AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Retour d'Expérience

Centre Hospitalier Simone Veil de Cannes

Attaque par rançongiciel

Contexte d'intervention

Centre Hospitalier Cannes Simone Veil

- Région : **Provence-Alpes-Côte d'Azur**
- **Centre Hospitalier :**
  - **2ème hôpital** du groupement hospitalier **des Alpes-Maritimes**
  - Plus de **2000 salariés** dont 230 médecins, 1200 paramédicaux et plus de 150 métiers différents
  - Plus de **800** lits et places d'hospitalisation

Origine(s) de la crise

- **Intrusion** sur le SI via un **compte compromis**
- **Élévation de privilèges** pour obtenir les droits d'administrateur de domaine
- **Déploiement** de la charge malveillante par **GPO**
- **Compromission** d'équipements périphériques suite à l'exploitation d'une **vulnérabilité éditeur**

Impacts et Risques identifiés

Impacts

- Coupure des **flux réseau**
- **Chiffrement** d'un **serveur de fichiers** et d'environ **15% des postes** du parc
- **Exfiltration** de données suspectée

Chronologie détaillée de l'incident

Compromission et actions illégitimes

Actions de l'établissement

15/04/2024 – 19:30

ACCÈS INITIAL

- CONNEXION VIA UN COMPTE COMPROMIS

16/04/2024 – 01:56

PREMIÈRE TENTATIVE

- TENTATIVE DE CHIFFREMENT

16/04/2024

CHIFFREMENT

- COMPROMISSION DES BOX PACS
- DEMANDE DE RANÇON
  - CHIFFREMENT DES PÉRIPHÉRIQUES
  - PAS DE TRACES DE LATÉRALISATION

16/04/2024 – 06:30

PREMIÈRE DÉTECTION ANTIVIRALE

- ALERTES ANTIVIRALES REMONTÉES SUR PLUSIEURS MACHINES

16/04/2024

MESURES DE CONFINEMENT

- COUPURE DE L'ENSEMBLE DES FLUX RÉSEAU INTERNES ET EXTERNES
- SAUVEGARDES DÉCONNECTÉES PHYSIQUEMENT DU SI
- ISOLEMENT DES SERVEURS AD

16/04/2024 – 17/04/2024

ASSURER LA CONTINUITÉ D'ACTIVITÉ

- BASCULEMENT DE PLUSIEURS SERVICES EN MODE DÉGRADÉ
- PRÉPARATION DE DÉPROGRAMMATION DE NON URGENT SI BESOIN

17/04/2024

DÉBUT DES ANALYSES

- TRANSMISSION DES PREMIÈRES COLLECTES
- DÉBUT DE L'ANALYSE

Chronologie des actions post-détection

PREMIÈRES ACTIONS

ACTIONS SUBSÉQUENTES

16/04
ALERTES ANTIVIRALES RELATIVES À UNE TENTATIVE DE CHIFFREMENT DU SI

DÉCISION DE COUPER L'ENSEMBLE DES FLUX RÉSEAU INTERNES ET EXTERNES
DÉCLARATION D'INCIDENT AU CERT SANTÉ

SAUVEGARDES DÉCONNECTÉES PHYSIQUEMENT DU SI
ISOLEMENT DES SERVEURS AD

17/04
DÉBUT DE L'ANALYSE DES PREMIÈRES COLLECTES

19/04
REDÉMARRAGE DES SERVICES SI INTERNES APRÈS MISE EN ŒUVRE DES MESURES DE REMÉDIATION

RÉOUVERTURE DES SERVICES DE STÉRILISATION

19/04 - …
LANCEMENT DES SCRIPTS DE VÉRIFICATION DES SAUVEGARDES
ACTIONS POST-CRISE

Accompagnement post- crise

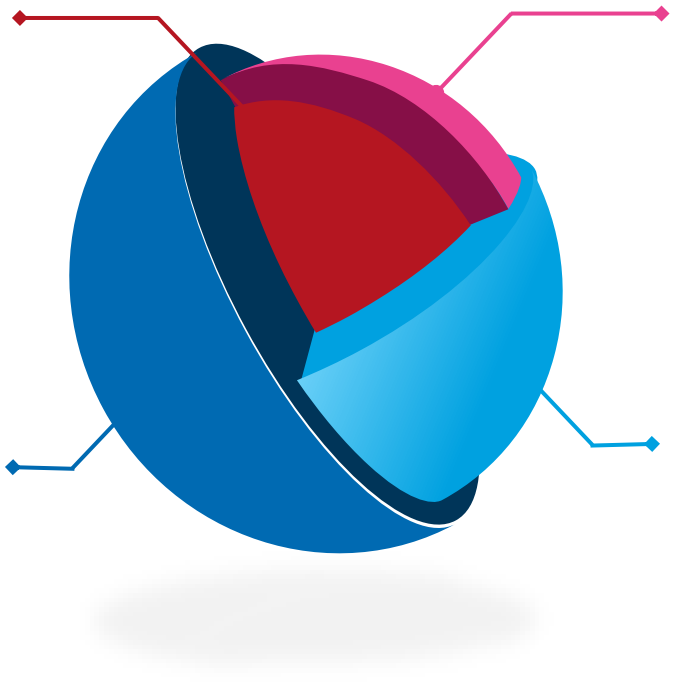
ACTIONS MISES EN ŒUVRE PAR LE CH CANNES SIMONE VEIL LORS DE LA CRISE

1. Alerter les entités compétentes

Alerter l'ANSSI et le CERT Santé pour assister à la gestion de la crise

2. Coupure des flux réseaux

Empêcher une propagation de l'attaque sur le reste du SI



4. Renforcement du SI suite à la crise

Mise en place de MFA pour les comptes à privilèges, renforcement de la politique de mot de passe, mise en place de règles EDR spécifiques, ainsi que d'autres actions de renforcement

3. Sécurisation des sauvegardes

Sauvegardes déconnectées physiquement du SI et vérifiées post-crise

AVRIL 2024

ACTIONS MISES EN ŒUVRE EN SOUTIEN DE LA CRISE PAR LE CERT SANTÉ

/ Les principaux **axes mis en œuvre** sont :

- **Accompagnement à la remédiation** et au pilotage organisationnel
- **Qualification de la crise** et accompagnement aux actions de confinement
- **Pilotage des actions** d'investigation et de rétro-ingénierie
- **Partage du compte-rendu** à la communauté

Bilan de l’accompagnement durant la crise

Rappel de la chronologie des évènements

15/04/2024 – 19:30 :
Connexion réussie sur un compte compromis

16/04/2024 – 01:56 :
Installation du rançongiciel Lockbit

16/04/2024 :
Tentative de chiffrement à l’aide rançongiciel Lockbit

16/04/2024 :
Accès malveillant à l’aide d’un compte administrateur sur plusieurs serveurs

16/04/2024 :
Compromission des box PACS
Chiffrement des périphériques

15:10 :
Levée d’alerte
Décision de couper l’ensemble des flux réseau

Résultats et éléments clés

L’attaquant s’est **introduit** sur le SI **via un compte compromis** avant d’opérer une élévation de privilèges. Le rançongiciel a chiffré **15 % des postes de travail** et **un serveur de fichiers**, perturbant ainsi les opérations du Centre Hospitalier Cannes Simone Veil.

Une **exfiltration de données est suspectée** car des **outils d'exfiltration** ont été **découverts sur le serveur compromis**.

Points à retenir

1. La déconnexion rapide des sauvegardes du système et l'isolation des serveurs AD ont permis de limiter les dommages et de protéger les données critiques, constituant une réponse efficace.

2. Il est vital de renforcer la sécurité des comptes privilégiés pour empêcher l'élévation de privilèges. De plus, il est indispensable de surveiller l’activité réseau pour anticiper d’éventuelles tentatives d’exfiltration.

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé