Identificar e entender consultas de DNS incomuns nos relatórios de atividades

Contents

Introdução

Este documento descreve a natureza e as causas das solicitações de DNS aleatório que podem aparecer em relatórios de atividades e como identificar sua origem.

Exemplos de solicitações de DNS aleatório

Você pode encontrar exemplos dessas solicitações, que frequentemente aparecem como strings incomuns ou aparentemente aleatórias:

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

Explicação de Solicitações DNS Aleatórias

Nem todos os provedores de serviços de Internet cumprem as regras de RFC para respostas DNS. Essas obscuras solicitações de DNS visíveis nos relatórios de pesquisa de atividades resultam do método do Google Chrome de enviar solicitações exclusivas para proteger os usuários finais.

Por que essas solicitações ocorrem?

- Alguns provedores de serviços de Internet respondem a consultas DNS para domínios não existentes com um registro A apontando para um endereço de propriedade do provedor. A página de destino resultante normalmente exibe anúncios e mensagens como "você quis dizer...". Uma visão geral desse tipo de manipulação e consequências associadas é explicada neste artigo da Wikipédia sobre o sequestro de DNS.

- De acordo com os padrões RFC, a resposta correta para uma solicitação DNS para um domínio não existente é NXDOMAIN. Como os anúncios são geralmente indesejados, o Google desenvolveu um método para testar esse comportamento. Na inicialização, o Chrome envia 3 solicitações e verifica qual é a resposta. Se os domínios de teste resolverem para o mesmo registro A em vez de resolverem para NXDOMAIN, o Chrome detecta esse comportamento e oculta anúncios do usuário final.

- Essa técnica não é a única causa para solicitações de DNS de aparência aleatória, mas representa um dos cenários mais comuns.

Como identificar o Chrome como a causa

- Procure grupos de três consultas incomuns de DNS enviadas do mesmo host interno. Este padrão indica que o Chrome está gerando as consultas de teste.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.