AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Retour d'Expérience

Hospices Civils de Lyon– Compromission du SI suite à l'exfiltration d'un compte utilisateur

Contexte d'intervention

Hospices Civils de Lyon

- Région : **Auvergne-Rhône-Alpes**
- HCL, **2nd CHU de France:**
  - Etablissement hospitalo-universitaire de référence en région AuRA
  - **13 établissements hospitaliers**
  - Plus de **24000** personnels de soins
  - Plus de **5000 lits**

Origine(s) de la crise

- Infection d'un poste personnel utilisateur (hors SI) et vol d'un compte HCL utilisé sur la machine.
- Réutilisation des identifiants volés pour initier des **connexions illégitimes** sur une machine virtuelle **via une ferme RDS.**
- **Réutilisation d'un navigateur Chrome** et évasion de contexte vers le système hôte
- **Tentative** de déploiement d'un **ensemble d'outils malveillants**.

Risques identifiés*

- **Exfiltration** de données **(identifiants)**
- Compromission **d'un serveur métier**
- **Accès illégitime** au SI
- **Risque de chiffrement** de certaines parties du SI

** Enumération des risques identifiés en cas de succès de l'attaque.*

Chronologie détaillée de l'incident

Compromission et actions illégitimes

13 décembre 2023

Accès initial

- Connexion a la ferme RDS depuis un compte volé précédemment
- Activités de reconnaissance réseau

14 décembre 2023 – 21:31

Latéralisation et persistence

- Nouvelle connexion a la ferme RDS
- Accès à des données internes via un navigateur
- Usurpation d'une session RDP

14 décembre 2023 – 21:31

Latéralisation et persistence

- 23:10 - Copie de rdpclip
- 00:18 - Tentative d'installation d'une charge de chiffrement
- 00:18 – 00:23 - Téléchargement d'exécutables
- 00:34 - Accès à gpedit

15 décembre 2023 00:06

Déploiement d'outils

- Tentative de téléchargement d'outils malveillants
- Nouvelle connexion RDP
- Commandes Powershell
- Lancement Mstsc.exe

Actions de l'établissement HCL

14 décembre 2023 – 21:31

Détection anti-virale

- Détection par l'anti-virus d'un exécutable (bloqué)

15 décembre 2023 – 00:18-00:50

Détection anti-virale

- Détection de plusieurs exécutables malveillants par l'EDR – blocage

15 décembre 2023

Confinement et neutralisation

- Blocage du compte compromis
- Isolation du poste de travail
- Blocage d'IP identifiées
- Rotation de mots de passe
- Fermeture des flux RDS pour le weekend

18 décembre 2023

Réouverture et restrictions d'accès RDS

- Fermeture des flux RDS hors heures ouvrées et hors France

Chronologie des actions post-détection

Actions de l'établissement HCL

Accompagnement du CERT Santé

15 décembre 7:00 — Détection de l'incident
Isolation de la machine compromise

15 décembre 08:00 — Démarrage des analyses
Renforcement de la surveillance

15 décembre 14:00 — Analyses complémentaires
Suivi de remédiation

15 décembre 17:00 — Revue des TTP
Demande de coupure des flux RDS

15 décembre 18:00 — Fermeture de la ferme RDS

18 décembre — Levée des actions de confinement

20 décembre — Renforcement des accès
Démarrage de la remédiation long terme
Analyses additionnelles
Rétro-ingénierie des outils illégitimes identifiés

*Evènements identifiés à postériori grâce à l'investigation

Accompagnement post- crise

JANVIER 2024

ANALYSE ET MISE EN PLACE DU PLAN DE REMÉDIATION

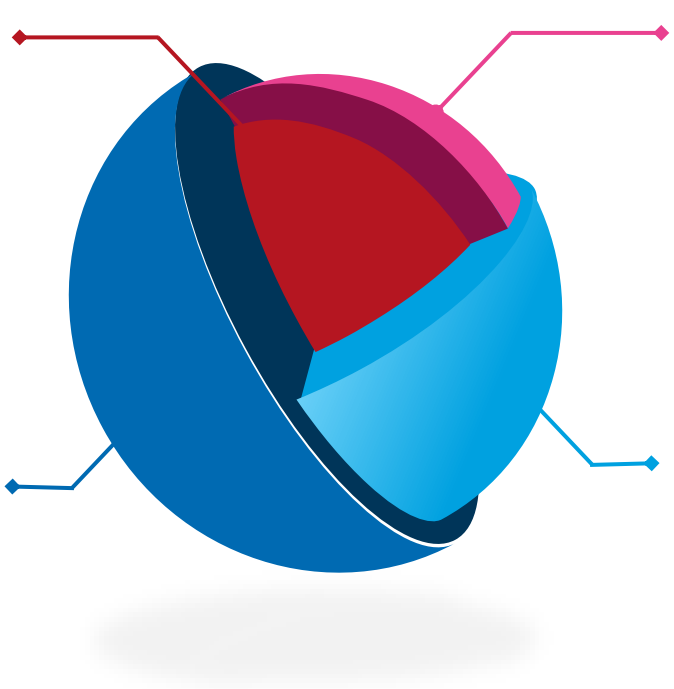
/ Les principaux **axes mis en œuvre** sont :

- **Rétro-ingénierie** des exécutables malveillants
- Collectes de **journaux supplémentaires**
- **Enrôlement MFA** pour l'accès au portail RDS
- Renforcement de la **sécurité de l'AD**
- **Revue** régulière des **comptes SPN**

Les étapes du déploiement du plan de remédiation

1. Socle du SI (firewall, etc.)
S'assurer que le cœur du système d'information est sécurisé et à jour

2. Services métiers
Contrôler les périmètres métiers et reprendre peu à peu un usage standard



3. Réouverture des flux réseaux
Réouvrir les flux réseaux moins prioritaires

4. Renforcement du PRA
Renforcer le PRA suite à l'incident et aux leçons apprises.

Bilan de l'accompagnement durant la crise

Rappel de la chronologie des évènements

13 décembre 2023 :
Début de l'incident suite à la réutilisation d'identifiants utilisateur

14 décembre 2023 :
Détection anti-virale

14 décembre 2023:
Reconnexion, latéralisation et persistence.

15 décembre 2023 :
Tentative de déploiement d'outils
Isolation de la machine compromise

18 décembre 2023 :
Confinement ferme RDS

Janvier 2024 :
Mise en place du plan remédiation long terme

Résultats et éléments clés

L'attaquant **a réutilisé des identifiants exfiltrés suite à une compromission du poste personnel** d'un interne.

Ces identifiants ont ensuite permis de se connecter au **système d'information interne**.

Plusieurs tentatives de déploiement d'outils malveillants ont été observés et bloqués sur le SI.

Points à retenir

1. Lors d'une crise, la **communication entre les acteurs externes et internes à l'établissement** est une des clés de la réussite.

2. Paramétrer les outils de sécurité internes permet de **limiter l'impact** mais n'évite pas **toutes les formes de compromission.**

3. Identifier les **équipements informatiques essentiels et les plus critiques** pour le système d'Information. Créer un **plan de maintien en conditions opérationnelles** cohérent avec les priorités précédemment établies.

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé