AGENCE DU NUMÉRIQUE EN SANTÉ

Cybersécurité dans le secteur médico-social

ANS - CERT Santé (Cellule ACSS)

Jeudi 15 avril 2021

Les intervenants

Cédric BERTRAND

Expert sécurité

cedric.bertrand@esante.gouv.fr

Emmanuel SOHIER

Responsable CERT Santé

Emmanuel.sohier@esante.gouv.fr

AGENCE DU NUMÉRIQUE EN SANTÉ

Sommaire

AGENCE DU NUMÉRIQUE EN SANTÉ

Sommaire

Cybersécurité: menaces, risques et bonne pratiques

Actualités

Hôpital Delafontaine de Saint-Denis : un scanner infecté à l'arrêt

GABRIEL/PHANIE/AFP

Juillet 2018. L'hôpital général de Saint-Denis (Seine-Saint-Denis) qui réunit deux établissements, Delafontaine et Casanova, est victime d'un rançongiciel. Le programme malveillant touch peu d'ordinateurs, mais contamii tout de même du matériel médical - un scanner - et le rend inutilisable. « L'aide au diagnostic des patients a été perturbé, ainsi que leur prise en charge », atteste un témoin de l'incident. Les services du Premier ministre interviennent rapidement, car cette structure de 815 lits traite 200 passages d'adultes chaque jour aux urgences. Le scanner est infecté car il est connecté au réseau et utilise une version ancienne de Windows. Cet épisode a été vécu comme un traumatisme

L'attaque du groupe Ramsay fait suite à une poignée de cyberattaques sur des hôpitaux et cliniques basées en France au cours des derniers mois. En un an, **trois établissements ont déjà été ciblés par des hackers** : Montpellier (Hérault), Saint-Denis (Seine-Saint-Denis), Condrieu (Rhône). Dans les deux derniers cas, il s'agissait là aussi d'un ransomware. La situation a même fait réagir le gouvernement français, rapportait l'Express le 26 juin dernier. « *Nous sommes obligés de réagir, il s'agit d'une question d'éthique lorsque des hôpitaux sont touchés* » explique Guillaume Poupard, directeur général de l'Anssi.

www.phonandroid.com › Actu Généraliste › Sécurité

Un ransomware paralyse 120 hôpitaux français : des ...

14 août 2019 — L'attaque du groupe Ramsay fait suite à une poignée de cyberattaques sur des hôpitaux et **cliniques** basées en France au cours des derniers ...

www.techniques-ingenieur.fr › actualite › articles › pira...

Piratage des hôpitaux : l'arbre qui cache la forêt

26 févr. 2021 — ... les attaques par **ransomwares** se sont multipliées ces derniers mois. ... plus de 400 hôpitaux, **cliniques** et autres établissements médicaux.

www.src-solution.com › ransomware-etablissements-de-...

Ransomware : Etablissements de santé, à qui le tour ? - SRC ...

1 mars 2021 — Pour un hôpital ou une **clinique**, la question n'est actuellement pas tant de savoir si un **ransomware** finira par paralyser ses activités de soin, ...

Cybersécurité: menaces, risques et bonne pratiques

Définition

Un rançongiciel, (**ransomware** en anglais), logiciel rançonneur, logiciel de rançon ou logiciel d'extorsion, est un logiciel malveillant qui prend en otage des données personnelles.

Cybersécurité: menaces, risques et bonne pratiques

Ransomware as a service

Ransomware : des balbutiements à l'industrialisation

Sécurité : *De toutes les combinaisons possibles d'attaques informatiques, le rançongiciel est certainement celle dont le développement est le plus lié à l'évolution des cybercriminalités. Si nous voulons comprendre comment les rançongiciels sont devenus les plus perfectionnés et les plus susceptibles de s'industrialiser, il faut mettre en évidence leur nature économique et sociale.*

ZDNet

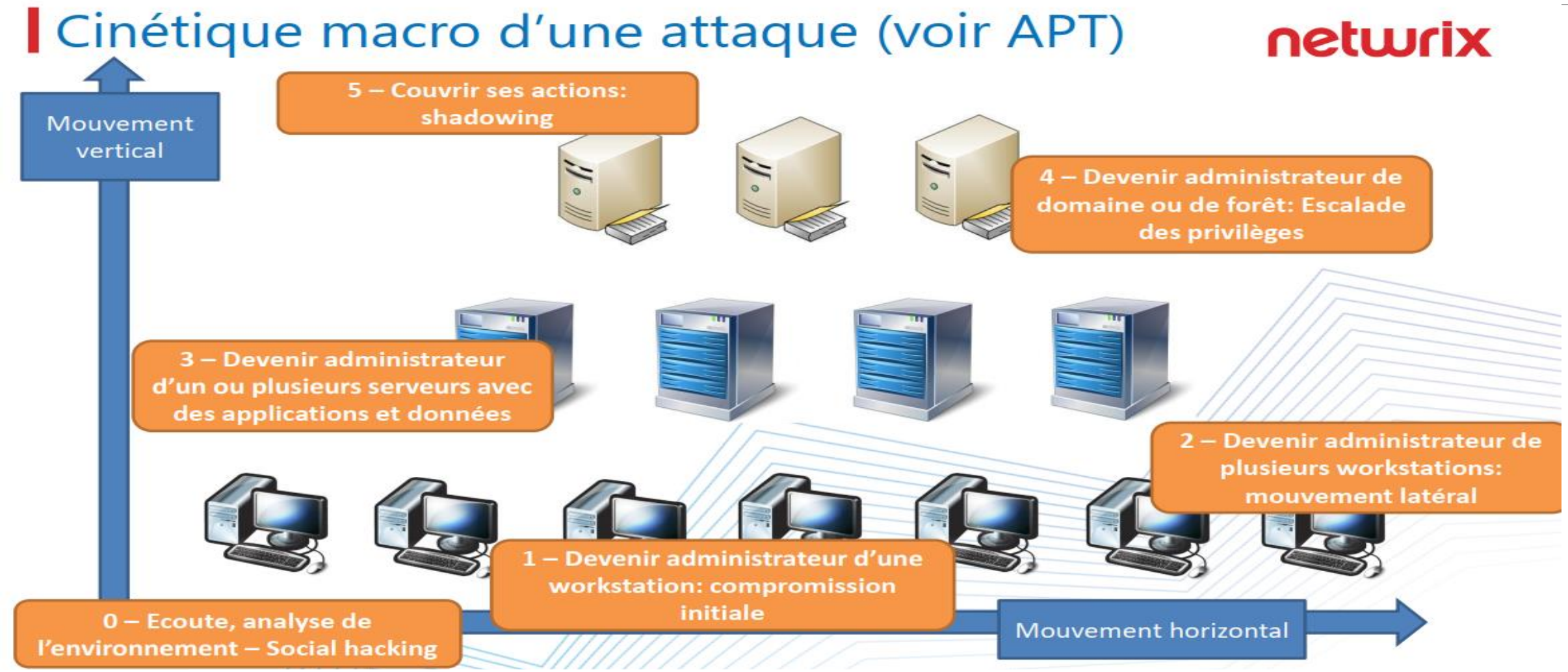
Par Corentin Durand | Mardi 10 Décembre 2019
Suivre @zdnetfr

