MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

DNPJ
DIRECTION NATIONALE
DE LA POLICE JUDICIAIRE

POLICE
NATIONALE

ESEA
e-santé en action
NOUVELLE-AQUITAINE

CELLULE CYBERSÉCURITÉ SANTÉ
NOUVELLE-AQUITAINE

RECYM
RÉSEAU DES EXPERTS CYBER-MENACES
DE LA DIRECTION NATIONALE
DE LA POLICE JUDICIAIRE

État actualisé de la menace et perspectives judiciaires

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

RECYM

RÉSEAU DES EXPERTS CYBER-MENACES
DE LA DIRECTION NATIONALE
DE LA POLICE JUDICIAIRE

SENSIBILISATION AUX RISQUES CYBER SECTEUR SANTÉ

DU 14/12/2023

ORGANISÉ PAR PÔLE EMPLOI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Présentation des animateurs

POLICE
NATIONALE

Pierre LABORDE & Damien RIBEIRO
Réservistes Police Nationale

Damien TEYSSIER
ESEA - Nouvelle Aquitaine

Chargés de prévention cybermenaces
Direction Zonale de la Police Judiciaire de Bordeaux

DZPJ Sud-Ouest
Hôtel de Police
23 rue François de Sourdis
33062 BORDEAUX

ESEA
e-santé en action
NOUVELLE-AQUITAINE

CELLULE CYBERSÉCURITÉ SANTÉ
NOUVELLE-AQUITAINE

En cas de suspicion ou d'attaque le seul contact à retenir :

cybermenaces-bordeaux@interieur.gouv.fr

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

1. Le réseau des Experts CyberMenaces

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Réseau des référents Cybermenaces - RECYM

POLICE
NATIONALE

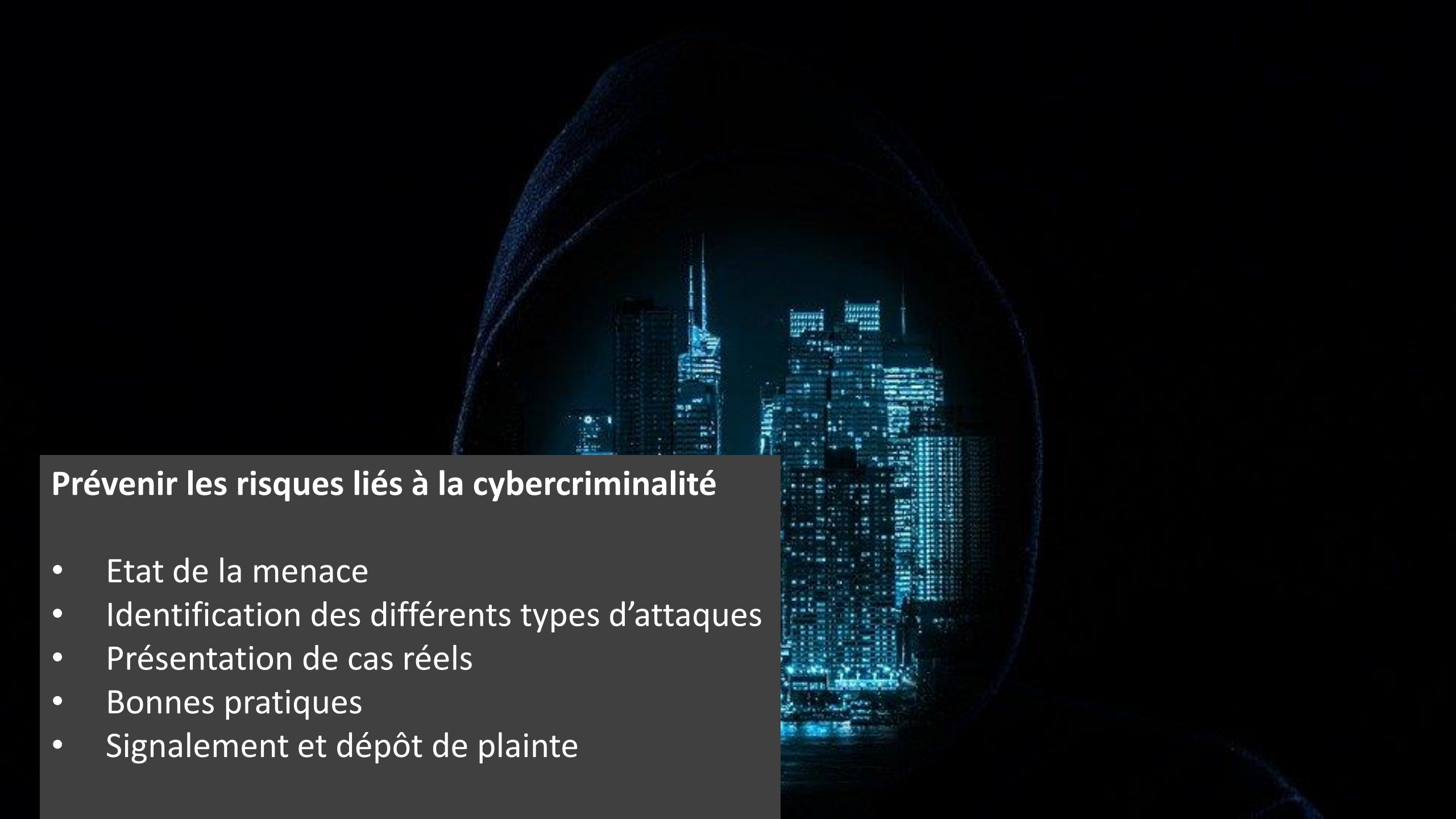
Dispositif lancé le 09 Mars 2018

Les réservistes interviennent sur 3 AXES

- Actions de sensibilisation
- Accompagnement des victimes de cyberattaques
- Une équipe déployée sur tout le territoire national

