

Measuring and Detecting Fast-Flux Service Networks

Thorsten Holz

Christian Gorecki

Konrad Rieck

Felix C. Freiling

High availability

Hardware failures

DDoS

Take-downs

Round-robin DNS

```
$ dig google.com
```

```
;; ANSWER SECTION:
```

google.com.	3600	IN	A	74.125.224.20
google.com.	3600	IN	A	74.125.224.16
google.com.	3600	IN	A	74.125.224.18
google.com.	3600	IN	A	74.125.224.19
google.com.	3600	IN	A	74.125.224.17

Content distribution networks

```
$ dig images.apple.com
```

```
;; ANSWER SECTION:
```

```
images.apple.com. 3597 IN CNAME i.a.c.edgesuite.net.
```

```
i.a.c.edgesuite.net. 21597 IN CNAME i.a.c.e.n.redir.akadns.net.
```

```
i.a.c.e.n.redir.akadns.net. 2904 IN CNAME a199.gi3.akamai.net.
```

```
a199.gi3.akamai.net. 18 IN A 96.17.8.162
```

```
a199.gi3.akamai.net. 18 IN A 96.17.8.154
```

Content distribution networks

```
$ dig images.apple.com
```

```
;; ANSWER SECTION:
```

```
images.apple.com. 3597 IN CNAME i.a.c.edgesuite.net.
```

```
i.a.c.edgesuite.net. 21597 IN CNAME i.a.c.e.n.redir.akadns.net.
```

```
i.a.c.e.n.redir.akadns.net. 2904 IN CNAME a199.gi3.akamai.net.
```

```
a199.gi3.akamai.net. 18 IN A 72.246.30.74
```

```
a199.gi3.akamai.net. 18 IN A 72.246.30.25
```

Fast-flux

```
$ dig thearmynext.info
```

```
;; ANSWER SECTION:
```

flux agents

```
thearmynext.info. 600 IN A 69.183.26.53
```

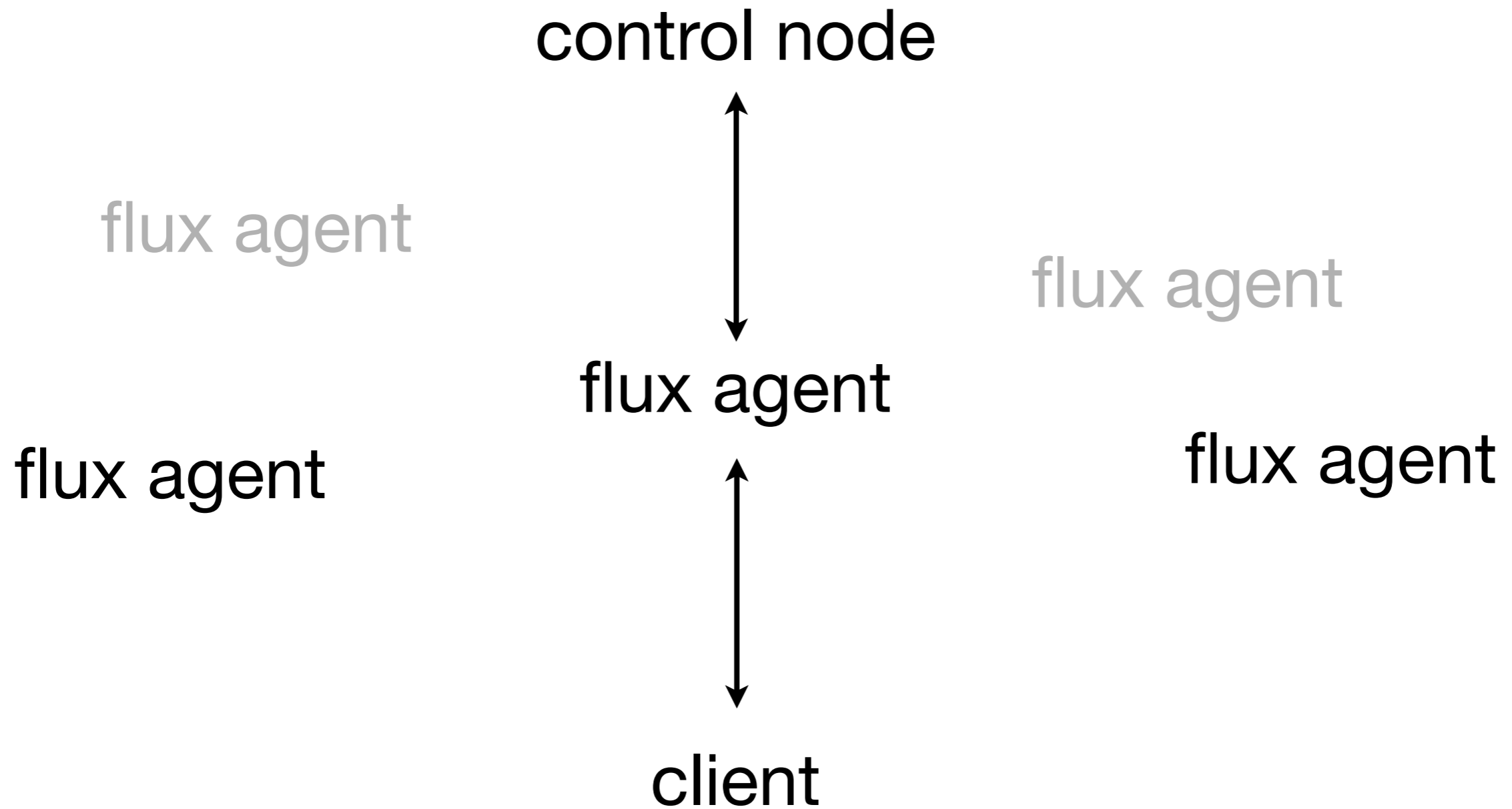
```
thearmynext.info. 600 IN A 76.205.234.131
```

```
thearmynext.info. 600 IN A 85.177.96.105
```

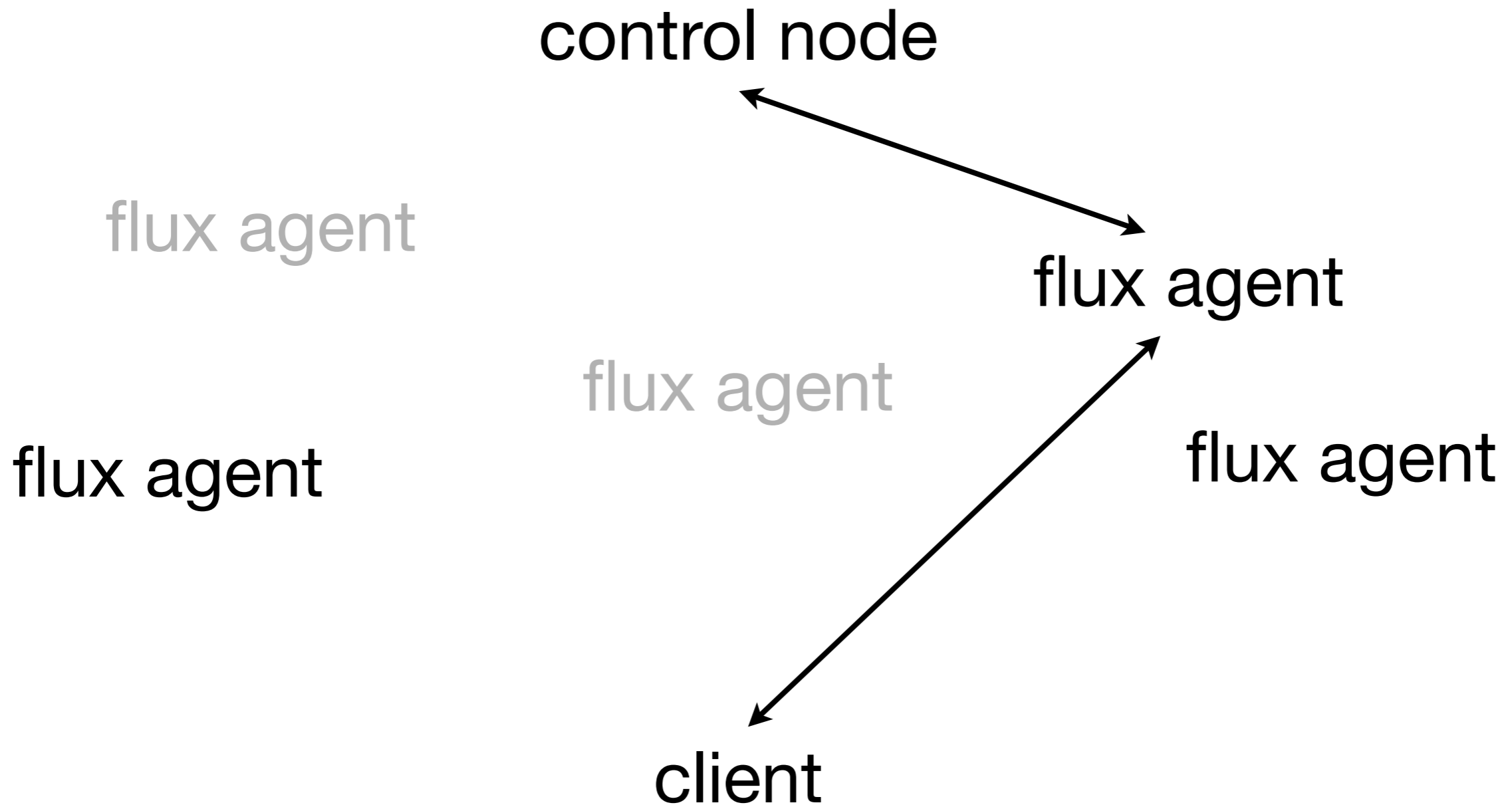
```
thearmynext.info. 600 IN A 217.129.178.138
```

```
thearmynext.info. 600 IN A 24.98.252.230
```

Fast-flux



Fast-flux



Characteristics

Diverse IP addresses

No physical agent control

(no guaranteed uptime)