Vers l'industrialisation

Le rançongiciel présente un avantage dont peu d'attaques informatiques peuvent se targuer : être rémunératrice et, en conséquence, auto-financée. Comme une entreprise informatique qui dégage des bénéfices, une entreprise cybercriminelle peut investir ses bénéfices dans la recherche et le développement, augmenter l'échelle de ses attaques et même, recruter. On observe bien là que la technique n'est pas première dans le succès du rançongiciel, mais secondaire, au sens où elle est permise par son économie et liée à un stade de maturité.

Cybersécurité: menaces, risques et bonne pratiques

Objectifs des attaques



Dès lors que le rançongiciel est parvenu à pénétrer le SI d'Altran, celui-ci a pris soin de chiffrer un à un les différents fichiers de l'entreprise.

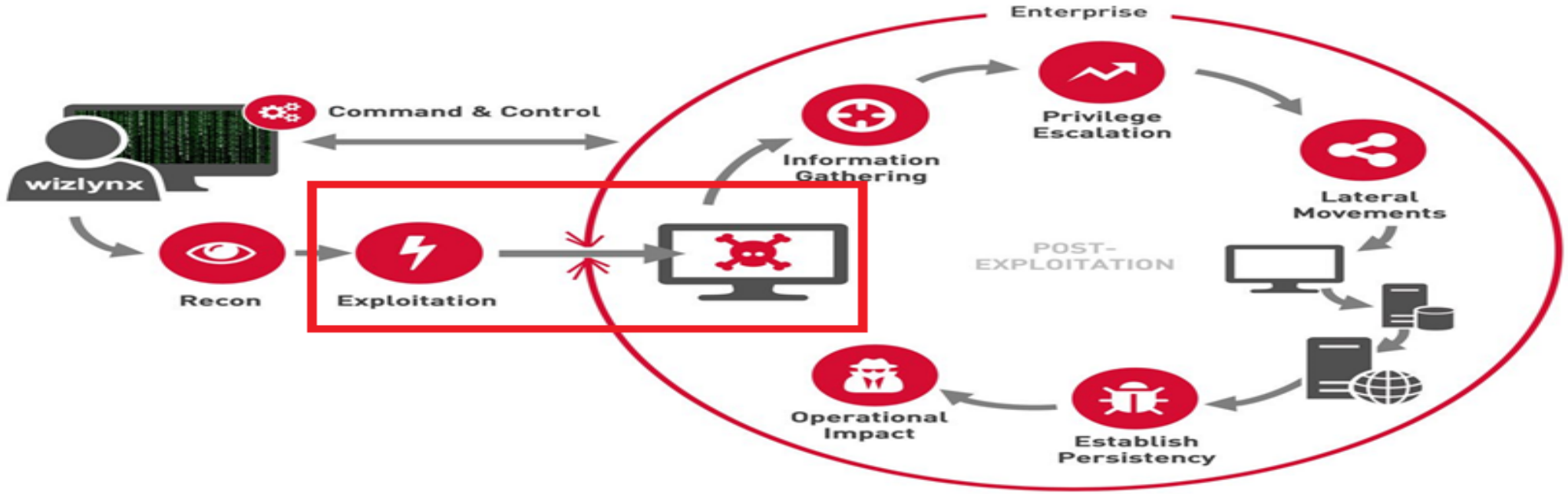
La société aurait alors décidé de payer la rançon (300 bitcoins soit près d'un million d'euro) et donc de ne pas se conformer aux recommandations des autorités. Seulement voilà, mal lui en a pris puisque jamais elle n'a reçu la clé de déchiffrement.

Cybersécurité: menaces, risques et bonne pratiques

Rançongiciel : mode opératoire des attaquants

Cybersécurité: menaces, risques et bonne pratiques

Méthodologie : Etape n°1 : Obtenir un accès au réseau interne



- Compromission initiale : obtenir un accès au réseau local
  - Multiples vecteurs d'intrusion
    - **RDP**
    - **Intrusion via un serveur web (tomcat, mysql)**
    - **Ré-utilisation d'un mot de passe**
    - **Clé USB**
    - **Courriel avec pièce jointe**

Vous trouverez ci-dessous les informations échangées lors de l'entretien et qui complète les informations déjà communiquées par mail.

L'attaquant a exploité des ports RDP exposés sur Internet pour infecter la première machine.

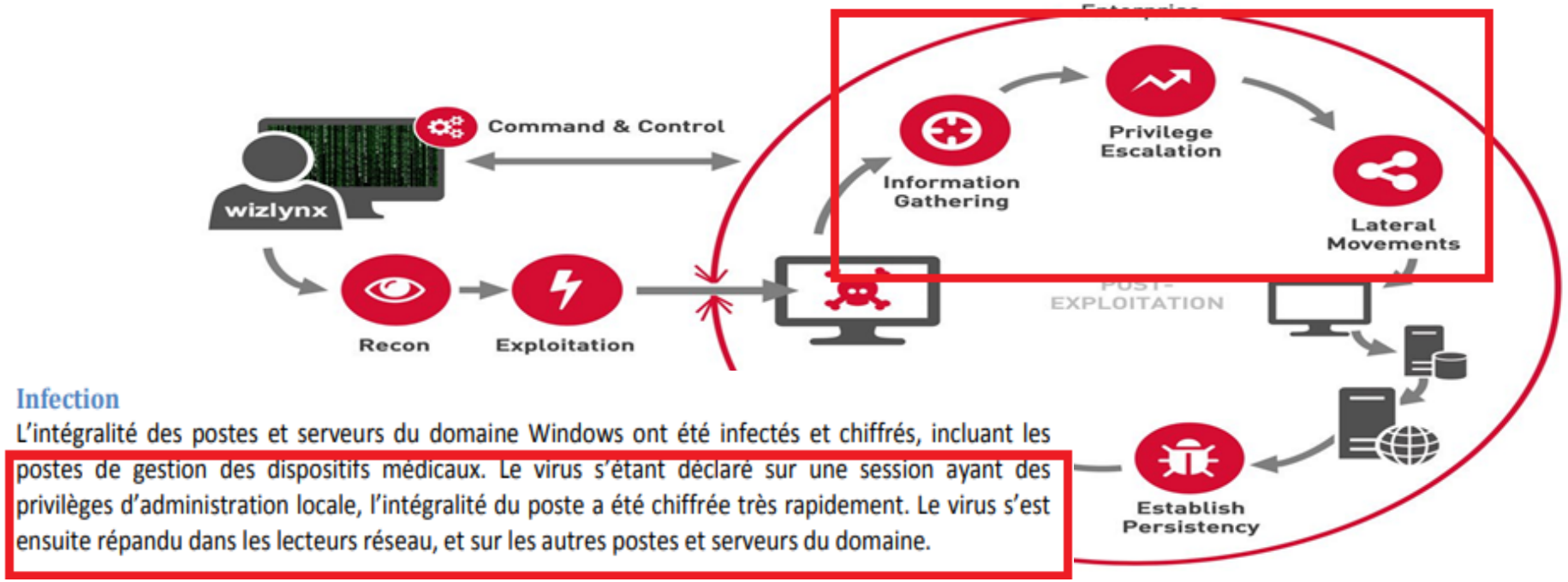
Il reste à confirmer la perte réelle de données à l'issue de la phase de restauration des systèmes.

Origine

L'origine de l'infection n'est pas confirmée. Toutefois, la structure dispose d'un réseau « propre », avec accès à internet fortement restreint (liste blanche), des restrictions sur les téléchargements et sur la connexion de supports USB. Seuls les emails sont autorisés pour une population identifiée. Un email malveillant ouvert par un utilisateur constitue la piste privilégiée.

Cybersécurité: menaces, risques et bonne pratiques

Méthodologie : Etape n°2 : Déplacements latéraux



- Récupération d'informations sur le poste et ré-utilisation des mots de passe locaux pour se déplacer sur d'autres postes
  - A partir d'un poste, rebond sur d'autres postes
    - **Mouvements latéraux (escalade horizontale) / déplacement latéral**
  - A partir d'un compte sans privilèges, obtention d'un compte administrateur
    - **Mouvements verticaux (escalade verticale)**

Cybersécurité: menaces, risques et bonne pratiques

Méthodologie : Etape n°2 : Déplacements latéraux

- Récupération d'informations sur le poste et ré-utilisation des mots de passe locaux pour se déplacer sur d'autres postes
  - **A partir d'un poste, rebond sur d'autres postes**
    - **Récupération des identifiants sur le poste et ré-utilisation sur d'autres postes (même compte administrateur local utilisé sur l'ensemble des postes)**
      - **Utilisation d'outils de dump de mots de passe**

Pourquoi Petya se propage-t-il bien plus vite que WannaCry ?

Petya intègre une charge utile supplémentaire visant à récupérer les informations d'identification, soit l'une des fonctions de Mimikatz. Mimikatz est un outil véritablement incroyable permettant d'évaluer les environnements d'authentification de Windows. Plus précisément, le but de Mimikatz est d'extraire les informations d'identification à l'aide de différentes techniques telles que la célèbre attaque « pass-the-hash ». Pour vous donner une idée de son impact, sachez que cette fonction s'empare du hash du réseau et tente de le réutiliser afin de s'authentifier sans connaître le mot de passe.

- **Utilisation de vulnérabilités Windows**

Petya intègre différentes charges utiles pour se propager et infecter ses victimes. En résumé, il renferme les mêmes exploits que WannaCry (EternalBlue et une variante baptisée EternalRomance). En mars 2017, Windows a publié le patch MS17-010 pour corriger les failles de sécurité.

Cybersécurité: menaces, risques et bonne pratiques

Méthodologie : Etape n°3 : Charge finale

- Une fois les identifiants des administrateurs récupérés
  - **Déploiement de la charge finale et demande de rançon**
  - **Exfiltration des données et diffusion des documents (pression)**

Cybersécurité: menaces, risques et bonne pratiques

Réaction à chaud à une attaque – Rappel des bons reflexes

- En cas de système d'information massivement compromis, dans l'ordre:
  - Déconnectez vous pour couper les communications de l'attaquant
  - N‘éteignez pas les systèmes compromis, déconnectez les, et si possible réalisez un snapshot ou dump mémoire
  - Vérifiez les taches planifiées, tuez les processus suspects
  - Protégez vos sauvegardes et vérifiez leur integrité

- Ensemble des actions à mener en cas d’incident lié à un maliciel rappelées sur la fiche « Agir contre un maliciel »
  - https://cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiche_Maliciel_IR_RSSI.pdf

Cybersécurité: menaces, risques et bonne pratiques

Bonnes pratiques

Recommandations et bonnes pratiques

- Fiche prévention contre les maliciels
  - https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiche_Maliciel_P_RSSI.pdf
- Plan d'action pour réduire l'impact d'une attaque par rançongiciel sur l'Active Directory et les sauvegardes (publié en fin de semaine)

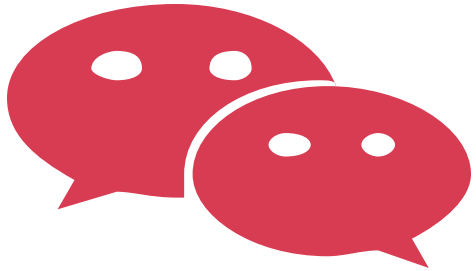
CRYPTOVIRUS : RECOMMANDATIONS POUR PROTÉGER LES SAUVEGARDES LOCALES

Un centre hospitalier a récemment été victime d'un cryptovirus qui a chiffré toutes les données de ses serveurs. Les sauvegardes présentes sur un serveur dédié, mais insuffisamment sécurisé du point de vue de l'accès réseau et des droits, ont aussi été chiffrées.

