AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

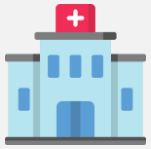
Retour d'Expérience

Centre Hospitalier Universitaire

Compromission de serveurs de téléphonie

Contexte d'intervention

Centre Hospitalier Universitaire



- **Centre Hospitalier Universitaire :**
  - **1er centre hospitalier universitaire de sa région,** pilier du Groupement Hospitalier de Territoire
  - Plus de **7 800 professionnels** dont près de 1 400 médecins, 4 800 personnels soignants et médico-techniques, représentant plus de 200 métiers différents
  - Environ **1 800** lits et places d'hospitalisation

Origine(s) de la crise

- **Fuite d'identifiants** ayant conduit à la compromission d'un compte prestataire
- **Intrusion sur le SI via le VPN**, exploitant les accès du compte compromis
- **Détection de l'incident par le SOC**, suite à une alerte émise par l'EDR

Impacts et Risques identifiés

Impacts :

- **Service de téléphonie** des patients **indisponible**
- **Exfiltration des mots de passe** Active Directory
- **Réutilisation de comptes compromis** pour étendre l'intrusion

Chronologie détaillée de l'incident

Compromission et actions illégitimes

11/03/2025 – 14h58

Accès initial au SI

- Connexion RDP depuis le compte VPN du prestataire, puis sur le serveur Windows gérant la téléphonie patient

12/03/2025 – 13h35

Extraction des Identifiants

- Dump du processus LSASS via l'outil Hash Suite Pro

12/03/2025

Mouvement latéral

- Tentative de latéralisation vers des serveurs Linux, avec ajout de clé SSH

12/03/2025

Tentative d'escalade de privilèges

- Tentative de Pass The Hash (attaque par envoi de hash)

21/03/2025

Reconnexion échouée

- Nouvelle tentative de connexion VPN avec l'utilisateur compromis, échec, puis utilisation d'autres comptes issus de la fuite, également en échec

Actions de **l'établissement**

12/03/2025

Détection comportementale

- L'EDR détecte un comportement anormal (Pass The Hash) et bloque certaines actions malveillantes

13/03/2025

Réaction immédiate

- Alerte EDR constatée au matin → isolement du serveur
- Notification au CERT Santé à 11h20
- Point technique avec le CERT Santé à 11h30
- Réunion technique à 14h00 avec l'éditeur de l'EDR et le CERT Santé

13/03/2025

Traitement de l'incident

- Début des analyses du serveur Windows compromis
- Désactivation du compte compromis via l'EDR

13/03/2025

Enquête post-incident

- Identification de fuites d'identifiants antérieures à l'incident

17/03/2025

Contre-mesures

- Début du plan d'action de durcissement de l'infrastructure

19/03/2025

Reprise technique

- Reconstruction de l'ensemble des serveurs liés à la téléphonie patient

Chronologie des actions post-détection

Premières actions

Actions subséquentes

12/03

Détection d'un comportement anormal et blocage automatique de certaines actions malveillantes (Pass The Hash)

13/03

Isolement du serveur compromis

Analyse technique du serveur Windows

Désactivation du compte compromis

Identification de fuites d'identifiants antérieures à l'incident

14/03

Traces de l'attaquant retrouvées sur d'autres serveurs de téléphonie

Lancement de la levée de doute

17/03

Début du plan de durcissement de l'infrastructure

19/03

Reconstruction des serveurs liés à la téléphonie patient

Coordination technique avec l'éditeur de téléphonie

21/03

Tentatives de reconnexion VPN avec identifiants compromis en échec

Fin mars – avril

Poursuite de l'analyse des traces

Désactivation des comptes génériques pour les accès distants des éditeurs

Prévu fin juin

Déploiement du 2FA pour les connexions VPN

Accompagnement post-crise

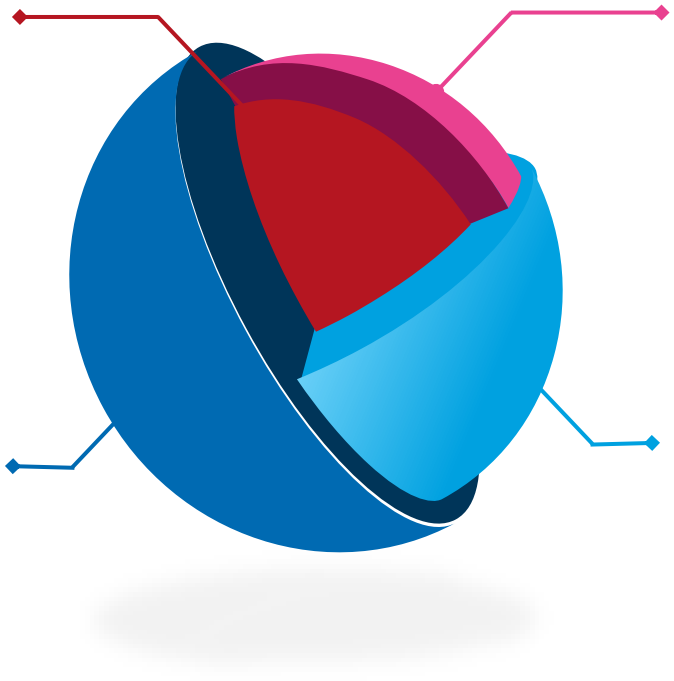
ACTIONS MISES EN ŒUVRE PAR LE CHU LORS DE LA CRISE

1. Confinement

Isolement des serveurs suspects via l'EDR, en particulier ceux liés au service de téléphonie

2. Alerte

Déclaration d'incident et demande d'accompagnement adressées au CERT Santé



4. Reconstruction et reprise

Reconstruction des serveurs impactés en lien avec l'éditeur de téléphonie, reprise progressive de l'activité

3. Renforcement des accès

Désactivation des identifiants AD sur le VPN, changement des mots de passe compromis, sécurisation des comptes sensibles

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 des mesures correctives
- **Qualification de l'incident** et accompagnement aux actions de confinement
- **Investigation technique** : analyse des traces via l'EDR et les outils du CERT
- **Coordination avec l'éditeur** pour pilotage technique
- **Élaboration du plan d'action** et suivi de sa mise en œuvre

Bilan de la gestion de l'incident

Rappel de la chronologie des évènements

- ***11/03/2024 :*** *Connexion RDP au serveur téléphonie avec un compte VPN/AD compromis*
- ***12/03/2024 :*** *Dump LSASS via Hash Suite Pro*
- ***12/03/2024 :*** *Tentative de Pass The Hash bloquée*
- ***13/03/2024 :*** *Détection par l'EDR et isolement du serveur*
- ***14/03/2024 :*** *Traces de l'attaquant retrouvées sur d'autres serveurs téléphonie*
- ***17/03/2024 :*** *Début du durcissement de l'infrastructure*
- ***19/03/2024 :*** *Reconstruction des serveurs téléphonie et reprise d'activité*
- ***21/03/2024*** *Tentative de connexion VPN avec les identifiants compromis (échec)*

Résultats et éléments clés

L'attaquant s'est introduit sur le SI via un **compte VPN et AD compromis** avant de récupérer la **base de hashs des mots de passe**. Il a ensuite tenté de se **latéraliser vers d'autres systèmes**, en particulier des serveurs Linux.

L'EDR a permis de **bloquer automatiquement certaines actions** malveillantes et a **généré des alertes** dès le 12/03.

L'attaque est **restée contenue au périmètre de la téléphonie patient**, sans propagation vers d'autres briques critiques du SI. Il a fait plusieurs **fautes d'orthographe dans ses commandes Linux**, indiquant une intrusion manuelle sur les serveurs, non automatisée.

Points à retenir

1. L'EDR a détecté et bloqué les activités malveillantes. Cependant, **l'absence de configuration de certains modules de l'EDR ont limité les capacités d'analyse avancé de l'outil**.

2. Le plan d'action établi par l'établissement a permis un suivi complet de l'incident, **une prise de décision rapide et une exécution efficaces des actions**.


AGENCE
DU NUMÉRIQUE
EN SANTÉ
CERT
Santé