Detection and Mitigation of Fast-Flux Service Networks

Thorsten Holz, Christian Gorecki,
Felix Freiling, Konrad Rieck

Pi1 - Laboratory for Dependable Distributed Systems

Motivation

- Yesterday: presentation by Dagon
    - “Corrupt DNS Resolution Paths”
- Today: How attackers use DNS for malicious purposes, e.g., scam hosting

Motivation

- Yesterday: presentation by Dagon
  - “Corrupt DNS Resolution Paths”
- Today: How attackers use DNS for malicious purposes, e.g., scam hosting

```
$ dig isoc.org

;; ANSWER SECTION:
isoc.org.                38679    IN      A       206.131.241.137
```

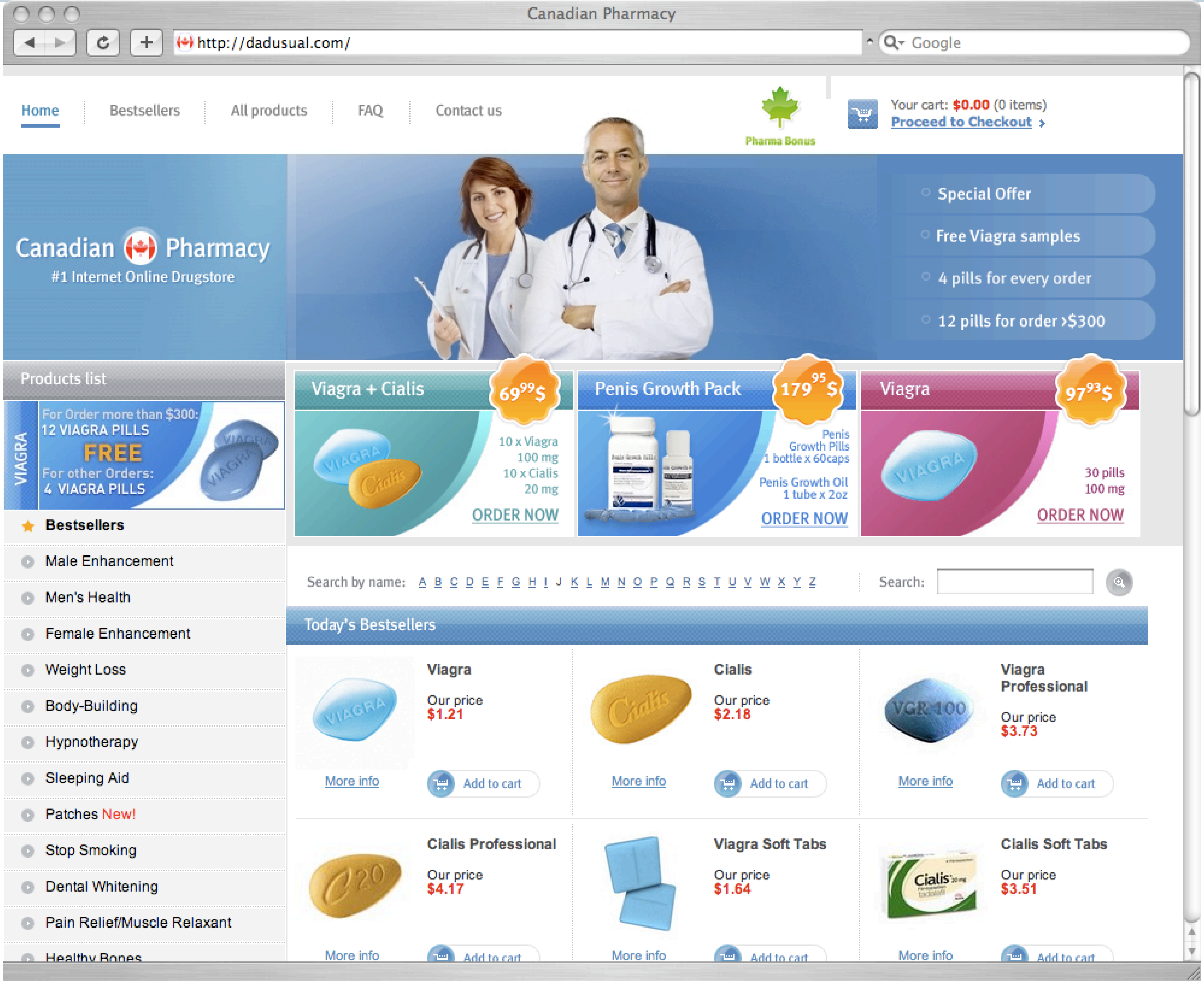
Motivation

```
$ dig dadusual.com

;; ANSWER SECTION:
dadusual.com.        300    IN    A    125.59.103.156
dadusual.com.        300    IN    A    218.254.9.205
dadusual.com.        300    IN    A    62.65.233.109
dadusual.com.        300    IN    A    76.181.194.207
dadusual.com.        300    IN    A    77.41.18.139
dadusual.com.        300    IN    A    78.84.69.132
dadusual.com.        300    IN    A    78.106.115.147
dadusual.com.        300    IN    A    78.106.180.151
dadusual.com.        300    IN    A    78.106.200.47
dadusual.com.        300    IN    A    78.106.224.174
dadusual.com.        300    IN    A    79.120.43.191
dadusual.com.        300    IN    A    80.222.32.58
dadusual.com.        300    IN    A    84.62.186.63
dadusual.com.        300    IN    A    85.177.42.179
dadusual.com.        300    IN    A    85.181.225.55
dadusual.com.        300    IN    A    89.112.4.172
```

Motivation

```
$ dig dadusual.com

;; ANSWER SECTION:
 cm125-59-103-156.hkcable.com.hk.                125.59.103.156
 cm218-254-9-205.hkcable.com.hk.                 218.254.9.205
 pc109.host41.starman.ee.                        62.65.233.109
 cpe-76-181-194-207.columbus.res.rr.com.         76.181.194.207
 host-77-41-18-139.qwerty.ru.                    77.41.18.139
                                                 78.84.69.132
dadusual.com.           300     IN      A        78.106.115.147
dadusual.com.           300     IN      A        78.106.180.151
dadusual.com.           300     IN      A        78.106.200.47
dadusual.com.           300     IN      A        78.106.224.174
dadusual.com.           300     IN      A        79.120.43.191
dadusual.com.           300     IN      A        80.222.32.58
dadusual.com.           300     IN      A        84.62.186.63
dadusual.com.           300     IN      A        85.177.42.179
dadusual.com.           300     IN      A        85.181.225.55
dadusual.com.           300     IN      A        89.112.4.172
```

Motivation



Canadian Pharmacy

http://dadusual.com/

Your cart: $0.00 (0 items)
Proceed to Checkout ›

Canadian Pharmacy
#1 Internet Online Drugstore

- Special Offer
- Free Viagra samples
- 4 pills for every order
- 12 pills for order >$300

Products list

VIAGRA
For Order more than $300:
12 VIAGRA PILLS
FREE
For other Orders:
4 VIAGRA PILLS

- Bestsellers
- Male Enhancement
- Men's Health
- Female Enhancement
- Weight Loss
- Body-Building
- Hypnotherapy
- Sleeping Aid
- Patches New!
- Stop Smoking
- Dental Whitening
- Pain Relief/Muscle Relaxant
- Healthy Bones

Viagra + Cialis
69.99 $
10 x Viagra
100 mg
10 x Cialis
20 mg
ORDER NOW

Penis Growth Pack
179.95 $
Penis Growth Pills
1 bottle x 60caps
Penis Growth Oil
1 tube x 2oz
ORDER NOW

Viagra
97.93 $
30 pills
100 mg
ORDER NOW

Search by name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Search:

Today's Bestsellers

Product	Our price
Viagra	$1.21
Cialis	$2.18
Viagra Professional	$3.73
Cialis Professional	$4.17
Viagra Soft Tabs	$1.64
Cialis Soft Tabs	$3.51

Outline

- Introduction
- Automated identification fast-flux domains
- Measurement results
  - Two month period in July / August 2007
- Mitigation (briefly)
- Conclusion

Introduction

- *Availability* is important for commercial services
- Techniques from the area of reliability engineering help to achieve availability
  - RAID or failover systems
  - Methods using DNS
    - Round-robin DNS
    - Content distribution networks (CDNs)

Introduction

- *Availability* is important for commercial services
- Techniques from the area of reliability engineering help to achieve availability

```
$ dig myspace.com

;; ANSWER SECTION:
myspace.com.            3410    IN      A       216.178.38.104
myspace.com.            3410    IN      A       216.178.38.121
myspace.com.            3410    IN      A       216.178.38.116
```

Introduction

- *Availability* is important for commercial services
- Techniques from the area of reliability engineering help to achieve availability

```
$ dig myspace.com

;; ANSWER SECTION:
myspace.com.            3409    IN      A       216.178.38.116
myspace.com.            3409    IN      A       216.178.38.104
myspace.com.            3409    IN      A       216.178.38.121
```

Introduction

- *Availability* is important for commercial services
- Techniques from the area of reliability engineering help to achieve availability

```
$ dig myspace.com

;; ANSWER SECTION:
myspace.com.            3408    IN      A       216.178.38.121
myspace.com.            3408    IN      A       216.178.38.116
myspace.com.            3408    IN      A       216.178.38.104
```

Introduction

- *Availability* is important for commercial services
- Techniques from the area of reliability engineering help to achieve availability
  - RAID or failover systems
  - Methods using DNS
    - Round-robin DNS
    - Content distribution networks (CDNs)

Introduction

- Note: illegal commercial organizations also need high availability
    - Scammer only earns money if pharmacy shop is online
    - Phisher needs to have phishing site online
- Our starting point:
    - *How do attackers achieve high availability?*

FFSNs

- If scammers could advertise multiple IP addresses for a given domain, shutdown would be harder
- Botherder could use idea behind RRDNS to split botnet across multiple C&C server
- Technique used: *Fast-flux service networks*
  - Fast change in DNS answers
  - Recent paper by Honeynet Project

FFSNs

- Given fast-flux domain returns few IP addresses from large pool of compromised machines (“flux agents”)
- After the (low) TTL expired, return different subset

FFSNs

- Given fast-flux domain returns few IP addresses from large pool of compromised machines (“flux agents”)
- After the (low) TTL expired, return different subset

```
;; ANSWER SECTION:
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
```

FFSNs

- Given fast-flux domain returns few IP addresses from large pool of compromised machines (“flux agents”)
- After the (low) TTL expired, return different subset

```
;; ANSWER SECTION:
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
```

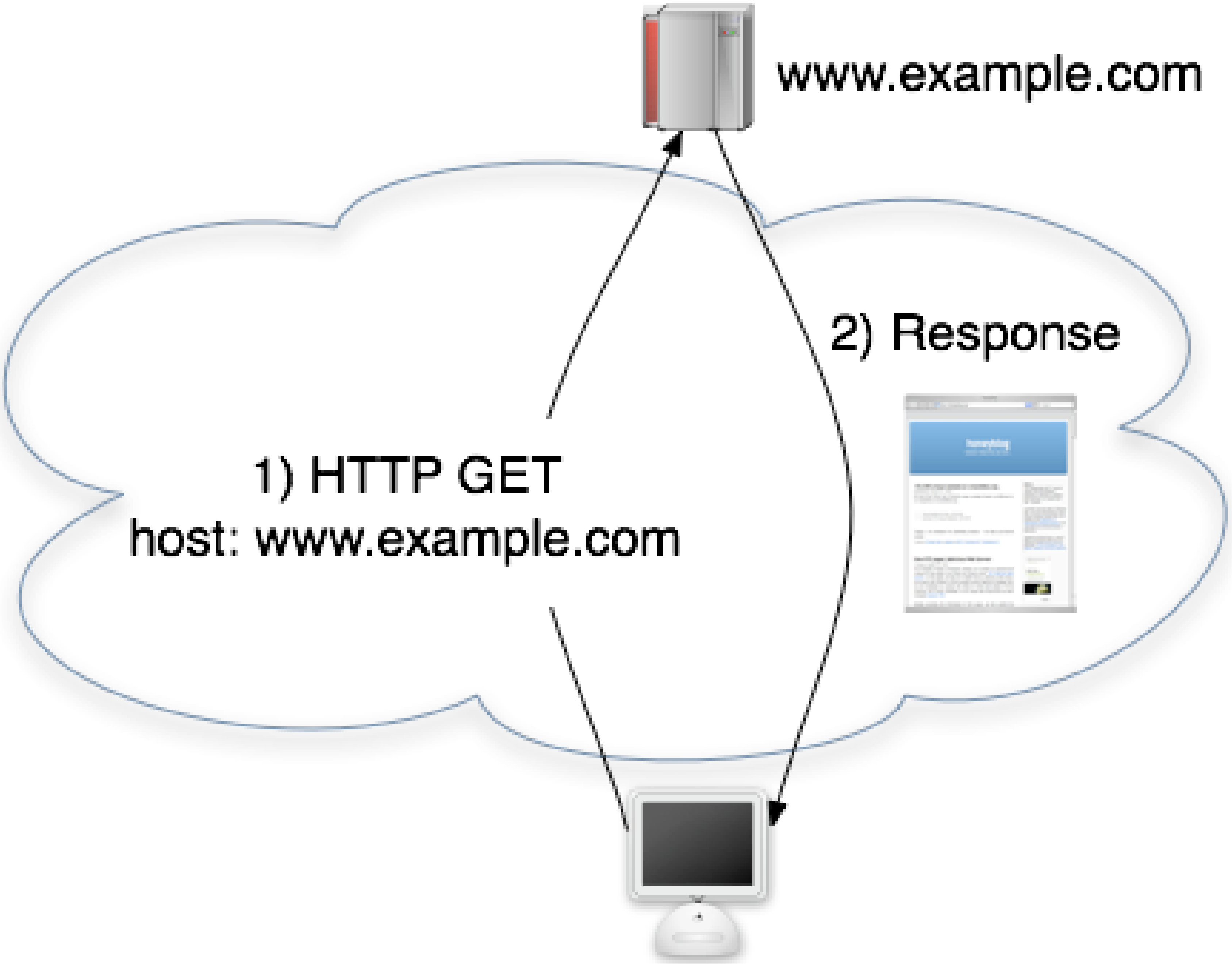
```
;; ANSWER SECTION:
thearmynext.info.       600     IN      A       213.47.148.82
thearmynext.info.       600     IN      A       213.91.251.16
thearmynext.info.       600     IN      A       69.183.207.99
thearmynext.info.       600     IN      A       91.148.168.92
thearmynext.info.       600     IN      A       195.38.60.79
```

