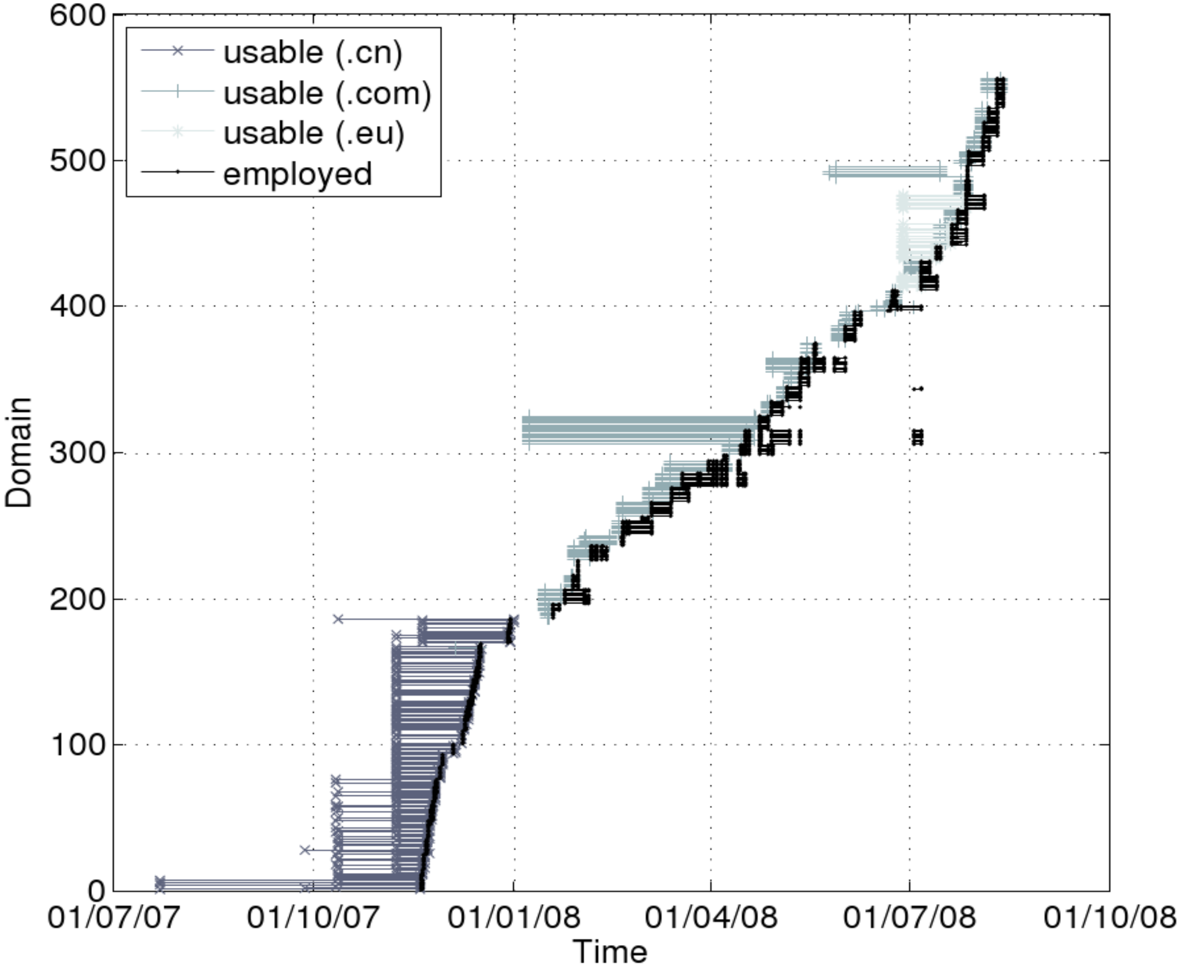
On the Potential of Proactive Domain Blacklisting