Dans le Sud-Ouest : **37** réservistes sous la supervision de la direction zonale de Police Judiciaire de Bordeaux

cybermenaces-bordeaux@interieur.gouv.fr



Prévenir les risques liés à la cybercriminalité

- Etat de la menace
- Identification des différents types d’attaques
- Présentation de cas réels
- Bonnes pratiques
- Signalement et dépôt de plainte

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE
NATIONALE

980
millions

Nombre de personnes concernées par une cyberattaque, chaque année.

MINISTÈRE DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Etat de la menace

POLICE NATIONALE

54 %

Taux des entreprises françaises attaquées en 2021

Les chiffres de la cybersécurité 2021 en France ont de quoi inquiéter. D'après le Baromètre de la cybersécurité en entreprise CESIN 2022, plus d'une entreprise française sur deux a vécu au moins une cyberattaque au cours de l'année 2021.

.

CESIN

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE
NATIONALE

+255 %

Attaques par "Ransomware"

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a constaté une **hausse de 255 % des attaques par rançongiciel** (ou ransomware) contre les organisations françaises en 2020 par rapport à 2019.

.

CERT-FR
Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE
NATIONALE

100

établissements « OSE » (Opérateurs de Services Essentiels)

ont déclaré au moins un incident de sécurité en 2022

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

CERT Santé

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE
NATIONALE

69 / 3000

Structures de santé

ayant déclaré plus de 2 incidents durant l'année 2022 sur 432 structures au total. 15 d'entre elles ont signalé au moins quatre incidents..

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

CERT Santé

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE NATIONALE

39%

Pourcentage de structures de santé

Qui ont été contraintes de mettre en place en 2022 un fonctionnement en mode dégradé du système de prise en charge des patients.

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
Liberté Égalité Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

CERT Santé

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE NATIONALE

63%

Pourcentage de structures de santé

indiquant que l'incident a eu un impact sur des données, qu'elles soient à caractère personnel, techniques ou relatives au fonctionnement de la structure..

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
Liberté Égalité Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

CERT Santé

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE NATIONALE

76

Mises en danger des patients

5 incidents ont entrainé une mise en danger patient avérée

(perte de chances vitales)

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
Liberté Égalité Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

CERT Santé

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE
NATIONALE

50K€

Coût médian d'une cyberattaque

Quand une entreprise se fait attaquer, il peut y avoir :

- Interruption du business
- Détérioration du matériel informatique
- Fuite de données nécessaire aux opérations
- Impact sur la notoriété.

C'est la somme de tous ces événements qui peut **coûter très cher** à l'entreprise qui se fait attaquer..

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE
NATIONALE

27 %

Perte moyenne du chiffre d'affaires en France

L'interruption d'un business suivant une cyberattaque a une **répercussion non négligeable sur le chiffre d'affaires annuel** l'entreprise. Le temps de remettre le système informatique en état, de récupérer les sauvegardes de données (s'il y en avait), une entreprise perd en moyenne 27 % de son chiffre d'affaires annuel. De plus, 60 % des PME attaquées ne se relèvent pas et **déposent le bilan dans les 18 mois suivant l'attaque**.

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE
NATIONALE

71 %

Des cyber attaques sont motivées financièrement.

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Etat de la menace

POLICE
NATIONALE

85 %

Des incidents de sécurité sont causés par une erreur humaine

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Pourquoi le secteur de la santé est-il visé par les cyberattaques ?

POLICE
NATIONALE

Parce que le domaine de la santé est considéré comme étant doté d'un **niveau de sécurité faible**

Parce que **ça peut rapporter beaucoup**

Parce que **la vie des patients peut être en (et un) jeu**

Parce que **les hackers n'ont pas d'éthique**

Parce qu'une **donnée de santé à un certain prix**

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

L'état de la Menace

POLICE NATIONALE

Une actualité cybercriminelle française

Le Département de Seine-Maritime parmi les 1 500 victimes d'un réseau de rançon après un piratage

Jeudi 26 janvier 2023, un important réseau de rançongiciel, un logiciel malveillant qui se sert des données personnelles volées sur un site pour les garder contre une rançon, a été démantelé. Le conseil départemental de Seine-Maritime fait partie des 58 victimes en France (entreprises ou des collectivités) qui avait porté plainte. Le réseau Hive est accusé d'avoir collecté plus de 100 millions de dollars de rançons.

Ramsay Santé encore victime d'une cyberattaque

avoir déjà subi une attaque informatique en 2019, le
de services hospitaliers Ramsay Santé a annoncé une
le intrusion dans son système d'information. Une grosse
de de rançon aurait été demandée.

Corbeil-Essonnes: le Centre hospitalier Sud Francilien visé par une cyberattaque

Cyberattaque chez Thales : le groupe de hackers a mis sa menace à exécution

Cyberattaque de Lille : les pirates ont dérobé les coordonnées bancaires des agents et des élus de la Ville

Dans une note interne diffusée vendredi 31 mars aux employés de la mairie, la Ville précise que parmi les données volées se trouvent les coordonnées bancaires des agents et des élus municipaux de Lille.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

L'état de la Menace (suite)

POLICE NATIONALE

Des réussites françaises

POLICE NATIONALE

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

L'état de la Menace (suite)

Les attaques visant les systèmes d'information

Articles du code pénal	Infractions	Exemples
323-1 al.1	Accès ou maintien, frauduleux, dans tout ou partie d'un STAD	Compromission d'un STAD tel que l'utilisation dans un réseau de machines zombies
323-1 al.2	Suite à cet accès, supprimer des données ou altérer le fonctionnement du STAD	Braquage 3.0 de banques, stations services ou plateformes d'échanges de crytptomonnaies : seront retenus l'altération du fonctionnement d'un STAD et le vol simple en BO (311-9 et s. CP)
323-2	Entraver ou fausser le fonctionnement d'un STAD	Spamming ou mail bombing : envoi massif et simultané de messages non sollicités constitutif d'une entrave Attaque par déni de service : altération du fonctionnement d'un site par saturation des requêtes
323-3	Le fait d'introduire frauduleusement des données dans un STAD, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient	L'extraction, la détention, la reproduction : correspondent au « vol » de données

POLICE
NATIONALE

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

L'état de la Menace (suite)

L'utilisation d'Internet à des fins criminelles

Les atteintes aux biens ou aux personnes commises par Internet

Articles du code pénal	Infractions	Exemples
313-1 à 313-3	Escroquerie simple ou en bande organisée ou tentative d'escroquerie	Phishing : hameçonage Fraude aux réparations informatiques
226-15	Atteinte au secret des correspondances électroniques	
312-10	Fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, la remise de fonds, de valeurs ou d'un bien quelconque	Chantage à la Webcam
312-1	Fait d'obtenir par contrainte la remise de fonds, de valeurs ou d'un bien quelconque	Une attaque par déni de service peut être constitutive s'il y a une demande de remise de fonds d'entrave au fonctionnement d'un STAD et d'extorsion

POLICE
NATIONALE

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

L'état de la Menace (suite)

L'utilisation d'Internet à des fins criminelles

Les escroqueries

Art 313-1 CP:

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.

- Escroqueries aux faux virements étrangers
- Escroqueries aux faux investissements sur le foreign exchange (FOREX)
- Escroqueries aux placements indexés sur les cryptomonnaies
- Escroqueries aux faux supports techniques
- Escroqueries à la fausse amitié (Scam romance)
- Escroquerie au RGPD
- Escroquerie au faux RIB d'employé
- Escroquerie au CV

POLICE NATIONALE

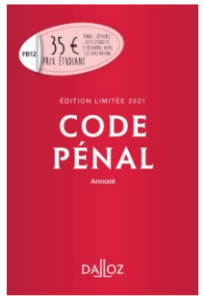
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

L'état de la Menace (suite)

L'utilisation d'Internet à des fins criminelles

Les extorsions

Art 312-1 CP:



L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque.

- Extorsions de fonds avec menace de divulgation de photos ou vidéos compromettantes
- « Sextorsion » chantage à la webcam prétendument piratée
- Extorsions de fonds avec violence lors d'un rendez-vous pris sur les réseaux sociaux

12 % des attaques ont pour conséquence un extorsion *

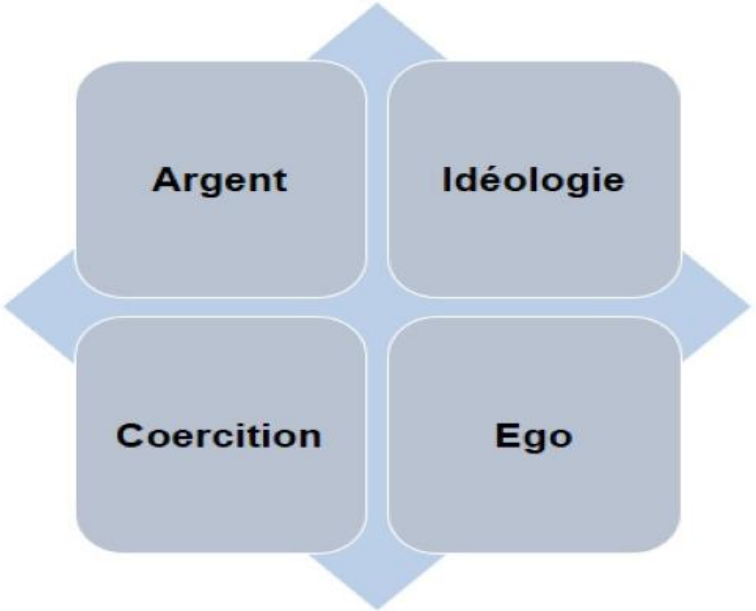
POLICE NATIONALE

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Matrice d'influence en escroquerie et ingénierie sociale sur les réseaux sociaux

