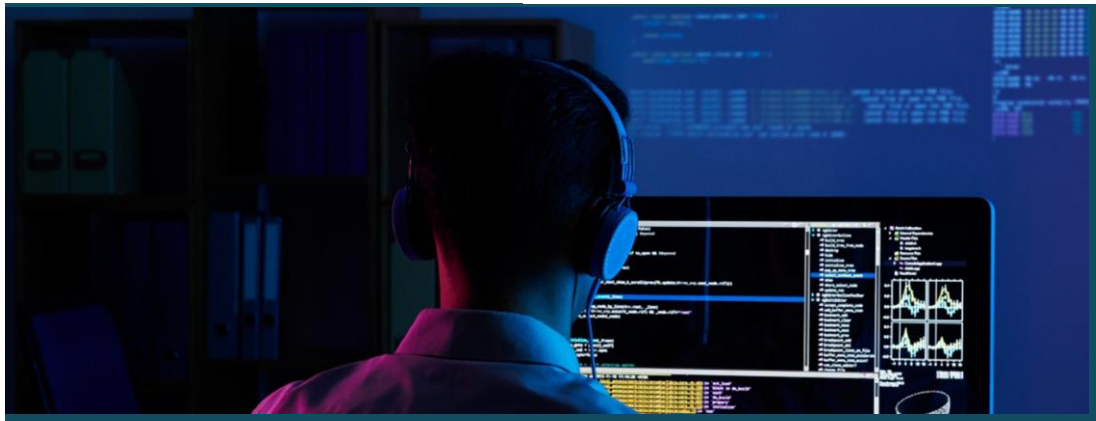
CONFÉDÉRATION DES PME

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

8 juillet 2021



WEBINAIRE

Cybersécurité : PME, quelles sont les menaces, comment s'en protéger

LA CPME EST LA PREMIÈRE ORGANISATION INTERPROFESSIONNELLE
À ÊTRE CERTIFIÉE ENGAGEMENT DE SERVICE QUALI'OP

ENGAGEMENT DE SERVICE
QUALI'OP
REF. 166
AFNOR CERTIFICATION
www.afnor.org

PROGRAMME

- ❑ La cybersécurité, protection indispensable pour une transition numérique réussie

Alain Assouline, Président de la Commission numérique, CPME

- ❑ Les principales menaces actuelles visant les PME ; le darkweb et la valeur des données des PME pour les hackers

Marc Bothorel, Référent cybersécurité, CPME

- ❑ Comment se protéger, vers qui se tourner pour se faire aider en cas d'attaque

Franck Gicquel, Responsable des partenariats, Cybermalveillance.gouv.fr,

- ❑ Questions/réponses

NB : Elles devront être rédigées dans l'onglet « questions »

cpme CONFÉDÉRATION DES PME

INTRODUCTION

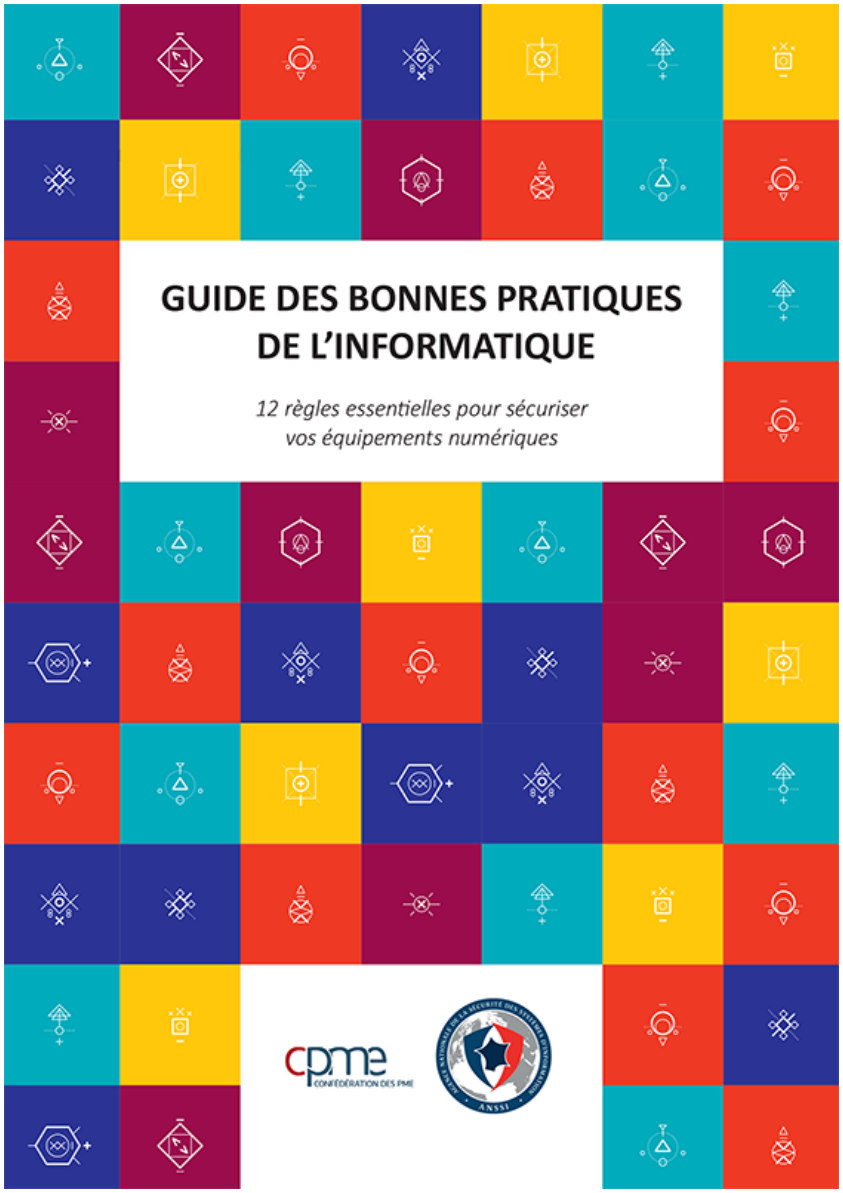
La cybersécurité, protection indispensable pour une transition numérique réussie

Alain Assouline

CPME,

Président de la Commission numérique

cpme CONFÉDÉRATION DES PME



MEMBRE DU DISPOSITIF
CYBERMALVEILLANCE.GOUV.FR

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

EN OCTOBRE J'AGIS POUR LE CYBER MOIS
#cybermois

https://www.cpme.fr/publications/guides/guide-des-bonnes-pratiques-de-linformatique

cpme CONFÉDÉRATION DES PME

Les principales menaces actuelles visant les PME ; le darkweb ; la valeur des données des PME pour les hackers

Marc Bothorel

CPME,

Référent cybersécurité

cpme CONFÉDÉRATION DES PME

QUELLE EST VOTRE CONNAISSANCE DU MONDE DE LA CYBERCRIMINALITÉ ?

1. Combien de nouveaux malwares sont générés chaque jour ?

350 000

2. Quelle proportion d'attaques de endpoints (PC/Mac) n'ont pas été interceptés par les antivirus ?

57%

3. Quelle proportion de TPE/PME a été victime d'une cyberattaque?

50%

4. Quelle proportion de brèches a exploité un mot de passe faible ou volé?

81%

5. Quelle proportion de sociétés a été victime d'une violation provenant initialement d'un endpoint (PC ou Mac)?

64%

TELETRAVAIL, COVID, CRISE ECONOMIQUE : UNE MANNE POUR LES CYBERCRIMINELS !

