Proactively Blacklisting Fast-Flux Networks

Shahan Sudusinghe
shsudusinghe@verisign.com
Verisign iDEFENSE Malcode Operations

What this presentation covers

- Different parts of fast-flux networks
- Different methods to gather fast-flux data
- Why all these different single sources not good enough stand-alone
- How to get a complete picture of an attack

What comprises a fast-flux network

- Domain names
- Authoritative name servers
- IP addresses
- C&C Servers/ Mothership Servers

What are Fast-Flux networks used for

- Hosting malware
- Launching phishing attacks
- Spam campaigns
- Money Mule scams
- Adult content

Sources to gather FF data

- Trojans that generate them
- Advertising agents (spam, etc...)
- Compromised webservers
- Dropsites, motherships
- Black-list domains/URL Lists from analysis systems
- No single source will ever give you the big picture

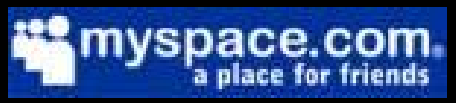
Why individually these methods not effective?

- IP addresses change all the time
- Attackers retire domains after a while
- Fast-Flux network may not utilize the ONLY source you are monitoring

Collecting FF domains from SPAM

- Collecting SPAM emails through SPAM Traps
- Storm, Weldec, Canadian Pharmacy, Online Pharmacy etc.
- Not limited to e-mails…

Expanding SPAM Traps



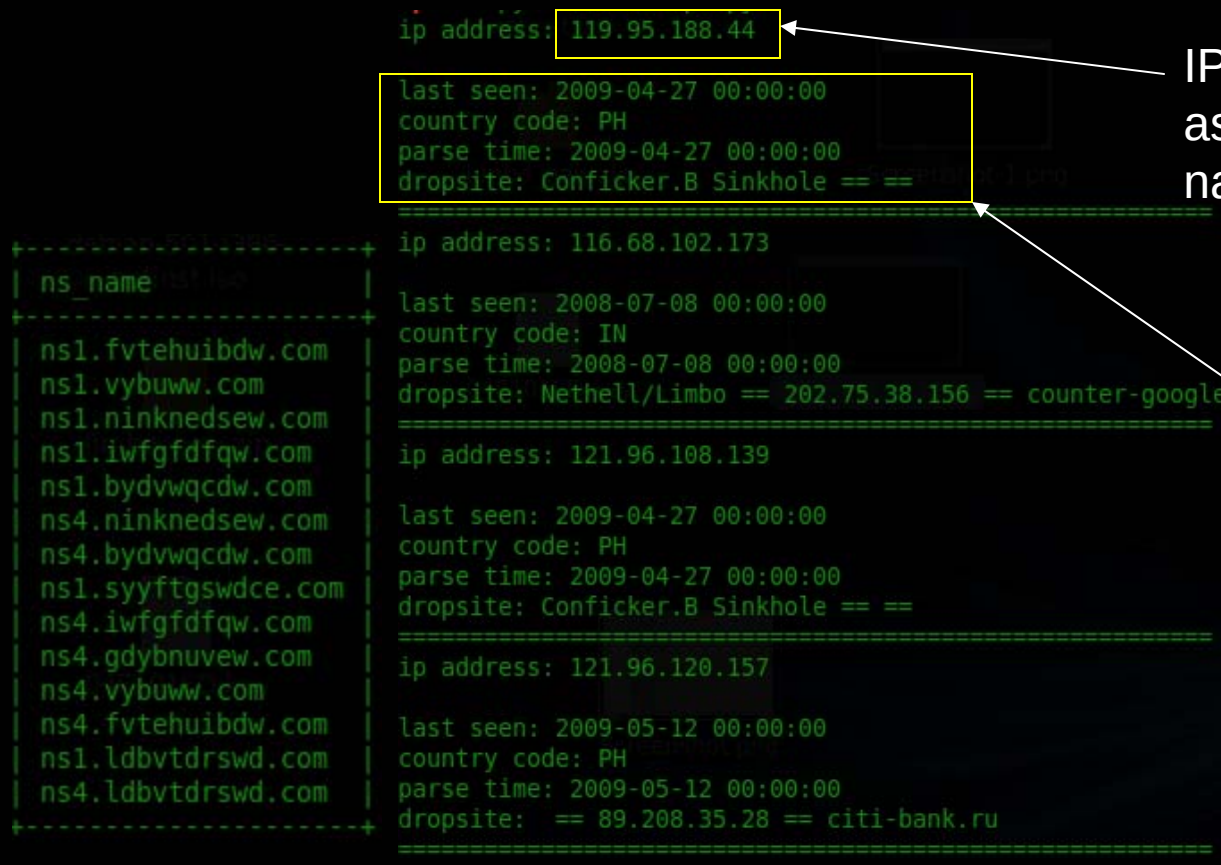
SPAM based Fast-Flux monitoring

- http://dnsbl.abuse.ch (honeypot based spam collection)
- http://honeynet.org.au (Australian Honeynet Project) Tracker

Dropsite data & Trojan data

- After infection Trojans report to dropsites
- Infected machines are used in botnets --→ fast-flux networks
- Identifying Trojan gives more information on the Fast-Flux network

Infected clients used in Fast-Flux hosting



IP address associated with name server

Same IP was reported as infected

Victim IP FF IP aggregation

- With two days worth FF data there was 20 IP matches
- 11 Conficker.B, 4 Zeus, 3 BManager, 1 Limbo and 1 Unknown
- 23 different domains hosting name servers

Rapid Zone Updates (RZU)

- Records every alteration to all authoritative name servers belong to that TLD
- Updates every 5 second interval
- Stores data in flat files

RZU file…

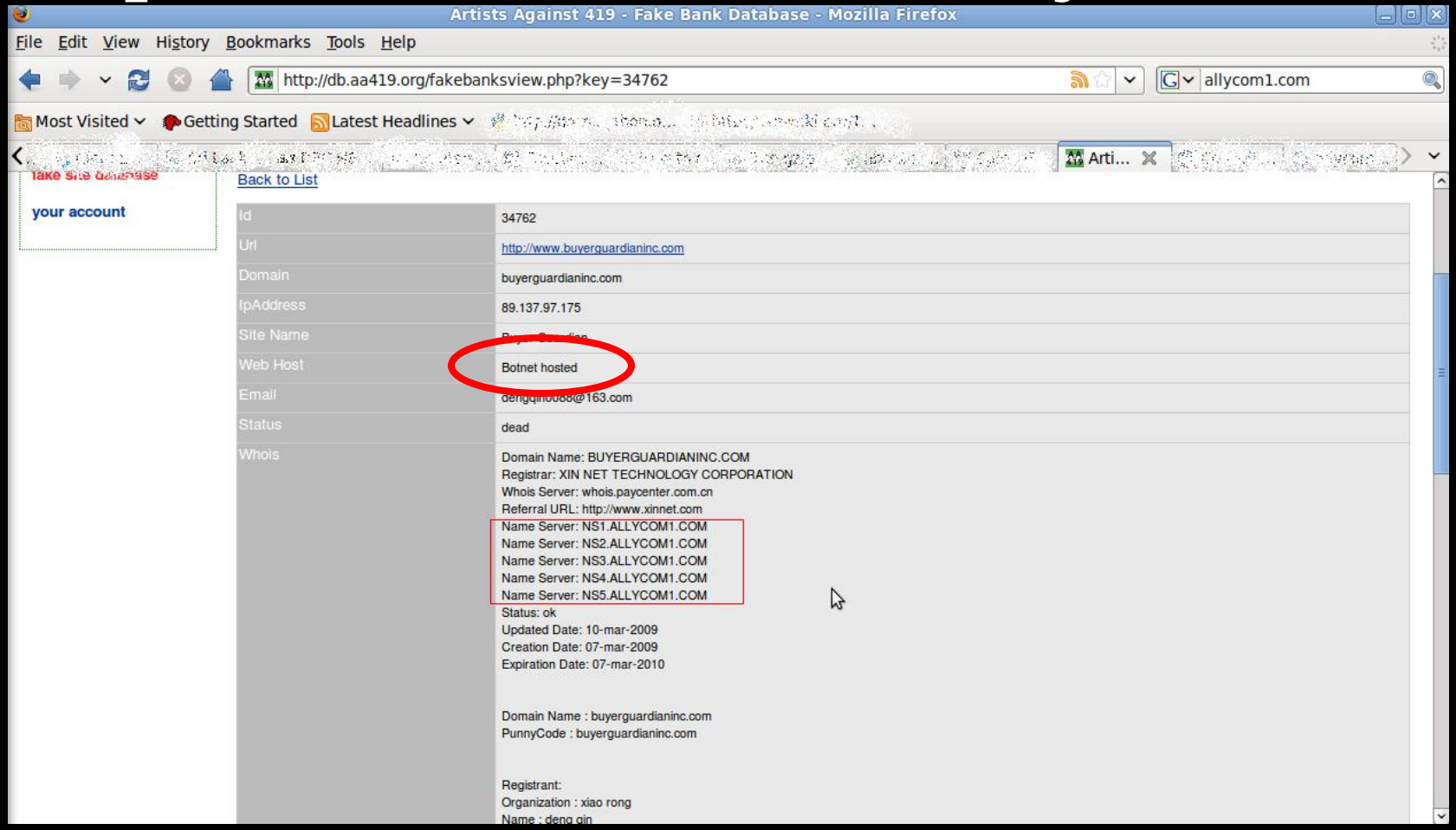
```
add mayfairsolicitors.com NS
add ecasinogoldens.com NS
delete mayfairsolicitors.com
delete gangstargear.net
add ecasino-goldens.com NS
add ecasino-goldens.com NS
add blueknightspavi.com NS
delete ns1.ecasino-goldens.com A 69.57.161.18
add ns1.ecasino-goldens.com A 69.57.161.18
add ilvetrodilivia.com NS
add chondrogenesis.com NS
delete ilvetrodilivia.com
add ecasino-goldens.com NS
add blueknightspavi.com NS
add satgng.net NS
add myglobetravel.com NS
add ecasino-goldens.com NS
add satgng.net NS
delete satgng.net NS ns4.domainsite.com
add ecasino-goldens.com NS
add triptica.net NS
add-new t-1273946207-1240983121197-1-dlqzw.com NS
add satgng.net NS
add-new t-1370129124-1240983121258-1-jxnpy.com NS
add triptica.net NS
delete triptica.net NS ns11.domaincontrol.com
delete triptica.net NS ns12.domaincontrol.com
delete t-1273946207-1240983121197-1-dlqzw.com
delete ns2.ecasino-goldens.com A 66.119.68.246
add ns2.ecasino-goldens.com A 66.119.68.246
delete t-1370129124-1240983121258-1-jxnpy.com
add triptica.net NS
add triptica.net NS ns51.domaincontrol.com
add triptica.net NS ns52.domaincontrol.com
delete t-1273946207-1240983121197-1-dlqzw.com
add buysellandconsign.com NS
delete t-1370129124-1240983121258-1-jxnpy.com
add ecasino-goldens.com NS
add mgaffiliatesearnonline.com NS
delete mgaffiliatesearnonline.com NS ns1.renewyourname.net
```

Double Flux name server

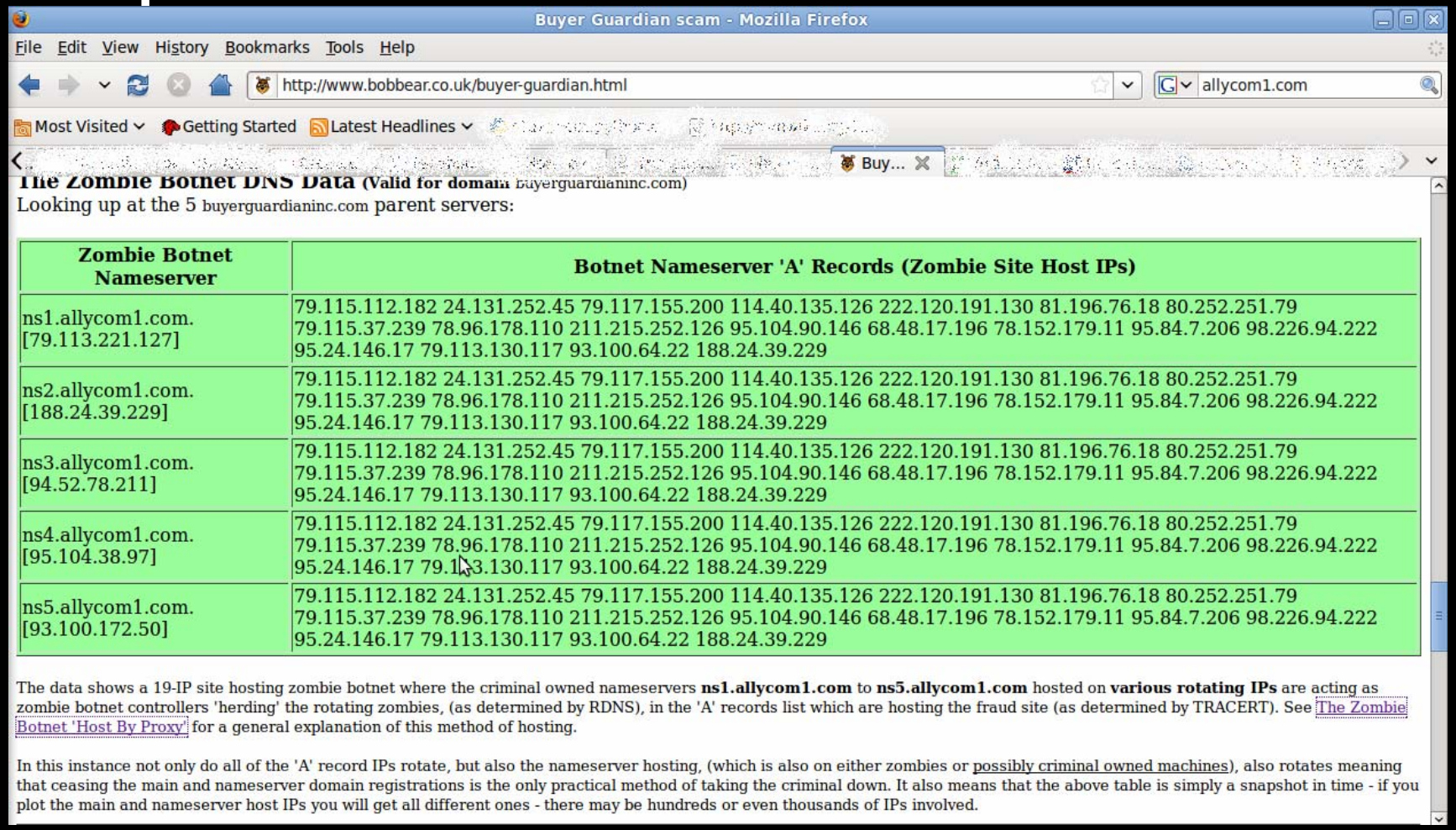
- Use of simple Linux commands to retrieve name servers
- Frequency of change
- Number of IPs associated with it and their net block
- If differs from the reasonably accepted rules it can be flagged as FF (eg name server have 50 IPs)

```
add ns4.allycom1.com A 86.123.197.211
add ns4.allycom1.com A 89.41.179.85
add ns4.allycom1.com A 80.252.247.187
add ns4.allycom1.com A 89.40.112.216
add ns4.allycom1.com A 79.116.194.248
add ns4.allycom1.com A 89.38.223.236
add ns4.allycom1.com A 122.147.82.48
add ns4.allycom1.com A 78.96.83.101
add ns4.allycom1.com A 123.141.67.46
add ns4.allycom1.com A 189.41.194.155
add ns4.allycom1.com A 91.200.138.154
add ns4.allycom1.com A 122.147.82.203
add ns4.allycom1.com A 213.164.224.45
add ns4.allycom1.com A 89.37.240.97
add ns4.allycom1.com A 79.117.202.28
add ns4.allycom1.com A 79.112.118.34
add ns4.allycom1.com A 124.161.3.31
add ns4.allycom1.com A 79.113.169.226
add ns4.allycom1.com A 89.45.89.244
add ns4.allycom1.com A 92.81.40.161
add ns4.allycom1.com A 95.104.44.238
add ns4.allycom1.com A 95.220.83.64
add ns4.allycom1.com A 79.113.36.217
add ns4.allycom1.com A 196.217.235.243
add ns4.allycom1.com A 200.68.93.91
```

Reported Fast-Flux on allycom1



Reported Fast-Flux



The Zombie Botnet DNS Data (Valid for domain buyerguardianinc.com)

Looking up at the 5 buyerguardianinc.com parent servers:

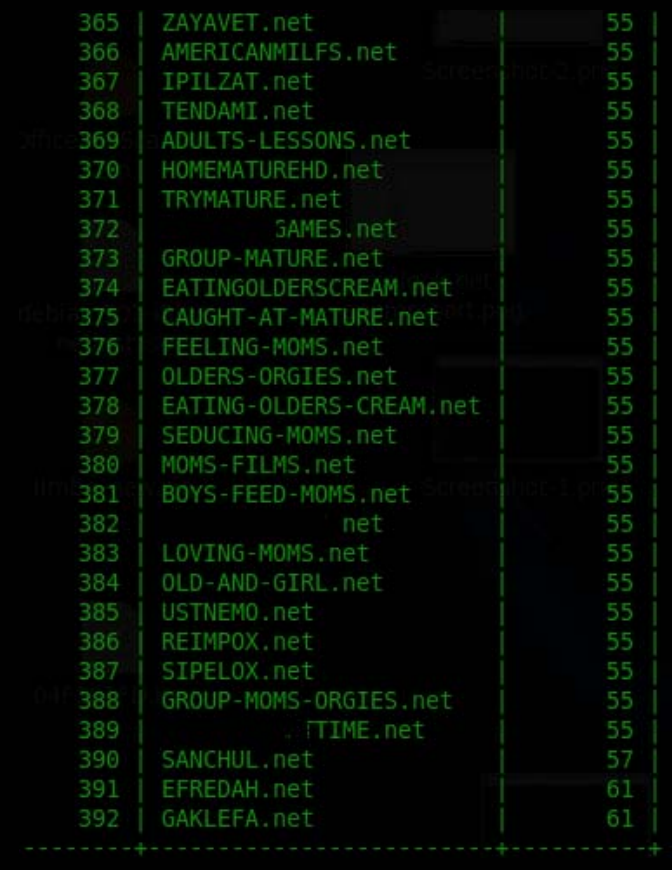
Zombie Botnet Nameserver	Botnet Nameserver 'A' Records (Zombie Site Host IPs)
ns1.allycom1.com. [79.113.221.127]	79.115.112.182 24.131.252.45 79.117.155.200 114.40.135.126 222.120.191.130 81.196.76.18 80.252.251.79 79.115.37.239 78.96.178.110 211.215.252.126 95.104.90.146 68.48.17.196 78.152.179.11 95.84.7.206 98.226.94.222 95.24.146.17 79.113.130.117 93.100.64.22 188.24.39.229
ns2.allycom1.com. [188.24.39.229]	79.115.112.182 24.131.252.45 79.117.155.200 114.40.135.126 222.120.191.130 81.196.76.18 80.252.251.79 79.115.37.239 78.96.178.110 211.215.252.126 95.104.90.146 68.48.17.196 78.152.179.11 95.84.7.206 98.226.94.222 95.24.146.17 79.113.130.117 93.100.64.22 188.24.39.229
ns3.allycom1.com. [94.52.78.211]	79.115.112.182 24.131.252.45 79.117.155.200 114.40.135.126 222.120.191.130 81.196.76.18 80.252.251.79 79.115.37.239 78.96.178.110 211.215.252.126 95.104.90.146 68.48.17.196 78.152.179.11 95.84.7.206 98.226.94.222 95.24.146.17 79.113.130.117 93.100.64.22 188.24.39.229
ns4.allycom1.com. [95.104.38.97]	79.115.112.182 24.131.252.45 79.117.155.200 114.40.135.126 222.120.191.130 81.196.76.18 80.252.251.79 79.115.37.239 78.96.178.110 211.215.252.126 95.104.90.146 68.48.17.196 78.152.179.11 95.84.7.206 98.226.94.222 95.24.146.17 79.113.130.117 93.100.64.22 188.24.39.229
ns5.allycom1.com. [93.100.172.50]	79.115.112.182 24.131.252.45 79.117.155.200 114.40.135.126 222.120.191.130 81.196.76.18 80.252.251.79 79.115.37.239 78.96.178.110 211.215.252.126 95.104.90.146 68.48.17.196 78.152.179.11 95.84.7.206 98.226.94.222 95.24.146.17 79.113.130.117 93.100.64.22 188.24.39.229

The data shows a 19-IP site hosting zombie botnet where the criminal owned nameservers **ns1.allycom1.com** to **ns5.allycom1.com** hosted on **various rotating IPs** are acting as zombie botnet controllers 'herding' the rotating zombies, (as determined by RDNS), in the 'A' records list which are hosting the fraud site (as determined by TRACERT). See The Zombie Botnet 'Host By Proxy' for a general explanation of this method of hosting.

In this instance not only do all of the 'A' record IPs rotate, but also the nameserver hosting, (which is also on either zombies or possibly criminal owned machines), also rotates meaning that ceasing the main and nameserver domain registrations is the only practical method of taking the criminal down. It also means that the above table is simply a snapshot in time - if you plot the main and nameserver host IPs you will get all different ones - there may be hundreds or even thousands of IPs involved.

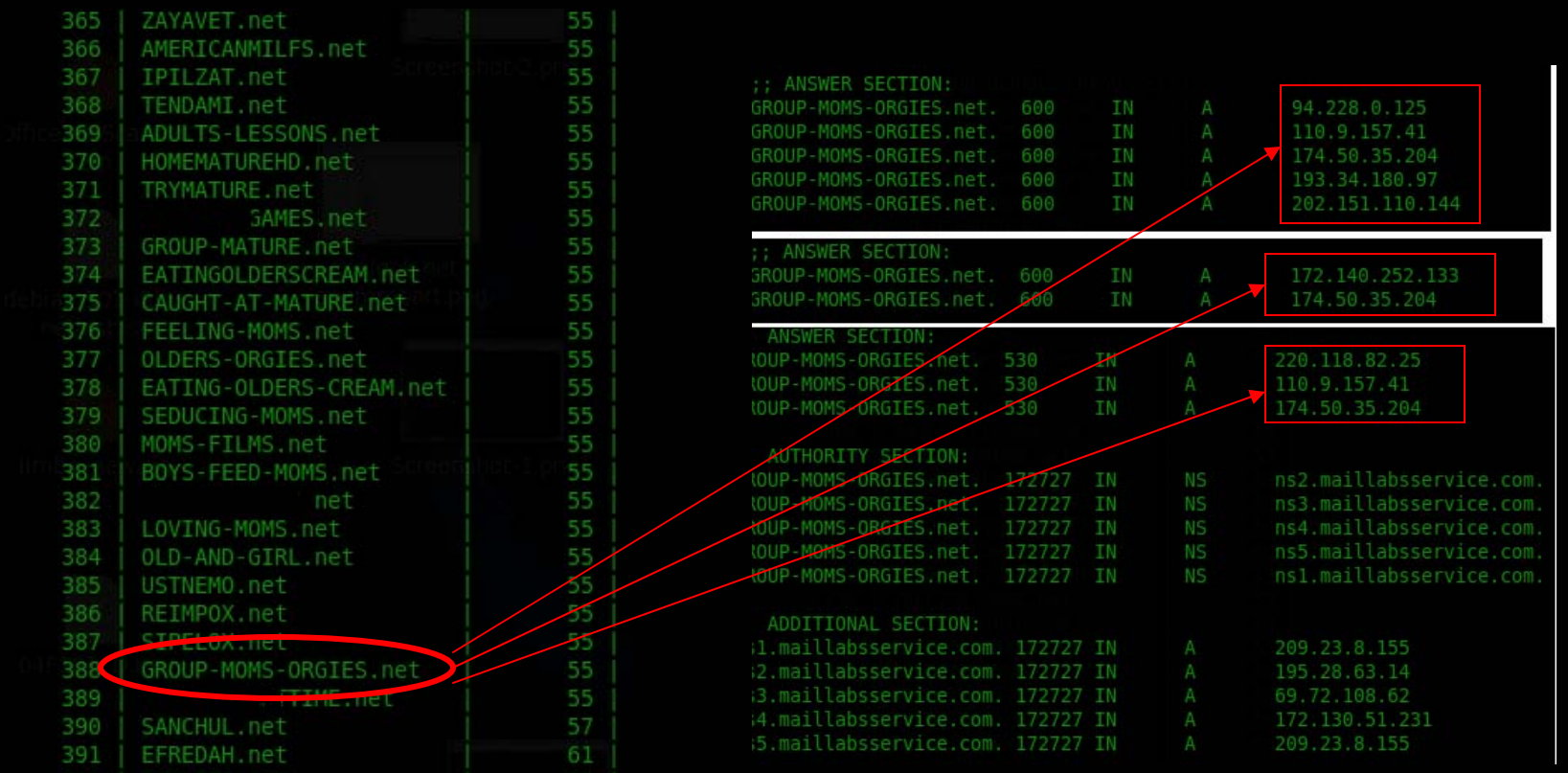
Domains for Double-Flux

- Difficult to obtain because no changes for name server in RZU
- RZU results has to combined with root zone file data
- Domains always do not belong to one TLD makes it difficult



365	ZAYAVET.net	55
366	AMERICANMILFS.net	55
367	IPILZAT.net	55
368	TENDAMI.net	55
369	ADULTS-LESSONS.net	55
370	HOMEMATUREHD.net	55
371	TRYMATURE.net	55
372	GAMES.net	55
373	GROUP-MATURE.net	55
374	EATINGOLDERSCREAM.net	55
375	CAUGHT-AT-MATURE.net	55
376	FEELING-MOMS.net	55
377	OLDERS-ORGIES.net	55
378	EATING-OLDERS-CREAM.net	55
379	SEDUCING-MOMS.net	55
380	MOMS-FILMS.net	55
381	BOYS-FEED-MOMS.net	55
382	net	55
383	LOVING-MOMS.net	55
384	OLD-AND-GIRL.net	55
385	USTNEMO.net	55
386	REIMPOX.net	55
387	SIPELOX.net	55
388	GROUP-MOMS-ORGIES.net	55
389	TIME.net	55
390	SANCHUL.net	57
391	EFREDAH.net	61
392	GAKLEFA.net	61

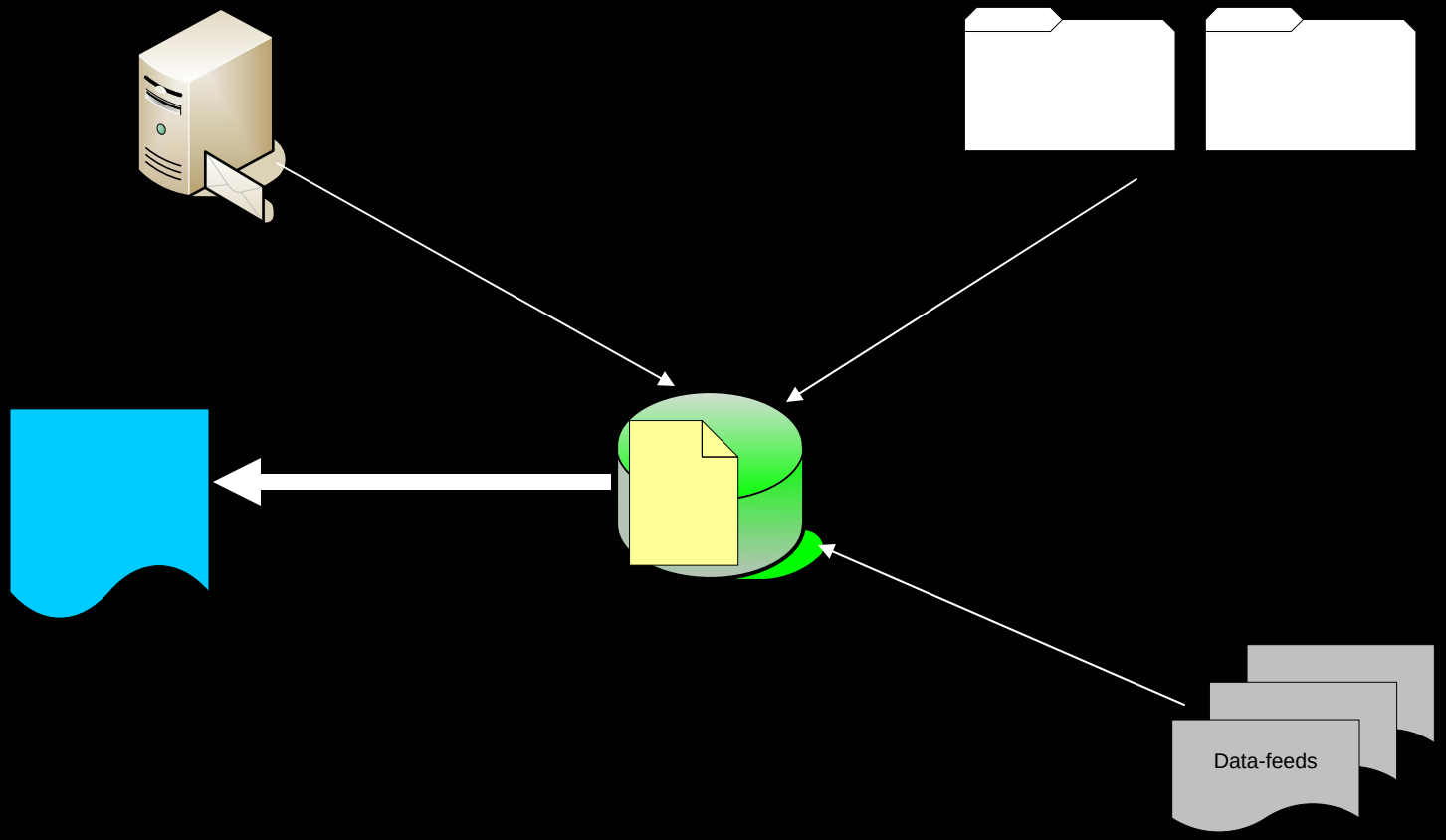
Single-Flux from RZU + Zone files



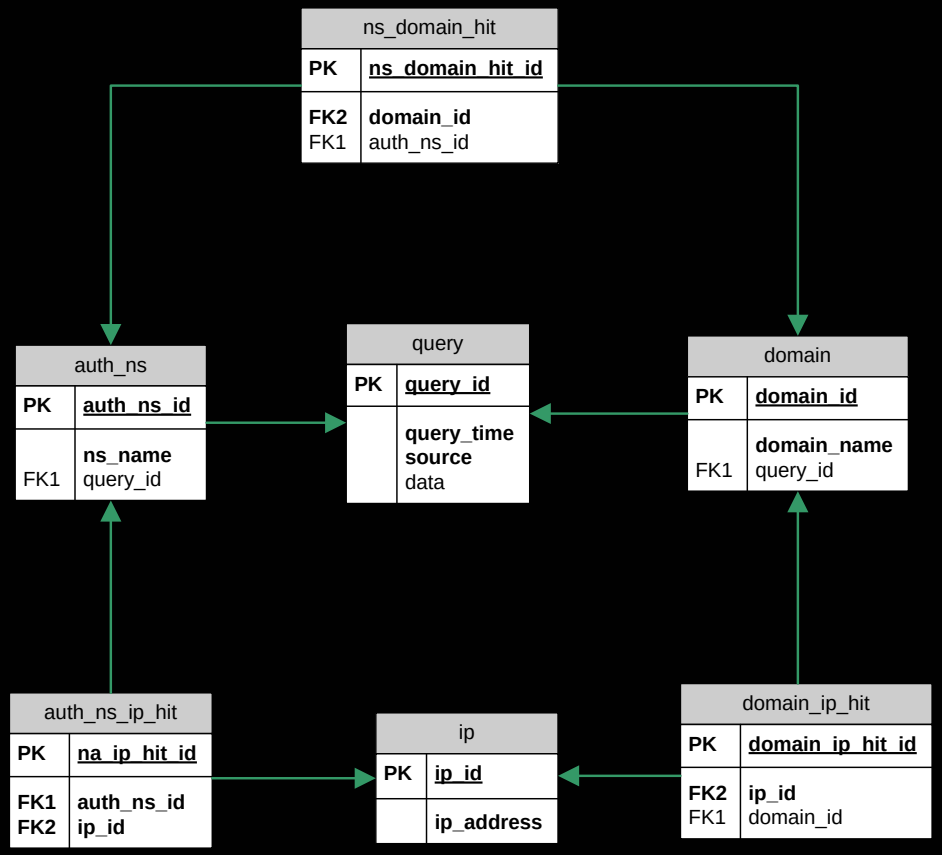
```
365 | ZAYAVET.net                  |  55 |
366 | AMERICANMILFS.net            |  55 |
367 | IPILZAT.net                  |  55 |
368 | TENDAMI.net                  |  55 |
369 | ADULTS-LESSONS.net           |  55 |
370 | HOMEMATUREHD.net             |  55 |
371 | TRYMATURE.net                |  55 |
372 |         GAMES.net            |  55 |
373 | GROUP-MATURE.net             |  55 |
374 | EATINGOLDERSCREAM.net        |  55 |
375 | CAUGHT-AT-MATURE.net         |  55 |
376 | FEELING-MOMS.net             |  55 |
377 | OLDERS-ORGIES.net            |  55 |
378 | EATING-OLDERS-CREAM.net      |  55 |
379 | SEDUCING-MOMS.net            |  55 |
380 | MOMS-FILMS.net               |  55 |
381 | BOYS-FEED-MOMS.net           |  55 |
382 |              net             |  55 |
383 | LOVING-MOMS.net              |  55 |
384 | OLD-AND-GIRL.net             |  55 |
385 | USTNEMO.net                  |  55 |
386 | REIMPOX.net                  |  55 |
387 | SIPELOX.net                  |  55 |
388 | GROUP-MOMS-ORGIES.net        |  55 |
389 |          TIME.net            |  55 |
390 | SANCHUL.net                  |  57 |
391 | EFREDAH.net                  |  61 |
392 | GAKLEFA.net                  |  61 |
```

```
;; ANSWER SECTION:
GROUP-MOMS-ORGIES.net.  600     IN      A       94.228.0.125
GROUP-MOMS-ORGIES.net.  600     IN      A       110.9.157.41
GROUP-MOMS-ORGIES.net.  600     IN      A       174.50.35.204
GROUP-MOMS-ORGIES.net.  600     IN      A       193.34.180.97
GROUP-MOMS-ORGIES.net.  600     IN      A       202.151.110.144

;; ANSWER SECTION:
GROUP-MOMS-ORGIES.net.  600     IN      A       172.140.252.133
GROUP-MOMS-ORGIES.net.  600     IN      A       174.50.35.204

 ANSWER SECTION:
OUP-MOMS-ORGIES.net.  530     IN      A       220.118.82.25
OUP-MOMS-ORGIES.net.  530     IN      A       110.9.157.41
OUP-MOMS-ORGIES.net.  530     IN      A       174.50.35.204

 AUTHORITY SECTION:
OUP-MOMS-ORGIES.net.  172727  IN      NS      ns2.maillabsservice.com.
OUP-MOMS-ORGIES.net.  172727  IN      NS      ns3.maillabsservice.com.
OUP-MOMS-ORGIES.net.  172727  IN      NS      ns4.maillabsservice.com.
OUP-MOMS-ORGIES.net.  172727  IN      NS      ns5.maillabsservice.com.
OUP-MOMS-ORGIES.net.  172727  IN      NS      ns1.maillabsservice.com.

 ADDITIONAL SECTION:
1.maillabsservice.com. 172727 IN      A       209.23.8.155
2.maillabsservice.com. 172727 IN      A       195.28.63.14
3.maillabsservice.com. 172727 IN      A       69.72.108.62
4.maillabsservice.com. 172727 IN      A       172.130.51.231
5.maillabsservice.com. 172727 IN      A       209.23.8.155
```

Aggregation gives fast results



Aggregation Data Base



Aggregation Database

- Need to expand to accommodate more data
- Uses series of Python scripts and shell commands to find data
- Uses multiple databases (victimip, spam)
- Currently do not follow domains actively after identification

Don’t wait take action

- Once you find few IP addresses, couple of domains monitor them to find more data
- Black-list/block on the slightest suspicion
- Don’t wait till you know its bad.
- Data aggregation gives fast results