





- Exfiltration: Use DNS tunneling for mock data: verify.

```
root@kali:~# tcpdump -i eth0 port 53 -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:03:44.853218 IP 192.168.0.170.49396 > 103.62.236.84.53: 53551+ A? update.googleapis.com. (39)
19:03:44.857447 IP 103.62.236.84.53 > 192.168.0.170.49396: 53551 1/0/0 A 142.250.182.99 (55)
19:05:37.576022 IP 192.168.0.170.49463 > 103.62.236.84.53: 41890+ A? service.weather.microsoft.com. (47)
19:05:37.581112 IP 103.62.236.84.53 > 192.168.0.170.49463: 41890 3/0/0 CNAME wildcard.weather.microsoft.com.edgekey.net., CNAME a15275.d.akamaiedge.net., A 104.108.246.65 (156)
19:05:37.627570 IP 192.168.0.170.52054 > 103.62.236.84.53: 44287+ A? foodanddrink.tile.apex.bing.com. (50)
19:05:37.657859 IP 103.62.236.84.53 > 192.168.0.170.52054: 44287 NXDomain 0/1/0 (148)
19:05:38.565515 IP 192.168.0.170.60286 > 103.62.236.84.53: 7248+ A? en-us.apex-ef.msn.com. (48)
19:05:38.563793 IP 192.168.0.170.60311 > 103.62.236.84.53: 54467+ A? finance.services.apex.bing.com. (49)
19:05:38.591794 IP 103.62.236.84.53 > 192.168.0.170.60311: 7249 3/0/0 CNAME www.msn.com.a-0003.a-msedge.net., CNAME a-0003.a-msedge.net., A 204.79.197.203 (115)
19:05:38.591795 IP 103.62.236.84.53 > 192.168.0.170.60311: 54467 3/0/0 CNAME finance.services.apex.bing.com.edgekey.net., CNAME e5112.g.akamaiedge.net., A 23.203.194.163 (158)
19:08:23.645222 IP 192.168.0.170.59144 > 103.62.236.84.53: 62673+ A? clientservices.googleapis.com. (47)
19:08:23.646192 IP 192.168.0.170.52524 > 103.62.236.84.53: 38749+ HTTPS? clientservices.googleapis.com. (47)
19:08:23.651769 IP 103.62.236.84.53 > 192.168.0.170.59144: 62673 1/0/0 A 142.250.183.227 (63)
19:08:23.653737 IP 103.62.236.84.53 > 192.168.0.170.52524: 38749 0/1/0 (107)
19:08:23.656739 IP 192.168.0.170.53490 > 103.62.236.84.53: 6543+ A? www.google.com. (32)
19:08:23.657772 IP 192.168.0.170.60294 > 103.62.236.84.53: 61020+ HTTPS? www.google.com. (32)
19:08:23.658486 IP 192.168.0.170.52015 > 103.62.236.84.53: 25620+ A? accounts.google.com. (37)
19:08:23.658673 IP 192.168.0.170.62488 > 103.62.236.84.53: 52763+ HTTPS? accounts.google.com. (37)
19:08:23.661291 IP 103.62.236.84.53 > 192.168.0.170.53490: 6543 1/0/0 A 142.250.193.132 (48)
19:08:23.661909 IP 103.62.236.84.53 > 192.168.0.170.60294: 61920 1/0/0 HTTPS (57)
19:08:23.663006 IP 103.62.236.84.53 > 192.168.0.170.52015: 25620 1/0/0 A 74.125.130.84 (53)
19:08:23.663557 IP 103.62.236.84.53 > 192.168.0.170.62488: 52763 0/1/0 (87)
19:08:24.344670 IP 192.168.0.170.08059 > 103.62.236.84.53: 35309+ A? www.gstatic.com. (33)
19:08:24.345210 IP 192.168.0.170.54173 > 103.62.236.84.53: 1888+ HTTPS? www.gstatic.com. (33)
19:08:24.348530 IP 103.62.236.84.53 > 192.168.0.170.08059: 35309 1/0/0 A 142.250.77.227 (49)
19:08:24.350197 IP 103.62.236.84.53 > 192.168.0.170.54173: 1888 0/1/0 (93)
19:08:24.563089 IP 192.168.0.170.50850 > 103.62.236.84.53: 8360+ A? ogads-pa.clients6.google.com. (46)
19:08:24.563769 IP 192.168.0.170.58887 > 103.62.236.84.53: 50829+ HTTPS? ogads-pa.clients6.google.com. (46)
19:08:24.566511 IP 103.62.236.84.53 > 192.168.0.170.50850: 8360 1/0/0 A 142.250.193.106 (62)
19:08:24.568195 IP 103.62.236.84.53 > 192.168.0.170.58887: 50829 0/1/0 (106)
19:08:24.687076 IP 192.168.0.170.62086 > 103.62.236.84.53: 47905+ A? apis.google.com. (33)
19:08:24.687435 IP 192.168.0.170.50465 > 103.62.236.84.53: 17929+ HTTPS? apis.google.com. (33)
19:08:24.610894 IP 103.62.236.84.53 > 192.168.0.170.62086: 47905 2/0/0 CNAME plus.l.google.com., A 142.250.193.142 (80)
19:08:24.610840 IP 103.62.236.84.53 > 192.168.0.170.50465: 17929 1/1/0 CNAME plus.l.google.com. (114)
19:08:25.544868 IP 192.168.0.170.57737 > 103.62.236.84.53: 39020+ A? play.google.com. (33)
19:08:25.545877 IP 192.168.0.170.57281 > 103.62.236.84.53: 50160+ HTTPS? play.google.com. (33)
19:08:25.549369 IP 103.62.236.84.53 > 192.168.0.170.57737: 39829 1/0/0 A 142.250.182.174 (49)
19:08:25.550076 IP 103.62.236.84.53 > 192.168.0.170.57281: 50160 0/1/0 (83)
19:08:25.778473 IP 192.168.0.170.52414 > 103.62.236.84.53: 63007+ A? update.googleapis.com. (39)
19:08:25.778918 IP 192.168.0.170.56887 > 103.62.236.84.53: 44535+ HTTPS? update.googleapis.com. (39)
19:08:25.781086 IP 103.62.236.84.53 > 192.168.0.170.52414: 63007 1/0/0 A 142.250.182.99 (55)
19:08:25.783957 IP 103.62.236.84.53 > 192.168.0.170.56887: 44535 0/1/0 (99)
19:08:28.811908 IP 192.168.0.170.54144 > 103.62.236.84.53: 24384+ A? chatgpt.com. (29)
19:08:28.818228 IP 192.168.0.170.53515 > 103.62.236.84.53: 9189+ HTTPS? chatgpt.com. (29)
19:08:28.838251 IP 103.62.236.84.53 > 192.168.0.170.54144: 24384 2/0/0 A 172.64.155.209, A 104.18.32.47 (61)
19:08:28.838255 IP 103.62.236.84.53 > 192.168.0.170.53515: 9189 0/1/0 (107)
19:08:29.315069 IP 192.168.0.170.51726 > 103.62.236.84.53: 14384+ A? cdn.oaistatic.com. (35)
```