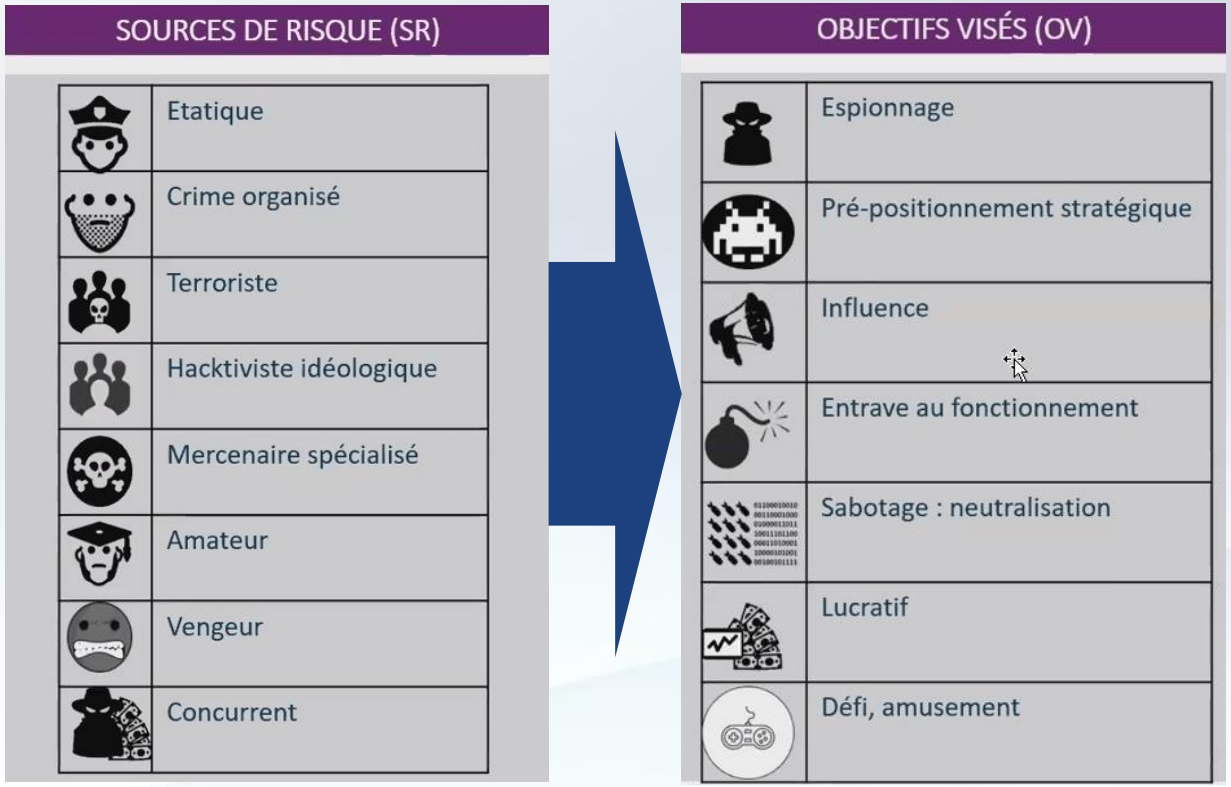
Comprendre les cyber attaques pour mieux se protéger

C’est quoi la cybersécurité ?

- La **SSI (Sécurité du Système d’Information)**, également appelée parfois **cybersécurité**, regroupe l’ensemble des moyens techniques, organisationnels, juridiques et humaines nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information. **La SSI vise à protéger l’entreprise (ses données, ses processus, ses activités….).**

- **Les principaux préjudices d’une cyberattaque:**
  - Destruction ou vol de données
  - Perte d’activité, arrêt de la production
  - Retard de livraison
  - Dégradation de l’image
  - Chomage technique
  - Sanctions financières (pénalité de retard , amende ,etc..)
  - Coût de la réparation (matériel et prestation de service)



Un point essentiel :
On sécurise l’information, pas l’informatique.

Adresse générique vs attaque avancée

Menaces génériques	
Niveau de technicité:	faible
Objectifs:	financier jeu
Nombre de cibles:	élevé à très élevé
Temps d'exécution:	court terme
Enjeux:	faible
Sphère impactée:	professionnelle et personnelle

Menaces avancées (APT)	
Niveau de technicité:	moyen à très élevé
Objectifs :	financier, int. éco, rens…
Nombre de cibles:	unitaire à groupe spécifique
Temps d'exécution:	moyen à long terme (mois)
Enjeux:	important à critiques
Sphère impactée:	quasi que professionnelle

En tant qu'entreprise, vous pouvez être victime de ces deux types d'attaque.

Comment se passe une cyberattaque avancée ?