Pour protéger les sauvegardes locales contre cette menace, il est recommandé :

- D'utiliser des serveurs physiques dédiés au stockage des sauvegardes ;
- De segmenter le réseau en sous-réseaux isolés entre eux et protégés d'internet par une DMZ ;
- De limiter les actions possibles depuis le réseau au dépôt de fichiers dans le respect du principe de moindre privilège :
  - Autoriser les connexions réseau (SFTP, SMB…) à des comptes dédiés au dépôt de sauvegardes (sans privilèges administrateur) ;
  - Bloquer toutes les connexions depuis le réseau à des comptes privilégiés ;
  - Accorder uniquement le droit de suppression des fichiers de sauvegarde à un administrateur local des serveurs.

En savoir plus sur les cryptovirus : https://www.cyberveillesante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiches_reflexes-Cryptovirus_v1.5.pdf



Temps d’échanges

Vos remarques ? Vos questions ?

AGENCE DU NUMÉRIQUE EN SANTÉ

Sommaire

CERT Santé

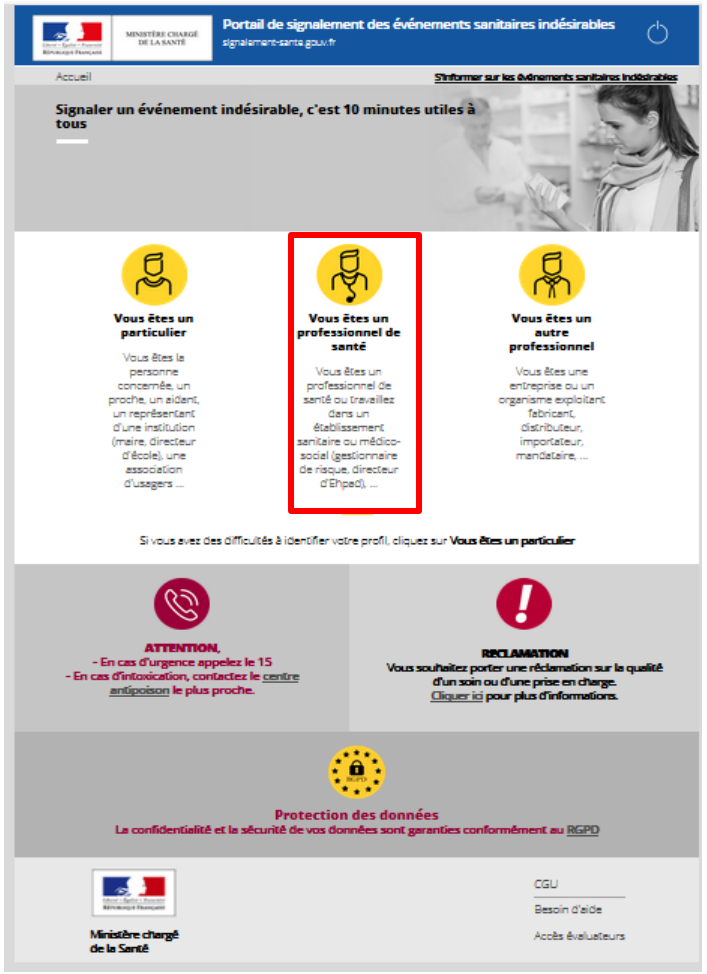
Observatoire des incidents de sécurité 2020

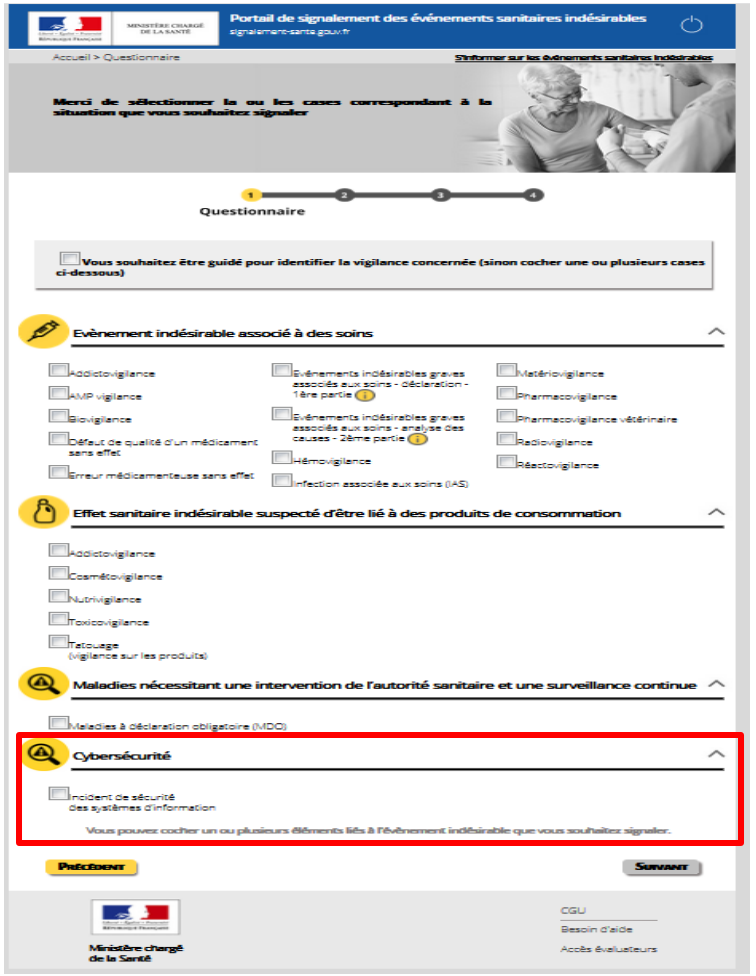
- Une croissance de la menace confirmée en 2020 – tendance partagée avec l'ANSSI
  - 60 % des incidents déclarés ont une origine malveillante (+17% par rapport à 2019)
    - 43% sont des maliciels (rançongiciels)
    - 35 % sont liés à une activité de hameçonnage (phishing)
    - 42 % sont liés à l'exploitation d'une vulnérabilité sur un accès à distance (Bureau à distance, VPN, Webmail)
  - 58 % des incidents ont un impact sur des informations patient à caractère personnel (disponibilité des données principalement)
    - Perturbation du fonctionnement de la structure pendant plusieurs jours voire plusieurs semaines
    - Perte d'activité et financière (report des soins et de rdv / intervention d'un prestataire spécialisé)
- Risque d'attaque moins important lorsque l'outil informatique n'est pas exposé sur Internet et lorsque les bonnes pratiques d'hygiène informatique sont respectées