MMA Entrepreneurs d'Assurances — 10To de données volées

orange Business Services — 339Mo données
20 clients touchés

Twitter

SPIE

Rabot Dutilleul Construction — Rançon 8M Euros

GARMIN — 2 jours d'arrêt de prod,
sites web,apps mobiles, tél, messagerie HS

MPM MARSEILLE PROVENCE METROPOLE — 3 mois de remise en état

Carlson Wagonlit Travel — 30 000 PC H.S.
2To données volées

Canon

xerox

LG Life's Good

mom GROUP, GoGo SQUEEZ, Materne, Mont Blanc — Fermeture des serveurs
Arrêt des sites de production

Cadiou Industrie

« On croit toujours que l'on a un antivirus à toute épreuve. Pour ma part, je me croyais à l'abri mais aujourd'hui, les pirates sont plus organisés que les entreprises et les virus plus dangereux qu'on ne le croit »

Vecteurs d'attaque :

Grande sociétés ➔ ingénierie sociale, phishing
PME ➔ principalement les failles RDP/RDS, phishing

cpme CONFÉDÉRATION DES PME

QUELQUES AUTRES EXEMPLES PLUS RÉCENTS (AVRIL 2021)

In Extenso experts-comptables

Rançonné +15 jours sans accès dossiers client
Avril 2021

facebook

550 Millions de comptes piratés dont 20 millions de français(nom, prénom, adresse, tel mobile, compte mail etc.)
Avril 2021

500 millions de comptes piratés
en vente sur le DarkWeb
Avril 2021

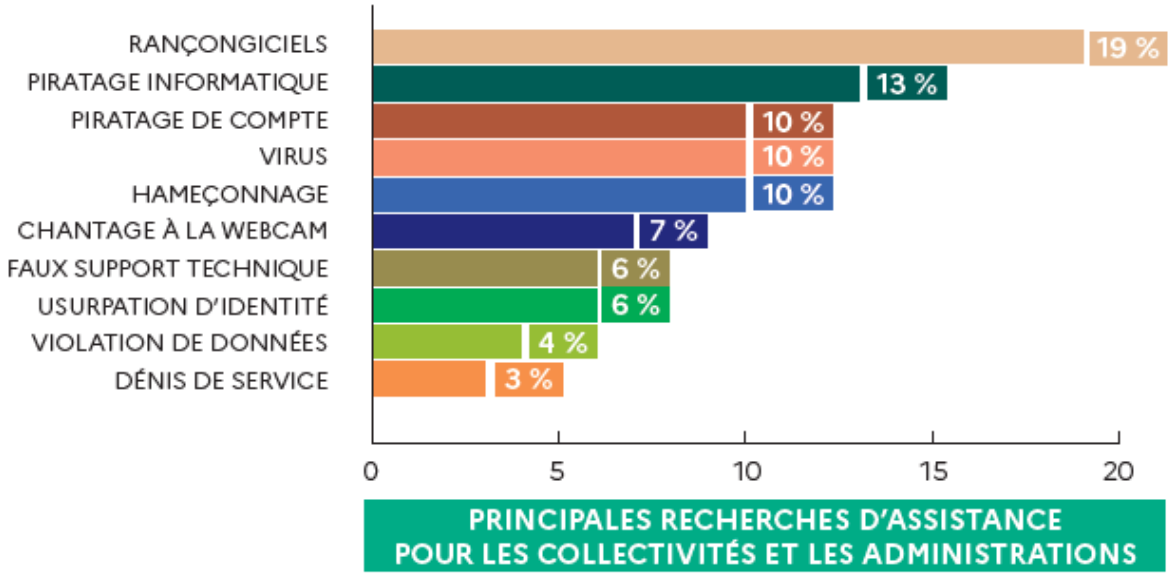
EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

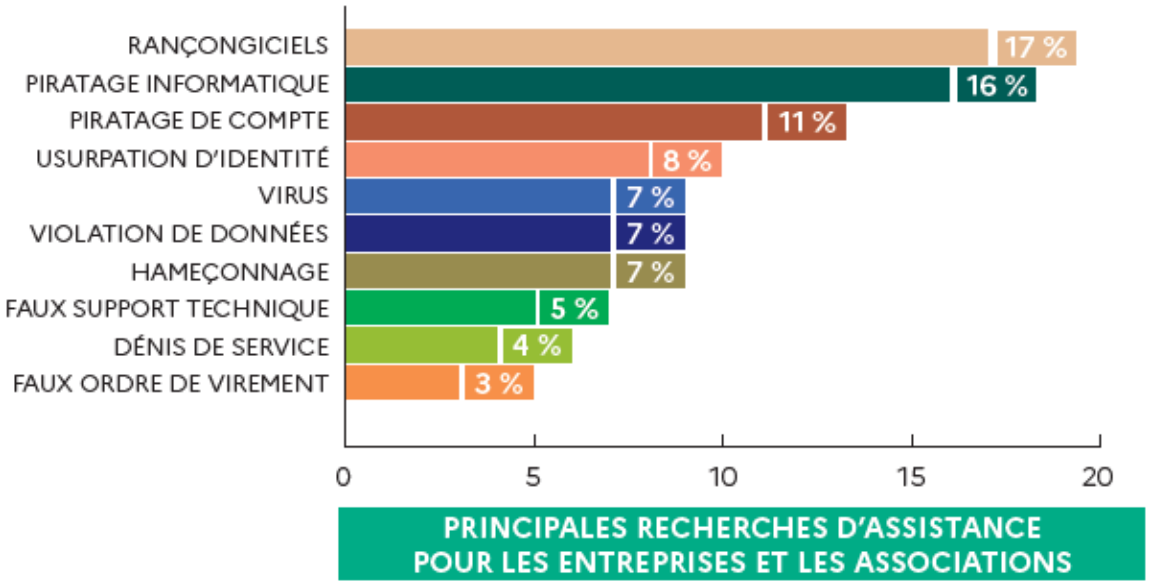
Vols de documents sur les vaccins AstraZeneca Pfizer et Bio Ntech.
Objectif : modifier les docs pour théorie du complot, vol des méthodes de commercialisation
Décembre 2020

CNED
AU SERVICE DE TOUTES LES RÉUSSITES

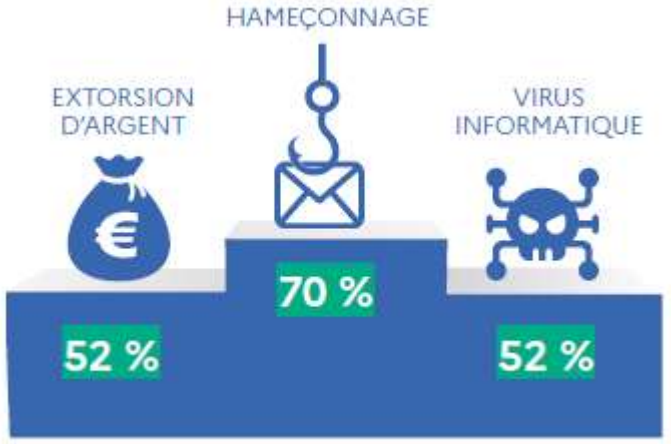
Serveurs bloqués par attaque DDoS Avril 2021

QUELS SONT LES PRINCIPAUX ACTES DE CYBERMALVEILLANCE EN 2020 EN FRANCE[1]?



