AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

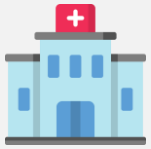
Retour d'Expérience

Centre Hospitalier Départemental Stell de Rueil-Malmaison

Compromission du SI et chiffrement des données

Contexte d'intervention

Centre Hospitalier Départemental



- **Centre Hospitalier Départemental :**
  - **Fondé en 1903** par le philanthrope Edward Tuck, le CH porte le nom de son épouse **Julia Stell**
  - Dispose d'un **Institut de Formation en Soins Infirmiers** (IFSI) d'environ 100 étudiants par promotions
  - Environ **240** lits et places d'hospitalisation, ainsi qu'un **EHPAD** et des **unités spécialisées**

Origine(s) de la crise

- **Mauvaise gestion** d'un ancien compte admin de domaine avec accès VPN et mot de passe faible
- **Intrusion sur le SI via le VPN**, exploitant les accès du compte compromis
- **Constatations du chiffrement** des serveurs du SI

Impacts et Risques identifiés

Impacts :

- Certains **soins indisponibles ou ralentis**
- **GAM et gestion repas** indisponibles
- **Exfiltration de données à caractère personnel** et métiers suspectés
- **Accès au DPI** rendu difficile

Chronologie détaillée de l'incident

Compromission et actions illégitimes

17/03/2025

Accès initial au SI

- Première connexion illégitime avec l'utilisateur ADW sur le VPN

22/03/2025 – 00:42

Mouvement latéral

- Latéralisation via connexion RDP sur le DC avec le compte ADW

22/03/2025 – 00:42

Escalade de privilèges

- Création du profil de l'utilisateur ADW sur le DC

22/03/2025 – 03:18

Persistance

- Ajout du service Pinggy sur le DC afin d'établir une connexion SSH sur le port 443 depuis l'extérieur

28/03/2025 – 20:59

Command and Control

- Mise en place d'un canal entre le DC et le serveur de l'attaquant avec Ngrok

28/03/2025 – 21:48

Mouvement latéral

- Latéralisation sur les autres serveurs du réseau local

28/03/2025 – 23:16

Impact

- Exécution du chiffrement sur les serveurs Windows du parc

29/03/2025

Suppression d'indicateurs

- Suppression des traces de l'attaque sur les systèmes

Actions de **l'établissement**

04/03/2025

Manipulation de compte

- Réactivation du compte à privilège ADW, administrateur de domaine et accès VPN, pour un audit Wi-fi.

31/03/2025

Constatation

- Constatation du chiffrement sur les serveurs
- Déclaration de l'incident à 10h30 à l'ANSSI
- Premier point technique avec le CERT Santé et l'ANSSI à 11h30

02/04/2025

Traitement de l'incident

- Début des analyses des serveurs Windows compromis
- Demande de matériel à l'ARS (Clé 4G, postes, etc.)

07/04/2025

Contre-mesures

- Début de la reconstruction AD

10/04/2025

Contre-mesures

- Fin de la bascule AD
- Relance du service de sauvegardes
- Formation d'administration sécurisée dispensée

Chronologie des actions post-détection

Premières actions

31/03

Détection d'un comportement anormal, coupure des flux VPN, isolement des serveurs impactés et signalement de l'incident.

01/04

Récupération et envoi des logs pour l'analyse. Tentative de redémarrage des serveurs. Mise hors réseau des sauvegardes et vérification de leur intégrité.

Déplacement de l'ANSSI et du CERT Santé sur le site du CHD.

02/04

Début des analyses, demande de matériels de secours à l'ARS et vérification de la non-latéralisation vers d'autres établissements.

07/04

Arrivé d'aides externes pour la remédiation AD et du réseau. Fin des analyses et confirmation du scénario de l'attaque.

Actions subséquentes

10/04

Fin de la bascule AD par l'ANSSI et restauration des services métiers impactés.

Avril – Mai

Rétablissement des services RH et admission.

Déploiement de nouveaux postes utilisateurs.

Juin - Septembre

Mise en place et adaptation au modèle par niveaux de privilège (Tiering modèle) pour l'AD.

Accompagnement post-crise

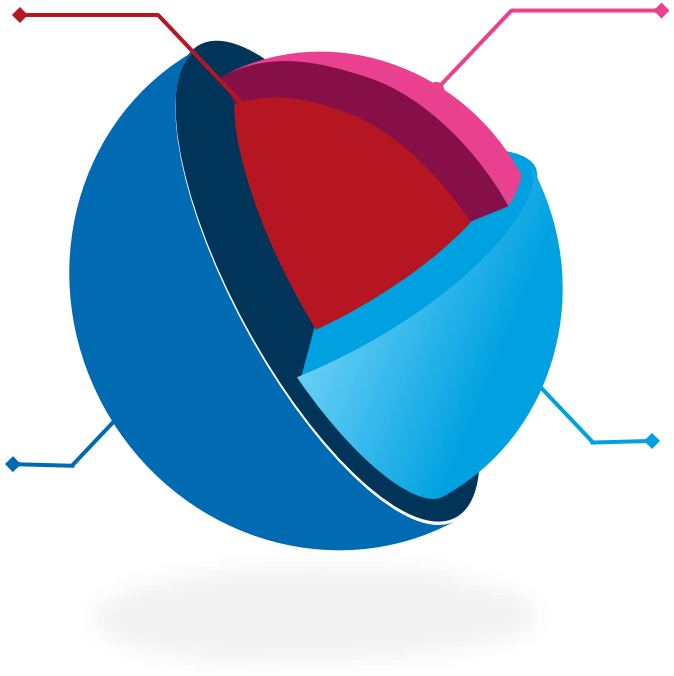
ACTIONS MISES EN ŒUVRE PAR LE CHD LORS DE LA CRISE

1. Confinement

Isolement des serveurs impactés et coupure des flux VPN et vers Internet

2. Alerte

Déclaration d'incident et demande d'accompagnement adressées à l'ANSSI et au CERT Santé



3. Renforcement des accès

Renouvellement de l'ensemble des mots de passe et revue des comptes

4. Reconstruction et reprise

Reconstruction et bascule de l'AD et des serveurs impactés par le rançongiciel, reprise progressive de l'activité

ACTIONS MISES EN ŒUVRE EN SOUTIEN DE LA CRISE PAR LE CERT SANTÉ ET L'ANSSI

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

- **Accompagnement à la remédiation** et au pilotage des mesures correctives
- **Qualification de l'incident** et accompagnement aux actions de confinement
- **Investigation technique basée** sur l'analyse des traces
- **Déplacement sur site pour être** au plus proche des équipes et des problèmes métier
- **Élaboration du plan d'action,** suivi de sa mise en œuvre et formation de cybersécurité

Bilan de la gestion de l'incident

Rappel de la chronologie des évènements

- ***04/03/2025 :*** *Manipulation d'un compte*
- ***17/03/2025 :*** *Première connexion illégitime sur le SI via le VPN*
- ***22/03/2025 :*** *Connexion au DC via RDP et déploiement d'un service de persistance*
- ***28/03/2025 :*** *Exécution du rançongiciel via un serveur distant de l'attaquant*
- ***29/03/2025 :*** *Suppression des traces de l'attaques*
- ***31/03/2025 :*** *Constatation du chiffrement, signalement de l'incident et mise en place d'une cellule de crise*
- ***02-07/04/2025 :*** *Analyse des traces et exécution du plan d'action*
- ***07-10/04/2025 :*** *Bascule de l'AD, durcissement du DC et restauration de services métiers*

Résultats et éléments clés

L'attaquant s'est introduit sur le SI via un **compte VPN et administrateur de domaine sur l'AD** avant de déployer un service de persistance pour faciliter l'accès illégitime au SI. Il a ensuite tenté de se **latéraliser vers d'autres serveurs Windows** et a activé un canal de communication vers son serveur de commande pour exécuter le rançongiciel.

Le compte utilisé est un **ancien compte de test**, qui a été **réactivé quelques jours auparavant** pour réaliser un audit légitime sur le réseau Wi-Fi.

L'attaque s'est **propagée sur l'ensemble des serveurs Windows** de l'établissement, touchant des services métiers critiques.

Points à retenir

1. Une **revue régulière des comptes** , même des comptes désactivés, sur les équipements donnant accès au SI depuis Internet, combiné à des **mots de passe robustes** ainsi qu'un **second facteur**, permet de **se protéger des attaques par brute force** ou **de fuites d'identifiants**, et par conséquent, **d'un accès illégitime au SI**.

2. Le plan d'action établi durant l'incident en collaboration avec l'ANSSI et le CERT Santé a permis un suivi complet de l'incident, **une prise de décision rapide et un durcissement de l'AD avancé**.


AGENCE
DU NUMÉRIQUE
EN SANTÉ
CERT
Santé