FFSNs

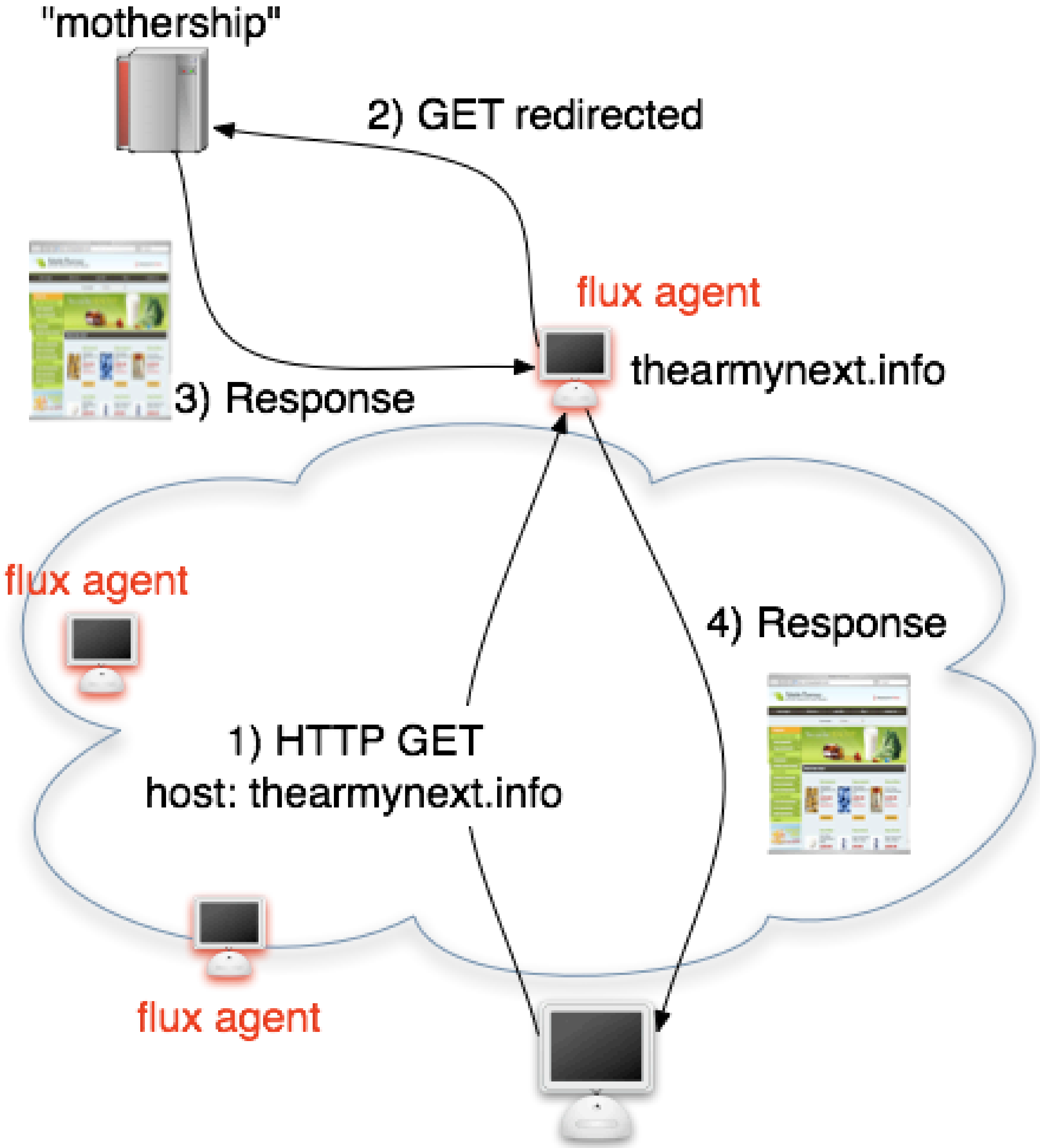
- Given fast-flux domain returns few IP addresses from large pool of compromised machines (“flux agents”)
- After the (low) TTL expired, return different subset

IP address returned in A record	Reverse DNS lookup for IP address	ASN	Country
69.183.26.53	69.183.26.53.adsl.snet.net.	7132	US
76.205.234.131	adsl-76-205-234-131.dsl.hstntx.sbcglobal.net.	7132	US
85.177.96.105	e177096105.adsl.alicedsl.de.	13184	DE
217.129.178.138	ac-217-129-178-138.netvisao.pt.	13156	PT
24.98.252.230	c-24-98-252-230.hsd1.ga.comcast.net.	7725	US

