SENSIBILISATION AUX
RISQUES CYBER

28 mars 2023

Présentation des **Animateurs**

Direction Zonale de la Police
Judiciaire de Bordeaux
DZPJ Sud-Ouest
Hôtel de Police
23 rue François de Sourdis
33062 BORDEAUX

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

cybermenaces-bordeaux@interieur.gouv.fr

Pierre LABORDE
Réserviste Police Nationale
Commandant Divisionnaire

Mathieu EPAULARD
Réserviste Police Nationale
Dirigeant société
sécurité informatique

Réseau des référents Cybermenaces

RCM

- Dispositif lancé le 09 Mars 2018
- **But du RCM** : **sensibiliser** le tissu économique local aux risques cyber et apporter un **premier niveau d'assistance** aux victimes
- Composé **d'enquêteurs de PJ** et de **réservistes** du secteur privé ou public
- **Dans le Sud-Ouest : 30** réservistes sous la supervision de la direction zonale de Police Judiciaire de Bordeaux

Point de contact pour les entreprises en Nouvelle-Aquitaine :

cybermenaces-bordeaux@interieur.gouv.fr

POLICE NATIONALE

PLAN

1 Etat de la menace

2 Identification des différents types d'attaques

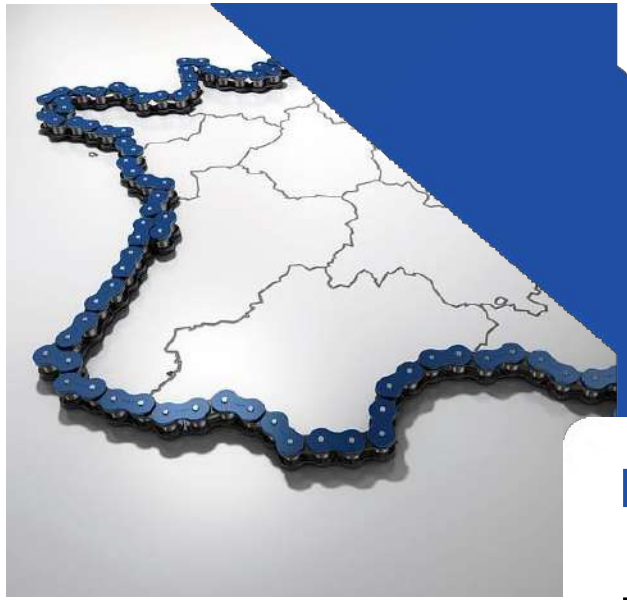
3 Présentation de cas réels

4 Bonnes pratiques

5 Signalement et dépôt de plainte

Évolution de la criminalité organisée **depuis 20 ans**

POLICE NATIONALE



Historique…

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

Actuel

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

Il s'agit de **cybercriminalité** et de **vrais criminels** .

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.

Toutefois, il est difficile de définir qui se cachent derrière le vol massif de données

POLICE NATIONALE

POLICE NATIONALE

Les intentions Criminelles

Le profit

Phishing,
Ransomware (rançogiciels)
Jackpotting, ...

L'atteinte à l'image

DDoS, Défacement

L'espionnage

Attaque par point d'eau /
Spearphishing

Le sabotage

Les droits d'auteur ne portent pas sur le NFT mais sur l'œuvre originale sous-jacente

Quelques **chiffres**

71%

Des cyber-attaques
sont motivées financièrement

Source : Verizon

POLICE NATIONALE

Quelques **chiffres**

POLICE NATIONALE

85%

Des incidents de sécurité sont causés par une erreur humaine

Source : Verizon

Quelques **chiffres**

94%

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

Source : Verizon

POLICE NATIONALE

Comprendre l’attaquant
Pour mieux s’en protéger

L'exploitation d'une **vulnérabilité humaine**

Ou « Ingénierie sociale »

