Ongebruikelijke DNS-query's identificeren en begrijpen in activiteitenrapporten

Inhoud

Inleiding

Dit document beschrijft de aard en oorzaken van willekeurige DNS-verzoeken die in activiteitenrapporten kunnen worden weergegeven en hoe de oorsprong ervan kan worden geïdentificeerd.

Voorbeelden van willekeurige DNS-verzoeken

U kunt voorbeelden van deze verzoeken vinden, die vaak als ongewone of schijnbaar willekeurige tekenreeksen verschijnen:

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

Uitleg van willekeurige DNS-verzoeken

Niet alle internetproviders houden zich aan de RFC-regels voor DNS-reacties. Deze obscure DNS-verzoeken die zichtbaar zijn in Activity Search Reports zijn het resultaat van de methode van Google Chrome om unieke verzoeken te verzenden om eindgebruikers te beschermen.

Waarom komen deze verzoeken voor?

- Sommige internetproviders reageren op DNS-zoekopdrachten voor niet-bestaande domeinen met een A-record dat verwijst naar een adres dat eigendom is van een provider. De resulterende bestemmingspagina geeft meestal advertenties en berichten weer zoals "bedoelde u …". Een overzicht van dit soort manipulatie en bijbehorende gevolgen wordt uitgelegd in dit Wikipedia-artikel over DNS-kaping.

- Volgens de RFC-normen is NXDOMAIN het juiste antwoord voor een DNS-verzoek op een niet-bestaand domein. Omdat advertenties meestal ongewenst zijn, heeft Google een methode ontwikkeld om dit gedrag te testen. Bij het opstarten verzendt Chrome 3 verzoeken en controleert het wat het antwoord is. Als de testdomeinen dezelfde A-record opslaan in plaats van naar NXDOMAIN, detecteert Chrome dit gedrag en verbergt het advertenties voor de eindgebruiker.

- Deze techniek is niet de enige oorzaak voor willekeurig uitziende DNS-verzoeken, maar het vertegenwoordigt een van de meest voorkomende scenario's.

Hoe Chrome te identificeren als de oorzaak

- Zoek naar groepen van drie ongewone DNS-query's die van dezelfde interne host worden verzonden. Dit patroon geeft aan dat Chrome de testquery's genereert.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.