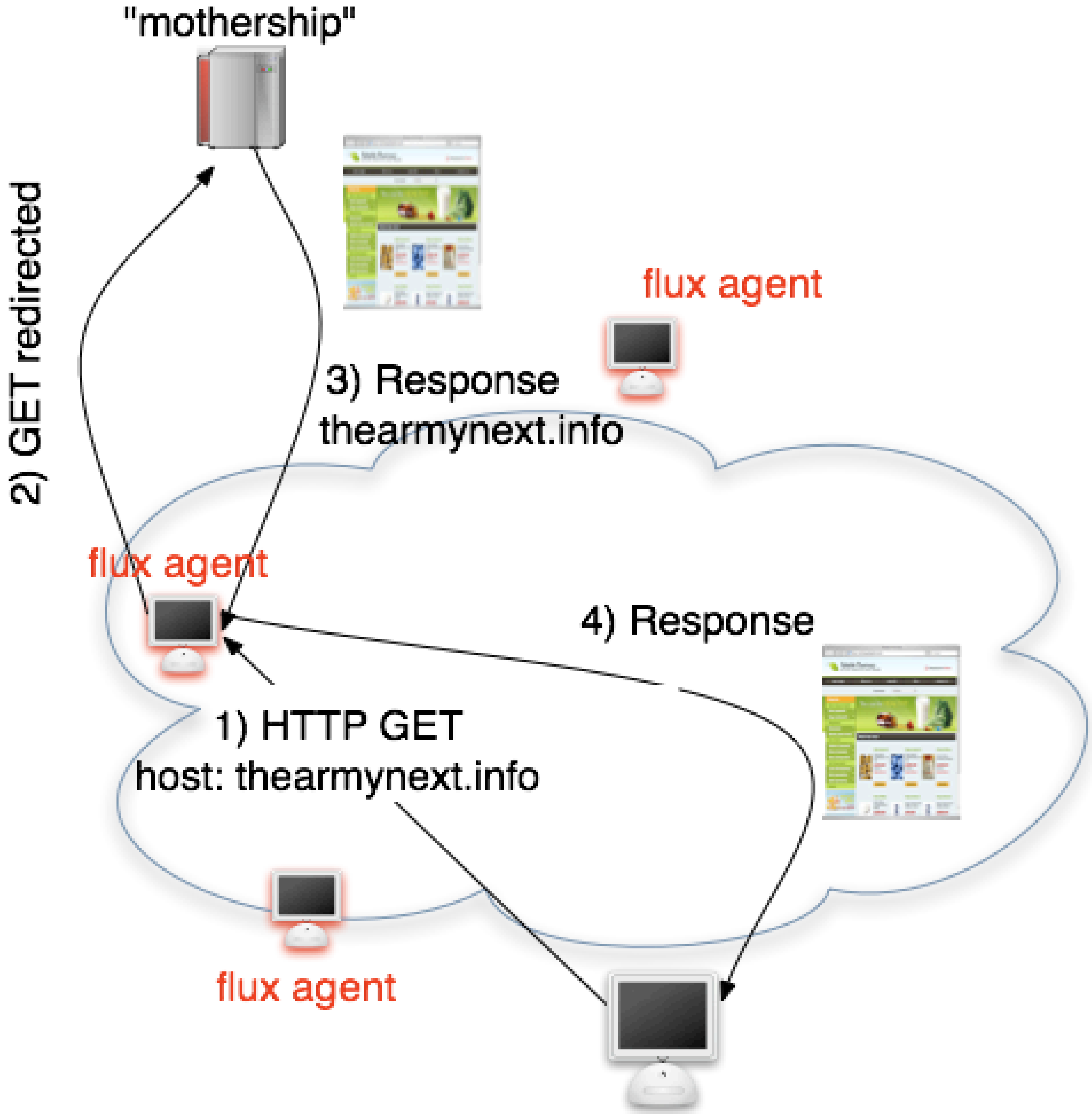
FFSNs



FFSNs

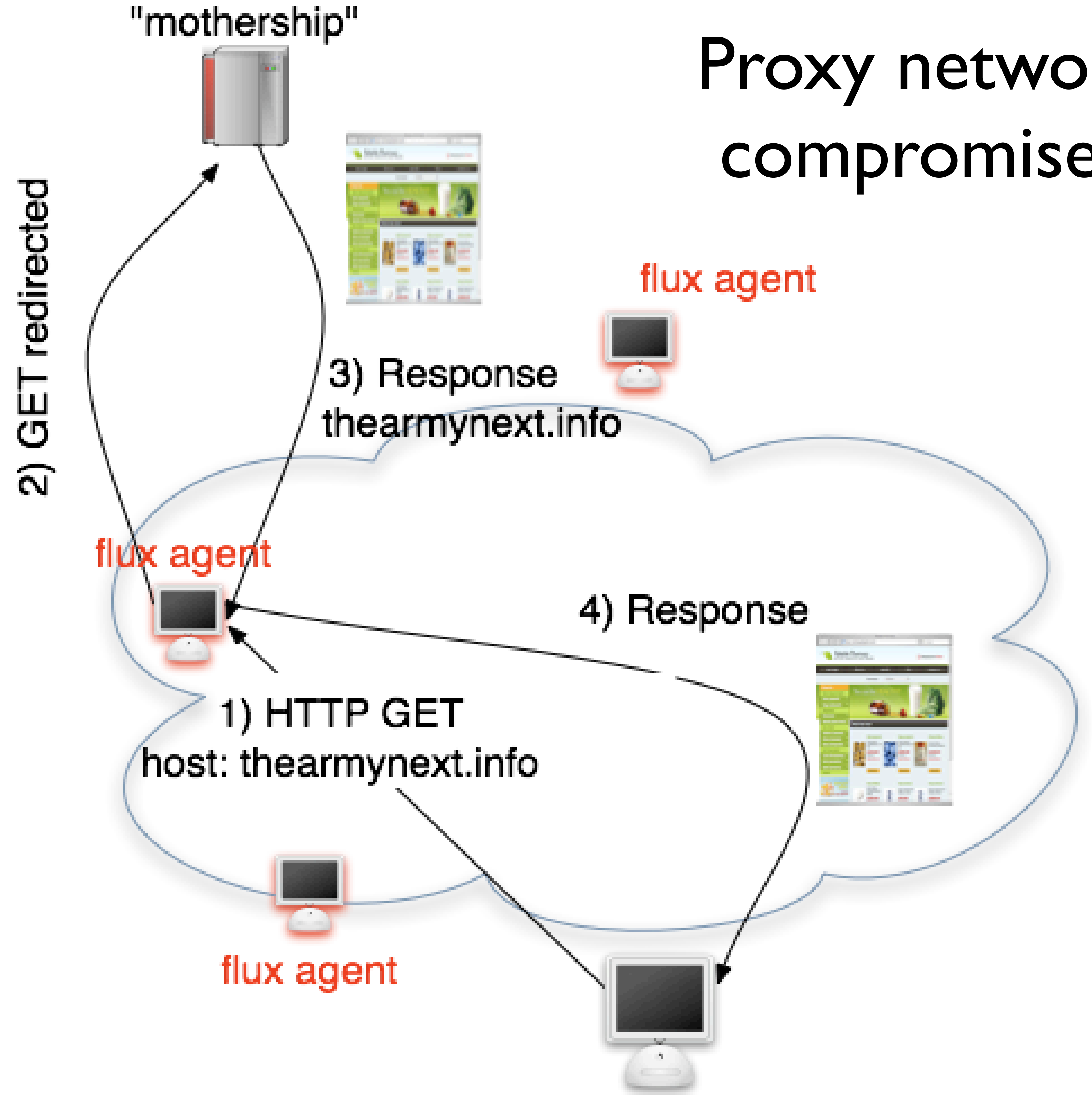

"mothership"
2) GET redirected
flux agent
thearmynext.info
3) Response
flux agent
4) Response
1) HTTP GET
host: thearmynext.info
flux agent

FFSNs


"mothership"
2) GET redirected
3) Response
thearmynext.info
flux agent
flux agent
4) Response
1) HTTP GET
host: thearmynext.info
flux agent

FFSNs

Proxy network on top of compromised machines



Automated Identification

Finding Fast Flux Service Networks

Metric

Metric

- Attacker's restrictions in establishing FFSNs
  - IP address diversity
  - No physical agent control

Metric

- Attacker's restrictions in establishing FFSNs
  - IP address diversity
  - No physical agent control
- Possible distinguishing parameters
  - Number of unique A records n_a in all lookups
  - Number of NS records in single lookup n_{NS}
  - Number of unique ASNs for all A records n_{ASN}

Flux-Score

- Vector x = (n_{A}, n_{NS}, n_{ASN}), weight vector ω
- Linear decision function

$$F(x) = \begin{cases} w^T x - b > 0 & \text{if } x \text{ is a fast-flux domain} \\ w^T x - b \leq 0 & \text{if } x \text{ is a benign domain} \end{cases}$$

- Use corpus of FF and benign domains to derive values for ω and b
- Compute optimal hyperplane
  - Efficient computation with linear programming

Flux-Score

- Obtain scoring metric f

$$f(x) = w^T x = w_1 \cdot n_A + w_2 \cdot n_{ASN} + w_3 \cdot n_{NS}$$

- Instantiate model with weights
  - 128 manually verified FF domains and 5,803 benign domains
  - 10-fold cross validation using different parameters

