MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

État actualisé de la menace et perspectives judiciaires

25 avril 2023 – Royan

L'ÉTAT DE LA MENACE

Les chiffres clés en France

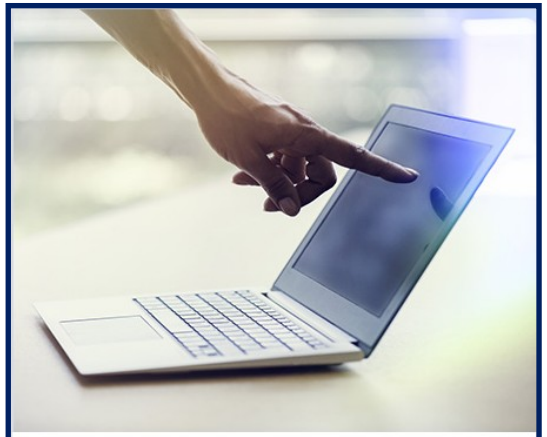
- **Top 3 des entités victimes** d'attaque par rançongiciels dans le cadre des incidents traités par l'ANSSI en 2021 *(Source : ANSSI - Panorama des menaces 2022)* :
  - 52 % : PME / TPE / ETI
  - 19 % : Collectivité territoriale / locale
  - 10 % : Entreprise stratégique
- Cybermalveillance a constaté une hausse de 95% des demandes d'assistance par les professionnels victimes de rançongiciel en 2021. *(Source : Cybermalveillance – rapport d'activité 2021)*
- 6 entreprises sur 10 ayant vécu une attaque informatique ont été impactées sur leur business, principalement en raison d'une perturbation de la production (21%) ou par la compromission d'information (14%) *(source : baromètre du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) 2022)*
- En cas de cyber-attaque, il y a une fuite de données dans 6 cas sur 10. *(source : La Cnil)*

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

Piratage



Escroquerie financière

Attaques internes

Intelligence économique

Rançongiciels DDOS

Faux ordres de virement, faux RIB ...

Malveillance, concurrence déloyale

Exfiltration de données Pré-positionnement

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

franceinfo:
3 nouvelle aquitaine

Charente : le réseau informatique de Grand-Cognac victime d'un virus de grande ampleur

Publié le 23/10/2019 à 11h40
Mis à jour le 11/06/2020 à 20h57

Écrit par C.Hinckel et A.Halpern avec AFP

Rubriques Rechercher La chaîne La chaîne Podcasts TV7 SUD OUEST Journal S'identifier
PREMIUM COMMUNES FAITS DIVERS COVID 19 FRANCE SPORT ÉCONOMIE ARCHIVES CARNET
BORDEAUX ARCACHON LIBOURNE LA ROCHELLE SAINTES ROYAN COGNAC ANGOULÊME PÉRIGUEUX AGEN PAU BAYONNE BIARRITZ MONT-DE-MARSAN DAX

Cyberattaque : l'hôpital de Dax devrait y voir plus clair le 15 mars

Lecture 2 min

Accueil • Landes • Dax

SUD OUEST 08/02/2021

LA RÉGION | 11

Vol de données à Cdiscount, un directeur mis en examen

Le système de traitement des données du leader français du e-commerce, composé de 33 millions de clients, a été mis en vente sur le Darknet

Le e-commerce n'a jamais aussi bien fonctionné depuis que la France vit au rythme des confinements. Cdiscount, le numéro1 national, a cumulé jusqu'à 22 millions de visiteurs uniques par mois, soit un tiers de la population française qui s'est connecté sur le site dont le siège social est installé aux bassins à flot à Bordeaux et dont les plus importants entrepôts logistiques sont basés à Cestas, en Gironde. Avec 33 millions de clients, le site internet du géant du e-commerce est régulièrement victime d'attaques. Celles-ci sont toujours déjouées par des mesures de sécurité sophistiquées qui veillent à la moindre intrusion dans le système.

