Incident sécurité CPPM 2025

PLAN

- Détection
- Actions immédiates
- Impacts
- Analyse
- Correctifs
- Reprise d’activité

Détection

- Post mortem on identifie le point de départ de l'incident le dimanche 27 Juillet (~10 heures UTC).
- Dès le lundi 28 , des pages web sont inaccessibles/corrompues ce qui entraine un regard de la part des admins qui identifie un problème suspect.
    - Ce mauvais fonctionnement de pages web n'était pas du fait direct de la compromission mais une conséquence.

- Des connexions ssh importantes sont faites depuis le laboratoire vers l'extérieur. Des communications vers des canaux irc sont identifiées.

Très vite il apparait que le laboratoire est victime d'une intrusion importante (plusieurs machines).

Actions immédiates

- Fermeture au niveau réseau local des connexion ssh sur nos machines identifiées comme compromises.
- Fermeture au niveau du WAN des connexions requêtes ssh et IRC
- On identifie assez rapidement que la propagation en interne (la latérisation) c'est fait par l'usage de clefs ssh d'utilisateurs et d'administrateurs.
  - Blocage des accès via les clefs ssh en conséquence.
  - Certaines de ces clefs étaient aussi utilisées pour des accès extérieurs au laboratoire.

Impacts

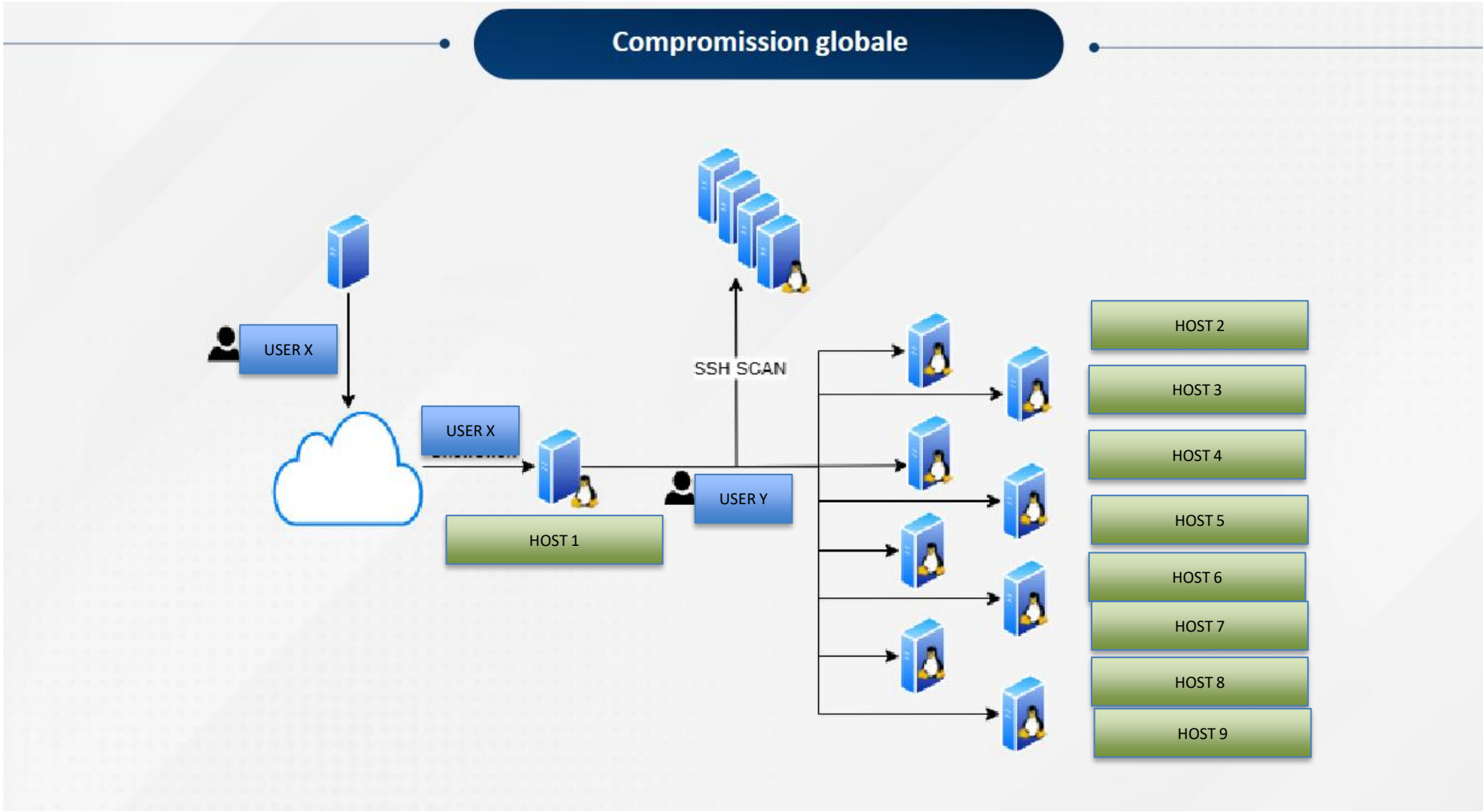
- Un jeu de clefs ssh utilisées dans nombre de machines a été utilisé pour propager la corruption
  - Services du laboratoire
  - Machine de grille
  - Machine plateforme cloud
  - Pas de poste perso

- Potentiellement l'ensemble des machines « de service » du laboratoire sont corrompues.
- La très grande majorité des machines des groupes de physiques sont stoppées.
- Des espaces de stockage (grille mais aussi des espaces utilisateurs locaux) sont stoppés.
- En pratique (post mortem) une vingtaine de machines ont été impactées.

