2019

Cloud Communication Case Study: App.carcollect.com

HENK-SJOERD HINRICHS, SANDER VAN DESSEL, MATHIAS VAN DE WATER

Inhoud

1. Inleiding

Anekdote vertelt door de ogen van Henk-Sjoerd: “Twee weken geleden was ik op het kantoor van het bedrijf Carcollect in Roosendaal (NL). Carcollect is een platform dat ervoor zorgt dat autohandelaren auto’s op een efficiënte en snelle manier kunnen kopen en verkopen. Iedereen was nog aan het werk op het moment dat ik binnenkwam. Een perfect moment voor mij om even een poortscan te doen op carcollect.com. Hierdoor kwam ik erachter dat poort 22 open stond, de secure shellpoort met als username root. Natuurlijk wist ik het wachtwoord niet, maar goed, misschien kon een brute force attack daar wel voor zorgen. Ik sprak met één van de developers erop aan. Al snel werd duidelijk dat carcollect.com niet de motor van het bedrijf was, dit bleek app.carcollect.com te zijn.

Ik voerde een ping request uit, en tot mijn verbazing kreeg ik bij elk ping request een ander IP-adres terug. Die maandag daarop vroeg ik meneer Portier naar de mogelijke oorzaak van dynamisch terugkrijgen van IP-adressen. Meneer Portier reageerde met het antwoord; “Dit lijkt mij een goede vraag voor een case study"”.

2. Verantwoording keuze case app.carcollect.com

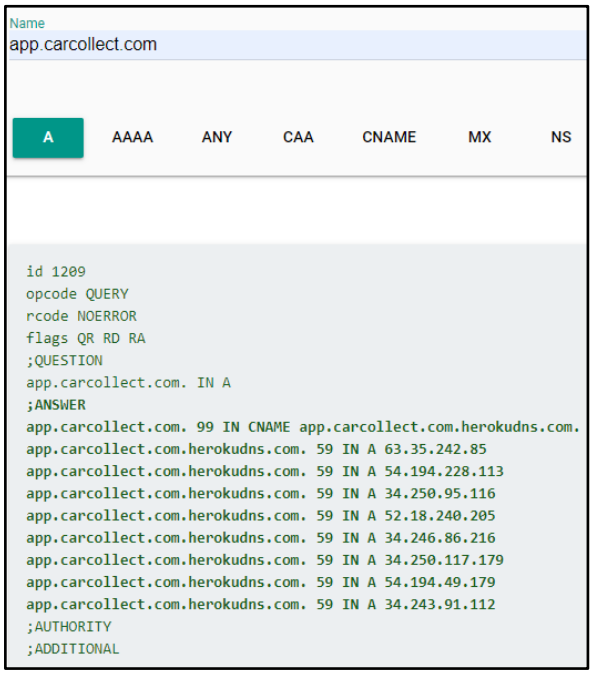
Vanuit een hackers perspectief is het belangrijk om erachter te komen hoe de infrastructuur van je potentiele target in elkaar zit. Op het moment dat je gaat uitzoeken hoe dingen in elkaar zitten begin je te begrijpen hoe het ook werkelijk in elkaar zit. Tijdens de reconnaissance fase willen we graag een profiel bouwen van onze target. DNS-enumeratie is een goede manier om informatie te verzamelen van onze target. Door een ping request uit te voeren naar onze target geeft dat ons een IP-adres terug. Dit IP-adres kunnen we in de scanning fase gebruiken om een poort scan op te doen. De ping requesten naar app.carcollect.com geven verschillende IP-adressen terug. Vanuit een hackers perspectief willen we eerst weten wat de reden is van de verschillende teruggekregen IP-adressen. Ten tweede willen we weten welke technologieën hierachter schuilgaan. Als laatste willen we weten wat de impact is van deze technologie voor ons onderzoek, en hoe we deze technologie mogelijk kunnen misbruiken.

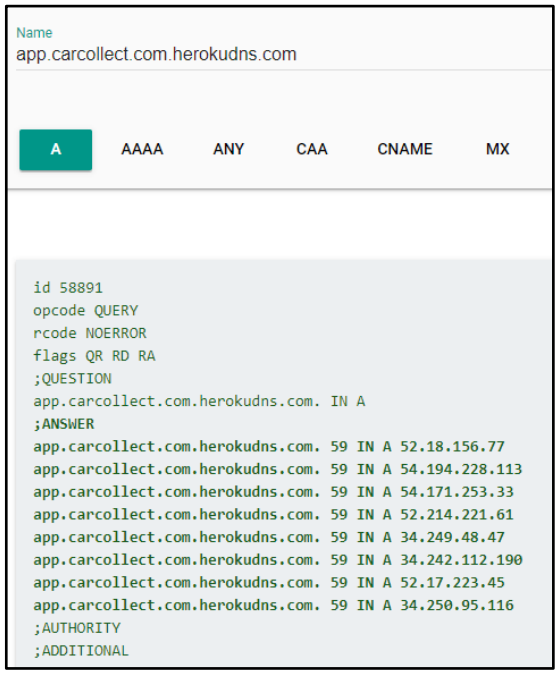
3. Vaststellingen omtrent app.carcollect.com

Als je het ping commando uitvoert via Windows cmd, dan kan je vaststellen dat het IP-adres van app.carcollect.com verscheidene keren veranderd. Ook krijgt de ping telkens een time-out (zie screenshot hieronder).

```
C:\Users\henks>ping app.carcollect.com

Pinging app.carcollect.com.herokudns.com [52.19.23.128] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 52.19.23.128:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\henks>ping app.carcollect.com.herokudns.com

Pinging app.carcollect.com.herokudns.com [34.242.94.16] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 34.242.94.16:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\henks>ping app.carcollect.com.herokudns.com

Pinging app.carcollect.com.herokudns.com [52.212.40.108] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 52.212.40.108:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Het rechtstreeks pingen naar de verkregen IP-adressen levert ook alleen maar time-outs op, ook al is de site bereikbaar via de webbrowser. Ook kan men vaststellen dat er achter app.carcollect.com een extra gedeelte komt, namelijk '.herokudns.com'. Als men dit adres pingt krijg je ook weer verschillende IP-adressen (indien je altijd hetzelfde krijgt is dit omdat de IP-adres nog gecached is. Open dan een nieuw terminal venster en voer de ping opnieuw uit.)





Wanneer je het domein opzoekt met behulp van DIG kom je verscheidene A-records uit: 8 bij app.carcollect.com, en 8 (waarvan 1 hetzelfde is) bij app.carcollect.com.herokudns.com.

Met het nslookup commando krijg je dezelfde IP-adressen als met het DIG commando. Een ping request via cmd zal een ICMP-pakket versturen en geeft een request time out. Als we de tool nping op Kali Linux gebruiken dan kunnen we een ping request specificeren en een tcp-pakket sturen. Dit levert wel een antwoord op.

```
root@kali:~# nping -c 1 --tcp app.carcollect.com

Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2019-12-03 13:38 EST
SENT (0.5687s) TCP 10.0.2.15:64533 > 54.194.228.113:80 S ttl=64 id=3030 iplen=40
  seq=4014568761 win=1480
RCVD (0.7672s) TCP 54.194.228.113:80 > 10.0.2.15:64533 SA ttl=64 id=6 iplen=44
seq=64001 win=65535 <mss 1460>

Max rtt: 197.503ms | Min rtt: 197.503ms | Avg rtt: 197.503ms
Raw packets sent: 1 (40B) | Rcvd: 1 (46B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.60 seconds
```

4. Wat/wie is Heroku?

Heroku is een Cloud-platform dat verscheidene programmeertalen ondersteund. Toepassingen die worden uitgevoerd op Heroku hebben meestal een uniek domein (meestal "applicatienaam.herokuapp.com") dat wordt gebruikt om HTTP-aanvragen naar de juiste dyno te routeren. Elk van de applicatiecontainers, of dynos, zijn verspreid over een "dyno-rooster" dat uit verschillende servers bestaat. De Git-server van Heroku verwerkt push-apps van toepassingen van toegestane gebruikers.

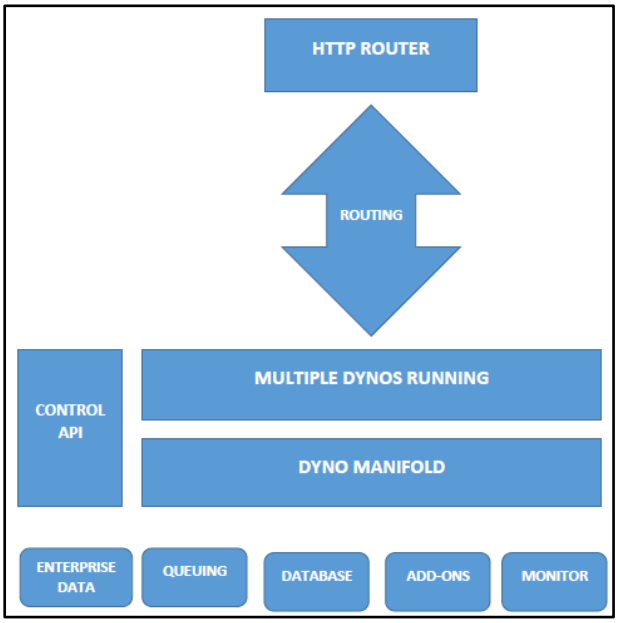
Alle Heroku-services worden gehost op het EC2 cloud computing-platform van Amazon. Hieronder is de uitkomt te zien van het traceroute commando naar app.carcollect.com. De ICMP-pakketten laten hier de route zien die wordt afgelegd naar de host. Als de ICMP-pakketten aankomen bij Amazon dan ontstaat er een request time out. Amazon maakt de ICMP-pakketten prioriteit loos of worden zelfs gedropped door Amazon.

```
C:\Users\henks>tracert app.carcollect.com

Tracing route to app.carcollect.com.herokudns.com [54.194.228.113]
over a maximum of 30 hops:

  1     7 ms     1 ms     1 ms  10.146.47.2
  2     3 ms     3 ms     2 ms  100.127.255.11
  3     1 ms     1 ms     1 ms  193.191.13.73
  4     4 ms     2 ms     4 ms  10.28.53.129
  5     6 ms     5 ms     5 ms  10.28.35.54
  6    20 ms    17 ms    18 ms  amazon-th2.par.franceix.net [37.49.236.118]
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
```

4.4.1 Het Heroku-platform

Het Heroku-netwerk draait de apps van de klant in virtuele containers die worden uitgevoerd in een betrouwbare runtime-omgeving. Heroku noemt deze containers 'Dynos'. Deze Dynos kunnen code uitvoeren die is geschreven in Node, Ruby, PHP, Go, Scala, Python, Java of Clojure. Heroku biedt ook aangepaste buildpacks waarmee de ontwikkelaar apps in elke andere taal kan implementeren. Met Heroku kan de ontwikkelaar de app direct schalen door het aantal dyno's te vergroten of door het type dyno te wijzigen waarin de app wordt uitgevoerd.

Diagram van het platform:



5. Waarom komt er extra gedeelte achter de URL?

hoe komt het dat de naam "app.carcollect.com" van naam verandert naar "app.carcollect.com.herokudns.com"?

Op het moment dat een persoon zijn domain aan Heroku koppelt, moet hij vervolgens zijn DNS provider laten verwijzen naar de DNS target van Heroku. Dit wordt gedaan door een nieuw CNAME record van je eigen DNS provider te verwijzen naar Heroku. In de volgende tabel kan je zien hoe dit kan opgebouwd worden.

Record	Name	Target
`CNAME`	`www`	`whispering-willow-5678.herokudns.com.`
`CNAME`	`othersubdomain`	`autumn-sunset-1495.herokudns.com.`
`CNAME`	`examplesecure`	`example-12345.ssl.herokudns.com.`

6. Waarom veranderen de IP's en wat is hier het nut van?

Uitleg welke technologie + nut

Omdat het Heroku-dyno-rooster dynamisch van aard is, is het IP-adres dat een bepaalde dyno in de loop van de tijd zal worden toegewezen zowel dynamisch als onvoorspelbaar. Deze dynamische sourcing van uitgaand verkeer kan het moeilijk maken om te integreren met API's of verbindingen te maken via firewalls die op IP gebaseerde whitelisting vereisen.

Proximo overwint deze beperking door een bekend, statisch IP-adres en een tunnel te bieden waardoor uw app uitgaand verkeer kan verzenden, zodat het altijd afkomstig is van uw toegewezen IP. U kunt dit IP-adres vervolgens aan een API-partner verstrekken of gebruiken

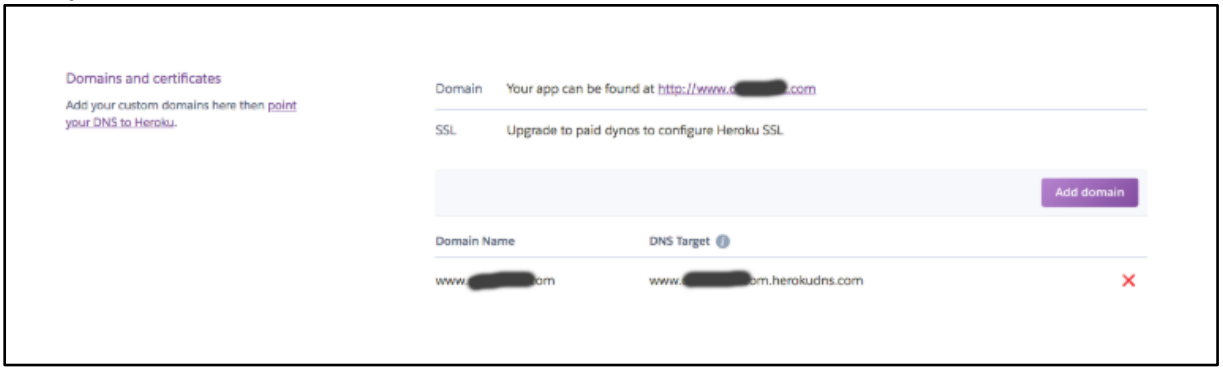
om de basis te vormen van inkomende firewallregels om verbinding te maken met een beschermde bron, zoals een interne API of database.

7. Hoe implementeer je deze methode?

Neem de volgende stappen als voorbeeld:

1 - Ga naar https://dashboard.heroku.com
2 - Klik op je app naam en ga naar Settings
3 - Vervolgens klik je op add domain
4 - Add domain en klik opslaan

Daarna kan je zien dat je domain met het DNS target is toegevoegd.
www.jouwdomain.com.herokudns.com



5 - Nu voegen we de bovenstaande gecreëerde DNS target www.jouwdomain.com.herokudns.com aan je eigen DNS CName record in het dashboard paneel.

6 - Nu kan je in de Heroku CLI in je terminal de volgende commando's uitvoeren.

```
heroku login
host www.yourdomain.com
```

7 - Als laatste stap voegen we het domain toe.

```
// Below command will enqueue your domain for addition
heroku domains:add www.yourdomain.com

// Below command will keep waiting and result in success once the
domain is added
heroku domains:wait 'yourdomain.com' // this command
```

8. Conclusie

De voornaamste reden van de dynamische IP-adressen is vanwege het Heroku-dyno-rooster die dynamisch van aard is. Heroku is cloud-based, platform-as-service (PaaS) product. Heroku is een container gebaseerd systeem voor het bouwen, runnen en managen van moderne apps. In een container omgeving is niks statisch, de configuratie veranderd constant en container word gaan up en down.

Waarom kiest Carcollect voor Heroku?

Onze hypothese is dat dit vooral vanuit het developers perspectief een geschikte keuze is geweest omdat, Heroku ervoor kan zorgen dat je apps snel bouwt en deployed. Het is een polygrot platform wat inhoudt dat het flexibel is naar jouw devolopment stijl. Het is schaalbaal, en goed combineerbaar met verschillende cloud services.