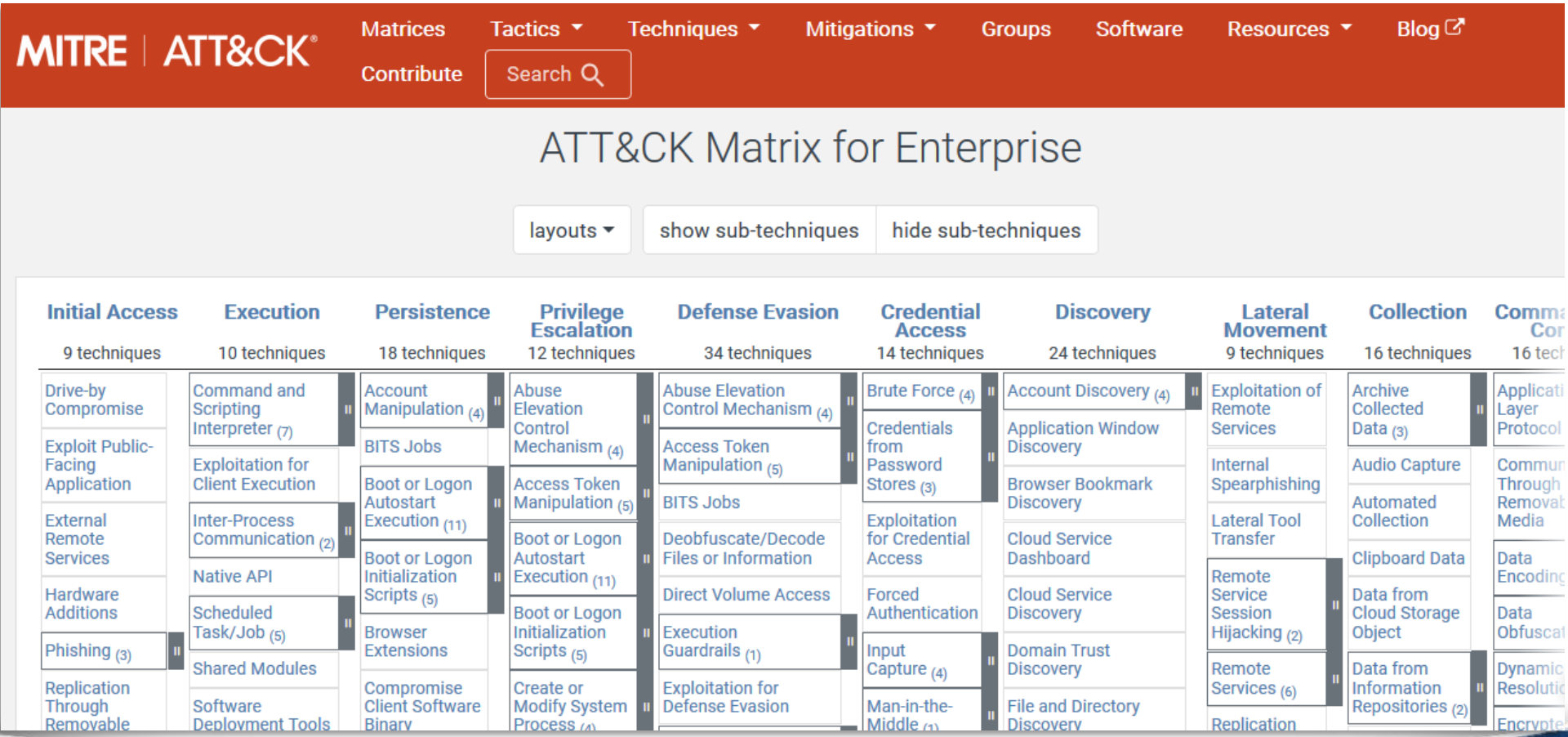
Acteurs : États commanditaires / groupes cybercriminels

Détection de rançongiciels : **Sodinokibi/Revil**…

ISACA Section de Québec

Menaces 2020

Pour en savoir plus sur les TTP (Tactiques, Techniques, Procédures) des groupes de cybercriminels :

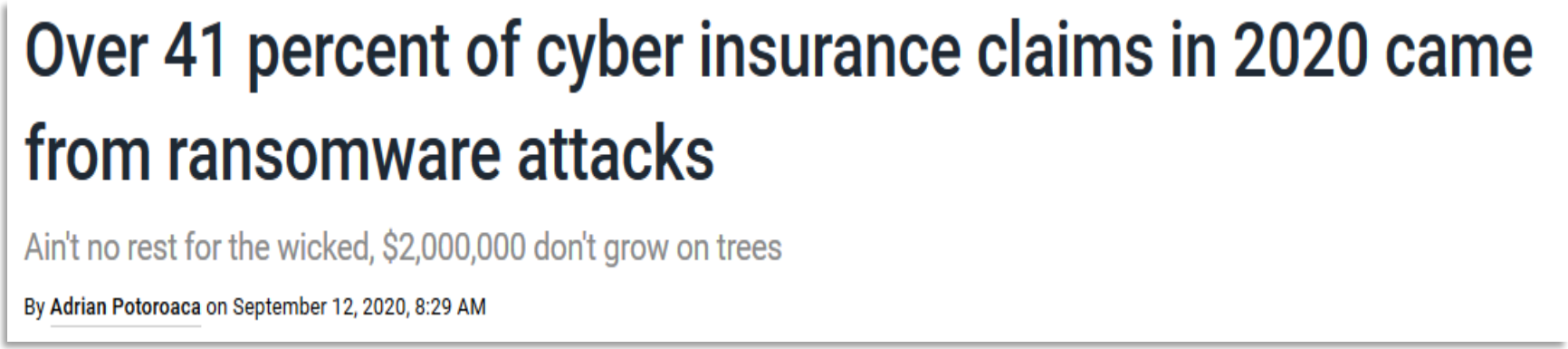


https://attack.mitre.org/

Menace 2020 mais aussi une Récurrence 2020

4- Rançongiciels :

Est-ce populaire encore ???



