Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MARS

***M**essage d'**A**lerte **R**apide **S**anitaire*

MINISTERE DES SOLIDARITES ET DE LA SANTE
DIRECTION GENERALE DE LA SANTE
DIRECTION GENERALE DE L'OFFRE DE SOINS
DIRECTION GENERALE DE LA COHESION SOCIALE
SERVICE DU HAUT FONCTIONNAIRE DE DEFENSE ET DE SECURITE

DATE : 12/02/2021 **REFERENCE :** MARS N°2021_10

OBJET : CYBERATTAQUE PAR RANÇONGICIEL

Pour action

☒Établissements médico-sociaux : (EHPAD) ☒Établissements hospitaliers

Pour information

☒DGOS ☒ARS ☐SpF

☒DGCS ☒ARS de Zone ☐ANSM ☒Autre : DNS, ANS

Mesdames, Messieurs,

Il est constaté ces derniers mois une recrudescence **des attaques par rançongiciels**, impactant notamment les établissements de santé.
Le ministère des solidarités et de la santé demande à l'ensemble des établissements et structures de santé de renforcer la vigilance.

Un **rançongiciel** est un programme malveillant parfois reçu par courriel ou déployé par d'autres moyens, qui provoque le chiffrement de tous les fichiers d'un ordinateur, serveur ou sauvegarde (et des fichiers accessibles en écriture sur les dossiers partagés si les ordinateurs de la structure sont connectés à un réseau informatique).

Rappel des principales mesures préventives à mettre en œuvre :

- **Sauvegarder les données** : Effectuer des sauvegardes fréquentes, disposer de copies déconnectées du réseau et vérifier régulièrement qu'elles sont opérantes ;
- **Sensibiliser le personnel** : Rappeler aux utilisateurs les consignes de bonnes pratiques sur la messagerie : ne pas ouvrir les courriels en cas de doute sur la légitimité ;
- **Limiter les droits des utilisateurs et les autorisations des applications** : Ne jamais ouvrir de courriels, ou naviguer depuis un compte ayant des droits « Administrateur » (y compris Administrateur local)
- **Maintenir à jour les logiciels**, les systèmes et les applications ;
- **Maîtriser les accès Internet** ;
- **Utiliser et maintenir à jour les logiciels antivirus** et mettez régulièrement à jour la base de signatures ;
- **Cloisonner le système d'information** : Sur un réseau informatique qui n'est pas cloisonné, un attaquant est susceptible de prendre le contrôle d'un grand nombre de ressources et ainsi amplifier les conséquences de l'attaque.

En cas d'incident :

- **Déconnecter** immédiatement la ou les machines concernées du réseau et ne les éteignez pas ;
- **Alerter** les services informatiques qui mèneront les actions de confinement/investigation/remédiation ;
- **Ne jamais payer la rançon**. Le paiement ne garantit en rien le déchiffrement de vos données ;
- **Déclarer l'incident** sur le portail dédié à cet effet, conformément à l'article L.1111-8-2 du code de la santé publique (https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil)
- **Déposer plainte** auprès des services de police ou de gendarmerie dont vous dépendez, ou auprès du procureur de la République du tribunal judiciaire dont vous dépendez ;
- **Notifier cette infection à la CNIL** s'il y a eu une violation de données à caractère personnel via le lien : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Pour vous aider :

Une fiche réflexe de l'Agence du numérique en santé concernant les « **maliciels** » est disponible via ce lien : https://cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiche_Maliciel_IR_RSSI.pdf

Un guide rédigé conjointement par l'ANSSI et la Direction des Affaires Criminelles et des Grâces du ministère de la Justice « **Attaque par rançongiciel, tous concernés - comment anticiper et réagir en cas d'incident** ? » est disponible également via ce lien : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf

Le Pôle cyber des ministères sociaux est disponible pour toutes questions : ssi@sg.social.gouv.fr

Katia Julienne	**Virginie Lasserre**	**Stéphane Pasquier**
Directrice générale de l'offre de soins	*Directrice générale de la cohésion sociale*	*FSSI des ministères sociaux PI*
Signé	Signé	Signé