Identifier et comprendre les requêtes DNS inhabituelles dans les rapports d'activité

Table des matières

Introduction

Ce document décrit la nature et les causes des requêtes DNS aléatoires qui peuvent apparaître dans les rapports d'activité et comment identifier leur origine.

Exemples de requêtes DNS aléatoires

Vous pouvez trouver des exemples de ces requêtes, qui apparaissent souvent comme des chaînes inhabituelles ou apparemment aléatoires :

```
iafkbge
nwvkqqojgx
uefakmvidzao
claeedov
cjkcmrh
cjemikolwaczyb
ccshpypwvddmro
cdsvmfjgvfcnbob
cegzaukxjexfrk
ceqmhxowbcys
cewigwgvfd
cexggxhwgt
```

Explication des requêtes DNS aléatoires

Tous les fournisseurs de services Internet ne respectent pas les règles RFC pour les réponses DNS. Ces requêtes DNS obscures visibles dans les rapports de recherche d'activité résultent de la méthode de Google Chrome d'envoyer des requêtes uniques pour protéger les utilisateurs finaux.

Pourquoi Ces Demandes Se Produisent-Elles ?

- Certains fournisseurs de services Internet répondent aux requêtes DNS pour les domaines inexistants avec un enregistrement A pointant vers une adresse appartenant au fournisseur. La page de renvoi qui en résulte affiche généralement des publicités et des messages tels que « Voulez-vous dire... ». Un aperçu de ce type de manipulation et des conséquences associées est expliqué dans cet article Wikipedia sur le piratage DNS.

- Selon les normes RFC, la réponse correcte pour une requête DNS à un domaine inexistant est NXDOMAIN. Étant donné que les publicités sont généralement indésirables, Google a développé une méthode pour tester ce comportement. Au démarrage, Chrome envoie 3 requêtes et vérifie pour voir quelle est la réponse. Si les domaines de test se résolvent au même enregistrement A au lieu de résoudre à NXDOMAIN, Chrome détecte ce comportement et masque les annonces de l'utilisateur final.

- Cette technique n’est pas la seule cause des requêtes DNS aléatoires, mais elle représente l’un des scénarios les plus courants.

Comment identifier Chrome comme la cause

- Recherchez des groupes de trois requêtes DNS inhabituelles envoyées à partir du même hôte interne. Ce modèle indique que Chrome génère les requêtes de test.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.