Rapport d’analyse – Dossier #2026-1179-C

Analyse informatique - Résidus de code et compromission système

1. Contexte de l’intervention

Le dossier #2026-1179-C concerne l’examen d’un terminal informatique saisi dans le cadre d’une enquête portant sur une possible intrusion numérique.

L’objectif était d’identifier :

- l’origine des anomalies détectées,
- la nature des manipulations effectuées,
- l’étendue de la compromission,
- les traces laissées par l’auteur des faits.

Les opérations ont été menées par l’unité d’analyse numérique du laboratoire PTS.

2. Paragraphe technique

Le laboratoire a procédé à l'analyse rigoureuse des données trouvées.
Analyses ont révélé un code source altéré.
Indice sur la console montrent une intrusion.
Bugs_ bloquent l'accès aux logs principaux.
Base de données montre un vidage complet.
Code malveillant inséré par un tiers inconnu.
IP__ tracée renvoie vers un serveur distant.
Flux de réseau interrompu à minuit pile.
Logs effacés juste après la manipulation.
Clés de chiffrement compromises hier soir.
Vers un piratage de grande envergure.
Plus de traces physiques sur le terminal.
Outil utilisé restant à identifier.
Script détecté sur le disque dur externe.
Données_ sont désormais sécurisées par nos experts.
L'enquête se poursuit afin d'identifier l'auteur des faits.

3. Analyse scientifique

Les éléments relevés indiquent une altération volontaire du code source, suivie d’un effacement ciblé des journaux système.

La compromission des clés de chiffrement et l’interruption nette du flux réseau à une heure précise suggèrent une action coordonnée.

Le script retrouvé sur le disque dur externe semble être un outil d’exécution automatisée, mais son origine reste inconnue.

L’IP distante identifiée renvoie vers un serveur hors juridiction locale, nécessitant une investigation complémentaire.

Le vidage complet de la base de données confirme une volonté de destruction ou d’exfiltration des informations.

4. Interprétation des résultats

Les manipulations observées sont compatibles avec une intrusion avancée menée par un individu maîtrisant les techniques de dissimulation numérique.

L’absence de traces physiques sur le terminal et l’effacement des logs indiquent une tentative de rendre l’analyse impossible.

Les anomalies relevées ne correspondent à aucun dysfonctionnement classique : elles sont intentionnelles.

Les données sécurisées par les experts ont permis de stabiliser le système et d’éviter une propagation éventuelle.

5. Conclusion

Le dossier #2026-1179-C révèle une compromission majeure du terminal analysé.

Les indices convergent vers un piratage de grande envergure, orchestré par un tiers non identifié.

Les éléments pertinents ont été transmis aux enquêteurs pour exploitation judiciaire.

L’enquête se poursuit afin d’identifier l’auteur des faits.