識別並理解活動報告中的異常DNS查詢

目錄

簡介

本文檔介紹活動報告中可能出現的隨機DNS請求的性質和原因，以及如何確定這些請求的來源。

隨機DNS請求示例

您可以找到這些請求的示例，這些請求通常顯示為不尋常或看似隨機的字串：

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

隨機DNS請求說明

並非所有網際網路服務提供商都遵守DNS響應的RFC規則。這些在活動搜尋報告中可見的模糊的DNS請求是Google Chrome為保護終端使用者傳送唯一請求的方法導致的。

為什麼會發生這些請求？

- 一些網際網路服務提供商響應不存在域的DNS查詢，其中A記錄指向提供商擁有的地址。生成的登入頁面通常顯示廣告和消息，例如「您是否……」。 有關DNS劫持的維基百科文章介紹了此類操作和相關後果的概述。

- 根據RFC標準，對不存在域的DNS請求的正確響應為NXDOMAIN。由於廣告通常是不需要的

，Google開發了一種方法來測試這種行為。啟動時，Chrome傳送3個請求並檢查響應內容。如果測試域解析為相同的A記錄，而不是解析為NXDOMAIN，Chrome會檢測此行為，並對終端使用者隱藏通告。

- 此技術不是造成隨機查詢DNS請求的唯一原因，但它代表了最常見的情況之一。

如何確定Chrome的原因

- 查詢從同一內部主機傳送的三個異常DNS查詢的組。此模式表示Chrome正在生成測試查詢。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。