Web°1H

Cyberattaques :

Comment les éviter ?

Comment réagir ?

5 octobre 2023

URPS MÉDECINS LIBÉRAUX Nouvelle-Aquitaine

ESEA e-santé en action NOUVELLE-AQUITAINE

RÉSEAU EXPERTS CYBER MENACES RECYM DE LA POLICE NATIONALE

Déroulement

- Dans quel monde vivons-nous ? Retour sur le risque cybersécurité
- Les bonnes pratiques pour éviter les cyberattaques
- Comment agir en cas d'attaque ?
- Quelles formations et quels accompagnements?
- Questions/réponses

Pour poser vos questions :

Intervenants : Commandant divisionnaire Pierre LABORDE – Police Nationale
Mme Léana GORGIUS - Référente - Cellule cybersécurité santé, ESEA
Dr Philippe DURANDET - cardiologue, élu à l'URPS ML NA, référent cybersécurité

Animation : Emmanuel BATAILLE - Directeur URPS Médecins Libéraux

Une réalité qui peut tous nous concerner

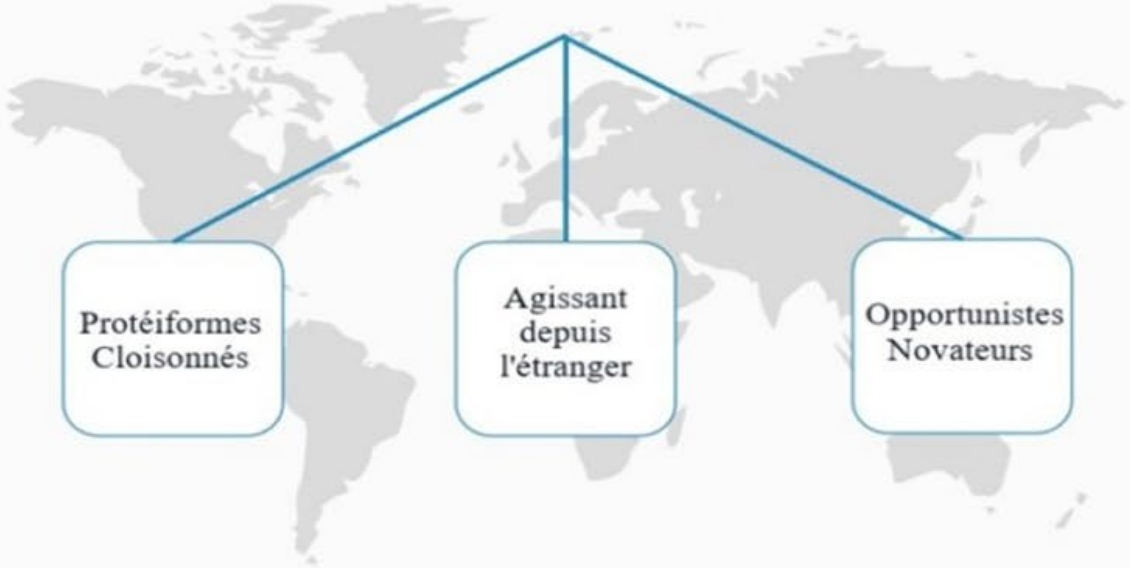
cliquez sur l'image
pour lancer la vidéo

Source: Febelfin: fédération belge du secteur financier

Evolution de la criminalité organisée depuis 20 ans

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

*…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 »

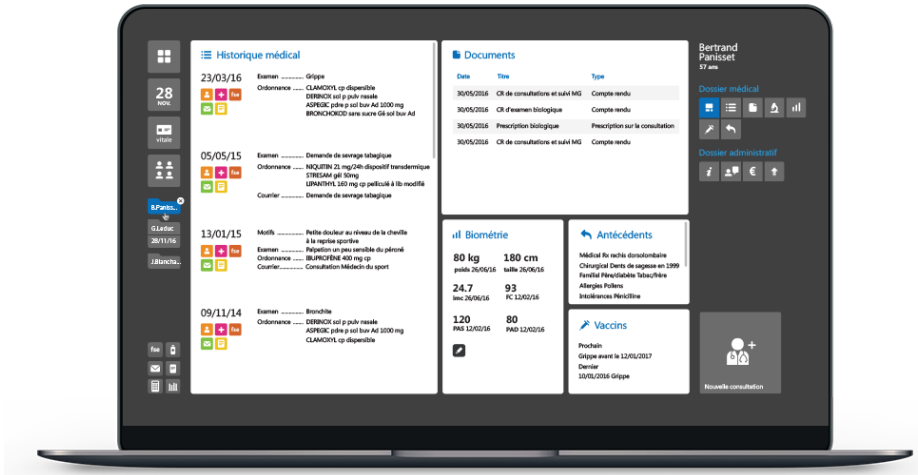
Disposent d'un panel de compétences (intrusion, élévation de privilèges, latéralisation pivot, déploiement de rançongiciel, captation de mémoire vive, …)

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

Pourquoi êtes-vous concernés ?

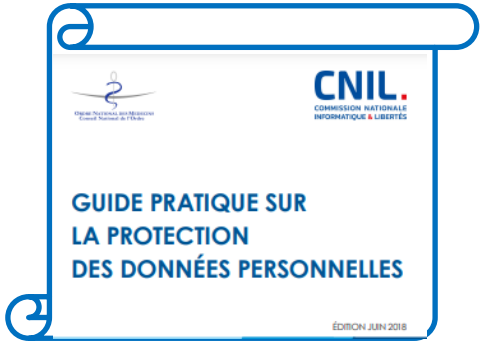
Vous êtes responsable des données transmises par vos patients.



Logiciel métier

- ❑ Nom
- ❑ Prénom
- ❑ Date de naissance
- ❑ Lieu de naissance
- ❑ Numéro de sécurité sociale
- ❑ Pathologie

Tenir un registre des traitements



2

Cyberattaques : **les bonnes pratiques** pour les éviter

Cyberattaques : les bonnes pratiques pour les éviter

QUIZ – Une question = une explication (messages essentiels)

Temps de réponse par question : 15 secondes

Question 1

De: IT <info1@pau.krakow.pl>
à: Recipients <info1@pau.krakow.pl>
Envoyé: jeudi 3 août 2023 10:31 CEST
Sujet : Mise à jour du mot de passe

Cher utilisateur,

Le mot de passe de votre compte de messagerie a expiré.

Pour éviter que votre compte soit désactivé,
veuillez utiliser le lien ci-dessous pour mettre à jour et continuer avec votre mot de passe actuel.

Conserver le mot de passe actuel

Votre accès à la messagerie sera désactivé après aujourd'hui,
N'ignorez pas cet e-mail afin de ne pas être bloqué sur votre compte.

Salutations
Assistance Zimbra

Les bonnes pratiques à retenir !

Ne mélangez pas usages pro et perso !

Utilisez des mots de passe complexes et uniques !

Mettez régulièrement à jour vos appareils !

N'ouvrez jamais les emails et les pièces jointes suspects !

Utilisez un antivirus !

Vérifiez l'adresse des expéditeurs !

Désinstallez les logiciels obsolètes ou inutilisés !

Eteignez votre ordinateur ou fermez votre session !

Evitez les sites non sûrs ou illicites !

Faites des sauvegardes régulières !

3 Comment agir en cas d'**attaque** ?

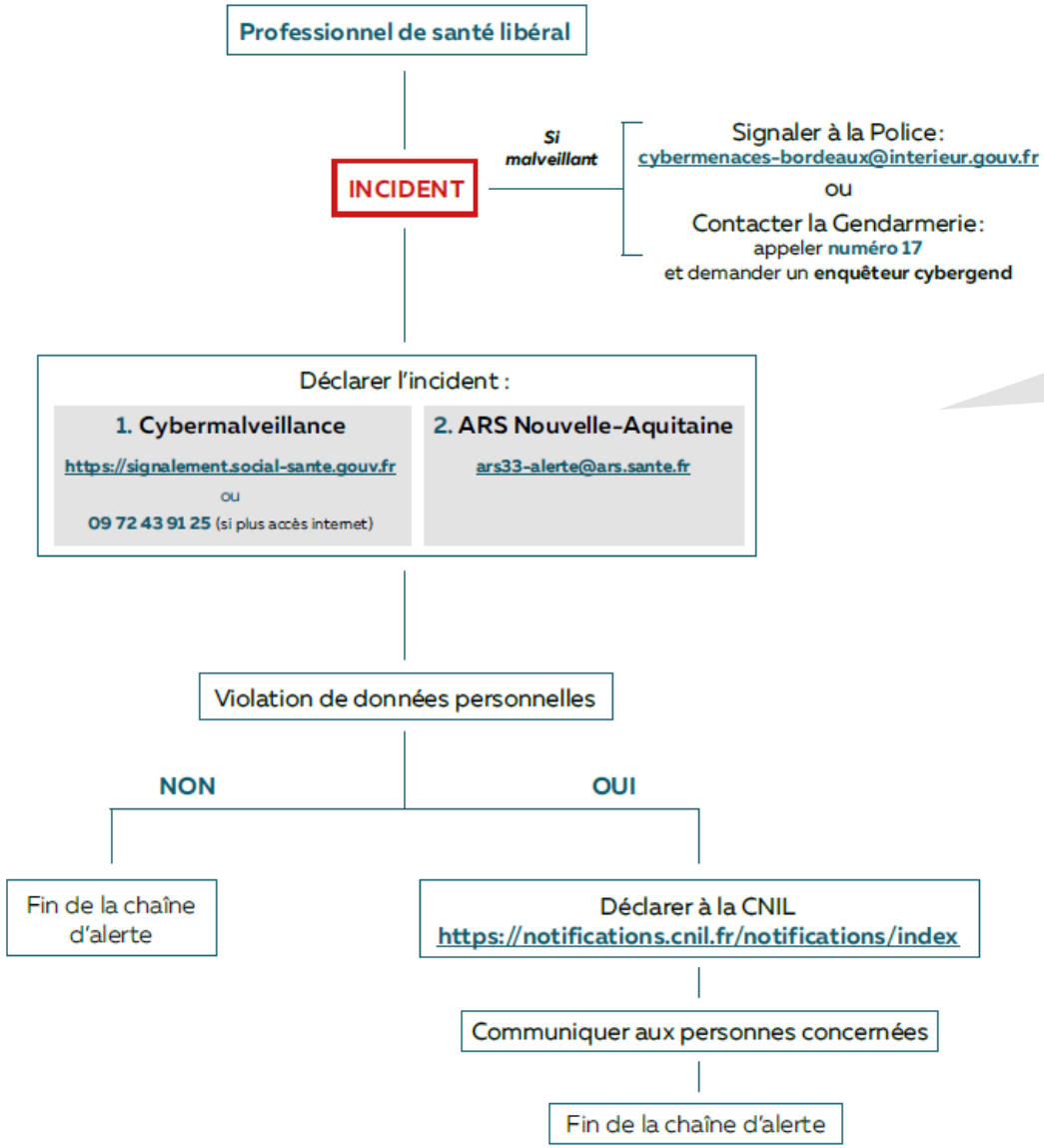
Les bons réflexes et la chaîne d'alerte

1. Déconnectez votre appareil du réseau internet (Ethernet et wifi)
2. Laissez votre appareil allumé !
3. Laissez l'alimentation électrique branchée

Besoin d'aide ?

Contactez le campus cyber sécurité de N-A :

0805 29 29 40



Cliquez sur le document

L'indispensable nécessité de déposer 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

Le dépôt de plainte

Quand et comment déposer plainte ?

Il est primordial de déposer une plainte en cas de menaces, pour les mêmes raisons que nous portons plainte pour tout acte répréhensible dont nous sommes victime.

- 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

- **masecurite.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

4

Formations et accompagnements possibles

Plateformes de formation + RELEA

- **Agence du numérique en santé** : https://esante-formation.coorpacademy.com/login
  Aborde l'ensemble des domaines e-santé avec des séquences sur la cybersécurité (types d'attaques et une nouvelle séquence sur les mots de passe)

- MOOC **ANSSI** : https://secnumacademie.gouv.fr/
  Initie à la cybersécurité (plus technique)

- **ELEA** : https://elea.esea-na.fr/enrol/index.php?id=130
  Aborde la notion « d'information » et de « prédation informationnelle » puis intègre les bonnes pratiques (10 conseils)

- **RELEA** : https://relea.esea-na.fr/
  Promouvoir les évènements et les initiatives des acteurs de la santé en Nouvelle-Aquitaine

Plateforme d'autoformation URPS Médecins Libéraux N-A

- A venir début 2024 !
- Plateforme d'autoformation et de sensibilisation (vidéos interactives) des médecins libéraux et de leur personnel administratif
- L'information directement dans votre boite mail !
- En partenariat avec l'entreprise Conscio technologies - agréée par la centrale d'achat de l'informatique hospitalière (CAIH)

5 Conclusion

En conclusion

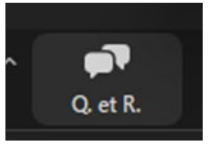
- Un accompagnement proposé par :
  - Le GRADeS ESEA avec un réseau de professionnels sur le terrain,
  - La Police Nationale avec un réseau de réservistes présent sur le territoire régional,
  - CONSCIO pour vous former !
- Rejoignez la brigade des ambassadeurs cyber !
- Des points clés :
  - Des mises à jour et des sauvegardes régulières,
  - Des mots de passe renforcés et uniques,
  - Dissocier vos usages,
  - … !
- Merci de répondre à notre enquête de satisfaction !

En savoir plus

- Ressources site URPS ML NA : ici
- Mémento de sécurité informatique pour les professionnels de santé en exercice libéral : ici et synthèse ici
- Fiche réflexe en cas d'incident de sécurité informatique : ici
- Site national sur la cybervigilance (fiches, bonnes pratiques, mémo…) : ici
- Vérifiez si votre adresse e-mail a été compromise lors d'une violation de données : ici
- Stockez, créez, testez vos mots de passe… : ici

6 Questions / Réponses

Pour poser vos questions :



Replay disponible

YouTube

@UrpsMedecinsNouvelleAquitaine

Merci !

URPS MÉDECINS LIBÉRAUX Nouvelle-Aquitaine

Annexe

GLOSSAIRE DES MENACES

Hameçonnage ou phishing (en anglais)
Technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance.

Harponnage
Les e-mails de harponnage sont élaborés minutieusement de manière à cibler un destinataire unique. Les malfaiteurs sélectionnent une cible au sein d'une entreprise, à l'aide des réseaux sociaux et d'autres informations publiques, puis confectionnent un faux e-mail spécialement pour cette personne.

Déni de service ou DoS attack (Denial of Service attack en anglais)
Attaque informatique ayant pour but de rendre indisponible à ses utilisateurs légitimes un service Internet. Elle peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web, empêcher la distribution de courriel dans une entreprise ou rendre indisponible un site internet.

Attaque de l'homme au milieu (HDM) ou man-in-the-middle attack (MITM), parfois appelée attaque du monstre du milieu ou monster-in-the-middle attack1,2 ou attaque de l'intercepteur, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de communication entre elles a été compromis.

Attaque par mot de passe
Une attaque de mot de passe est tout simplement une tentative de vol de mot de passe par un hacker. Les attaques de mot de passe constituent l'une des formes les plus courantes de violation des données d'entreprise et personnelles.

Logiciels malveillants
sont des programmes développés dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.

Un rançongiciel ou Ransomware (en anglais)
C'est un code malveillant qui bloque l'accès à votre appareil ou à des fichiers en les chiffrant et qui vous réclame le paiement d'une rançon pour obtenir le déchiffrement de vos données.

Cheval de troie
Programme en apparence inoffensif contenant une fonction illicite cachée et connue de l'attaquant seul. Cette fonction lui permet de prendre le contrôle de la machine infectée.