





Cyber - (.*)

octobre 2022

Liminaire



« Le seul système informatique vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés.

Même dans ces conditions, je ne parierais pas ma vie dessus. »

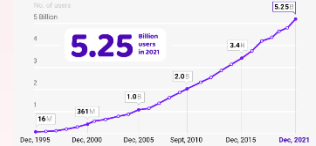
Pr .Eugene Spafford
Purdue University



(chiffres février 2022)

↗ 6,25 milliards d'utilisateurs dans le monde (60,92 millions en France)

- ↗ 32% des utilisateurs d'internet ont entre 25 et 34 ans, 19% entre 35-44 ans
- ↗ 28,5 milliards d'appareils connectés dans le monde
- ↗ Temps passé sur les réseaux sociaux par les 15-24 ans : 2h07 par jour
- ↗ 5h34 de temps passé en ligne par jour !
- ↗ 1,4 milliard d'emails envoyés en France par jour (333,2 milliards d'emails dans le monde] et 85% sont des spams !

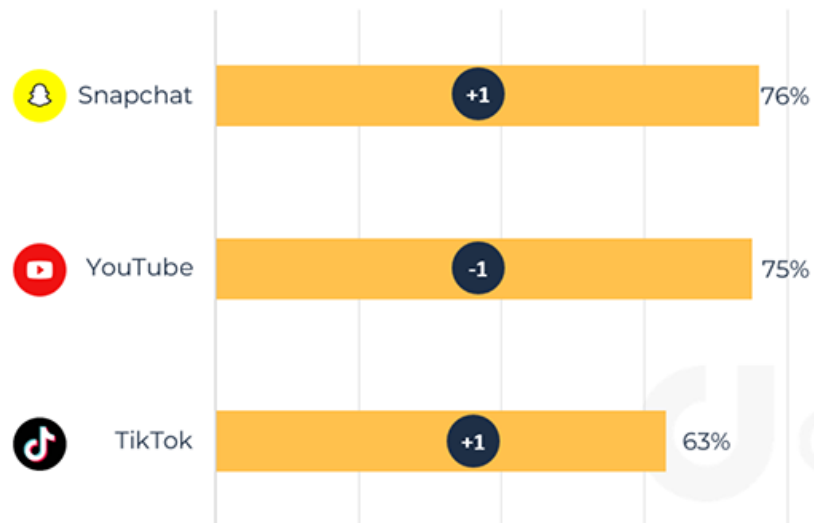


- ↗ Google Chrome représente 65,9% du marché des navigateurs
- ↗ 92,17% des utilisateurs utilise le moteur de recherche de Google (100 Millions de Go indexés)

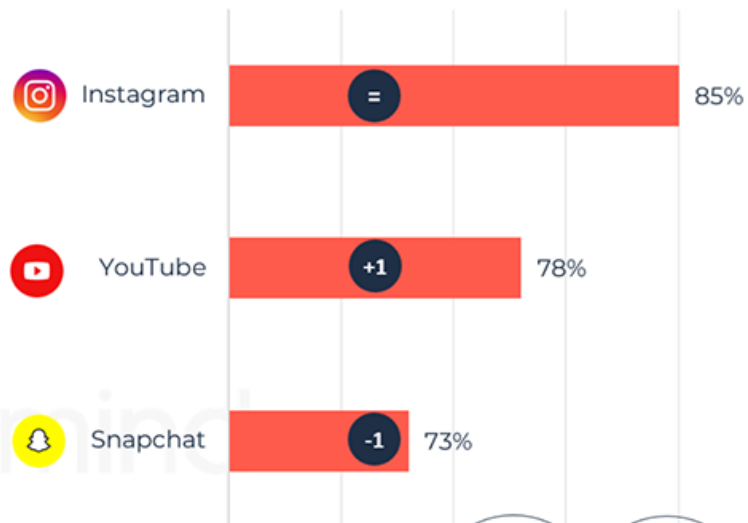
Les plateformes sociales préférées des 11-18 ans



11-14 ans



15-18 ans



11-18 ans
France

Les
médias
sociaux
utilisés

Source : Génération Numérique – Enquête 2021-2022- 17013 jeunes



Evolutions 2022 / 2021 en position



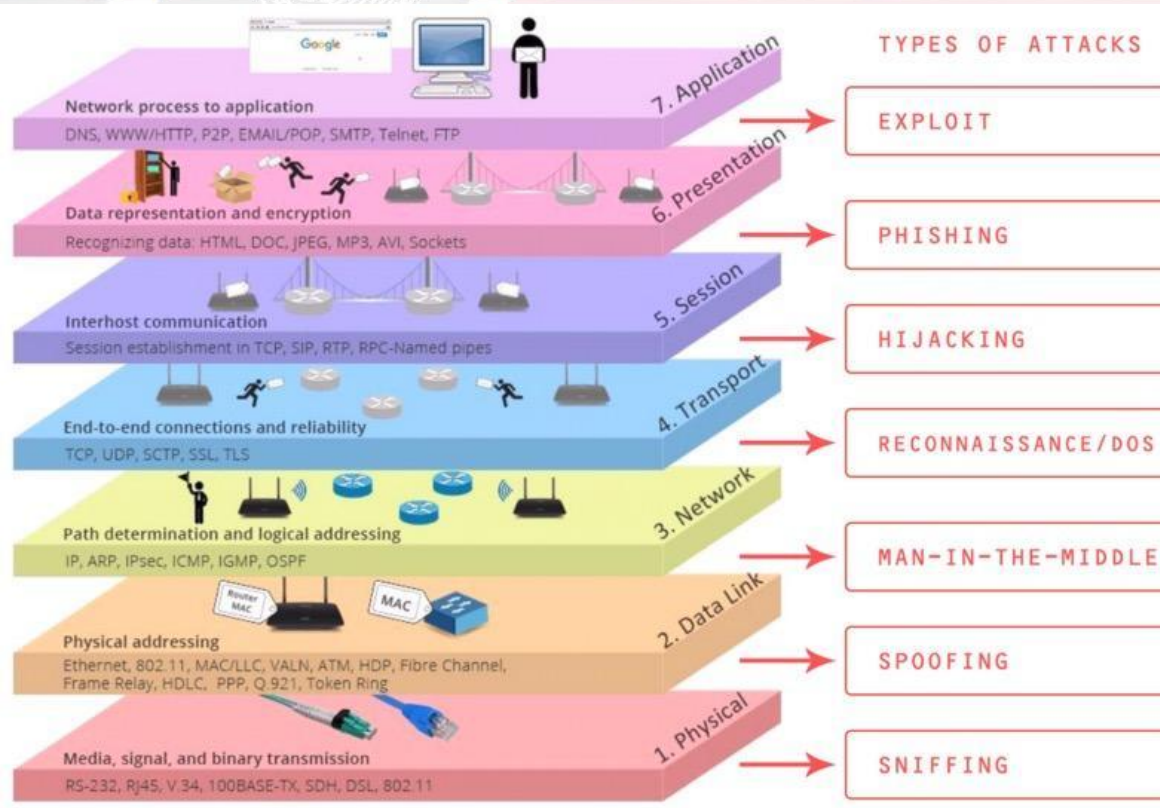
An illustration of an iceberg floating in a blue ocean. The tip of the iceberg, which is above the water line, is light yellow and jagged. A small red flag with a white heart is planted on its peak. The much larger part of the iceberg is submerged in the water, appearing as a dark blue, jagged shape. The background is a gradient of light blue at the top and darker blue at the bottom, representing the sky and the ocean respectively.

Surface Web

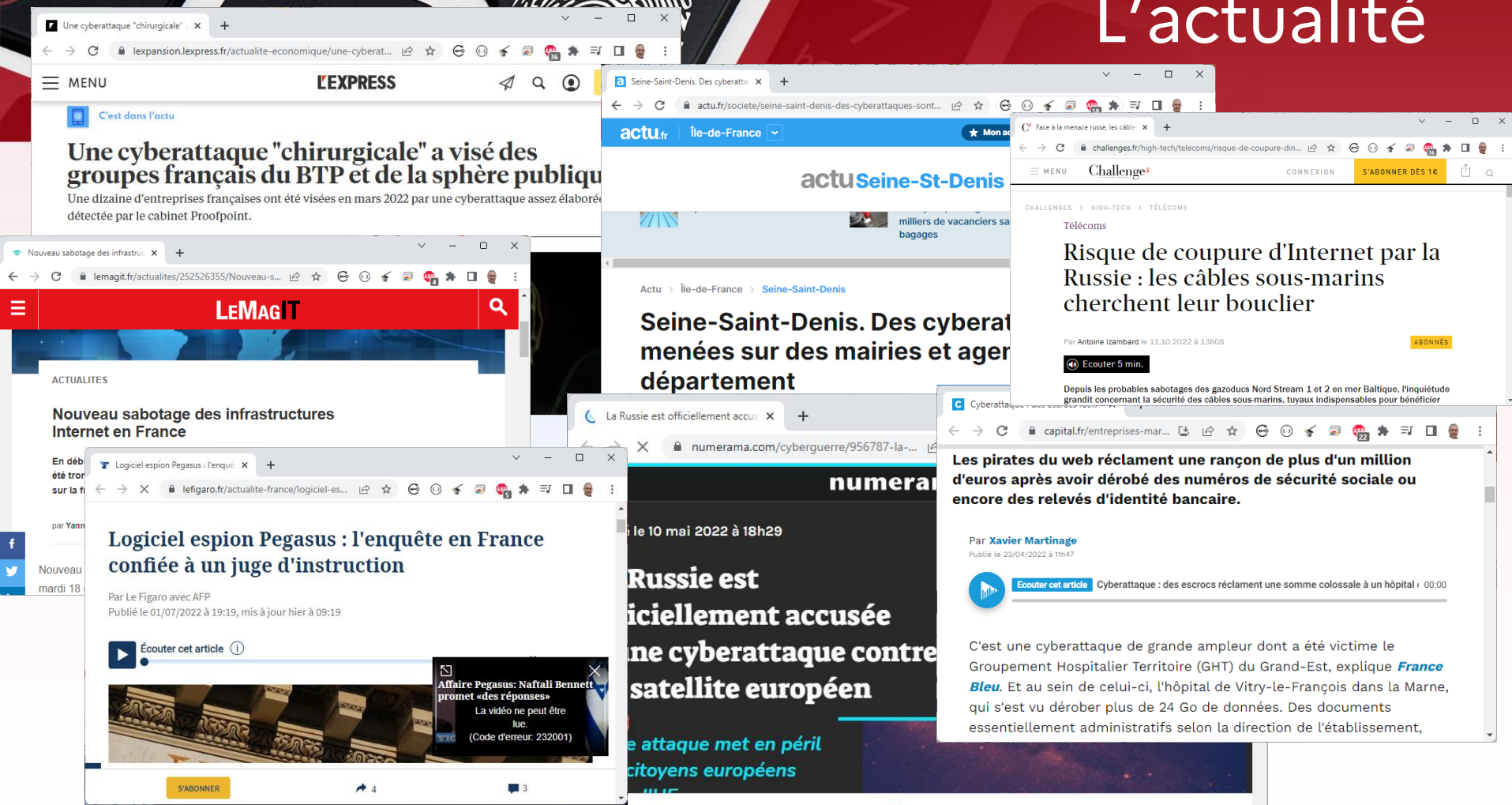
Deep Web

Dark Web

Internet



L'actualité



Une cyberattaque "chirurgicale" a visé des groupes français du BTP et de la sphère publique

Une dizaine d'entreprises françaises ont été visées en mars 2022 par une cyberattaque assez élaborée détectée par le cabinet Proofpoint.

Nouveau sabotage des infrastructures

LeMAGIT

ACTUALITES

Nouveau sabotage des infrastructures Internet en France

En déb
été tron
sur la fi

par Yann

Nouveau
mardi 18

Logiciel espion Pegasus : l'enquête en France confiée à un juge d'instruction

Par Le Figaro avec AFP
Publié le 01/07/2022 à 19:19, mis à jour hier à 09:19

Écouter cet article



S'ABONNER

4

3

Seine-Saint-Denis. Des cyberattaques menées sur des mairies et agences du département

actuSeine-St-Denis

Actu > Île-de-France > Seine-Saint-Denis

milliers de vacanciers sa bagages

Seine-Saint-Denis. Des cyberattaques menées sur des mairies et agences du département

La Russie est officiellement accusée d'une cyberattaque contre un satellite européen

numerama

le 10 mai 2022 à 18h29

Russie est officiellement accusée d'une cyberattaque contre un satellite européen

Face à la menace russe, les câbles : le risque de coupure d'Internet par la Russie : les câbles sous-marins cherchent leur bouclier

Challenge

Risque de coupure d'Internet par la Russie : les câbles sous-marins cherchent leur bouclier

Par Antoine Izambard le 11.10.2022 à 13h08

Écouter 5 min.

Depuis les probables sabotages des gazoducs Nord Stream 1 et 2 en mer Baltique, l'inquiétude grandit concernant la sécurité des câbles sous-marins, tuyaux indispensables pour bénéficier

Cyberattaque : des escrocs réclament une somme colossale à un hôpital

Les pirates du web réclament une rançon de plus d'un million d'euros après avoir dérobé des numéros de sécurité sociale ou encore des relevés d'identité bancaire.

Par Xavier Martinage
Publié le 23/04/2022 à 11h47

Écouter cet article

Cyberattaque : des escrocs réclament une somme colossale à un hôpital 00:00

C'est une cyberattaque de grande ampleur dont a été victime le Groupement Hospitalier Territoire (GHT) du Grand-Est, explique France Bleu. Et au sein de celui-ci, l'hôpital de Vitry-le-François dans la Marne, qui s'est vu dérober plus de 24 Go de données. Des documents essentiellement administratifs selon la direction de l'établissement,



Des faits (récents) en France

- des logiciels espion
 - des faits de guerre et de désinformation
 - Des sabotages
-
- des vols de données
 - des demandes de rançon (ransomware)



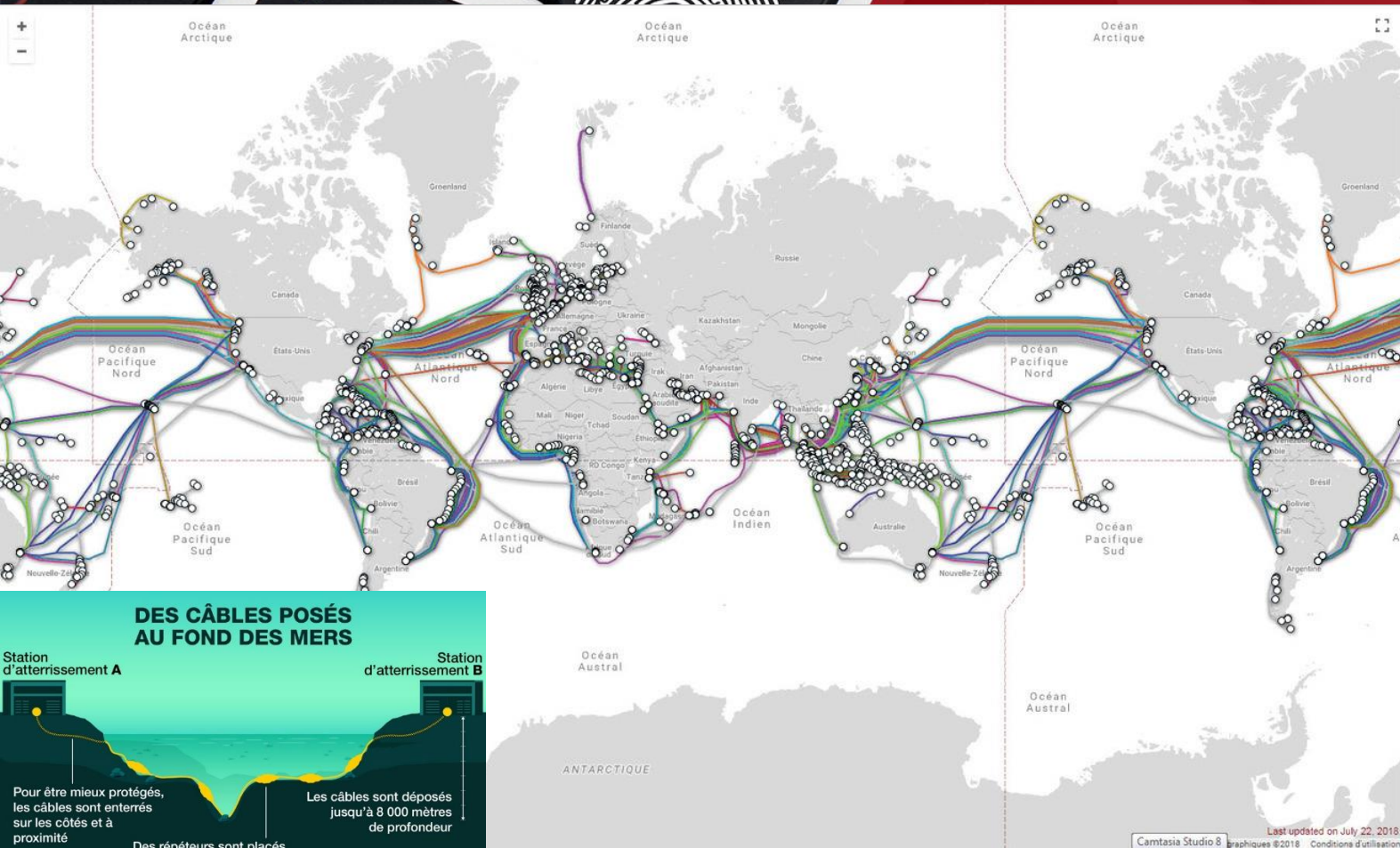
Un constat

- Une motivation principale : l'argent
(1 280 milliards de \$ générés / an)
- Un levier majeur : la mise en confiance

Un constat



➤ Confiance dans les réseaux utilisés (infrastructure)



TeleGeography Submarine Cable Map

The Submarine Cable Map is a free and regularly updated resource from TeleGeography.

Got a question about how we make this map? Or about how submarine cables work? Look no further.



Sponsored in part by Huawei Marine

Feedback [Twitter](#) [Facebook](#) [GitHub](#)

Search

Submarine Cables

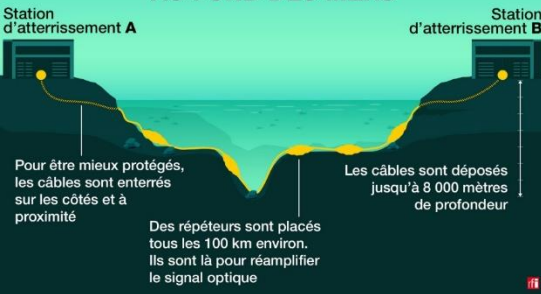
- ACS Alaska-Oregon Network (AKORN)
- Aden-Djibouti
- Adria-1
- AEC-1
- Africa Coast to Europe (ACE)
- Africa-1
- Alaska United East
- Alaska United Southeast
- Alaska United Turnagain Arm (AUTA)
- Alaska United West
- ALBA-1
- Aletar
- Alonso de Ojeda
- ALPAL-2
- America Movil Submarine Cable System-1 (AMX-1)
- American Samoa-Hawaii (ASH)
- Americas-I North
- Americas-II
- Amerigo Vespucci
- Antillas 1
- APCN-2
- Aphrodite 2
- Apollo
- Aqualink
- ARBR
- ARCOS
- ARSAT Submarine Fiber Optic Cable
- Asia Africa Europe-1 (AAE-1)
- Asia Pacific Gateway (APG)
- Asia Submarine-cable Express (ASE)/Cahaya Malaysia
- Asia-America Gateway (AAG) Cable System
- Atisa