$$f(x) \quad = \quad 1.32 \cdot n_A + 18.54 \cdot n_{ASN} + 0 \cdot n_{NS}$$

$$\text{with} \;\; b = 142.38$$

detection accuracy 99.98%, standard deviation 0.05%

Empirical Results

Measuring FFSNs in July / August 2007

Scam Hosting

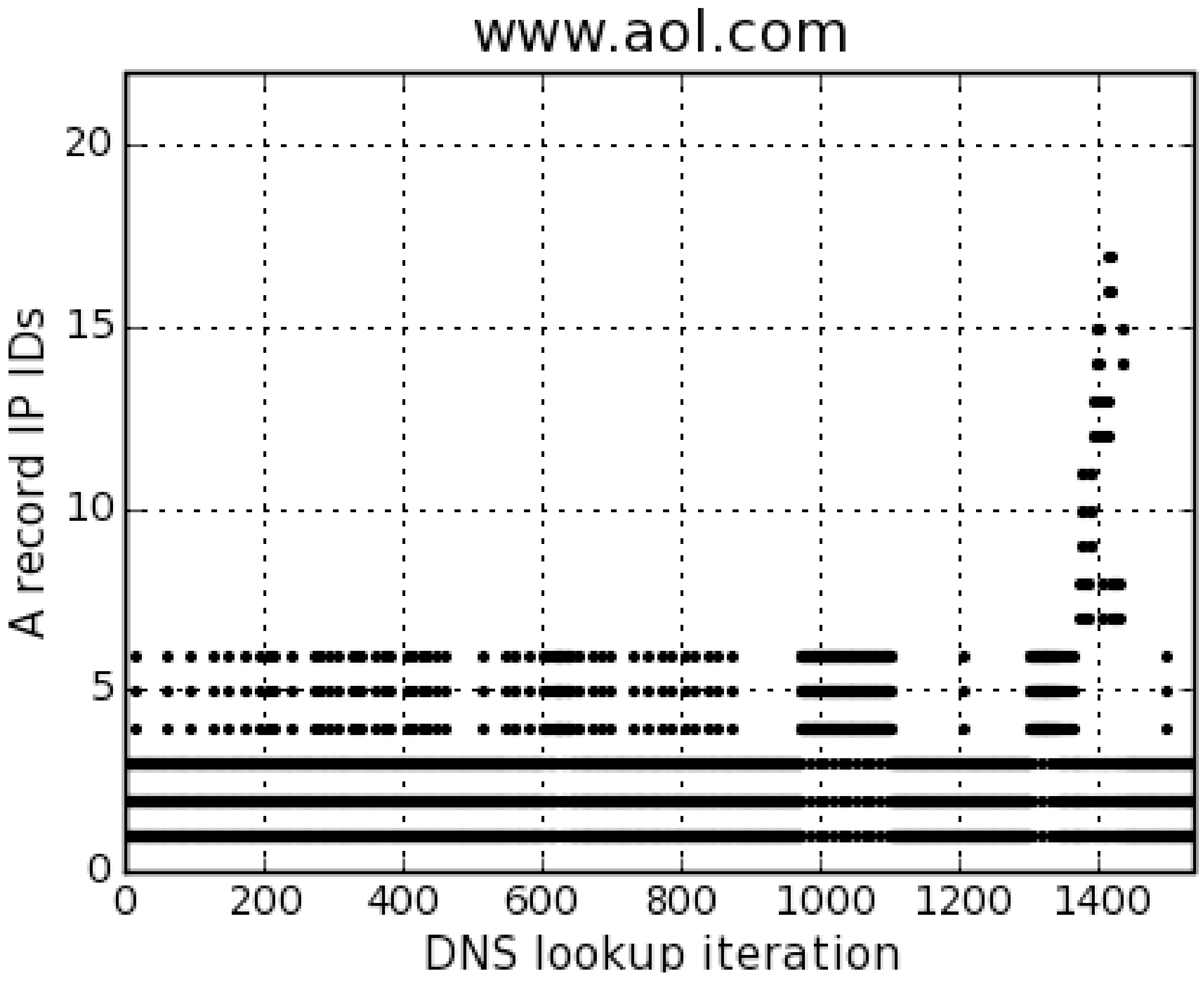
- Spamscatter (USENIX'07, Anderson et al.)
  - No FFSNs identified
  - 6% of scams hosted on multiple IPs (45 IPs max)
- Spamcorpus with 22K mails from August 2007
  - Contained 7,389 unique domains
  - Based on flux-score, 2,197 (29.7%) are FFSNs
    - 563 unique fast-flux domains (w/o wildcards)
    - 1,737 unique IP addresses

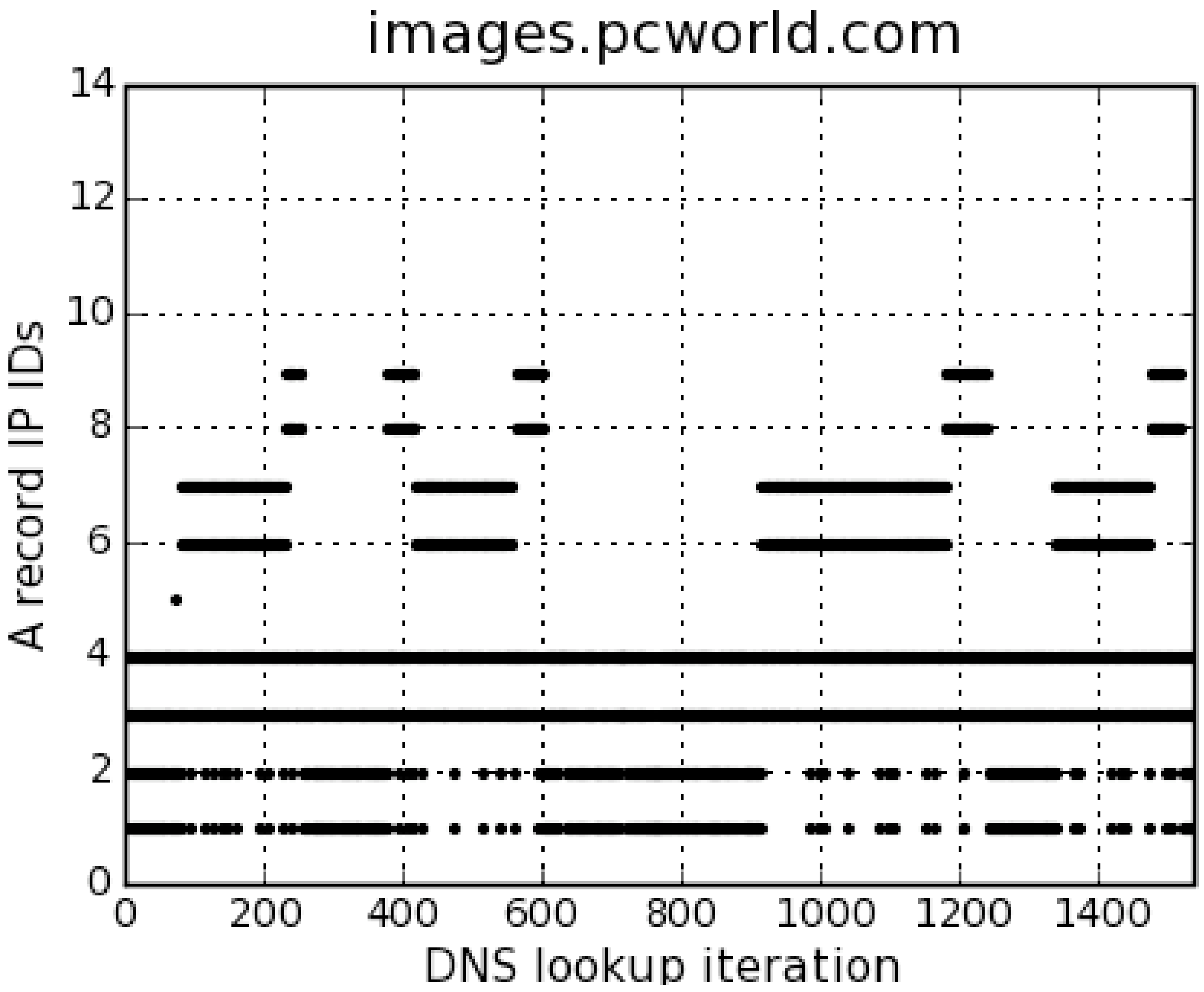
Long-Term

- 33 FFSNs were tracked for 7 weeks every 300s
    - 18,214 unique IP addresses monitored
        - Does not take churn by DHCP into account
        - NAT is no problem since machines need to be reachable
    - 818 unique AS (43.3% in top 10 AS)

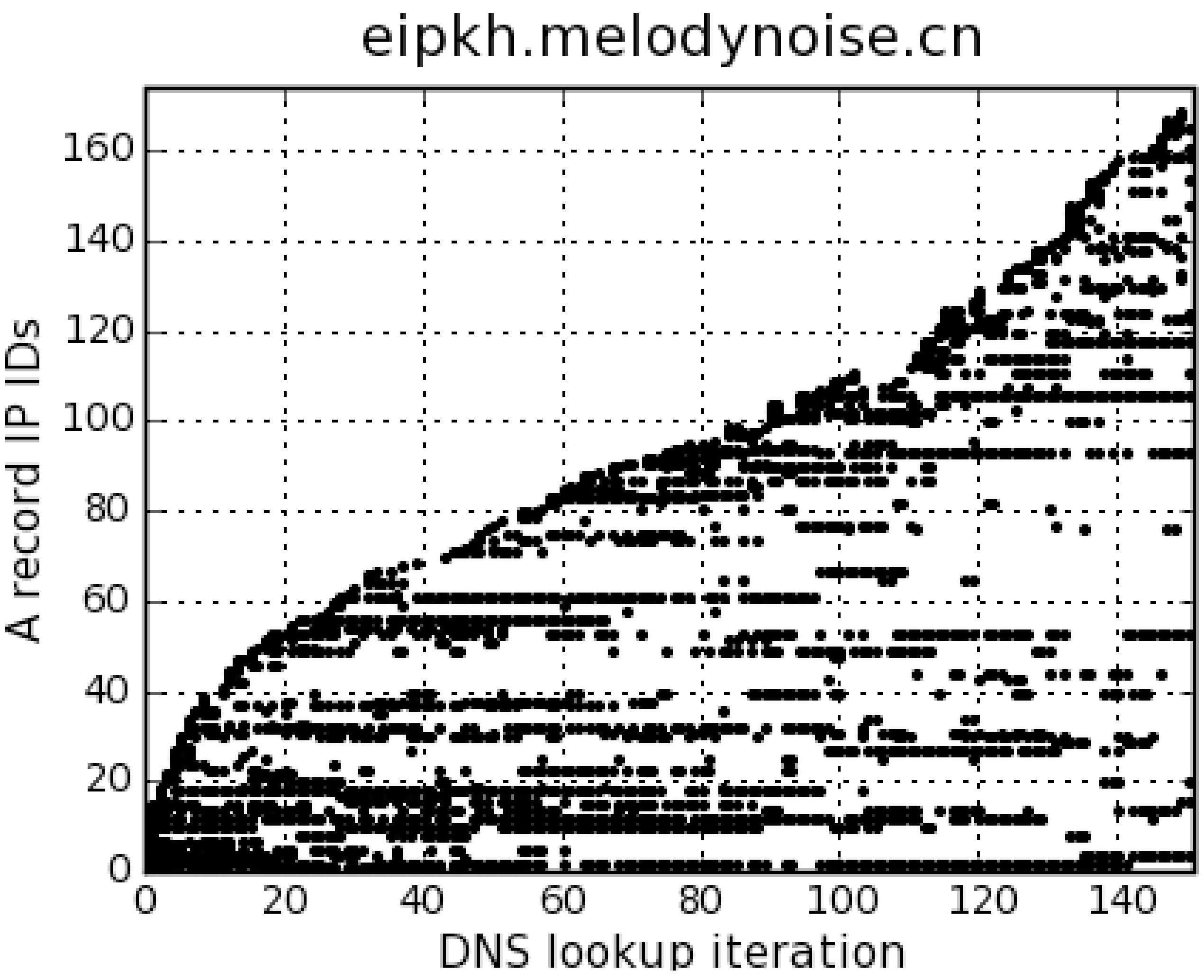
1)	7132	(AT&T Internet Services, US)	2,677	2)	9304	(Hutchison Global, HK)	1,797
3)	4766	(Korea Telecom, KR)	590	4)	3320	(Deutsche Telekom, DE)	500
5)	8551	(Bezeqint Internet, IL)	445	6)	12322	(Proxad/Free ISP, FR)	418
7)	8402	(Corbina telecom, RU)	397	8)	1680	(NetVision Ltd., US)	361

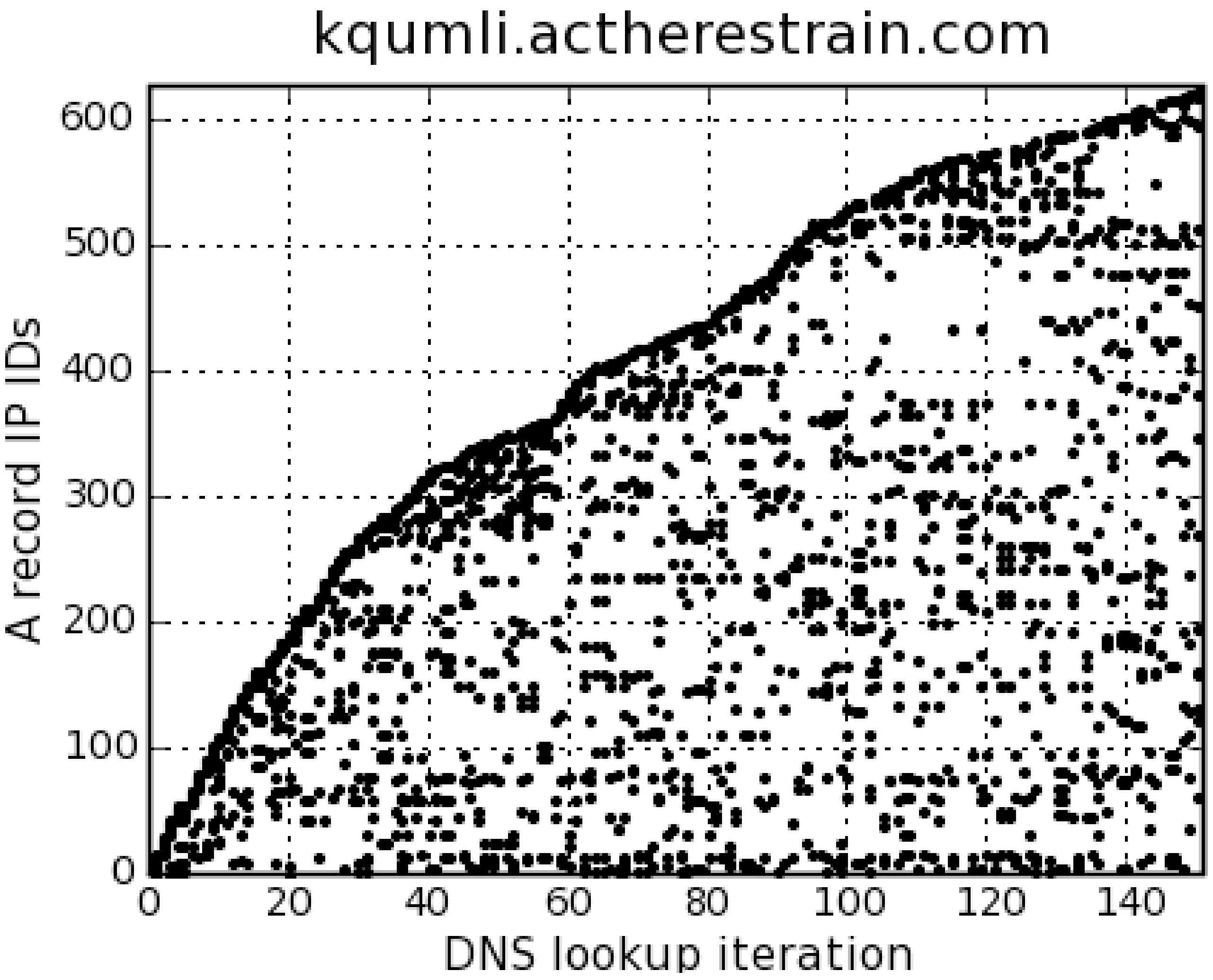
Diversity


www.aol.com
A record IP IDs
0
5
10
15
20
0
200
400
600
800
1000
1200
1400
DNS lookup iteration

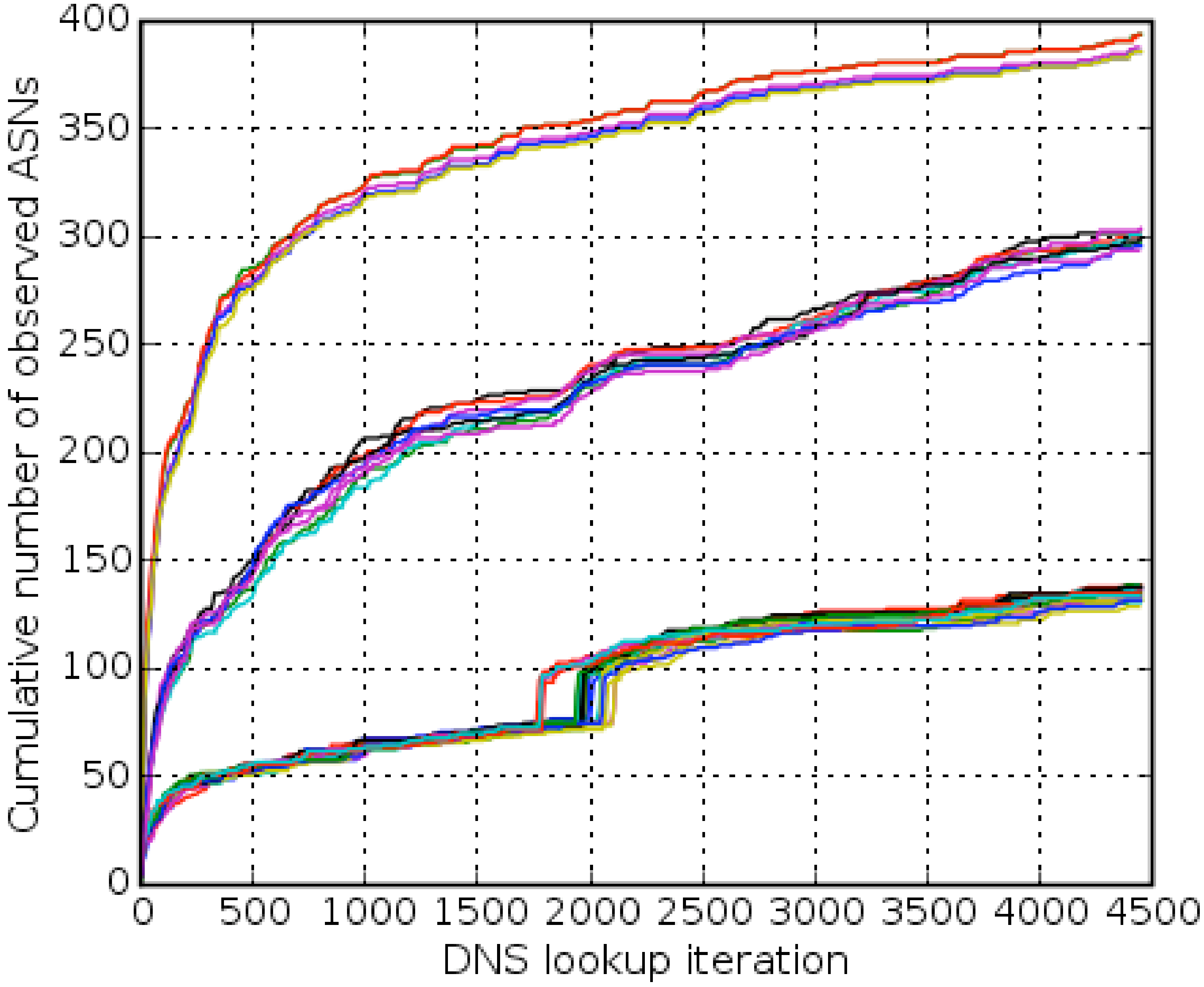

images.pcworld.com
A record IP IDs
0
2
4
6
8
10
12
14
0
200
400
600
800
1000
1200
1400
DNS lookup iteration

Diversity


eipkh.melodynoise.cn
A record IP IDs
0
20
40
60
80
100
120
140
160
0
20
40
60
80
100
120
140
DNS lookup iteration


kqumli.actherestrain.com
A record IP IDs
0
100
200
300
400
500
600
0
20
40
60
80
100
120
140
DNS lookup iteration

Long-Term



Cumulative number of distinct ASNs observed for 33 FFSNs (15 days)

Other Abuses

- Storm Worm uses fast changing DNS entries to host web site with malware binary
  - Observed more than 50K IP addresses in four week period
- Rock Phish, a large phishing group, uses FFSNs to host phishing site
  - Observed 1,121 unique IP addresses in 4 days
- FFSNs could be used to host IRC, SMTP, ...

Mitigation

Stopping the Threat

Mitigation

- Domain blacklist
  - Collaboration with registrar / monitoring DNS
  - Content-based spam filtering
- Identifying control node
  - Tracing in proxy network is hard
  - Mark specific request and trace it through network (needs ISP collaboration)

Conclusion

- First empirical study of FFSNs, a new and emerging threat
- Developed a metric to automatically identify fast-flux domains
- Empirical measurement results
- Future work
  - Improve flux-score
  - Estimate size of FFSN based on capture-recapture methods

Thorsten Holz

http://pi1.informatik.uni-mannheim.de/
thorsten.holz@informatik.uni-mannheim.de

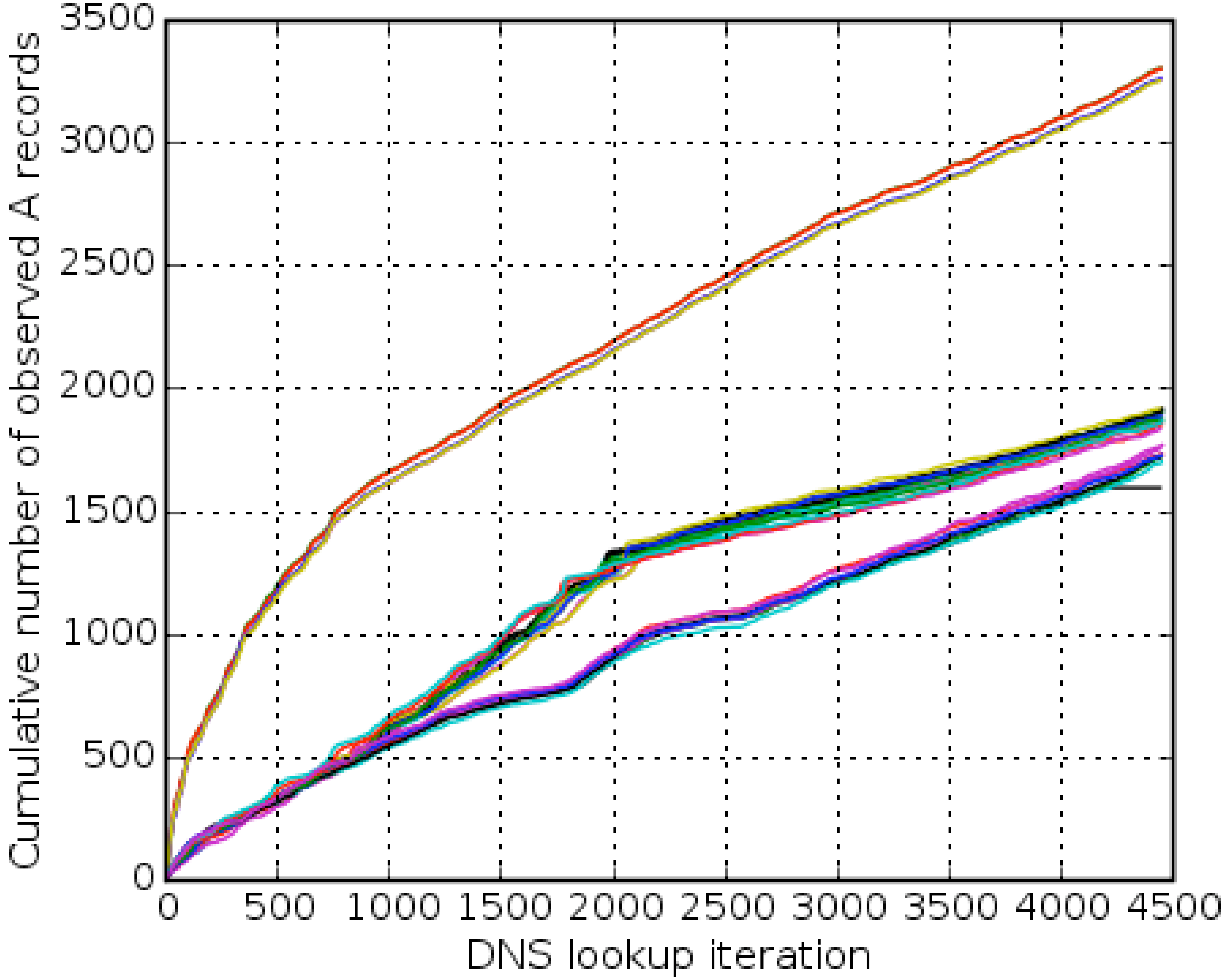
Acknowledgments:
Thanks to anonymous reviewers and Fabian Monrose

Data available:
http://pi1.informatik.uni-mannheim.de/fast-flux

Fluxiness

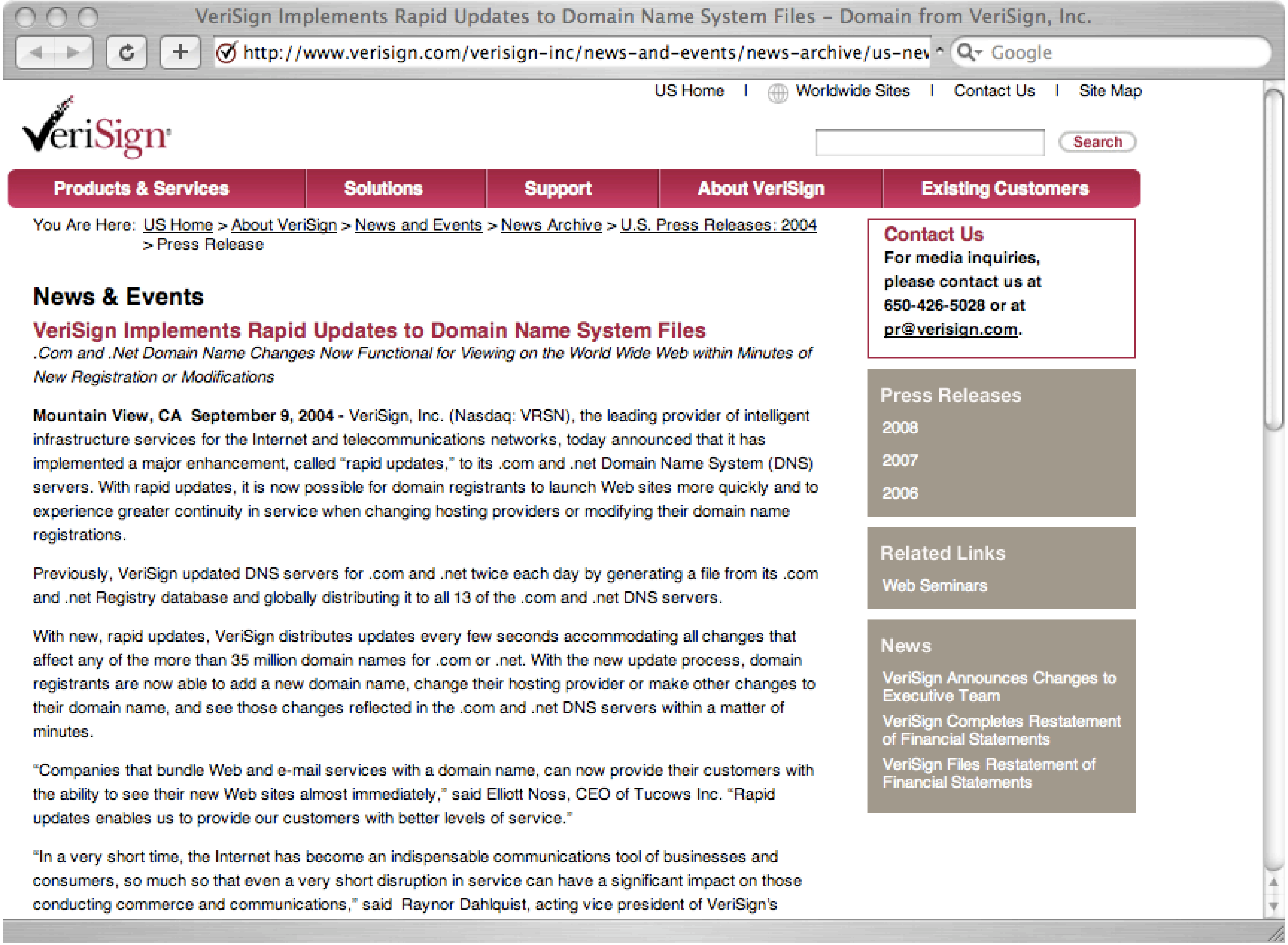
- Metric to distinguish FFSNs from benign domains can be defined as function of n_a, n_{NS}, and n_{ASN}
- Fluxiness: $\varphi = n_a / n_{single}$
  - n_{single} is number of A records in single lookup
  - $\varphi = 1.0$: constant set of A records returned
  - $\varphi = 2.0$ in previous example
  - Implicitly contained in n_A and n_{ASN}

Long-Term



Cumulative number of distinct A records observed for 33 FFSNs (15 days)

Updates


VeriSign Implements Rapid Updates to Domain Name System Files – Domain from VeriSign, Inc.
http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-nev
Google
US Home | Worldwide Sites | Contact Us | Site Map
VeriSign
Search
Products & Services
Solutions
Support
About VeriSign
Existing Customers

You Are Here: US Home > About VeriSign > News and Events > News Archive > U.S. Press Releases: 2004 > Press Release

News & Events

VeriSign Implements Rapid Updates to Domain Name System Files

.Com and .Net Domain Name Changes Now Functional for Viewing on the World Wide Web within Minutes of New Registration or Modifications

Mountain View, CA September 9, 2004 - VeriSign, Inc. (Nasdaq: VRSN), the leading provider of intelligent infrastructure services for the Internet and telecommunications networks, today announced that it has implemented a major enhancement, called "rapid updates," to its .com and .net Domain Name System (DNS) servers. With rapid updates, it is now possible for domain registrants to launch Web sites more quickly and to experience greater continuity in service when changing hosting providers or modifying their domain name registrations.

Previously, VeriSign updated DNS servers for .com and .net twice each day by generating a file from its .com and .net Registry database and globally distributing it to all 13 of the .com and .net DNS servers.

With new, rapid updates, VeriSign distributes updates every few seconds accommodating all changes that affect any of the more than 35 million domain names for .com or .net. With the new update process, domain registrants are now able to add a new domain name, change their hosting provider or make other changes to their domain name, and see those changes reflected in the .com and .net DNS servers within a matter of minutes.

"Companies that bundle Web and e-mail services with a domain name, can now provide their customers with the ability to see their new Web sites almost immediately," said Elliott Noss, CEO of Tucows Inc. "Rapid updates enables us to provide our customers with better levels of service."

"In a very short time, the Internet has become an indispensable communications tool of businesses and consumers, so much so that even a very short disruption in service can have a significant impact on those conducting commerce and communications," said Raynor Dahlquist, acting vice president of VeriSign's

Contact Us
For media inquiries, please contact us at 650-426-5028 or at pr@verisign.com.

Press Releases
2008
2007
2006

Related Links
Web Seminars

News
VeriSign Announces Changes to Executive Team
VeriSign Completes Restatement of Financial Statements
VeriSign Files Restatement of Financial Statements