Installation d'un logiciel malveillant

Chantage/ pression

Vol matériel

Soudoiement d'une ressource interne

Ingénierie sociale

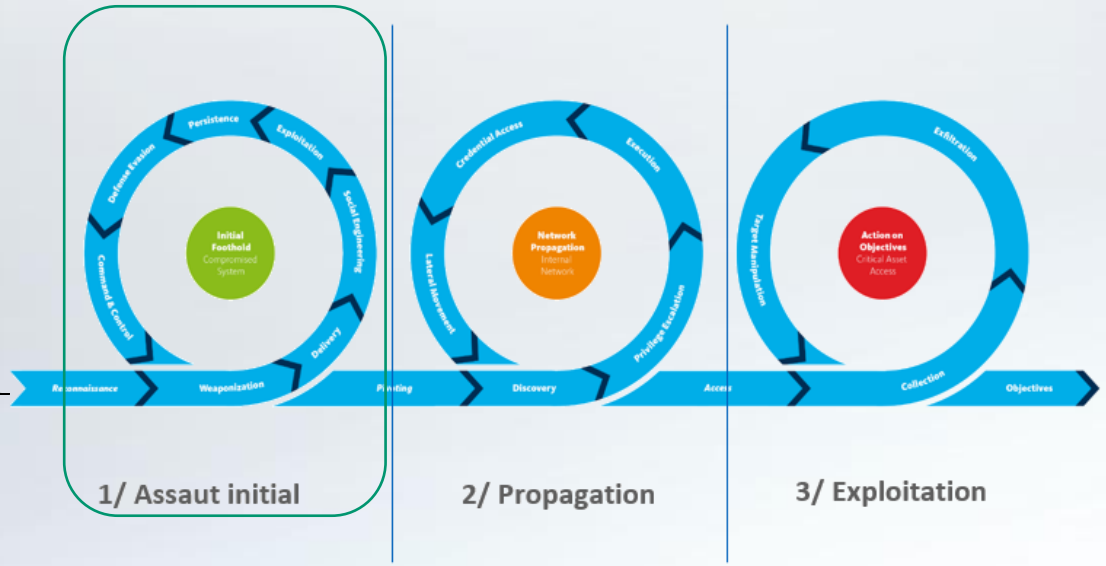
Vol d'identifiant et mot de passe

Défaut de configuration

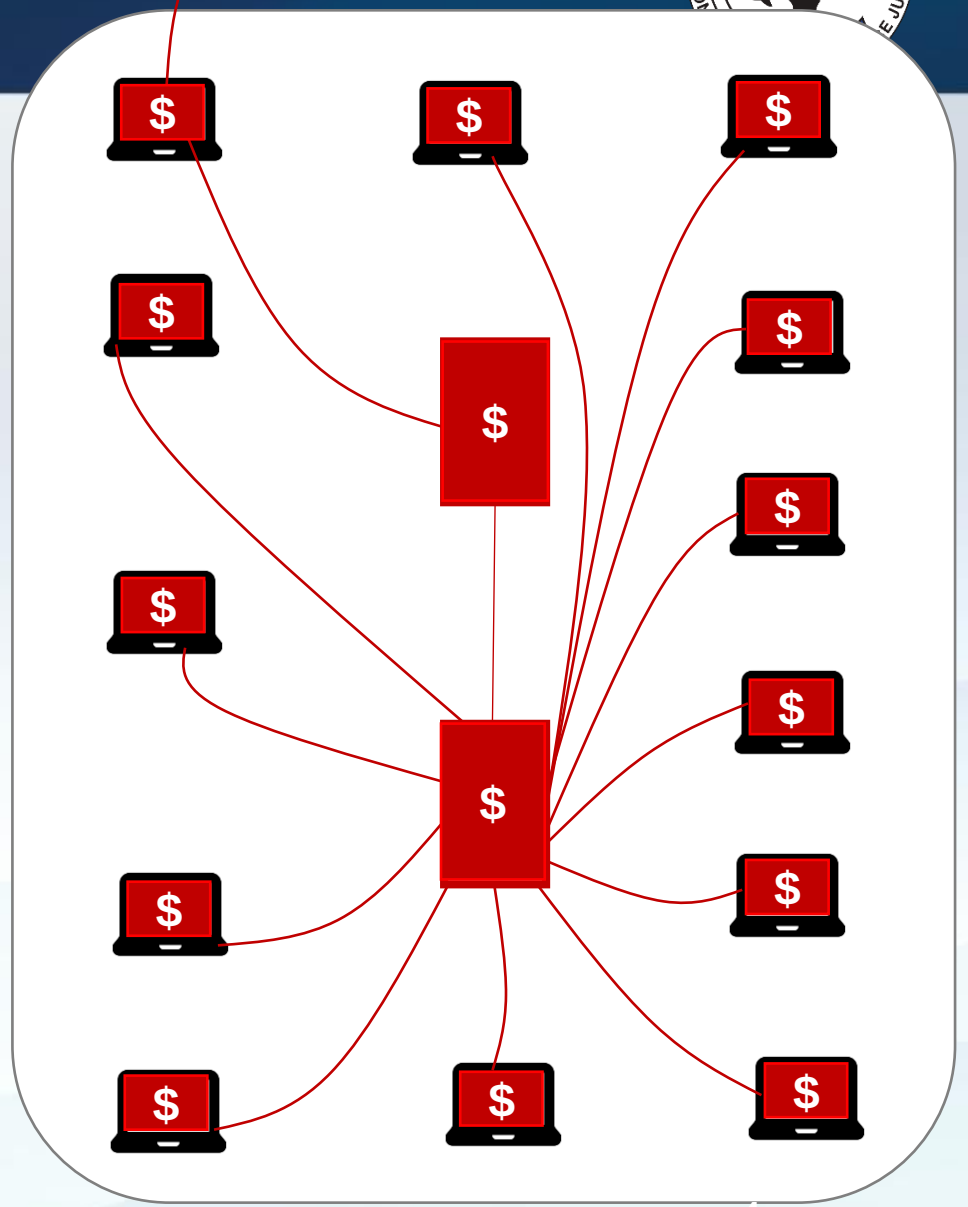
Rebond depuis un sous traitant

Phishing / spear phishing

3 étapes clés d'une cyberattaque (kill chain associée)



De quelques minutes…. à plusieurs mois pour réaliser ces 3 étapes clés.
94 jours en moyenne pour détecter une intrusion.



Un exemple de cyber attaque avancée

« **Chaque maillon de la chaîne a fait les frais de l'attaque**. Les correspondants, les rédacteurs ont dû livrer leurs articles plus tôt que d'habitude. Ensuite, les secrétaires de rédaction ont dû monter les pages dans un temps plus court.»

« On est revenu plus de vingt ans en arrière »

« J'ai été prévenu vers 4-5h du matin. L'échange était bref et anxiogène », propos du DSI

Huit personnes, des membres de la direction générale et des professionnels de la technologie, se sont regroupées au siège du journal au petit matin

« **On a dû être encore plus violent que l'attaque pour se protéger**. Ce ne sont pas des décisions faciles à prendre », propos du président du Directoire

« On se prépare à des attaques, **mais je n'avais jamais vu ça en 20 ans »** reconnaît un membre du service informatique

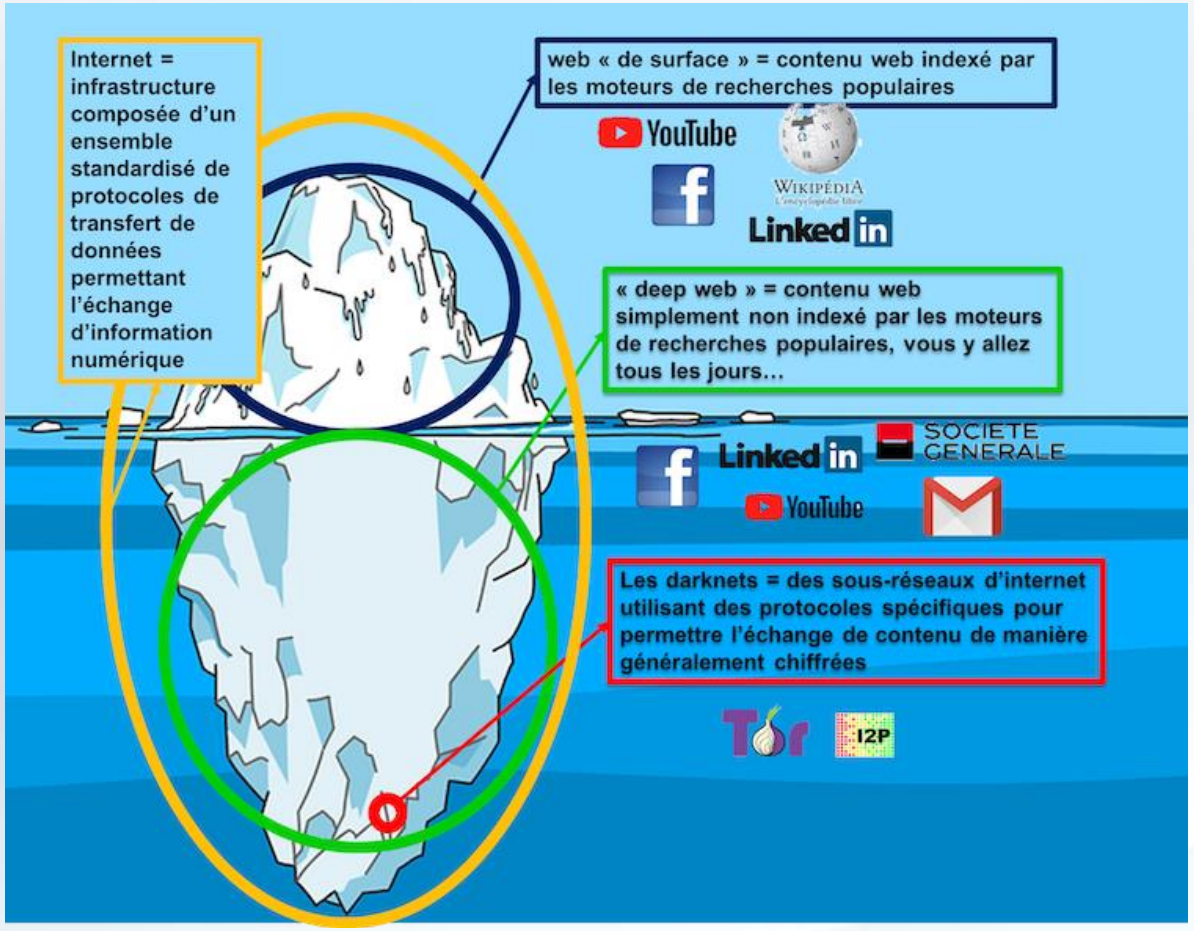
« On aura beau construire toutes les forteresses techniques sur le système d'information, **la faille pourra se situer au niveau des comportements humains** »

Deux mois plus tard, l'heure est au premier bilan:
-**Une « expérience douloureuse »,**
-**50 personnes mobilisées**
-**De nombreux coûts indirects (prime exceptionnelle de crise et 1429 heures sup)**

L'attaque a débuté par **un (simple) mail piégé avec un lien malicieux**.

Récit complet de la cyberattaque contre Ouest France disponible ici:
https://www.ouest-france.fr/societe/cyberattaque/dans-les-coulisses-de-la-cyberattaque-vecue-a-ouest-france-7139874

Une phase essentielle: la préparation



Internet, une masse quasi infinie d'information, plus ou moins accessible

DEMO

INTERNET ARCHIVE WayBackMachine

Internet, un support qui n'oublie pas

DEMO

Google Dork

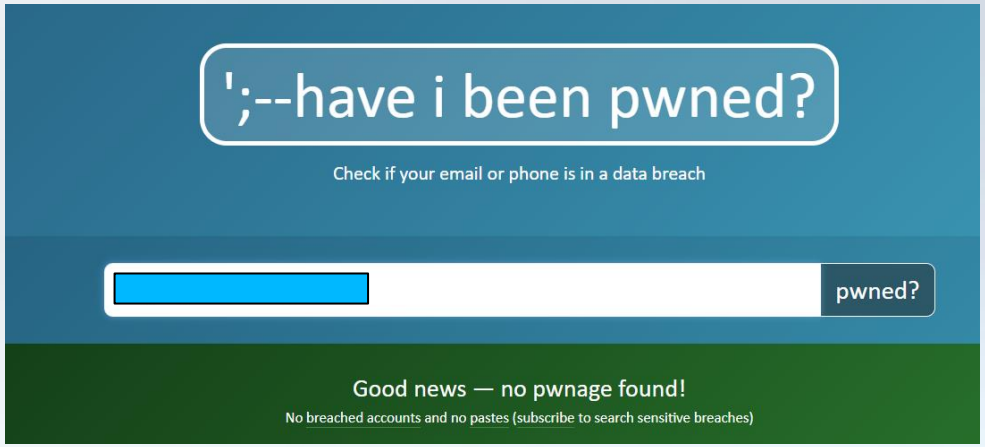
Internet, un support sur lequel on peut facilement outiller les recherches

Quelques exemples de renseignement cyber

COMBIEN DE TEMPS POUR CRAQUER VOTRE MOT DE PASSE ?

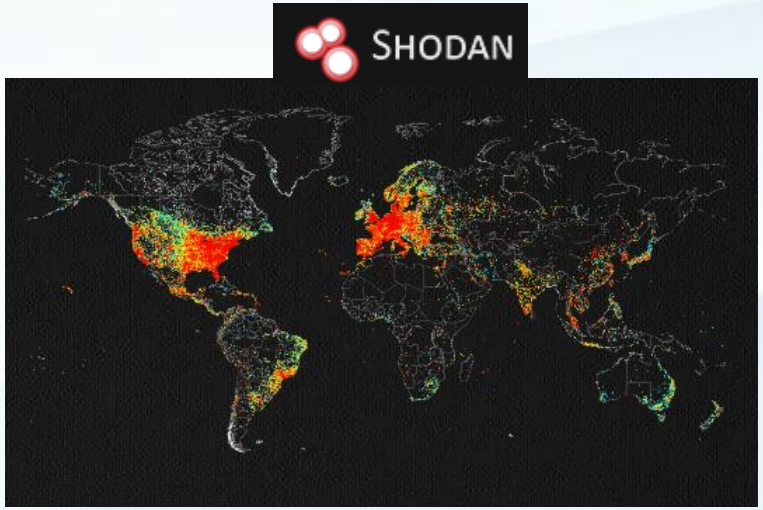
NOMBRE DE CARACTÈRES	UNIQUEMENT DES CHIFFRES	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES + CARACTÈRES SPECIAUX
4	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT
6	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	1 sec	5 sec
8	IMMÉDIAT	5 sec	22 min	1 Heure	9 Heures
10	IMMÉDIAT	58 min	1 mois	7 mois	5 ans
12	45 sec	3 semaines	300 ans	2 000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d' années	200 millions d' années

Source : SCSP / Nacime AISSANI



Casser un mot de passer n'est qu'une question de temps, qui peut être fortement réduit avec des dictionnaires.

Exemple avec « Le projet Richelieu »



Quelques règles essentielles

1. La meilleure protection est l'absence de publication. Demandez vous toujours avant de publier une donnée si celle-ci peut vous porter préjudice aujourd'hui, demain ou dans 10 ans.

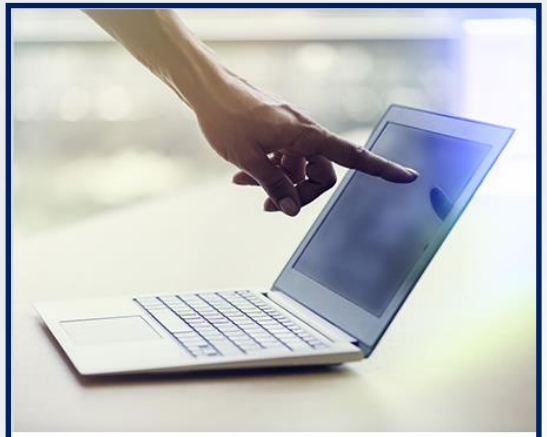
1. Adaptez votre posture à la sensibilité des données que vous traitez.