Manipulation psychologique

Exploite la

Vulnérabilité **humaine**

Dans un objectif

Escroquerie financière

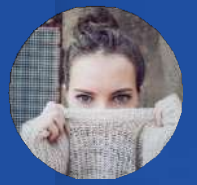
Ou

Accès / Vol de **données**

L'ingénierie sociale :
les 2 principaux ingrédients

POLICE NATIONALE

Exemple d'attaque



Usurpation d'identité
Physique ou morale

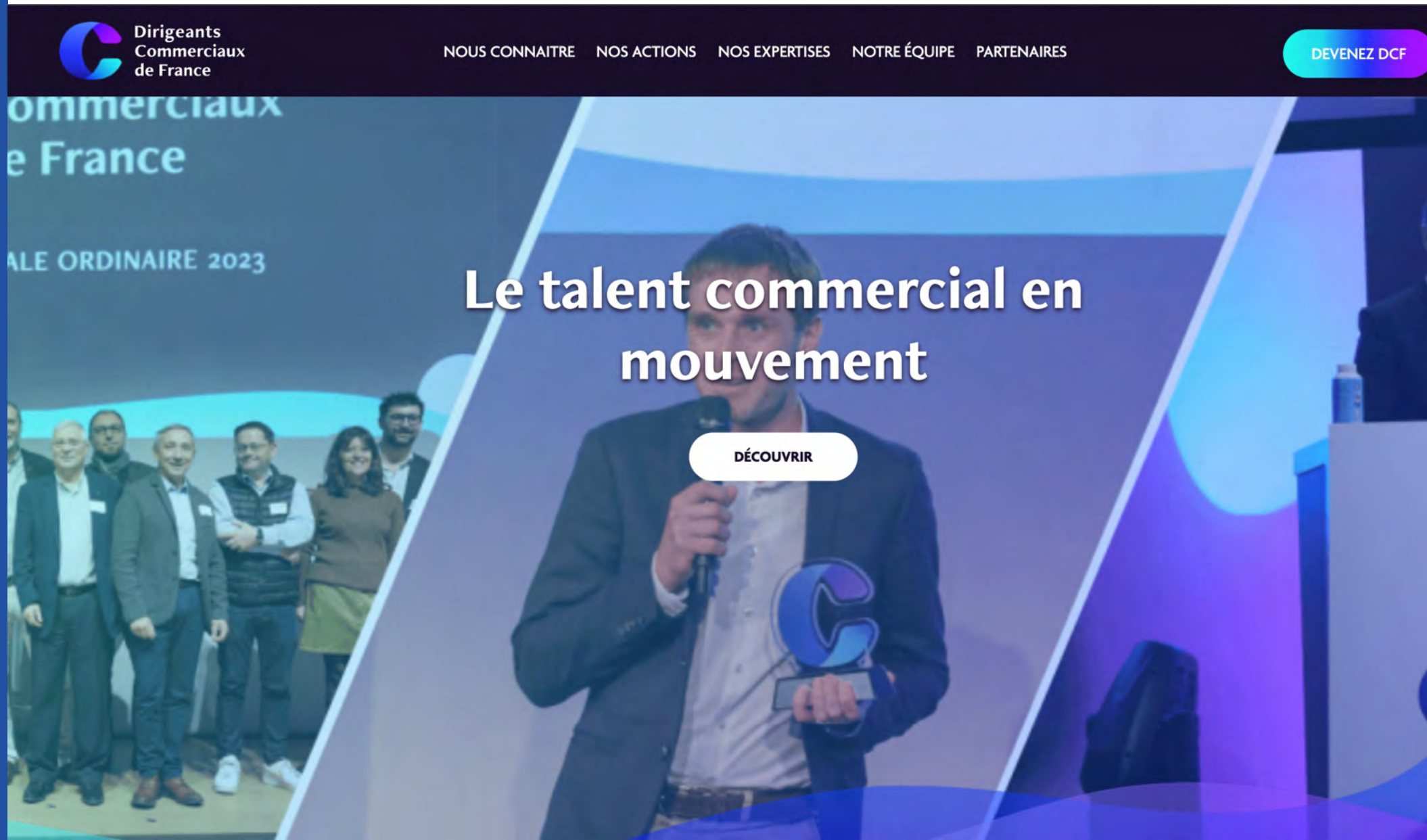
Pression, émotion
sur la victime

L'ingénierie sociale : **simple et efficace !**

Scénario D'attaque

Les bases de **l'OSINT** (Open Source Intelligence) ou **ROSO** (renseignement d'origine sources ouvertes)

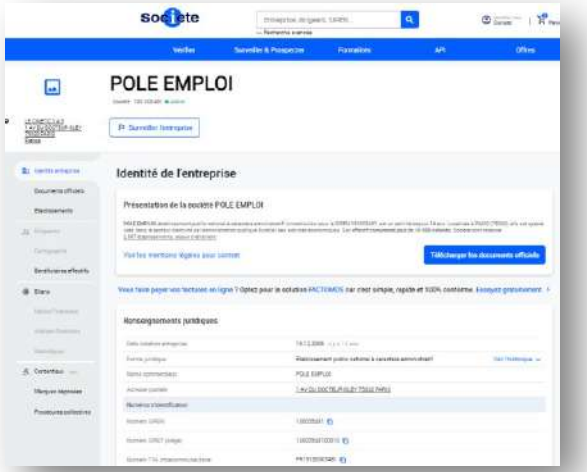
POLICE NATIONALE



L'ingénierie sociale : **simple et efficace !**

Scénario D'attaque

Les bases de **l'OSINT** (Open Source Intelligence) ou **ROSO** (renseignement d'origine sources ouvertes)



Exploration des **données publiques**

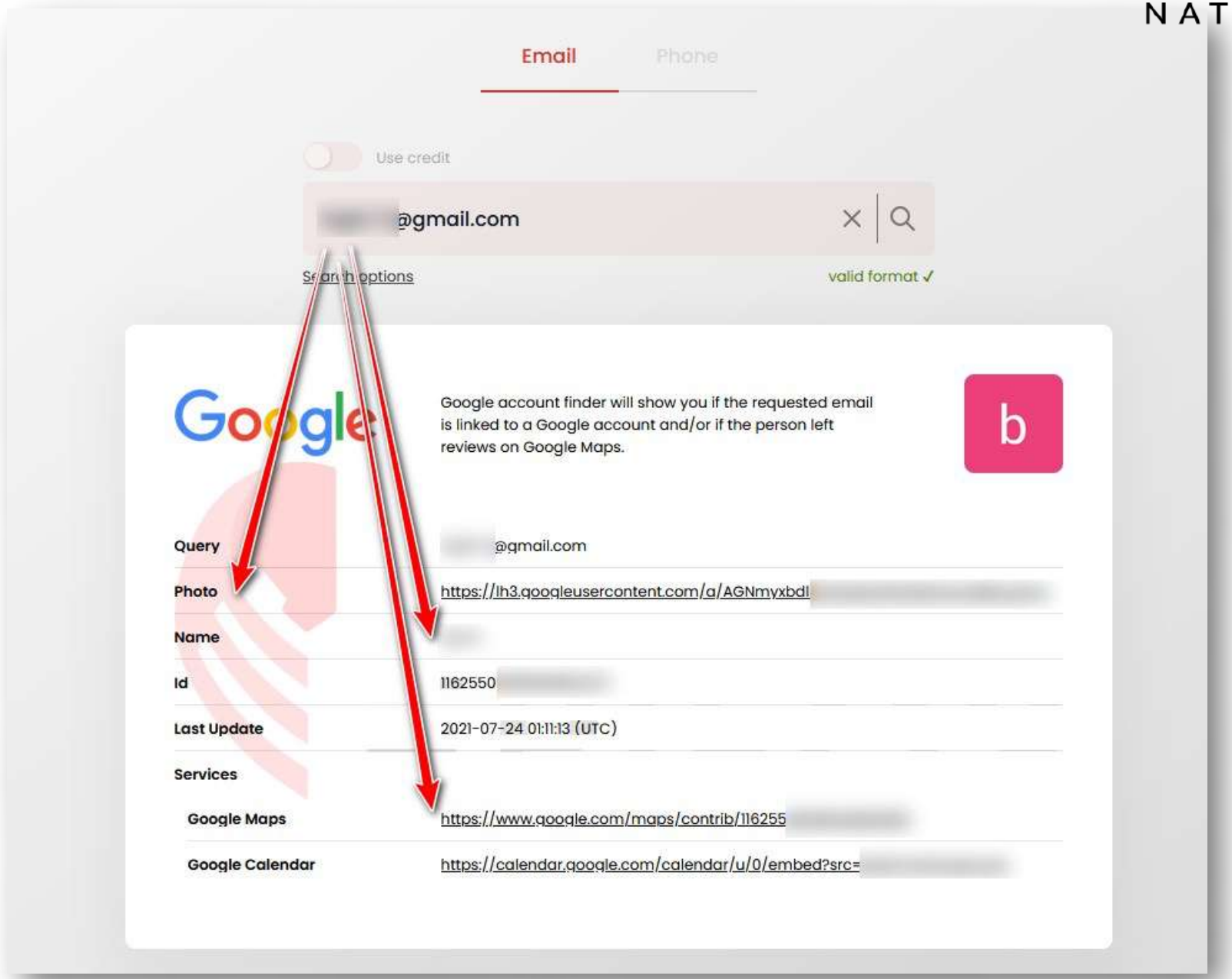
Exploration des **réseaux professionnels**