20 000 dollars le fichier

A la veille du week-end dernier, c'est une société spécialisée dans la lutte contre la cybercriminalité qui a été intriguée par la

Dans les entrepôts Cdiscount de Cestas. S. LARTIGUE/"SO"

Bordeaux, saisis par le parquet, ont remonté la trace du hacker

garde à vue au commissariat central de Bordeaux. Lors de son

SUD OUEST Mardi 18 juin 2019 — Actu France

Un des plus gros trafics du Darknet démantelé

BORDEAUX Un militaire girondin de 32 ans est soupçonné d'avoir pris part à la plus importante plateforme du Darknet francophone

Jean-Michel Desplos
jm.desplos@sudouest.fr

Cela faisait plusieurs années qu'ils officiaient dans l'ombre. Depuis ce week-end, trois hommes ont été mis en examen et deux ont été placés en détention provisoire, dont un militaire girondin habitant à Martignas-sur-Jalle, dans la banlieue de Bordeaux. C'est en 2018 que les enquêteurs de la cyberdouane de la Direction nationale du renseignement et des enquêtes douanières (DNRED) se sont intéressés de près à l'activité d'une équipe qui animait le forum French Deep Web-Market, considérée comme la plus importante plateforme du Darknet francophone.

En milieu de semaine dernière

Les enquêteurs de la police judiciaire, comme les douanes, sont experts dans la lutte contre la cybercriminalité. PHOTO L. THIBAULT/« S. O. »

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 Desplos
jmdesplos@sudouest.fr

Des serveurs 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 2016, la société 130 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 2016 qui a mis la puce à l'oreille des dirigeants de la société. Quelques semaines plus tard, une nouvelle

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

quet, 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 230 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 maîtriser 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 Poggerenler.

Le tribunal, présidé par Caroline Barat, a également confisqué les

18 — Gironde — Vendredi 20 septembre 2019 SUD OUEST

Des escrocs visent un promoteur

BORDEAUX Des escrocs ont tenté de soutirer 1,3 million d'euros à un promoteur du chantier Euratlantique. La PJ a été saisie de l'affaire

Jean-Michel Desplos
jm.desplos@sudouest.fr

La clairvoyance d'un banquier a permis d'éviter une catastrophe à un important promoteur immobilier implanté dans plusieurs métropoles du Sud de la France, dont Bordeaux.

Le 6 septembre dernier, ce banquier a bloqué le virement de 1,3 million d'euros prêt à partir vers un tout autre compte que celui d'une entreprise de génie civil industriel basé à la périphérie de Toulouse.

C'est au cœur de l'été, début août, qu'une comptable de l'agence bordelaise du promoteur, spécialisé dans le logement haut de gamme, reçoit un coup de fil. Téléphone. L'homme au bout du fil indique être un des responsables d'une entreprise du bâtiment et de génie civil industriel, ayant travaillé sur l'immeuble chantier Euratlantique du quartier Saint-Jean-Belcier qui a vu la construction de 7 500 logements ainsi que 90 000 mètres carrés de bureaux.

Car les escrocs spécialisés dans la cybercriminalité s'intéressent à l'actualité économique en France et suivent tous les projets avec une grande acuité.

Mise en confiance

Euratlantique ne leur a pas échappé. Quand le faux dirigeant toulousain appelle le service comptabilité du promoteur bordelais en prenant soin de passer par le standard, le stratagème est réglé comme du papier à musique. L'homme explique que sa société vient de changer de banque et qu'il va envoyer par mail les nouvelles coordonnées pour percevoir une créance de 1,3 million d'euros. Quelques heures plus tard, un Iban (International bank account number) est transmis par courriel avec le logo de la société parfaitement imité.

La comptable est bernée mais tarde à effectuer le paiement. Début septembre, les escrocs se manifestent et rappellent la veille d'un week-end. L'interlocuteur semble s'impatienter mais évoque un autre chantier, bien réel, donne des détails et met en confiance son interlocutrice. Le virement est effectué dans la matinée du 6 septembre mais est aussitôt gelé dans la journée par la banque, suspicieuse, qui donne l'alerte.

Une plainte est déposée et l'affaire est confiée à la division des affaires économiques et financières de la direction interrégionale de la police judiciaire (DIPJ) de Bordeaux. « Malgré des campagnes de prévention, des entreprises continuent à se faire piéger », déplore le commissaire Paul Bousquet, chef de la division des affaires économiques et financières à la DIPJ. « Une holding qui détient des grands crus, un office HLM, une société de négoce font partie des récentes victimes mais, à l'heure actuelle, ce sont des entreprises du bâtiment les plus touchées. »

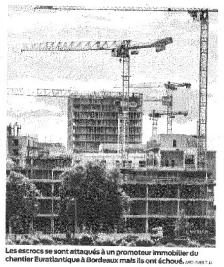
Pas d'informations sur Internet

Depuis plus d'un an, le commissaire de police parcourt la région à la rencontre de patrons et de banquiers pour les sensibiliser sur les faux ordres de virements internationaux (fovi) et toutes les arnaques réalisées sur Internet par des hackers toujours plus imaginatifs.

« Il faut saisir la police au plus vite car c'est dans les premières heures que nous pouvons agir et récupérer tout ou partie de l'argent volé sur un compte à l'étranger, dit encore le commissaire Paul Bousquet. Car ensuite, l'argent part en Israël ou en Chine, et c'est beaucoup plus compliqué. »

Dans le cas du promoteur immobilier bordelais, le banquier a eu le bon réflexe « trouver les entreprises, quelle que soit leur taille, sont des cibles potentielles, rappelle le commissaire. Nous les incitons à ne pas divulguer d'information stratégique sur leur site internet et suggérons à leurs collaborateurs de faire un contre-appel téléphonique systématique et à informer leur hiérarchie. »

Depuis 2010, les escroqueries aux FOVI ont touché plusieurs centaines d'entreprises en France pour un préjudice supérieur à



Les escrocs se sont attaqués à un promoteur immobilier du chantier Euratlantique à Bordeaux mais ils ont échoué. GPC-SUD O.

POLICE
NATIONALE

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

1

Choisir avec soin ses mots de passe

Dans le cadre de ses fonctions de comptable, Julien va régulièrement consulter l'état des comptes de son entreprise sur le site Internet mis à disposition par l'établissement bancaire. Par simplicité, il a choisi un mot de passe faible : 123456. Ce mot de passe a très facilement été reconstitué lors d'une attaque utilisant un outil automatisé : l'entreprise s'est fait voler 10 000 euros.

2

Mettre à jour régulièrement vos logiciels

Carole, administrateur du système d'information d'une PME, ne met pas toujours à jour ses logiciels. Elle a ouvert par mégarde une pièce jointe piégée. Suite à cette erreur, des attaquants ont pu utiliser une vulnérabilité logicielle et ont pénétré son ordinateur pour espionner les activités de l'entreprise.*

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

3

Bien connaître ses utilisateurs et ses prestataires

Noémie naviguait sur Internet depuis un compte administrateur de son entreprise. Elle a cliqué par inadvertance sur un lien conçu spécifiquement pour l'attirer vers une page web infectée. Un programme malveillant s'est alors installé automatiquement sur sa machine. L'attaquant a pu désactiver l'antivirus de l'ordinateur et avoir accès à l'ensemble des données de son service, y compris à la base de données de sa clientèle.*

4

Effectuer des sauvegardes régulières

Patrick, commerçant, a perdu la totalité de son fichier client suite à une panne d'ordinateur. Il n'avait pas effectué de copie de sauvegarde.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

5

Sécuriser l'accès Wi-Fi de votre entreprise

La borne d'accès à Internet (box) de la boutique de Julie est configurée pour utiliser le chiffrement WEP. Sans que Julie ne s'en aperçoive, un voisin a réussi en moins de deux minutes, à l'aide d'un logiciel, à déchiffrer la clé de connexion. Il a utilisé ce point d'accès Wi-Fi pour participer à une attaque contre un site Internet gouvernemental. Désormais, Julie est mise en cause dans l'enquête de police.*

6

Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur

Arthur possède un ordiphone qu'il utilise à titre personnel comme professionnel. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, l'éditeur de l'application peut accéder à tous les SMS présents sur son téléphone.

