TACHE 2 : SURVEILLANCE DES ALERTES DE SÉCURITÉ ET SIMULATION DE RÉPONSE AUX INCIDENTS

RAPPORT DE RÉPONSE AUX INCIDENTS SÉCURITÉ

Référence : INC-2025-07-03

Statut : Final

Sévérité : CRITIQUE

AUTEUR : BARIKI Wilson

Date du rapport : 9 Janvier 2026

I- RÉSUMÉ EXÉCUTIF

Le 03 juillet 2025, entre 04:18 et 09:10, une série d'activités malveillantes coordonnées a été détectée sur le réseau. L'attaque a progressé d'une phase de reconnaissance et d'infection par chevaux de Troie vers une phase critique de **comportement de Ransomware** ciblant des ressources internes. Plusieurs comptes utilisateurs (Bob, Alice) et serveurs (172.16.0.3) ont été compromis. Des mesures d'urgence ont été prises pour isoler les systèmes touchés et bloquer les communications externes suspectes.

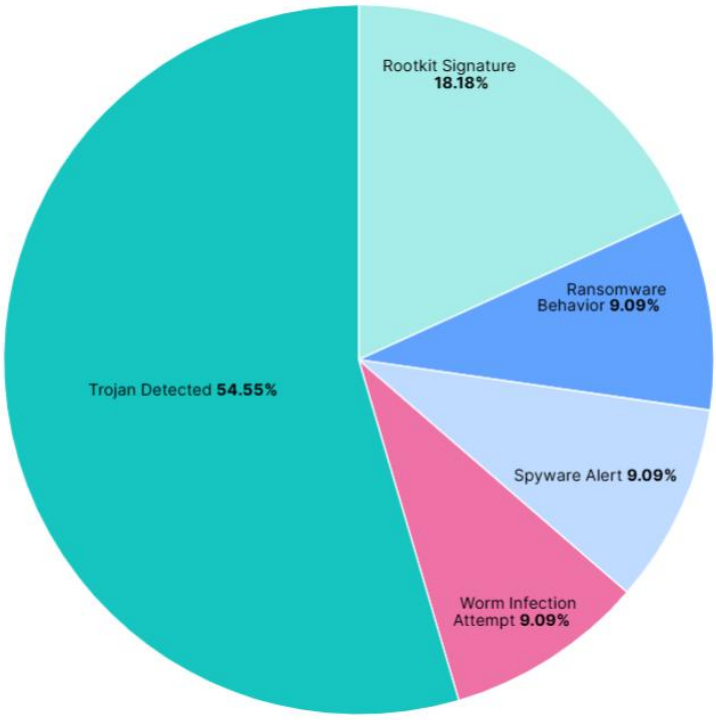

Figure 1 : Répartition des menaces détectées via le SIEM (Prédominance de Trojans et détection de Ransomware).

II- CHRONOLOGIE DES ÉVÉNEMENTS (TIMELINE)

Basé sur l'analyse des logs SIEM Elastic.

- **04:18:14 :** Première activité suspecte. Connexion réussie de l'utilisateur **Bob** depuis une IP inhabituelle (**198.51.100.42**).
- **04:19:14 :** Alerte **Rootkit Signature** déclenchée sur le poste d'**Alice**. Indique une compromission profonde du noyau système.
- **05:06:14 :** Détection d'une tentative d'infection par un **Ver (Worm)** depuis l'IP **203.0.113.77** associée à Bob.
- **07:02:14 :** Début d'une tentative de force brute (plusieurs échecs de connexion) sur le compte d'Alice depuis l'IP **203.0.113.77**.

- **09:10:14 : INCIDENT MAJEUR :** Détection d'un comportement de **Ransomware** sur le serveur **172.16.0.3** (Session de Bob).

Figure 2 : Détail du log critique identifiant le comportement de Ransomware sur le compte de Bob.

III- ANALYSE TECHNIQUE ET TRIAGE

L'analyse montre que l'attaquant a utilisé plusieurs vecteurs :

1. **Vecteur d'entrée :** Compromission de comptes via des adresses IP externes suspectes (198.51.100.42 et 203.0.113.77).
2. **Mouvement latéral :** L'utilisation du malware de type "Worm" suggère une tentative de l'attaquant de se propager d'un poste à un autre sur le segment réseau 172.16.0.x.
3. **Objectif final :** Le déclenchement du Ransomware à 09:10 indique que l'attaquant était prêt à exfiltrer ou chiffrer les données sensibles sur le serveur de fichiers.

Classification des alertes analysées :

- **Utilisateur le plus impacté :** Bob (associé au Ransomware et au Worm).
- **IP source la plus dangereuse :** 203.0.113.77 (Source de multiples attaques).

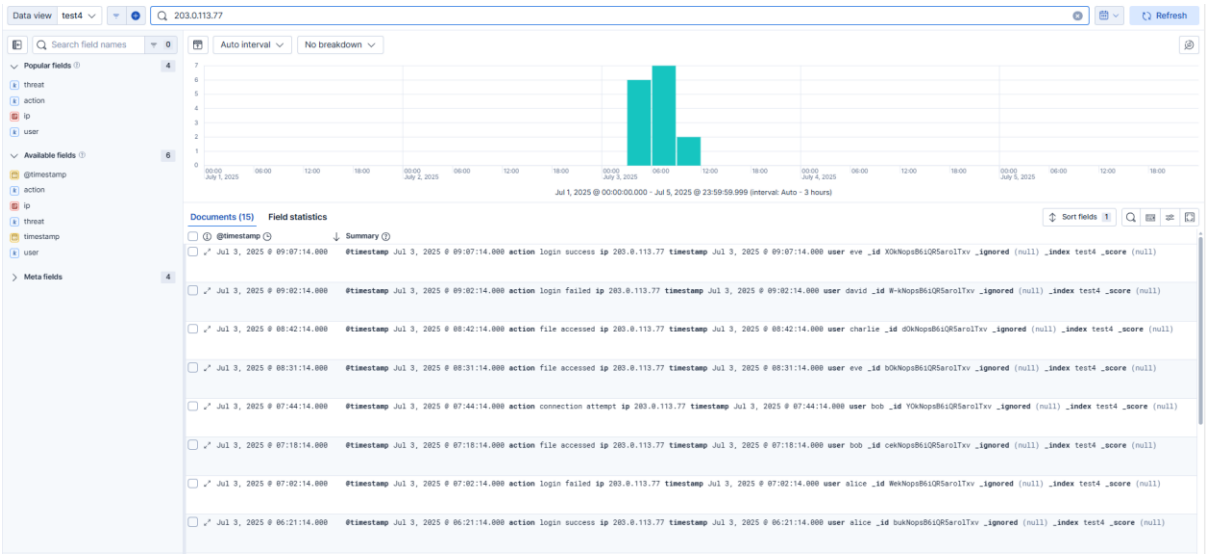

Figure 3 : Historique des activités malveillantes provenant de l'IP source 203.0.113.77

IV- ANALYSE DE L'IMPACT

- **Confidentialité :** Élevée. Risque de vol de données via le Rootkit et les accès réussis.
- **Intégrité :** Critique. Le Ransomware menace l'intégrité des fichiers sur le serveur de production.
- **Disponibilité :** Élevée. Risque d'arrêt complet des services si les fichiers sont chiffrés.

V- MESURES DE CONFINEMENT ET REMÉDIATION (PLAYBOOK)

Conformément aux procédures du SOC, les actions suivantes ont été recommandées/appliquées :

- **Mesures immédiates (Confinement) :**

- Isolation réseau du serveur 172.16.0.3 et du poste de travail de Bob.
- Blocage immédiat des adresses IP 203.0.113.77 et 198.51.100.42 sur le firewall périmétrique.
- Désactivation temporaire des comptes utilisateurs "Bob" et "Alice".

- **Mesures de nettoyage (Éradication) :**

- Analyse complète (Full Scan) avec l'antivirus EDR sur tous les postes mentionnés.
- Réinstallation complète (Re-imaging) du poste d'Alice (dû à la présence du Rootkit).

- **Récupération :**

- Restauration des fichiers du serveur 172.16.0.3 à partir des sauvegardes saines (si nécessaire).
- Réinitialisation forcée des mots de passe de tous les utilisateurs impactés avec exigence de MFA (Authentification Multi-Facteurs).

VI- RECOMMANDATIONS

- **Renforcement de l'authentification :** Déployer l'authentification multi-facteurs (MFA) sur tous les comptes, en priorité pour Bob et Alice qui ont été les cibles principales.
- **Filtrage IP et Géo-blocage :** Configurer le pare-feu pour bloquer systématiquement les adresses IP externes non répertoriées (notamment 203.0.113.77 et 198.51.100.42) et restreindre les accès aux zones géographiques utiles à l'entreprise.
- **Gestion des privilèges :** Appliquer le principe du "moindre privilège". L'utilisateur Bob n'aurait pas dû avoir les droits suffisants pour exécuter un processus de type ransomware sur le serveur de fichiers.
- **Sensibilisation (Security Awareness) :** Organiser une session de formation sur le phishing et les malwares pour les employés, car l'infection initiale par Trojan suggère une erreur humaine (clic sur un lien ou pièce jointe).

CONCLUSION

L'incident détecté le 03 juillet 2025 a été **maîtrisé avec succès**. Grâce à la réactivité des alertes paramétrées dans notre SIEM Elastic, le comportement de type Ransomware a été stoppé avant le chiffrement complet des données.
À l'heure actuelle, la menace est considérée comme **éradiquée** : les IP malveillantes sont bannies et les postes infectés sont isolés. Bien que l'impact opérationnel ait été limité à quelques heures d'indisponibilité pour les postes ciblés, cet incident souligne la nécessité de durcir nos politiques d'accès externes.