AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Retour d'Expérience

Cyberattaque suite à la compromission d'un compte utilisateur

Contexte d'intervention

Entité hospitalière

- **La DSI gère plusieurs établissements**
- **2 administrateurs systèmes**
- **3 administrateurs réseaux**
- 4420 postes utilisateurs
- 180 serveurs physiques
- 650 machines virtuelles (VM)
- 14 contrôleurs de domaine

Origine(s) de la crise

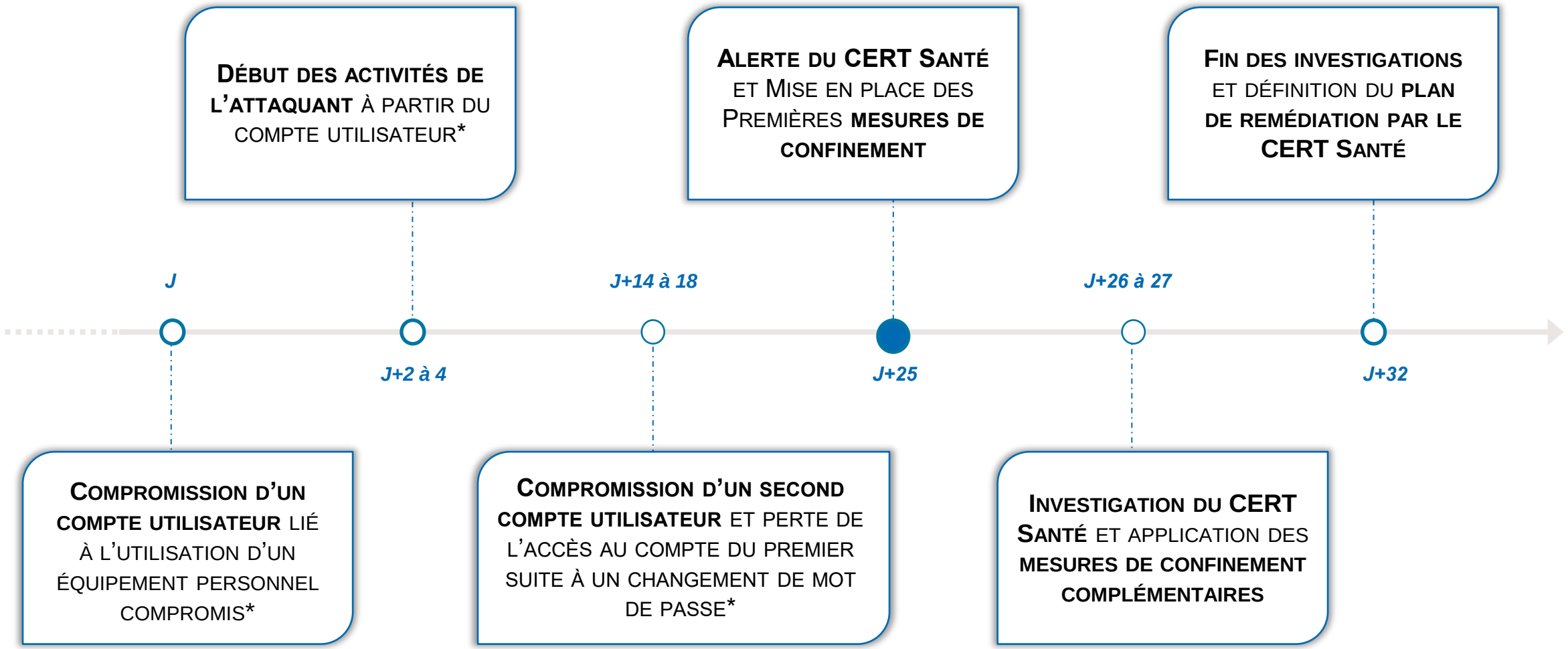
- **Compromission** d'un compte utilisateur suite à l'**utilisation d'un équipement personnel**
- **Compromission de l'AD du Centre Hospitalier**