Analyses

- Vecteur (analyse post mortem) de l'intrusion
  - Un ex-utilisateur du laboratoire avait un accès, via clef ssh , sur une machine d'un groupe de physique.
  - Cette clef a été utilisée pour accéder à cette machine.
  - Utilisation d'un rootkit sur cette machine qui avait un OS obsolète.
  - Suite à cette élévation de privilèges , acquisition de nouvelles clefs ssh et notamment une utilisée sur la grande majorité des machines du laboratoire.
  - A partir de là un certain nombre de machines on été corrompues et un logiciel malveillant a été installé.
  - Des scan ssh ont été fait pour latéralisé en dehors du labo la compromission.

Analyses


Compromission globale
USER X
USER X
HOST 1
SSH SCAN
USER Y
HOST 2
HOST 3
HOST 4
HOST 5
HOST 6
HOST 7
HOST 8
HOST 9

Analyses

- En pratique
  - Exploitation de la vulnérabilité **PwnKit (CVE-2021-4034).**
  - L'attaquant a déployé un **botnet IRC/SSH** sur les équipements compromis.
  - Utilisation de **6 codes malveillants différents (Botnet, porte dérobée, outil de masquage).**
  - Menace de type **cybercriminelle / opportuniste.**
    - Pas de vol de données
  - Méthodes employées pour assurer la persistance :
    - Remplacement de binaires légitimes par le logiciel malveillant **6can**.
      - Ex : ls, zcat, nologin. Visudo, /etc/ld.so.conf, des man ,…..
    - Modification de **crontabs**
      - Le monthly, le crontab,….
    - Modification des **configurations SSH**
      - Changement dans le authorized
    - Ajout de clés **SSH autorisées**
      - Notamment une clef a été rajouté dans le « compte game »
    - Exploitation des loader des librairies dynamiques

Analyses

- Quelques détails
  - La commande ls n'a pas la taille initiale, elle renvoie des infos « aléatoires » et surtout elle régénère les mécanismes de persistance du logiciel malveillant.
  - Le compte « game » est normalement affecté à un shell nologin, qui est lui-même un binaire corrompu (voir ls ci-dessus). Une clef étant rajoutée sur ce compte il suffit d'invoquer une connexion ssh sur ce compte pour lancer nologin et donc régénérer le logiciel malveillant.
  - Le chargement des librairies dynamiques étant corrompu, potentiellement toutes commandes qui utilise des librairies dynamiques donne des résultats faux et surtout régénère le logiciel.
  - Les crontab étaient surtout utilisés pour permettre à une machine encore contaminée de recontaminé une machine en cours de « rémission »

Correctifs

- Mise à jour OS autant que faire se peut et même plus que ca.
  - Définition d'un OS de référence pour le laboratoire.
  - Bannissement autant que ce faire se peut des clefs ssh.
  - Document de références définissant les bonnes pratiques pour une installation de serveur.
- Usage d'un portail pour rentrer dans le laboratoire obligatoire.
- Bastionisation des accès administrateurs sur les serveurs.
  - 3 bastions : Machines de services laboratoire, machines de grille/cloud, machines de groupes (ayant des utilisateurs)
  - Seul une poignée d'admin peut accéder au bastion (protection forte pour cet accès)
- Installation systématique d'une interface de management sur les machines de services.
- Définition d'une politique de mots de passes administrateurs (OS et management) qui garantie une unicité de celui-ci.

Reprise d'activité

- Dans le doute, ou dès que cela était faisable, on a réinstallé les machines.
  - Machines des services labo en priorité.
  - Machines des groupes de Physique.
  - Corolaire : Passage sur une infra virtualisée pour ces nouvelles installations.
- Mise en place des bastions.
- Migration des machines dans le bastion approprié.
  - En cours pour les existantes où celles qui ont été « remontées » en urgence.
  - Obligatoire pour tout nouveau serveur arrivant au laboratoire.

Reprise d'activité (grille)

- On a éteint la grille complètement dès le début de l'incident. (Downtime de plus de deux mois)
  - Pas prioritaire, notamment car l'incident a eu lieu en plein durant les vacances estivales.
  - Sanctuarisation de la DB du SE.
- Création d'un bastion grille/cloud
  - Réinstallation de 100% des machines dans le bastion.
  - Priorité au stockage.
- Réinstallation stockage de grille
  - OS up to date, dcache up to date,…..
- Réinstallation CE, squid,….
  - OS up to date, reinstallation CE, workers from scratch

Hors-sujet

- Réinstallation SE
  - Installer serveur de base de données avec l'assurance de l'intégrité de la DB.
  - Installation du headnode (SE).
  - Réinstallation à la main des disques serveurs (préservation des datas indispensable).
  - Garder une config « identique » à celle d'avant.
  - Puis une semaine de galère pour faire fonctionner le truc
    - Passage de dcache 8 à dcache 10
    - Des méthodes/fonctionnalités dcache (notamment id token/voms/…) très différentes entre dcache 8 et dcache 10.
    - Des configs issus de la migration dpm vers dcache.
    - Un manque de compétence.
    - Reprise quasi from scratch de la config dcache.