Márk Félegyházi, Christian Kreibich and Vern Paxson

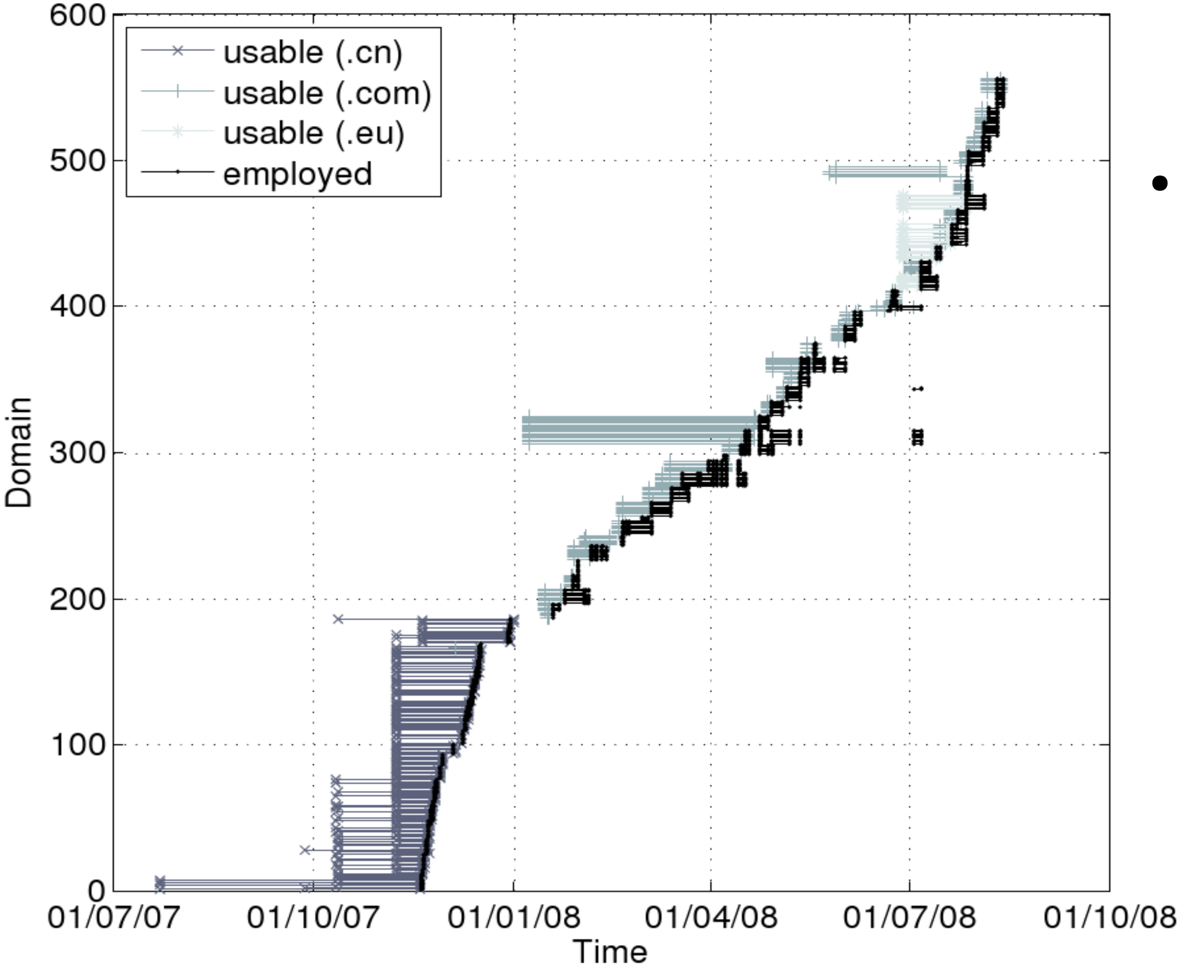
ICSI, Berkeley

Spam domain registrations



Kreibich et al., “Spamcraft: An inside look at spam campaign orchestration” LEET 2009
(CCIED: The Collaborative Center for Internet Epidemiology and Defenses)

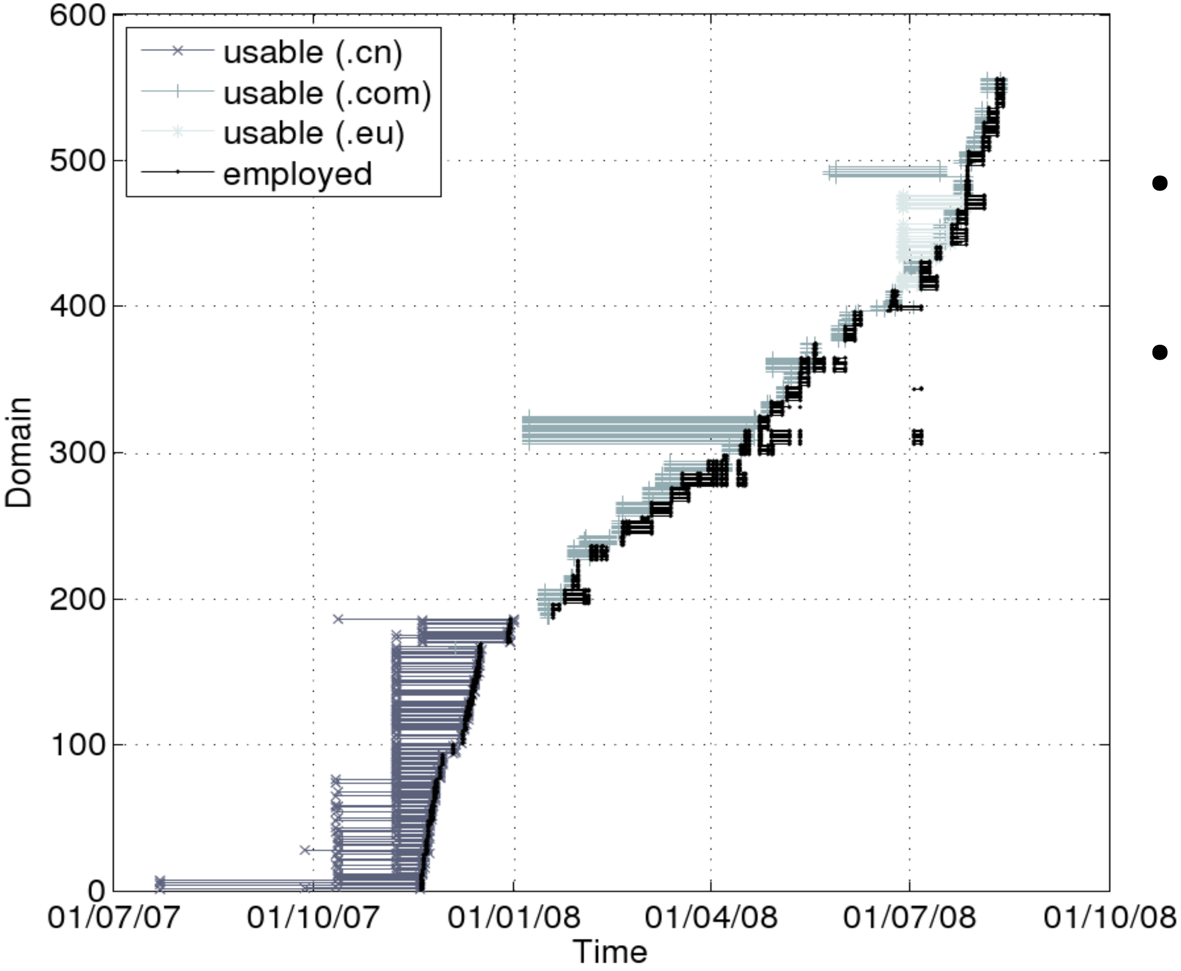
Spam domain registrations



- domains dropped soon after blacklisted

Kreibich et al., “Spamcraft: An inside look at spam campaign orchestration” LEET 2009
(CCIED: The Collaborative Center for Internet Epidemiology and Defenses)

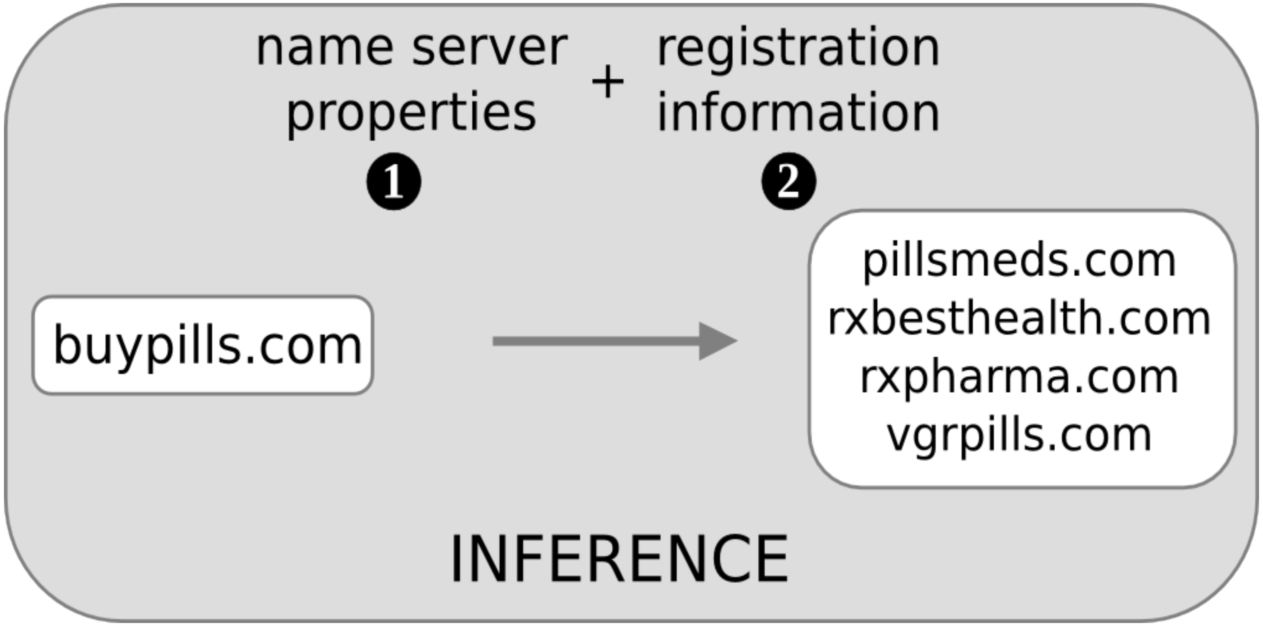
Spam domain registrations



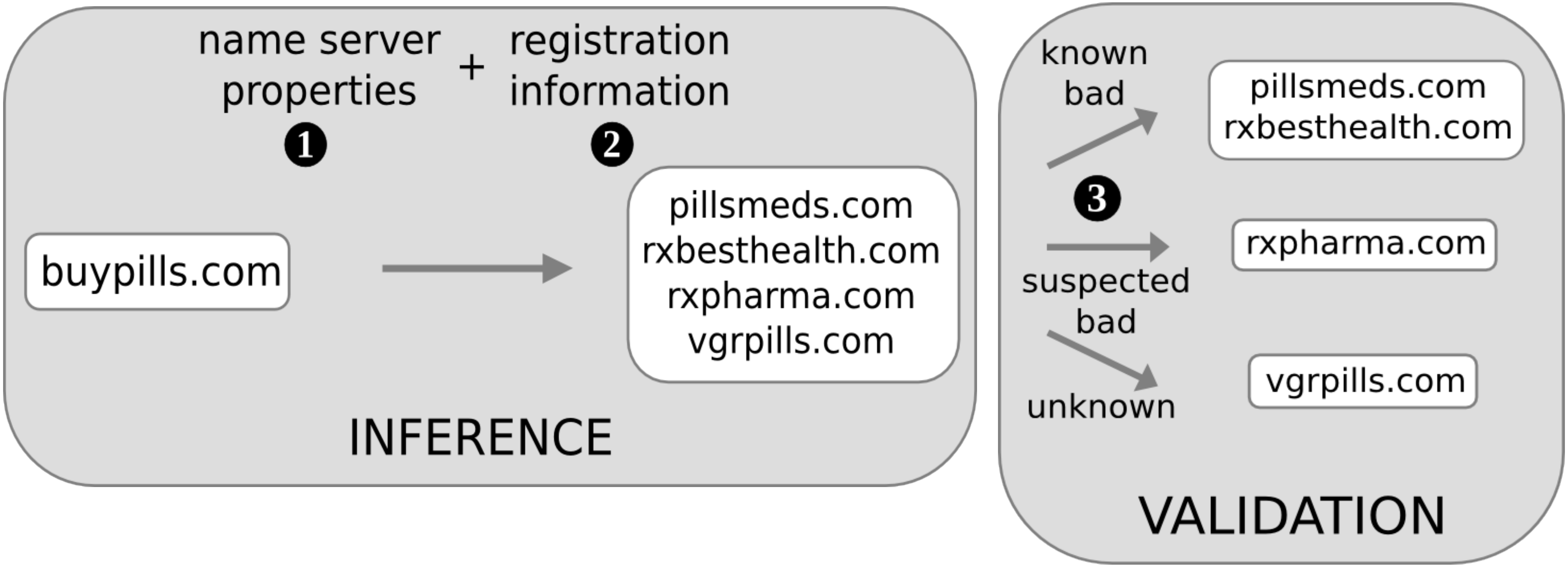
- domains dropped soon after blacklisted
- domains registered in batches

Kreibich et al., “Spamcraft: An inside look at spam campaign orchestration” LEET 2009
