AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Retour d'Expérience

Un Groupement Hospitalier victime d'une compromission de son SI suite à une fuite d'identifiants

Contexte d'intervention

Entité hospitalière

- Plus de **6 000 agents et professionnels de santé** au service de près de 300 000 habitants

---

- **32 informaticiens** dont 9 pour l'infrastructure
- ~ **3 600 postes utilisateurs**
- ~ **800 machines virtuelles** sur 75 serveurs physiques
- **10 Active Directory** sur 21 serveurs

Origine(s) de la crise

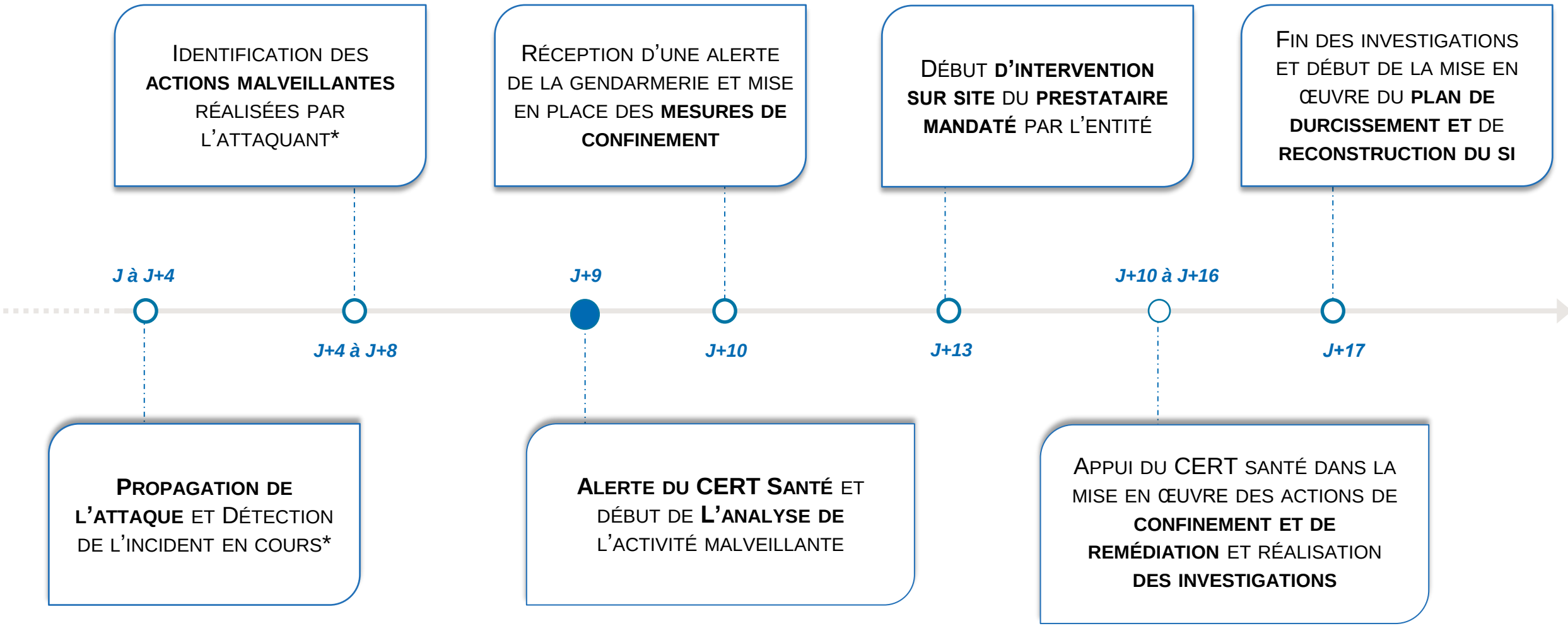
- Exploitation très probable de la **faille CVE-2018-13379 sur l'équipement Fortigate d'un des établissement du groupement afin d'obtenir des identifiants VPN**
- **Propagation** rapide de l'attaquant **sur le contrôleur de domaine de deux établissements de santé du groupement**

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 opération de l'attaquant sur le SI*

- Intrusion de l'attaquant sur le SI d'un des ES appartenant au GH en exploitant une faille logicielle

J+2

Détection par l'antivirus d'une action malveillante*

- Détection par l'antivirus du virus NESHTA sur 1 serveur AD et 30 postes utilisateurs
- Déconnexion immédiate du serveur AD

J+3 à J+4

Propagation de l'attaquant sur deux contrôleurs de domaine du GH*

- L'attaquant se propage sur le contrôleur de domaine (DC) de 2 ES appartenant au GH
- Un ES procède à l'isolement du DC d'un de ses siteS (initie un changement des mots de passe du domaine) et à une déconnexion du réseau des baies de stockage et de sauvegarde

J+4 à J+8

Identification des actions malveillantes réalisées par l'attaquant*

- Constatation de connexions illégitimes de l'attaquant par VPN

J+9

Découverte par l'ES d'un rançongiciel

- Un Fichier malveillant a été retrouvé sur 2 serveurs dont l'AD du GH

J+10 à J+11

Lancement des actions de confinement et notification CNIL

- Réception d'une Alerte de la gendarmerie
- Coupure de toutes les connexions internet en entrée et sortie de tous les établissements du GH
- Mise en sécurité des sauvegardes par déconnexion des baies de l'ensemble des établissements du GH
- Ouverture d'une cellule de crise élevée au niveau du GH pour contrôles et priorisation
- déclaration de l'incident à la CNIL

J+10 à J+16

Lancement des actions de Remédiation

- réinitialisation de tous les mots de passe internes du GH
- Modification de tous les mots de passe externes au GH
- Vérification des fichiers volés
- Filtrage des accès au réseau intersites
- Rétention des courriers entrants
- Début d'intervention sur site du partenaire sélectionné

J+17

Dépôt de plainte et Lancement du plan de durcissement et de reconstruction du SI

- Moyens de communications alternatifs
- Passerelle sécurisée internet unique
- Liste blanche de sites web
- Partenaires/prestataires
- Durcissement AD
- EDR/SOC Managé
- …

Accompagnement du **CERT Santé**

J+9

Notification au CERT Santé d'une vente de données concernant le GH

- L'Analyse de la fuite permet d'identifier des fichiers qui semblent appartenir à un établissement de santé
- Prise de contact avec l'établissement
- Premières analyses de l'activité malveillante

J+10

Lancement des investigations et appui dans la mise en œuvre de mesures d'urgence

- Demande des logs VPN et des serveurs exposés pour la période précédent le 20 avril
- Appui à la mise en place du confinement

J+17

Fin des investigationS

- Identification des failles utilisées pour réaliser l'attaque & transmission d'IOC à la police judiciaire (adresses IP, domaines etc.)
- (adresses IP, domaines etc.)
- Suivi des actions de remédiation
- Poursuite des investigations par le prestataire mandaté
- Suite de la phase de durcissement puis lancement du plan de reconstruction du SI

*Evènements identifiés à postériori grâce à l'investigation

Accompagnement post-crise aiguë

J+17

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

/ Les principales **recommandations** sont :

La maitrise (mise à jour, comptes admin, surveillance des consoles, ...) et la **rationalisation du SI** afin de limiter le nombre de services à administrer par l'équipe informatique au regard de ses effectifs réduits

L'utilisation de référentiels d'authentification et d'autorisation de sécurité distincts sur les **ressources critiques** du SI (sauvegarde, hyperviseur, ...)

L'application des **bonnes pratiques d'hygiène informatique**

La **mise en place d'un bastion d'administration** afin d'assurer le suivi et la journalisation des logs et des actions d'administration réalisées

La nécessité d'être accompagné par un prestataire de sécurité (PRIS) pour la reconstruction du SI

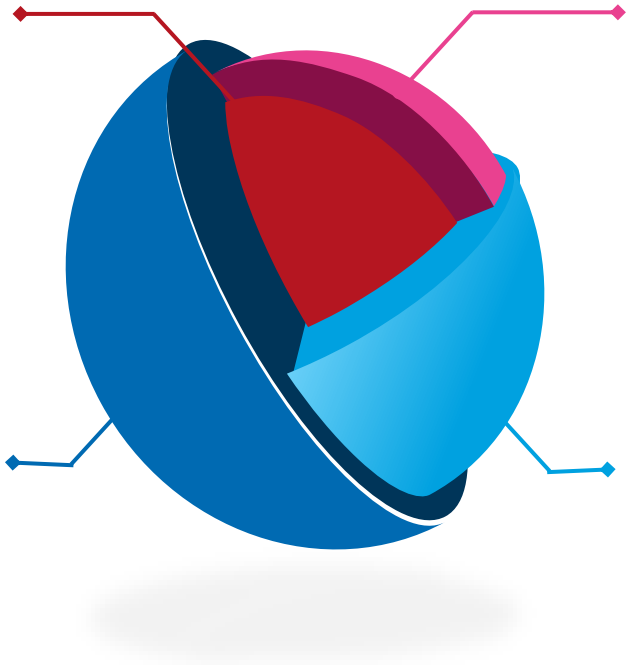
Les étapes du déploiement du plan de durcissement

1. Maitrise du SI

S'assurer que le système d'information est sécurisé notamment avec la construction d'une nouvelle architecture AD unique

2. Rationalisation du SI

Eviter l'existence de doublon ou de ressources redondantes, faciliter le maintien en conditions de sécurité



3. Contrôle des actions d'administration

Mettre en place un bastion d'administration

4. Maintien en conditions de sécurité du SI

Suivre les règles d'hygiène de l'ANSSI

Bilan de l'accompagnement durant la crise

Rappel de la chronologie des évènements

J :
Première opération de l'attaquant sur le SI

J+2 :
Détection par l'antivirus du virus NESHTA sur 1 serveur AD et 30 postes utilisateurs

J+3 à J+4 :
Propagation de l'attaquant sur deux contrôleurs de domaine de 2 ES appartenant à la structure

J+4 à J+8 :
Identification des actions malveillantes réalisées par l'attaquant

J+9 :
Le CERT Santé est alerté par un membre de l'InterCERT France concernant l'un de ses bénéficiaires - Information de l'ES et lancement de l'analyse

J+10 :
Réunion entre l'ES et le CERT Santé et mise en oeuvre des premières mesures de confinement

J+10 à J+16 :
Mise en œuvre des premières mesures de remédiation. L'incident a également été déclaré à la CNIL

J+17 :
Fin de l'investigation du CERT Santé et début des travaux de durcissement. Le prestataire complète l'investigation et entame les actions de remédiation

Résultats et éléments clés

L'intervention du CERT Santé a permis **une investigation approfondie** et une **identification de la faille utilisée et d'un scenario d'attaque vraisemblable**

Les **données** des dossiers **patients ont été impactées** par l'attaque. Un vol de données a été recensé. Une **déclaration a été faite à la CNIL** pour les 3 établissements avec un important travail d'identification et d'information des personnes concernées.

La coupure du réseau Internet en entrée et sortie de tous les établissements afin de stopper l'intrusion a, entre autres, conduit à **de fortes perturbations des services (service d'imagerie, résultats d'analyses, SAMU, administratifs,...)** ainsi que divers **dysfonctionnements** (l'indisponibilité de la messagerie, perte des mises à jour logiciels, la perte de la géolocalisation du SAMU, la perte de la télésurveillance des patients, …)

Points à retenir

1. **La veille sur les menaces de cybersécurité et le partage d'information au sein de la communauté InterCERT France** a permis au CERT Santé d'intervenir de façon proactive vis-à-vis du GH

   Le CERT Santé a été alerté par un membre de l'InterCERT France et il y a eu une forte mobilisation et réaction des équipes SI et sécurité du GH (au profit des 2 sites directement touchés)

2. **Les alertes Antivirus concernant les serveurs doivent** faire l'objet d'une analyse particulière. Lorsqu'une alerte concerne un Active Directory, il faut systématiquement et immédiatement **communiquer avec le CERT Santé .**

   L'antivirus avait relevé la vulnérabilité mais l'ES n'a pas pu réaliser une analyse suffisante

3. **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 permet d'identifier des mesures de remédiation afin d'avancer sur tous les SI du GH de manière homogène

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé