

Lab 01

Cybersecurity 3 / Exemple Rapport

Analyse Forensique d'un poste Windows compromis

Rapport d'Analyse Forensique

Référence : RF-2025-001

Auteur : Équipe Forensic / CERT interne

Date du rapport : 15 juillet 2025

Objet : Analyse forensique suite à suspicion d'intrusion sur un poste utilisateur

1. Contexte de l'investigation

Le 10 juillet 2025 à 9h45, le SOC (Security Operation Center) a détecté une activité anormale sur le poste utilisateur **WIN-DEV-07** appartenant à un développeur de l'équipe R&D. L'alerte provenait de l'EDR SentinelOne, signalant l'exécution d'un binaire suspect inconnu par l'utilisateur.

2. Objectifs de l'analyse

- Confirmer ou infirmer la compromission du poste.
- Identifier les vecteurs d'attaque utilisés.
- Déterminer le périmètre de l'intrusion.
- Relever les artefacts de persistance, escalade de privilèges, mouvements latéraux.
- Proposer des mesures correctives et préventives.

3. Méthodologie

Les outils suivants ont été utilisés :

Outil	Utilisation principale
Autopsy	Analyse du disque (.E01)
Volatility	Analyse du dump mémoire
FTK Imager	Acquisition des images disque et RAM
Sysinternals	Collecte d'artefacts (Preethi, registry)

Outil	Utilisation principale
Wireshark	Analyse du trafic réseau capturé (.pcap)

4. Sources analysées

Source	Type de preuve
WIN-DEV-07.E01	Image disque
RAM-WIN-DEV-07.raw	Dump mémoire
network_traffic_10-07.pcap	Capture réseau
Fichiers artefacts	Prefetch, LNK, Registry, Logs EVTX

5. Chronologie des événements

Heure	Événement clé
10/07 - 08:42	Ouverture d'un email avec pièce jointe facture.exe
10/07 - 08:43	Exécution du fichier via double-clic (observé via Prefetch + logs AppCompatCache)
10/07 - 08:44	Création d'un processus inconnu msupdater.exe dans %APPDATA%\Roaming\
10/07 - 08:45	Ouverture d'un canal réseau vers l'IP 185.234.218.15:443 (non référencée DNS)
10/07 - 08:46	Création d'une tâche planifiée nommée WindowsUpdaterDaily (persistance)
10/07 - 08:49	Dump des identifiants Windows via lsass (observé en mémoire)

6. Indicateurs de compromission (IoC)

6.1. Fichier malveillant

Nom du fichier	Hash SHA256	Emplacement
facture.exe	4e0d86d2d95351ae781c875ebbf1d1a54fda8d0f4ccf8c1e6fa...	Téléchargé depuis Outlook

6.2. Processus anormaux

- msupdater.exe : non signé, lancé depuis %APPDATA%
- Utilisation de rundll32.exe pour exécuter une DLL obfusquée

6.3. Connexion réseau suspecte

IP distante	Port	Protocole	Pays d'origine (GeoIP)
185.234.218.15	443	TLS	Russie

6.4. Persistence

- Tâche planifiée : WindowsUpdaterDaily
- Clé de registre : HKCU\Software\Microsoft\Windows\CurrentVersion\Run

7. Analyse mémoire

- Processus lsass.exe injecté (indication de Mimikatz ou équivalent)
- Présence d'un binaire en mémoire nommé postex.dll (outil post-exploitation)
- Sections mémoire non mappées, exécutées directement en RAM

8. Analyse réseau

- Chiffrement TLS custom (pas de SNI, protocole non standard)
- Période de communication : toutes les 5 minutes
- Probable commande & contrôle (C2)

9. Évaluation de la compromission

Élément	Présence
Exécution de code distant	✓
Escalade de privilèges	✗ (utilisateur simple)
Mouvement latéral	✗
Dump de credentials	✓ (présence d'identifiants)
Persistence implantée	✓

Conclusion : le poste a été **compromis**, mais l'intrusion semble limitée à cet hôte.

10. Préconisations

Court terme (immédiat)

- Déconnexion du poste WIN-DEV-07 du réseau
- Réinitialisation des mots de passe de l'utilisateur
- Scan complet de tous les postes du réseau pour les IoCs identifiés

Moyen terme

- Campagne de sensibilisation à l'hameçonnage
- Renforcement de la détection des binaires inconnus (EDR + sandboxing)
- Surveillance des connexions sortantes suspectes

Long terme

- Implémentation de la journalisation centralisée des événements de sécurité
- Mise en œuvre de l'authentification multi-facteurs (MFA)
- Révision de la politique de privilèges utilisateurs

11. Annexes

- Hashs de tous les fichiers analysés
- Logs Windows Event Viewer (EVTX) extraits
- Liste des clés de registre modifiées
- PCAP annoté avec marquage des connexions suspectes
- Dump mémoire compressé (archive sécurisée)