FICHE RÉFLEXE

SUSPICION DE RANSOMWARE

DÉFINITION

Les ransomwares (ou rançongiciels) sont la menace numéro un pour les établissements de santé, car ils peuvent paralyser l'activité médicale. Les cyberattaquants rendent inaccessible les fichiers d'un ou plusieurs poste(s) en les chiffrant, en échange d'une rançon s'élevant parfois à plusieurs millions d'euros.

#1

IDENTIFIER LES SIGNES

- Fichiers renommés avec des extensions bizarres (.locked, .crypt).
- Message à l'écran réclamant une rançon.

#2

ISOLER LA MACHINE

- Couper la connexion réseau (Wi-Fi, Ethernet). Il est important de couper le poste infecté de toute connexion internet, afin d'empêcher davantage l'exécution d'actions frauduleuses orchestré par le cyberattaquant. Cela permet de réduire considérablement les dégâts occasionnés par cette attaque sur le système d'information de l'hôpital.
- Ne pas redémarrer la machine ni fermer le message pour préserver les preuves.

#3

INFORMER LE SERVICE INFORMATIQUE

- Communiquer le plus de détails possible (capture d'écran, noms des fichiers chiffrés).
- Les personnes habilitées à identifier le problème détermineront les étapes à suivre à suivre (analyse approfondie, déclenchement potentiel d'une cellule de crise).
- Il est important de bien suivre les instructions de la procédure dégradée en cas d'une coupure réseau de votre service/ unité

#4

NE JAMAIS PAYER LA RANÇON

- Le paiement finance la cybercriminalité et ne garantit pas la récupération des fichiers.

#5

ACTIONS APRÈS-CRISE

- Changer tous les mots de passe utilisés sur la machine compromise, ainsi que ceux potentiellement obtenus pendant l'attaque.
- Vérifier et restaurer les fichiers à partir des sauvegardes antérieures à l'attaque.

SIGNALEZ IMMÉDIATEMENT

- Toute lenteur ou anomalie suspecte (ex. : fichiers qui disparaissent).
- Un pop-up de menace ou demande de paiement en cryptomonnaie.

Avertir le service informatique
1017 ou 05 55 43 10 17

Demander à parler
au **Référent Sécurité**

Ou nous contacter sur
informatique@ch-esquirol-limoges.fr