Risques identifiés*

- **Prise de contrôle à distance** des équipements
- **Chiffrement des données et des systèmes** par le biais d'un rançongiciel 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 l'attaque et de la gestion de la crise

Evènements et actions concernant le **CENTRE HOSPITALIER**

J

Début de l'attaque*

- Compromission du compte d'un premier compte utilisateur par un équipement personnel
- Connexion illégitime via Citrix

J+2 à 4

Début des activités avec le compte utilisateur par l'attaquant*

- Aucun impact visible par le CH

J+14 à 18

Extension de la compromission*

- Compromission d'un second compte utilisateur
- .L'attaquant ne semble plus avoir accès au premier compte utilisateur suite à un changement de mot de passe

J+22 à 23

Activité de l'attaquant au sein du SI*

- Récupération d'un compte d'administrateur de domaine par l'attaquant et compromission de l'AD
  - Effacement des events windows (droits privilégiés sur le domaine ad du CH)
- Connexion au travers de l'accès a distance CITRIX
- Accès à la console de l'hyperviseur mais sans action réalisée

J+25 à 27

Confinement du SI

- Mise en place d'actions de confinement
  - Sécurisation des sauvegardes
  - Filtrage des PJ en entrées depuis internet sur les messagerie
  - Communication sur le fait de remontées tout évènement suspect
  - Changement des mots de passe KRBTG 2 fois de suite sur tous les AD
  - Changement des mots de passe administrateurs et renforcement de la politique d'accès

J+32

Lancement des actions de Remédiation

- Mise en place des actions de remédiation afin de pouvoir lever progressivement les mesures de confinement et procéder à la reconstruction

Accompagnement du **CERT Santé**

J+25

Réception d'une l'alerte et mise en place de mesures de confinement

- Prise de contact du CERT Santé avec le CH
- Mise en place de mesures de confinement :
  - Coupure internet en entrée et en sortie sur tous les établissements
  - Kill de toutes les sessions VPN/Citrix en cours
  - snapshot des contrôleurs de domaine CH & GH
  - Désactivation de la majorité des comptes d'admin des domaines de tous les établissements
  - Désactivation des comptes compromis
  - Inventaire d'intégrité des GPO
  - Coupure de l'accès DNS vers internet pour l'AD

J+26 à 27

Investigation réalisée par le CERT Santé

- Récupération des logs et de la journalisation de l'antivirus
- Constat de compromission et d'accès au si
- Aucune alerte remontée par l'antivirus sur la période de compromission

J+32

Fin de l'investigation et identification des axes de remédiation

- Revoir les pratiques d'administration
- Revoir le filtrage et sa politique
- Interdire l'accès internet en sortie de tous les serveurs
- Mettre en place un proxy sur tous les postes
- Revoir les politiques de mots de passe,
- Mettre à jour les ressources dont Citrix et les OS obsolètes et procéder à du durcissement
- Solliciter l'accompagnement d'un PRIS pour cette remédiation

*Evènements identifiés à postériori grâce à l'investigation

Accompagnement post- crise

J+32

ACCOMPAGNEMENT DU CERT SANTÉ À LA PRÉPARATION D'UN PLAN DE REMÉDIATION

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

- **Segmenter et micro-segmenter le réseau** du système d'information pour limiter les canaux d'administration
- **Revoir les filtres antivirus et leur configuration** mais aussi la politique de gestion des logs associée
- Assainir puis réaliser la **bascule de l'AD et son durcissement**
- **Changer** les **pratiques** d'administration du système d'information
- **Mettre à jour et suivre l'état du SI** : Citrix, OS obsolètes, services critiques, des équipements
- **Mettre en place une authentification forte** pour tous les postes VPN et limiter l'accès au VPN public
- Déployer un **proxy internet** dans tous les établissements
- **Coordination avec un PRIS** pour la mise en œuvre du plan de remédiation

