MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

État actualisé de la menace et perspectives judiciaires

4èmes rencontres de la cybersécurité Nouvelle Aquitaine

24 novembre 2022

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

L'ÉTAT DE LA MENACE

Les chiffres clés en 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)*

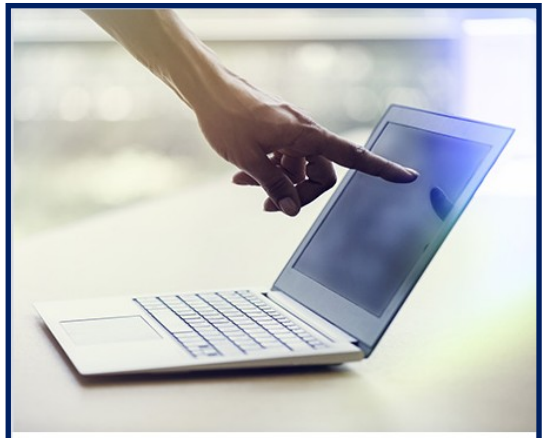
POLICE
NATIONALE

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

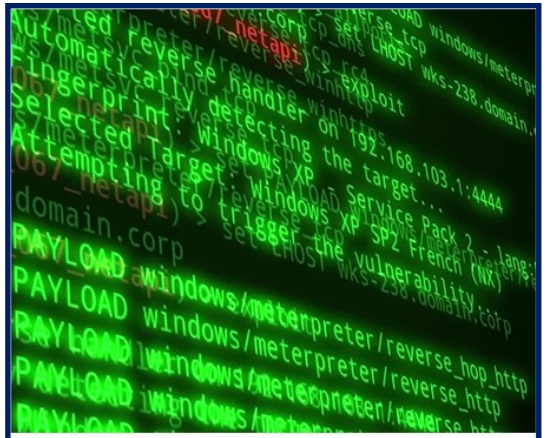
POLICE
NATIONALE

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


SUD OUEST

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.

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


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

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


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

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

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

La DCPJ en 2022

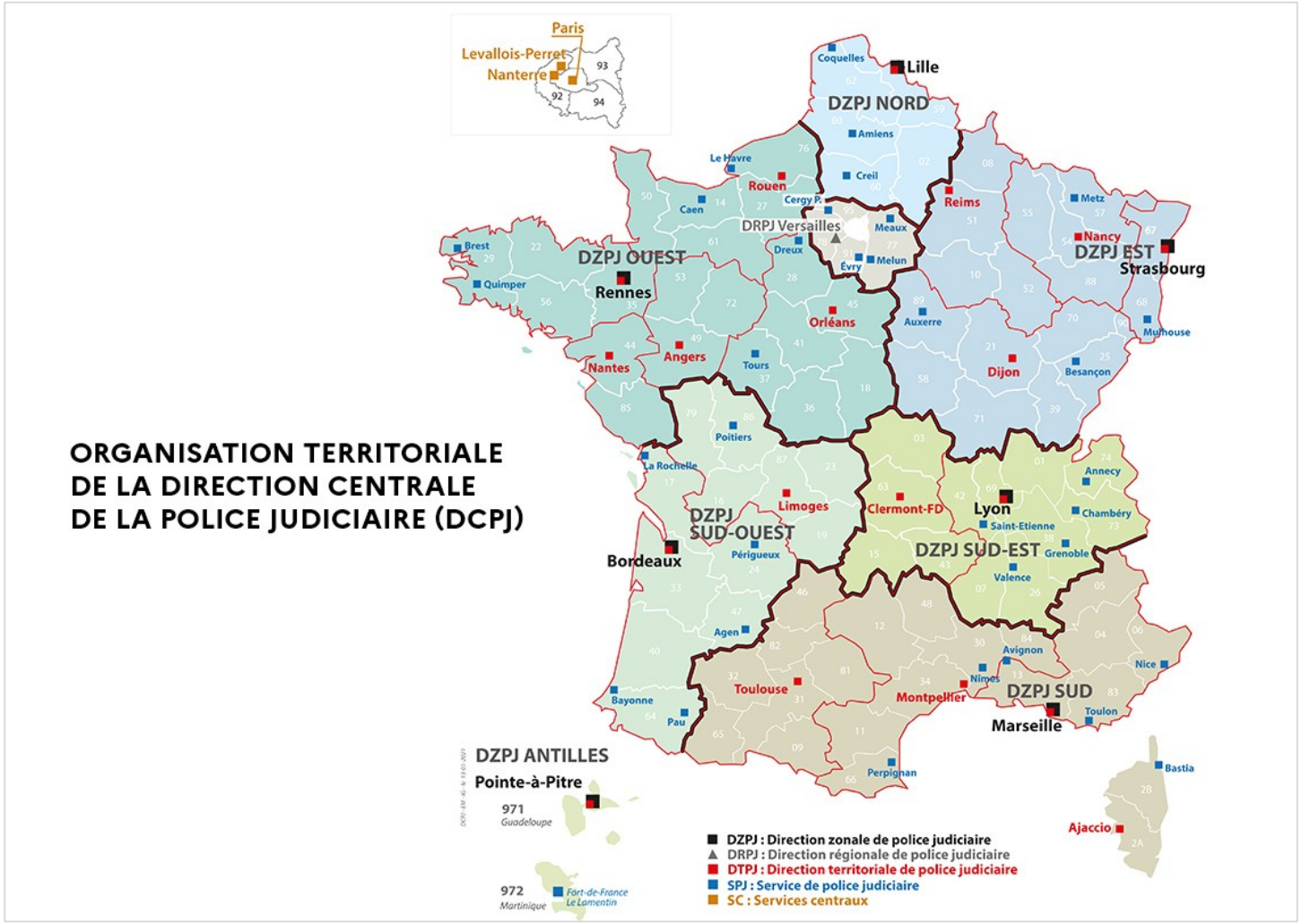
POLICE NATIONALE

STRUCTURES TERRITORIALES

5 739 personnels

En charge de la lutte contre :

- la criminalité organisée
- les formes graves et complexes de délinquance spécialisée ou transnationale
- le terrorisme
- la cybercriminalité



MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

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.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

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

MINISTÈRE
DE L'INTÉRIEUR

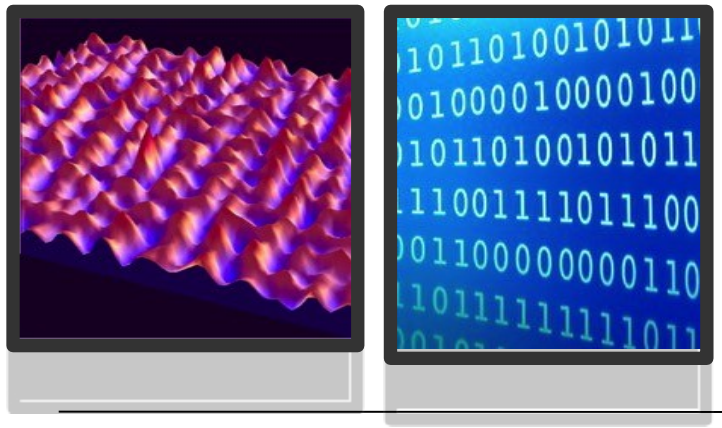
Liberté
Égalité
Fraternité

POLICE NATIONALE

Qu'est-ce que la preuve numérique ?

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

Binaire



```
FF D8 FF E0 00 10 4A 46
01 2C 00 00 FF DB 00 43
03 03 03 04 03 03 04 05
07 06 08 0C 0A 0C 0C 0B
0E 11 0E 0B 0B 10 16 10
17 18 16 14 18 12 14 15
04 05 04 05 09 05 05 09
14 14 14 14 14 14 14 14
14 14 14 14 14 14 14 14
14 14 14 14 14 14 14 14
00 11 08 02 EE 04 F1 03
01 FF C4 00 1D 00 00 00
```

Volatile ou persistante

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

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 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.

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 ?

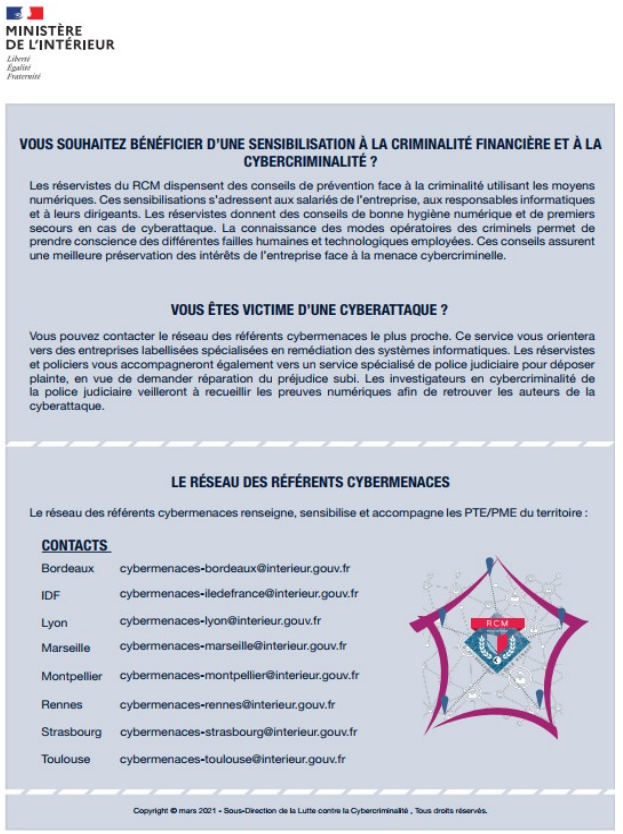
La Police judiciaire vous propose un point de contact unique pour le territoire : **Nouvelle-Aquitaine**

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

Copyright © mars 2021 - Sous-Direction de la Lutte contre la Cybercriminalité , Tous droits réservés.