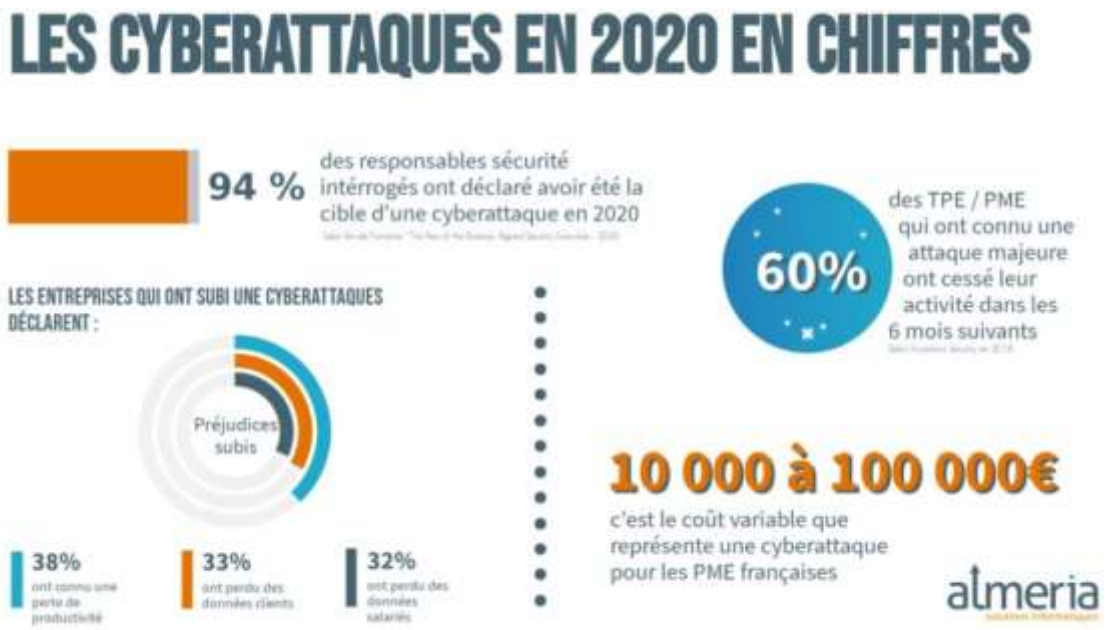


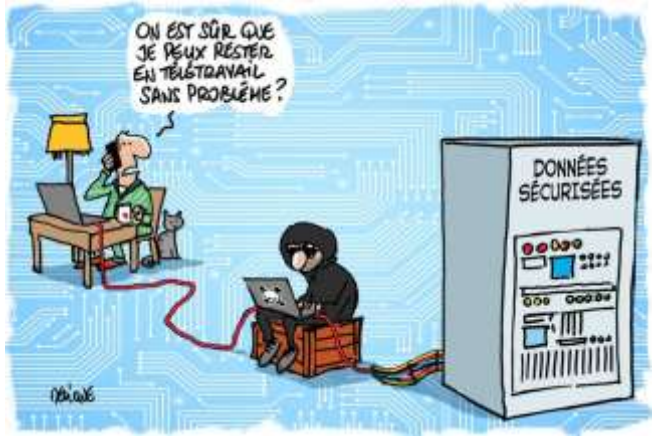
3 actes de cybermalveillance le plus souvent rencontrés en 2020 en France



*Rapport cybermalveillance.gouv.fr 2020

QUELQUES CHIFFRES SUR L'ACTIVITÉ CYBERCRIMINELLE EN 2020 (FRANCE)





INCIDENTS CYBER EN 2019/2020 ET PROJECTIONS 2025

CYBERCRIMINALITÉ EN FRANCE

En 2018, 80% des entreprises ont constaté un incident de cybercriminalité
En 2019, 90 % des entreprises ont constaté un incident de cybercriminalité en France, 43 % étant des PME
En 2020, Ce taux a été multiplié par 4
Le télétravail est devenu la source de **20%** des incidents de cybercriminalité

COÛT DE LA CYBERCRIMINALITÉ

2017 : 600 milliards de dollars

2018 : coût moyen par entreprise a été de 8,6 millions d'euros pour les entreprises françaises.

2021 :6000 milliards de dollars (190.000 dollars à la seconde) avec pourtant des coûts de mise en œuvre faibles (5 dollars en moyenne pour acheter un virus ou équivalent sur le darknet)

2025 : prévisionnel à 10500 milliards de dollars ce qui, si on devait mesurer le poids du risque cyber en en faisant un pays, le positionnerait en troisième économie mondiale derrière les Etats-Unis et la Chine

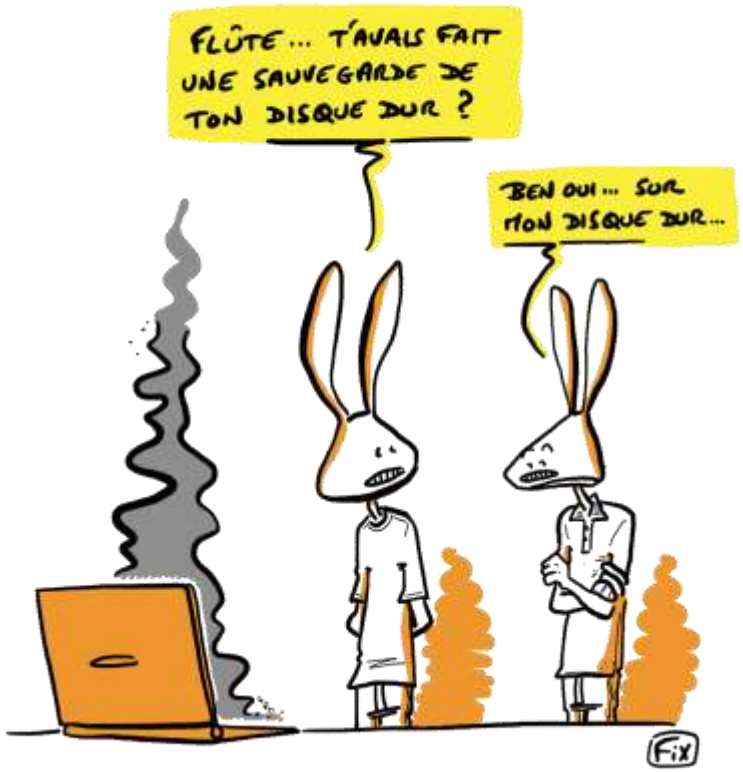
LES IMPACTS SUR NOS ENTREPRISES

Après annonce d'un cyber incident[1]:

- Risque de défaillance augmenté de **80%** dans les 3 mois
- Perte de **8 à 10%** de la valorisation de l'entreprise
- Dommage à la réputation "l'actif immatériel le plus précieux dont dispose l'entreprise »

OR..

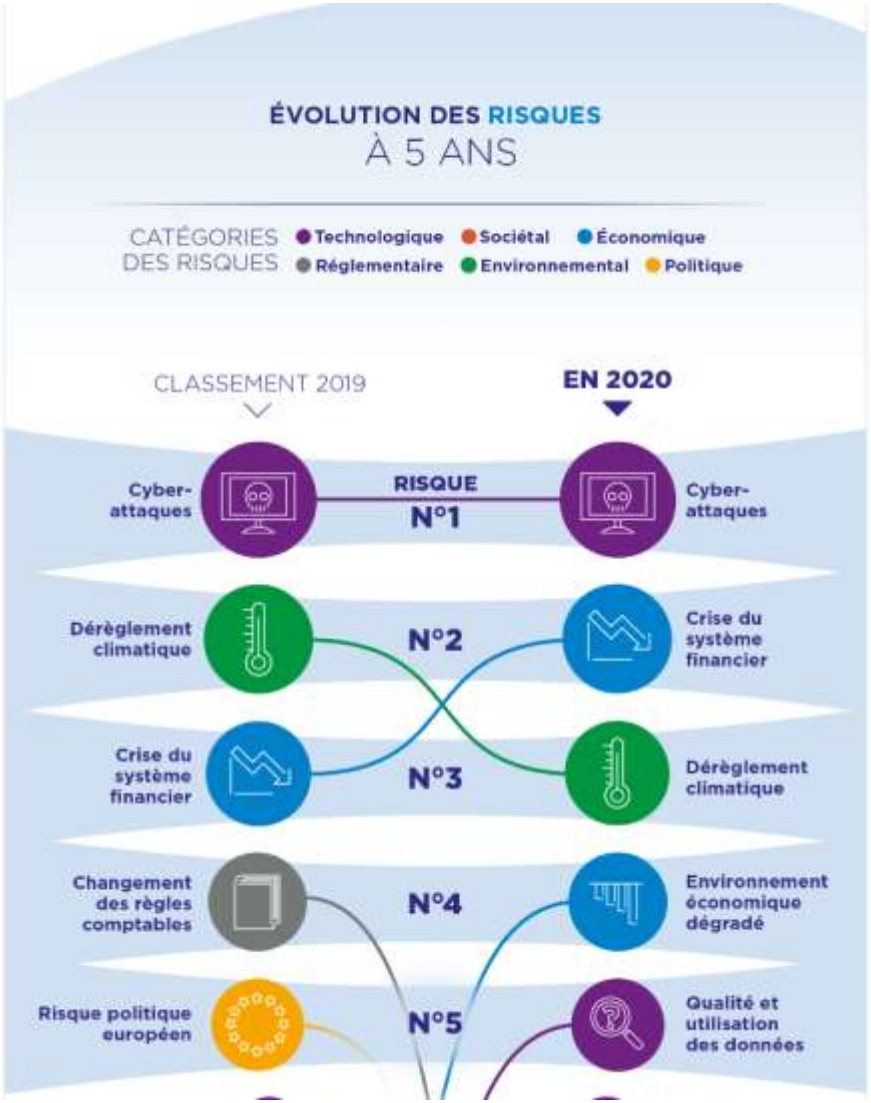
- **80%** des entreprises françaises n'ont pas de plan de réponse aux incidents robustes[2]
- **86%** des entreprises françaises n'ont pas souscrit à une cyberassurance[3]