Last updated on July 22, 2018

Camtasia Studio 8 Graphics ©2018 Conditions d'utilisation

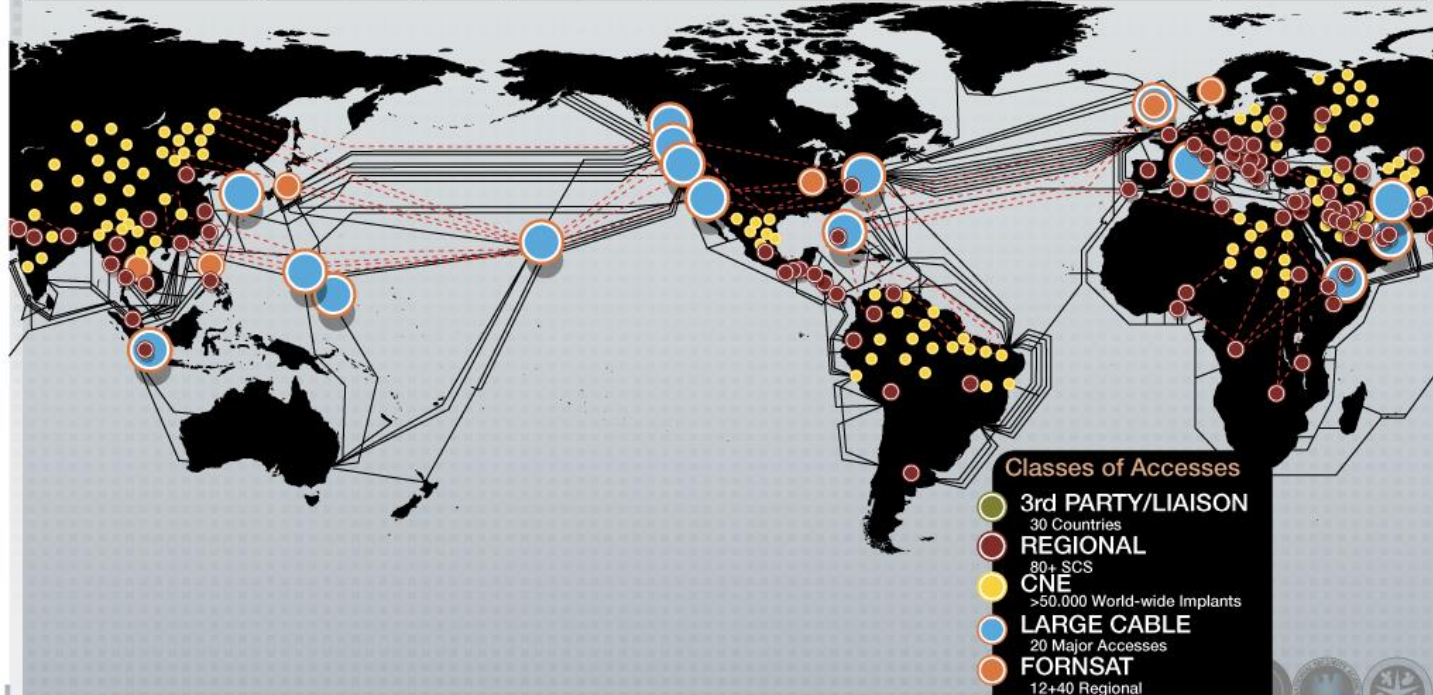
All content © 2018 PriMetrica, Inc.

DES CÂBLES POSÉS AU FOND DES MERS



<https://www.submarinecablemap.com>

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform





Incendie OVHCloud (Strasbourg) : 9-10 mars 2021
→ 3,6 millions de sites impactés





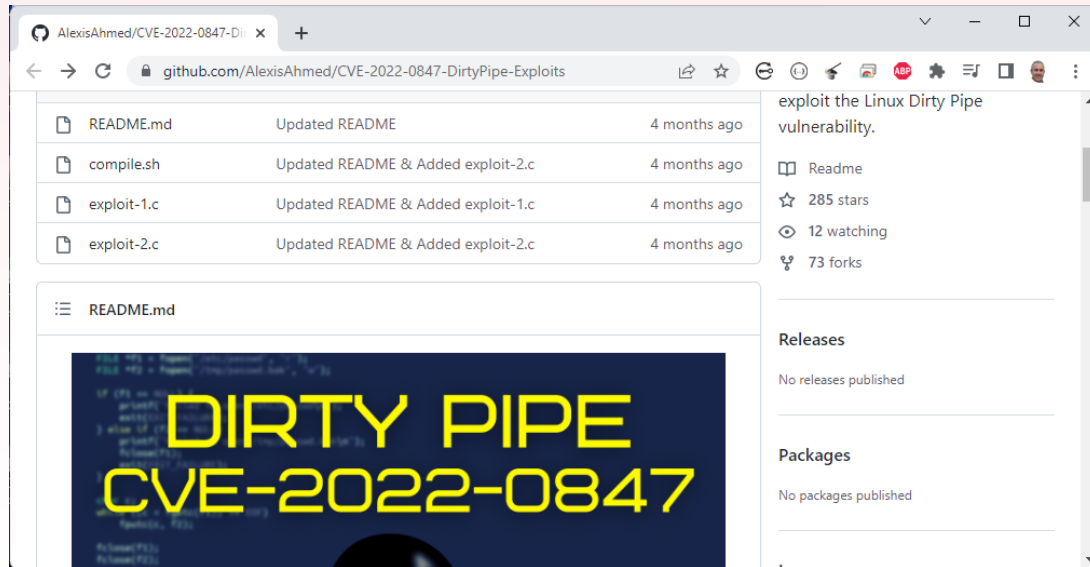
Un constat

- ↗ Confiance dans les réseaux utilisés (infrastructure)
- ↗ Confiance dans les machines (PC, smartphones, ...)