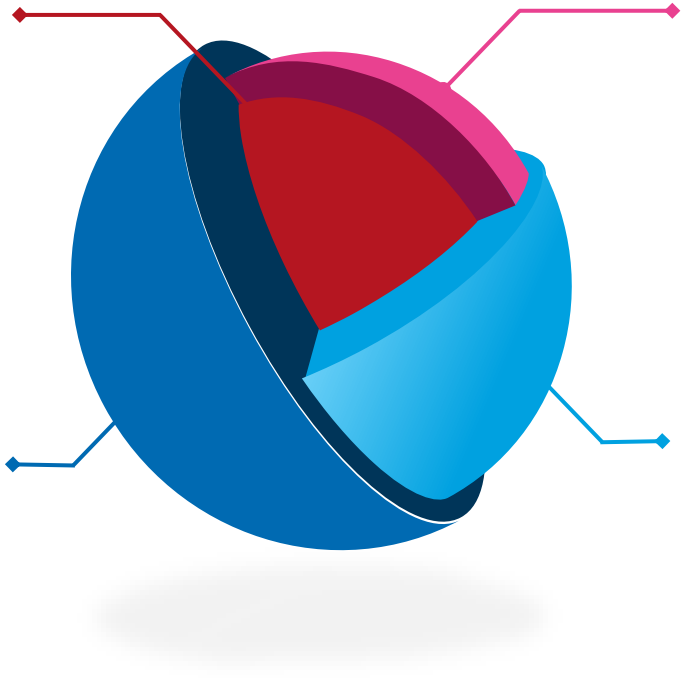
Les étapes du déploiement du plan de remédiation

1. Socle du SI (firewall,etc.)

S'assurer que le cœur du système d'information est sécurisé

2. Réseau et segmentation

Mettre en place un proxy dans tous les établissements du groupe



4. Mots de passe et administration

Renforcer l'accès au SI pour tous les utilisateurs mais en particulier pour les actions d'administration

3. Antivirus et mise à jour

Revoir la politique d'antivirus, surveiller les alertes, centraliser les logs etc. Contrôler la mise à jour des SI

Bilan de l'accompagnement durant la crise

Rappel de la chronologie des évènements

J :
Début de l'attaque : compromission d'un compte utilisateur

J+2 à 4 :
Réalisation d'actions malveillantes depuis le premier compte utilisateur

J+25 :
Alerte du CERT Santé et de l'ANSSI et mise en place des premières mesures de confinement

J+26 à +27 :
Poursuite du confinement du SI et investigations du CERT Santé

J+32 :
Fin des investigations et définition d'actions de remédiation

Résultats et éléments clés

L'attaque a abouti grâce à l'utilisation sur un compte utilisateur d'un **équipement personnel compromis** qui a conduit à la **compromission de deux comptes utilisateurs et de l'AD du Centre Hospitalier**

Les **données** des dossiers patients **n'ont pas été impactées par l'attaque car l'attaquant n'a pas mené d'action sur les systèmes, applications et les données avant le confinement.** Les **tentatives de connexion à l'infrastructure** VMWARE et aux serveurs de bases de données ont été **infructueuses.**

L'impact principal constaté se trouve lors de la mise en place des mesures de confinement avec la **coupure de l'accès à internet** en sortie (sauf messagerie mais seulement sans pièce jointe à risque) et par suite **l'inaccessibilité des services**

Points à retenir

1. **Alerté par un membre de l'InterCERT France, le CERT Santé** a pu intervenir pour une mise en œuvre rapide des mesures de confinement, d'investigation et de remédiation évitant ainsi des impacts majeurs
   - Alerte du CERT Santé et de l'ANSSI
2. **Une mise à disposition d'experts en cybersécurité par la DSI de l'établissement** afin de mettre en place les recommandations du CERT Santé
   - Accompagnement du CERT Santé au déploiement des capacités et moyens nécessaires afin de réaliser des investigations plus poussées
3. Importance de la **collaboration** pour **le confinement et les investigations** lors de d'incident de sécurité
   - Travail conjoint entre l'établissement, l'ANSSI et le CERT Santé sur les mesures de remédiation suite au signalement réalisé

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé