AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Retour d'Expérience

Un groupement hospitalier victime de compromission de comptes

Contexte d'intervention

Entité hospitalière

- Plus de **1 200 agents et professionnels de santé**

- **20 informaticiens** dont 5 pour l'infrastructure
- **1200 postes utilisateurs**
- **+200 serveurs**
- **4 contrôleurs de domaines**

Origine(s) de la crise

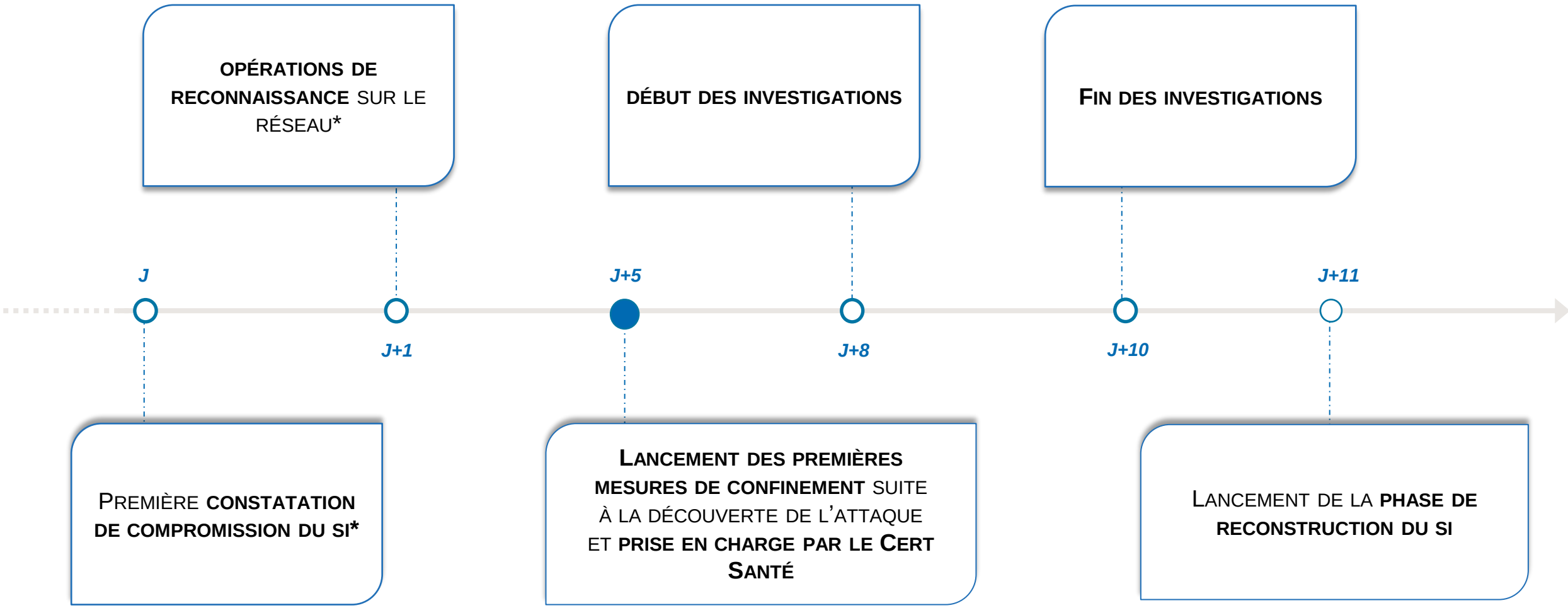
- **Compromission** du SI suite à la **réutilisation d'un identifiant de compte prestataire sur le VPN**

Risques identifiés*

- **Prise de contrôle à distance** des équipements
- **Possibilité de déploiement d'un rançongiciel** (chiffrement des données et des systèmes) provoquant l'**indisponibilité des ressources**
- **Perte irréversible des données et des ressources** (données, comptabilité, etc.)
- **Fuite / vol de données sensibles** des patients et/ou des collaborateurs

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

Chronologie des événements de la crise



*Evènements identifiés à postériori grâce à l'investigation

Chronologie détaillée de la crise

Evènements et actions concernant le **Groupement Hospitalier (GH)**

J

Première constatation de compromission du SI*

- Connexion depuis l'extérieur
- Non légitimée

J+1

Escalade vers un compte administrateur

- opérations de reconnaissance sur le réseau

J+5

Découverte de l'attaque et lancement des premières mesures de confinement

- Isolation totale d'internet
- Passage à un mode dégradé
- Isolation des ordinateurs et serveurs compromis du réseau
- Signalement de l'incident (CERT Santé)

