I know what you did™

DNS resolver hijack tester

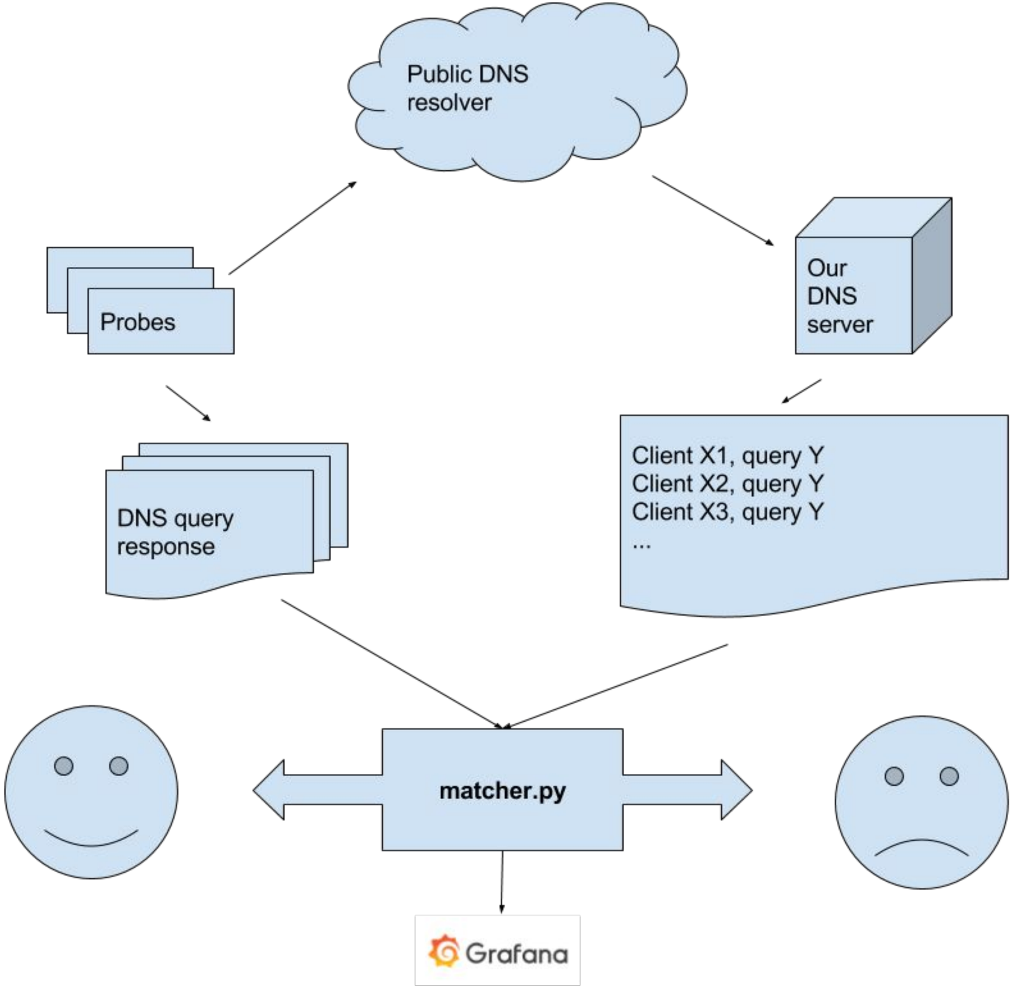
Blu-ray Disc
I KNOW WHAT YOU DID LAST SUMMER
"More laughs and chills than SCREAM."
EXPERIENCE HIGH DEFINITION

Some context...

Ingredients: Pork with Ham, Salt, Water, Modified Potato Starch, Sugar, Sodium Nitrite
SPAM®
Classic
U.S. INSPECTED AND PASSED BY DEPARTMENT OF AGRICULTURE
Serving Suggestion
NET WT 12 OZ (340g)

GENERICCOMPANY

Idea


Public DNS resolver
Probes
Our DNS server
DNS query response
Client X1, query Y
Client X2, query Y
Client X3, query Y
...
matcher.py
Grafana

First iteration

- 1 Probe using @8.8.8.8 as resolver
- Results:
    - query arrived to the DNS server via ASN 15169, good!

Second iteration

- 100 Probes using @8.8.8.8 as resolver
- Results:
    - All* queries arrived to the DNS server via ASN 15169, good!

How do we test this?

DNS Fingerprint to the rescue!

BAD-PROBES.txt

-90 probe IDs with a fingerprint that indicates some kind of DNS hijacking/weird behavior

-tested with our setup (54 responses), 48 DNS queries were marked with DNS hijacking/weird behavior

Lets go big...

9500 probes!

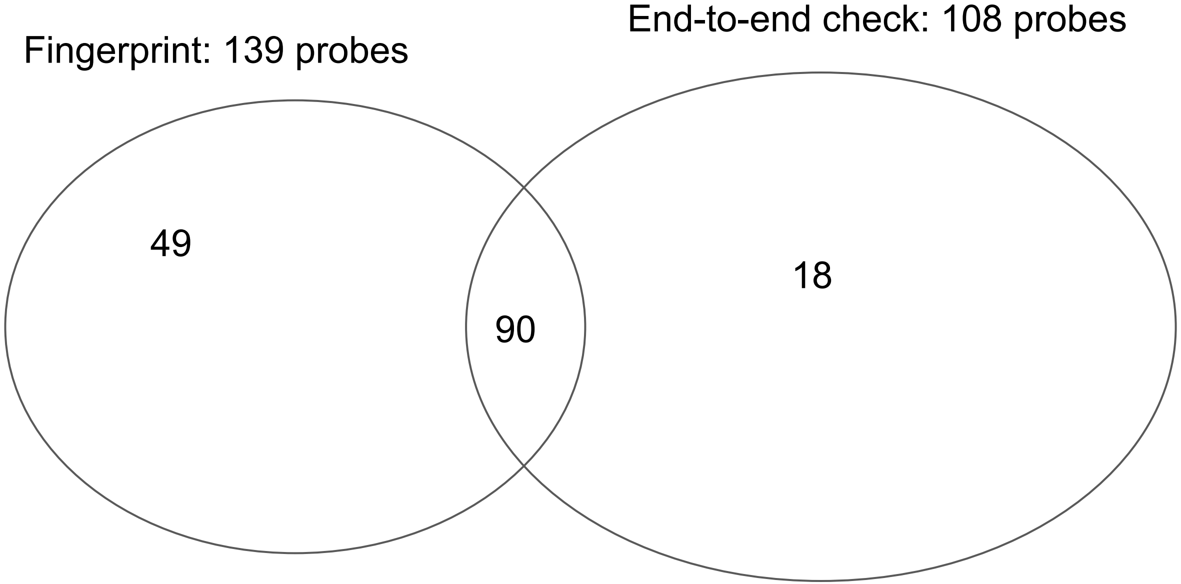
-using @8.8.8.8 as DNS resolver

-got response from aprox 6700 probes

-113 DNS queries were marked with DNS hijacking/weird behavior

Working together

Comparing with Fingerprint results



End-to-end check: 108 probes

Fingerprint: 139 probes

49

90

18

Advantage of Active Method

- Hard to block
  - Queries are completely normal
  - Auth zone for active monitoring is simple to setup
- No reliance on server implementation or features
- Flexible. Easy to extend beyond matching only the DNS query source address

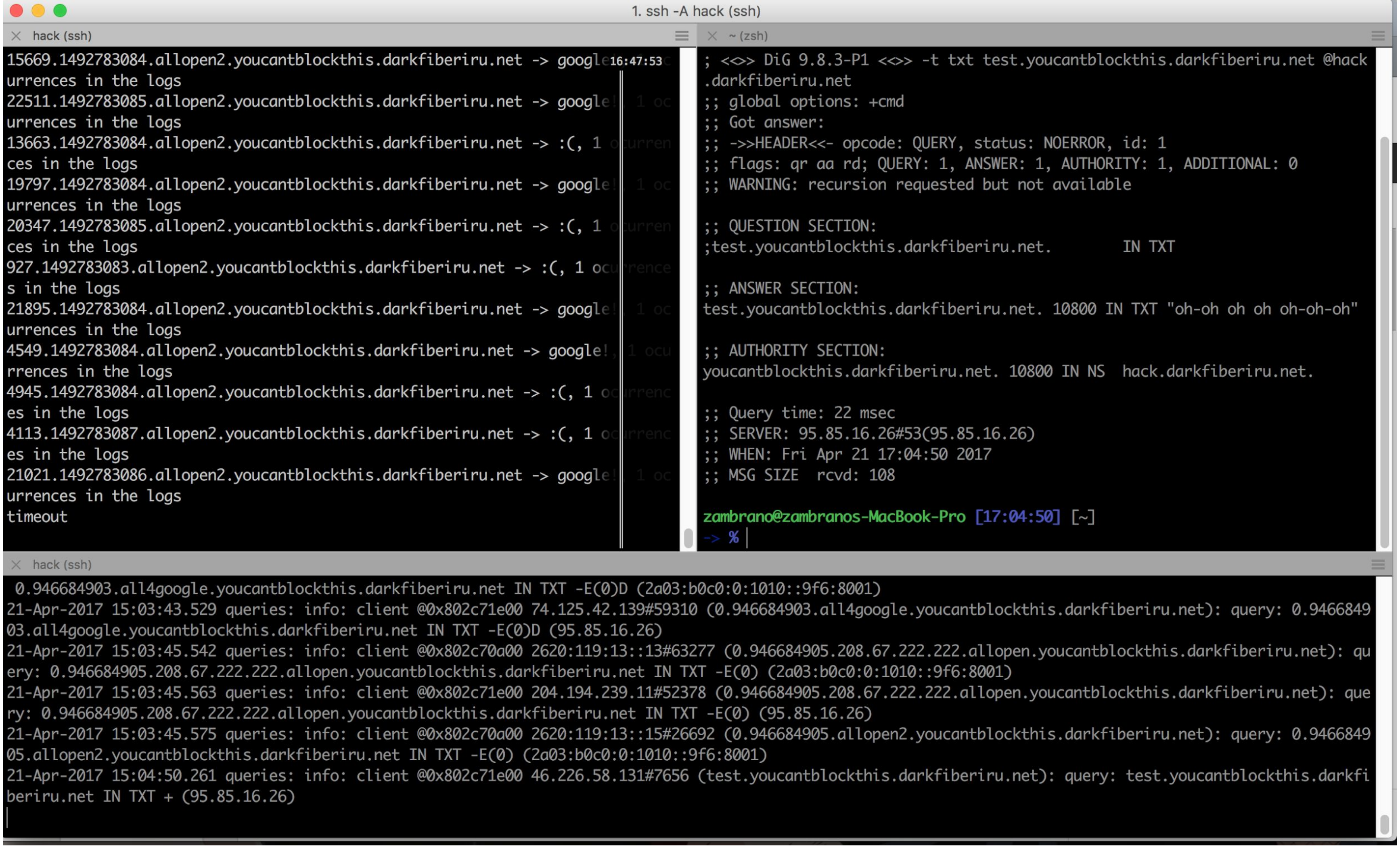
Disadvantages

- Can’t see situation where MITM forwards traffic onto Resolver afterward
    - Unless dns requests get duplicated
- Don’t know what are the consequences of these DNS changes, we just know that It is not common behaviour.