1. Vous êtes des cibles de choix, vous pouvez être victime d'attaque ciblée.

1. Dans le monde numérique, soyez conscient que tout peut être falsifié. Une saine méfiance vous permettra donc d'identifier l'immense majorité des arnaques ou tentatives d'attaque .

« Merci pour votre écoute ! »

Piratage



Escroquerie financière

Attaques internes

Intelligence économique

Rançongiciels DDOS

Faux ordres de virement, faux RIB ...

Malveillance, concurrence déloyale

Exfiltration de données Pré-positionnement

POLICE NATIONALE

Une petite revue de presse ...

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 TV7 La chaîne Tipik La chaîne Podcasts 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.

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

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

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

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

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. THEILLET/« 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
jm.desplos@sudouest.fr

Des revenus publicitaires détournés à hauteur de 30 %, une intrusion frauduleuse qui efface des données de travail et entraîne une baisse considérable du chiffre d'affaires. Fin 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

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 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 Paygrenier.

Le tribunal, présidé par Caroline Baret, *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 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'immense* chantier Euratlantique du quartier Saint-Jean-Belcier qui a vu la construction de 7 500 logements ainsi que 90 000 mètres carrés de bureau.

Car les escrocs spécialisés dans

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 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 banques 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 viré 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. »

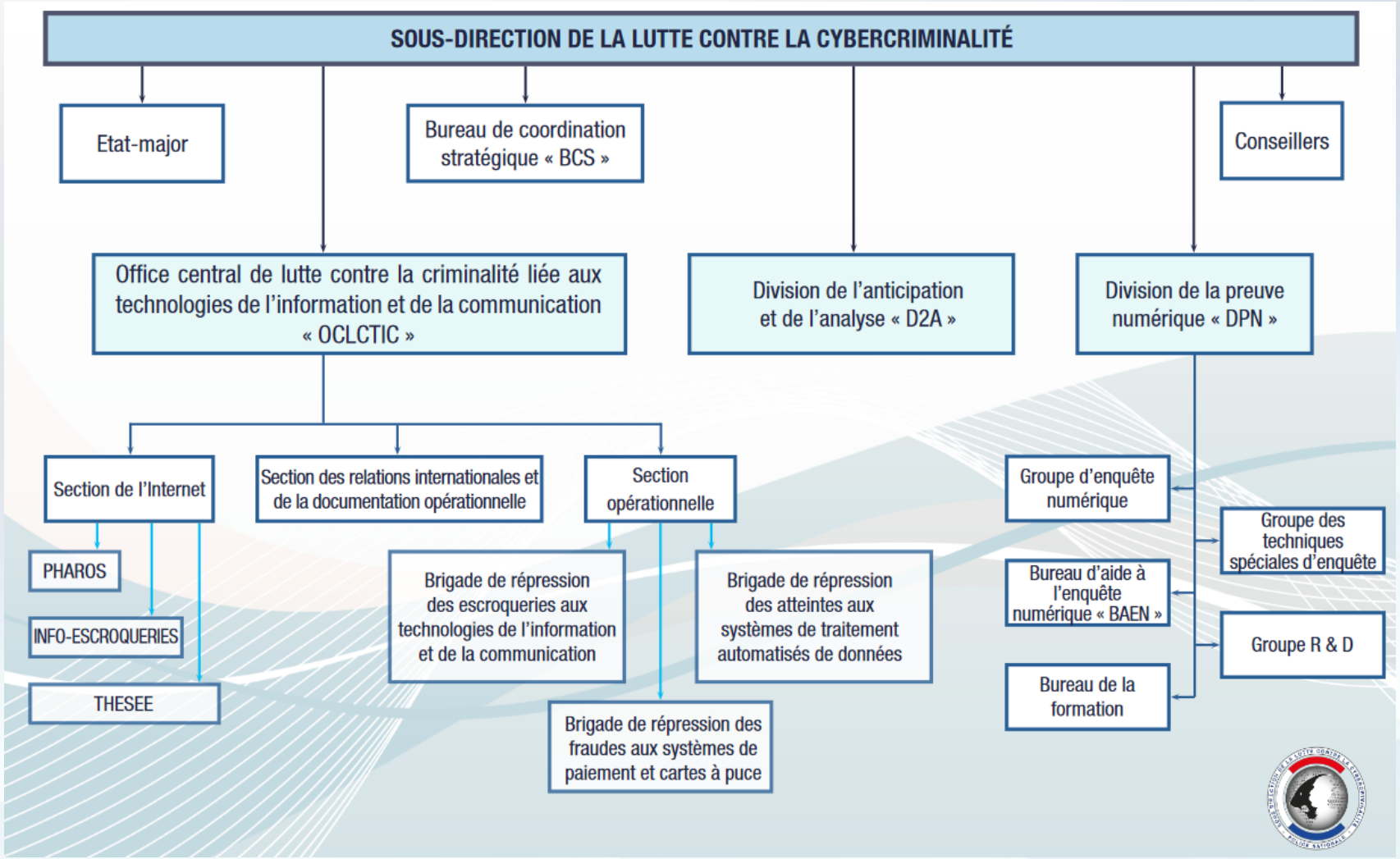
Dans le cas du promoteur immobilier bordelais, le banquier a eu le bon réflexe « toutes les entreprises, quelle que soit leur taille, sont des cibles potentielles, rappelle le commissaire. Nous les incitons à ne pas divulguer d'information stratégique sur leur site internet et suggérons à leurs collaborateurs 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. ARCHIVES S. G.

