Identifizieren und Verstehen ungewöhnlicher DNS-Abfragen in Aktivitätsberichten

Inhalt

Einleitung

In diesem Dokument werden die Art und die Ursachen von zufälligen DNS-Anfragen beschrieben, die in Aktivitätsberichten auftreten können, und es wird beschrieben, wie sie identifiziert werden können.

Beispiele für zufällige DNS-Anfragen

Beispiele für diese Anfragen, die oft als ungewöhnliche oder scheinbar zufällige Strings erscheinen, finden Sie hier:

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

Erläuterung von zufälligen DNS-Anfragen

Nicht alle Internetdienstanbieter halten sich an die RFC-Regeln für DNS-Antworten. Diese unklaren DNS-Anfragen, die in den Berichten zur Aktivitätssuche angezeigt werden, stammen aus der Methode von Google Chrome, eindeutige Anfragen zu senden, um die Endbenutzer zu schützen.

Warum treten diese Anfragen auf?

- Einige Internetdienstanbieter beantworten DNS-Abfragen für nicht vorhandene Domänen mit einem A-Eintrag, der auf eine Adresse im Besitz des Anbieters verweist. Auf der Landing Page werden in der Regel Werbeanzeigen und Meldungen wie "Was meinten Sie?" angezeigt. Ein Überblick über diese Art der Manipulation und die damit verbundenen Folgen wird in diesem Wikipedia-Artikel über DNS-Hijacking erklärt.

- Gemäß RFC-Standards ist die richtige Antwort für eine DNS-Anfrage an eine nicht vorhandene Domäne NXDOMAIN. Da Werbung in der Regel unerwünscht ist, hat Google eine Methode entwickelt, um dieses Verhalten zu testen. Beim Start sendet Chrome 3 Anfragen und überprüft, was die Antwort ist. Wenn die Test-Domänen zum gleichen A-Datensatz auflösen, anstatt zu NXDOMAIN aufzulösen, erkennt Chrome dieses Verhalten und blendet Werbung vor dem Endbenutzer aus.

- Diese Technik ist nicht die einzige Ursache für zufällig aussehende DNS-Anfragen, aber sie stellt eines der häufigsten Szenarien dar.

Wie Chrome als Ursache zu erkennen

- Suchen Sie nach Gruppen mit drei ungewöhnlichen DNS-Abfragen, die vom gleichen internen Host gesendet werden. Dieses Muster zeigt an, dass Chrome die Testabfragen generiert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.