POLICE
NATIONALE

Matrice MICE



+

Réseaux sociaux

Instagram

Pinterest

viadeo

LinkedIn

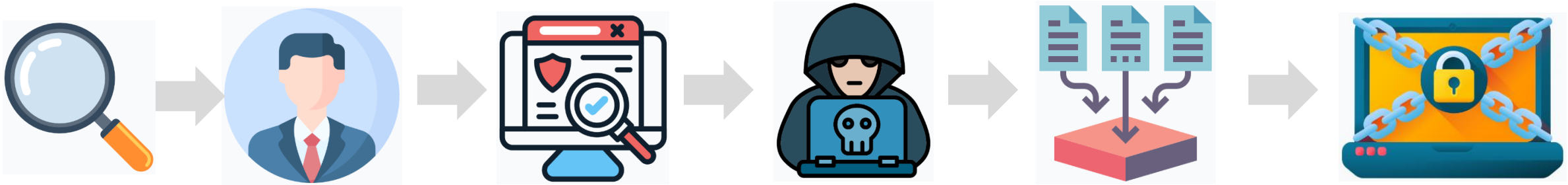
Comprendre l’attaquant
Pour mieux s’en protéger

MINISTÈRE DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Les grandes étapes d'une attaque

POLICE NATIONALE



Renseignement

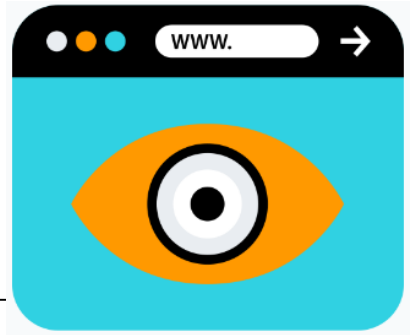
Organisation et contacts facilitateurs

Scan technique

Exploitation d'une vulnérabilité *(technique ou humaine)*

Accès et téléchargement de données

Chiffrement, demande de rançon (chantage)



Diffusion des données
sur le Darweb (forums, boutiques, sites web…)

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

L'état de la Menace (suite)

Les cybercriminels travaillent par spécialités

Les concepteurs de malware

Programmateurs expérimentés trouvant des débouchés économiques plus importantes dans la criminalité

Conçoivent seul ou en équipe les souches ou les variants de virus, vers, cheveaux de Troie, Keylogger, etc.

Ces malwares sont ensuite revendus ou loués sur des plateformes de cybercriminels, avec leur notice d'utilisation et leur tutos. Les gains sont parfois partagés avec les exploiteurs.

Les ouvreurs de portes

Modes opératoires:

• E-mail frauduleux déclenchant un petit programme d'accès furtif

• Accès réseau compromis découvert par un balayage réseau accompagné de test de mot de passe

Ces accès sont ensuite revendus sur des plateformes à d'autres cybercriminels. Les gains sont parfois partagés avec les exploiteurs

Les exploiteurs ou « moissonneurs »

Disposent d'un panel de compétences (intrusion, élévation de privilèges, latéralisation pivot, déploiement de rançongiciel, captation de mémoire vive, …)

Achètent ou louent les logiciels et les accès aux fins de monétisation. Ils peuvent de plus disposer d'informations financières afin d'ajuster le prix de la rançon dans le cas de rançongiciels. Ils diffusent même parfois quelques fichiers volés afin de d'accentuer la pression sur le paiement de la rançon.

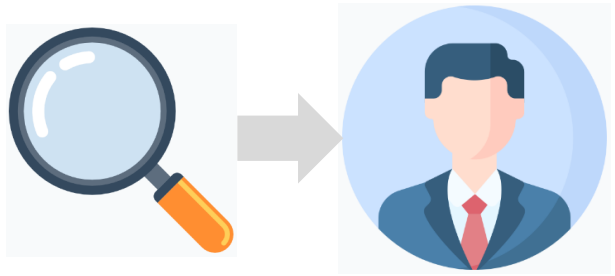
MINISTÈRE DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Les grandes étapes d'une attaque

POLICE NATIONALE

S'informer sur la cible



Renseignement

Organisation et contacts facilitateurs

Paul H
Directeur

Charlotte B
Infirmière

Marie-Gaëlle S
Secrétaire médicale

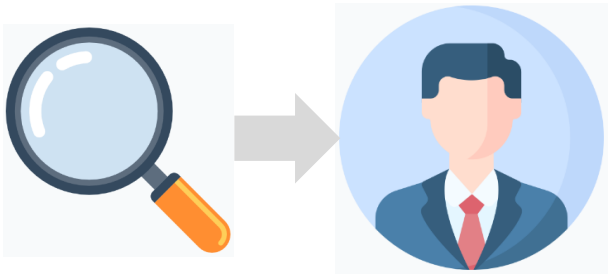
MINISTÈRE DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Les grandes étapes d'une attaque

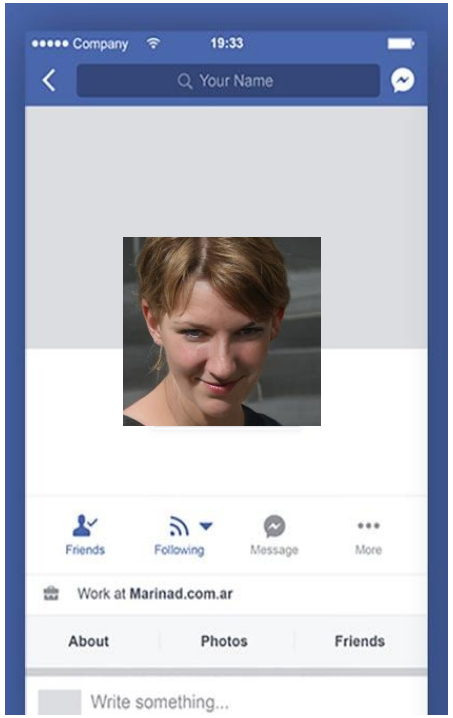
POLICE NATIONALE

S'informer sur la cible



Renseignement

Organisation et contacts facilitateurs



Analyse du profil public

- Age : 32 ans
- Ville : Pessac (33)
- Statut : Mariée à Marc F
- Famille : Sœur de Sébastien S
- Profession : Secrétaire
- 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
- …

MINISTÈRE DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Les grandes étapes d'une attaque

POLICE NATIONALE

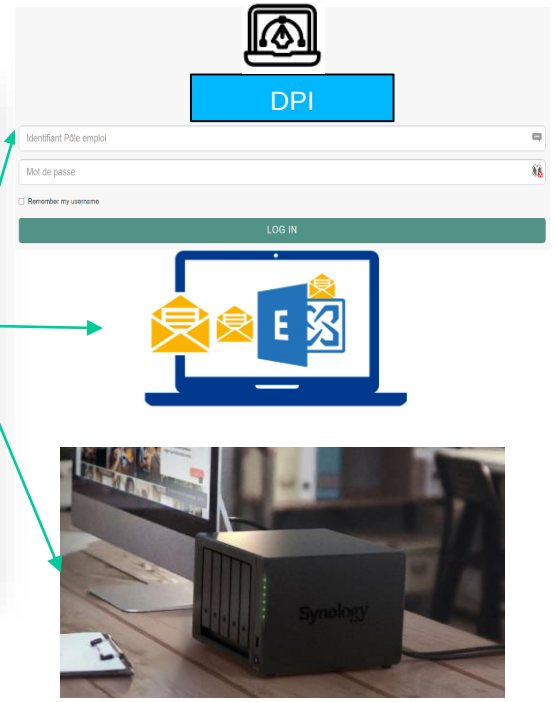
S'informer sur l'infrastructure

Scan technique

SHODAN

```
Starting Nmap 7.90 ( https://nmap.org ) at ye
Nmap scan report for site.domain (xx.xx.xx.xx
Host is up (0.15s latency).
Not shown: 89 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned i
```



Recherche d'informations techniques

Interrogation des serveurs

Découverte de services en ligne

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternit

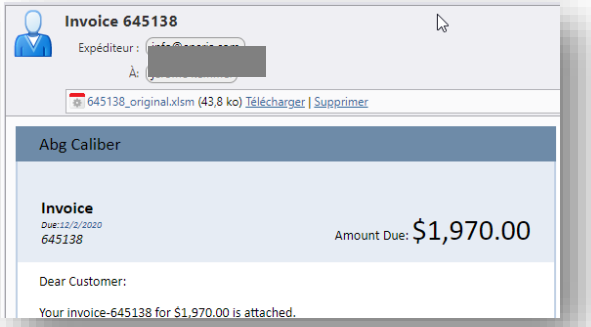
Pour quels objectifs ?

POLICE
NATIONALE

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

MINISTÈRE
DE L'INTÉRIEUR

Les autres formes d'attaques

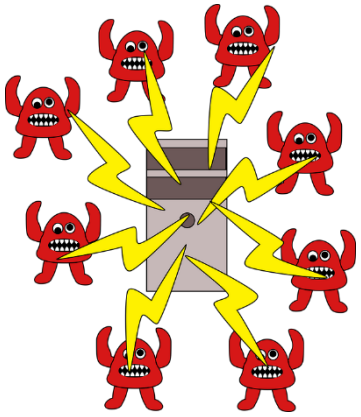
POLICE
NATIONALE

Attaque par dictionnaire
pour trouver un mot de passe

Exploitation d'une absence de M.A.J pour réussir à s'infiltrer

Attaque interne par des fournisseurs, des visiteurs, des patients…

Recherche d'informations
ouvertes et/ou oubliées



Déni de service pour paralyser les infrastructures

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Zoom l'ingénierie sociale

POLICE
NATIONALE

Manipulation psychologique

Exploite la

Vulnérabilité **humaine**

Dans un objectif

Escroquerie financière

Ou

Accès / Vol de **données**

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Zoom l'ingénierie sociale

POLICE
NATIONALE

Usurpation d'identité

Physique ou morale

Pression, émotion

De la victime

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

Doctolib Pro

Sécurité de votre compte

Bonjour,

Votre compte Doctolib semble avoir été la cible d'une connexion suspicieuse.

Détails :

- Pays : Malaysia
- Date : 17 mars 2022 à 14h51
- Système : Windows 10.5.4

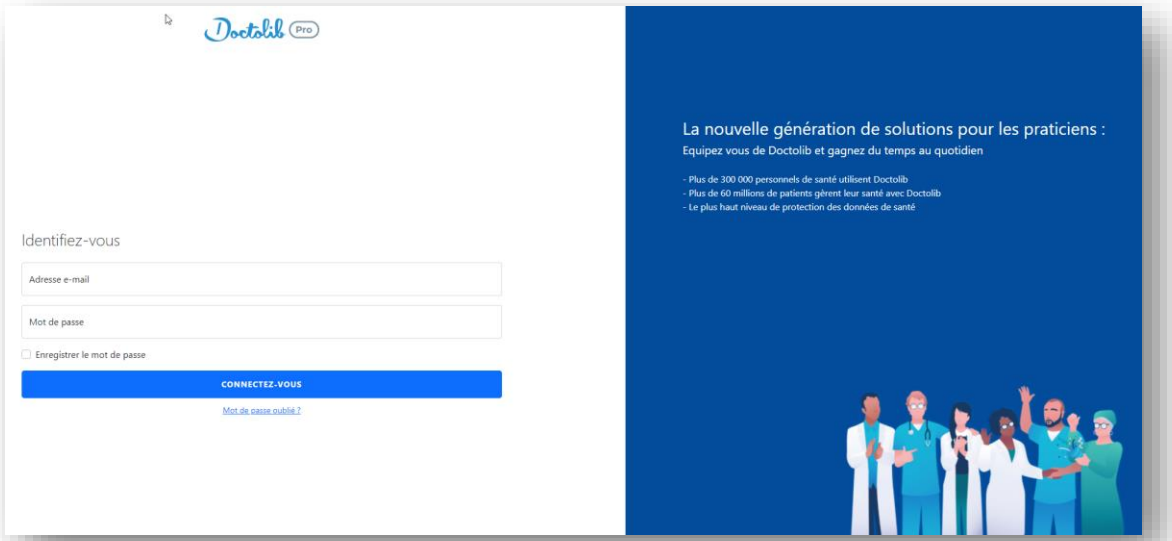
Pour des raisons de sécurité, votre compte est bloqué. Nous vous invitons à nous signaler si vous êtes à l'origine de cette action en cliquant sur l'un des bouton ci-dessous :

Il s'agit d'une connexion légitime

Je ne suis pas à l'origine de cette action

et e-mail vous a été envoyé pour vous informer de modifications importantes apportées à votre compte et aux services Google que vous utilisez.

© 2022 Doctolib



MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Les principales menaces

POLICE NATIONALE

Absence de mise à jour

Ingénierie sociale

Complexité des mots de passe

Publication des outils

Les attaques aboutissent-elles ?

Absence de vigilance / Sensibilisation

Absence de protection minimale

Séparation des usages

Connaissance de la cible

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Les sources de risques

POLICE NATIONALE

Pirate informatique

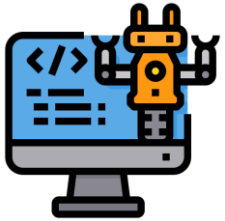
Escrocs

Bénéficiaires / Patients

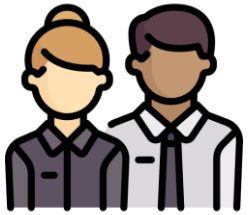
Qui peut-être à l'origine d'un incident de sécurité ?

Tiers

Sous-traitants / concurrents…



Bot's



Collaborateurs

Catastrophe naturelle

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Les conséquences

POLICE NATIONALE

Arrêt de l'activité

Perte financière / Liquidation

Difficultés juridiques / contractuelles

Quels sont les impacts ?

Pression psychologique

Notoriété / Image de marque

Confidentialité / Secret

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

Mot de passe

- Utilisez des mots de passe « complexes »
- Protégez vos mots de passe (ne pas les afficher dans un salle commune)
- N'enregistrez pas vos mots de passe sur les navigateurs (Chrome, Firefox…)
- N'enregistrez pas vos mots de passe sur votre ordinateur (Word, Excel…)
- Utilisez la double authentification lorsque cela est possible
- Désactivez les comptes des anciens collaborateurs

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

- Effectuez les MAJ recommandées
- Effectuez les MAJ de sécurité (téléphone, ordinateurs…)

- Installez un Antivirus sur l'ensemble de vos appareils (PC, téléphone, serveurs…)
- Effectuez la MAJ de ces antivirus (base virale et logiciel)

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

- N'affichez pas (ne transmettez pas) les mots de passe Wifi de votre réseau
- Evitez l'utilisation des réseaux publics

- Utilisez des supports amovibles dédiés à votre activité professionnelle
- Séparez les usages vie privée / vie professionnelle
- Ne chargez pas vos smartphones sur les ordinateurs professionnels

- Effectuez régulièrement des sauvegardes des données les plus sensibles
- Testez vos sauvegardes


Focus cas réels
Focus sur le RIB

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Les symptômes d'un système infecté

POLICE
NATIONALE

Signaux faibles

- Ralentissement du système
- Connexions ou activités inhabituelles
- Impossibilité de se connecter à la machine
- Services ouverts non autorisés

Signaux forts

- Fichier(s) disparu(s) ou chiffré(s), inaccessible(s)
- Modification du coffre-fort de mots de passe
- Messages de rançon
- Création ou destruction de comptes utilisateurs
- Envoi de mails de votre part

MINISTÈRE DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Comment réagir ?

Les gestes de premiers secours

POLICE NATIONALE

Isoler

***Ne pas éteindre** les postes infectés mais couper tous les accès réseaux*

Confiner

Mettre en quarantaine les postes infectés et les supports amovibles

Conserver

Les journaux d'activité, docs, emails, fichiers, trafic réseau + copie des supports / acquisition mémoire vive

Communiquer

Auprès des collaborateurs, des fournisseurs, banque… pour éviter le surincident

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité

Comment réagir ?

Communiquer

POLICE
NATIONALE

- Aux personnels de l'entreprise les recommandations adaptées à la gestion de l'incident
- A la CNIL lorsqu'il s'agit d'une violation de données à caractère personnel dans les 72h (RGPD)
- Aux personnes concernées par la violation des données à caractère personnel (RGPD)

CNIL.

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Comment réagir ?

Déposer plainte

POLICE
NATIONALE

Pourquoi déposer plainte ?

- Parce que vous êtes victime !
- Pour se protéger (ex. : usurpation d'identité)
- Pour faire valoir ses droits (auprès des banques, de l'assurance…)
- Pour permettre *(dans certains cas)* le blocage des fonds
- Pour contribuer aux enquêtes de Police (regroupement d'affaires similaires…)

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Comment réagir ?

Déposer plainte

POLICE
NATIONALE

Quand et comment déposer plainte ?

- Prendre contact **immédiatement** avec la Police Judiciaire par l'adresse mail : **cybermenaces-bordeaux@interieur.gouv.fr**
- Possibilité d'effectuer une **pré-plainte en ligne** : **https://www.pre-plainte-en-ligne.gouv.fr**
- Prise de plainte sur rendez-vous, avec les documents nécessaires, en présence *(si possible)* du responsable informatique

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Comment réagir ?

Déposer plainte

POLICE
NATIONALE

- Pour les personnes morales : les mandataires sociaux ou les titulaires d'une délégation de pouvoir
- Auprès d'un service de police spécialisé dans la cybercriminalité (LION, SDLC)
- Plainte avec constitution de partie civile

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Comment réagir ?

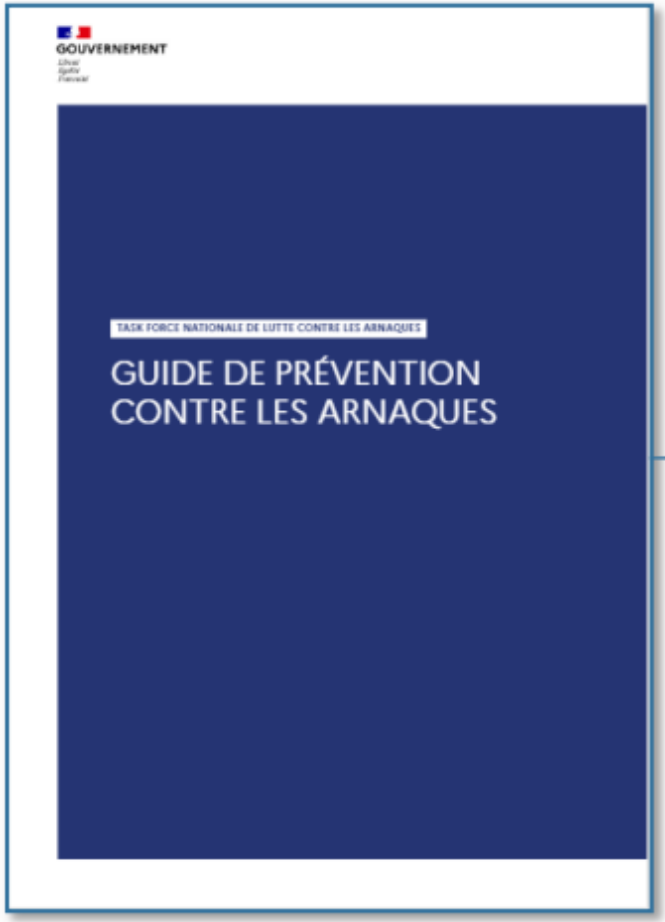
Quels documents pour déposer plainte

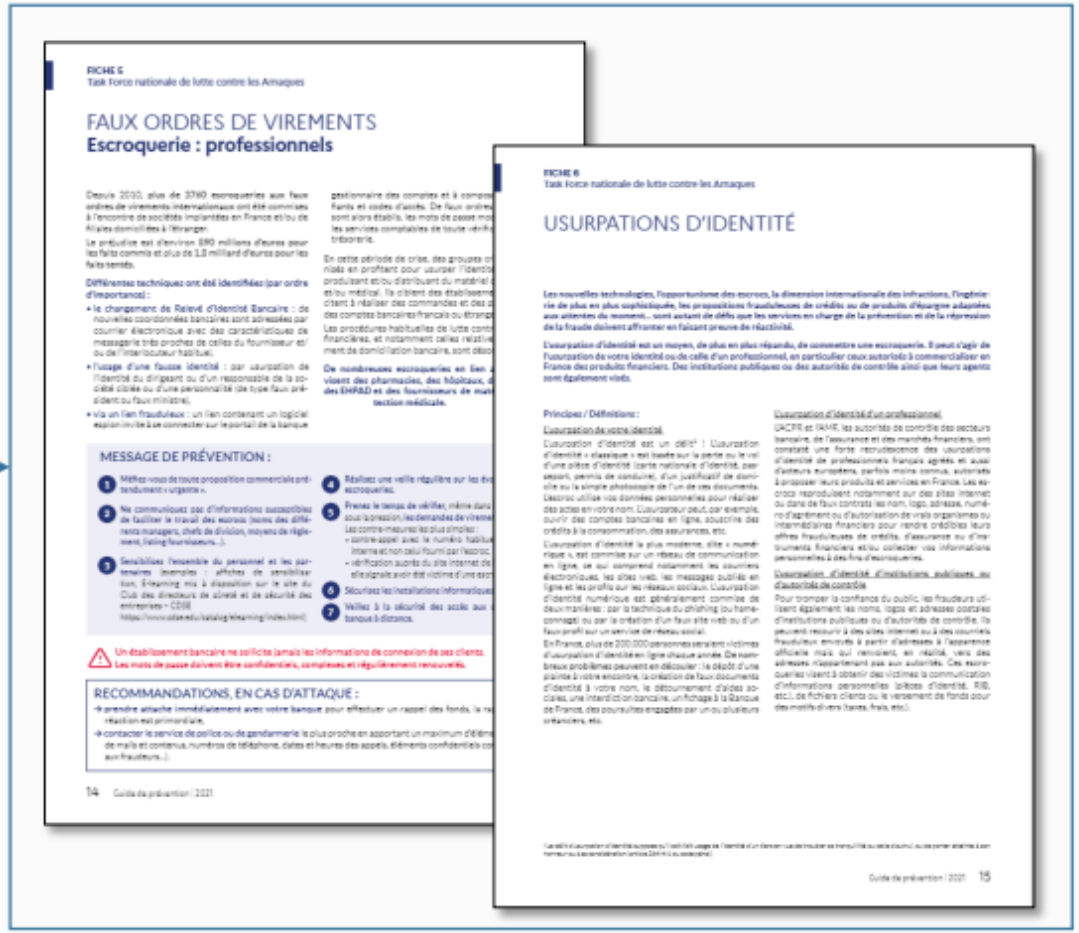
POLICE NATIONALE

- Descriptif précis de l'incident (périmètre de l'incident, contexte)
- Coordonnées de l'ensemble des intervenants ou prestataires susceptibles d'apporter des informations aux enquêteurs
- Eléments techniques : logs de connexions, adresse des machines infectées (ordinateurs, serveurs), données réseaux
- Architecture du réseau
- Les mails en lien avec l'infraction et les copies d'écran

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

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

- Signaler un courriel malveillant : www.signal-spam.fr

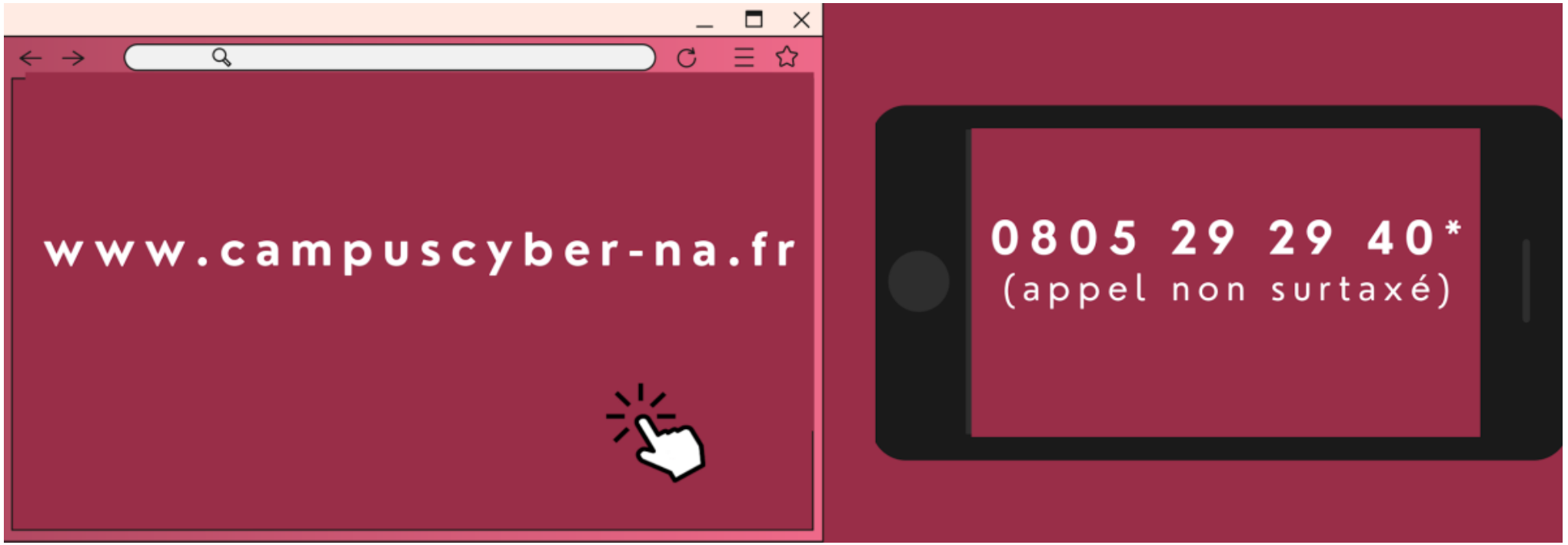
- Signaler une adresse URL de phishing : www.phishing-initiative.fr

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE
Nouvelle-Aquitaine

POLICE NATIONALE



MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

POLICE
NATIONALE

ESEA
e-santé en action
NOUVELLE-AQUITAINE

CELLULE CYBERSÉCURITÉ SANTÉ
NOUVELLE-AQUITAINE