Peering into Botnets via Fast Flux Enumeration: The ATLAS Experience

ARBOR® NETWORKS

Jose Nazario, Ph.D.

FIRST 2008 NSM-SIG

Vancouver

Project

- **ATLAS - global Internet monitoring**

- **Fast flux - used to discover bots/infected hosts**
  - Active probing
- **Added to ATLAS Q1 2008**

Operational Uses

- Tracking botnets
- Storm, Rock phishing, etc

Observations

- Storm - sometimes used
- Rock phish - used heavily
- Other spam, phishing - used often
- Malcode distribution - Spring 08 SQL injection

Botnet Visibility

- Botnets need good server management when using fast flux

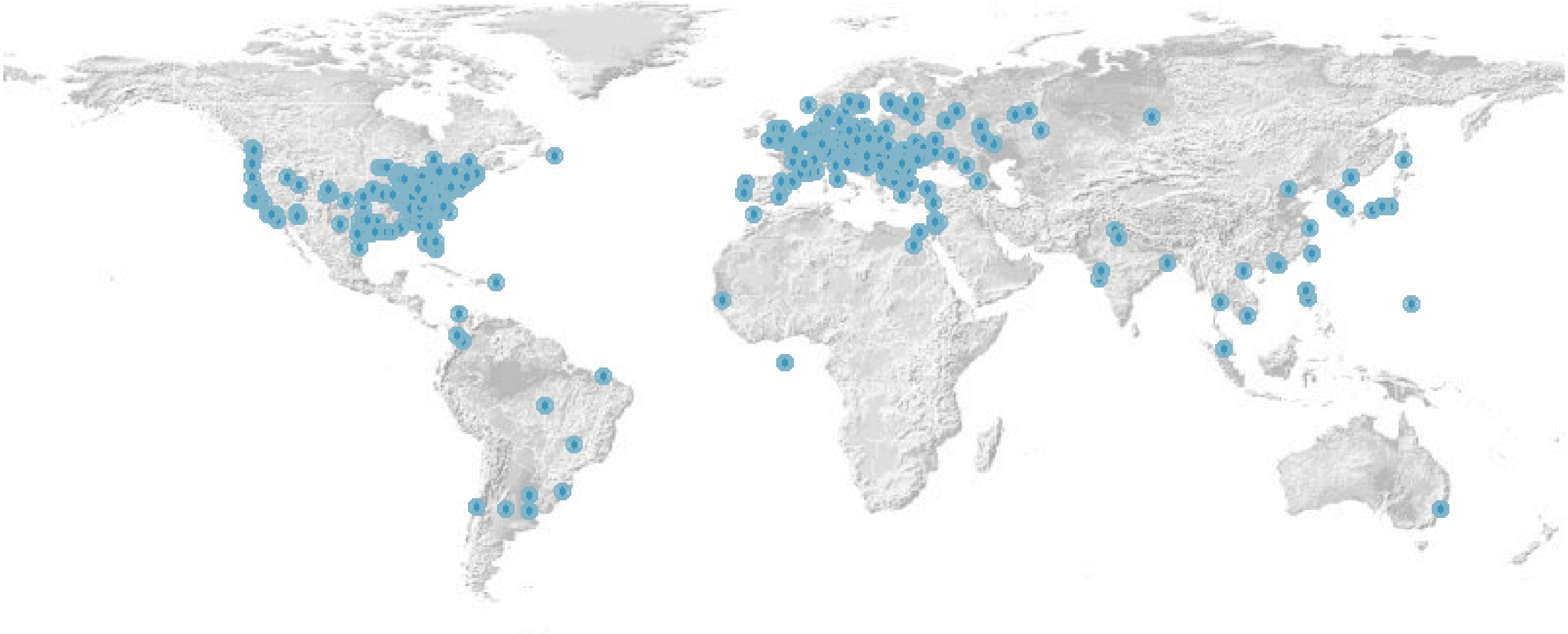
- Let them do the host qualifications

- Only globally unique IP addresses
- Other factors - uptime, speed - vary

Botnet Visibility via DNS Mining

~10%?

24 Hours of Fast Flux Bots



Calling it Fast Flux

- Heuristics

- Based on discussions with R. Danford, T. Holz
- Using Danford's heuristics as base

Qualifying Fast Flux Domain Names

- **Domain name - A record query**
- **Short TTL - under 900 sec**
- **TTL < 2 treated specially, aggressively**
- **More than 5 IPs**
- **IP list has average “distance” > /16**
  - More than 8 IPs? Score is +2
- **IP list has more than 2 ASNs represented**
- **…**

Qualifying Fast Flux Domain Names

```
;; ANSWER SECTION:
clickbnr.com.           600     IN      A       96.28.27.85
clickbnr.com.           600     IN      A       71.204.120.243
clickbnr.com.           600     IN      A       88.168.128.191
clickbnr.com.           600     IN      A       75.181.90.242
clickbnr.com.           600     IN      A       72.226.191.199
clickbnr.com.           600     IN      A       76.18.84.109
clickbnr.com.           600     IN      A       67.185.50.195
clickbnr.com.           600     IN      A       74.65.213.40
clickbnr.com.           600     IN      A       71.56.67.60
clickbnr.com.           600     IN      A       66.90.158.152
clickbnr.com.           600     IN      A       76.31.155.100
clickbnr.com.           600     IN      A       24.164.58.120
clickbnr.com.           600     IN      A       71.201.126.62
clickbnr.com.           600     IN      A       84.25.70.94
```

TTL < 900sec

- TTL < 2sec treated special

More than 5 IPs in RRset

Avg. “Distance” > /16

-More than 8 IPs? +2

More than 2 ASNs

Qualifying Fast Flux Domain Names (cont)

- Domain name NS query
- NS results average “distance” > /16
- More than 3 NS entries

- SOA query
- Minimum retry < 15min

Qualifying Fast Flux Domains (cont)

```
;; ANSWER SECTION:
clickbnr.com.           600     IN      NS      ns6.clickbnr.com.
clickbnr.com.           600     IN      NS      ns8.clickbnr.com.
clickbnr.com.           600     IN      NS      ns4.clickbnr.com.
clickbnr.com.           600     IN      NS      ns2.clickbnr.com.
clickbnr.com.           600     IN      NS      ns10.clickbnr.com.
clickbnr.com.           600     IN      NS      ns9.clickbnr.com.
clickbnr.com.           600     IN      NS      ns11.clickbnr.com.
clickbnr.com.           600     IN      NS      ns7.clickbnr.com.
clickbnr.com.           600     IN      NS      ns5.clickbnr.com.
clickbnr.com.           600     IN      NS      ns1.clickbnr.com.
clickbnr.com.           600     IN      NS      ns3.clickbnr.com.

;; ADDITIONAL SECTION:
ns5.clickbnr.com.       600     IN      A       75.129.134.139
ns6.clickbnr.com.       600     IN      A       68.202.106.222
ns7.clickbnr.com.       600     IN      A       75.137.93.12
ns8.clickbnr.com.       600     IN      A       83.5.235.157
ns9.clickbnr.com.       600     IN      A       71.59.102.113
ns10.clickbnr.com.      600     IN      A       79.184.34.183
ns11.clickbnr.com.      600     IN      A       89.228.212.197
```

More than 3 NS entries

Avg. “Distance” > /16

Qualifying Fast Flux Domain Names (cont)

- **Each attribute is 1 pt**
- **If more than 4 points - fluxy**
- **Exclude whitelist behaviors**
- **Confirm with SURBL**
  - If not, just suspect

Benign Fast Flux Symptoms

```
;; ANSWER SECTION:
database.clamav.net.    60      IN      CNAME   db.local.clamav.net.
db.local.clamav.net.    7200    IN      CNAME   db.us.rr.clamav.net.
db.us.rr.clamav.net.    900     IN      A       64.246.134.219
db.us.rr.clamav.net.    900     IN      A       155.98.64.86
db.us.rr.clamav.net.    900     IN      A       199.239.233.95
db.us.rr.clamav.net.    900     IN      A       209.170.150.7

;; AUTHORITY SECTION:
rr.clamav.net.          7200    IN      NS      ns3.clamav.net.
rr.clamav.net.          7200    IN      NS      ns7.clamav.net.
rr.clamav.net.          7200    IN      NS      ns5.clamav.net.
rr.clamav.net.          7200    IN      NS      ns2.clamav.net.
rr.clamav.net.          7200    IN      NS      ns6.clamav.net.
rr.clamav.net.          7200    IN      NS      ns1.clamav.net.
rr.clamav.net.          7200    IN      NS      ns4.clamav.net.

;; ADDITIONAL SECTION:
ns2.clamav.net.         101522  IN      A       63.166.28.2
ns4.clamav.net.         94322   IN      A       209.9.232.3
ns5.clamav.net.         108723  IN      A       213.92.8.2
ns5.clamav.net.         70221   IN      AAAA    2001:1418:13:1::1
ns6.clamav.net.         94322   IN      A       208.201.249.238
ns7.clamav.net.         101522  IN      A       209.204.159.15
ns1.clamav.net.         69122   IN      A       69.61.68.204
```

Code and Components

- **Python**
- **High speed DNS query engine**
  - Libevent - evdns
  - GNU adns
- **ATLAS data stores**
  - Time series data
  - Geo-lookups of IPs
  - Query front end

ATLAS Querying

- **Every TTL+1, run queries**
- **Store results**

- **Dead detection**
  - After 1 day of failure to grow, prune from list
  - 0 IPs (eg pulled domain) or a parked domain name

Discovering Domains

- Implemented qualifying domain name screening tool
- Data sources
  - Spam feed
  - DNS names from malcode analysis
  - Malware, spam domains lists
- Added manually

Assessing Domain Discovery Methods

- **Looked at interval between domain name registration date and first seen actively “fluxing”**

- **Average interval: 28.8 days**
- **Minimum 0.4 days**
- **Maximum 263.6 days**

- **Possible reasons**
  - ATLAS visibility (e.g. weak spam feed)
  - *“Sleeper” domains*

Global Fast Flux Trends

- Domains in use by one botnet

- Simple set-based approach to peek

$$\frac{\text{Net1} \cap \text{Net2}}{\text{Net1} \cup \text{Net2}}$$

Near 0: no common members
Near 1: same botnet

Active Fast Flux Botnets

- **428 active domains analyzed**
  - May 30, 2008 - 24 hour snapshot

- **Results**
  - 26 active and distinct clusters
  - Indicates 26 active botnets using fast flux techniques
    - Some failures to cluster

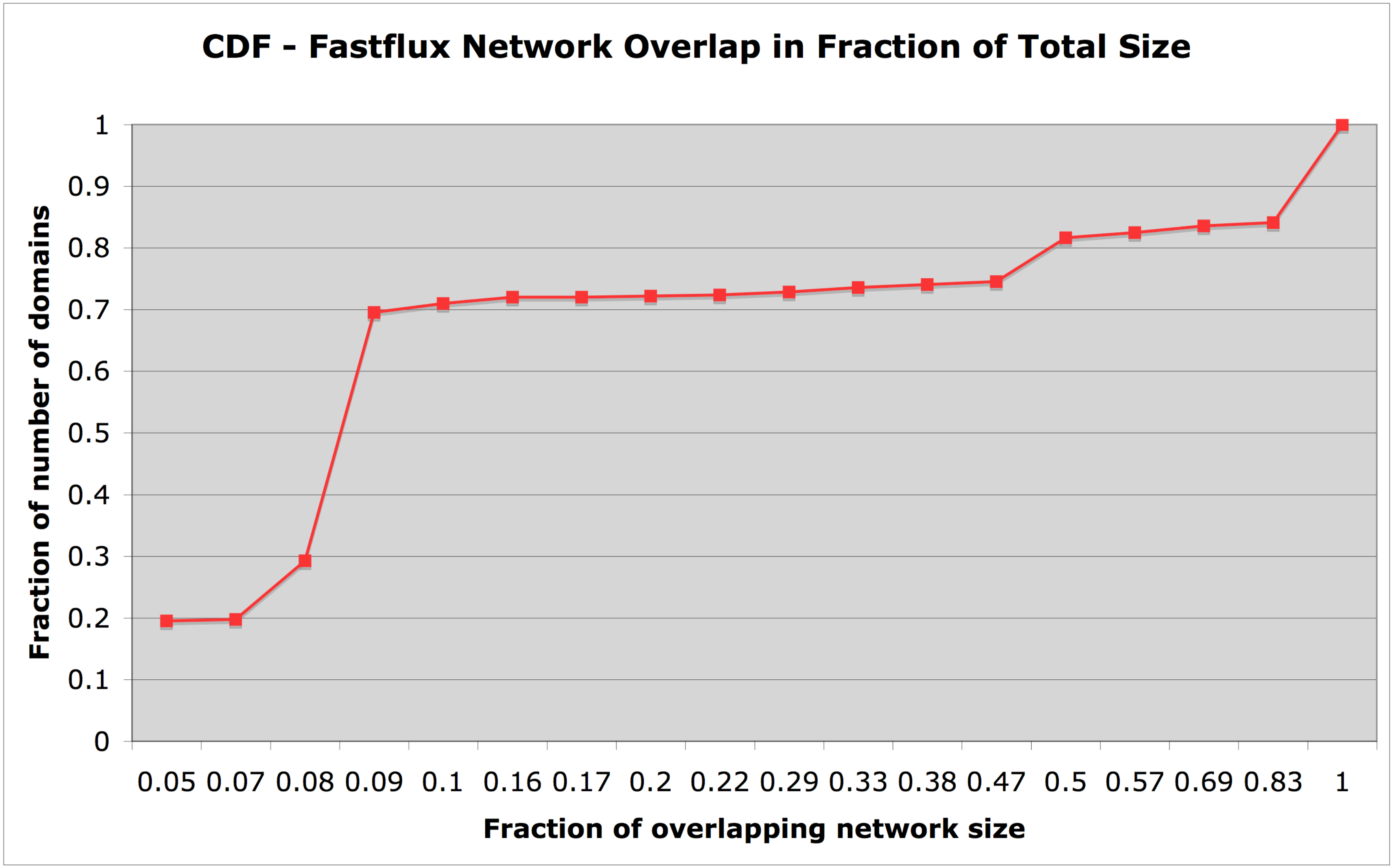
Botnet Purposes

- **Based on post-facto analysis of 26 clusters**

  Data assistance from CastleCops, PhishTank

  - 1 Casino
  - 1 Enlargement
  - 4 Malware
  - 10 Pharmacy
  - 13 Phishing

Some are used for multiple purposes



Multiple infections? Partial overlaps? *Partial advertisements*?

Based on 24h snapshot, June 2 2008

ARBOR® NETWORKS

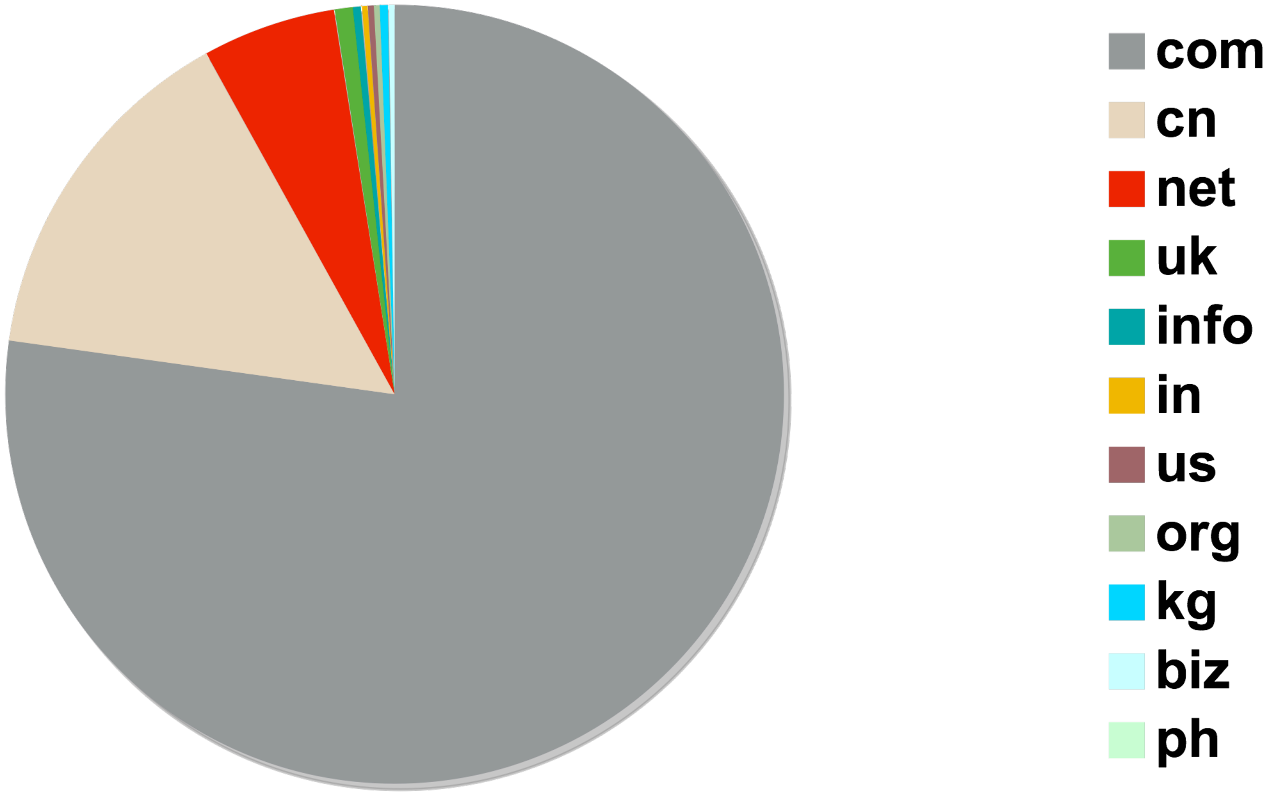
6 Months of Data

- Starting with our ATLAS fast flux tracking

- Data: Jan 18 - June 4, 2008
- 912 domains monitored

Increasingly Global Registrar Problem

- gTLDs used by fast flux domains



Broader distribution than found in Holz *et al*, 2007

Lifetimes

- **Average: 18.5 days**

- **Longest**
  - 60 days+ (ibank-halifax.com)
  - 59 days+ (armsummer.com)
  - 57 days+ (croptriangle.com)

Based on dates of first to last tracking

Sizes

- **Average size: 2683 IPs (cumulative)**

- **Largest nets:**
  - ibank-halifax.com, 100,379 IPs
  - armsummer.com, 14,233 IPs
  - boardhour.com, 11,900 IPs

Mitigation

- **Local**
  - DNS blocklist methods
- **Global**
  - Kill domain with registrar
  - Kill ‘mothership’
- **Getting tougher with new ‘features’ from registrars**
- **ICANN SSAC**

Fast Flux Data Availability

- ATLAS public portal
- Free accounts

- Recently added domain list

- Actively tracks 400-600 fast flux domains a day

Missing Data

- **Registrar data**
  - Would be valuable
  - Key for cleanup, remediation
- **Malcode/family**
- **Content/purpose**
  - Inferred post-facto
- **NS records**
  - Double flux
  - Common NS, hosting nets

Acknowledgements

- ATLAS, ASERT teams at Arbor

- Robert
- Thorsten

- Jeff and William (SURBL)

- Carol and everyone at FIRST