Exploration des **réseaux personnels**

L'ingénierie sociale : **simple et efficace !**

Scénario D'attaque

Exemple **d'OSINT** depuis Une **adresse email**
-
Identification des **publications liées à son compte google** : avis, photos, calendrier



POLICE NATIONALE

Enquête sur la cible

Vos contacts DCF

Fédération Nationale des Dirigeants Commerciaux de France

1 villa George Sand, 75016 PARIS

Tel : 01 45 25 11 44 - Fax : 01 40 50 15 56

federation@reseau-dcf.fr

Les permanents de la fédération

Responsable Administrative, Comptable et CNC

Béatrice ROA 01 45 25 72 53

Responsable de la Communication, contact presse

Pierre BOUZIN 01 45 25 84 30

Chef de projets

Elise ORTIS 01 45 25 72 54

Chargé de mission Internet et gestion de communauté

Juliette GRIMBERT

POLICE NATIONALE

Usurpation d'identité

--

Juliette GRIMBERT Chargé de mission Internet et gestion de communauté
Fédération des Dirigeants Commerciaux de France
13 rue Dulong - 75017 PARIS
01 45 25 75 55
Juliette.GRIMBERT@reseau-dcf.fr

DCF

www.reseau-dcf.fr
Réseau DCF
@FederationDCF

http://www.leboncoin.xnce.fr

leboncoin Déposer une annonce Rechercher

Mes recherches Favoris Messages Se connecter

Immobilier • Véhicules • Vacances • Emploi • Mode • Maison • Multimédia • Loisirs • Matériel Professionnel • Autres

Des millions de petites annonces et autant d'occasions de se faire plaisir

Offres Demandes

Catégories | Que recherchez-vous ? | Saisissez une ville et un rayon

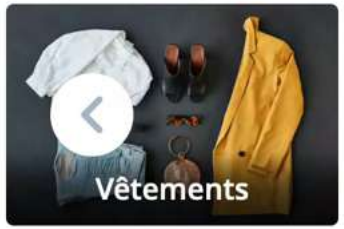
Prix

Voir également les annonces disponibles en livraison

Rechercher (63 046 081 résultats)

Déposer une annonce

Top catégories



http://www.leboncoin.xnce.fr

leboncoin Déposer une annonce Rechercher

Mes recherches Favoris Messages Se connecter

Immobilier • Véhicules • Vacances • Emploi • Mode • Maison • Multimédia • Loisirs • Matériel Professionnel • Autres

Des millions de petites annonces et autant d'occasions de se faire plaisir

http://www.leboncoin.xnce.fr

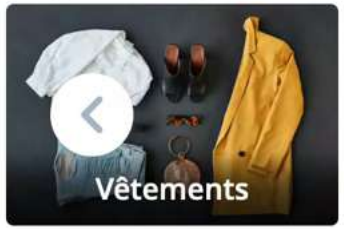
Prix

Voir également les annonces disponibles en livraison

Rechercher (63 046 081 résultats)

Déposer une annonce

Top catégories



Usurpation **d'identité**

Phishing

De Societe Generale <particuliers@societegnerale.fr>
Sujet **Confirmez votre Pass Sécurité**
Pour [redacted]

SOCIETE GENERALE

Cher(e) client(e),

Selon la nouvelle réglementation en vigueur relative à la sécurisation des données bancaire en France, nous somme dans le regret de vous annoncer, que si vous ne confirmez pas votre Pass Sécurité (1) auprès de nos services dans les plus bref délais, vous serez limité dans vos transactions.

Nous vous invitons à confirmer votre Pass Sécurité via notre service en ligne:

Confirmer mon Pass Sécurité

Nous nous excusons pour tout désagrément et vous remercions pour votre coopération.

Cordialement

Claude BAGNARD,
directeur de la relation Clients

Usurpation **d'identité**

Hacking

Trend Micro fournit les détails suivants à *20 Minutes.* Entre la mi-mars et la mi-avril, des hackers russes **ont créé quatre noms de domaine ressemblant à ceux de l'équipe officielle d'En Marche** pour tenter de piéger des collaborateurs :

- onedrive-en-marche.fr (15 mars 2017)
- portal-office.fr (14 avril 2017)
- mail-en-marche.fr (12 avril 2017)
- accounts-office.fr (17 avril 2017)

Selon les chercheurs, « ces noms de domaine ont vraisemblablement été utilisés par Pawn Storm pour cibler la campagne de Macron », qui utilise le service email de Microsoft d'Office 365. La procédure est classique et vise en général **à se faire passer pour un courriel officiel afin de convaincre une personne** d'entrer son mot de passe lors d'une remise à zéro. Selon Trend Micro, les hackers ont également tenté d'infecter des ordinateurs avec un malware Javascript à la recherche d'éventuelles failles.

