



Cybersécurité dans le secteur médico-social

ANS - CERT Santé (Cellule ACSS)

Jeudi 15 avril 2021

Cédric BERTRAND

Expert sécurité

cedric.bertrand@esante.gouv.fr



Emmanuel SOHIER

Responsable CERT Santé

Emmanuel.sohier@esante.gouv.fr





Sommaire

Cybersécurité : menaces, risques et bonnes pratiques

Déclaration d'incident : les obligations réglementaires et démarches à réaliser

Pour aller plus loin : Les ressources méthodologiques et outils accessibles



Sommaire

Cybersécurité : menaces, risques et bonnes pratiques

Déclaration d'incident : les obligations réglementaires et démarches à réaliser

Pour aller plus loin : Les ressources méthodologiques et outils accessibles

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



tout de même du matériel médical - un scanner - et le rend inutilisable. « L'aide au diagnostic des patients a été perturbée, 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

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 touché peu d'ordinateurs, mais contaminé

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-etablislements-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, ...

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.



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.*

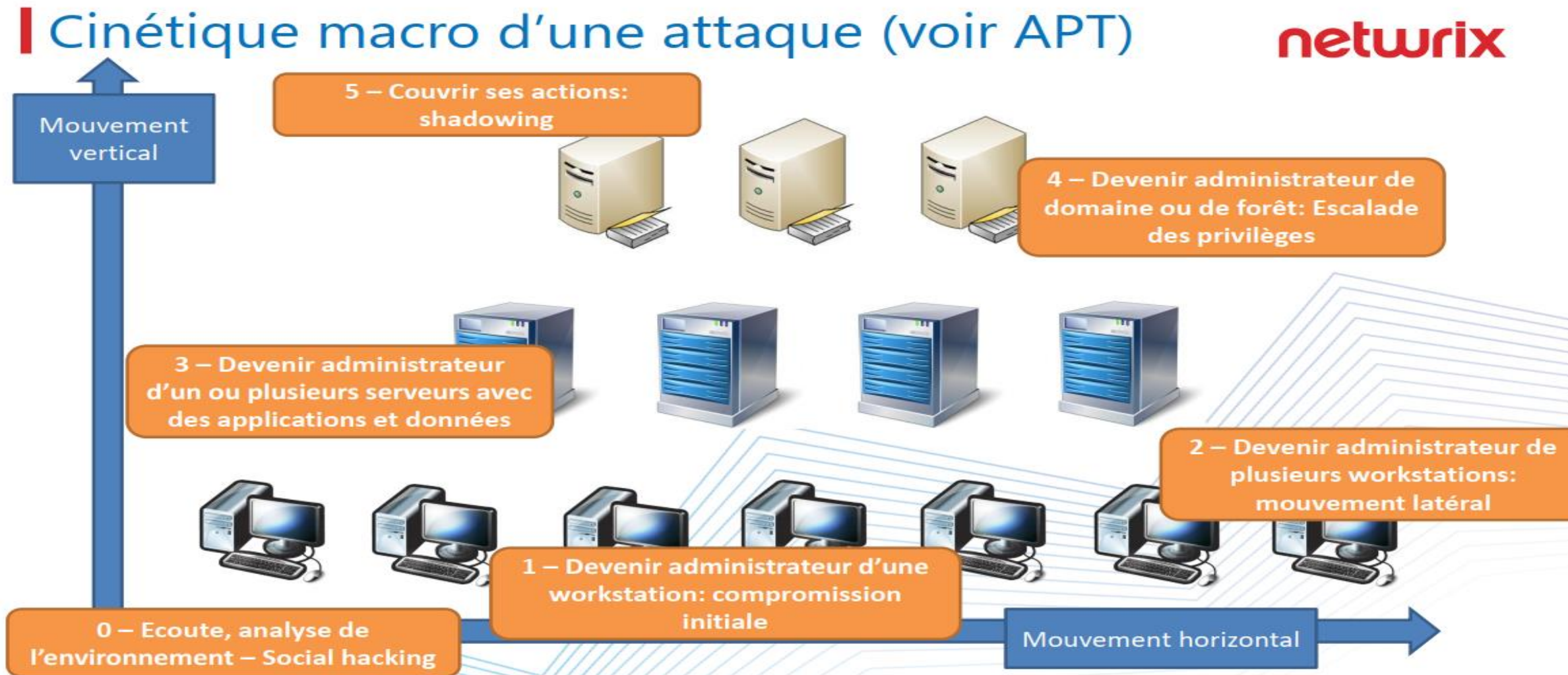


Par Corentin Durand | Mardi 10 Décembre 2019
Suivre @zdnetfr

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.

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.

L'attaquant envoie un spam

1.



Le spam évite le filtre anti-spam de la victime et arrive dans sa boîte mail

2.



La victime clique sur un lien malveillant

3.



Echec des mécanismes de protection du poste

4.



8.



7.



6.



5.

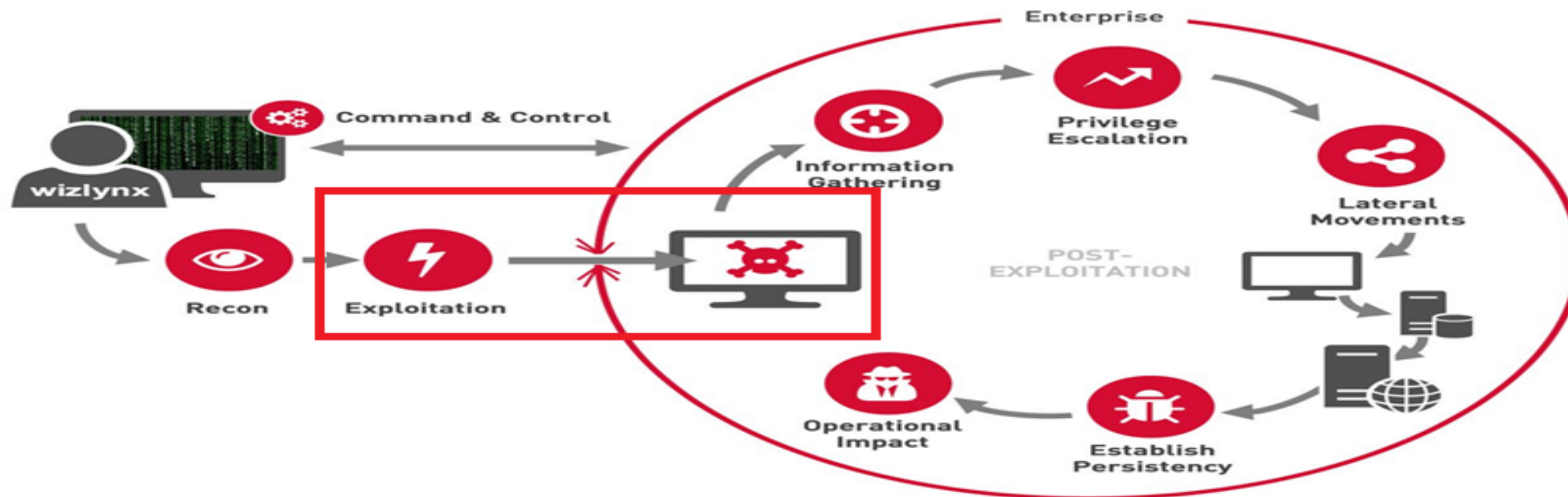


L'attaquant tente de répandre le virus de façon latérale aux autres ordinateurs de l'entreprise

Envoi d'une notification, en général une demande de rançon

Le ransomware chiffre les données de la victime

Le malware se connecte grâce à un serveur C&C pour donner des instructions*



► 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.

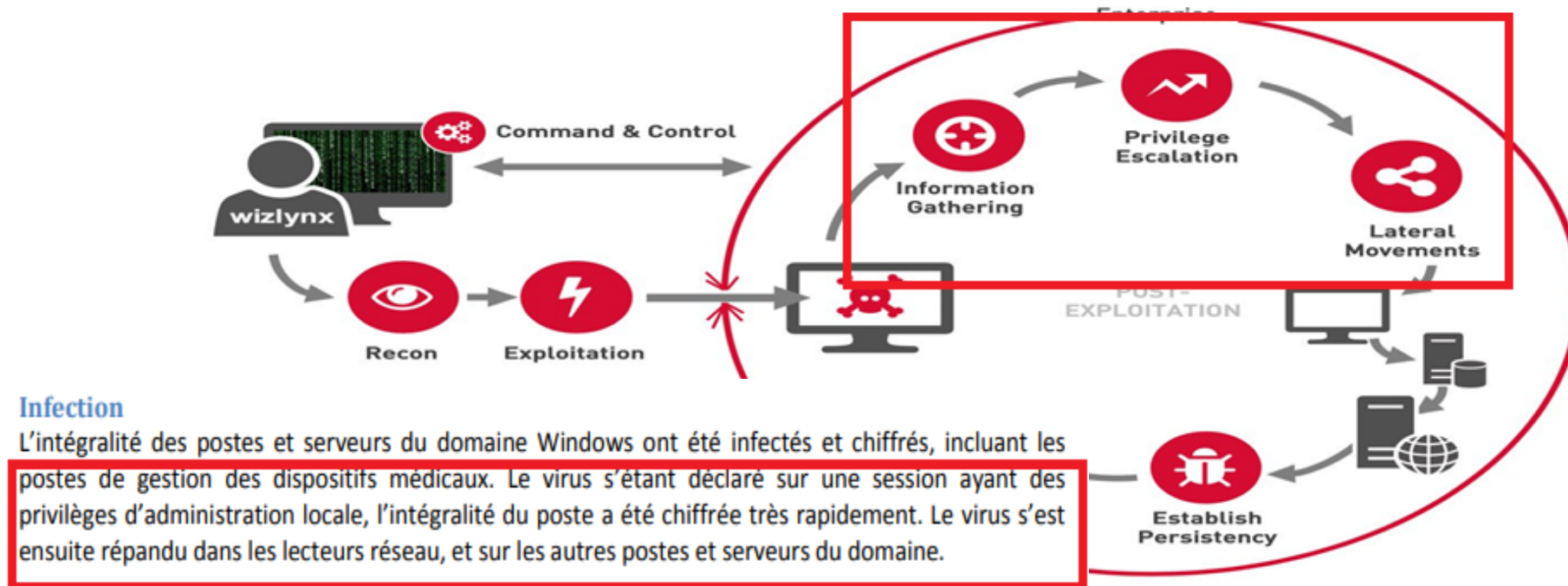
Il reste à confirmer la perte réelle de données à l'issue de la phase de restauration des systèmes.

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 bonnes 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 bonnes 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

Ransomware: les attaques sur les hôpitaux français se ...

L'hôpital Nord-Ouest, situé à Villefranche-sur-Saône, Tarare et Trévoux, est victime d'un rançongiciel qui a bloqué plus de 3 000 postes ...

16 févr. 2021

Pierre Fabre : Le groupe Revil revendique l'attaque

Le groupe de ransomware Revil/Sodinokibi a revendiqué l'attaque, en diffusant sur son site des documents volés sur le SI de la société. Louis ...

Il y a 4 heures

Des hackers s'attaquent au Téléthon : la biotech YposKesi ...

... s'attaquent au Téléthon : la biotech YposKesi cible d'un ransomware ... de 23 Go de données issues du système informatique de YposKesi.

Il y a 2 semaines

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

- ▶ 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 intégrité

- ▶ 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

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)

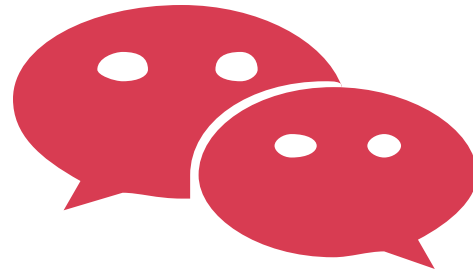
CRYPTOVIRUS : RECOMMANDATIONS POUR PROTÉGER LES SAUVEGARDES LOCALES

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 ?



Sommaire

Cybersécurité : menaces, risques et bonnes pratiques

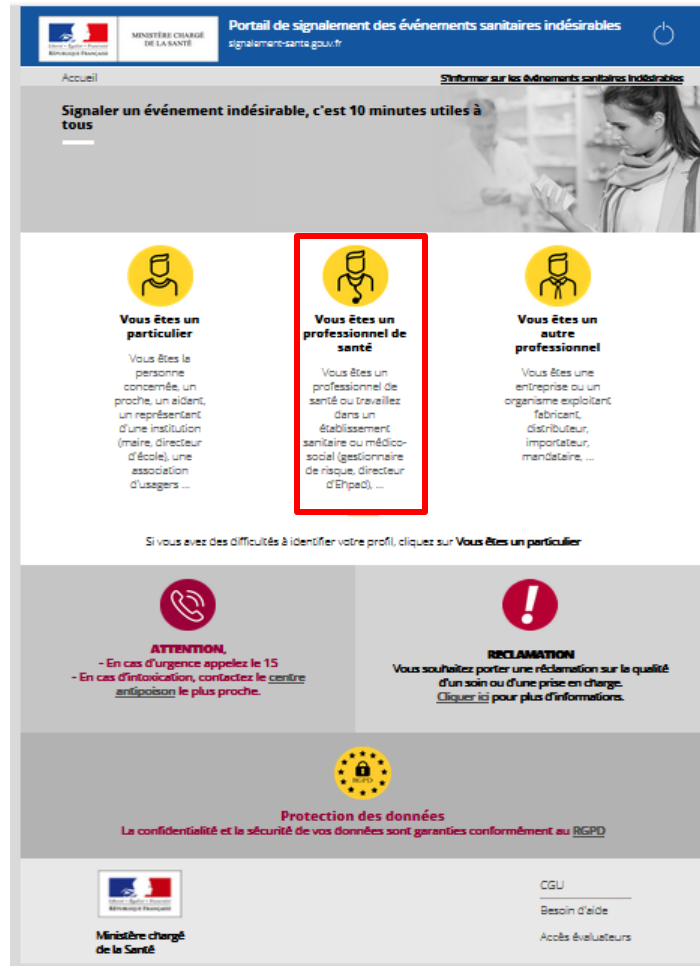
Déclaration d'incident : les obligations réglementaires et démarches à réaliser

Pour aller plus loin : Les ressources méthodologiques et outils accessibles

- ▶ 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

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 événements sanitaires indésirables
 - <https://signalement.social-sante.gouv.fr> - Espace « Professionnels de Santé »



Portail de signalement des événements sanitaires indésirables
signalement-social-sante.gouv.fr

Accueil

Signaler un événement indésirable, c'est 10 minutes utiles à tous

Vous êtes un particulier
Vous êtes la personne concernée, un proche, un aidant, un représentant d'une institution (maire, directeur d'école), une association de usagers...

Vous êtes un professionnel de santé
Vous êtes un professionnel de santé ou travaillez dans un établissement sanitaire ou médico-social (gestionnaire de risque, directeur d'établissement)...

Vous êtes un autre professionnel
Vous êtes une entreprise ou un organisme exploitant fabricant, distributeur, importateur, mandataire, ...

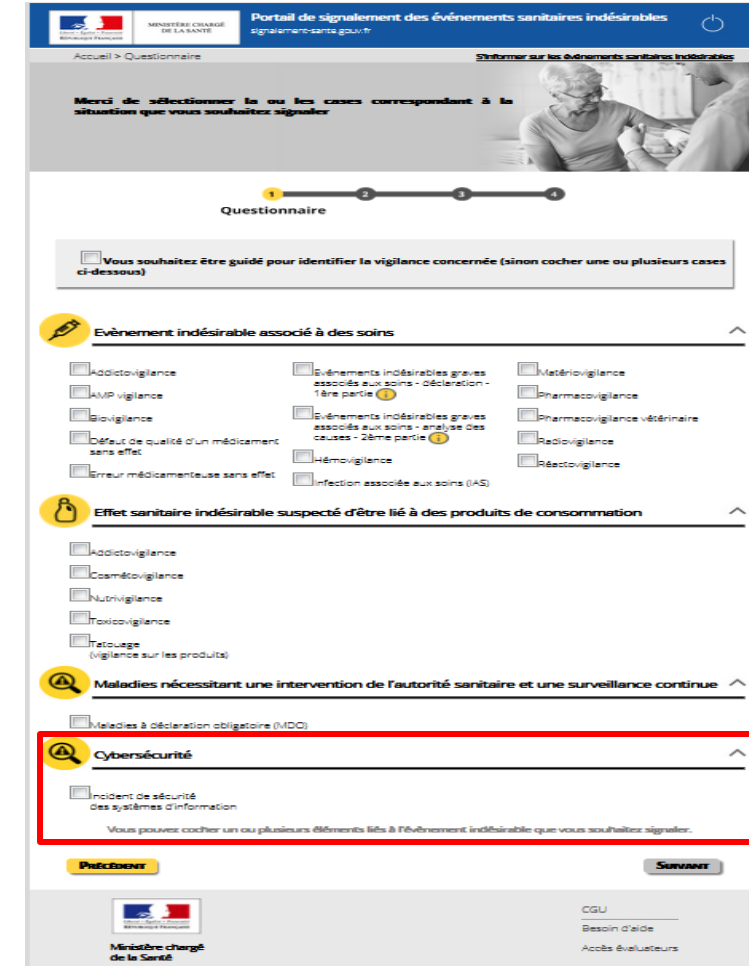
Si vous avez des difficultés à identifier votre profil, cliquez sur **Vous êtes un particulier**

ATTENTION
- En cas d'urgence appelez le 15
- En cas d'intoxication, contactez le centre antipoison le plus proche.

RECLAMATION
Vous souhaitez porter une réclamation sur la qualité d'un soin ou d'une prise en charge. [Cliquez ici](#) pour plus d'informations.

Protection des données
La confidentialité et la sécurité de vos données sont garanties conformément au RGPD

CGU
Besoin d'aide
Accès évaluateurs

Portail de signalement des événements sanitaires indésirables
signalement-social-sante.gouv.fr

Accueil > Questionnaire

Merci de sélectionner la ou les cases correspondant à la situation que vous souhaitez signaler

Questionnaire

☐ Vous souhaitez être guidé pour identifier la vigilance concernée (sinon cocher une ou plusieurs cases ci-dessous)

Événement indésirable associé à des soins

☐ Addictovigilance
☐ ALMP vigilance
☐ Biovigilance
☐ Défaut de qualité d'un médicament sans effet
☐ Erreur médicamenteuse sans effet

☐ Événements indésirables graves associés aux soins - 1ère partie
☐ Événements indésirables graves associés aux soins - 2ème partie
☐ Hémo-vigilance
☐ Infection associée aux soins (IAS)

☐ Matérovigilance
☐ Pharmacovigilance
☐ Pharmacovigilance vétérinaire
☐ Radiovigilance
☐ Réactovigilance

Effet sanitaire indésirable suspecté d'être lié à des produits de consommation

☐ Addictovigilance
☐ Cosmétovigilance
☐ Nutrivigilance
☐ Toxicovigilance
☐ Traçage (vigilance sur les produits)

Maladies nécessitant une intervention de l'autorité sanitaire et une surveillance continue

☐ Maladies à déclaration obligatoire (MDO)

Cybersécurité

☐ Incident de sécurité des systèmes d'information

Vous pouvez cocher un ou plusieurs éléments liés à l'événement indésirable que vous souhaitez signaler.

PRÉCÉDENT **SUIVANT**

CGU
Besoin d'aide
Accès évaluateurs

Déclaration d'incident : les démarches réglementaires

Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr

Accueil > Questionnaire

1 2 3 4

Questionnaire

Votre déclaration concerne un incident de sécurité des systèmes d'information

Vous allez signaler un incident de sécurité des systèmes d'information ayant des conséquences potentielles ou avérées sur la sécurité des soins, sur la disponibilité, l'intégrité et/ou la confidentialité des données de santé, ou sur le fonctionnement normal de l'établissement. Vous pouvez aussi signaler toute action ou suspicion d'action malveillante causant une indisponibilité partielle ou totale de systèmes informatiques, une altération ou une perte de données.

Tous les renseignements fournis seront traités dans le respect de la confidentialité des données à caractère personnel, du secret médical et professionnel. Vos données personnelles sont protégées selon la législation en vigueur Hébergement (HDS) et transmission sécurisés.

Pour saisir en ligne cliquer sur COMMENCER. Pour visualiser le formulaire cliquer sur MODÈLE.

PRÉCÉDENT MODÈLE DU FORMULAIRE COMMENCER



Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr

Accueil > Questionnaire > Saisie du signalement

1 2 3 4

Déclaration

Tous les champs avec un * sont obligatoires.

Vos informations personnelles

Profession du déclarant de l'incident grave de sécurité de systèmes d'information : -- Sélectionner une réponse --

Nom * :

Prénom * :

Téléphone * : votre numéro sans espace : 01XXXXXXXX

Adresse électronique * : le courriel permettra de vous envoyer l'accusé de réception de votre déclaration

Nom de l'établissement ou de l'organisme * :

Adresse postale * : Veuillez renseigner l'adresse postale de la structure impactée

Code postal / Commune * : Dans le cas d'un groupement de structures, veuillez déposer une déclaration pour chacune des structures impactées

Service :

Type de la structure : -- Sélectionner une réponse --

Localisation précise du ou des site(s) impacté(s) au sein de la structure :

Déclaration d'incident : les démarches réglementaires


 MINISTÈRE CHARGÉ DE LA SANTÉ
 signalement-sante.gouv.fr

Portail de signalement des événements sanitaires indésirables

Accueil > Questionnaire > Saisie du signalement

[S'informer sur les événements sanitaires indésirables](#)

1 2 3 4

Déclaration

Tous les champs avec un * sont obligatoires.


Date de survenue de l'incident

Date à laquelle l'incident a été constaté * :

Date du début de l'incident : *(si connue, ou le cas échéant, estimée)*

Si l'incident est résolu, veuillez préciser la date de résolution :




 MINISTÈRE CHARGÉ DE LA SANTÉ
 signalement-sante.gouv.fr

Portail de signalement des événements sanitaires indésirables

Accueil > Questionnaire > Saisie du signalement

[S'informer sur les événements sanitaires indésirables](#)

1 2 3 4

Déclaration

Tous les champs avec un * sont obligatoires.


Périmètre de l'incident de sécurité

Description succincte de l'incident :

Existe-t-il une mise en danger d'un ou plusieurs patients? *

Pensez-vous qu'une action malveillante soit à l'origine de l'incident de sécurité? *

A ce stade, l'incident a-t-il touché les composants techniques suivants * :

Des données ont-elles été touchées par l'incident, en termes de disponibilité, d'intégrité ou de confidentialité? *

☐ Applications : logiciel d'aide à la prescription
☐ Applications : logiciel d'aide à la dispensation
☐ Applications : logiciels utilisés en biologie médicale
☐ Applications : autres
☐ Serveur
☐ Infrastructure de stockage
☐ Infrastructure réseau
☐ Poste de travail
☐ Dispositif médical
☐ Objet connecté
☐ Automate / chaîne de production
☐ Infrastructure d'administration du SI
☐ Infrastructure d'accès au SI (annuaire type AD, portail d'authentification)
☐ Equipement de sécurité et infrastructure d'administration associée
☐ Téléphonie
☐ Liaisons réseau et télécom
☐ Archivage
☐ Autre équipement connecté au réseau (vidéosurveillance, système de chauffage, tout système de supervision d'équipements techniques connectés à Internet)
☐ Aucun

Données : patients, autres données personnelles, données techniques sensibles, etc.

Déclaration d'incident : les démarches réglementaires



Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr

Accueil > Questionnaire > Saisie du signalement

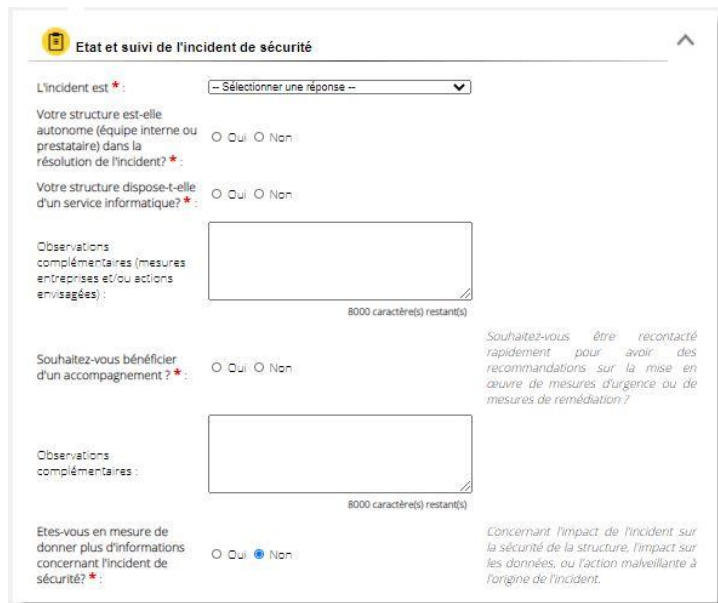
Déclaration
Tous les champs avec un * sont obligatoires.



Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr

Accueil > Questionnaire > Saisie du signalement

Déclaration
Tous les champs avec un * sont obligatoires.



Etat et suivi de l'incident de sécurité

L'incident est * : -- Sélectionner une réponse --

Votre structure est-elle autonome (équipe interne ou prestataire) dans la résolution de l'incident? * : ☐ Oui ☐ Non

Votre structure dispose-t-elle d'un service informatique? * : ☐ Oui ☐ Non

Observations complémentaires (mesures entreprises et/ou actions envisagées) :

8000 caractères(s) restant(s)

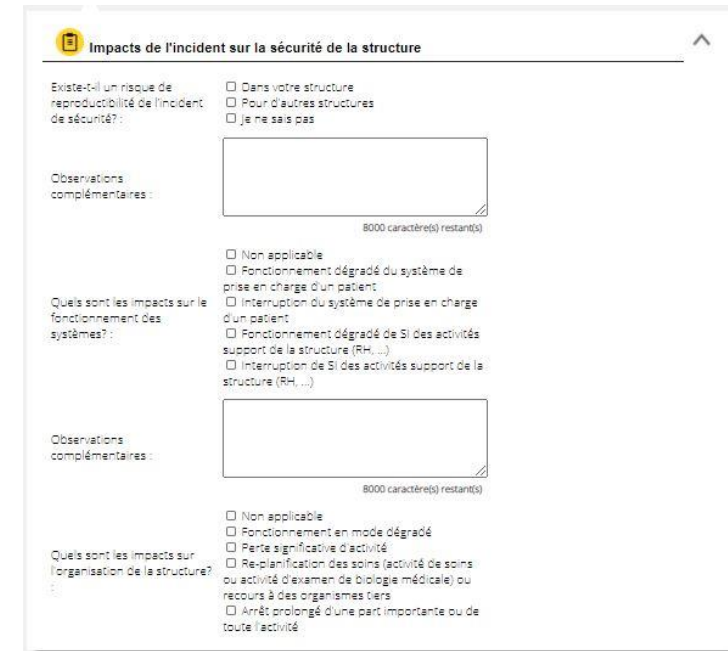
Souhaitez-vous bénéficier d'un accompagnement? * : ☐ Oui ☐ Non