Over 41 percent of cyber insurance claims in 2020 came from ransomware attacks

Ain't no rest for the wicked, $2,000,000 don't grow on trees

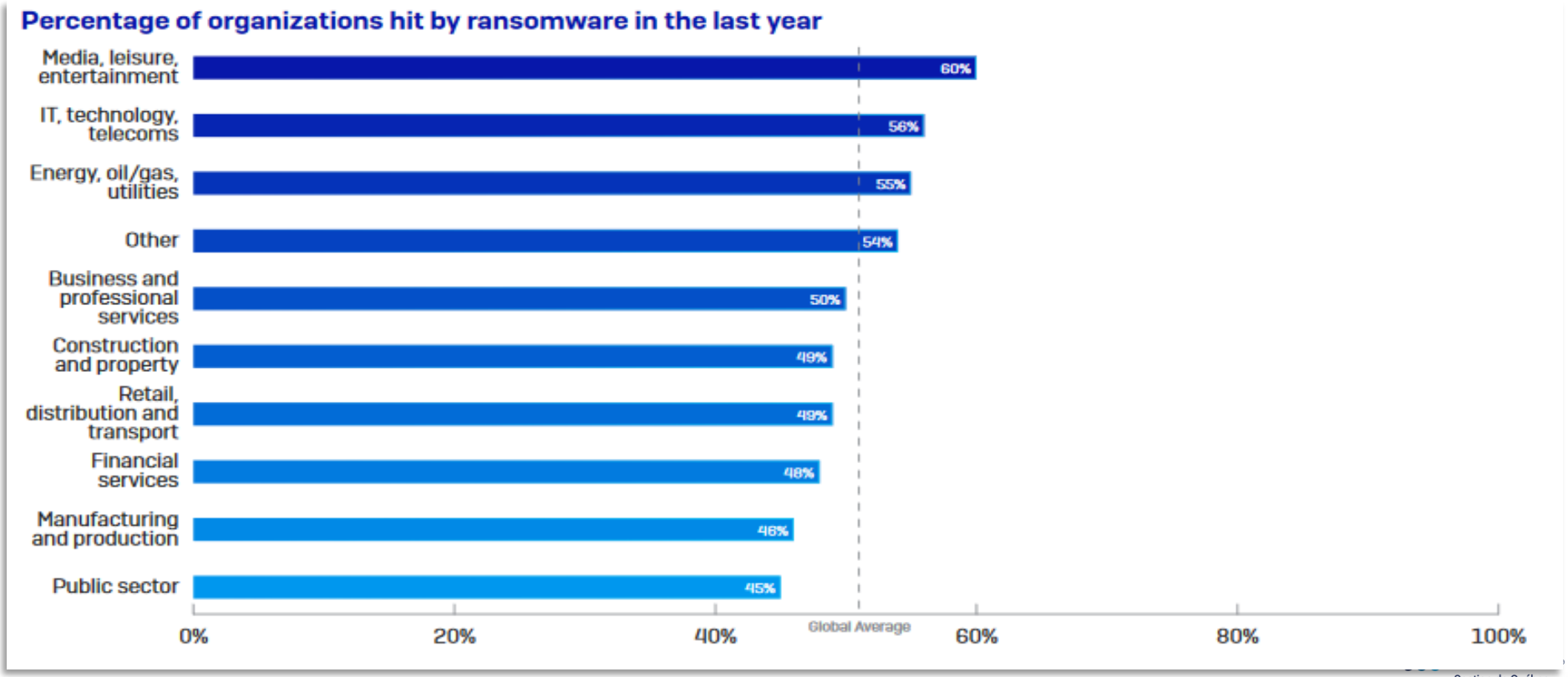
By **Adrian Potoroaca** on September 12, 2020, 8:29 AM

https://www.techspot.com/news/86714-over-41-percent-cyber-insurance-claims-2020-came.html

ISACA Section de Québec

Menace 2020 mais aussi une Récurrence 2020

Peu importe la cible…tous sont frappés par les rançongiciels :

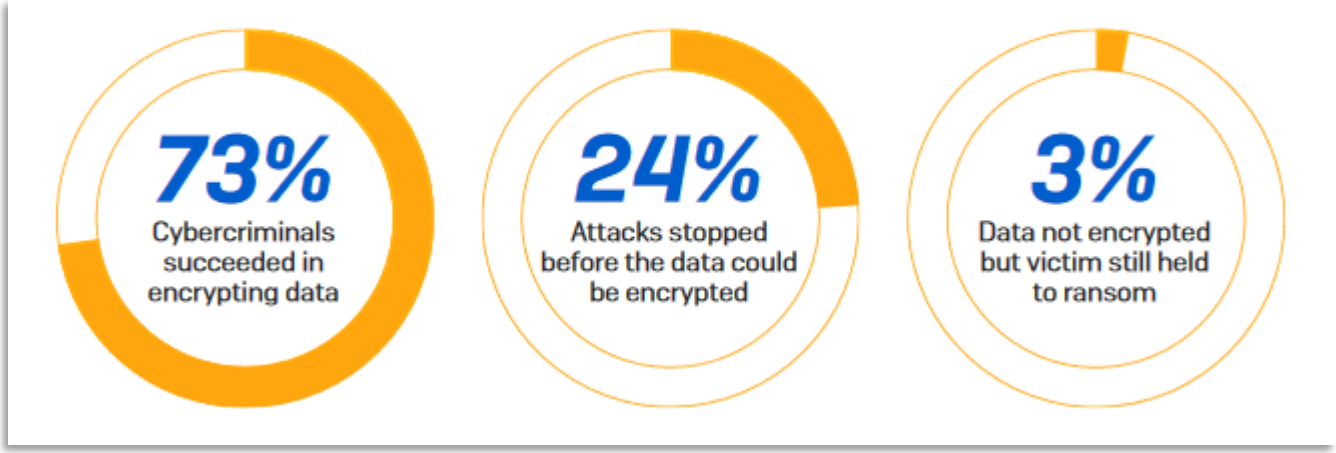


https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Menace 2020 mais aussi une Récurrence 2020

Impacts ?

¾ du temps les données sont chiffrées!

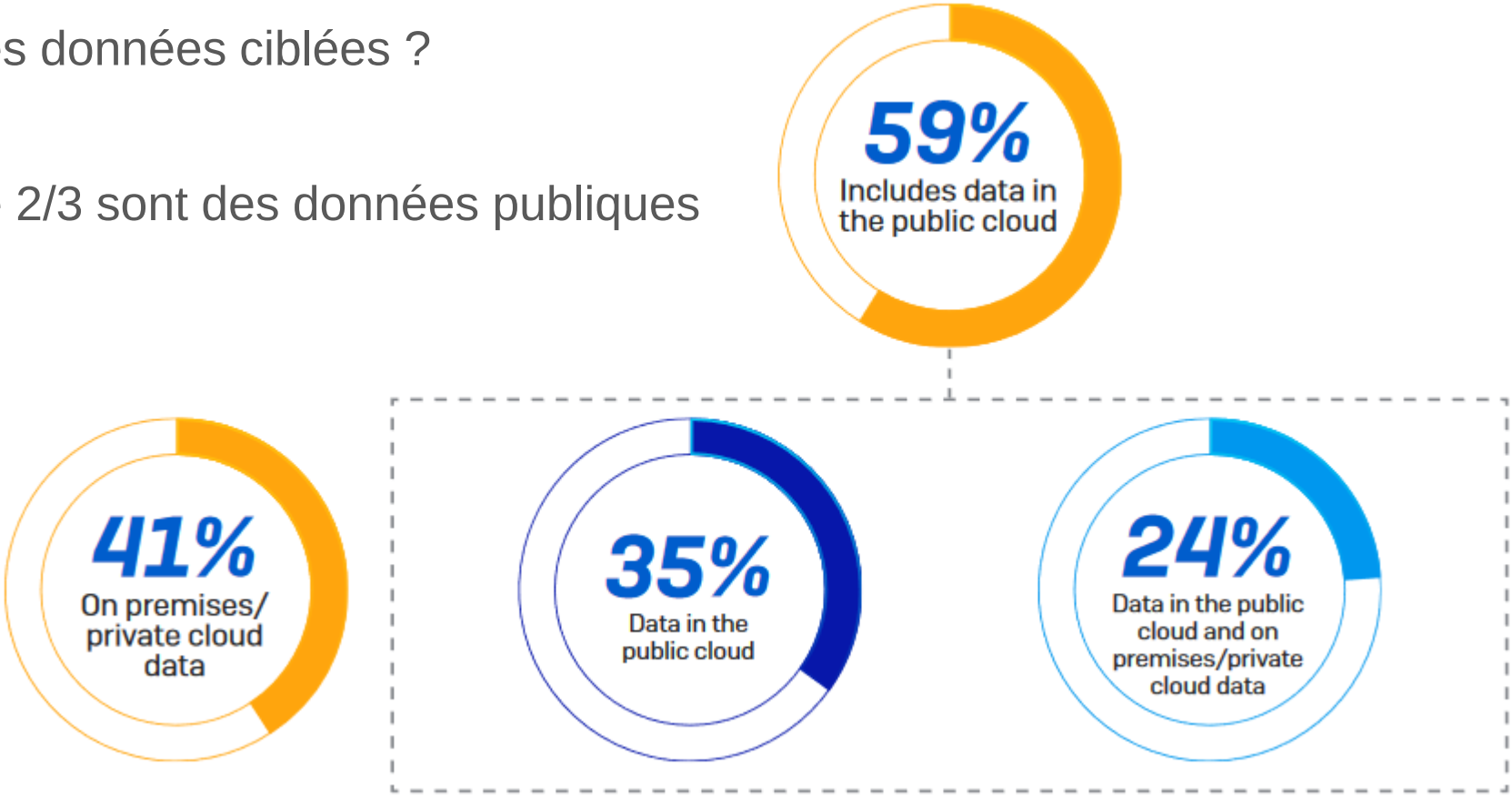


https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Menace 2020 mais aussi une Récurrence 2020

Les données ciblées ?

Le 2/3 sont des données publiques



https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Menace 2020 mais aussi une Récurrence 2020

Les coûts de la remédiation ?

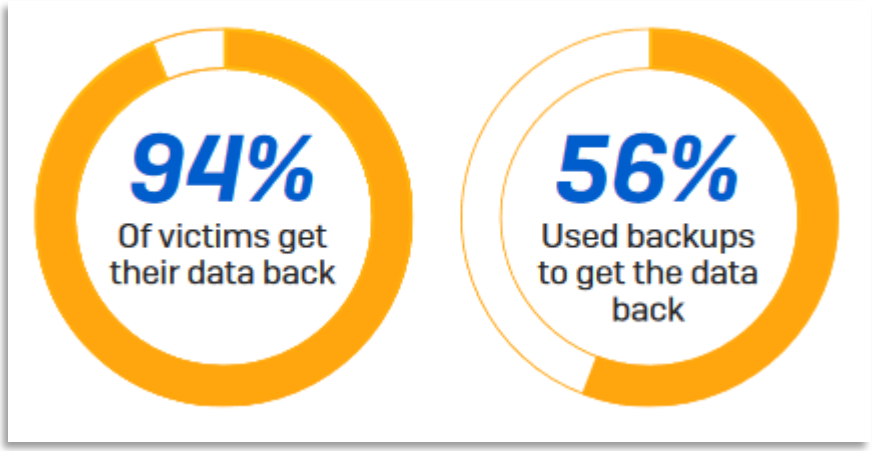
$$

https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Menace 2020 mais aussi une Récurrence 2020

Les données retrouvées ?

OUI!!!



https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

ISACA Section de Québec

Menace 2020 mais aussi une Récurrence 2020

Les campagnes les plus payantes ?

10. How much money have recent cyber attacks raised?

#	Name of ransomware	Period	Profit evaluation
1	CryptoLocker	2013	~$3 million
2	Cryptowall	2014-16	~$18-320 million
3	Locky		$7.8-150 million
4	Cerber		$6.9 million
5	WannaCry	2016	$55,000-$140,000
6	Petya/NotPetya		$10,000

https://dataprot.net/statistics/ransomware-statistics/

ISACA Section de Québec

Menaces 2020

5.1- Infonuagique

Azure/AWS : compromission de comptes via des attaques d'hameçonnage – lien vers une page clonée d'authentification Azure/AWS

Défense ? MFA / 2FA

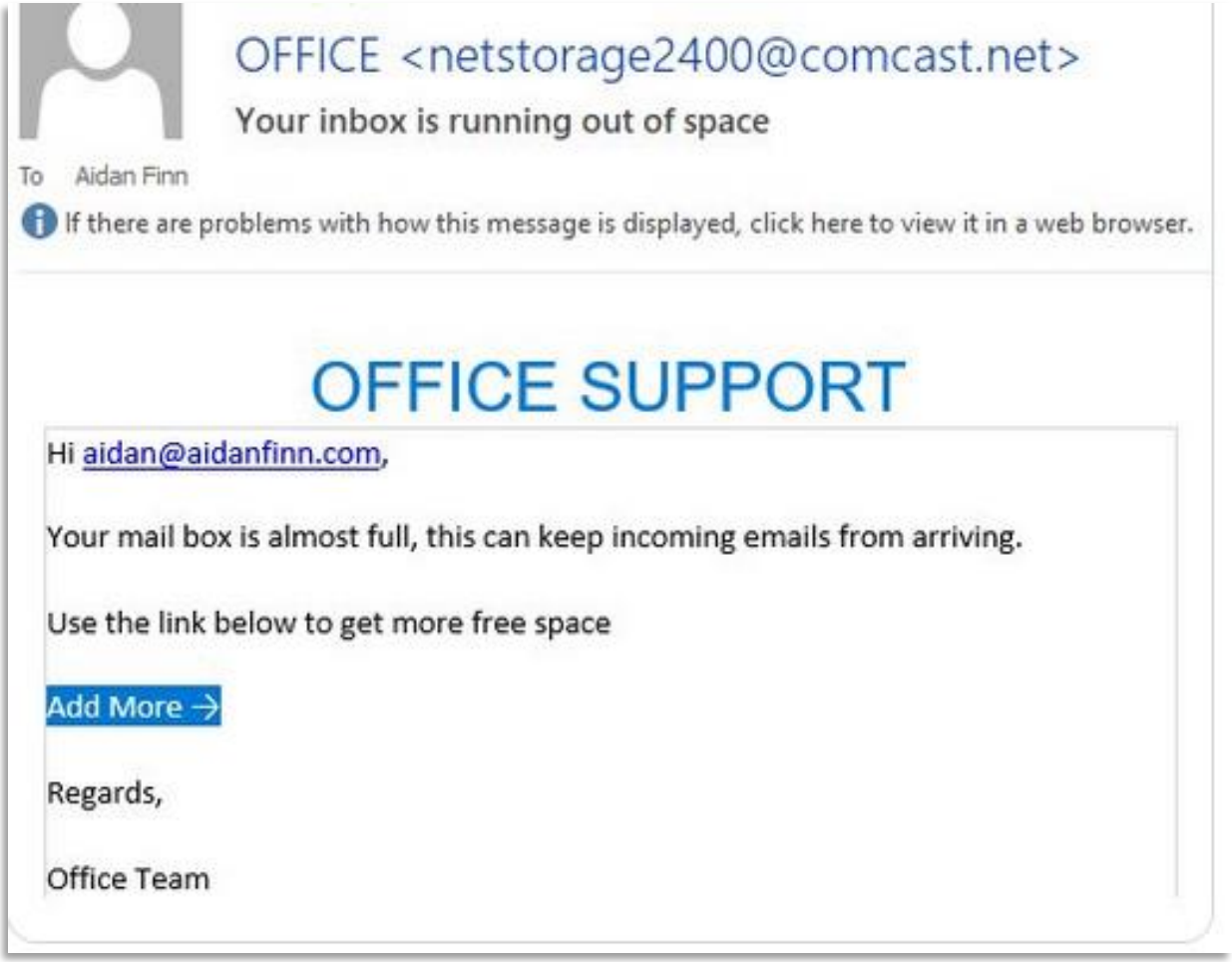
https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Recommandations : CIS Benchmark (Azure & Office 365)

https://learn.cisecurity.org/benchmarks

Webcast : Legacy Authentication and Password Spray, Understanding and Stopping Attackers Favorite TTPs in Azure AD SANS 19 août 2019

Menaces 2020



OFFICE <netstorage2400@comcast.net>

Your inbox is running out of space

To Aidan Finn

If there are problems with how this message is displayed, click here to view it in a web browser.

OFFICE SUPPORT

Hi aidan@aidanfinn.com,

Your mail box is almost full, this can keep incoming emails from arriving.

Use the link below to get more free space

Add More →

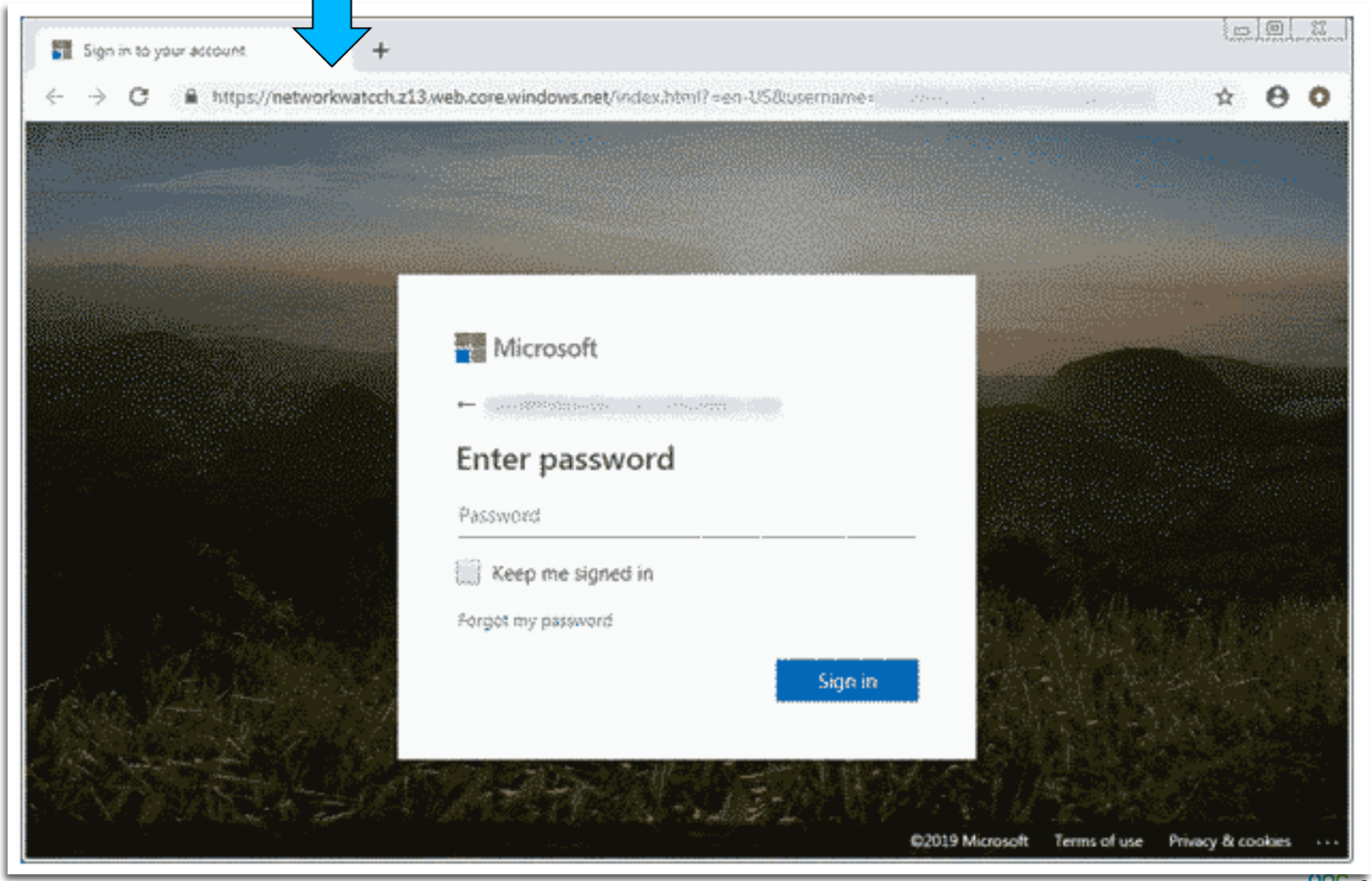
Regards,

Office Team

Un exemple de courriel d'hameçonnage

ISACA Section de Québec

Menaces 2020



Un exemple de fausse page d'authentification Azure

ISACA Section de Québec

Menaces 2020

Oups!

Interestingly, Coalition found that companies using Microsoft Office 365 were three times more likely to experience a business email compromise incident than companies using alternatives such as G Suite or WPS Office.

https://www.techspot.com/news/86714-over-41-percent-cyber-insurance-claims-2020-came.html

Menaces 2020

5.2- Infonuagique

Azure/AWS : réutilisation du mot de passe / “password spray”

https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

Défense ? MFA / 2FA

Recommandations : CIS Benchmark (Azure & Office 365)

https://learn.cisecurity.org/benchmarks

Webcast : Legacy Authentication and Password Spray, Understanding and Stopping Attackers Favorite TTPs in Azure AD SANS 19 août 2019

ISACA Section de Québec

Menaces 2020

Remote Cloud Execution – Critical Vulnerabilities in Azure Cloud Infrastructure

https://research.checkpoint.com/2020/remote-cloud-execution-critical vulnerabilities-in-azure-cloud-infrastructure-part-i/

https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/

Menaces 2020

chuttttt!!!

https://github.com/Greenwolf/Spray
(Outlook Web Access)

https://github.com/sensepost/ruler
(Outlook Web Access)

Divers “scanners” et “exploits” de Metasploit (owa, exchange, etc.)

Menaces 2020

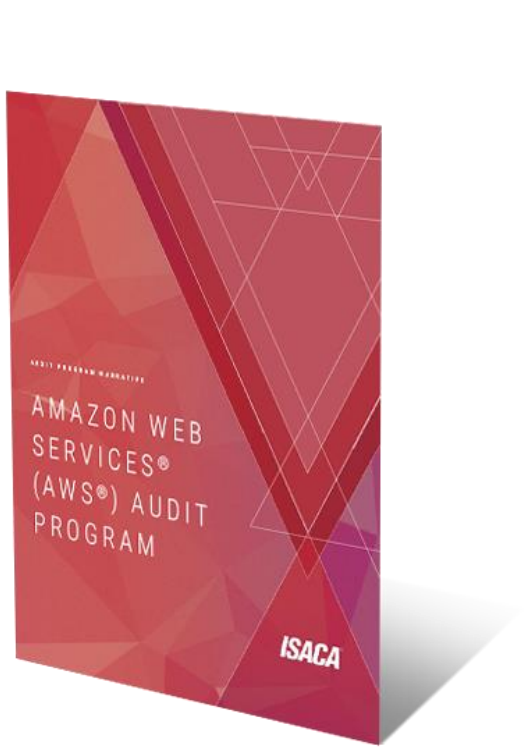
Exploits dans Metasploit :

```
root@kali: ~

┌──(root㉿ kali)-[~]
└─# searchsploit Azure
------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                           |  Path
------------------------------------------------------------------------- ---------------------------------
Azure Data Expert Ultimate 2.2.16 - Remote Buffer Overflow               | windows/remote/41545.py
Azuresites CMS - Multiple Vulnerabilities                                | php/webapps/5702.txt
Azureus HTML WebUI 0.7.6 - Cross-Site Request Forgery                    | multiple/webapps/31673.txt
------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(root㉿ kali)-[~]
└─# searchsploit Amazon
------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                           |  Path
------------------------------------------------------------------------- ---------------------------------
Amazon S3 Uploadify Script - 'Uploadify.php' Arbitrary File Upload       | php/webapps/37450.txt
DUware DUamazon Pro 3.0/3.1 - 'catDelete.asp?iCat' SQL Injection         | asp/webapps/25863.txt
DUware DUamazon Pro 3.0/3.1 - 'detail.asp?iSub' SQL Injection            | asp/webapps/25865.txt
DUware DUamazon Pro 3.0/3.1 - 'productDelete.asp?iCat' SQL Injection     | php/webapps/25861.txt
DUware DUamazon Pro 3.0/3.1 - 'productEdit.asp?iCat' SQL Injection       | php/webapps/25862.txt
DUware DUamazon Pro 3.0/3.1 - 'review.asp?iPro' SQL Injection            | asp/webapps/25864.txt
DUware DUamazon Pro 3.0/3.1 - 'type.asp?iType' SQL Injection             | php/webapps/25860.txt
FS Amazon Clone - 'category_id' SQL Injection                            | php/webapps/43035.txt
FS Amazon Clone 1.0 - SQL Injection                                      | php/webapps/43259.txt
GhostScripter Amazon Shop 5.0 - 'search.php' SQL Injection               | php/webapps/26653.txt
Just William's Amazon Webstore - 'Closeup.php?Image' Cross-Site Scripting | php/webapps/25560.txt
Just William's Amazon Webstore - 'CurrentIsExpanded' Cross-Site Scripting | php/webapps/25564.txt
Just William's Amazon Webstore - 'CurrentNumber' Cross-Site Scripting    | php/webapps/25566.txt
Just William's Amazon Webstore - 'searchFor' Cross-Site Scripting        | php/webapps/25565.txt
Just William's Amazon Webstore - HTTP Response Splitting                 | php/webapps/25567.txt
MRCGIGUY Amazon Directory 1.0/2.0 - Insecure Cookie Handling             | php/webapps/8685.txt
phpBB Amazonia Mod - 'zufallscodepart.php' Remote File Inclusion         | php/webapps/2544.pl
tghostscripter Amazon Shop - Cross-Site Scripting / Directory Traversal / Remote File Inclusion | php/webapps/8145.txt
------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Searchsploit (Kali Linux)

Interlude : ISACA ☺

Publications au sujet de la sécurité / infonuagique par ISACA



https://www.isaca.org/bookstore/audit-control-and-security-essentials/waaws
https://www.isaca.org/bookstore/audit-control-and-security-essentials/waazu

ISACA Section de Québec

Menaces 2020

6- Télétravail :

Beaucoup d’articles ont été publiés ou de conférences et de formations présentées depuis mars 2020 concernant le télétravail.

Un nombre élevé d’exploitation de vulnérabilités des applications de vidéo-conférence (Zoom, MS Teams, etc.).

Menaces 2020

Selon Verizon, 30 % des attaques depuis le début de l'année comporte "un acteur interne" et ces attaques ont couté environ 11 millions $ selon Ponemon.

- Employé malveillant = 14%
- Employé "compromis" = 23%
- Employé négligent = 62%

Le télétravail a créé des conditions parfaites pour devenir LA menace de 2020 ?

https://www.digitalshadows.com/blog-and-research/2020-verizon-data-breach-investigations-report-dbir-ciso-view/

https://www.observeit.com/cost-of-insider-threats/

Menaces 2020

Risques ?

- Vol de temps?
- Vol d'informations sensibles?
- Utilisation des équipements personnels pour le travail?
- Aucune utilisation de chiffrement (communication, données, etc.)?
- On oublie les mises à jour?
- On oublie que nous travaillons pour notre employeur?!
- On laisse des documents sensibles à la vue des autres…?!
- …

Menaces 2020

Mesures ?

- Chiffrement des communications (VPN);
- Chiffrement de vos données sensibles;
- Politique de sécurité (utilisation de périphériques USB, accès à distance, BYOD);
- Surveiller l'utilisation de protocoles et d'applications (à distance).

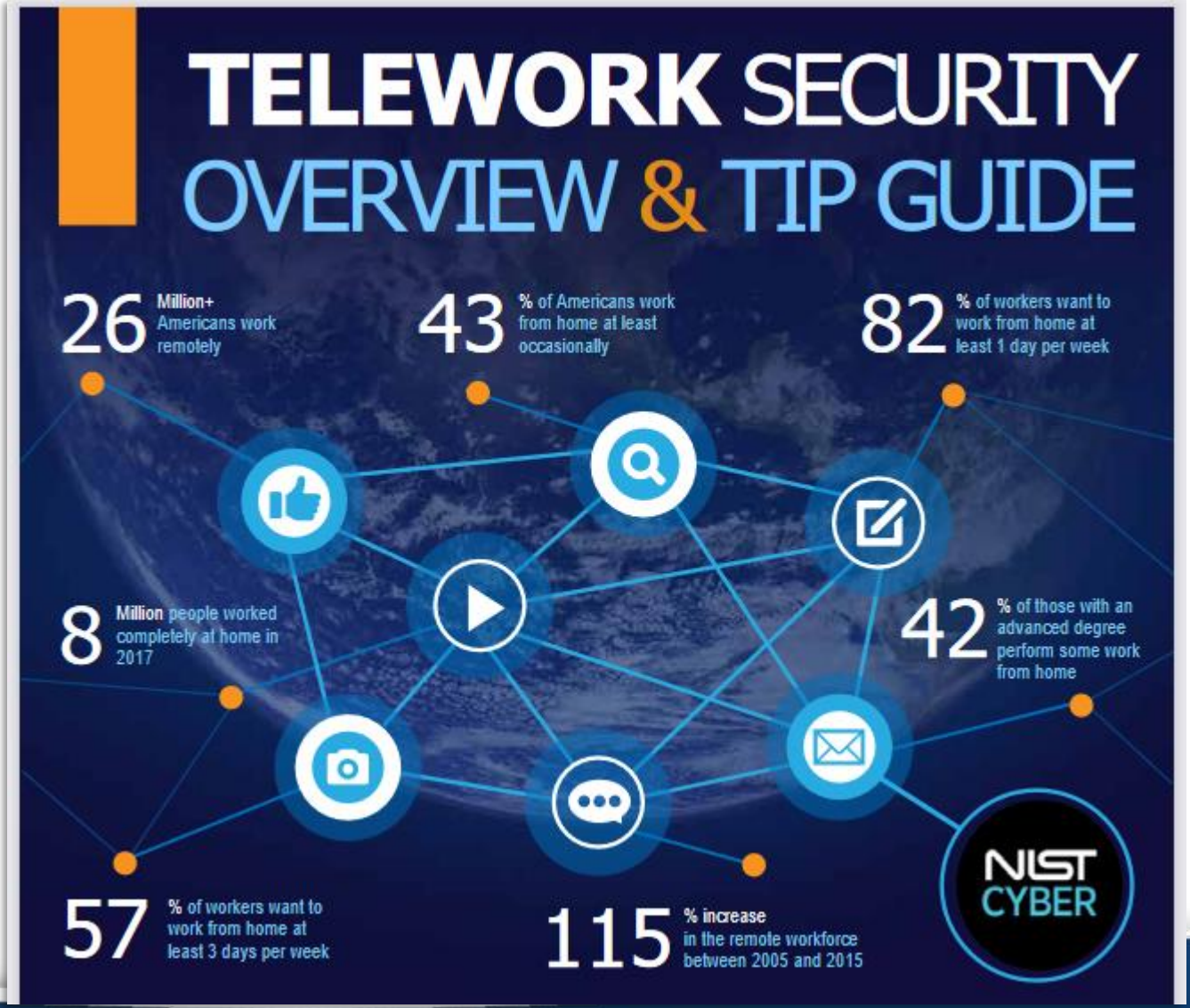
Vulnérabilités à surveiller reliées au télétravail :

- Pulse Secure, Fortinet, Palo Alto, Citrix, Cisco, MS Exchange, Remote Desktop, MS Office, outils de vidéo-conférence, etc.

ISACA
Section de Québec

Menaces 2020

Mesures ?



https://www.nist.gov/system/files/documents/2020/03/18/Telework%20Overview%20and%20Tips.pdf

Interlude : ISACA ☺

Publication au sujet du télétravail par ISACA

Réussir le télétravail pendant (et après) la pandémie de COVID-19

Author: Michel Lambert, CISA, CISM, CGEIT, CRISC, modérateur du forum 'Information and Cybersecurity' d'ISACA, ancien président et conseiller stratégique au conseil d'administration du chapitre de Québec d'ISACA; Jean-Louis Louiset, CISA, conseiller au conseil d'administration du chapitre de Québec d'ISACA; and Marie-Jeanne Sidibe, ISO 9001, conseillère au conseil d'administration du chapitre de Québec d'ISACA

Date Published: 5 May 2020

English

https://www.isaca.org/fr-fr/resources/news-and-trends/isaca-now-blog/2020/telework-successfully-during-and-after-the-covid-19-pandemic

ISACA Section de Québec

Selon ISACA QC :

Télétravail avec des ordinateurs personnels

Pour mitiger le risque que l'équipement personnel des télétravailleurs puisse compromettre les données et les applications de l'entreprise, une condition préalable est d'entreprendre le télétravail avec une machine propre en utilisant un bon logiciel antivirus. Les télétravailleurs devraient alors:

1. Mettre à jour tous leurs logiciels et applications.
2. Activer l'option de chiffrement du disque local.
3. Créer un compte séparé pour le télétravail (pas d'administrateur).
4. Configurer leur Wi-Fi avec un mot de passe fort et le protocole WPA2, puis chiffrer tout ce qu'ils transmettent à partir d'un Wi-Fi public.
5. Se mettre d'accord avec leur employeur sur l'endroit où ils doivent placer une copie des données.
6. Si possible, utiliser la boîte de courriel (boîte mail) de l'organisation
7. Utiliser un outil de gestion des mots de passe.

Télétravail avec des ordinateurs d'entreprise

Fournir aux télétravailleurs les équipements de l'entreprise peut leur permettre d'atteindre tous leurs objectifs et réduire considérablement le risque d'interruption des activités.

1. Utiliser le VPN pour se connecter aux serveurs de l'entreprise.
2. Adopter une authentification à double facteur.
3. Utiliser uniquement les applications installées par l'entreprise.
4. Utiliser les équipements qu'à des fins professionnelles.
5. Ne pas autoriser l'accès à d'autres personnes.
6. Utiliser uniquement les solutions fournies par l'entreprise pour collaborer avec les collègues.
7. Utiliser uniquement la boîte de courriel (boîte mail) de l'organisation.

https://www.isaca.org/fr-fr/resources/news-and-trends/isaca-now-blog/2020/telework-successfully-during-and-after-the-covid-19-pandemic

Menaces 2020

7- Informations sensibles (codes sources, etc.) sur Github

Une utilisation très importante de Github pour le dépôt de codes sources… surveillez-vous vos développeurs? Sécurisation des dépôts?

Risque : Divulgation d'informations sensibles…

Outil : https://github.com/michenriksen/gitrob

Défense : Politique de sécurité – Surveillance

Menaces 2020

8- Services web comme Buckets SW3

Informations sensibles dans vos “Buckets” publics ? Un storage public infonuagique (Amazon Web Services (AWS) Simple Storage Service).

Risque : Divulgation d’informations sensibles…

Outil : https://buckets.grayhatwarfare.com/

Défense : Politique de sécurité – Surveillance

Menaces 2020

9- Typosquatting/Cybersquatting

Pour le fraudeurs/hameçonneur/pirate, c'est la technique utilisée pour identifier les possibilités d'enregistrer des noms de domaines qui s'apparentent au nom de domaine de l'entreprtise qu'il veut cibler lors d'une campagne d'hameçonnage. Les noms de domaine ont des erreurs de frappes, des remplacements de lettres, divers TLD, etc.

Problèmes ? Certains registraires permettent plus de 1000 enregistrements de noms de domaine !

Menaces 2020

Risques ?

- Campagne d’hameçonnage ciblant votre entreprise ?
- Utilisation de votre image de marque ?

ISACA Section de Québec

Menaces 2020

Mesures ?

Vérifier les noms de domaine qui sont enregistrés et qui ressemblent à votre nom de domaine : ils sont probablement enregistrés par des fraudeurs!

Enregistrez les noms de domaine avec les divers TLD. Ex : vous avez le .com, pourquoi ne pas acheter aussi le .org, .io, .net, etc.?

Outil : URL Crazy (Kali Linux)

Intéressant : https://www.techrepublic.com/article/how-fraudulent-domain-names-are-powering-phishing-attacks/

Menaces 2020

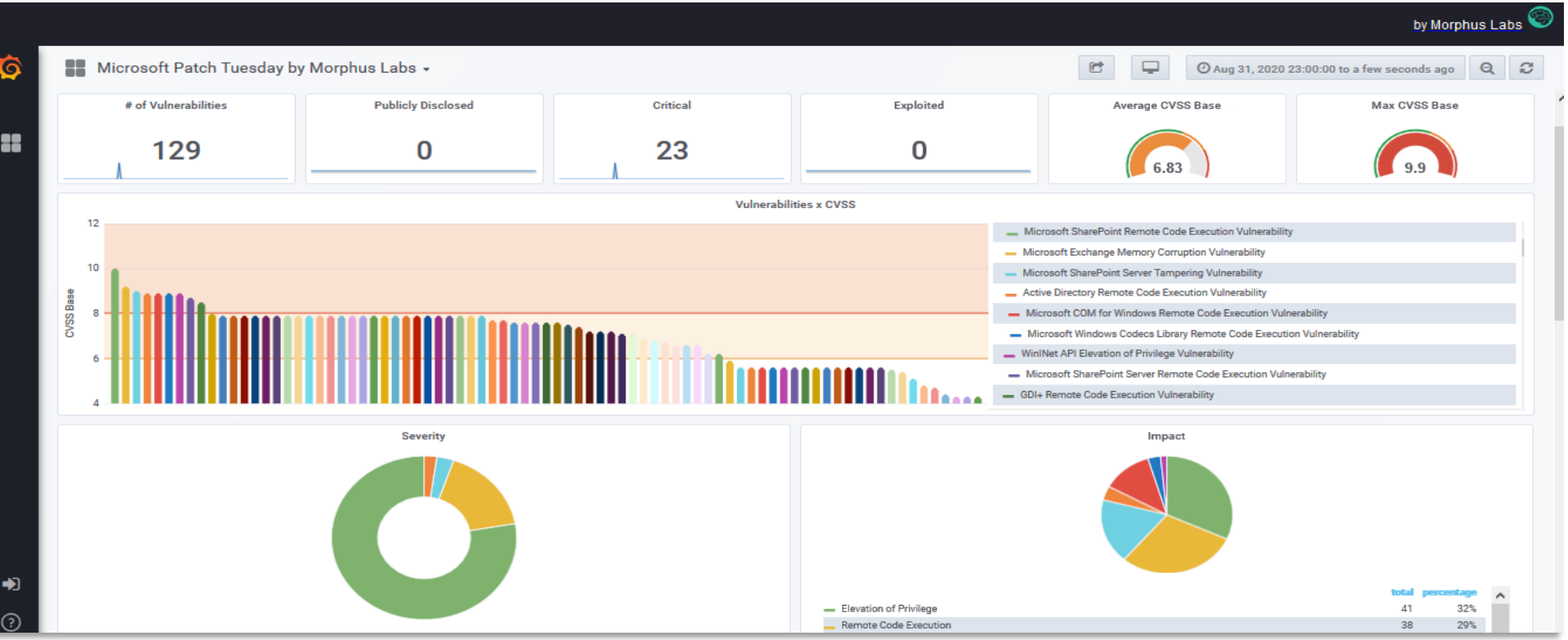
```
┌──(root㉿kali)-[/opt/urlcrazy]
└─# ./urlcrazy bmo.com -p
Warning. File descriptor limit may be too low. Check with `ulimit -a` and change with `ulimit -n 10000`

URLCrazy Domain Report
Domain    : bmo.com
Keyboard  : qwerty
At        : 2020-09-30 18:43:36 -0400
# Please wait. 1985 hostnames to process

^Z
zsh: suspended  ./urlcrazy bmo.com -p

┌──(root㉿kali)-[/opt/urlcrazy]
└─# ./urlcrazy pepsi.com -p
Warning. File descriptor limit may be too low. Check with `ulimit -a` and change with `ulimit -n 10000`

URLCrazy Domain Report
Domain    : pepsi.com
Keyboard  : qwerty
At        : 2020-09-30 18:43:41 -0400
# Please wait. 2014 hostnames to process

^Z
zsh: suspended  ./urlcrazy pepsi.com -p

┌──(root㉿kali)-[/opt/urlcrazy]
└─# ./urlcrazy isaca.org -p
Warning. File descriptor limit may be too low. Check with `ulimit -a` and change with `ulimit -n 10000`

URLCrazy Domain Report
Domain    : isaca.org
Keyboard  : qwerty
At        : 2020-09-30 18:43:51 -0400
# Please wait. 2011 hostnames to process

^Z
zsh: suspended  ./urlcrazy isaca.org -p
```

ISACA Section de Québec

URL Crazy (Kali Linux)

Menace 2020 mais aussi une Récurrence 2020

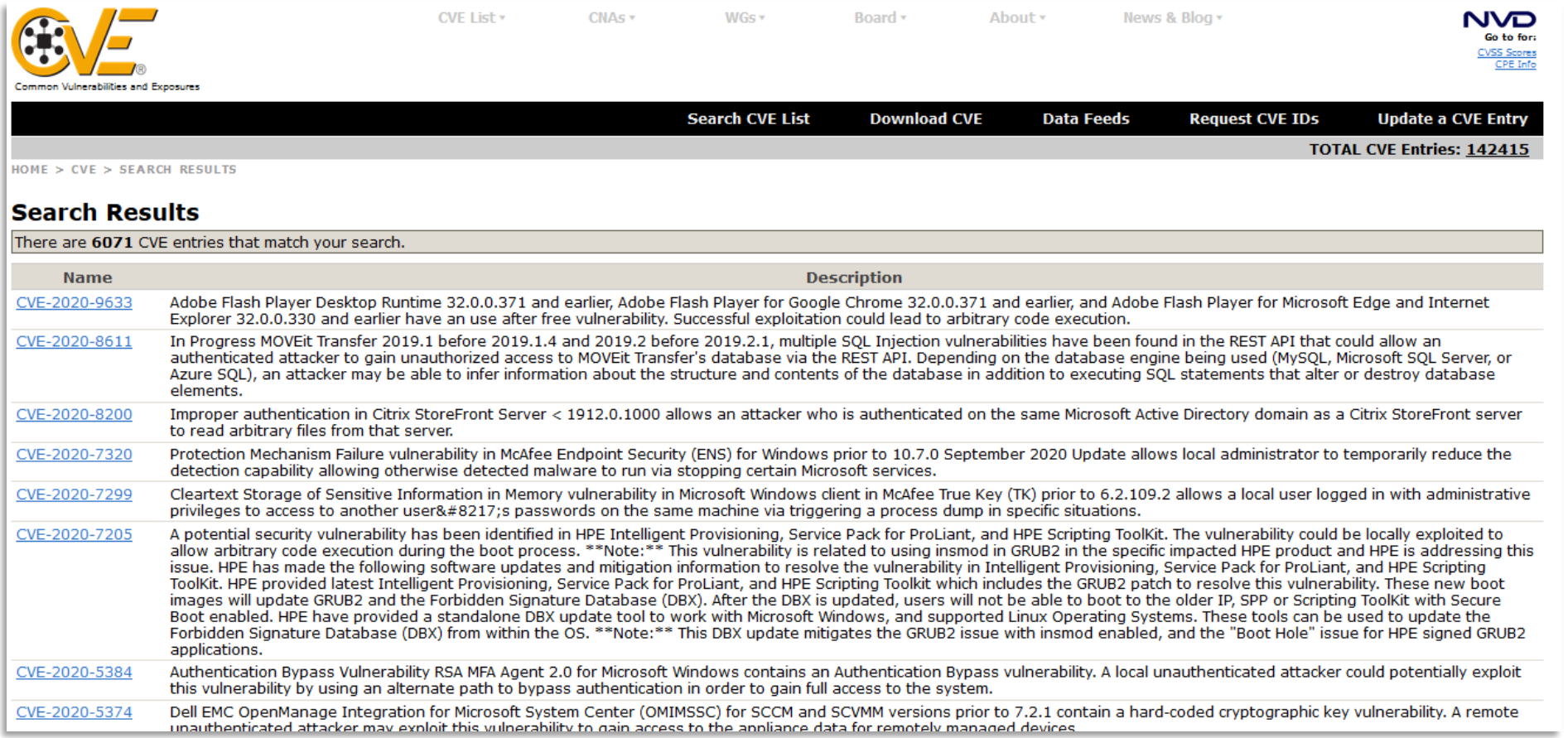
10- Les vulnérabilités Microsoft Windows



https://patchtuesdaydashboard.com/

ISACA Section de Québec

Menace 2020 mais aussi une Récurrence 2020



CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

Common Vulnerabilities and Exposures

NVD
Go to for:
CVSS Scores
CPE Info

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 142415

HOME > CVE > SEARCH RESULTS

Search Results

There are **6071** CVE entries that match your search.

Name	Description
CVE-2020-9633	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-8611	In Progress MOVEit Transfer 2019.1 before 2019.1.4 and 2019.2 before 2019.2.1, multiple SQL Injection vulnerabilities have been found in the REST API that could allow an authenticated attacker to gain unauthorized access to MOVEit Transfer's database via the REST API. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or destroy database elements.
CVE-2020-8200	Improper authentication in Citrix StoreFront Server < 1912.0.1000 allows an attacker who is authenticated on the same Microsoft Active Directory domain as a Citrix StoreFront server to read arbitrary files from that server.
CVE-2020-7320	Protection Mechanism Failure vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local administrator to temporarily reduce the detection capability allowing otherwise detected malware to run via stopping certain Microsoft services.
CVE-2020-7299	Cleartext Storage of Sensitive Information in Memory vulnerability in Microsoft Windows client in McAfee True Key (TK) prior to 6.2.109.2 allows a local user logged in with administrative privileges to access to another user’s passwords on the same machine via triggering a process dump in specific situations.
CVE-2020-7205	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications.
CVE-2020-5384	Authentication Bypass Vulnerability RSA MFA Agent 2.0 for Microsoft Windows contains an Authentication Bypass vulnerability. A local unauthenticated attacker could potentially exploit this vulnerability by using an alternate path to bypass authentication in order to gain full access to the system.
CVE-2020-5374	Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC) for SCCM and SCVMM versions prior to 7.2.1 contain a hard-coded cryptographic key vulnerability. A remote unauthenticated attacker may exploit this vulnerability to gain access to the appliance data for remotely managed devices

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=microsoft
https://www.beyondtrust.com/resources/whitepapers/microsoft-vulnerability-report

ISACA Section de Québec

Menace 2020 mais aussi une Récurrence 2020

Windows est toujours le SE le plus utilisé!

OS Platform Statistics

2020	Win10	Win8	Win7	WinXP	Linux	Mac	Chrome OS	Mobile
August	61.0%	3.2%	6.8%	0.1%	4.9%	10.3%	0.3%	13.5%
July	61.0%	3.0%	7.2%	0.1%	5.0%	10.6%	0.3%	12.9%
June	61.0%	3.0%	7.2%	0.1%	4.9%	11.3%	0.3%	12.1%
May	60.1%	3.1%	7.2%	0.1%	4.9%	11.9%	0.4%	12.3%
April	60.1%	3.2%	7.4%	0.1%	4.8%	12.4%	0.4%	11.8%
March	60.6%	3.2%	8.5%	0.1%	5.4%	11.1%	0.4%	10.8%
February	59.1%	3.5%	9.8%	0.2%	5.9%	9.9%	0.0%	11.4%
January	58.1%	3.6%	10.6%	0.2%	6.4%	9.7%	0.4%	11.2%

https://www.w3schools.com/browsers/browsers_os.asp

Menace 2020

Publié le 29 septembre !

- In 2019, we blocked over 13 billion malicious and suspicious mails, out of which more than 1 billion were URLs set up for the explicit purpose of launching a phishing credential attack.
- Ransomware is the most common reason behind our incident response engagements from October 2019 through July 2020.
- The most common attack techniques used by nation-state actors in the past year are reconnaissance, credential harvesting, malware and virtual private network (VPN) exploits.
- IoT threats are constantly expanding and evolving. The first half of 2020 saw an approximate 35% increase in total attack volume compared to the second half of 2019.

https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

Tendances 2021

Attaques Cloud

Rançongiciel

BYOD

Menace interne

IOT

Manque de “cyber talents”

Données sensibles

Intelligence artificielle

Covid-19

ISACA Section de Québec

Autres liens

https://www.helpnetsecurity.com/2019/12/09/compromised-passwords-microsoft-accounts/

https://adeliarisk.com/secure-cloud-computing-7-ways-id-hack-aws/#Hack_1_The_Little_Phish_The_Password_is_Catch_of_the_Day

https://www.forbes.com/sites/zakdoffman/2020/03/07/microsoft-confirms-really-really-high-hacking-threat-for-millions-of-users-heres-what-you-do-now/#31f0db8f9b66

https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-

ISACA Section de Québec

Autres liens ISACA

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-2/cloud-insecurities

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-3/security-mysteries-in-the-cloud

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/cloud-computing-are-your-data-secure-in-the-cloud

https://www.isaca.org/bookstore/audit-control-and-security-essentials/waaws

https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2020/isacas-new-azure-audit-program-focuses-on-a-leading-cloud-service-provider

https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2018/isaca-issues-new-audit-and-assurance-programs-for-microsoft-platforms

https://www.isaca.org/bookstore/audit-control-and-security-essentials/waazu

Merci!

Questions ?

Divers webinaires sur ISACA-Quebec.ca

Et aussi :

https://www.getcybersafe.gc.ca/fr/mois-de-la-sensibilisation-la-cybersecurite

nadia.vigneault@protonmail.com

ISACA®
Section de Québec