CERT Santé

Déclaration d'incident : les démarches réglementaires

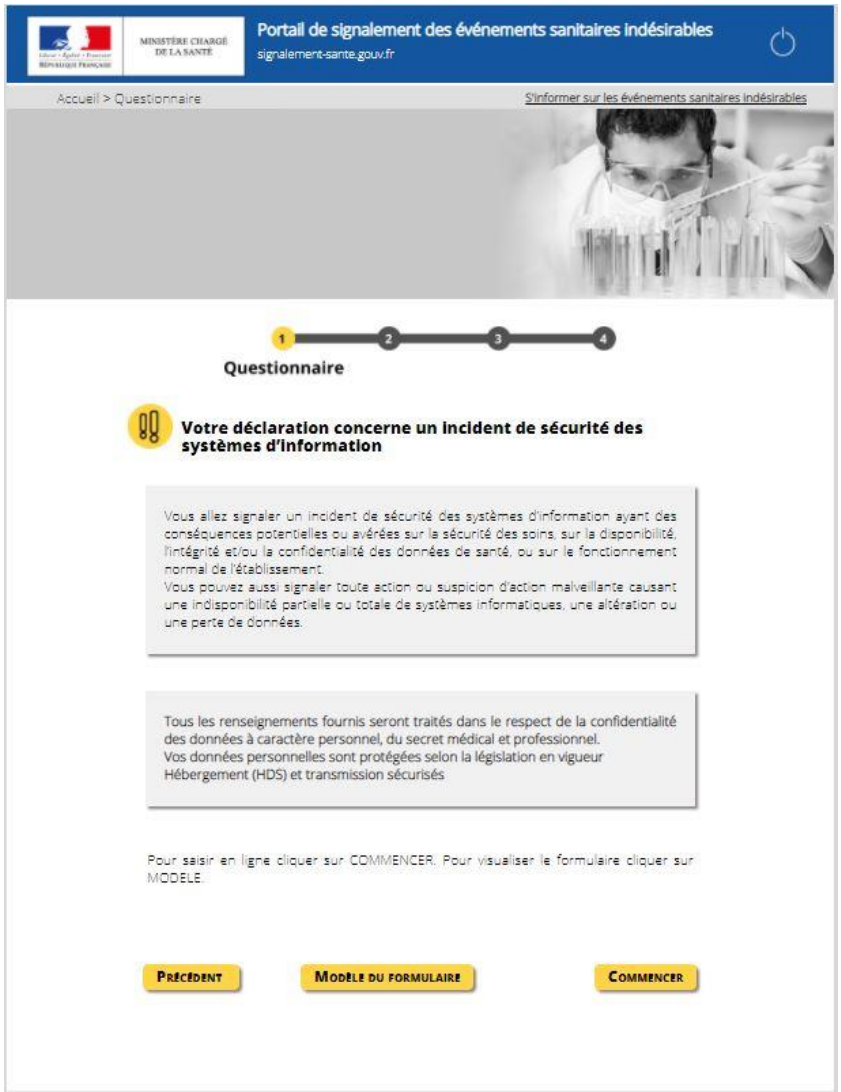
- Déclarer son incident et demander un appui (décret n°2016-1214 du 12 septembre 2016 et l'arrêté du 30 octobre 2017 / ordonnance n° 2020-1407 du 18 novembre 2020)
  - Portail des signalements des évènements sanitaires indésirables
    - https://signalement.social-sante.gouv.fr - Espace « Professionnels de Santé »