POLICE
NATIONALE

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

7

Protéger ses données lors de ses déplacements

Dans un aéroport, Charles sympathise avec un voyageur prétendant avoir des connaissances en commun. Lorsque celui-ci lui demande s'il peut utiliser son ordinateur pour recharger son ordiphone, Charles ne se méfie pas. L'inconnu en a profité pour exfiltrer les données concernant la mission professionnelle très confidentielle de Charles.

8

Être prudent lors de l'utilisation de sa messagerie

Suite à la réception d'un courriel semblant provenir d'un de ses collègues, Jean-Louis a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Jean-Louis le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

9

Télécharger ses programmes sur les sites officiels des éditeurs

Emma, voulant se protéger des logiciels espions (spyware), a téléchargé un logiciel spécialisé proposé par son moteur de recherche. Sans le savoir, elle a installé un cheval de Troie.*

10

Être vigilant lors d'un paiement sur Internet

Céline a acheté sur Internet des fournitures de bureau pour son entreprise sans vérifier l'état de sécurité du site de commerce en ligne. Ce dernier n'était pas sécurisé. Des attaquants ont intercepté le numéro de carte bancaire de l'entreprise et ont soutiré 1 000 euros.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

11

Séparer les usages personnels des usages professionnels

Paul rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de Paul. Des informations sensibles ont été volées puis revendues à la concurrence.

12

Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Alain reçoit un courriel lui proposant de participer à un concours pour gagner un ordinateur portable. Pour ce faire, il doit transmettre son adresse électronique. Finalement, Alain n'a pas gagné mais reçoit désormais de nombreux courriels non désirés.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

L'enquête judiciaire en cybercriminalité

La spécialisation et la centralisation des poursuites :
Compétence nationale de la section J3 du Parquet de Paris (OIV, RSW ...)
Désignation de services de police judiciaire coordonnateurs

Une cooperation internationale efficace
EUROPOL : apporte un soutien aux états membres de l'UE par le biais de ses capacités techniques, son soutien opérationnel, ses bases de données.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

Préserver les preuves numériques
Quelles sont les 1ères actions à mettre en place ?

Confiner | **Isoler** | **Sauvegarder** | **Collecter** | **Communiquer**

Isoler des réseaux / confiner
Contacter les services de police dés le début
Effectuer une copie de la machine infectée
Ré-installer le système d'exploitation à partir d'une version saine
Supprimer tous les services inutiles
Appliquer tous les correctifs de sécurité préconisés
Restaurer les données d'après une copie de sauvegarde non compromise
Changer tous les mots de passe

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

POLICE
NATIONALE

Pourquoi faut-il déposer plainte

Porter à la connaissance des autorités judiciaires l'existence d'un incident permet de :

- Obtenir de l'aide pour remédier à la cyberattaque,
- Identifier, interpeller et présenter les auteurs à la justice (pas de plainte = pas de preuve = pas d'enquête = par d'arrestation des cybercriminels qui peuvent continuer en toute impunité),
- Obtenir une indemnisation par son assurance (si depôt de plainte dans les 72 heures).,
- Déterminer les responsabilités, internes, externes, liées à l'attaque de façon à mettre les actions adéquates en place,
- Récupérer tout ou partie des fonds ou des données dérobés par l'action policière ou le développement d'outils spécifiques,
- Se conformer à la loi, notamment dans le cadre du RGPD de la CNIL.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

Comment alerter / déposer plainte

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

FICHE DE CONTACT
RÉSEAU DES RÉFÉRENTS CYBERMENACES DE LA POLICE NATIONALE

Vous êtes une société ?
Entreprise unipersonnelle, artisan, profession libérale, TPE/PME ?
Vous êtes victime d'une cyberattaque, d'une escroquerie utilisant Internet ou les réseaux sociaux ?

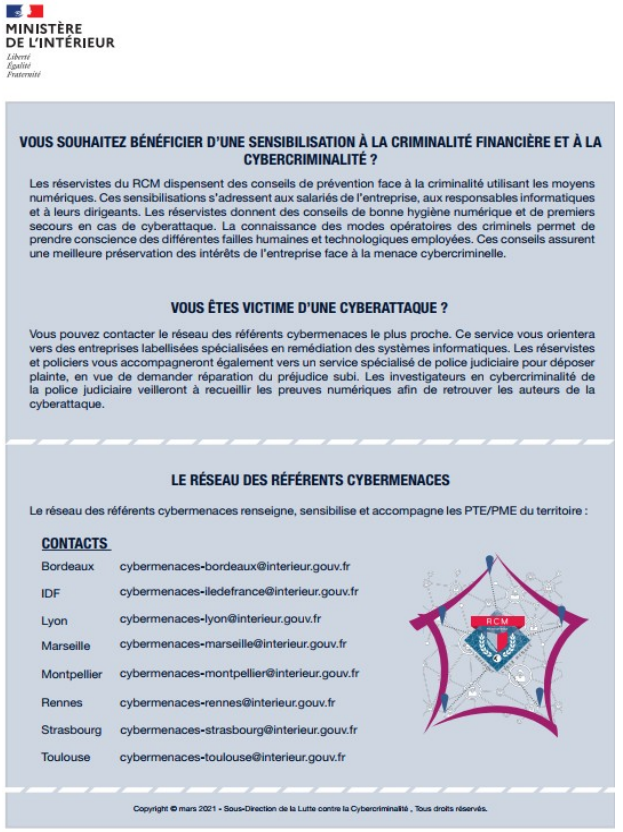
La Police judiciaire vous propose un point de contact unique pour le territoire : **Nouvelle-Aquitaine**

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 des entreprises labellisées spécialisées en remédiation des systèmes informatiques. Les réservistes et policiers vous accompagneront également vers un service spécialisé de police judiciaire 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
IDF	cybermenaces-iledefrance@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

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

RCM
POLICE NATIONALE

POLICE
NATIONALE

Qui sont les reservistes ?

Des citoyens engagés et bénévoles, ayant une expérience de l'entreprise et/ou du numérique : chef d'entreprise,responsable de la sécurité des systèmes d'information, juriste, chercheur ...

qui interviennent, sous le contrôle, et en relation étroite, avec les enquêteurs de la Police Judiciaire.

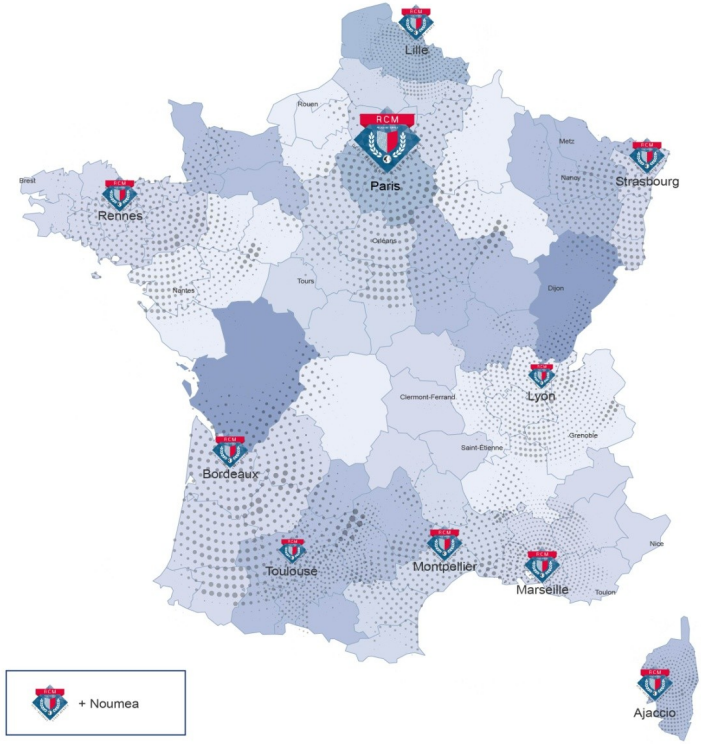
MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

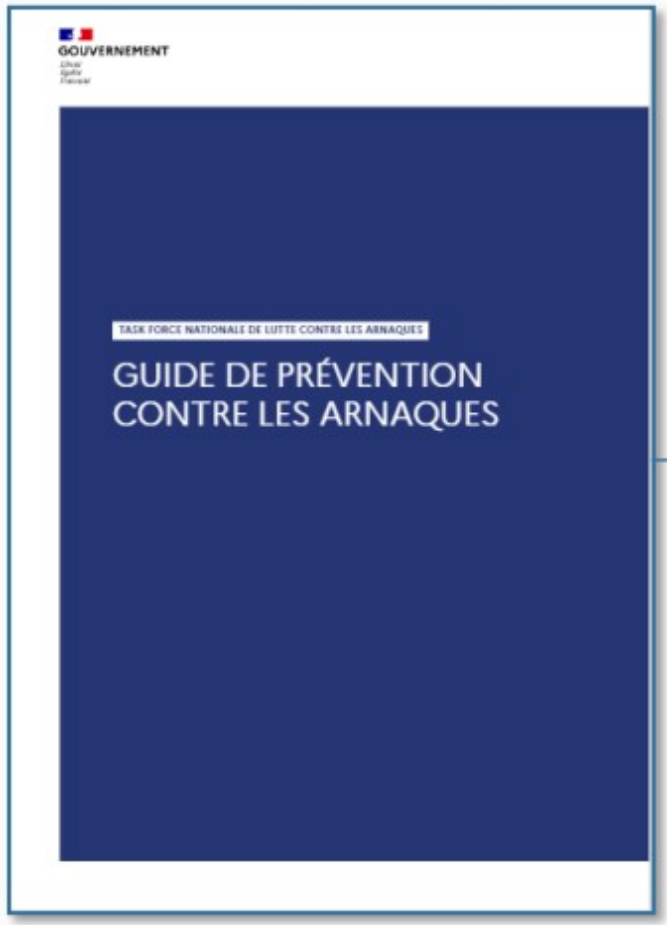
Rôle et missions des réservistes

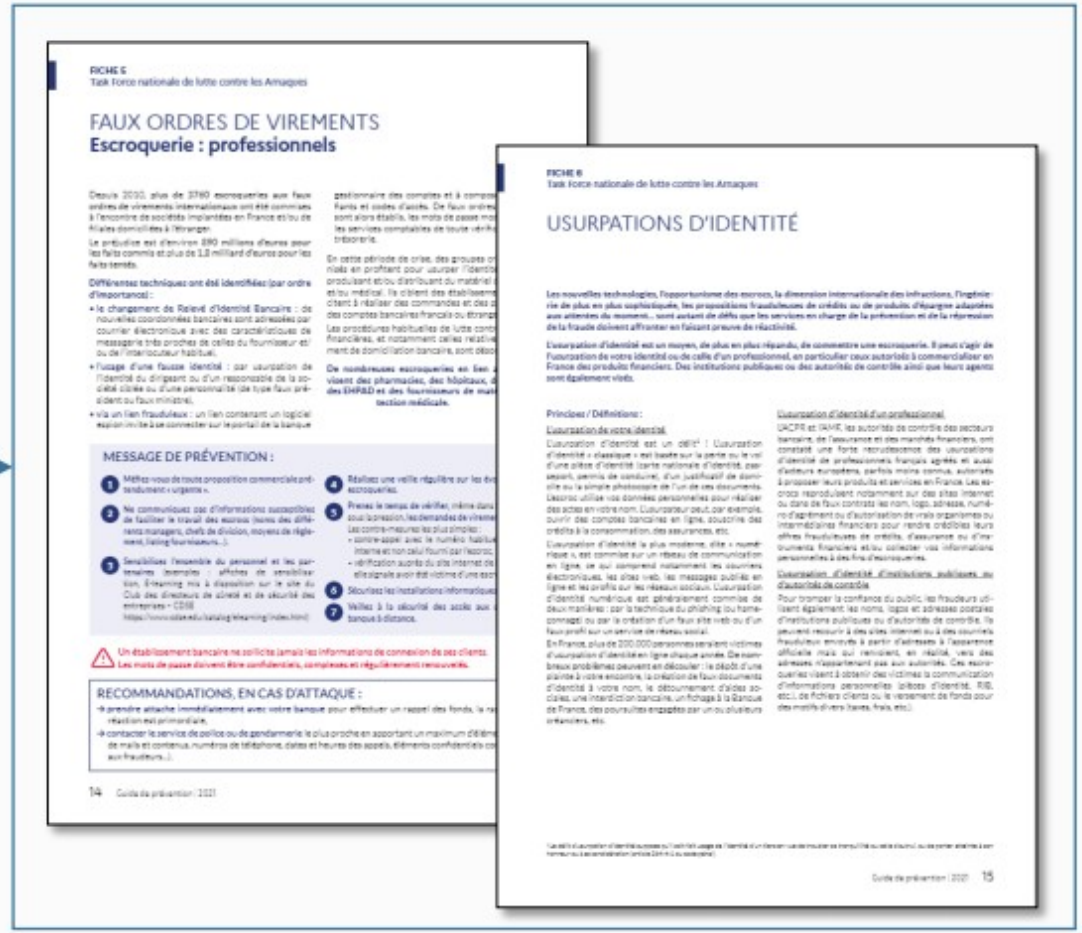
- **sensibiliser les entreprises** et structures publiques (dirigeants et collaborateurs)
- réaliser des actions de prévention et de communication
- **Conseiller et orienter** les victimes en cas d'incident cyber
- Faire remonter les alertes à la PJ