J+11

Lancement de la phase de reprise progressive et de reconstruction

- Réouverture des flux techniques sur le firewall
- Réouverture des services de messagerie prévue entre le 8/9 et le 11/9
- Déclaration de l'incident (CNIL)

Accompagnement du **CERT Santé**

J+5

Début de prise en charge par le CERT Santé

- Appui au confinement

J+8

Début des investigations

- Premières analyses de l'activité malveillante

J+10

Fin des investigations du CERT Santé

- Identification des failles exploitées pour réaliser l'attaque
- Préparation du plan de reconstruction et de durcissement du SI

*Evènements identifiés à postériori grâce à l'investigation

Accompagnement post-crise

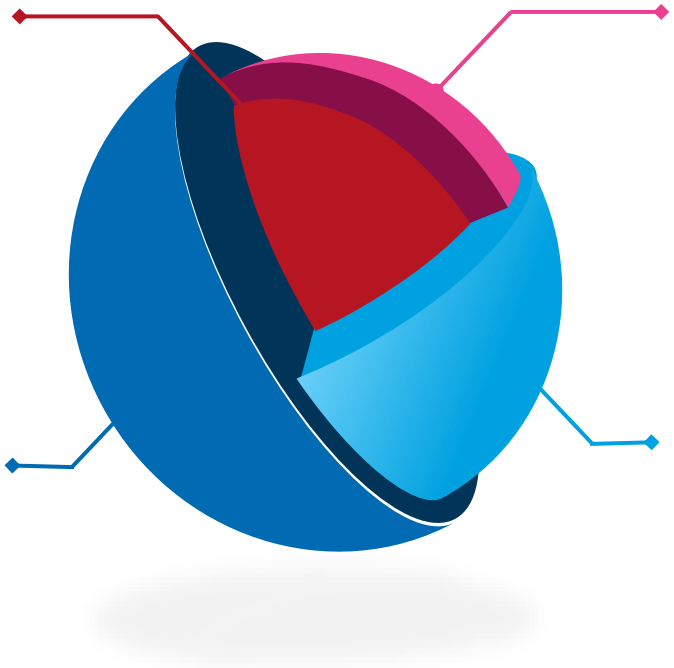
DÉFINITION D'UN PLAN DE REMÉDIATION ET ACCOMPAGNEMENT DU CERT SANTÉ

/ Les principales **recommandations** sont :

- **Renouvellement** des **identifiants** et isolation des comptes suspects
- **Renforcement** de **l'Active Directory**
- **Réinstallation des postes compromis** et **mise à jour** (logicielles, de règles de sécurité)
- **Renforcement** des **politiques de mot de passe** et début du **silotage**
- **Mise en place du MFA**, décommissionnement de postes obsolètes et **gestion centralisée des mots de passe**

Les étapes du déploiement du plan de remédiation

1. Services critiques / socle SI
S'assurer que le cœur de l'infrastructure est sécurisé



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

3. Postes de travail
Remettre en service les postes de travail pour tous les collaborateurs

4. Interconnexions et services exposés
Rétablir les connexions extérieures et les solutions de surveillance

Bilan de l'accompagnement durant la crise

Rappel de la chronologie des évènements

J :
Première opération de l'attaquant sur le SI

J+1 :
Escalade vers un compte administrateur

J+5 :
Découverte de l'attaque, début de l'intervention du CERT Santé et lancement des actions de confinement

J+8 :
Début des investigations du CERT Santé

J+10 :
Identification des actions malveillantes réalisées par l'attaquant suite aux investigations

J+11 :
Lancement de la phase de reconstruction du SI

Résultats et éléments clés

L'intervention du CERT Santé a permis **une investigation approfondie** et une **identification de la faille utilisée par l'attaquant. L'infiltration** sur le parc a eu lieu **via la réutilisation d'un identifiant de compte prestataire sur l'accès VPN.**

Plusieurs identifiants ont été exfiltrés au cours de l'incident. Au moins **un compte administrateur de domaine** ainsi qu'un compte utilisateur ont été compromis et **accédés depuis l'extérieur**.

Aucun impact constaté **sur la prise en charge patient.**

Points à retenir

1

L'étape d'investigation doit permettre d'identifier les vulnérabilités du SI exploitées par l'attaquant afin de renforcer sa sécurité

L'investigation permet d'identifier les scénarii possibles de la compromission, les faiblesses intrinsèques du SI et de proposer des mesures de remédiation adéquates

2

Importance de la **collaboration** pour **l'investigation et la remédiation** lors de l'incident de sécurité

Travail conjoint entre l'établissement et l'APHP sur les mesures de remédiation et investigation numérique du CERT Santé afin d'identifier le scénario de compromission

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé