Forensic Challenge

Cas 1 : Intrusion sur un serveur Windows

1. Introduction

1.1 Contexte

Un serveur Windows appartenant à l'entreprise a présenté des comportements suspects, notamment des connexions réseau inhabituelles et des processus inconnus. Une image forensique du système a été réalisée pour analyse approfondie.

1.2 Résumé

Compromission du serveur : résumé des événements

Entre le 4 et le 9 février 2024, le serveur, accessible à distance via Internet pour permettre le télétravail de l'administrateur, a été compromis suite à une attaque par bruteforce. Les attaquants ont testé des milliers de combinaisons jusqu'à trouver un mot de passe administrateur valide. Une fois l'accès obtenu, ils ont créé un nouveau compte "admin", installé des outils d'administration et de repérage pour cartographier le réseau, et affaibli l'antivirus intégré afin d'éviter toute détection.

Par la suite, ils ont déposé et extrait une archive contenant deux programmes malveillants déguisés en outils Windows, appartenant à la famille Petya (chiffrement des données à des fins d'extorsion). En parallèle, ils ont compressé et exfiltré le dossier partagé des utilisateurs du serveur. Une note de rançon est également apparue. Enfin, les attaquants ont propagé et exécuté automatiquement le programme malveillant sur six ordinateurs du réseau.

---

2. Analyse technique

Les opérateurs ont :

- Créé et utilisé un compte local admin.
- Installé Npcap (7045 dans System.evtx) et légitimé sa persistance via une tâche planifiée \ npcapwatchdog.
- Réduit les défenses en arrêtant Microsoft Defender (7036 dans System.evtx).
- Déposé/extrait une archive (**important.zip**) contenant dir.exe et rename.exe
- Laissé apparaître une note de rançon RyukReadMe.txt
- Préparé un déploiement latéral via la tâche planifiée \Enterpries backup (fichier XML de tâche) qui exécute PsExec vers Desktop-001…006.

Des indices d'exfiltration sont visibles (share.zip ≈ 700 Mo créé puis supprimé — $MFT/$J).

2.1 Sources et méthodes

- **Journaux Windows** : Security.evtx, System.evtx, PowerShell/Operational.evtx, RemoteConnectionManager/Operational.evtx
- **Registre** : ruche SYSTEM, SECURITY, SOFWARE, etc...
- **NTFS** : extractions $MFT et USN Journal ($J)
- **Tâches planifiées** : fichiers XML de \npcapwatchdog et \Enterpries backup.

---

3. Analyses

3.1 Journaux d’événements Windows (bruteforce, RDP, PowerShell, services)

- **Premiers RDP réussis observés** :
  - 05/02/2024 08:52:06 UTC depuis 195.21.1.97 vers BRANCHOFFICE\Administrator (4624, LogonType=10, Security.evtx).
  - D’autres succès suivent depuis 185.229.66.183 (soir du 05/02) et 31.220.85.162 (06/02 19:52 UTC).
- **Volumétrie d’échecs (bruteforce)** : grand nombre de 4625 (échecs d’authentification).
- **PowerShell** : événements 4104 (Script Block Logging) et 4103 (Module Logging) autour de 23:42 UTC le 05/02, montrant le chargement/usage du module **ScheduledTasks**.
- **Services** :
  - Installation d’un service : **Npcap Packet Driver (NPCAP)**, 7045 le 05/02/2024 23:42:42 UTC.
  - Arrêt d’un service de sécurité : **Microsoft Defender Antivirus Service**, 7036 à 21:31:54 UTC le 06/02.

3.2 Base de registre Windows

- **État RDP** :
  - HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\ → fDenyTSConnections=0 (RDP autorisé).
  - Port WinStations\RDP-Tcp\PortNumber=3389.

3.3 Artefacts de persistance

- **\npcapwatchdog** : tâche planifiée exécutant C:\Program Files\Npcap\CheckStatus.bat (XML de tâche).
- **\Enterpries backup** : tâche planifiée créée le 06/02/2024 21:49:21 (XML de tâche RegistrationInfo/Date) avec action :

```
C:\Users\admin\Downloads\SysinternalsSuite\PsExec.exe -accept-eula \\Desktop-001,Desktop-002,Desktop-003,Desktop-004,Desktop-005,Desktop-006 -c -d -u admin -p letmein -realtime C:\Users\admin\Desktop\rename.exe
```

→ Objectif : pousser puis exécuter rename.exe à distance via les partages ADMIN$ des postes.

3.4 Fichiers, outillage et indices d’exfiltration

- **Archive et binaires** :
    - important.zip (déposé/extrait) livrant dir.exe et rename.exe sur le Bureau de admin ($MFT/$J dans la fenêtre 06/02 ~20:09–20:13 UTC) binaire **petya** respectivement "plein format" et dropper.
    - Hash de rename.exe :
        - MD5 : af2379cc4d607a45ac44d62135fb7015.
        - SHA-1 : 39b6d40906c7f7f080e6befa93324dddadcbd9fa.
    - Hash de dire.exe
        - MD5 : a92f13f3a1b3b39833d3cc336301b713
        - SHA-1 : d1c62ac62e68875085b62fa651fb17d4d7313887

- **Note de rançon** : RyukReadMe.txt apparue le 06/02/2024 20:53 UTC sur le Bureau.
- **Exfiltration probable** : share.zip (~700 Mo) créé puis supprimé le 06/02/2024 22:14:44 UTC.
- **Scan réseau** : fichiers Zenmap/Nmap indiquant des scans “Intense scan” réalisés le

- 06/02/2024 21:09 UTC et le 07/02/2024 10:16 UTC.

3.5 Chronologie (UTC)

(en construction …)

4. Résultats

4.1 Découvertes et IoC

- **Adresses IP externes** :
  - 195.21.1.97, 185.229.66.183, 31.220.85.162.
- **Postes internes ciblés** :
  - Desktop-001 → 10.44.24.1, Desktop-002 → 10.44.24.6, etc.
- **Fichiers/artefacts** :
  - important.zip, dir.exe, rename.exe, RyukReadMe.txt, share.zip.

4.2 Étendue de la compromission

- Serveur compromis (accès RDP, outillage installé, défense affaiblie).
- Tentative de latéralisation via PsExec.
- Indicateurs d'exfiltration (share.zip).

---

5. Recommandations

5.1 Mesures immédiates

- Isolement réseau du serveur et des hôtes compromis.
- Réinitialisation des mots de passe administrateurs.
- Blocage des IP externes identifiées.
- Conservation des artefacts pour preuve.

5.2 Renforcement

- Sécurisation RDP (NLA, MFA, audits).
- Renforcement des défenses (EDR, durcissement Defender).
- Gestion des comptes (LAPS).
- Sauvegardes immuables.

5.3 Surveillance continue

- Détection des événements suspects (7045, 7036, tâches planifiées, PsExec).
- Corrélation des journaux RDP (Schannel, 4624/1149).

---

6. Conclusion

Les artefacts montrent une compromission RDP suivie de déploiement d’outils, réduction des défenses, exfiltration probable et tentative de latéralisation. Les recommandations visent à éradiquer la menace, remédier aux impacts et prévenir les récidives.