AGENCE DU NUMÉRIQUE EN SANTÉ

Retour d'Expérience

CH de Cahors – Compromission potentielle de serveurs RDS

Contexte d'intervention

CH de Cahors

- Région : **Occitanie**
- **Le Centre Hospitalier de Cahors est le principal établissement de santé du Lot :**
  - Il assure une prise en charge multidisciplinaire (plus d'une vingtaine de spécialités médicales, chirurgicales et gynéco-obstétricales).
  - Au sein de la communauté hospitalière du Quercy, le Centre Hospitalier de Cahors est aussi le référent territorial pour de nombreuses activités médicales et médico-techniques.

CH de Gourdon (Jean Coulon)

- Région : **Occitanie**
- **Le Centre Hospitalier de Gourdon propose les services suivants :**
  - Imagerie médicale, scanner, Unité de chirurgie ambulatoire, Urgences, Consultations externes, plateforme de répit et d'accompagnement pour les aidants proches atteints de pathologies neuro dégénératives.

Origine(s) de la crise

- Le CH de Cahors ainsi que le CH de Gourdon ont constaté des comportements anormaux depuis le 13/01/2025.
- Plusieurs alertes anti-virales relevées par l'hébergeur Okantis sur des serveurs critiques d'une ferme RDS
- Plusieurs postes du parc victimes de scans UDP depuis l'externe et l'interne
- Désactivation de plusieurs agents EDR et anti-virus

Impacts et risques identifiés

- Risque d'accès illégitime au SI via la ferme RDS compromise
- Isolement de l'accès aux fermes RDS permettant l'accès à DxCare et aux plannings de soins
- Dégradation de l'accès à distance

Chronologie détaillée de l'incident

Alertes et signaux Pouvant mener à une compromission

22/01/2025 – 21:36

SUSPICION D'ACCÈS INITIAL

- POSSIBLE EXPLOITATION DE VULNÉRABILITÉS SUR UN SERVEUR RDS

22/01/2025 – 23:11

NOUVELLES ACTIVITÉS IDENTIFIÉES

- DÉTECTION PAR L'ANTI-VIRUS DE FICHIERS SUSPECTS SUR UN SECOND SERVEUR

22/01/2025 – 23:17

POURSUITE DES ACTIONS

- DÉTECTION DE SCAN DE PORTS UDP ENTRE DEUX SERVEURS INTERNES

Actions de **l'établissement**

22/01/2025 – 07:17

DÉTECTIONS INITIALES

- ALERTES ANTIVIRALES SUR L'EXISTENCE D'UNE VULNÉRABILITÉ SUR UN SERVEUR MÉTIER

22/01/2025 – 21:36

PREMIÈRES ANALYSES

- TRAITEMENT ET ANALYSE DES ALERTES ANTIVIRALES

23/01/2025

MESURES DE CONFINEMENT ET PREMIÈRES RECOMMANDATIONS

- ISOLATION DES SERVEURS SUSPECTÉS

23/01/2025

POINT DE SUIVI TECHNIQUE

- DÉCLENCHEMENT D'UNE CELLULE DE SUIVI D'INCIDENT

23/01/2025

INVESTIGATIONS

- SOLLICITATION DU CERT SANTÉ

24/01/2025

PRÉPARATION DE LA RECONSTRUCTION

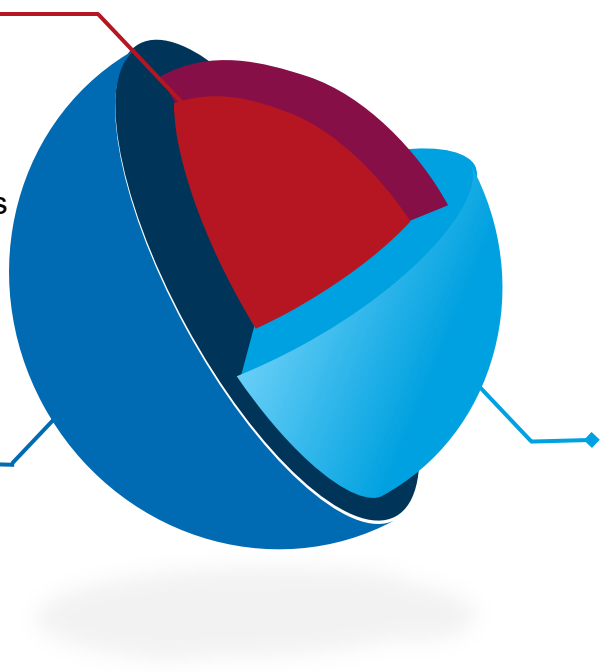
- RETOURS SUITE AUX ANALYSES RÉALISÉES

Accompagnement post- crise

ACTIONS MISES EN ŒUVRE PAR LE CH DE CAHORS LORS DE LA CRISE

1. Confinement

- Isolement des postes ayant leur agent Crowdstrike désactivé
- Isolement du serveur RDS de profils
- Isolement d'un serveur RDS relais



2. Remédiation

Reconstruction à neuf d'un serveur RDS de gestion des profils

3. Demande d'assistance et de suivi

Demande d'un suivi d'incident et d'une assistance à l'analyse au CERT Santé

JANVIER 2025

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

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

Levée de doutes par analyse des traces des serveurs suspectés

Etude des vulnérabilités détectées

Chronologie des actions post-détection

DURANT LA CRISE

SUITE À LA CRISE

MISE EN PLACE D'UN CONFINEMENT DES SERVEURS SUSPECTÉS

ISOLEMENT DU SERVEUR RDS DE PROFILS

SIMPLIFICATION DES RÈGLES ANTI-VIRALES

RECONSTRUCTION À NEUF D'UN SERVEUR RDS DE PROFILS

*Evènements identifiés à postériori grâce à l'investigation

Bilan de l’accompagnement durant la crise

Rappel de la chronologie des évènements

22/01/2025 – 07:17
Alertes antivirales sur l'existence d'une vulnérabilité sur un serveur métier

22/01/2025 – 21:36
Alertes antivirales sur une possible exploitation de vulnérabilités

22/01/2025 - 23:11
Détection par l'antivirus de fichiers potentiellement malveillants sur un second serveur

22/01/2025 - 23:17
Détection de scan de ports UDP entre deux serveurs internes

23/01/2025
Isolation des serveurs compromis

23/01/2025
Déclenchement d'une cellule de prise en charge d'un incident

23/01/2025
Sollicitation du CERT Santé

Résultats et éléments clefs

La série de détections réalisées par l’anti-virus est **vraisemblablement liée à une mise à jour antivirale** ayant **fait remonter d'anciens composants présents sur les serveurs comme indésirables. I**l ne s’agit pas de la détection d'une activité malveillante sur le SI. Néanmoins, les signes suspects observés ont déclenché une prise en charge de crise similaire à celle d’un incident majeur.

Aucun binaire ni script malveillant ayant conduit à la désactivation des agents Crowdstrike **n’a été observé sur les postes suspects**. L’hypothèse retenue est celle d'un faux-positif lié à la **mise à jour d'une base anti-virale.**

Aucune connexion malveillante aux serveurs RDS n’a été identifiée.

Points principaux à retenir

La crise a été gérée de manière conjointe par le CH de Cahors et le CH de Gourdon.

Suite à la crise, la simplification des conditions de détection a été réalisée ainsi qu’une reconstruction d'un serveur RDS de profils.


AGENCE
DU NUMÉRIQUE
EN SANTÉ
CERT
Santé