Observations complémentaires :

8000 caractères(s) restant(s)

Etes-vous en mesure de donner plus d'informations concernant l'incident de sécurité? * : ☐ Oui ☒ Non

Concernant l'impact de l'incident sur la sécurité de la structure, l'impact sur les données, ou l'action malveillante à l'origine de l'incident.



Impacts de l'incident sur la sécurité de la structure

Existe-t-il un risque de reproductibilité de l'incident de sécurité? : ☐ Dans votre structure ☐ Pour d'autres structures ☐ Je ne sais pas

Observations complémentaires :

8000 caractères(s) restant(s)

Quels sont les impacts sur le fonctionnement des systèmes? : ☐ Non applicable ☐ Fonctionnement dégradé du système de prise en charge d'un patient ☐ Interruption du système de prise en charge d'un patient ☐ Fonctionnement dégradé de SI des activités support de la structure (RH, ...) ☐ Interruption de SI des activités support de la structure (RH, ...)

Observations complémentaires :

8000 caractères(s) restant(s)

Quels sont les impacts sur l'organisation de la structure? : ☐ Non applicable ☐ Fonctionnement en mode dégradé ☐ Perte significative d'activité ☐ Re-planification des soins (activité de soins ou activité d'examen de biologie médicale) ou recours à des organismes tiers ☐ Arrêt prolongé d'une part importante ou de toute l'activité

Déclaration d'incident : les démarches réglementaires

Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr

Accueil > Questionnaire > Saisie du signalement

[S'informer sur les événements sanitaires indésirables](#)

1 2 3 4

Déclaration
Tous les champs avec un * sont obligatoires.

Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr

Accueil > Questionnaire > Saisie du signalement

[S'informer sur les événements sanitaires indésirables](#)

1 2 3 4

Déclaration
Tous les champs avec un * sont obligatoires.

Impacts de l'incident sur les données

Quelle est la nature des données impactées ?

- ☐ Non applicable
- ☐ Information patient à caractère personnel (dossier patient, résultat d'analyses, ...)
- ☐ Information à caractère personnel hors données patients (données relatives aux salariés de l'établissement, données d'accès de type identifiant/mot de passe, ressources humaines)
- ☐ Données techniques sensibles (mots de passe, clés cryptographiques, documents d'architecture et de configuration, ...)
- ☐ Information confidentielle / stratégique non personnelle (information interne à l'établissement ; financière, comptable, contractuelle, ...)
- ☐ Autre

Si vous avez saisi "Autre", veuillez préciser :

Quel est l'impact sur ces données ?

- ☐ Non applicable
- ☐ Perte de données ou impossibilité d'accéder à des données
- ☐ Atteinte à l'intégrité des données
- ☐ Divulgaration ou accès non autorisé à des informations à caractère personnel
- ☐ Divulgaration ou accès non autorisé à des données relatives à la structure
- ☐ Autre

Si vous avez saisi "Autre", veuillez préciser :

Quels sont les impacts probables sur les personnes dont les données personnelles ont été impactées ?

- ☐ Non applicable
- ☐ Préjudice moral, atteinte à la vie privée
- ☐ Vol, escroquerie, chantage, perte de preuves dans un contentieux
- ☐ Perte d'emploi, résiliation de contrat de prêt ou d'assurance
- ☐ Perte d'accès à des services publics ou commerciaux, à des services en ligne
- ☐ Discrimination, harcèlement, diffamation, perte de réputation
- ☐ Publicité ciblée et messages indésirables



Origine de l'incident

Origine de l'incident :

- ☒ Action malveillante suspectée
- ☐ Dysfonctionnement de l'infrastructure (locale ou du prestataire)
- ☐ Bug applicatif
- ☐ Panne électrique
- ☐ Perte du lien télécom
- ☐ Intervention accidentelle sur le SI
- ☐ Autre

Action malveillante suspectée :

- ☐ Défiguration d'un site internet
- ☐ Compromission d'un système d'information
- ☐ Attaque par déni de service
- ☐ Message électronique malveillant
- ☐ Logiciel malveillant / virus
- ☐ Fuite d'information
- ☐ Vol d'équipement
- ☐ Autre

Si vous avez saisi "Autre", veuillez préciser :

En cas d'action malveillante identifiée, avez-vous déconnecté les machines potentiellement infectées ?

