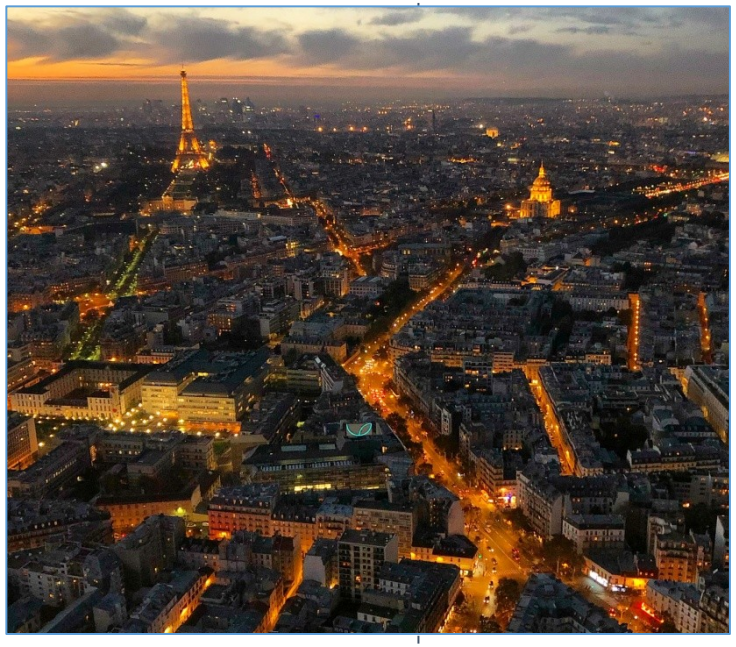
Cybercriminalité – Escroqueries en ligne

Comment se protéger ?.

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Les chiffres clés 2020

En France



- **Le nombre de cyberattaques a été multiplié par 4 en 2020**

- **Le rançongiciel** représente la menace la plus susceptible de provoquer une interruption des systèmes supérieure à 24h dans les PME comme dans les grandes entreprises. (bien plus que le risque incendie)

- Les attaques par phishing ont augmenté de 667 % pendant le premier confinement

- Le budget consacré par les entreprises françaises à la cybersécurité représente **13%** de leur budget informatique total contre 9% en 2019

- En 2020, **91 %** des entreprises françaises ont été ciblés par une cyberattaque au cours des 12 derniers mois

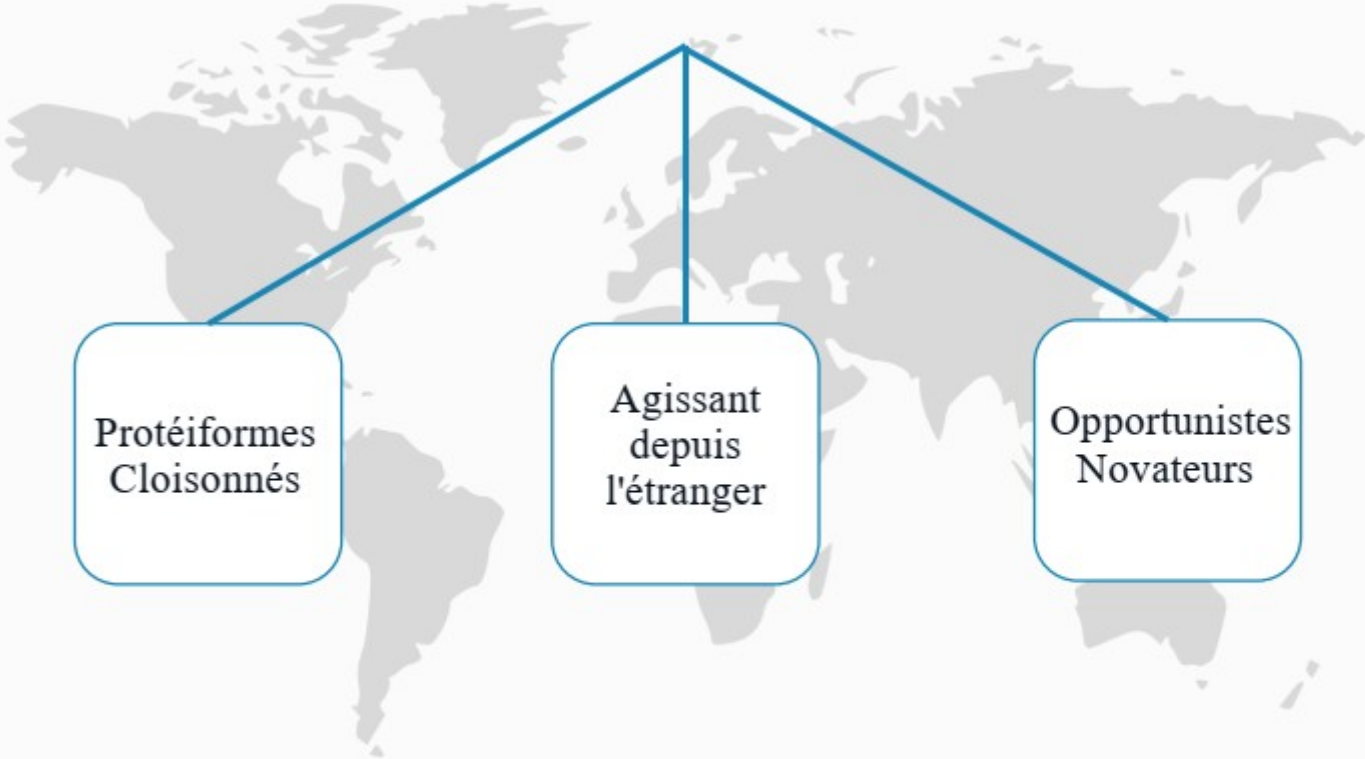
- Les conséquences des cyberattaques subies par les entreprises françaises sont la fuite de données sensibles (44%), l'impact sur la valeur de l'entreprise (43%), l'atteinte à la marque/réputation (41%), la perturbation de l'activité (40%) et les pertes financières (29%)

POLICE
NATIONALE

Evolution de la criminalité organisée depuis 20 ans

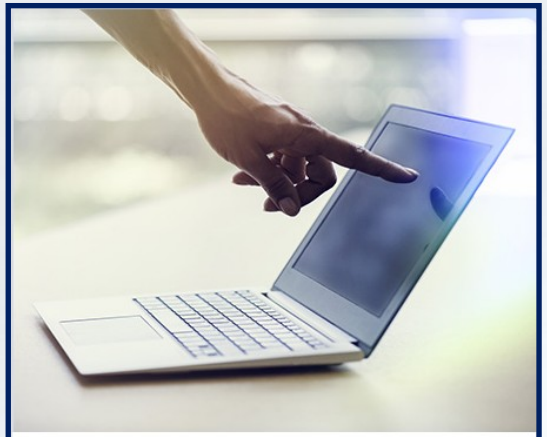
Evolution d'une délinquance en bande organisée au niveau national…

*…à une délinquance en Groupe Criminel Organisé (**GCO**) transnational*



L'état de la menace

Piratage



Escroquerie financière

Malveillance

Intelligence économique

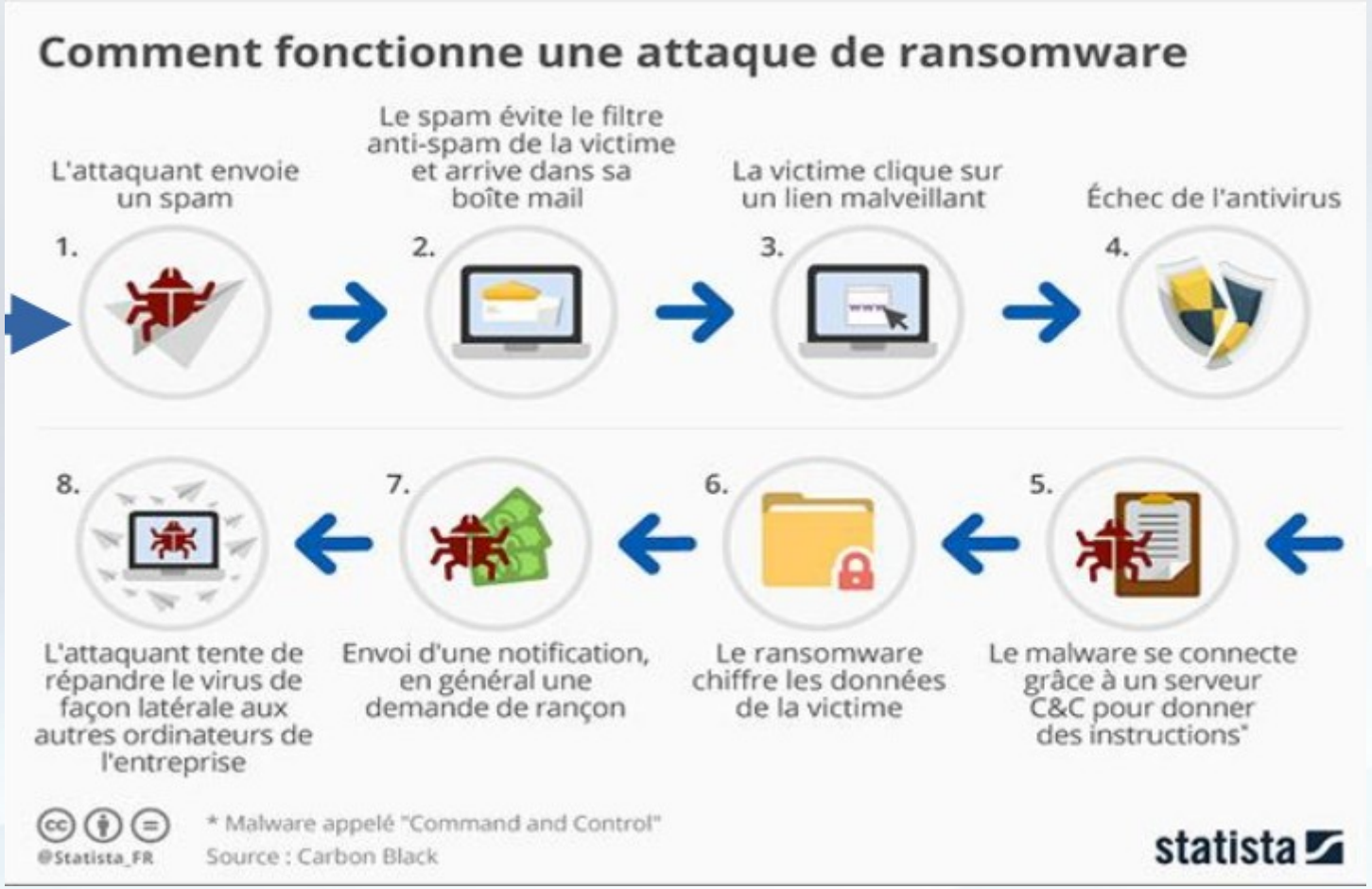
Rançongiciels DDOS

Escroqueries

Attaques internes

Exfiltration de données Pré-positionnement

Le rançongiciel



L'attaque interne

- collaborateur, ex-collaborateur, concurrent ...

SUD OUEST Mercredi 12 février 2020 Gironde 15

Un cyberpirate condamné à 2 ans de prison avec sursis

BORDEAUX

Une société éditrice de sites web a été victime des attaques de l'un de ses ex-employés

Jean-Michel Despics
jmdespics@sudouest.fr

Des revenus publicitaires détournés à hauteur de 10 %, une intrusion frauduleuse qui efface des données de travail et entraîne une baisse considérable du chiffre d'affaires. En 2018, la société 2-30 Media, éditrice de sites web à Bordeaux, spécialisée dans la mise en ligne et la gestion de sites internet publicitaires, a vécu une période difficile après avoir été piratée à plusieurs reprises. Son développement s'est trouvé menacé.

C'est la chute inquiétante des revenus publicitaires enregistrée depuis le mois de septembre 2018 qui a mis la puce à l'oreille des dirigeants de la société. Quelques semaines plus tard, une nouvelle attaque était menée et 31 sites internet, avec lesquels 2-30 Media travaillait, disparaissaient des logiciels. Seul un spécialiste en informatique pouvait être l'auteur de ces intrusions dans le système de traitement automatisé des données.

Un million d'euros

En fin connaisseur, le cyberpirate s'est à chaque fois connecté via un VPN (Virtual Private Network), un réseau privé virtuel qui est un système permettant d'être totalement anonyme sur Internet, tout en protégeant ses données et en ne laissant aucune trace de la navigation. Les dirigeants de 2-30 Media ont déposé une plainte en novembre 2018. L'enquête a été confiée au groupe de lutte contre la cybercriminalité de la Direction interrégionale de la police judiciaire (DIPJ) de Bordeaux.

Les enquêteurs ont analysé le mode opératoire de l'escroc qui avait créé un compte Google AdSense sur lequel il avait versé plus de 14 000 euros. Mais au final, la société 2-30 Media, qui a des bureaux en France et dans plusieurs pays (Espagne, Italie, Pologne, Belgique, Portugal, Mexique, Colombie et Brésil), évalue son préjudice à près d'un million d'euros pour un chiffre d'affaires annuel estimé de 4 à 5 millions.

L'ancien salarié a eu accès au coffre-fort en ligne de la société. ILLUSTRATION AFP

Apporter la preuve numérique

Comme souvent dans ce type d'affaire, les policiers ont immédiatement travaillé dans le cercle proche de la société. Et, ils ont très vite appris qu'un salarié avait quitté 2-30 Media à la fin du mois d'août 2018, suite à une rupture conventionnelle. Ce salarié, qui possédait aussi un mandat d'administrateur, avait accès au coffre-fort en ligne de la société lui permettant de récupérer des identifiants ainsi que les mots de passe pour se connecter sur des sites lui fournissant les adresses mails des clients et les données techniques commerciales et confidentielles.

« Nous devions apporter la preuve numérique de la responsabilité de l'auteur », explique le commissaire divisionnaire Paul Bousquet, chef de la division des affaires économiques et financières de la DIPJ. Au terme de leurs investigations, les policiers spécialisés dans l'investigation numérique sont parvenus à confondre l'ancien salarié de 2-30 Media, un franco brésilien de 40 ans qui vit à Nantes après avoir quitté la Gironde.

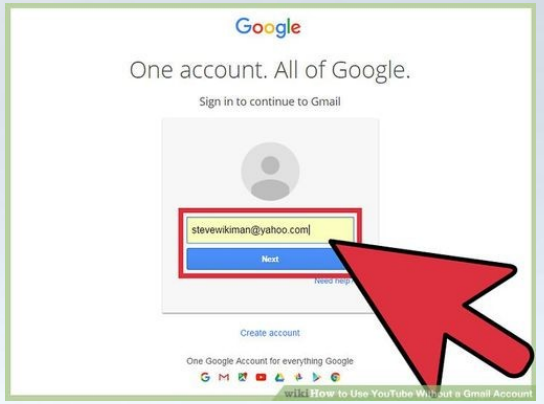
Ordinateurs saisis

Interpellé et placé en garde à vue, il a tenté de minimiser les faits. Mais l'analyse de ses téléphones portables et ordinateurs récupérés en perquisition l'a trahi. Les policiers ont notamment découvert des fichiers de la société.

Convoqué la semaine dernière devant le tribunal correctionnel pour des faits de vol, accès frauduleux dans un système de traitement automatisé, introduction frauduleuse de données et entrave au fonctionnement d'un système de traitement, l'ancien salarié a été condamné à deux ans de prison avec sursis conformément aux réquisitions du substitut du procureur de la République, Guillaume Puygrenier.

Le tribunal, présidé par Caroline Baret, a également confisqué les 12 154 euros récupérés par la PJ sur les comptes bancaires du prévenu. Cette somme a été remise au profit de l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (Agrasc). « Pour nous, il est important de pouvoir agir très vite, confie le commissaire divisionnaire Paul Bousquet. Quand une société est victime d'une attaque, elle doit se rapprocher de nos services dans les trois jours. »

Pour cela, la PJ a mis en place une adresse mail : cybermenaces-bordeaux@interieur.gouv.fr



30 % des attaques viennent de l'intérieur de l'entreprise

L'escroquerie

Article 313-1 du Code Pénal :

« L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende. »

Article 313-2 dernier alinéa du Code Pénal :

« …
Les peines sont portées à dix ans d'emprisonnement et à 1 000 000 euros d'amende lorsque l'escroquerie est commise en bande organisée. »

Caractéristiques générales

Des escroqueries basées sur :

- La crédulité des victimes (naïveté, appât du gain, peur ...) ;
- L'usurpation d'identité, obtenue par le recours à la cybercriminalité et/ou aux méthodes d'ingénierie sociale ;
- L'utilisation de moyens techniques d'anonymisation (internet, VO IP, neobanques ...)

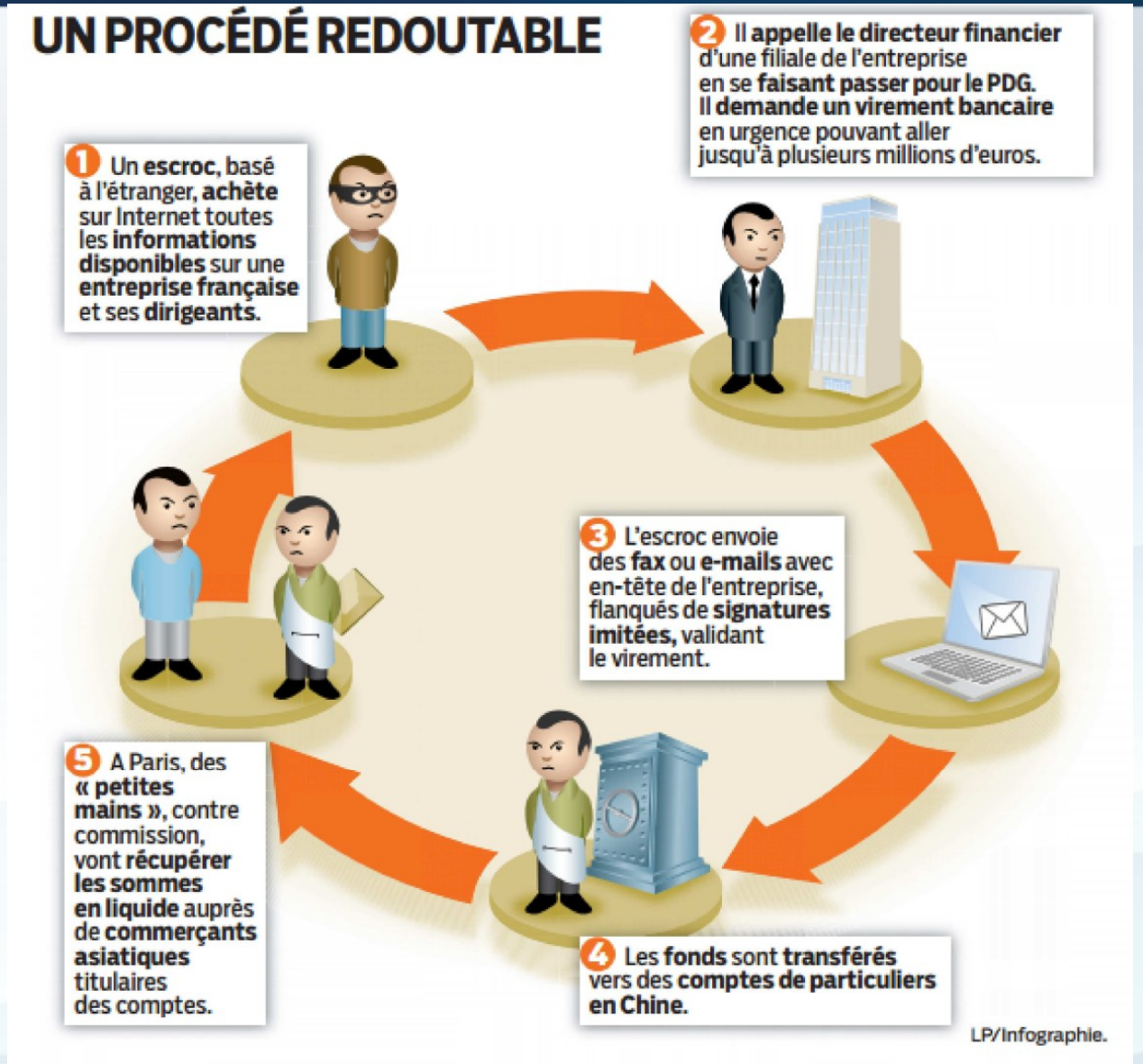
Les escroqueries ciblant les particuliers

- *L'escroquerie au sentiment*
- *L'escroquerie à la loterie*
- *L'escroquerie à l'investissement*
- *L'escroquerie au faux conseiller bancaire*
- *L'escroquerie à la fausse offre d'emploi*
- *l'escroquerie à … ?...*

Les escroqueries ciblant les entreprises

- *l'escroquerie au faux ordre de virement*

- *l'escroquerie à la fausse commande*



Comprendre l’attaquant
Pour s’en protéger

Le saviez-vous ?

71% Des cyber-attaques **sont motivées financièrement**

Source : Verizon

Le saviez-vous ?

85% Des incidents de sécurité **sont causés par une erreur humaine**

Source : Verizon

Le saviez-vous ?

94% Des cyber-attaques **se déclenchent à partir d'un e-mail**

Source : Email Threat Report 2020, Teiss

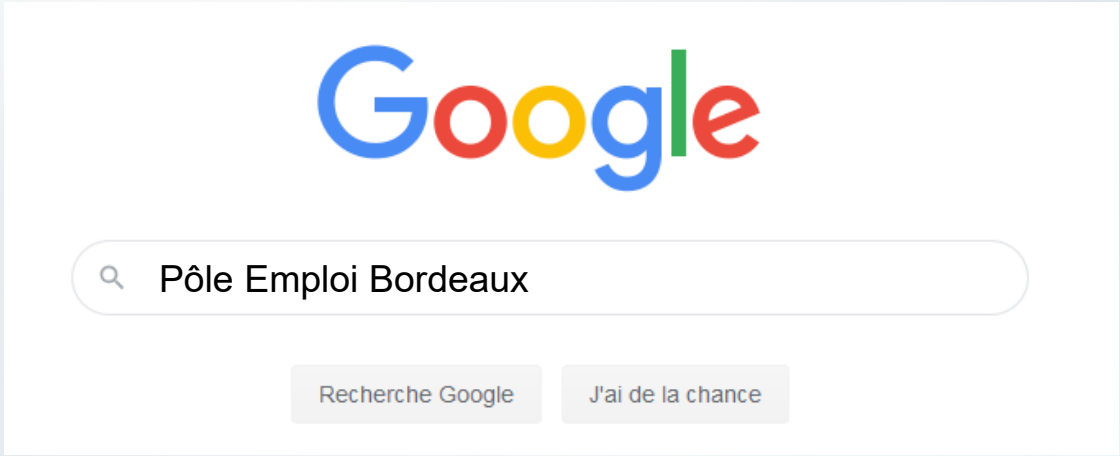
A votre avis…

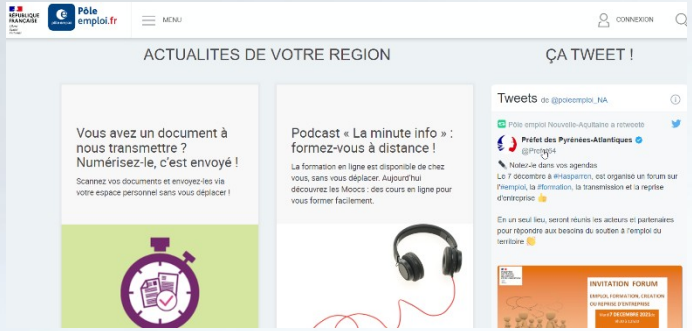
Quel est l'outil préféré

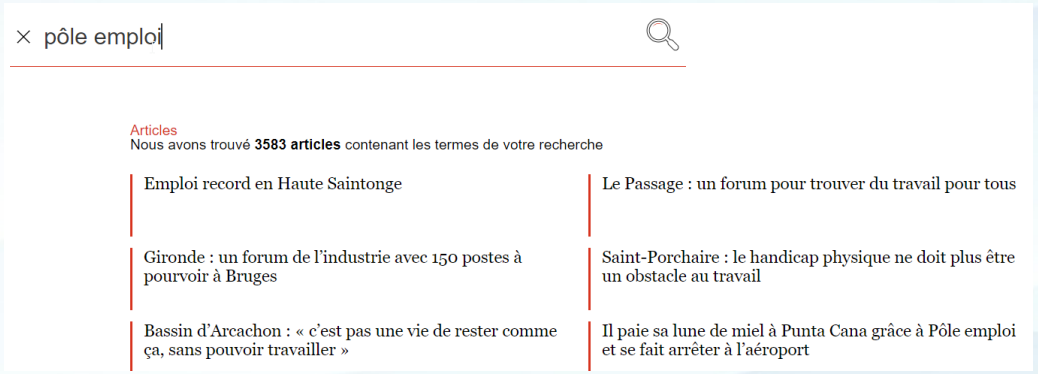
des hackers ?

Etape 1

S’informer sur la cible







OSINT : Le **renseignement de sources ouvertes** (***open source intelligence***, *OSINT*) est un renseignement obtenu par une source d'information publique.

Etape 2

Identifier des profils facilitateurs

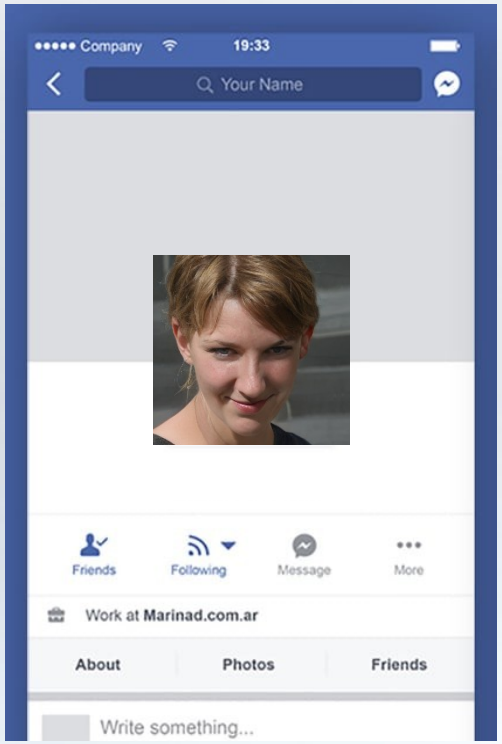
Paul H
Responsable de service

Charlotte B
Conseillère Pôle Emploi

Marie-Gaëlle S
Chargée de communication

Etape 3

Analyser les réseaux sociaux



Analyse du profil public

- Age : 32 ans
- Ville : Pessac (33)
- Statut : Mariée à Marc F
- Famille : Sœur de Sébastien S
- Profession : En recherche d'emploi
- Date de naissance : 26/03/1987

- 2 enfants : Théo & Anaïs
- 1 chat : Mojito
- Aime : la musique, le théâtre, l'escalade

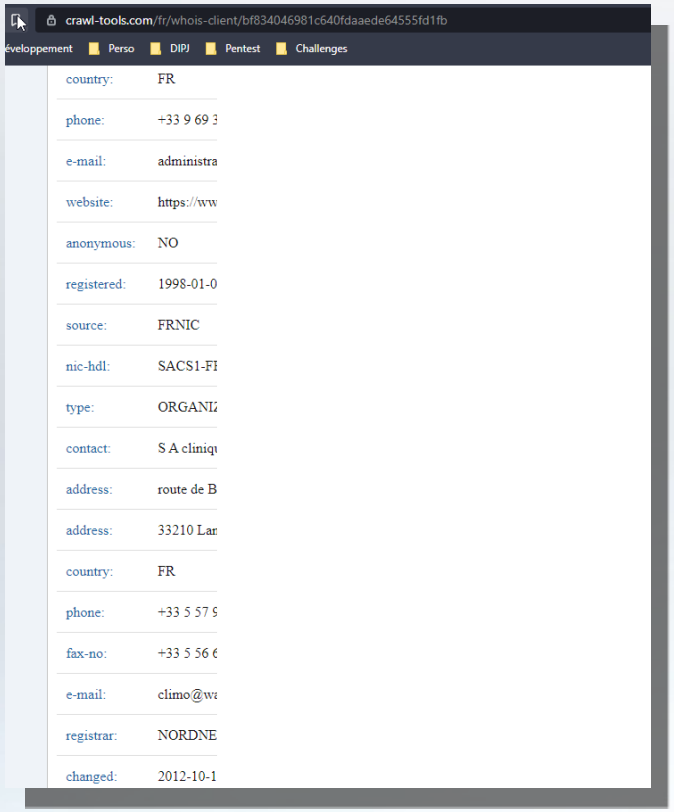
- Email : charlotte.b****@gmail.com
- Téléphone : 07 85 ** ** **

Analyse des publications

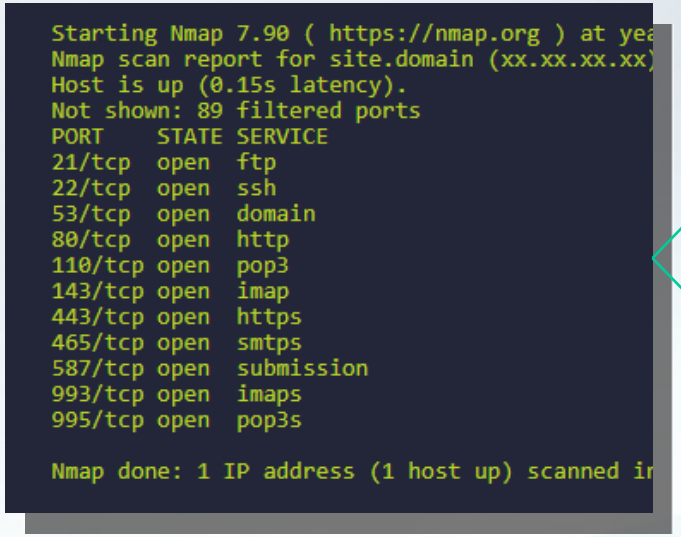
- Dispose d'un ordinateur portable
- Jour de l'an prévu avec Jean-Marc
- En vacances du 1 au 8 déc 2019
- Série en cours : G.O.T
- Super concert de –M- a l'ARENA
- …

Etape 4

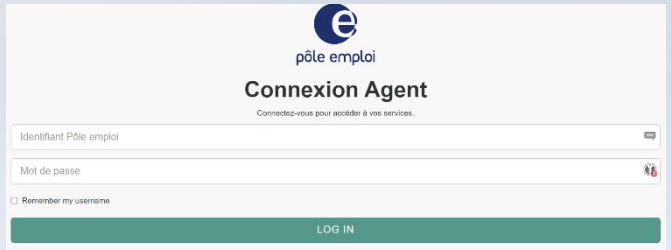
Scanner l’infrastructure cible



Recherche d’informations publiques



Interrogation des serveurs



Découverte de services en ligne

Etape 5

Agréger les informations

Construction de l'organigramme de la structure

Regroupement des postes facilitateurs

Description du poste
Intitulé du poste
Fiche de fonction ou métier correspondant
Positionnement dans l'organisation et responsabilités managériales
Missions principales
Activités et tâches
Moyens et prérogatives
Relations internes et externes
Conditions et lieu de travail

Profil du poste
Compétences
Expérience professionnelle
Formations / diplômes

Création d'un annuaire de victimes

Adresse e-mail du type :
nom.prenom@pole-emploi.fr

Identification des chercheurs d'emploi:
celine.azerty@gmail.com
fabrice.azerty@hotmail.com
chachou33@hotmail.com
…

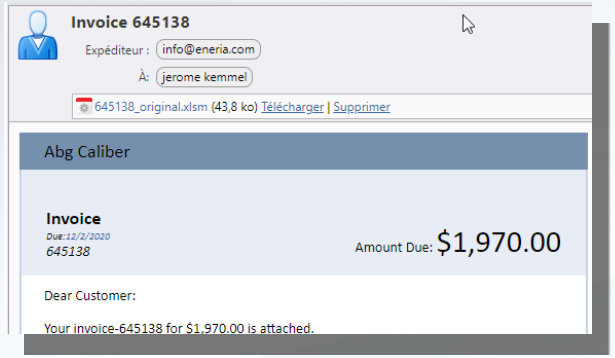
N° de téléphone du type :
05 57 02 ** ** (4 chiffres par services)

Pour quels objectifs ?

Phishing pour collecter des données personnelles

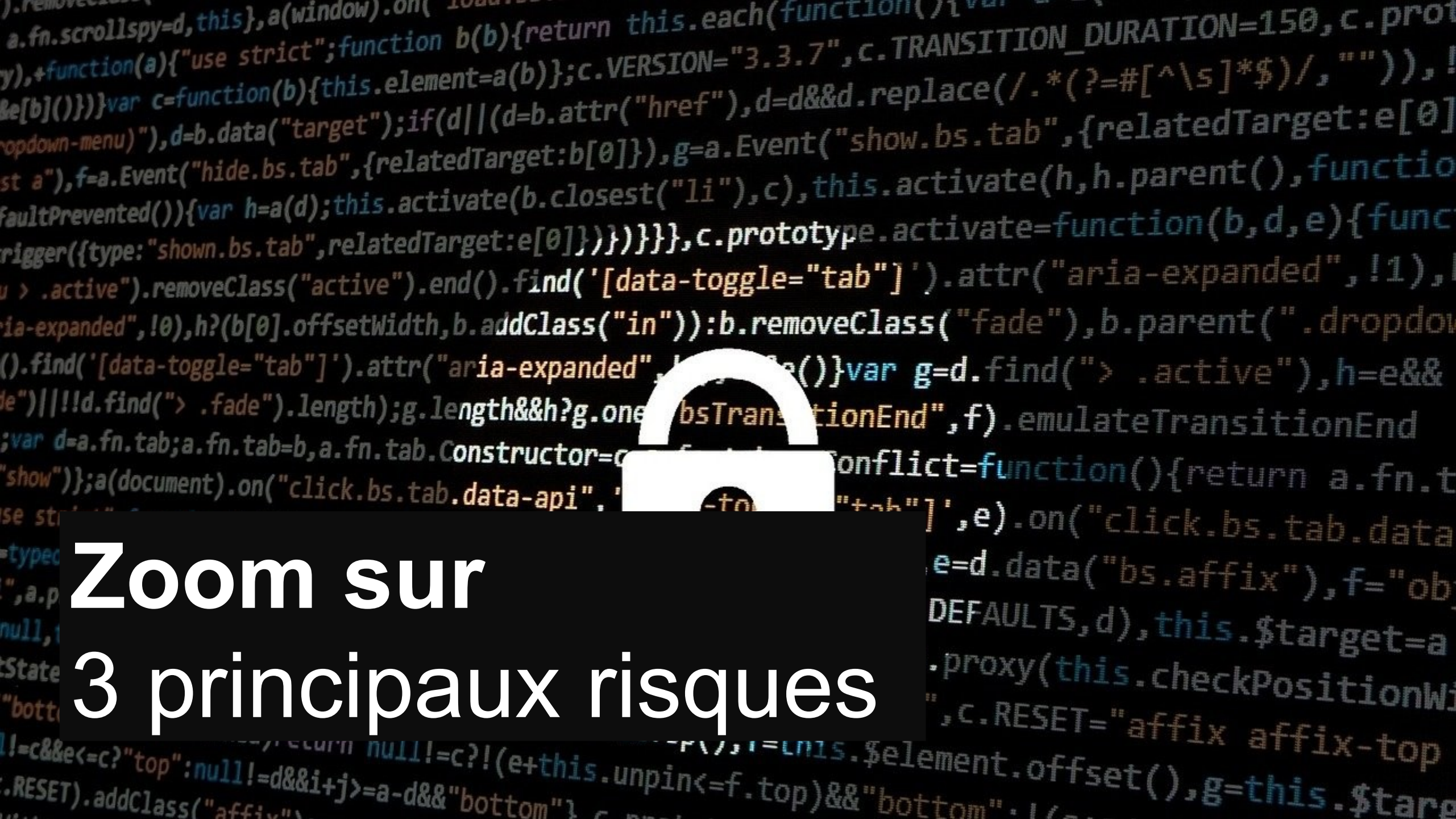
Faux support informatique pour prise de contrôle à distance

« perte » volontaire d'une clé USB infectée pour diffuser du code malveillant



Pièce-jointe malveillante pour infecter le terminal cible

Fausse facture de prestation pour escroquerie financière



Zoom sur
3 principaux risques

L’ingénierie Sociale, c’est quoi ?

Manipulation psychologique

Exploite la

Vulnérabilité **humaine**

Dans un objectif

Escroquerie financière

Ou

Accès / Vol de **données**

L’ingénierie Sociale : 2 principaux ingrédients

Usurpation d’identité

Physique ou morale

Pression, émotion

De la victime

POLICE NATIONALE

Zoom sur 3 risques :

L'ingénierie sociale

POLICE NATIONALE · DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

Le phishing, par l'exemple

Pôle emploi.fr

Rendez-vous confirmé

Bonjour,

Vous trouverez ci-dessous une demande de rendez-vous avec votre conseiller Pôle Emploi. Nous vous remerciant de bien vouloir **répondre sous 24h00** afin de conserver vos droits d'allocation chômage.

Date proposée :

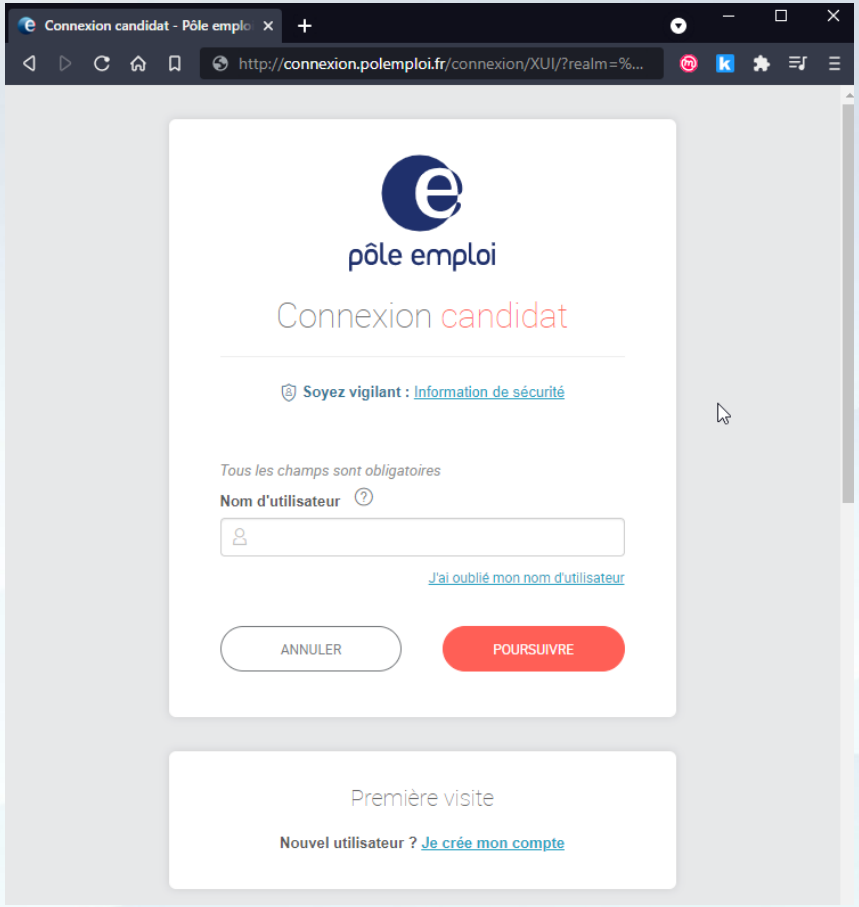
24/12/2021 à 17h15
à votre agence habituelle

Sans réponse de votre part **sous 24h00** dès réception de votre e-mail, vos droits d'allocation chômage **seront suspendus**.

Je souhaite reporter mon rendez-vous

Je souhaite confirmer mon rendez-vous

Cordialement,
Votre conseiller Pôle Emploi



POLICE NATIONALE

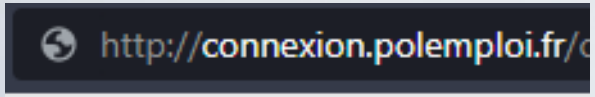
Zoom sur 3 risques :

L'ingénierie sociale

POLICE NATIONALE · DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

Le Phishing, comment s'en protéger ?

Règle n°1 : **Contrôler TOUJOURS** votre source



Ne vous fiez pas au lien présent sur l'e-mail mais à celui qui s'affiche dans votre navigateur : est-il vraiment celui de votre fournisseur ?

Règle n°2 : **Vérifiez TOUJOURS** si la communication est chiffrée

Le cadenas et la mention https sont indispensables pour garantir le chiffrement de la connexion avec le serveur web du destinataire.

Règle n°3 : **Ayez TOUJOURS** un doute !

Vous êtes surpris par le contenu d'un mail ?
On vous demande vos coordonnées bancaires ?
Vous n'avez jamais commandé sur le site en question ?

STOP ! Il s'agit probablement d'une arnaque.
Contactez votre responsable informatique ou le fournisseur concerné !

POLICE NATIONALE

Zoom sur 3 risques :

La gestion des mots de passe

POLICE NATIONALE · DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

Le mot de passe : votre clé privée !

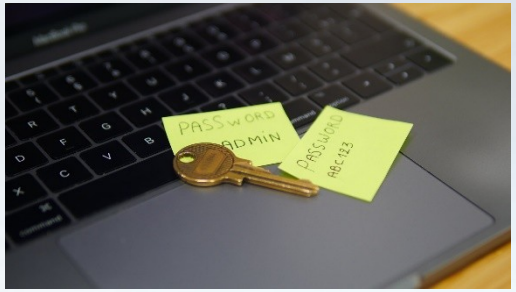
- Quelque soit le service que vous utilisez, **votre mot de passe est personnel !**
- **Ne transmettez jamais** votre mot de passe
- **Choisissez un mot de passe « complexe ».** C'est-à-dire « difficile à deviner » pour l'attaquant
- **N'utilisez pas le même** mot de passe pour deux services différents
- **N'enregistrez pas** vos mots de passe sur vos cahiers ou sur votre ordinateur

Zoom sur 3 risques :

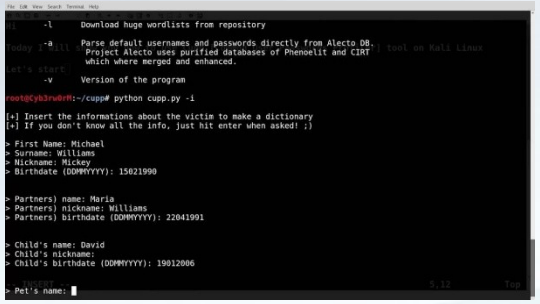
La gestion des mots de passe

Protéger ses mots de passe, pour éviter…

Les attaques :
•Par dictionnaire
•Par « brute-force »



La divulgation :
•Les post-it
•Les enregistrements non protégés



De le deviner :
•A partir de vos données personnelles publiques

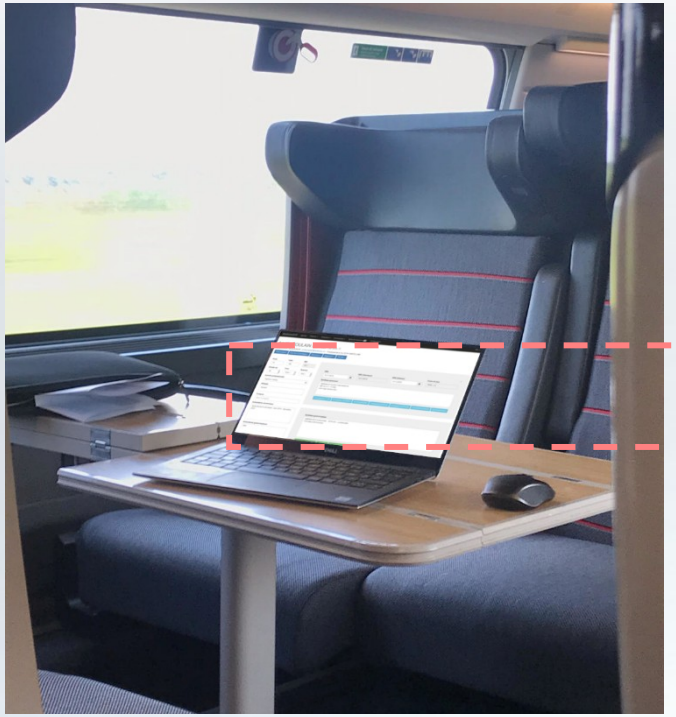
La malveillance et les risques d'erreurs :
•Interne
•Externe

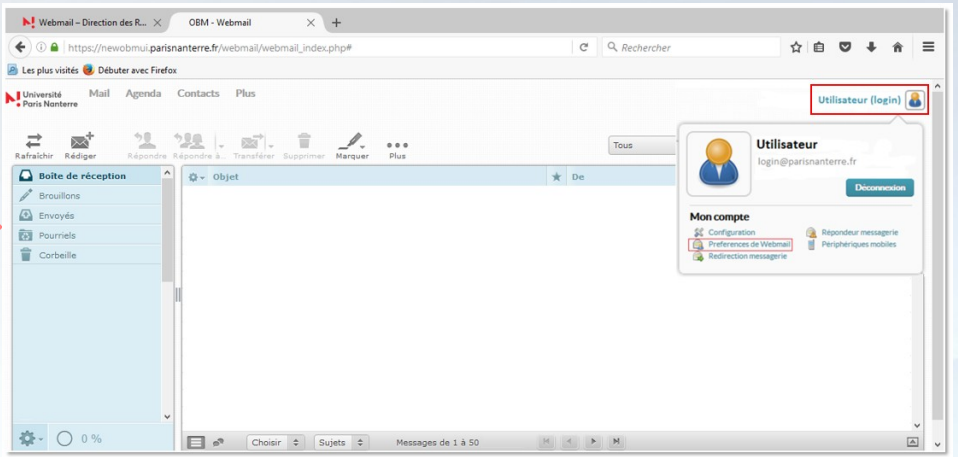
POLICE NATIONALE

Zoom sur 3 risques :

La mobilité et la séparation des usages

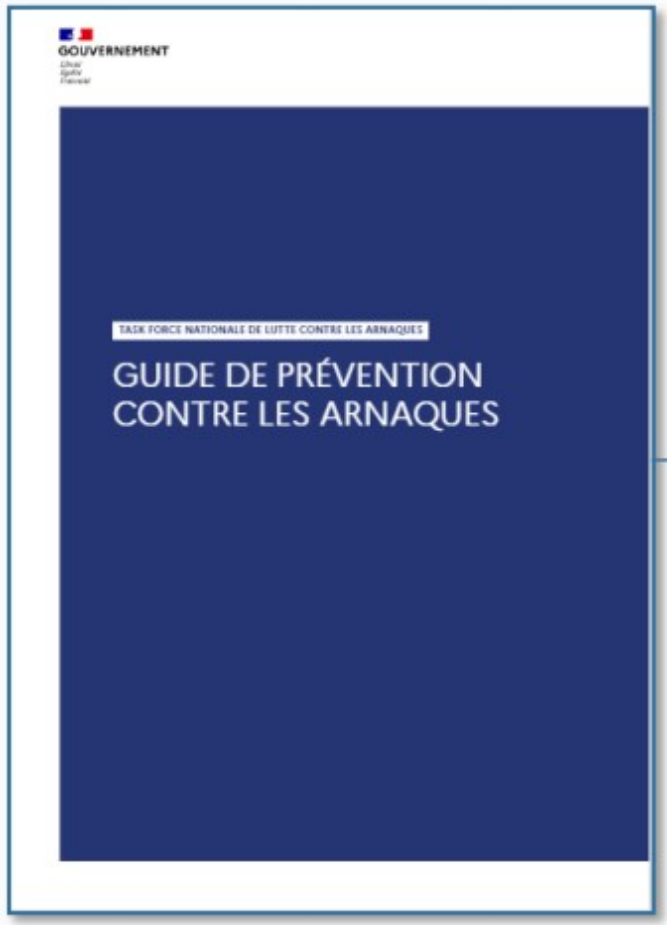
POLICE NATIONALE · DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

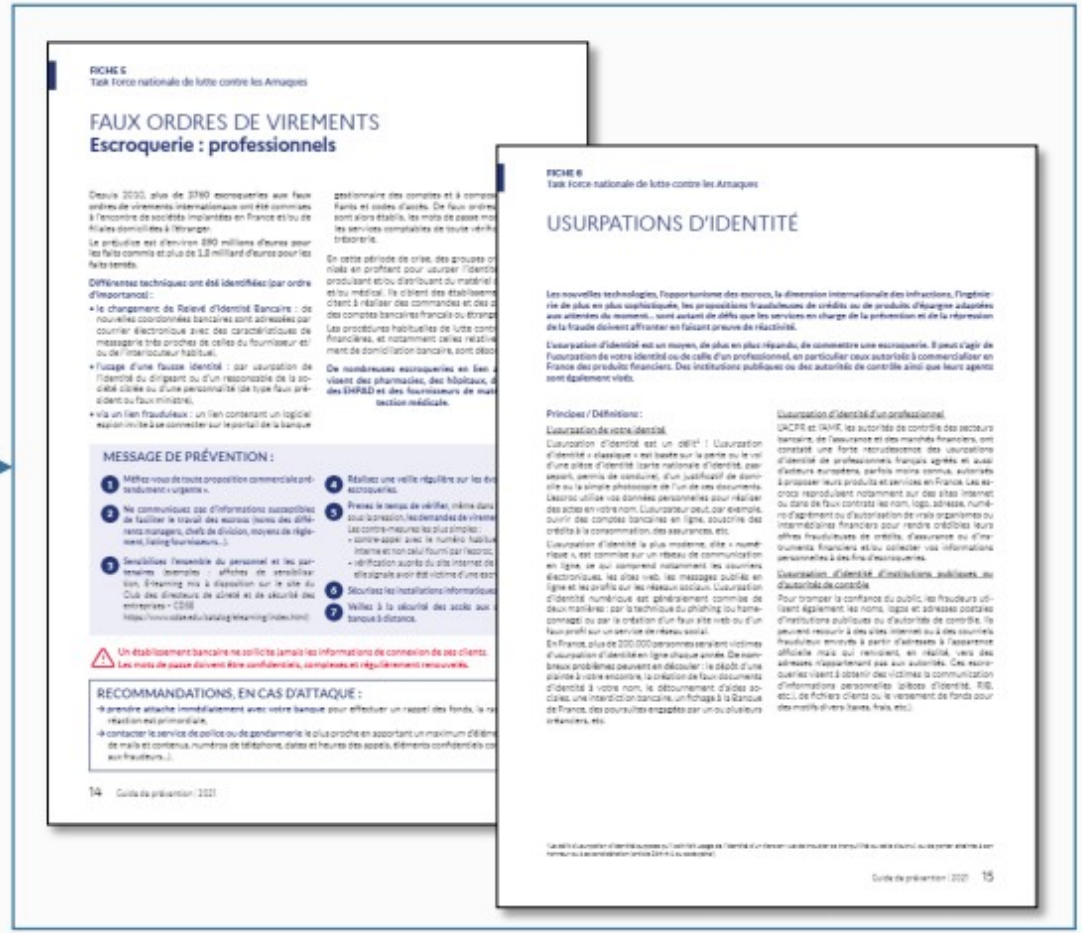




Des ressources

« La Task-Force nationale de lutte contre les arnaques se mobilise et publie un guide de prévention contre les arnaques »





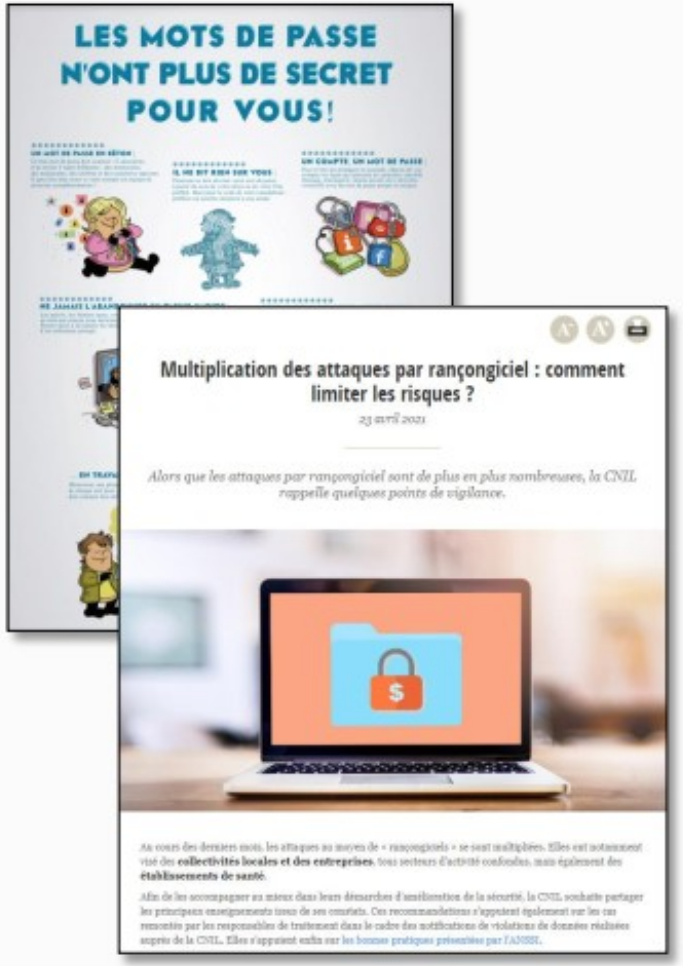
Des ressources

https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

https://secnumacademie.gouv.fr/

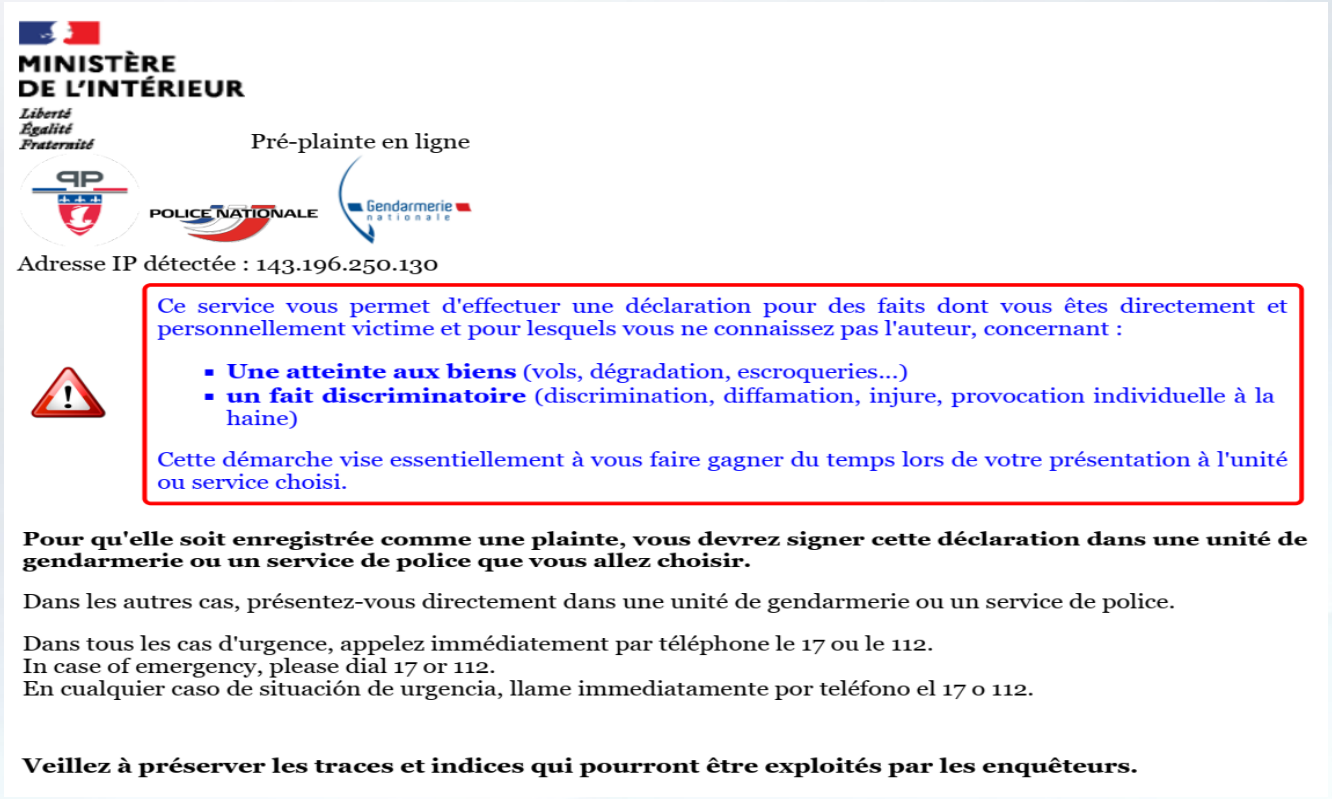
CNIL.

https://www.cnil.fr/fr/cybersecurite



https://www.cybermalveillance.gouv.fr/cybermenaces

Vous êtes une entreprise ?



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Pré-plainte en ligne

Adresse IP détectée : 143.196.250.130

Ce service vous permet d'effectuer une déclaration pour des faits dont vous êtes directement et personnellement victime et pour lesquels vous ne connaissez pas l'auteur, concernant :

- **Une atteinte aux biens** (vols, dégradation, escroqueries...)
- **un fait discriminatoire** (discrimination, diffamation, injure, provocation individuelle à la haine)

Cette démarche vise essentiellement à vous faire gagner du temps lors de votre présentation à l'unité ou service choisi.

Pour qu'elle soit enregistrée comme une plainte, vous devrez signer cette déclaration dans une unité de gendarmerie ou un service de police que vous allez choisir.

Dans les autres cas, présentez-vous directement dans une unité de gendarmerie ou un service de police.

Dans tous les cas d'urgence, appelez immédiatement par téléphone le 17 ou le 112.
In case of emergency, please dial 17 or 112.
En cualquier caso de situación de urgencia, llame immediatamente por teléfono el 17 o 112.

Veillez à préserver les traces et indices qui pourront être exploités par les enquêteurs.

https://www.pre-plainte-en-ligne.gouv.fr

Vous êtes un particulier ?

POLICE NATIONALE

POLICE NATIONALE · DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

FICHE DE CONTACT
RÉSEAU DES RÉFÉRENTS CYBERMENACES DE LA POLICE NATIONALE

La Police judiciaire vous propose un point de contact unique pour le territoire : **Nouvelle-Aquitaine**

cybermenaces-bordeaux@interieur.gouv.fr

POLICE NATIONALE

Le réseau des référents cybermenaces de la Police nationale est une structure innovante composée de :

- **Réservistes** issus du monde de l'entreprise engagés dans la lutte contre la cybercriminalité
- **Policiers spécialisés**
- **Investigateurs en cybercriminalité**
- **Professionnels et Institutions partenaires**

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

VOUS SOUHAITEZ BÉNÉFICIER D'UNE SENSIBILISATION À LA CRIMINALITÉ FINANCIÈRE ET À LA CYBERCRIMINALITÉ ?

Les réservistes du RCM dispensent des conseils de prévention face à la criminalité utilisant les moyens numériques. Ces sensibilisations s'adressent aux salariés de l'entreprise, aux responsables informatiques et à leurs dirigeants. Les réservistes donnent des conseils de bonne hygiène numérique et de premiers secours en cas de cyberattaque. La connaissance des modes opératoires des criminels permet de prendre conscience des différentes failles humaines et technologiques employées. Ces conseils assurent une meilleure préservation des intérêts de l'entreprise face à la menace cybercriminelle.

VOUS ÊTES VICTIME D'UNE CYBERATTAQUE ?

Vous pouvez contacter le réseau des référents cybermenaces le plus proche. Ce service vous orientera vers les entreprises labellisées spécialisées en remédiation des systèmes informatiques. Les réservistes et policiers vous accompagneront également vers un service spécialisé de la Police nationale pour déposer plainte, en vue de demander réparation du préjudice subi. Les investigateurs en cybercriminalité de la police judiciaire veilleront à recueillir les preuves numériques afin de retrouver les auteurs de la cyberattaque.

LE RÉSEAU DES RÉFÉRENTS CYBERMENACES

Le réseau des référents cybermenaces renseigne, sensibilise et accompagne les PTE/PME du territoire :

CONTACTS

Bordeaux	cybermenaces-bordeaux@interieur.gouv.fr
Lille	cybermenaces-lille@interieur.gouv.fr
Lyon	cybermenaces-lyon@interieur.gouv.fr
Marseille	cybermenaces-marseille@interieur.gouv.fr
Montpellier	cybermenaces-montpellier@interieur.gouv.fr
Rennes	cybermenaces-rennes@interieur.gouv.fr
Strasbourg	cybermenaces-strasbourg@interieur.gouv.fr
Toulouse	cybermenaces-toulouse@interieur.gouv.fr