L’action de la Police Judiciaire dans la lutte contre la cybercriminalité

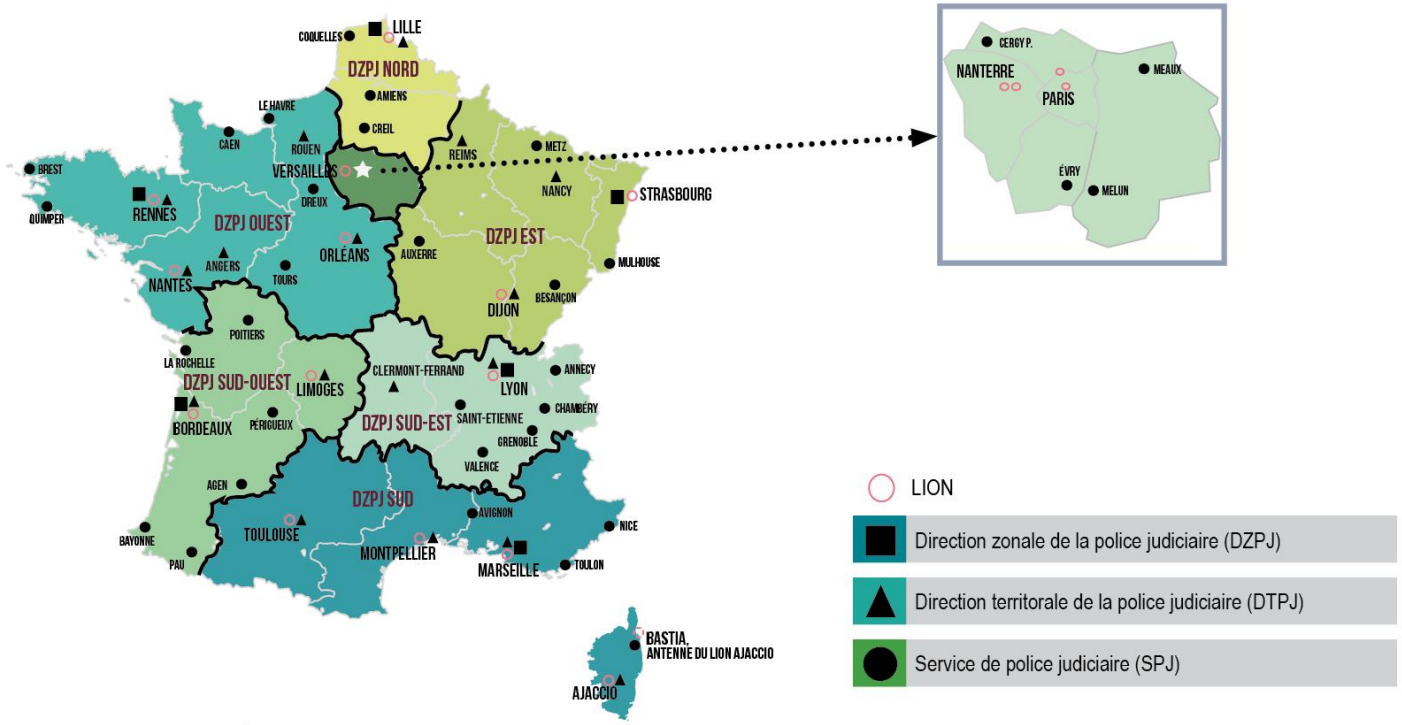
Une organisation nationale



POLICE NATIONALE

Une organisation régionale

Cartographie de l'organisation territoriale de la direction centrale de la police judiciaire et des laboratoires d'investigation opérationnelle numérique



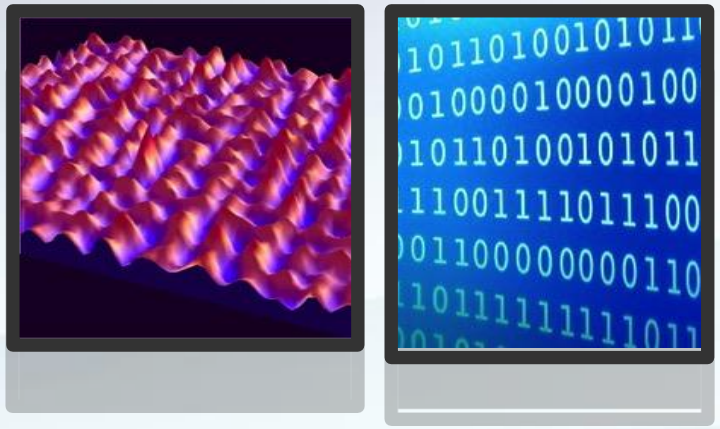
+ **DZPJ et DTPJ** à POINTE-À-PITRE
+ **SPJ** à FORT DE FRANCE

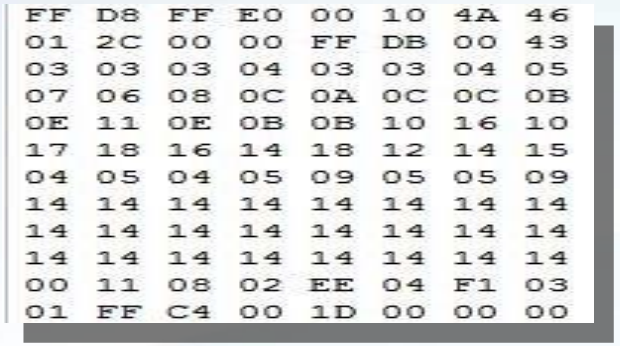
POLICE NATIONALE

Qu’est-ce que la preuve numérique ?

Toute information numérique pouvant être utilisée comme preuve dans une affaire de type judiciaire

Binaire

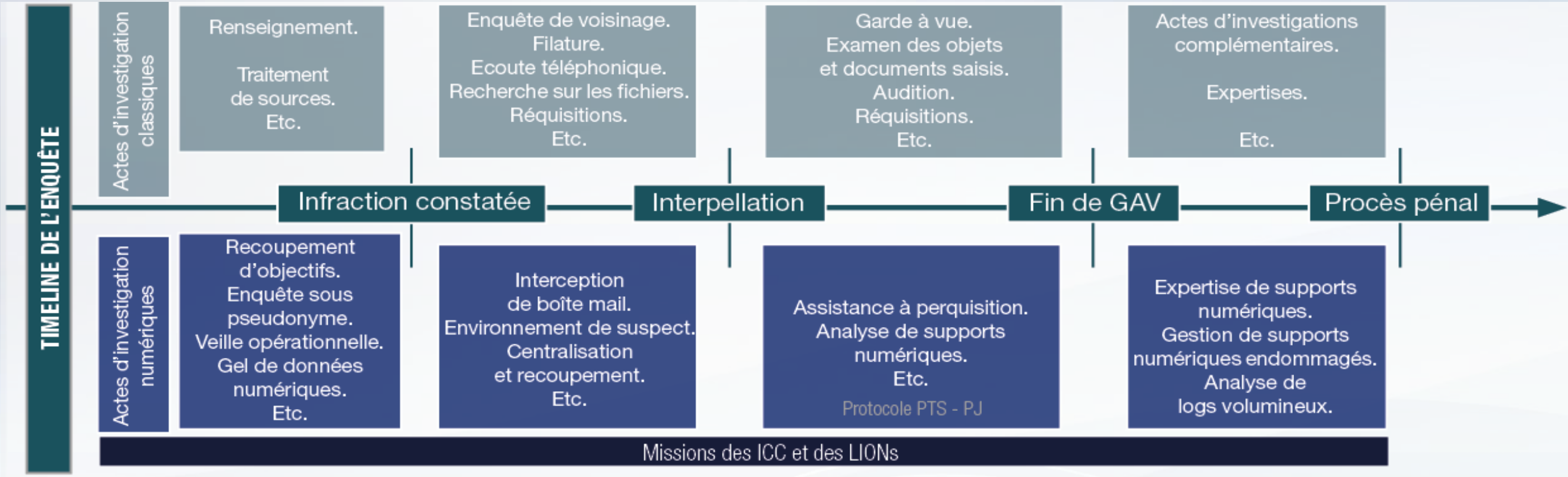




Volatile ou persistante

POLICE NATIONALE

Les techniques d'enquête en matière de cybercriminalité



POLICE NATIONALE

Sous l'autorité de

Le parquet en matière de cybercriminalité

Le Procureur de la République engage l'action publique et dirige la police judiciaire.
La technicité particulière des infractions de cybercriminalité requiert une formation particulière des magistrats du parquet et une certaine centralisation
.
La **section J3 du Parquet de Paris** a ainsi une compétence nationale :

- Lorsque les faits visent des systèmes informatiques étatiques, institutionnels et Opérateurs d'importance vitale, porteraient atteinte aux intérêts fondamentaux de la Nation.
- Lorsque les victimes sont dispersées sur l'ensemble du territoire national, en particulier pour les phénomènes massifs et sériels nécessitant une **centralisation de l'enquête** (exemple d'attaques par « rançongiciels »).
- La section J3 du Parquet de Paris est enfin compétente lorsque les informations portées à sa connaissance proviennent d'autorités policières ou judiciaires étrangères.

POLICE NATIONALE

L’enquête en cybercriminalité: un fort volet de coopération internationale

EUROJUST : Unité de coopération judiciaire pour les Etats membres de l’UE, incluant la criminalité informatique.

EUROPOL : apporte un soutien aux états membres de l’UE par le biais de ses capacités techniques, son soutien opérationnel, ses bases de données. Elle coordonne des enquêtes sur l’ensemble de l’UE, notamment dans la lutte contre la pédopornographie et la cybercriminalité avec la Joint cybercrime action taskforce (J-CAT)

INTERPOL : Service de soutien et d’expertise dans les enquêtes de criminalités internationale, et diffusion de fiches d’alerte. Cette agence met à disposition des outils de collaboration interservices étrangers sur les sujets de la cybercriminalité, de la lutte contre la pédopornographie et la criminalité financière