☐ Oui ☐ Non

En cas d'acte malveillant, envisagez-vous de déposer plainte ?

☐ Oui ☐ Non

Si non, pourquoi ?

8000 caractères(s) restant(s)

Déclaration d'incident : les démarches réglementaires

Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr

Accueil > Questionnaire > Saisie du signalement > Récapitulatif

Récapitulatif de votre signalement

Merci de vérifier les éléments de votre signalement avant de l'envoyer

1 2 3 4

Récapitulatif

Vous êtes sur le point de signaler : un incident de sécurité des systèmes d'information

Pour l'incident de sécurité informatique

Agence du Numérique en Santé / CERT Santé
Accompagnement Cybersécurité des Structures de Santé par CERT Santé
9 rue George Pitard
75015 PARIS

cybenvelle@sante.gouv.fr

ARS CENTRE-VAL DE LOIRE
INCIDENT SI
131 rue du faubourg Bannier
BP 74409
45044 Orléans Cedex 1

☐ En cochant cette case, je reconnais avoir lu et accepté les [conditions générales d'utilisation](#).

☐ Je ne suis pas un robot

PRÉCÉDENT **ENVOYER**



Merci d'avoir complété ce formulaire.

Votre signalement du 16/09/2020 13:57:31 (GMT+2) a bien été enregistré sous la référence 20200916135731298.

Cette référence vous sera envoyée par mail.

Afin d'améliorer le portail des signalements, prenez 3 minutes et donnez votre avis.

Pour l'incident de sécurité informatique

Agence du Numérique en Santé / CERT Santé
Accompagnement Cybersécurité des Structures de Santé par CERT Santé
9 rue George Pitard
75015 PARIS

cybenvelle@sante.gouv.fr

ARS CENTRE-VAL DE LOIRE
INCIDENT SI
131 rue du faubourg Bannier
BP 74409
45044 Orléans Cedex 1

IMPORTANT !

Si vous voulez conserver une copie de votre signalement, vous devez cliquer sur la flèche pour le télécharger ou l'imprimer.

TÉLÉCHARGER

Le service de traitement des signalements de l'ASIP Santé est effectué en jours ouvrés (9h-18h). En cas d'incident critique suspecté, le PSSI pourra être saisi directement à l'adresse : ssi@sgs-social.gouv.fr (PSSI-MCAS). Pour des informations sur des fiches réflexes, les bonnes pratiques et l'actualité SSI : <http://www.cybersecurite-sante.gouv.fr>

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

- Portail des signalements des événements 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



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



Sommaire

Cybersécurité : menaces, risques et bonnes pratiques

Déclaration d'incident : les obligations réglementaires
et démarches à réaliser

**Pour aller plus loin : Les ressources méthodologiques
et outils accessibles**



➤ Portail cyberveille-santé (<https://www.cyberveille-sante.gouv.fr/>)

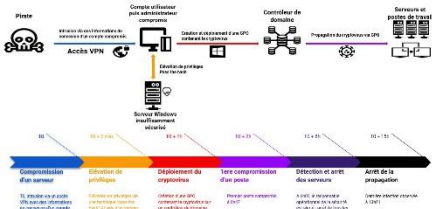
- Publication de bulletins d'information et d'alertes (vulnérabilités de dispositifs médicaux, de logiciels de santé ou de logiciels standard, actes de cybermalveillance) - 10 bulletins par semaine en moyenne
- 11 fiches reflexes présentant des recommandations pour répondre à des incidents ayant différentes 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

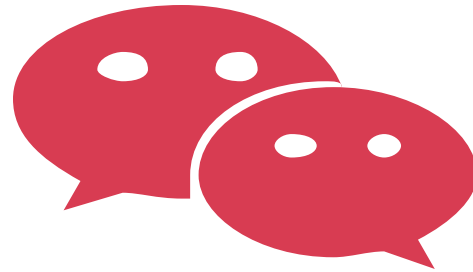
➤ Mise à disposition de retours d'expérience et d'un forum d'échanges sur l'espace privé du portail pour favoriser la coopération et l'entraide entre les acteurs (ministère, ARS et structures de santé) face à la menace de cybersécurité

- 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 ?