[1]: source Etude cabinet Bessé [2]: Source IBM Ponemon [3]: Source CLUSIF

FFA: BAROMÈTRE 2020 DES RISQUES ÉMERGENTS À 5 ANS

En 2019 et 2020, le risque cyber est LE risque numéro 1



QUELQUES CARTES INTERACTIVES EN TEMPS RÉEL DES CYBERMENACES….

https://threatmap.checkpoint.com/

https://cybermap.kaspersky.com/stats

https://threatmap.bitdefender.com/

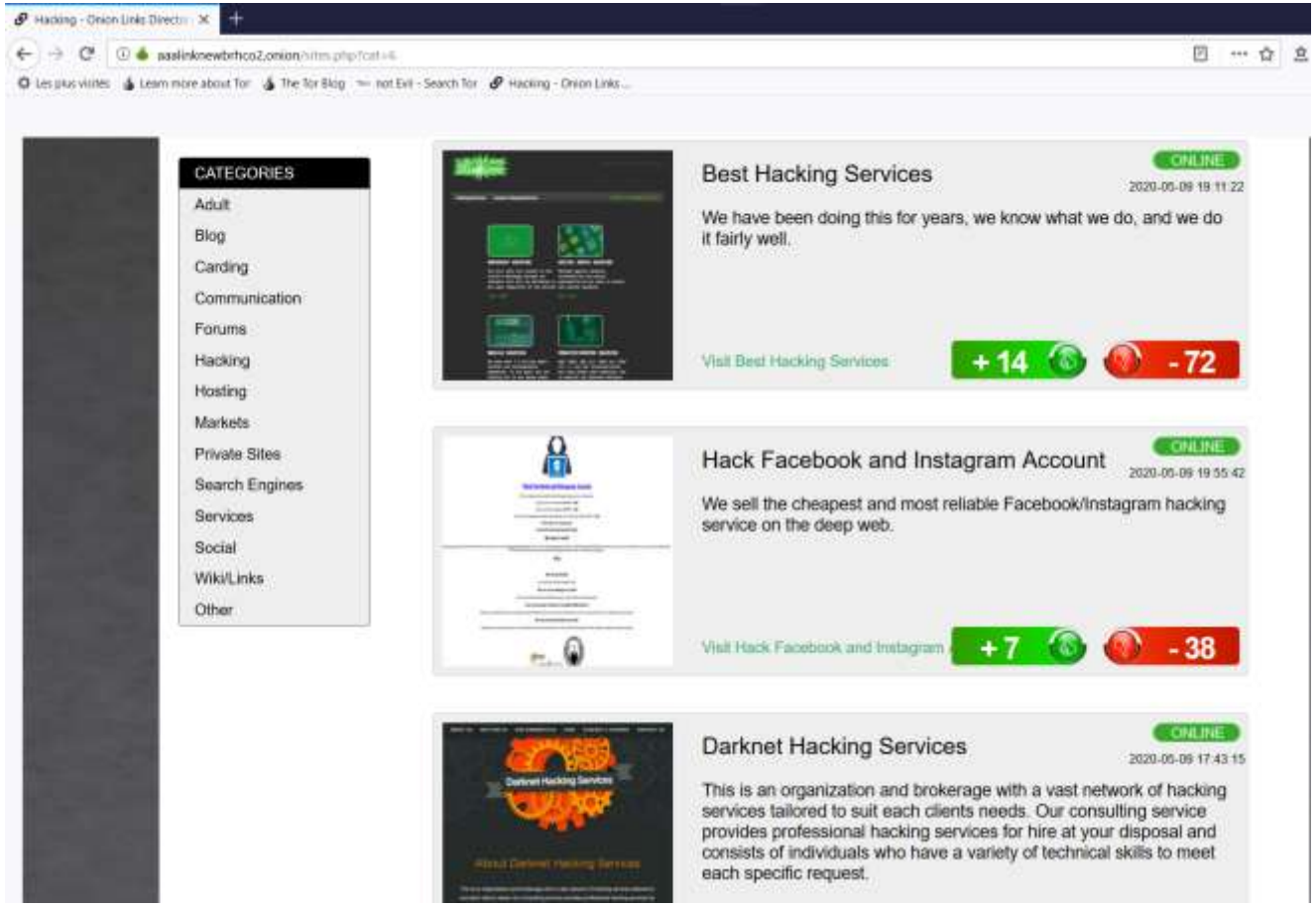
https://www.digitalattackmap.com/

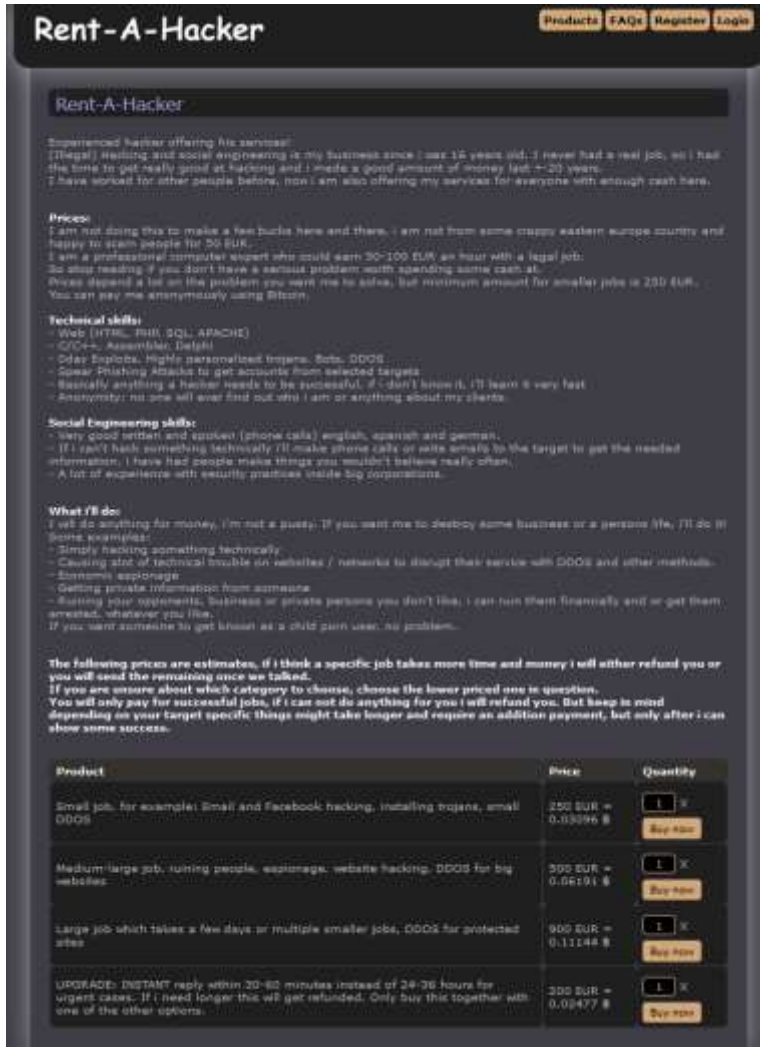
WEB – DEEPWEB - DARKWEB ???

le deepweb est plus de **500 fois plus gros** que le web indexable

- Le ***deepweb***, ou « web profond », parfois même « web invisible », est souvent défini comme le web accessible mais non indexé par les moteurs de recherche
- Le ***dark web*** désigne le contenu du **World Wide Web** se trouvant sur les **darknets**
- On appelle ***darknet*** les réseaux overlays, à l'origine isolés du réseau public. accessible qu'à l'aide d'outils spécifiques. Les plus connus sont Tor, i2p et Freenet.