Distinguishing parameters

n_A = number of all unique A records

n_{NS} = number of name server records

n_{ASN} = number of unique ASNs for A records

Flux score

$$x = (n_A, n_{ASN}, n_{NS})$$

$$F(x) = w^T x - b$$

$$F(x) > 0 \text{ if } x \text{ is a fast-flux domain}$$

$$F(x) \leq 0 \text{ if } x \text{ is a benign domain}$$

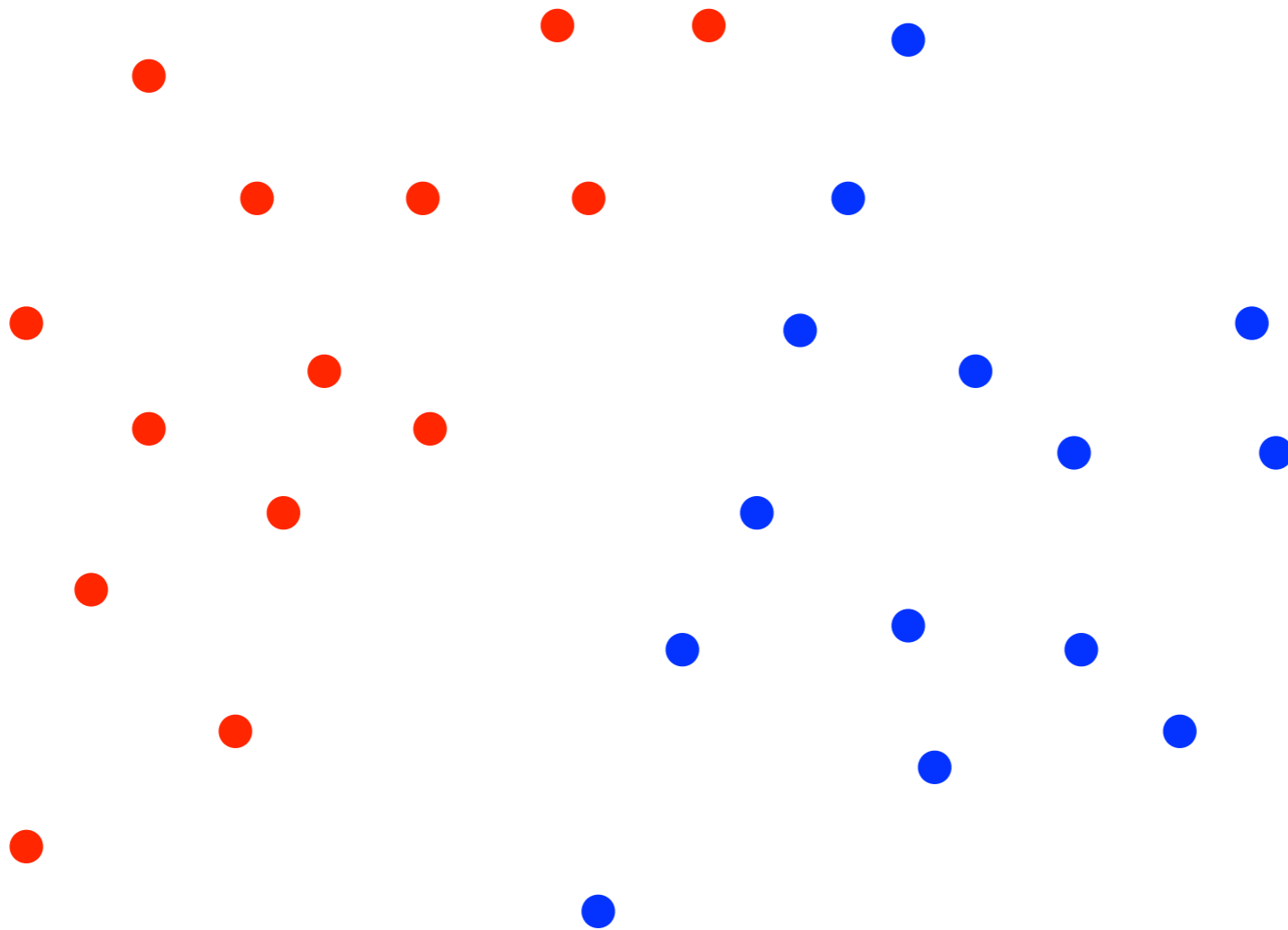
Computing w

128 fast-flux and 5,803 benign domains

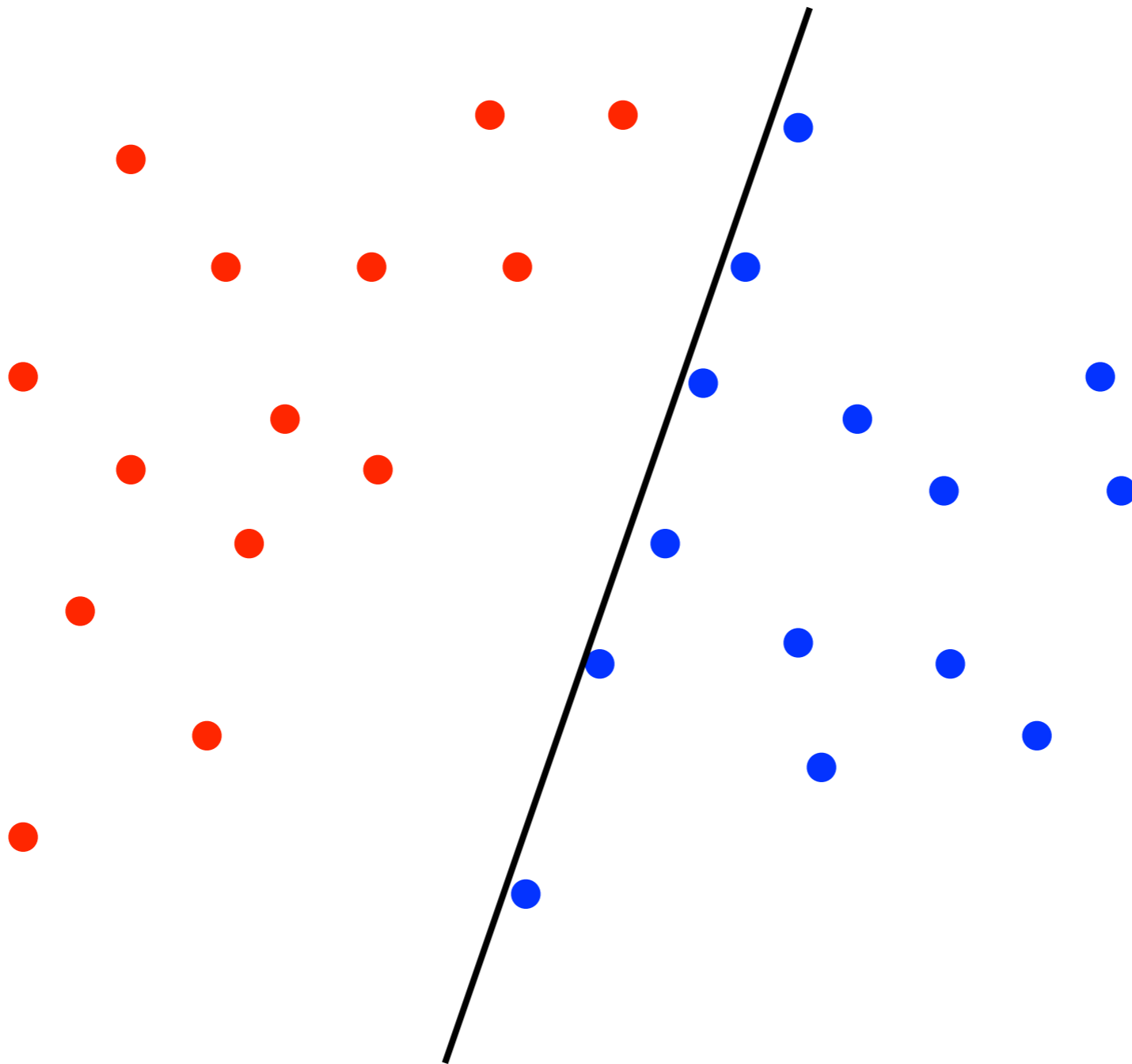
Perform pairs of DNS lookups, TTL apart, to measure n_A , n_{NS} , n_{ASN}

Compute “optimal hyperplane”

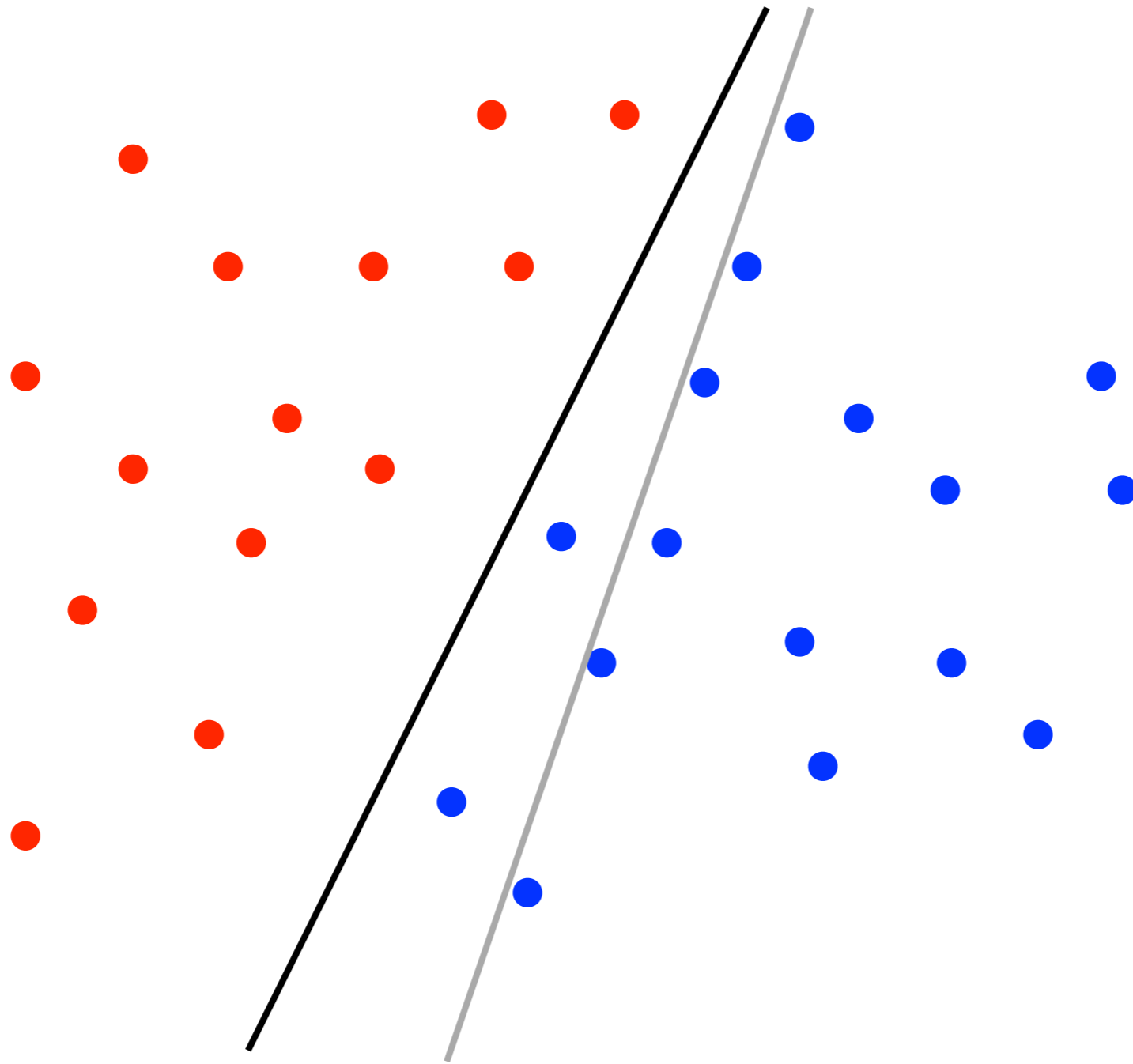
Computing \mathcal{W}



Computing w



Computing w



Computing w

10-fold cross-validation

9/10 of data for training, 1/10 for testing

“The best model achieves an average detection accuracy of 99.98% with a standard deviation of 0.05%”

$$w = (1.32, 18.54, 0)$$

$$b = 142.38$$

Scam web sites

22,264 spam e-mails (August 2007)

7,389 unique domains

2,197 fast-flux domains (21.7%)

563 unique fast-flux domains

Long-term measurements

33 fast-flux domains

DNS lookup per 300 seconds, for 7 weeks

(July 24th to September 10th 2007)

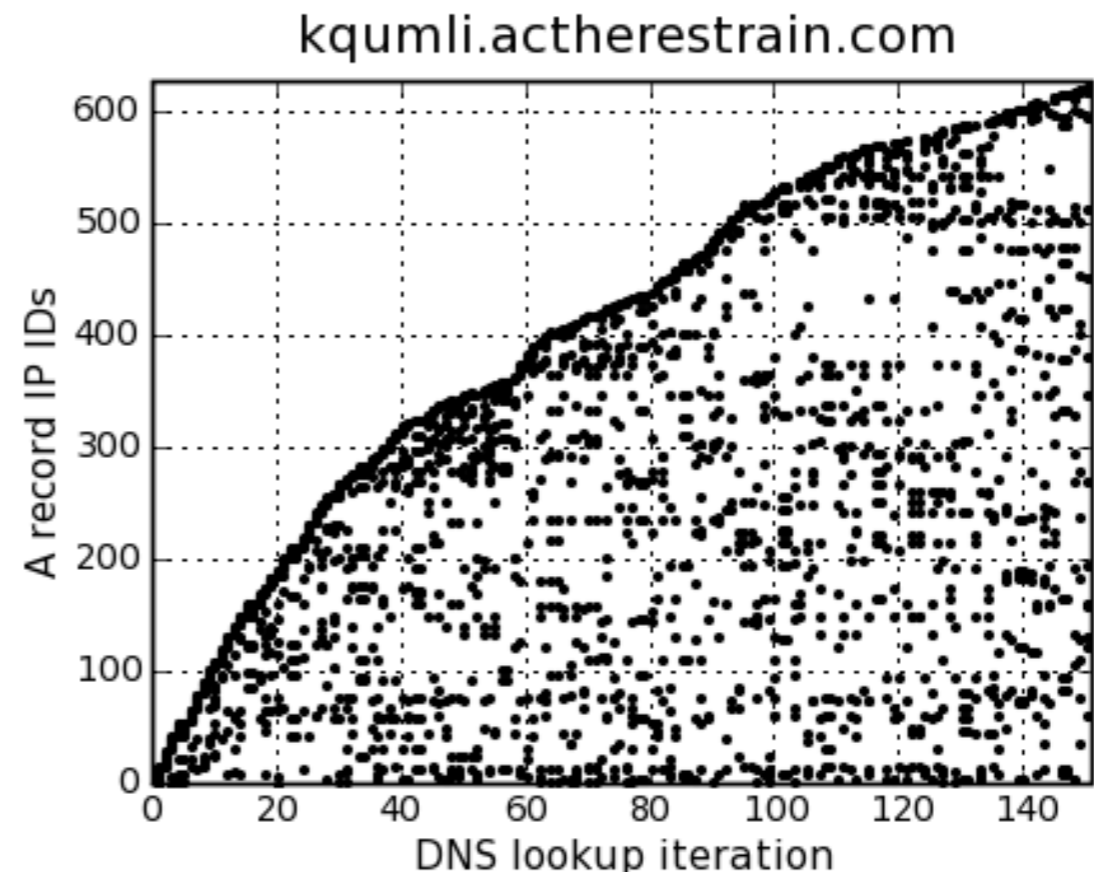
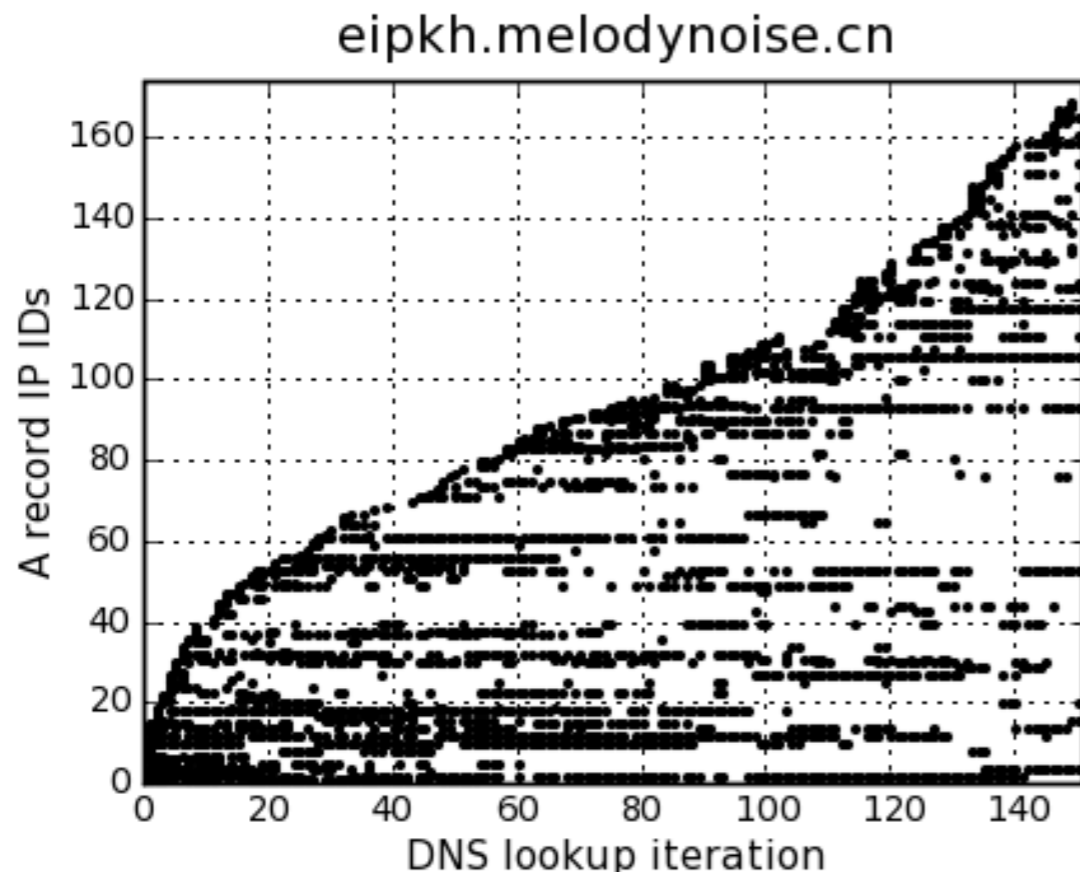
Long-term measurements

18,214 unique IP addresses

818 unique ASNs

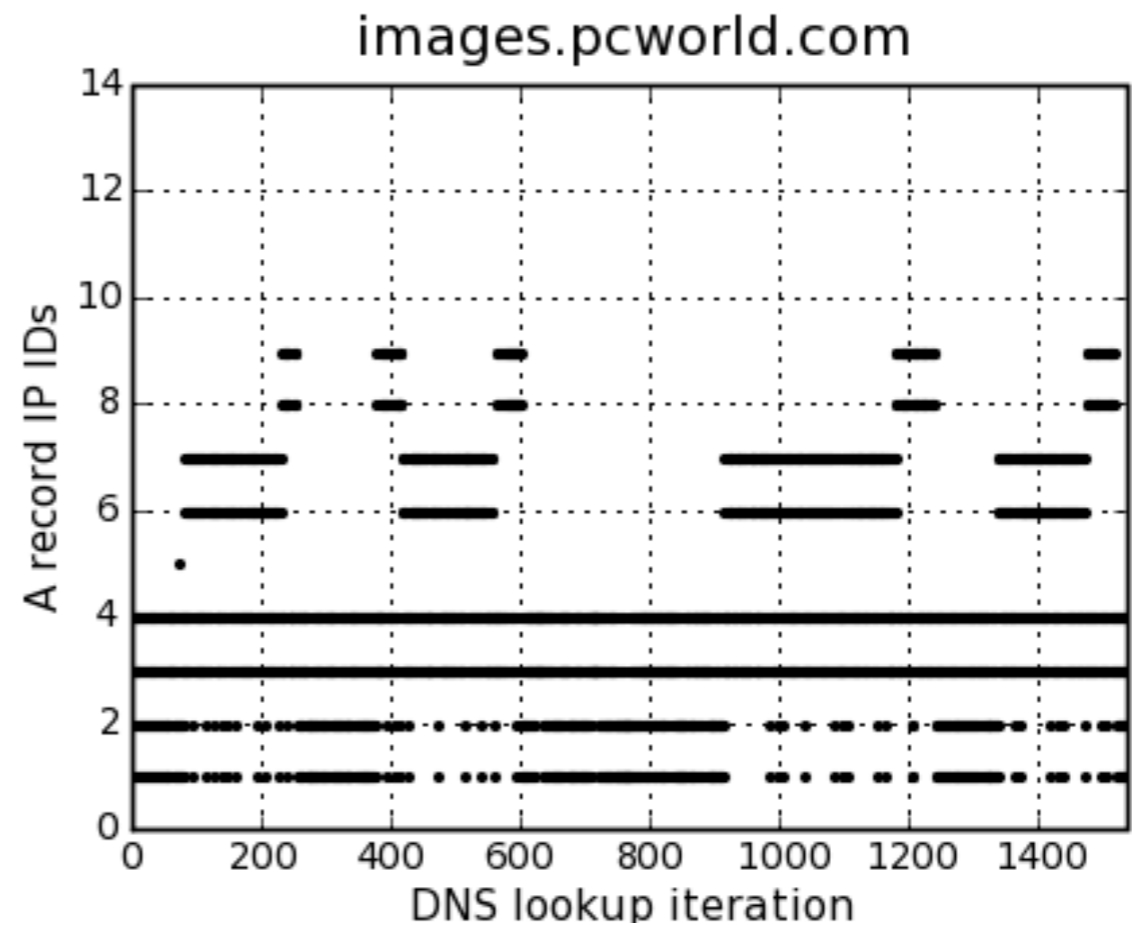
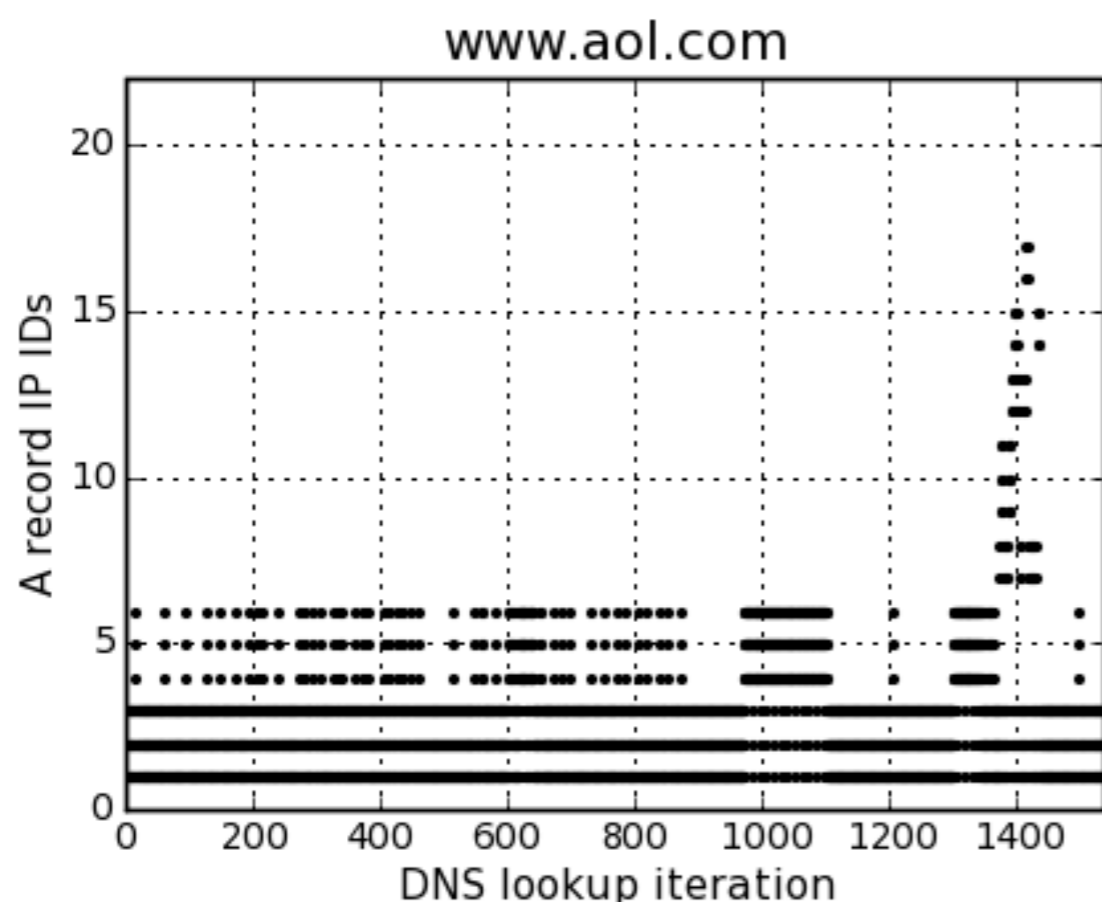
Long tail — 43.3% of IPs in top 10 ASNs

Long-term measurements



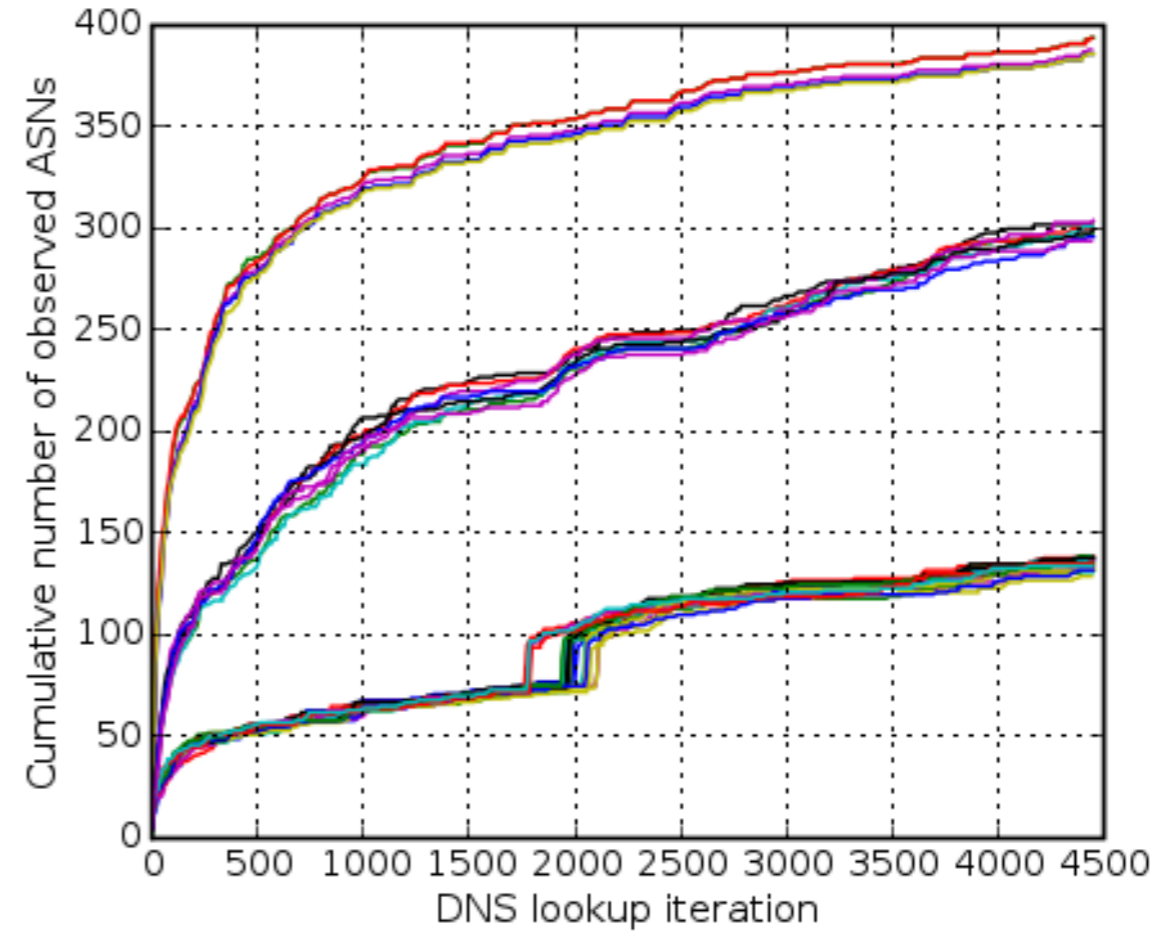
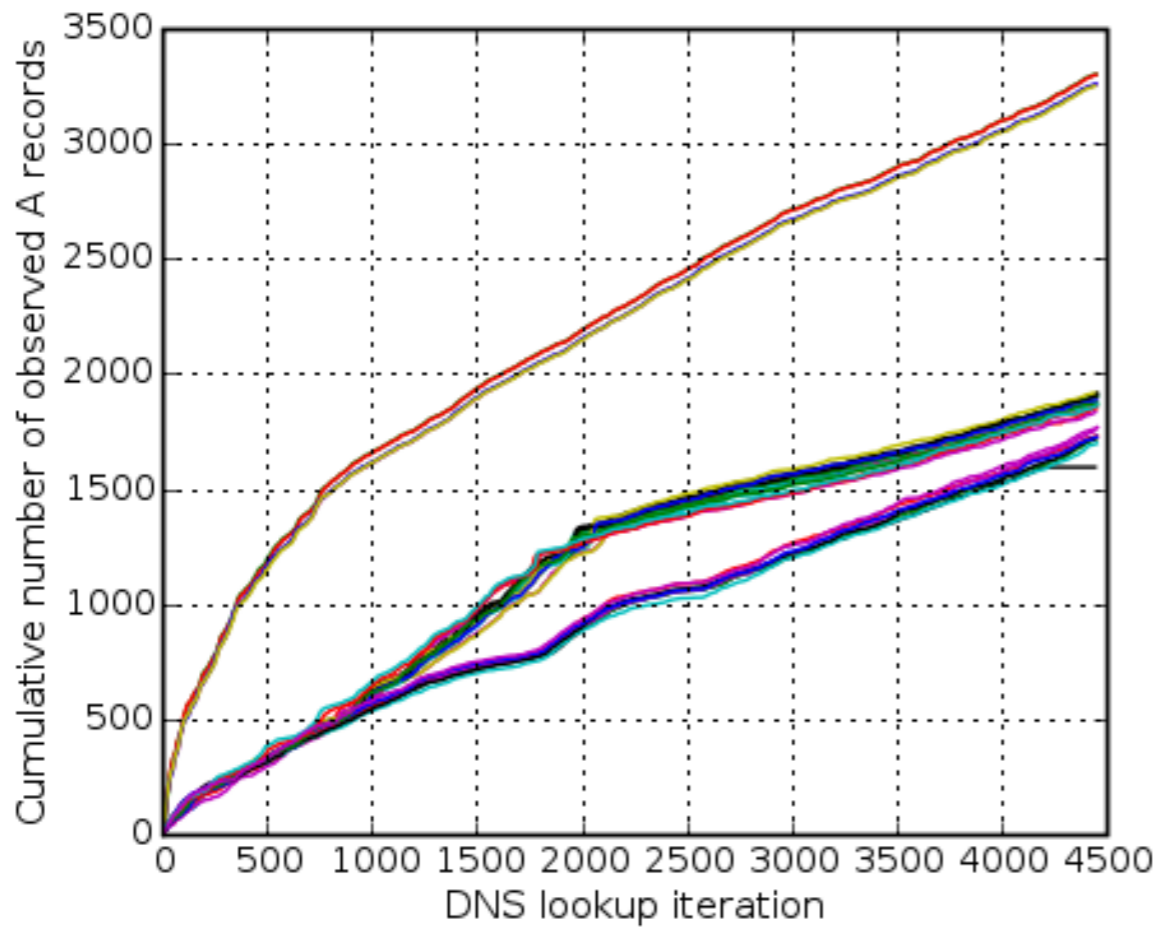
during 12 hours

Long-term measurements



during 120 hours

Long-term measurements



Long-term measurements

4.60% of fast-flux DNS queries failed

0.01% of legitimate DNS queries failed

Fast-flux users

Rock phish (“a well-known phishing toolkit”)

`regs26.com`: 1,121 IPs over 4 days

Storm worm

Fast-flux for hosting bot binaries

`tibeam.com`: 50,000 IPs over 4 weeks

Mitigation

Automated domain blacklist

Take-down

Blackholing

Spam filtering

Block incoming connections?