Types of malware



- Des « exploits » liés à la qualité du code (CVE – Common Vulnerabilities and Exposures)





Un constat

- ↗ Confiance dans les réseaux utilisés (infrastructure)
- ↗ Confiance dans les machines (PC, smartphones, ...)
- ↗ Confiance dans les personnes derrière les machines

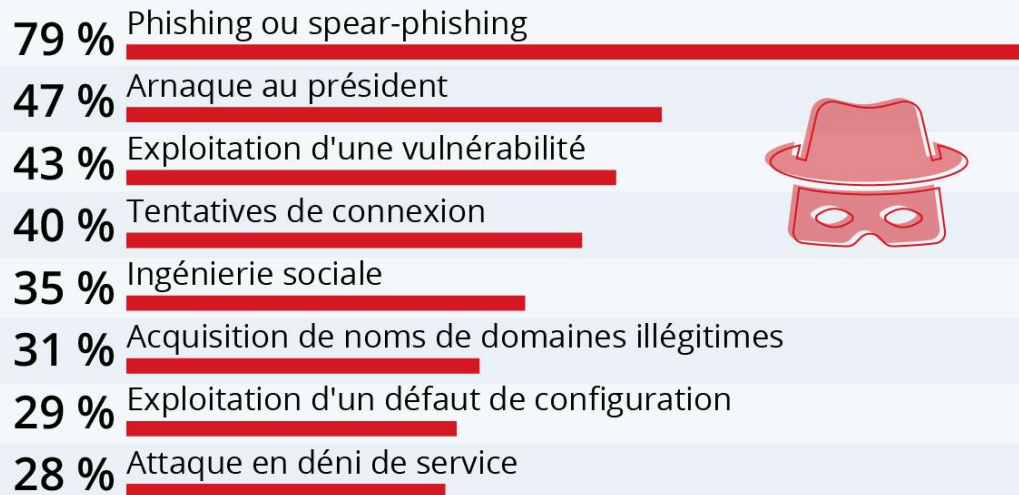


"On the Internet, nobody knows you're a dog."

Peter Steiner, New Yorker, 05/07/1993

Les cyberattaques les plus courantes contre les entreprises

Types d'attaques les plus constatés par les entreprises françaises en 2019 *

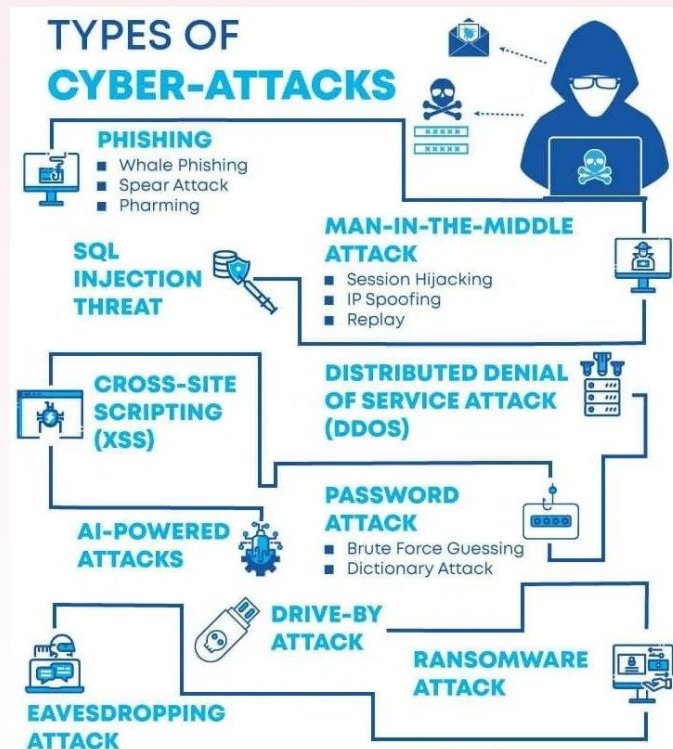


* Plusieurs réponses possibles, sélection des résultats supérieurs à 20 %.
En moyenne : 3,9 types d'attaques constatés parmi les entreprises ayant subi au moins une attaque.

Sources : CESIN, OpinionWay



Un constat





En résumé ...

- Comment se protéger en tant qu'individu ou professionnel ?
- Souvent, grâce au « GBS » !
- Et en respectant quelques règles ...

En résumé ...

- Menace 1 : on parle beaucoup ... trop !

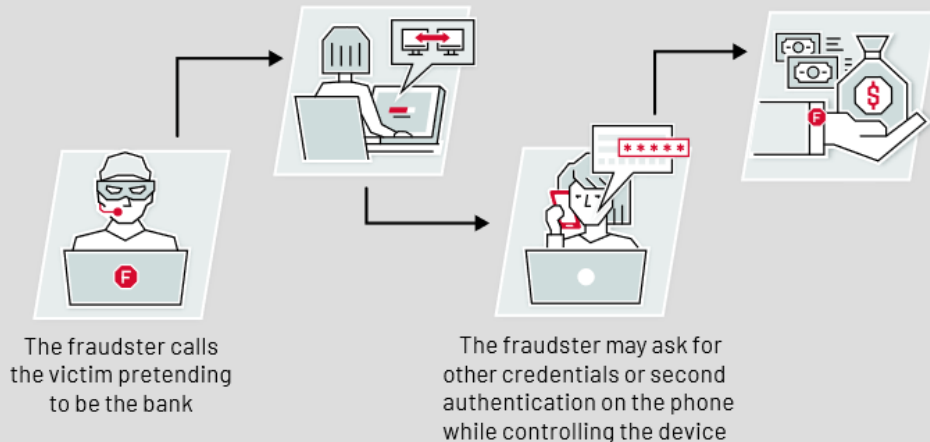


{turnoff.us}

SOPHISTICATED (RAT) VISHING

The fraudster instructs the victim to install a remote desktop application (e.g. TeamViewer)

The fraudster controls victim's computer to steal the money



mots de passe



Login: admin
Password: admin



NOMBRE DE CARACTÈRES	UNIQUEMENT DES CHIFFRES	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES + CARACTÈRES SPÉCIAUX
4	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT
6	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	1 sec	5 sec
8	IMMÉDIATEMENT	5 sec	22 min	1 heure	9 heures
10	IMMÉDIATEMENT	58 min	1 mois	7 mois	5 ans
12	45 sec	3 semaines	300 ans	2000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d'années	200 millions d'années

*source : SCSP Community (Seasoned Cyber Security Professionals)

- Menace 2 : on clique beaucoup (trop) ...

Rançongiciel une prise d'otage informatique

1 Envoi d'e-mails infectés

Exploitant une faille du système informatique, des pirates envoient des millions d'e-mails avec, en pièce jointe, un virus de type rançongiciel.

2 Contamination de l'ordinateur

L'internaute visé ouvre le fichier infecté qu'il a reçu en pièce jointe sans se douter de sa dangerosité.



3 Cryptage des fichiers

Le logiciel malveillant chiffre tous les fichiers (disques durs externes, clés USB...) pour les rendre inutilisables.

4 Demande de rançon

Un message apparaît sur l'écran avec une demande de rançon.



5 Paiement de la rançon

Si l'utilisateur accepte le chantage, il paie en bitcoin, une monnaie virtuelle et anonyme, et peut espérer récupérer ses fichiers.



5 Refus du paiement

Si l'utilisateur ne paie pas, ses données restent inutilisables. Il peut toutefois réinitialiser son ordinateur au prix de la perte de toutes ses données.