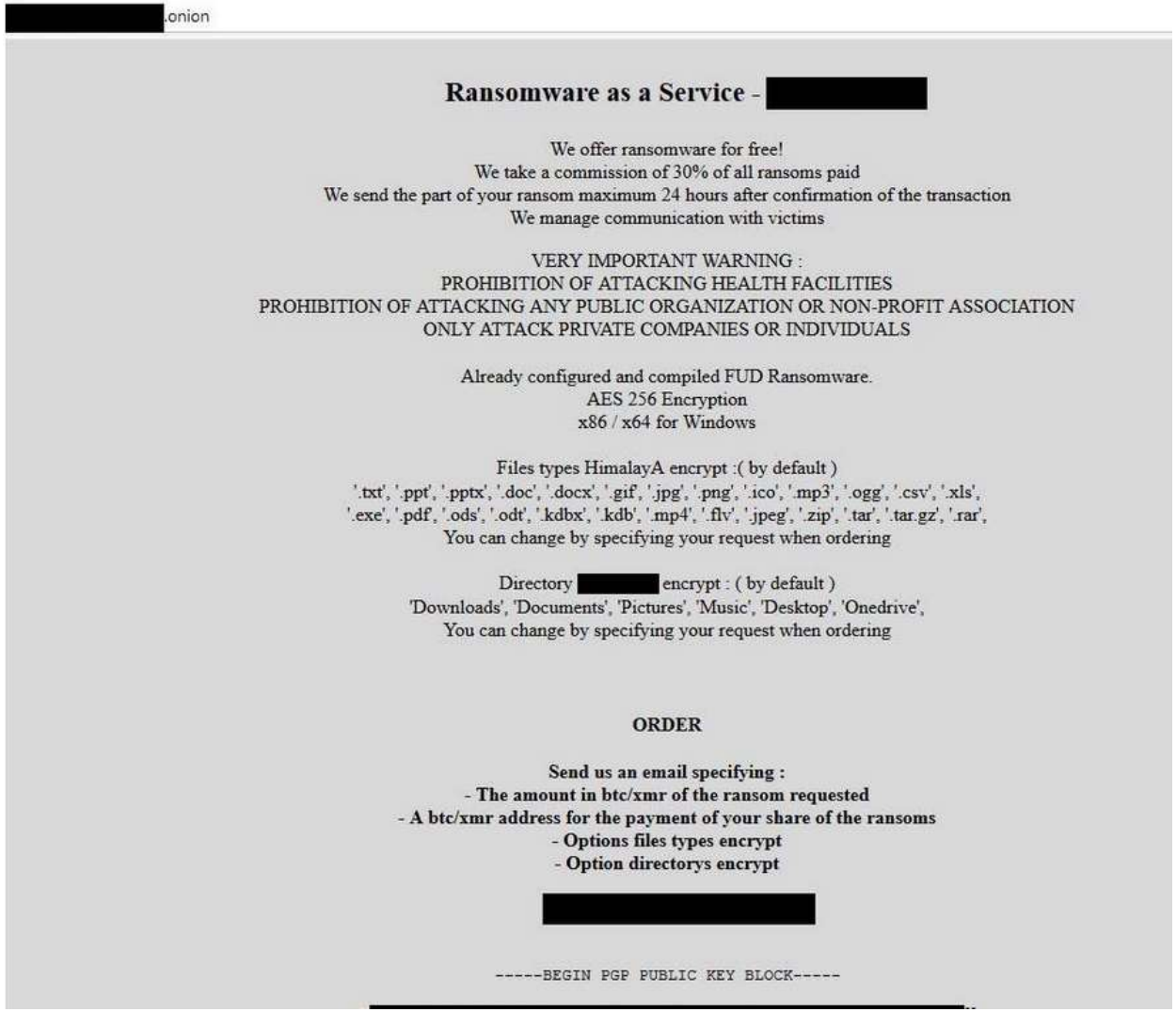
LE HACKING, UN **VRAI** BUSINESS, UNE ECONOMIE PARALLELE





$2000 MILLIARDS DE REVENUS EN 2019[1].

Le Ransomware : un VRAI business !!


[redacted].onion

Ransomware as a Service - [redacted]

We offer ransomware for free!
We take a commission of 30% of all ransoms paid
We send the part of your ransom maximum 24 hours after confirmation of the transaction
We manage communication with victims

VERY IMPORTANT WARNING :
PROHIBITION OF ATTACKING HEALTH FACILITIES
PROHIBITION OF ATTACKING ANY PUBLIC ORGANIZATION OR NON-PROFIT ASSOCIATION
ONLY ATTACK PRIVATE COMPANIES OR INDIVIDUALS

Already configured and compiled FUD Ransomware.
AES 256 Encryption
x86 / x64 for Windows

Files types HimalayA encrypt :(by default)
'.txt', '.ppt', '.pptx', '.doc', '.docx', '.gif', '.jpg', '.png', '.ico', '.mp3', '.ogg', '.csv', '.xls',
'.exe', '.pdf', '.ods', '.odt', '.kdbx', '.kdb', '.mp4', '.flv', '.jpeg', '.zip', '.tar', '.tar.gz', '.rar',
You can change by specifying your request when ordering

Directory [redacted] encrypt : (by default)
'Downloads', 'Documents', 'Pictures', 'Music', 'Desktop', 'Onedrive',
You can change by specifying your request when ordering

ORDER

Send us an email specifying :
- The amount in btc/xmr of the ransom requested
- A btc/xmr address for the payment of your share of the ransoms
- Options files types encrypt
- Option directorys encrypt

[redacted]

-----BEGIN PGP PUBLIC KEY BLOCK-----

[redacted]

PRIX MOYENS DE VOS DONNÉES SUR LE DARK WEB

Cartes de crédit clonées et données associées

Produit	Prix moyen sur le dark web
Carte Mastercard clonée avec code PIN	15 $
Clonage dune carte American Express avec un code PIN	35 $
Carte VISA clonée avec code PIN	25 $
Détails de la carte de crédit, solde du compte jusqu'à 1000 $	12 $
Détails de la carte de crédit, solde du compte jusqu'à 5000 $	20 $
Les identifiants bancaires de compte en ligne volés, minimum 100 $ sur le compte	35 $
Identifiants bancaires de compte en ligne volés, minimum 2000 $ sur le compte	65 $
Compte Walmart avec une carte de crédit	10 $

Documents falsifiés

Produit	Prix moyen sur le dark web
Permis de conduire américain, qualité moyenne	70 $
Permis de conduire américain, haute qualité	550 $
Carte d'assurance automobile	70 $
Carte de membre du service routier d'urgence AAA	70 $
Relevé bancaire de Wells Fargo	25 $
Relevé bancaire de Wells Fargo avec des transactions de	80 $
Carte d'étudiant de l'université de Rutgers	70 $
Passeport américain, canadien ou européen	1500 $
Carte d'identité nationale européenne	550 $

Les médias sociaux

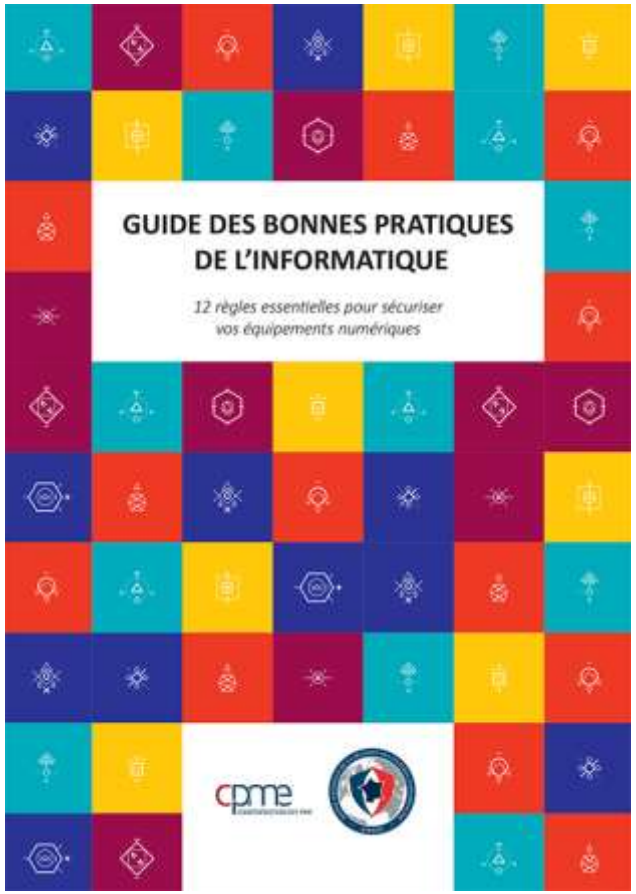
Produit	Prix moyen sur le dark web
Compte Facebook piraté	74,5 $
Compte Instagram piraté	55,45 $
Compte Twitter piraté	49 $
Compte Gmail piraté	155,73 $
Followers sur Instagram x 1000	7 $
Followers sur Spotify x 1000	3 $
Followers sur Twitch x 1000	6 $
Followers sur Tick Tok x 1000	15 $
Followers sur LinkedIn x 1000	10 $
Followers d'une page d'entreprise LinkedIn x 1000	10 $
Followers sur Pinterest x 1000	5 $
Nombre d'écoutes sur Soundcloud x 1000	1 $
Vues sur Daily Motion x 1000	2 $
Twitts et retweets x 1000	25 $
likes sur Instagram x 1000	6 $