Escroquerie
Exemple d'atteinte

Faux recrutement

Scénario
D'attaque

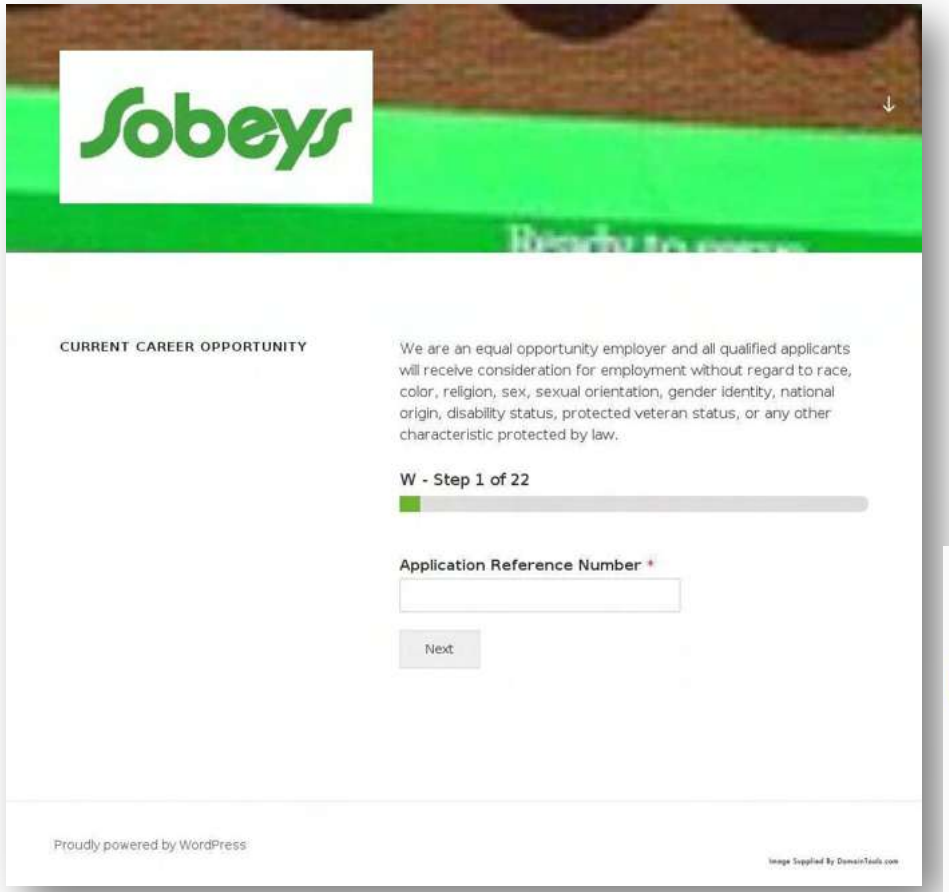
WIPO Arbitration and Mediation Center

Sobeys Capital Incorporated v. Private By Design, LLC / Max Bill and Billi Max

Case No. D2020-1670

http://interview-Sobeys.com

POLICE NATIONALE



The Respondent registered the First Disputed Domain Name on May 29, 2020 and the Second Disputed Domain Name on May 6, 2020. The First Disputed Domain Name is used to direct users to a fake SOBEYS website, which prominently features the Complainant's Trademark, trade name, and other details about the Complainant, all without any authorization. This fake website is used to solicit "job applications" from prospective employees requiring the provision of confidential personal information.

Email addresses associated with the Disputed Domain Names have also been used to send third parties solicitation emails purporting to emanate from the Complainant and offering employment with the Complainant's business. These fraudulent emails represent that they are being sent by human resources personnel employed by the Complainant, and solicit confidential personal and financial information from the victims of the scam. Among other things, recipients are requested to sign an "Employment Contract" and to also provide confidential personal and financial information including copies of government documents, banking information, and postal addresses in order to "accept" the employment position offered by the Respondent posing as "Sobeys" after first submitting a "job application" through the fake website hosted at the First Disputed Domain Name. As with the fake website operated by the Respondent, the "Employment Contract" and other materials sent to recipients of these emails prominently feature the Complainant's Trademark and include references to the Complainant's actual activities.

Escroquerie
Exemple d'atteinte
Visant Pole Emploi

Scénario
D'attaque

https://pole-emploi.fr

http://poleemploifrance.fr

http://polle-emploi.fr

N° de dossier	Nom de domaine	Date de publication	Procédure
FR-2022-03066	poleemploifrance.fr	01/02/23 16:42:54	SYRELI
FR-2022-02885	polle-emploi.fr	29/08/22 09:46:13	SYRELI

https://pajemploi.urssaf.fr

http://pajemploiurssaf.fr

N° de dossier	Nom de domaine	Date de publication	Procédure
FR-2022-02706	pajemploiurssaf.fr	19/04/22 12:18:25	SYRELI
FR-2021-02476	pajemploie.fr	11/10/21 09:44:01	SYRELI
FR-2021-02467	pajemploi.fr	11/10/21 09:44:24	SYRELI

Usurpation **d'identité**

Homographe

http: // airfrance.com

POLICE NATIONALE

POLICE NATIONALE

Attaque typosquatting

POLICE NATIONALE

Usurpation d'identité

--

Juliette GRIMBERT Chargé de mission Internet et gestion de communauté
Fédération des Dirigeants Commerciaux de France
13 rue Dulong - 75017 PARIS
01 45 25 75 55
Juliette.GRIMBERT@reseau-dcf.fr

mailto:juliette.grimbert@reseaux-dcf.fr

Infobulle en mettant le curseur de la souris sans cliquer

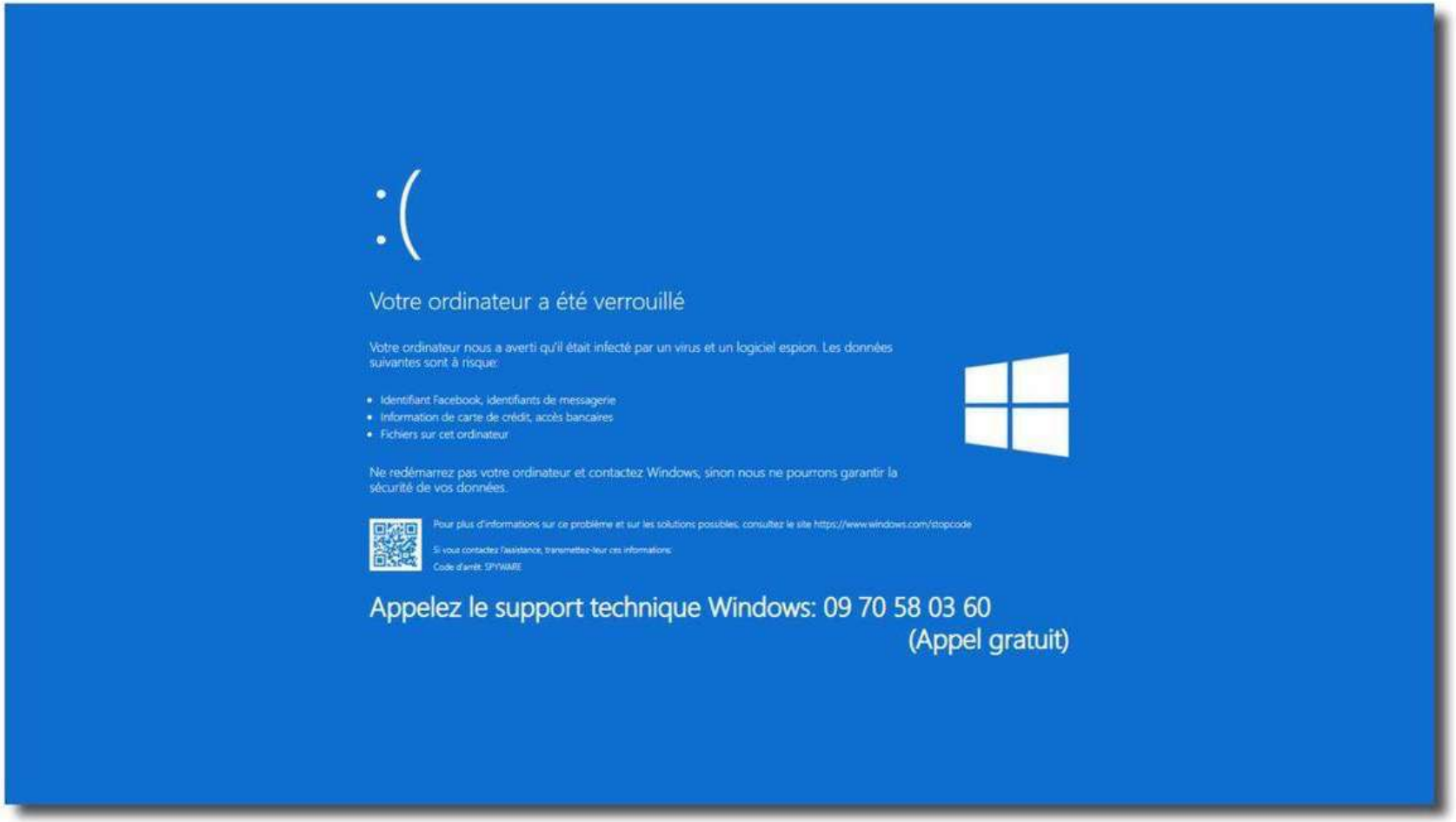
DCF

www.reseau-dcf.fr
Réseau DCF
@FederationDCF

L'ingénierie sociale : **Comment ça marche ?**

POLICE NATIONALE

Le faux support technique



L'ingénierie sociale : **Comment ça marche ?**

Le faux support technique

L'exploitation d'une **vulnérabilité technique**

Les 3 principaux facteurs techniques d'attaques informatiques

L'absence des mises à jour
(Fonctionnelles et de sécurité)

L'absence de politique de mot de passe
(complexité, contrôle, renouvellement…)

La publication des outils sur internet et l'absence de contrôle des utilisateurs et des prestataires

Les **3 principaux facteurs** techniques d'attaques informatiques

POLICE NATIONALE

Pourquoi faut-il un mot de passe complexe?

Attaque par Bruteforce:

Craquer un mot de passe en testant successivement les combinaisons.
L'outil teste des milliers de combinaisons/seconde
->Optimisation heuristique

Enquête sur la société, de la personne, du champs lexical...

```
root@JEFFLAB-DEB02:~/CrackMapExec# cme smb JEFFLAB-APP01 -u Administrator -d builtin -p ~/passwords.txt
SMB         192.168.12.240  445    JEFFLAB-APP01    [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-APP0
1) (domain:builtin) (signing:False) (SMBv1:True)
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Winter2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:P4$$word STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Fall2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Spring2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Summer2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:$ummer2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Fall2015 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Spring2015 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Summer2015 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:$ummer2015 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Fall2014 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Spring2014 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Summer2014 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:$ummer2014 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Fall2016 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Spring2016 STATUS_LOGON_FAILURE
```

POLICE NATIONALE

Qu’est-ce qu’un ransomware?

Hôpital de Dax

POLICE NATIONALE

3 nouvelle aquitaine

chez moi programmes menu

Cyberattaque de l'hôpital de Dax : une rançon demandée pour décrypter les données

Publié le 10/02/2

Écrit par V.D.

mpte 2300 personnels • © Google Street View

Le coût total de la cyberattaque du CH de Dax s'est élevé à 2,3 millions d'euros

#5373 #Informatique #Organisation #Politique de santé #5229
#Achats #E-santé #5386

11/04/2022 < 6

(Par Wassinia ZIRAR, au congrès de l'Apssis)

LE MANS, 11 avril 2022 (TecHopital) - Le coût total de l'attaque informatique subie par le centre hospitalier (CH) de Dax dans la nuit du 8 au 9 février 2021 s'élève à 2,3 millions d'euros "compensés par l'agence régionale de santé" (ARS), a rapporté le 7 avril le responsable de la sécurité des systèmes d'information de l'hôpital, Nicolas Terrade.

PIXELS · CYBERCRIMINALITÉ

L'hôpital de Dax en partie paralysé par une attaque informatique

Un logiciel malveillant a bloqué, mardi, le fonctionnement du système informatique de l'hôpital landais, le rendant inaccessible. Le centre de vaccination contre le Covid-19 a dû fermer ses portes.

Par Claire Mayer (Bordeaux, correspondante)

Publié le 10 février 2021 à 10h15, mis à jour le 11 février 2021 à 06h01 · Lecture 3 min.

Ajouter à vos sélections

onnels qui doivent
alier de Dax (Landes) a
e attaque
l malveillant a chiffré

Faites-vous ac
IONOS

Les plu
1 La co
Hug
mé

Victime d'une cyberattaque, l'hôpital de Dax fonctionne au ralenti

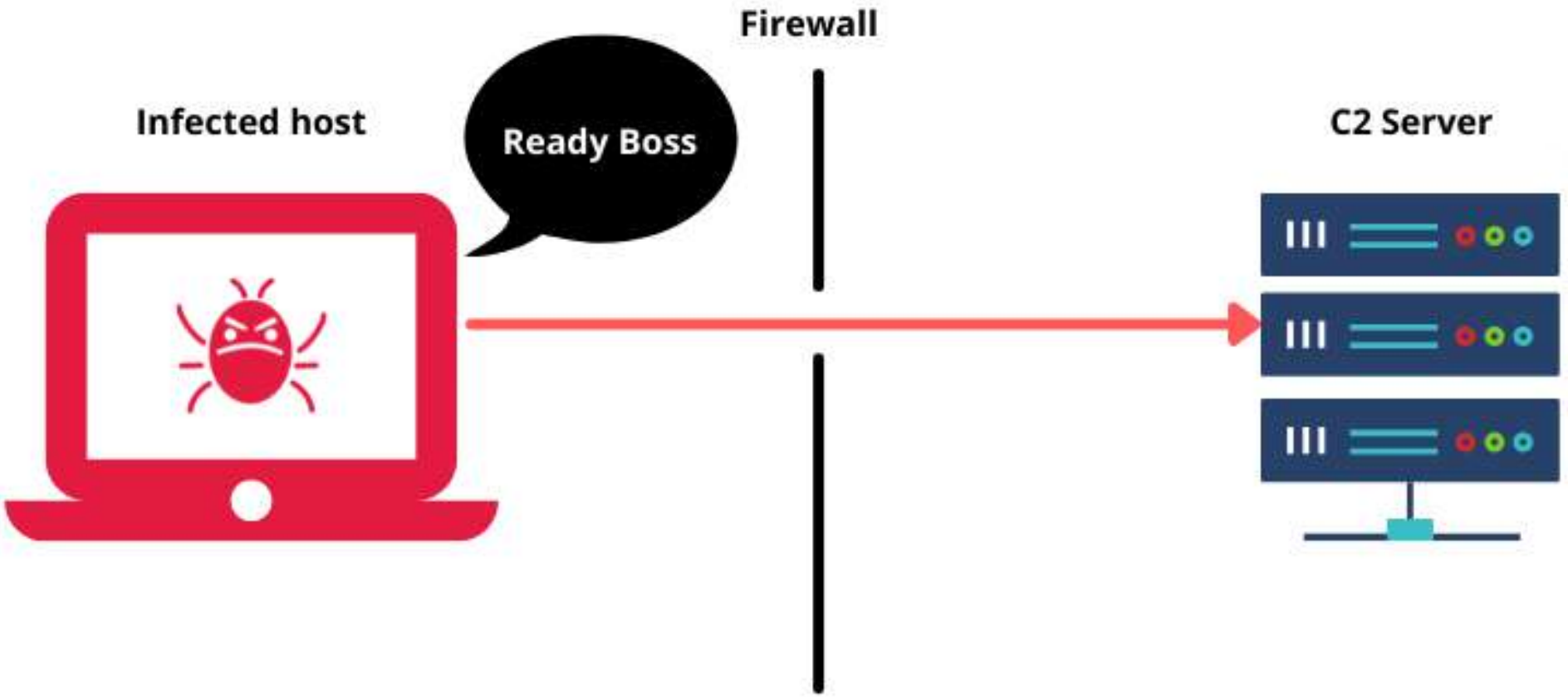
Le système d'information de l'hôpital de Dax a été mis hors service à la suite d'une attaque informatique. Les dossiers patients entièrement numérisés ne sont plus accessibles, de même que certains équipements médicaux, tels que les stérilisateurs utilisés dans les blocs opératoires. Une enquête judiciaire a été ouverte.

Alice Vitard

10 Février 2021 \ 12h14

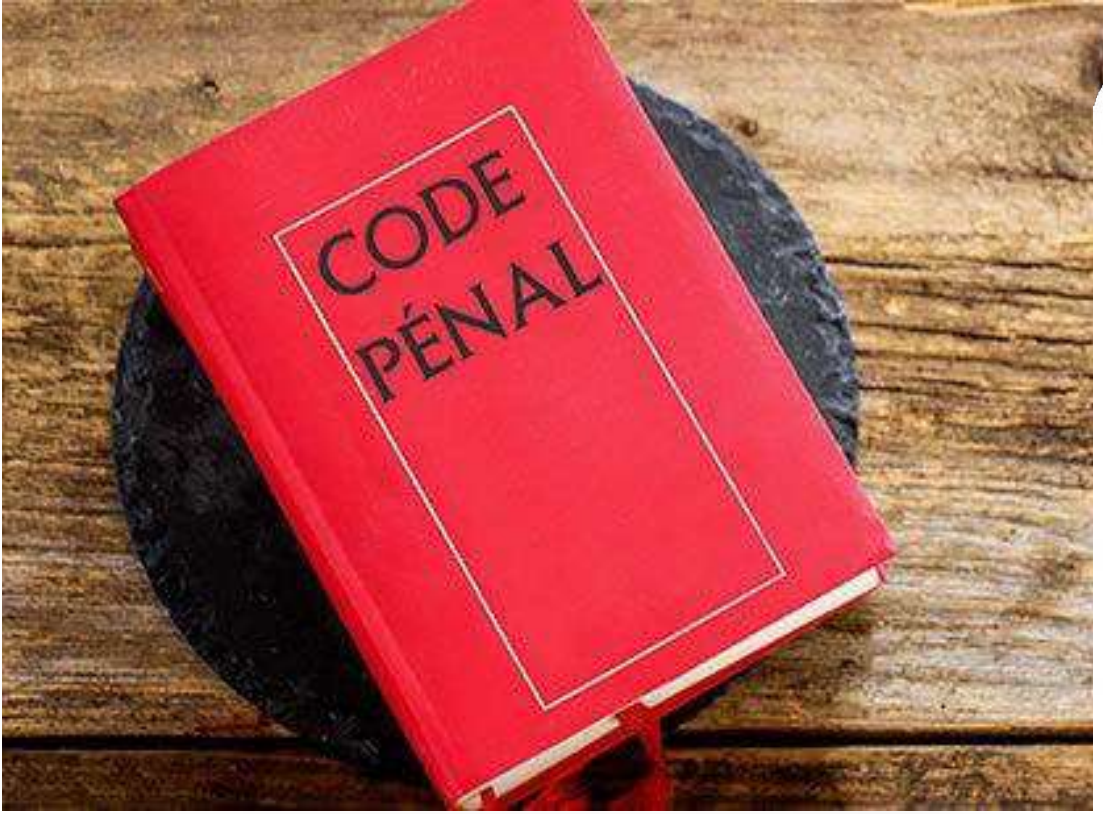
Le ransomware

Fonctionnement: *Command and control*



POLICE NATIONALE

Les escroqueries



- 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**

Article 313-1

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.

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

POLICE NATIONALE

Matrice **MICE**

Les piliers de la manipulation

\+






Money
Argent

Ideology (idéologie)
(convictions religieuses, politiques, etc.) ou intérêt (passe-droits)

Coercition
chantage, menaces, kompromat, torture, etc.

Ego
vanité, désir de se mettre en avant

Escroquerie
Les impacts

Scénario
D'attaque

Arrêt des activités

Perte financière / Liquidation

Difficultés juridiques

Pression psychologique

Image de marque / Notoriété

Confidentialité / Secret

Comment se protéger ?

pour éviter **l'incident** ?

Comment se **protéger** ?

1) Protégez vous !

La **suite** de sécurité

Elle permet une protection contre :

- Les logiciels **malveillants**
- Les **comportements** suspicieux
- Les **pièce-jointes** malicieuses
- Les fichiers dangereux
- Les **sites** internet

Les conditions pour assurer votre sécurité :

- Installation sur **tous les appareils**
- L'outil doit être activé en **permanence**
- La base de données virale doit **être à jour**

Comment se **protéger** ?

2) Soyez vigilants aux mails !

POLICE NATIONALE

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 ?

Le Phishing **comment s'en protéger ?**

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

Escroquerie –

Vérifier un
Nom de domaine

http://who.is
https://gwhois.org

WHOIS
DOMAIN
LOOKUP

Recherche d'information sur **un nom de domaine**

POLICE NATIONALE

https://pole-emploi.fr

domain:	pole-emploi.fr
status:	ACTIVE
Expiry Date:	2023-09-21T09:42:27Z
created:	2008-10-10T14:47:02Z

nic-hdl:	PEAD28-FRNIC
type:	ORGANIZATION
contact:	POLE-EMPLOI admin-domaines-internet
address:	POLE EMPLOI
address:	70 rue de Lagny
address:	93558 MONTREUIL
country:	FR
phone:	+33.155817000
fax-no:	+33.155817984
e-mail:	admin-domaines-internet@pole-emploi.fr

http://poleemploifrance.fr

domain:	poleemploifrance.fr
status:	FROZEN
Expiry Date:	2023-10-13T11:09:31.993649Z
created:	2022-10-13T11:09:32.017576Z

nic-hdl:	ANO00-FRNIC
type:	PERSON
contact:	Ano Nymous
registrar:	OVH
changed:	2020-03-27T09:04:06Z
anonymous:	YES
remarks:	---------- WARNING ----------
remarks:	While the registrar knows him/her,
remarks:	this person chose to restrict access
remarks:	to his/her personal data. So PLEASE,
remarks:	don't send emails to Ano Nymous. This
remarks:	address is bogus and there is no hope
remarks:	of a reply.
remarks:	---------- WARNING ----------

Comment se **protéger** ?

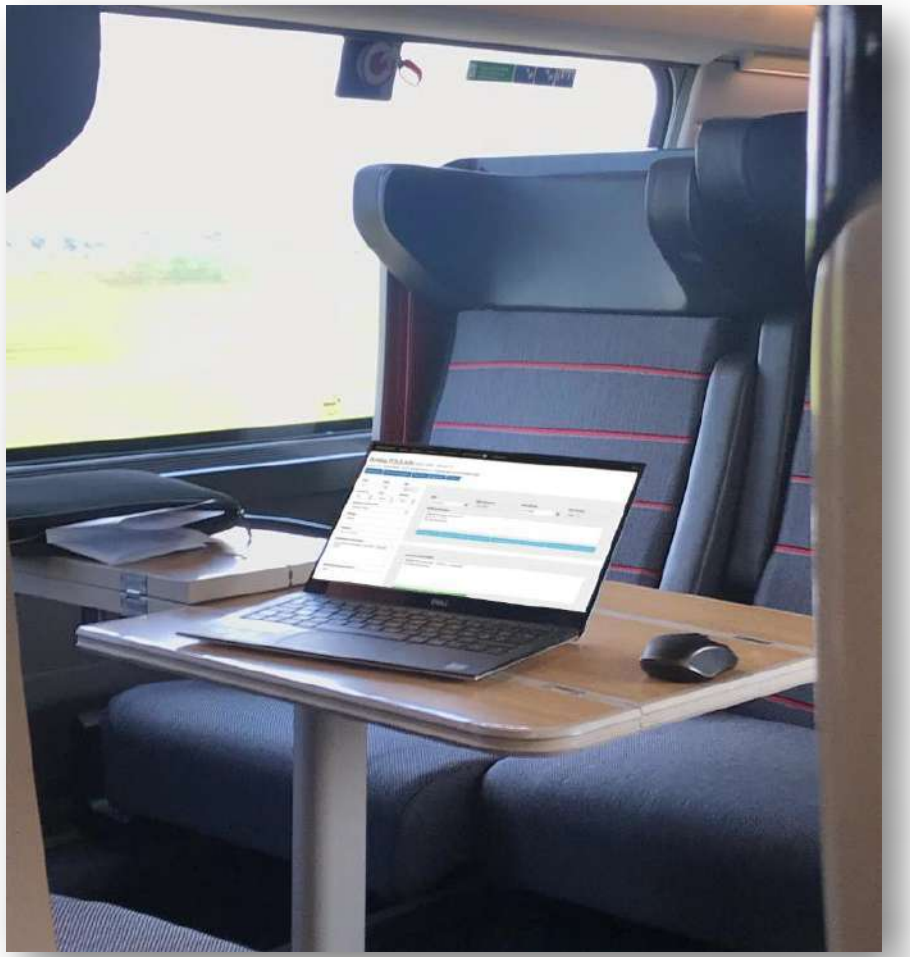
3) Sécurisez vos accès !

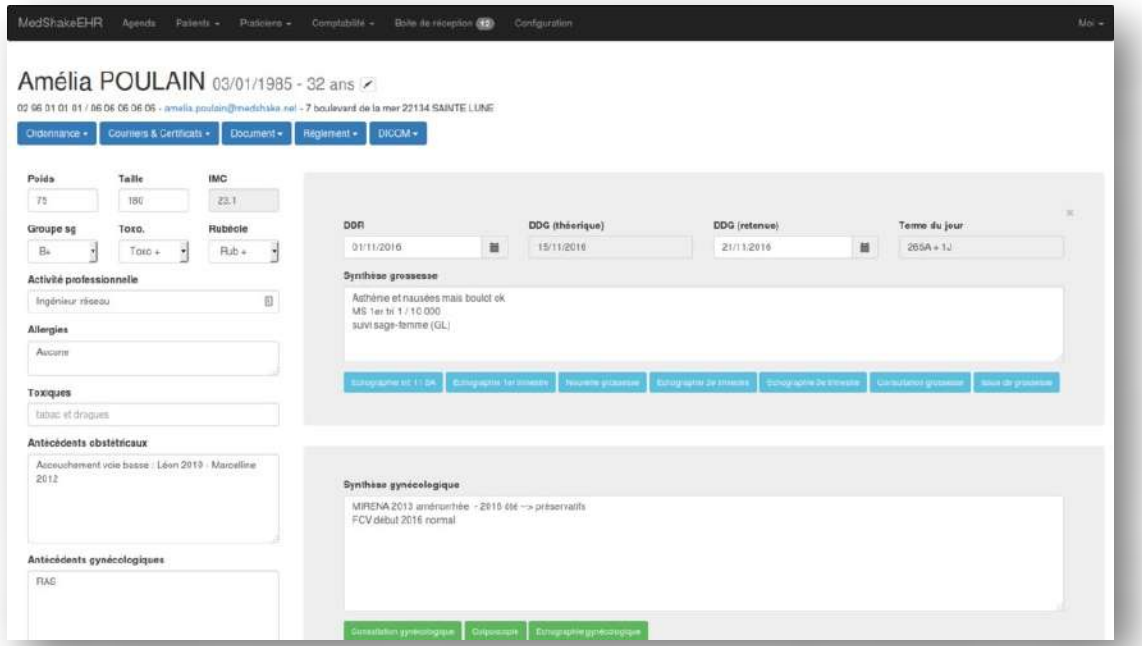
Le mot de passe : **votre clé privée !**

- 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

Comment se **protéger** ?

4) Surveillez votre matériel





POLICE NATIONALE

Comment se **protéger** ?
5) Sauvegardez vos données !

Vous hébergez votre logiciel métier chez un prestataire ?
Attention à votre contrat !

Vous hébergez vous-même vos données ?
Réfléchissez à la stratégie en fonction de la sensibilité !

Exemple de stratégie en 3 - 2 - 1

- 3 **copies** des données
- 2 **supports** de sauvegardes
- 1 copie « **hors site** »

POLICE NATIONALE

Comment se **protéger** ?

6) Effectuez vos mises à jour !

La mise à jour corrige des **vulnérabilités** !

L'application des mises à jour est un **élément essentiel** pour assurer la sécurité de votre matériel.

Vous disposez d'un informaticien ?
Posez lui la question.

Comment se **protéger** ?

7) Sensibilisez au maximum

POLICE NATIONALE

Vos collaborateurs

- Intégration
- Contrat de travail
- Charte informatique
- Sensibilisation ponctuelle
- Surveillance…

Vos prestataires

- Contrat de prestation
- Charte prestataire
- Accompagnement
- Surveillance…

Votre entourage

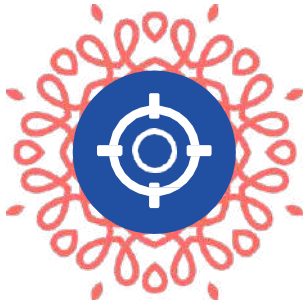
- Séparation des usages
- Confidentialité pro / perso
- Sensibilisation en famille
- …

Comment **réagir**
En cas d'incident ?

Réactions face **à une cyber attaque**

Isoler

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

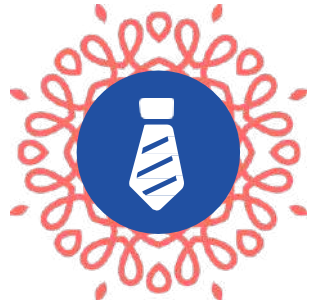


Confiner

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**... pour éviter le surincident

Le dépôt **de plainte**

Pourquoi déposer plainte ?

Parce que vous êtes victime !

- Pour **comprendre les raisons** et/ou contexte de l'attaque
- Pour **identifier les modes opératoires** et les vulnérabilités
- Pour **récupérer les données métiers** et limiter leur diffusion
- Pour permettre (dans certains cas) le **blocage des fonds**
- Pour **se protéger** (ex. : usurpation d'identité)
- Pour **faire valoir ses droits** (auprès des banques, de l'assurance...)
- Pour **contribuer aux enquêtes** de Police

POLICE NATIONALE

Gendarmerie nationale

Le dépôt **de plainte**

Quand et comment déposer plainte ?

cybermenaces-bordeaux@interieur.gouv.fr

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

- La création **d'un point de contact unique et privilégié sur la Nouvelle-Aquitaine** avec une adresse mail dédiée en cas de doute ou d'attaque avérée : 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

POLICE NATIONALE

Gendarmerie nationale

Ressources

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

https://secnumacademie.gouv.fr/

CNIL.

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

CYBER MALVEILLANCE .GOUV.FR

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

Merci pour votre attention

Vos questions ?

Pierre LABORDE
Commandant Divisionnaire
Réserviste Police Nationale
cybermenaces-bordeaux@interieur.gouv.fr

POLICE NATIONALE

RCM
POLICE NATIONALE
DCPJ • RÉFÉRENT CYBER MENACE

Mathieu EPAULARD
Réserviste Police Nationale
Dirigeant société
sécurité informatique