SMiShing



+33 6 14 57 48 50

Bonjour Philippe, votre commande a ete livree le 13.10.2021 au point de collection. Voir la ou vous pouvez prendre vos colis: ytov.me/9YqnI2



+33 7 44 52 26 06

Votre solde C.P.F. a ete mis a jour !
Consultez votre solde et reclamez votre formation integrelement finanee.
--> <https://cutt.ly/ZRyl89R>
NoPub=stop



+33 6 01 35 08 93

Ameli : Votre nouvelle carte vitale est disponible. Veuillez suivre les indications ci-dessous pour confirmer l'expédition : <https://fr-macartevitale.com/>

Phishing

Fichier Edition Affichage Aller à Messages Événements et tâches Outils Aide

Courrier entrant - Philippe.Truillet [MESSAGE MARQUE SPAM : X]

Relever Écrire Messagerie instantanée Adresses Étiquette Filtre rapide Rechercher <Ctrl+K> Config

De Cdiscount <anniversaire@cdiscout.com> ☆

Sujet [MESSAGE MARQUE SPAM : MOYEN] Félicitations ! Vous avez été choisi pour gagner un smartphone . 06:39

Pour philippe.truillet@irit.fr ☆

cdiscout

Félicitations !

Aujourd'hui, **28-10-2021**, nous célébrons donc le 22e anniversaire de notre activité en ligne, Cette journée auelles on sélectionne 1000 clients pour recevoir des cadeaux. Félicitations vous faites partie des personnes sélectionnées pour recevoir un cadeau de notre part

Cela ne vous prendra qu'une minute et vous pourrez choisir n'importe quel cadeau parmi nos **Articles** disponible En stock cadeaux !

[Dépêchez-vous, le nombre d'offres gratuites en stock disponibles est limité !](#)

Il reste une quantité d'articles limite en stocks.

Veuillez ajouter votre choix au panier et valider votre adresse de livraison afin de recevoir votre cadeau sous 2 à 3 jours ouvrés.

Merci pour votre confiance.

Invitations : 3 Panneau « Aujourd'hui »

https://cdiscout-deal.com/web

Phishing

Shop - Cdiscount

cdiscout-deal.com/web/

Cdiscount Qu'est-ce qui vous ferait plaisir ? Cdiscount à volonté

Tous nos rayons

Voyages Mes Courses Forfait Mobile Electricité Occasion Voitures

Electroménager Lavage - séchage Froid Cuisson Café - Robot & Appareil de cuisson Art Culinaire & Art de la Table Entretien de la maison et du linge Beauté - Hygiène & Santé

Accueil > Offres Gratuites (3)

CATEGORIES

< Offres Gratuites

Aspirateur balai (33)

AFFINER PAR

Livraison express gratuite avec Cdiscount à volonté

Choix de livraison

Expédié par cdiscount

Livraison express

Livraison gratuite

Marque

Dreame (2)

Dyson (12)

Koticidin (1)

Proscenic (4)

Vbestlife (2)

+ de choix

Pays de Livraison

Allemagne (13)

Félicitations !

Aujourd'hui, **28-10-2021**, nous célébrons donc le 22e anniversaire de notre activité en ligne. Cette journée auxquelles on sélectionne 1000 clients pour recevoir des cadeaux. Félicitations vous faites partie des personnes sélectionnées pour recevoir un cadeau de notre part.

Cela ne vous prendra qu'une minute et vous pourrez choisir n'importe quel cadeau parmi nos **Articles** disponible En stock cadeaux !

Dépêchez-vous, le nombre d'offres gratuites en stock disponibles est limité !

Il reste une quantité d'articles limite en stocks, afin de bénéficier d'une offre et payer votre livraison (Moins de 2 EUR).

Veuillez ajouter votre choix au panier et valider votre adresse de livraison afin de recevoir votre cadeau sous 2 à 3 jours ouvrés.

Trier par Offres Gratuites Meilleures ventes Prix Avis client

Top offres

SAMSUNG Galaxy S20 FE - 128 Go

★★★★★ (82)

En stock ! Moins de offres gratuites !

Produit Cdiscount à volonté

Taille de la diagonale : 6.5

Vendu et expédié par Cdiscount

949€00

Offre gratuite

dont 2,00 € frais de livraison

Ajouter au panier

Livraison gratuite(1)

Cdiscount : Meuble, Déco, High ?

cdiscout.com

Cdiscount Qu'est-ce qui vous ferait plaisir ? Cdiscount à volonté

Tous nos rayons

Voyages Mes Courses Forfait Mobile Spectacles Occasion Mutuelle

Promotions et Actualités Jouets Jeux Vidéo Sport Electroménager Meuble Déco Literie Bricolage Informatique TV Son Photo Téléphonie Reconditionné et Seconde main Jardin Animalerie Beauté Mode Bijoux Bébé Auto Moto La Cave

ALORS ON JOUE ?

DES OFFRES POUR LES PETITS ET LES GRANDS ENFANTS

jusqu'à **60%** d'économie

Nos stars de Noël

Univers **playmobil**

Univers **Lego**

L'OFFRE DU JOUR !

SAMSUNG

VENTE FLASH

72H seulement

Phishing



MINISTÈRE DE LA JUSTICE ET GARDE DES SCAUX
TRIBUNAL DE PREMIÈRE INSTANCE DE RENNES
7 RUE PIERRE ABELARD CS 73127 35031 Rennes



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

AVIS D'INCULPATION

A votre attention :

Je suis le Lieutenant Sébastien Possemé Commandant de la brigade numérique de la gendarmerie de Rennes, Chef de la brigade de Protection des Mineurs (BPM) et de la lutte contre les violences conjugales.

Je vous contacte après une saisie informatique de cyber-infiltration (autorisée, notamment en matière de pédopornographie, pédophilie, Cyber pornographie, exhibitionnisme, trafic sexuel) pour vous informer que vous faites l'objet de plusieurs poursuites judiciaires en vigueur :

- Pédopornographie
- Pédophilie
- Exhibitionnisme
- Cyber pornographie
- Trafic sexuel

Pour votre information, La loi n° 2016-297 du 14 mars 2016 aggrave les peines lorsque compromis et harcèlements sexuels ou viols ont pu être commis via internet.

Vous avez commis ces infractions après avoir été ciblé sur internet (sites d'annonces, sites à caractères pornographiques, sites de rencontres...), puis pendant certaines conversations avec des mineurs.

Nous disposons de plusieurs éléments qui ont été enregistrés par notre cyber-gendarmerie et constituent les preuves de vos infractions.

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications afin qu'elles soient mises en examen et vérifiées pour évaluer les sanctions ; ceci dans un délai strict de 48 heures.

Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport à M. François Molins, procureur au tribunal de grande instance de Paris et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre. Ensuite ce mandat sera transmis à la gendarmerie la plus proche de votre lieu de résidence pour votre arrestation et vous fichier comme délinquant sexuel.

Votre dossier sera également transmis aux médias pour une diffusion où votre famille, vos proches et toute la France entière verront ce que vous faites devant votre ordinateur.

Maintenant vous êtes prévenu.
Cordialement.

Lieutenant Sébastien Possemé Commandant de la brigade numérique de la gendarmerie de Rennes, Chef de la brigade de Protection des Mineurs (BPM) et de la lutte contre les violences conjugales.

Brigade numérique de la gendarmerie nationale -magendarmerie
Adresse : 85 boulevard Clémenceau, 35000 Rennes, France

Lieutenant Sébastien Possemé Commandant

De POST-FEDPOL <juandres_9@usal.es>

Pour undisclosed-recipients;

Réponse à direction.fedpolsuisse.ch@gmail.com

Sujet Citation à Comparaitre.

Bonjour,
(Ci-joint, les détails).
Cordialement

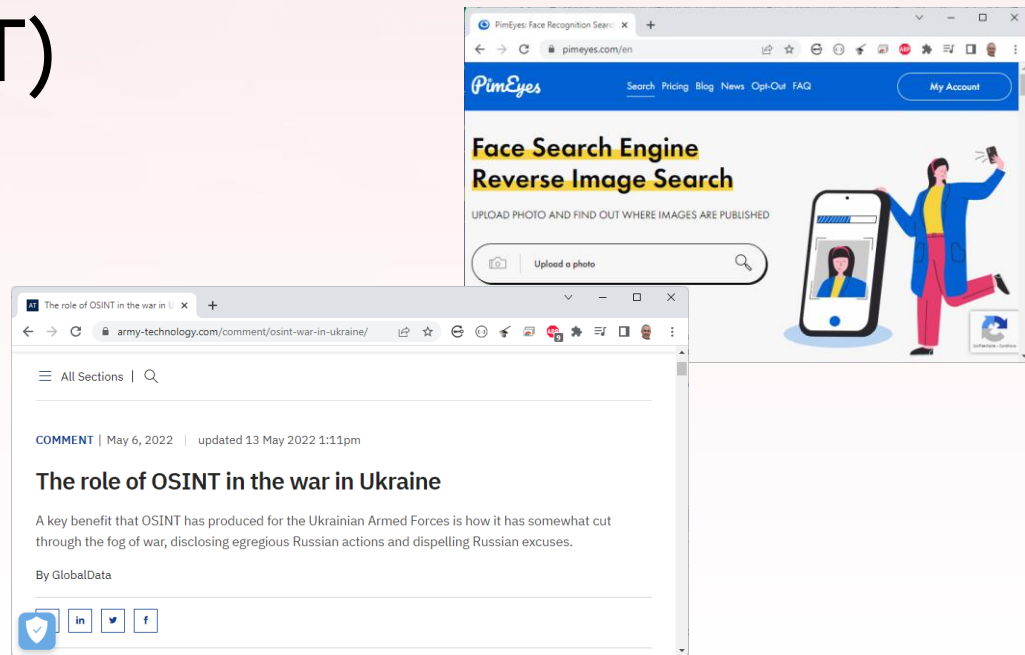
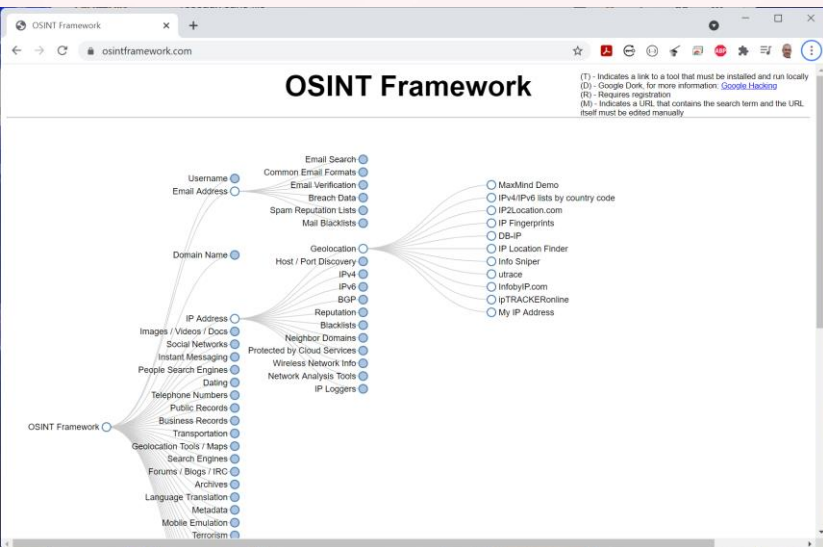
—Arrestation n° 2133611.jpg—



✓ 1 pièce jointe : Arrestation n° 2133611.jpg 550 Ko

En résumé ...

- Menace 3 : on laisse beaucoup (trop) de traces (→ OSINT)




- Données EXIF (géoloc)
- QR-Code
- Réseaux sociaux,
- ...

verexif.com/fr/ver.php

EXIF DONNÉES


Fabricant de la caméra : Xiaomi
Modèle de caméra : Redmi Note 7
Date et heure : 2021/04/03 17:14:11
Résolution : 4000 x 2250
Il a utilisé Flash : No
Distance focale : 4.7mm
Temps d'exposition : 0.0003 s (1/2904)
Ouverture : f/1.8
ISO equiv. : 250
Balance des blancs : Auto
Mode de mesure : center weight
Latitude GPS : N 43° 27' 11.4084"
Longitude GPS : E 1° 12' 54.1007"
Altitude GPS : 254.11m
JPEG Quality : 78



[Retirer Exif](#) [Une autre photo](#)

LIEU OÙ LA PHOTO A ÉTÉ PRISE

43°27'11.4"N 1°12'54.1"E
377 Rte de Saint-Clar, 31600 Lherm
[Agrandir le plan](#)



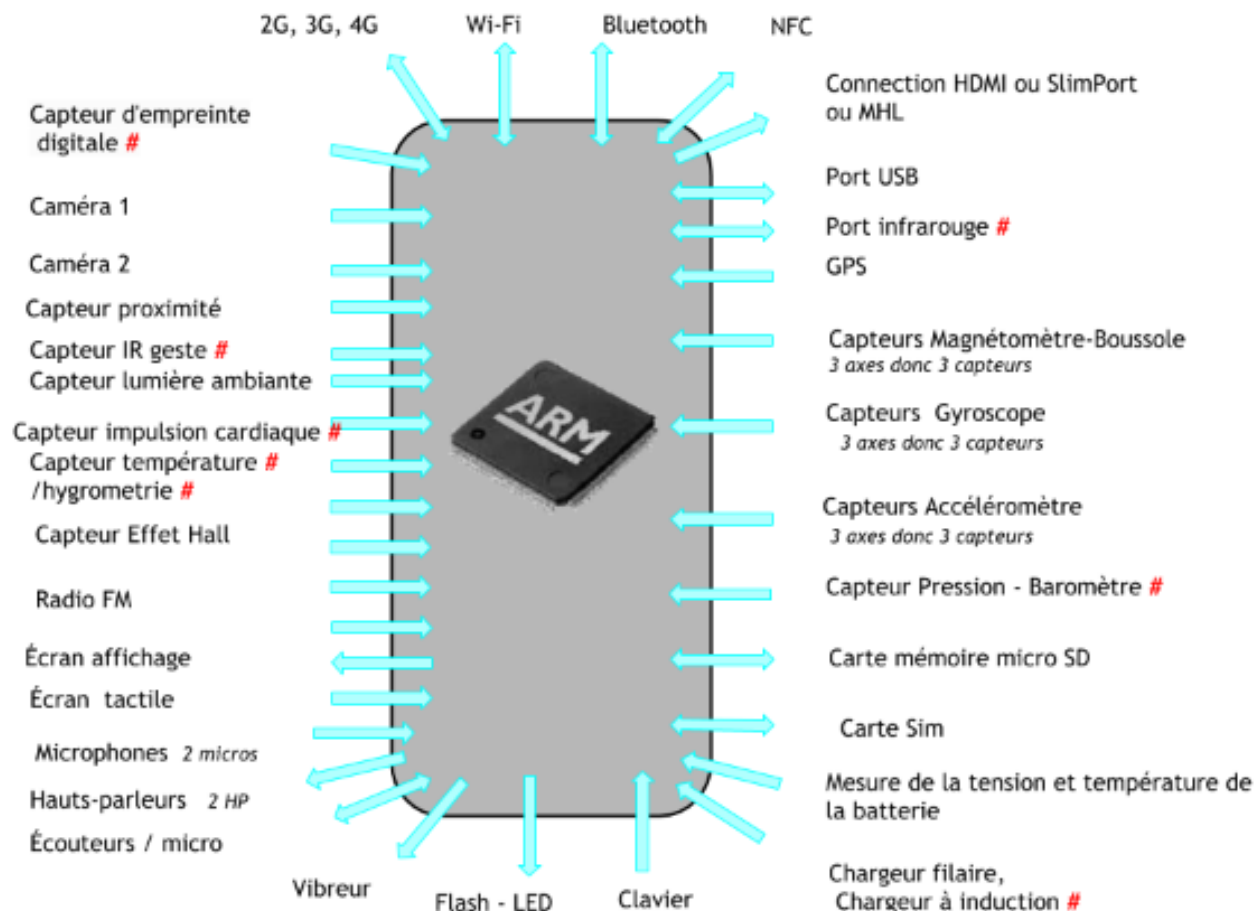
61 [Recommander](#)

En résumé ...

- Menace 4 : notre « double » numérique ... Le smartphone !
 - Il contient vie privée et vie publique
 - Bourré de capteurs
 - Facile à pirater (spyware)



Un SmartPhone = Un SuperOrdinateur

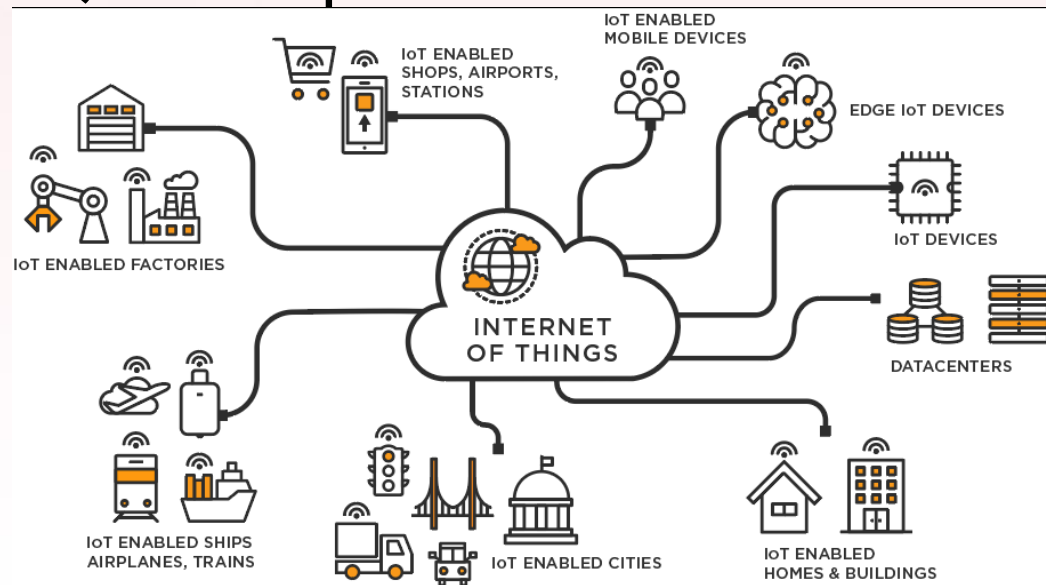


Les composants du Smartphone

= dans smartphone ou tablette haut de gamme

En résumé ...

- Et au delà ... Menace 5 : l'IoT
 - des milliards (25 ?) de capteurs disséminés
 - des problèmes de sécurité



STRAVA

Mobile

Fonctionnalités

Inscription

Blog

S'inscrire

Se connecter

Carte mondiale des activités

Couleur de la carte des activités

Vif

Bleu

Purple

Gris

Rouge

Type d'activité

Tous



Opacité

0%

40%

60%

80%

100%

Couches

Carte

Étiquettes

Styles de carte

Sombre

Lumineuse

Standard

Chercher



En résumé ...

- Les techniques utilisées sont nombreuses
- Elles évoluent avec la technologie et les usages
- Un mot d'ordre : la vigilance





CNIL.

<https://www.cnil.fr/fr/securite-des-donnees>

→ 3 niveaux





La Brigade Numérique

Signaler un contenu illicite : <https://www.internet-signalement.gouv.fr/PharosS1>

Contactez la Gendarmerie : <https://magendarmerie.fr>



<https://www.cybermalveillance.gouv.fr>



ANSSI

Agence nationale de la sécurité
des systèmes d'information

<https://ssi.gouv.fr>