Les attaques DDoS

Produit	Prix moyen sur le dark web
Site web non protégé, 10 à 50 000 consultations par seconde, 1 heure	10 $
Site web non protégé, 10-50 000 demandes par seconde, 24 heures	60 $
site web non protégé, 10 à 50 000 demandes par seconde, 1 semaine	400 $
Site web non protégé, 10-50k demandes par seconde, 1 mois	800 $
Site web Premium protégé , 20 à 50 000 requêtes par seconde, 24 heures	24 200 $

LA PROTECTION PASSE PAR LA FORMATION ET SENSIBILISATION DES UTILISATEURS

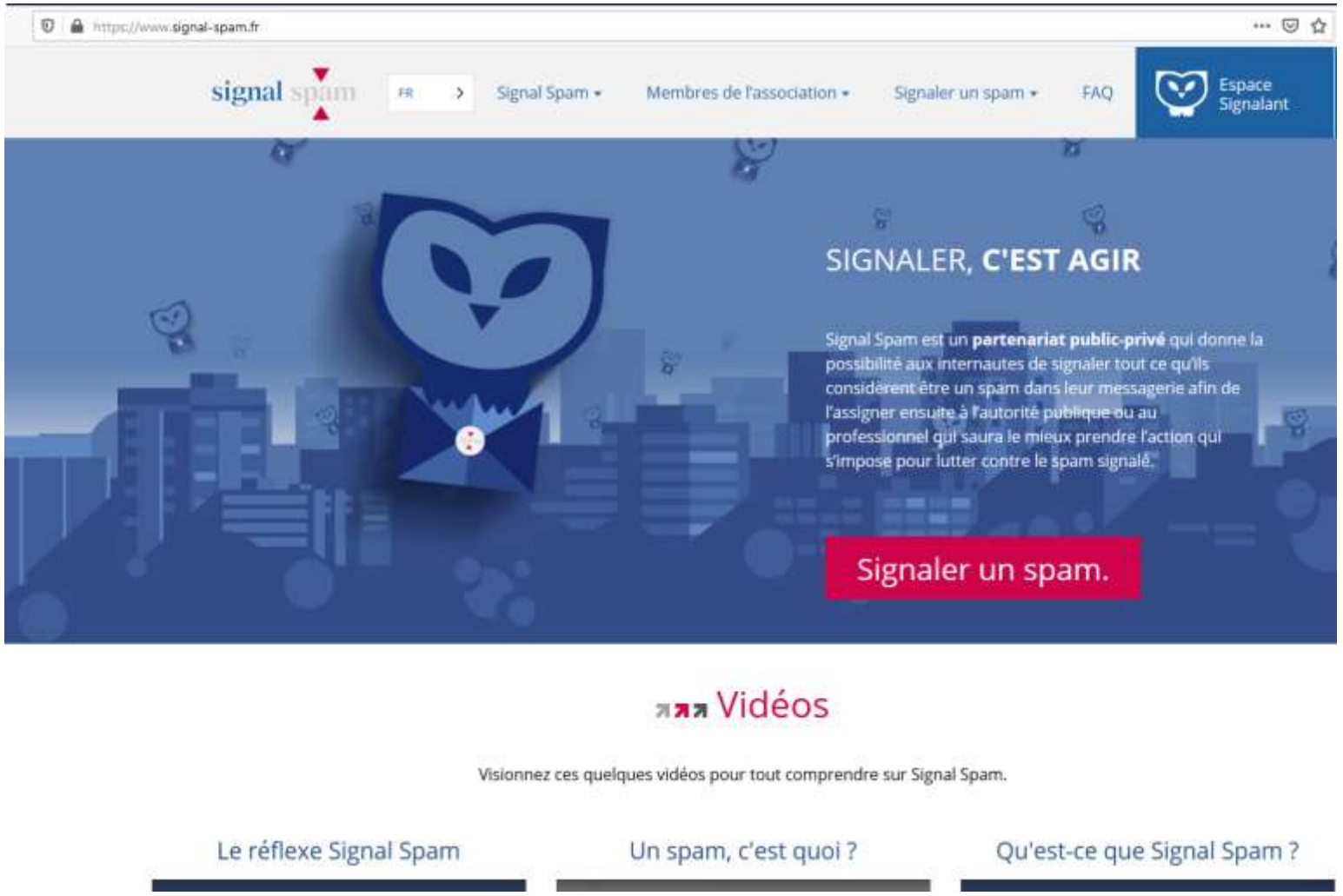
VOTRE PREMIER REMPART DE VOTRE CYBERDÉFENSE EST ENCORE TROP SOUVENT
« LE MAILLON FAIBLE EST ENTRE LA CHAISE ET LE CLAVIER »



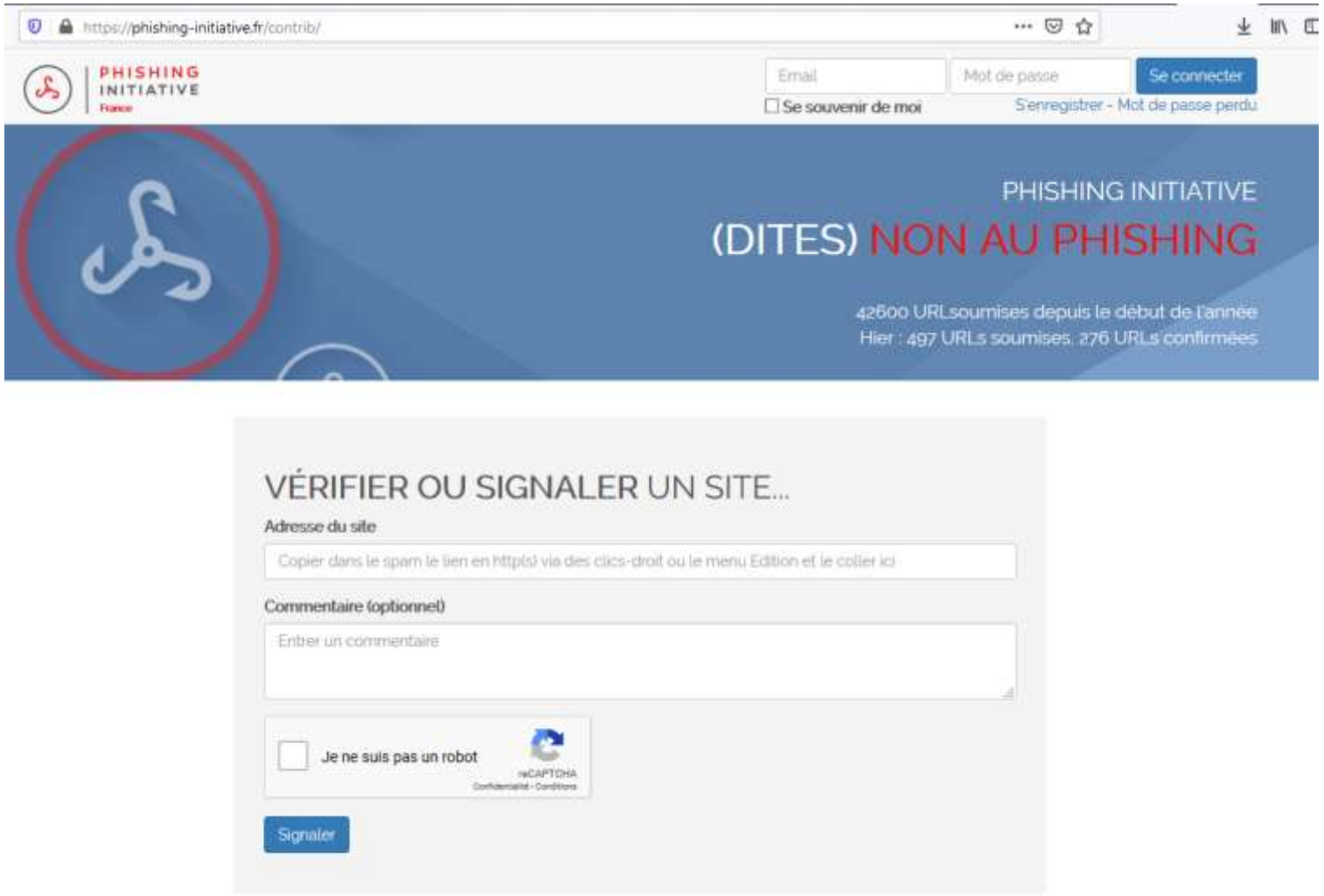
CYBERMALVEILLANCE.GOUV.FR : LA PLATEFORME D'AIDE AUX CYBERVICTIMES

déclarer une fraude ou du contenu inapproprié : internet-signalement.gouv.fr

SIGNALER UN SPAM : www.signal-spam.fr



SIGNALER UNE TENTATIVE DE PHISHING : https://phishing-initiative.fr/contrib/



QUELQUES LIENS UTILES À CONNAÎTRE….