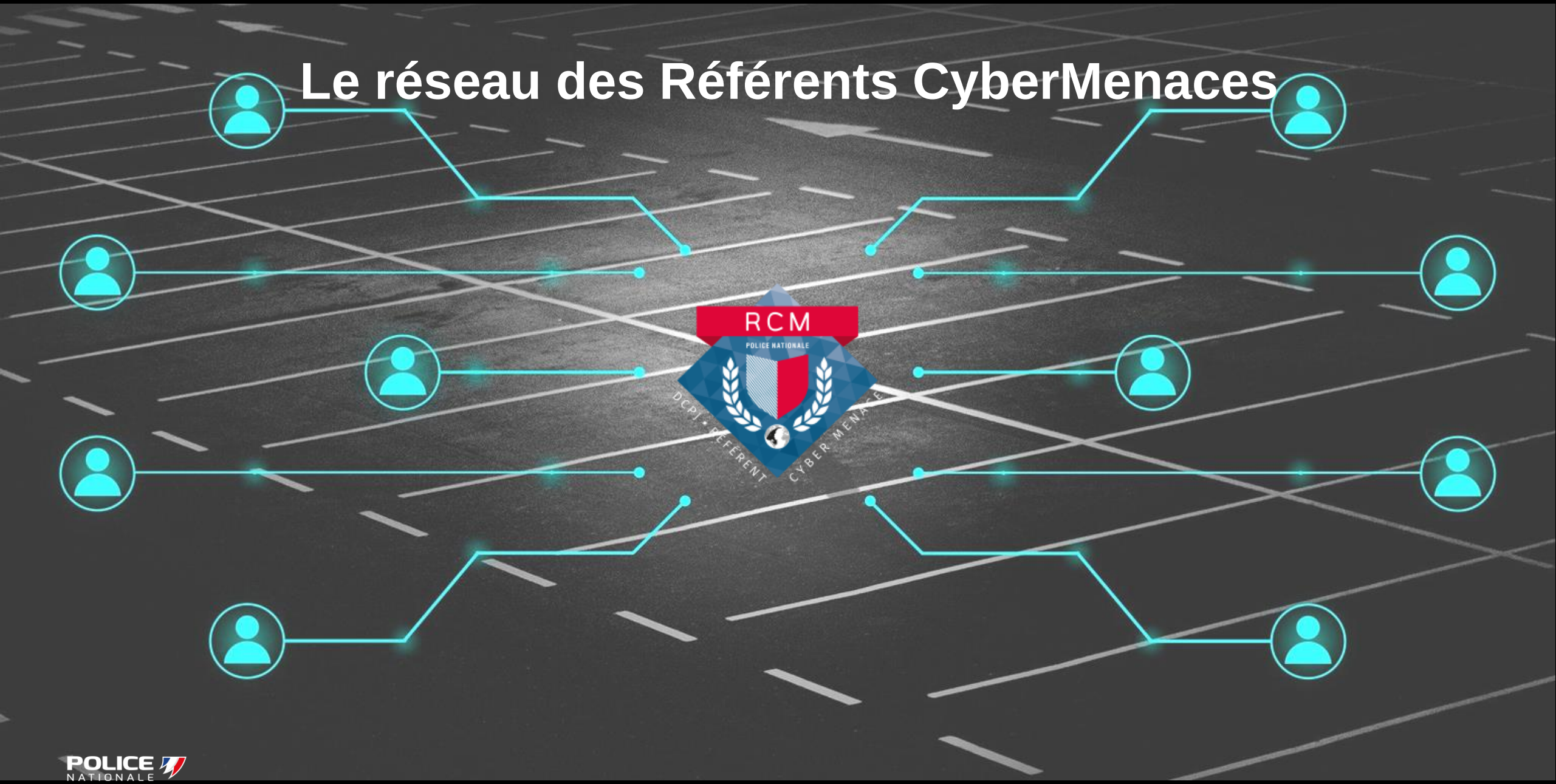
POLICE NATIONALE

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 le droit à réparation du préjudice subi en se portant partie civile,
- 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.

Le réseau des Référents CyberMenaces



POLICE NATIONALE

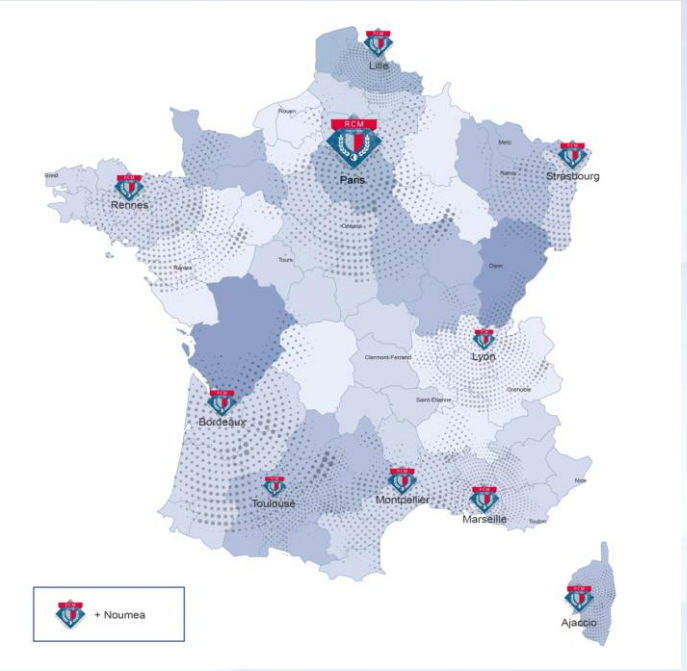
Qui sont les reservistes ?

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.

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



Comment alerter / déposer plainte ?

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 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

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


RCM
POLICE NATIONALE
DCPJ • RÉFÉRENT CYBER MENACE