Analyse préliminaire des workflows malicieux liés à l'attaque GhostAction

Bahloul Rami

12 septembre 2025

1 Introduction

L'objectif de ce travail de recherche est d'identifier et d'analyser les **workflows malicieux impliqués dans l'attaque GhostAction**, documentée par StepSecurity (GhostAction Campaign). L'article fournit des exemples de workflows exfiltrant des secrets GitHub, mais ne liste pas l'ensemble des workflows affectés. Cette recherche vise donc à récupérer des workflows suspects, à les analyser et à préparer les bases pour une simulation expérimentale sécurisée.

2 Méthodologie

2.1 Clonage et récupération des workflows

- Les dépôts GitHub associés à l'attaque ont été **clonés localement**.
- Les fichiers YAML des workflows ont été extraits et regroupés pour analyse.
- Les informations collectées incluent : nom du workflow, triggers, jobs, secrets utilisés, nombre de jobs et de secrets, indication de suspicion.

2.2 Organisation et visualisation des données

- Les données ont été importées dans un **DataFrame Pandas** pour comparer les workflows et identifier les jobs et secrets potentiellement malicieux.
- Les informations ont été **exportées en CSV** pour documentation et visualisation.

3 Workflows suspects identifiés

Fichier	Workflow
.github_gitflow_linters.yml	Linters
.github_workflows_nightly_build.yml	Nightly Build
.github_workflows_publish.yml	Publish
.github_workflows_release_nightly.yml	Langflow Nightly Build
main.yml	Daily Checks for appcodeEcomme
out_checkstyle_checkstyle_.github_workflows_diff_report.yml	DiffReport
out_sass_sass_.github_workflows_ci.yml	CI

Observations préliminaires : Les workflows identifiés sont suspects mais ne correspondent pas nécessairement aux workflows exacts mentionnés dans l'article. Les triggers sont souvent vides, nécessitant des vérifications supplémentaires.

4 Problèmes rencontrés

1. **Correspondance partielle :** Les workflows récupérés ne correspondent pas exactement aux workflows documentés par StepSecurity.
2. **Informations manquantes :** Certains fichiers YAML ne détaillent pas complètement les secrets ou triggers utilisés.
3. **Accès externe impossible :** Tentative d'accès à des API pour récupérer des workflows supplémentaires échouée.
4. **Sécurité des secrets :** Nécessité d'utiliser uniquement des secrets factices pour éviter toute fuite accidentelle.

5 Prochaine étape

La prochaine phase consistera à mettre en place un **environnement minimal réaliste** pour simuler l'exécution des workflows. Nous allons étudier les sept workflows suspects identifiés afin d'examiner leurs comportements et de comparer leur fonctionnement avec les problèmes documentés par StepSecurity. Pour cela, nous ferons des **hypothèses simplificatrices**, par exemple en simulant le workflow `CI` en utilisant des secrets factices, afin de comprendre comment un workflow pourrait exfiltrer des secrets. Cette étude et cette comparaison seront réalisées dans un **environnement isolé**, garantissant ainsi la sécurité et évitant toute fuite de données réelles.

6 Conclusion

Cette première étape a permis :

- D'identifier et documenter plusieurs workflows suspects.
- De structurer les données pour une analyse plus approfondie.
- De préparer les bases pour simuler les attaques dans un environnement sécurisé.

Ces travaux fournissent une base solide pour la suite de la recherche, avec un accent sur la sécurité et la reproductibilité.