Vérification si son adresse mail et d'autres informations ont été hackées et disponibles (à la vente) dans le DarkWeb
https://sec.hpi.de/ilc/?lang=en (le plus complet)
https://haveibeenpwned.com/
https://www.dehashed.com/
https://www.watchguard.com/fr/wgrd-resource-center/dark-web-scan

Vérification d'un pièce jointe, fichier quelconque, adresse site web par tous les antivirus du marché
www.virustotal.com

Site d'aide à la récupération de données chiffrées (pas de garantie sur les derniers rançongiciels non encore analysés)
https://www.nomoreransom.org/fr/index.html

Site de veille d'alerte et de réponse –correctifs- de l'ANSSI pour corriger ses systèmes informatiques
https://www.cert.ssi.gouv.fr/

Comment se protéger, vers qui se tourner pour se faire aider en cas d'attaque

Franck Gicquel

Cybermalveillance.gouv.fr

Responsable des partenariats

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

cpme CONFÉDÉRATION DES PME

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

Dispositif national de sensibilisation, prévention et d'assistance aux victimes

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

I- Présentation du dispositif

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES MISSIONS DU DISPOSITIF

1. **ASSISTER LES VICTIMES** d'actes de cybermalveillance
2. **INFORMER & SENSIBILISER** à la sécurité numérique
3. **OBSERVER & ANTICIPER** le risque numérique

QUI EST CONCERNÉ ?

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

CYBERMALVEILLANCE.GOUV.FR EN QUELQUES CHIFFRES

50

organisations membres
(publiques et privées) du GIP ACYMA

1100

prestataires référencés
sur l'ensemble du territoire

270 000

victimes assistées
depuis fin 2017

47

types d'incidents
traités

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

STRUCTURE : UN GROUPEMENT D'INTÉRÊT PUBLIC
50 MEMBRES PUBLICS ET PRIVÉS

PREMIER MINISTRE

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

SECRÉTARIAT D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES COMMUNICATIONS ÉLECTRONIQUES

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

II- État de la menace

PRINCIPES DE L'OBSERVATION DE LA MENACE

Capteurs :

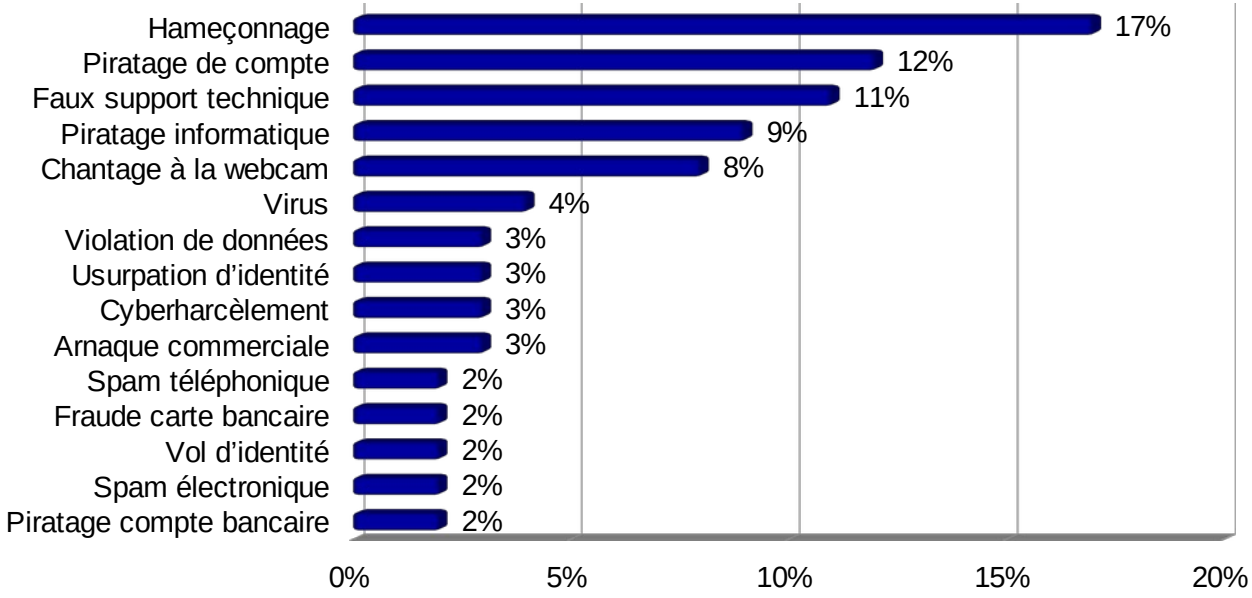
- **Parcours des victimes** sur la plateforme
- **Rapports des prestataires** référencés
- **Veille** sur la cybermenace (sources ouvertes)
- **Signalements** par des utilisateurs (réseaux sociaux, partenaires…)

Démarche :

- **Qualification** de l'information
- **Alerte** (conseils, **coopérations** au besoin/si possible)
- **Ajustement des parcours d'assistance** aux victimes
- Production de nouveaux **supports de sensibilisation** ou ajustement

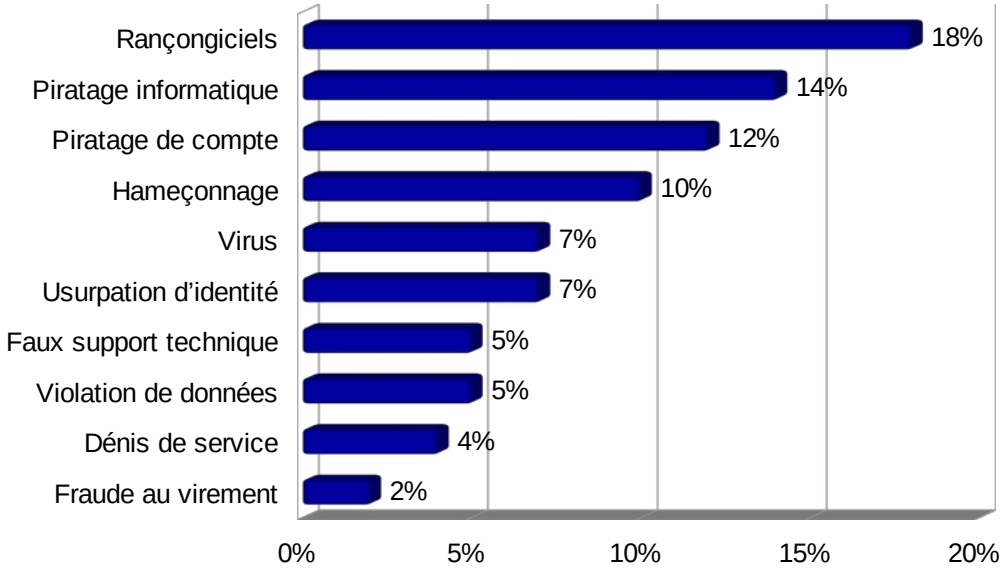
PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2020

Particuliers :