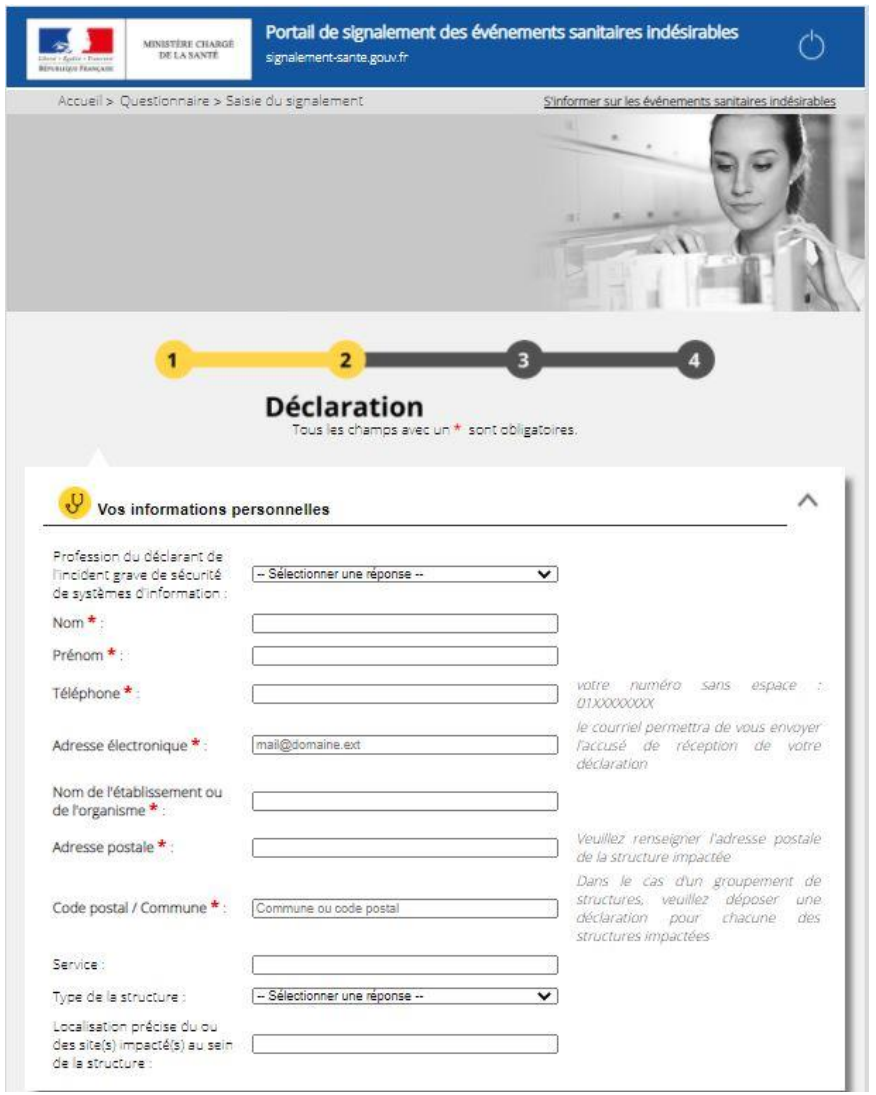




CERT Santé

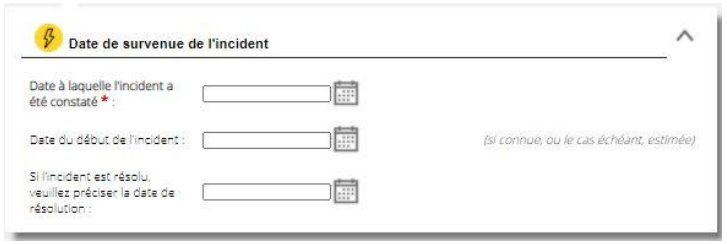
Déclaration d'incident : les démarches réglementaires

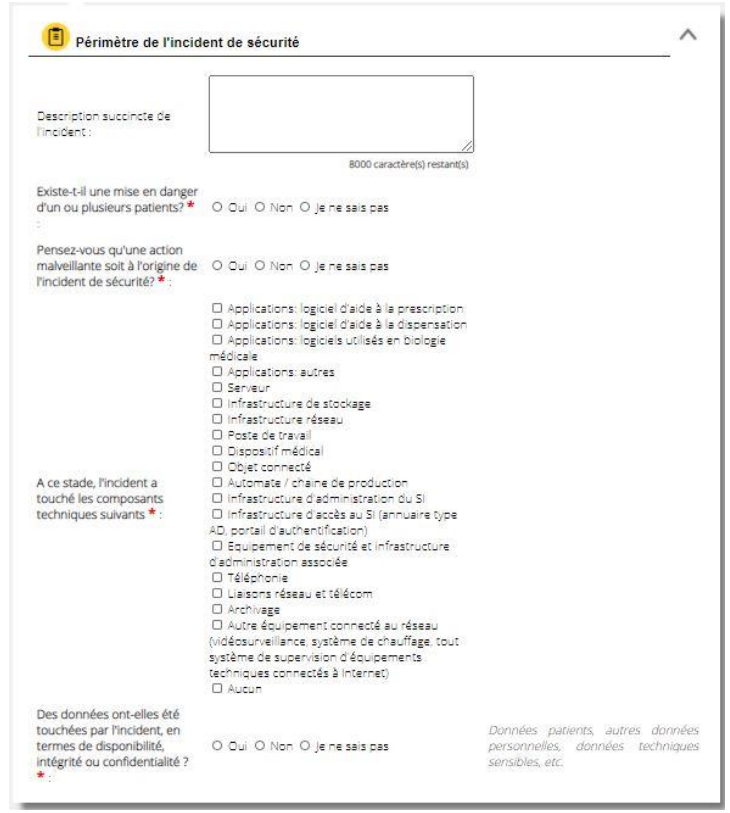




CERT Santé

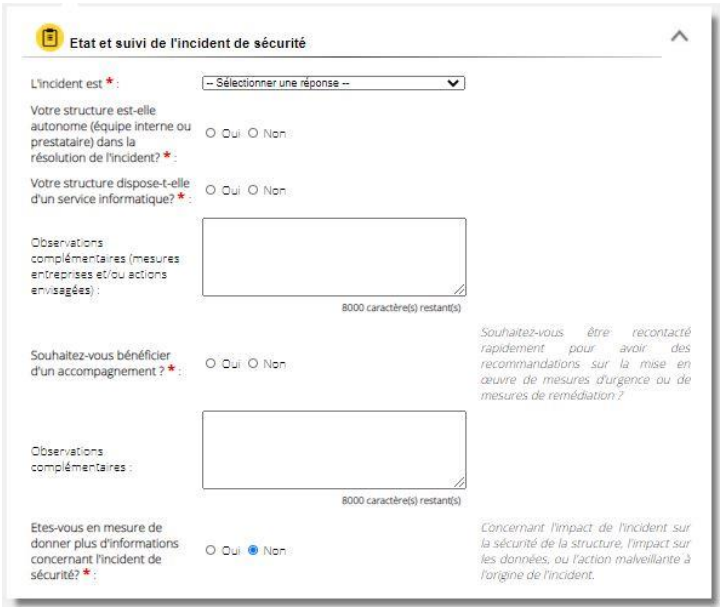
Déclaration d'incident : les démarches réglementaires

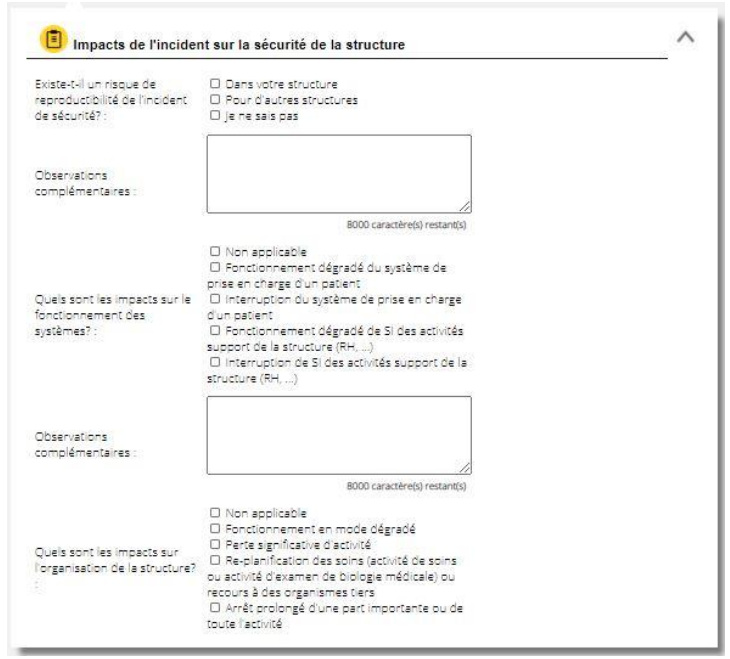




CERT Santé

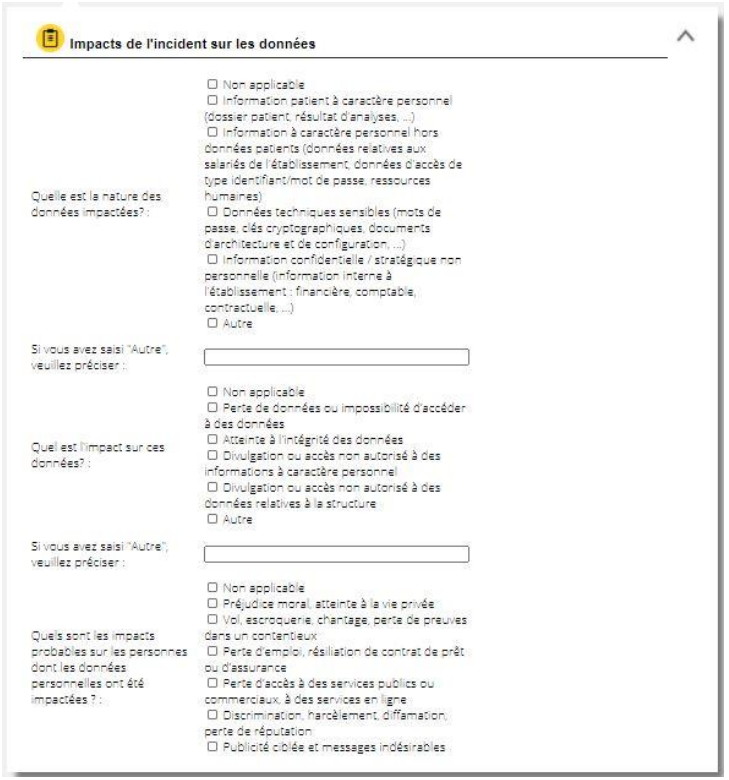
Déclaration d'incident : les démarches réglementaires

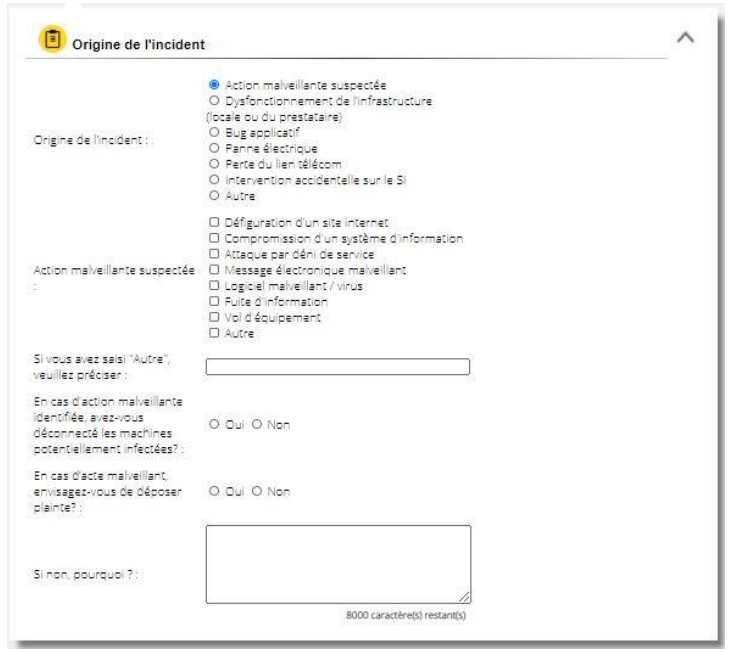




CERT Santé

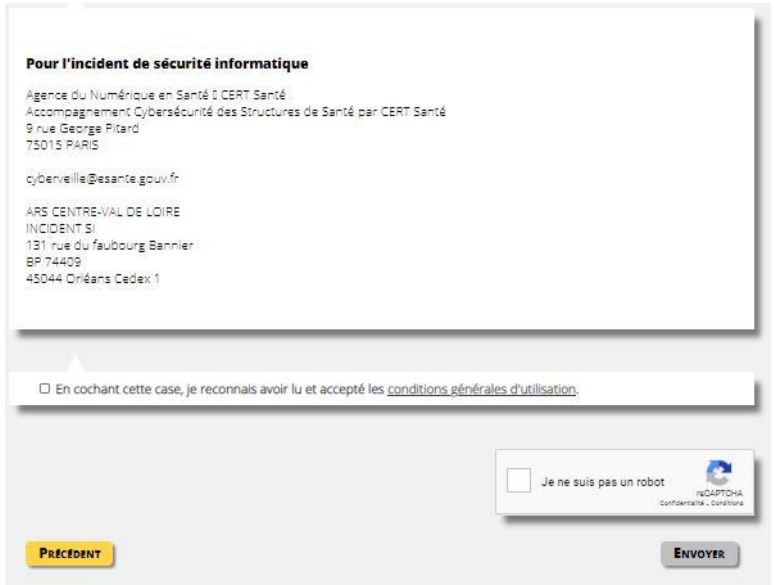
Déclaration d'incident : les démarches réglementaires

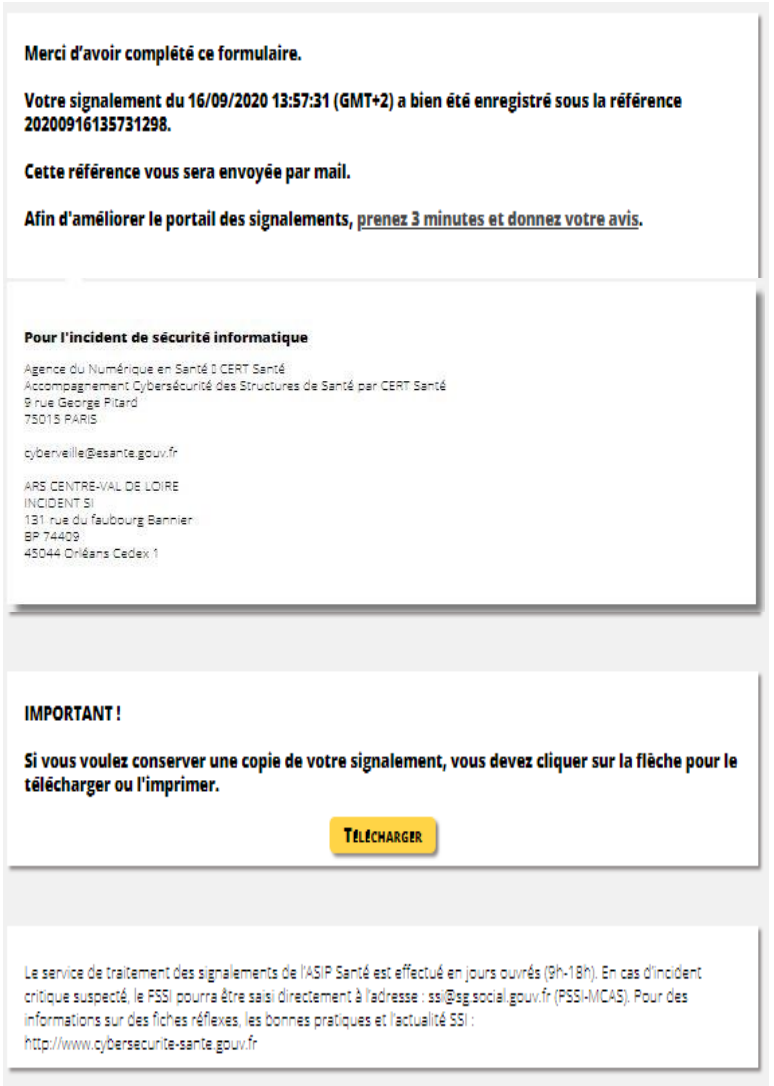




CERT Santé

Déclaration d'incident : les démarches réglementaires





CERT Santé

Réponse aux incidents de sécurité

Déclaration de l'incident et demande d'un appui du CERT Santé

- Portail des signalements des évènements sanitaires indésirables - **https://signalement.social-sante.gouv.fr/**
- En cas d'urgence / incident majeur – accueil téléphonique en heures ouvrées 9h-18h sans interruption ((horaires métropole)) - **+33 09 72 43 91 25 / cyberveille@esante.gouv.fr**
- En cas d'incident majeur en HNO/JNO, les demandes sont prises en charge par l'astreinte HFDS / FSSI et l'ANSSI - **ssi@sg.social.gouv.fr / cert-fr.cossi@ssi.gouv.fr - +33 (0)1 71 75 84 68**

Qualification de l'incident et coordination de la réponse

- Analyse et qualifie les incidents signalés en vue de prioriser leur traitement
- Informe systématiquement le FSSI et l'ARS compétente territorialement ainsi que l'ANSSI pour les OSE (CHU) ou les incidents majeurs
- Alerte le CORRUSS/DGS en cas d'impact ou de suspicion d'impact sanitaire
- Formule des recommandations et renvoie vers les fiches réflexes (portail cyberveille-santé)
- Assure le suivi du traitement jusqu'à sa clôture

CERT Santé

Réponse aux incidents de sécurité

Fiche de présentation de l'appui sur le portail cyberveille-santé

https://cyberveille-sante.gouv.fr/sites/default/files/documents/ACSS_Accompagnement_Reponse_Incident.pdf

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Coopération avec le GIP cybermalveillance.gouv.fr pour aider les victimes à qualifier l'incident et identifier un prestataire de proximité

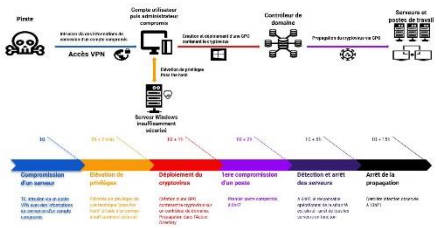
AGENCE DU NUMÉRIQUE EN SANTÉ

Sommaire

CERT Santé

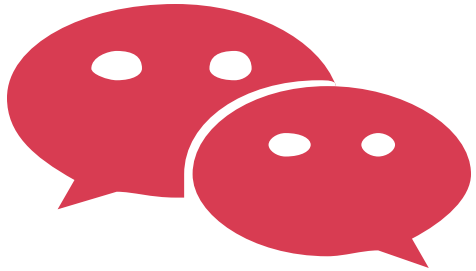
Les ressources méthodologiques et les outils accessibles

- Portail cyberveille-santé (https://www.cyberveille-sante.gouv.fr/)
  - Publication de bulletins d'information et d'alertes (vulnérabilités de dispositifs médicaux, de logiciels de santé ou de logiciels standard, actes de cybermalveillance) - 10 bulletins par semaine en moyenne
  - 11 fiches reflexes présentant des recommandations pour répondre à des incidents ayant différentes origines malveillantes - 2 fiches spécifiques sur les maliciels / rançongiciels
  - 650 comptes d'accès à l'espace privé du portail / une majorité de RSSI de structures du secteur public



- Mise à disposition de retours d'expérience et d'un forum d'échanges sur l'espace privé du portail pour favoriser la coopération et l'entraide entre les acteurs (ministère, ARS et structures de santé) face à la menace de cybersécurité
  - Mise à disposition d'un retex sur une attaque par cryptovirus d'un groupe de centres de dialyse

- Animation trimestrielle d'un webinaire sur un sujet de cybersécurité
  - Présentation d'un bilan après 18 mois du service de cyber-surveillance en octobre 2020
  - Présentation de l'appui à la réponse à incident et sa dimension technique en janvier 2021



Temps d’échanges

Vos remarques ? Vos questions ?