Possible Future Work

- Group “bad probes” into related types
- Crunch data for geographic percentages of “bad probes”
- Adapt to run the test from Laptop or phone at regular intervals to see if you are affected (instead of the RIPE atlas probes)
- Crunch data via grafana (already compatible)

https://github.com/bigzaqui/ripe-hackaton-apr-2017/



```
15669.1492783084.allopen2.youcantblockthis.darkfiberiru.net -> googl16:47:53c
urrences in the logs
22511.1492783085.allopen2.youcantblockthis.darkfiberiru.net -> google!, 1 oc
urrences in the logs
13663.1492783084.allopen2.youcantblockthis.darkfiberiru.net -> :(, 1 ocurren
ces in the logs
19797.1492783084.allopen2.youcantblockthis.darkfiberiru.net -> google!, 1 oc
urrences in the logs
20347.1492783085.allopen2.youcantblockthis.darkfiberiru.net -> :(, 1 ocurren
ces in the logs
927.1492783083.allopen2.youcantblockthis.darkfiberiru.net -> :(, 1 ocurrence
s in the logs
21895.1492783084.allopen2.youcantblockthis.darkfiberiru.net -> google!, 1 oc
urrences in the logs
4549.1492783084.allopen2.youcantblockthis.darkfiberiru.net -> google!, 1 ocu
rrences in the logs
4945.1492783084.allopen2.youcantblockthis.darkfiberiru.net -> :(, 1 ocurrenc
es in the logs
4113.1492783087.allopen2.youcantblockthis.darkfiberiru.net -> :(, 1 ocurrenc
es in the logs
21021.1492783086.allopen2.youcantblockthis.darkfiberiru.net -> google!, 1 oc
urrences in the logs
timeout
```

```
; <<>> DiG 9.8.3-P1 <<>> -t txt test.youcantblockthis.darkfiberiru.net @hack
.darkfiberiru.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;test.youcantblockthis.darkfiberiru.net.        IN TXT

;; ANSWER SECTION:
test.youcantblockthis.darkfiberiru.net. 10800 IN TXT "oh-oh oh oh oh-oh-oh"

;; AUTHORITY SECTION:
youcantblockthis.darkfiberiru.net. 10800 IN NS  hack.darkfiberiru.net.

;; Query time: 22 msec
;; SERVER: 95.85.16.26#53(95.85.16.26)
;; WHEN: Fri Apr 21 17:04:50 2017
;; MSG SIZE  rcvd: 108

zambrano@zambranos-MacBook-Pro [17:04:50] [~]
-> %
```

```
 0.946684903.all4google.youcantblockthis.darkfiberiru.net IN TXT -E(0)D (2a03:b0c0:0:1010::9f6:8001)
21-Apr-2017 15:03:43.529 queries: info: client @0x802c71e00 74.125.42.139#59310 (0.946684903.all4google.youcantblockthis.darkfiberiru.net): query: 0.9466849
03.all4google.youcantblockthis.darkfiberiru.net IN TXT -E(0)D (95.85.16.26)
21-Apr-2017 15:03:45.542 queries: info: client @0x802c70a00 2620:119:13::13#63277 (0.946684905.208.67.222.222.allopen.youcantblockthis.darkfiberiru.net): qu
ery: 0.946684905.208.67.222.222.allopen.youcantblockthis.darkfiberiru.net IN TXT -E(0) (2a03:b0c0:0:1010::9f6:8001)
21-Apr-2017 15:03:45.563 queries: info: client @0x802c71e00 204.194.239.11#52378 (0.946684905.208.67.222.222.allopen.youcantblockthis.darkfiberiru.net): que
ry: 0.946684905.208.67.222.222.allopen.youcantblockthis.darkfiberiru.net IN TXT -E(0) (95.85.16.26)
21-Apr-2017 15:03:45.575 queries: info: client @0x802c70a00 2620:119:13::15#26692 (0.946684905.allopen2.youcantblockthis.darkfiberiru.net): query: 0.9466849
05.allopen2.youcantblockthis.darkfiberiru.net IN TXT -E(0) (2a03:b0c0:0:1010::9f6:8001)
21-Apr-2017 15:04:50.261 queries: info: client @0x802c71e00 46.226.58.131#7656 (test.youcantblockthis.darkfiberiru.net): query: test.youcantblockthis.darkfi
beriru.net IN TXT + (95.85.16.26)
```