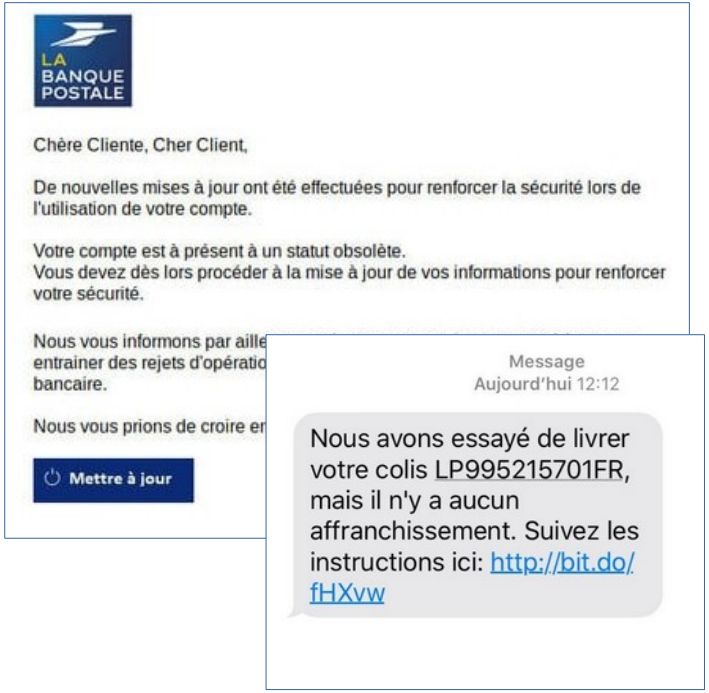
PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2020

Professionnels (entreprises, collectivités...) :



L'HAMEÇONNAGE (*PHISHING*) : LA MÈRE DES ATTAQUES

- **Menace prédominante et en hausse**
  (N° 1 pour les particuliers et N° 4 pour les professionnels)
- **Des attaques toujours plus sophistiquées**
  (de l'artisanat à la « professionnalisation »)
- **Effet démultiplicateur avec la crise sanitaire**
  (isolement numérique, télétravail...)
- **Principale cause d'autres malveillances**
  (piratage de compte, rançongiciel, fraude bancaire…)
- **Développement important des attaques par SMS**
  (confiance, difficulté de contrôle)

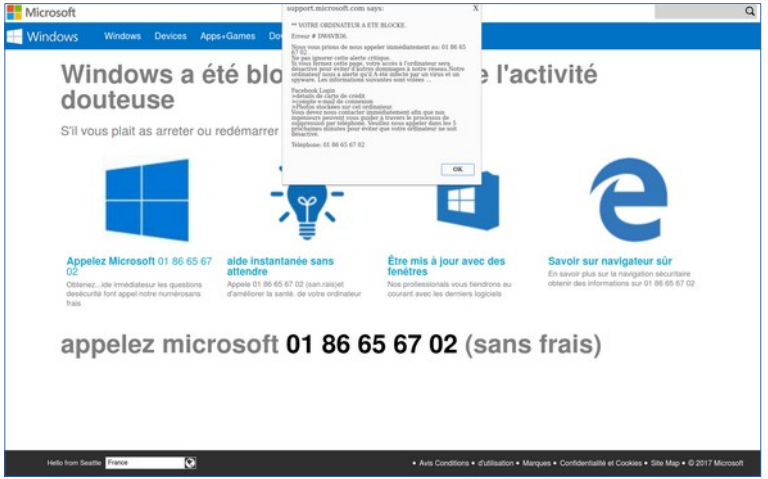


LE PIRATAGE DE COMPTE

- **Menace majeure et en expansion**
  (N° 2 pour les particuliers et les professionnels)
- **Messageries, réseaux sociaux et banques visés**
  (fort intérêt des cybercriminels pour les données revendues)
- **Des origines diverses**
  (hameçonnage, fuite de mots de passe...)
- **Cause majeure d'autres malveillances**
  (Usurpation d'identité, fraude bancaire ou au virement…)
- **Impacts de plus en plus importants pour les victimes**

LES FAUX SUPPORTS TECHNIQUES

- **Menace détectée en 2017 et toujours en tête**
  (N° 3 pour les particuliers et N° 7 pour les professionnels)
- **Concerne également les professionnels**
  (en particulier les petites structures sans support)
- **Evolution des modes opératoires toujours plus agressifs**
  (résurgence, piratage de données, recouvrement...)
- **1ère cause d'intervention des professionnels référencés**
- **Les seniors les moins aguerris restent en tête des victimes**



LES RANÇONGICIELS

- **1ère menace pour les professionnels (entreprises, collectivités...)**
  (~1 000 recherches d'assistance en 2020, +54 %)
- **Tous types et tailles d'organisations ciblées en nombre**
  (PME, grands groupes, métropoles, hôpitaux, petites collectivités...)
- **Un écosystème cybercriminel redoutable qui fonctionne en cartel**
  (développement, intrusion, négociation, blanchiment...)
- **L'intrusion via les accès externes 1er vecteur de compromission**
  (failles non corrigées, mots de passe trop simples, hameçonnage)
- **Vol de données avec menace de divulgation pour accentuer la pression depuis fin 2019**
  (médiatisation, impacts RGPD et réputationnels)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

III- Comment se prémunir ?

COMMENT SE PRÉMUNIR ?

Volet technique

Volet humain

COMMENT SE PRÉMUNIR ?

Volet technique

- Mettre en place une stratégie de sécurité
- Suivre les préconisations de l'ANSSI
- Se faire accompagner par des professionnels

LE LABEL EXPERTCYBER

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

L'objectif :

- Reconnaître l'expertise en sécurité numérique
- Sur les activités d'installation, maintenance et assistance
- Pour les clients (TPE-PME / Associations / Collectivités)

Pensé par et pour l'écosystème :

- Avec les représentants du secteur : CINOV NUMÉRIQUE, FEDERATION EBEN ENTREPRISES DU BUREAU ET DU NUMÉRIQUE, numeum, Fédération Française de l'Assurance
- En partenariat avec : afnor GROUPE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMMENT SE PRÉMUNIR ?

Volet humain

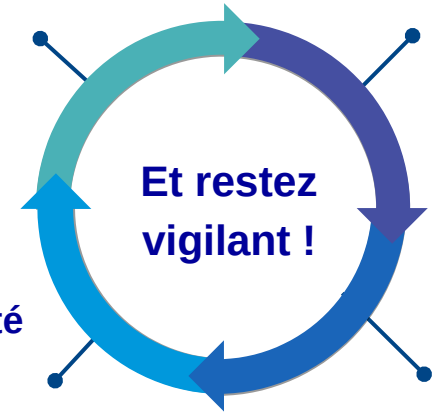
- Créer une charte informatique
- Organiser des sensibilisations en interne
- S’appuyer sur les conseils et ressources de Cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

GESTES ESSENTIELS DE SÉCURITÉ NUMÉRIQUE

Utilisez des **mots de passe uniques et solides** et activez la **double authentification** chaque fois que c'est possible



Utilisez un antivirus et vérifier son bon fonctionnement

Appliquez les **mises à jour de sécurité** sur vos équipements connectés (serveurs, ordinateurs, téléphones…) dès qu'elles sont disponibles

Faites régulièrement des **sauvegardes de vos données** et gardez en une copie déconnectée et **testez-les** !

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

SENSIBILISATION ET PRÉVENTION

Objectifs :

- Sensibiliser aux risques
- Partager les bonnes pratiques
- Alerter

Publics :

- Particuliers
- Entreprises
- Collectivités

17 thématiques

6 types de contenus :

- Fiches pratiques/réflexes
- Vidéos
- Mémos et infographie
- Alertes sur les réseaux sociaux @cybervictimes
- Articles

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

www.cybermalveillance.gouv.fr

@cybervictimes

@cybervictimes

@cybermalveillancegouvfr

CONFÉDÉRATION DES PME

Réponses aux interrogations

CONFÉDÉRATION DES PME

MERCI POUR VOTRE ATTENTION ET PARTICIPATION !

Pour toute information : contact@cpme.fr

LA CPME EST LA PREMIÈRE ORGANISATION INTERPROFESSIONNELLE
À ÊTRE CERTIFIÉE ENGAGEMENT DE SERVICE QUALI'OP

ENGAGEMENT DE SERVICE
QUALI'OP
REF. 166
AFNOR CERTIFICATION
www.afnor.org