Des ressources

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





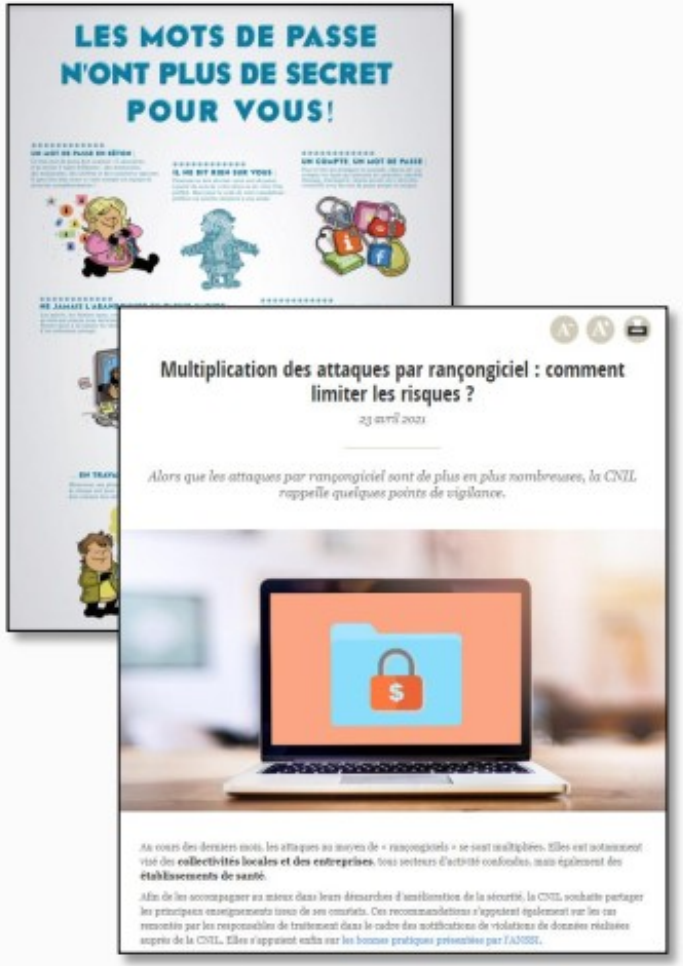
Des ressources

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