(CCIED: The Collaborative Center for Internet Epidemiology and Defenses)

Proactive domain clustering



Proactive domain clustering



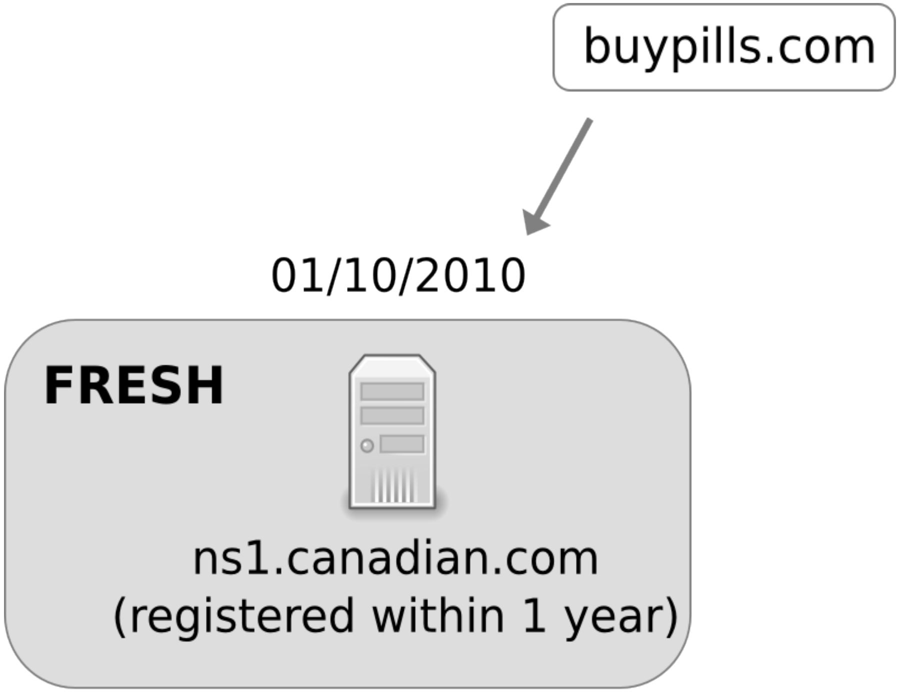
Name server features

.COM zone file - NS records

buypills.com

Name server features

.COM zone file - NS records



buypills.com

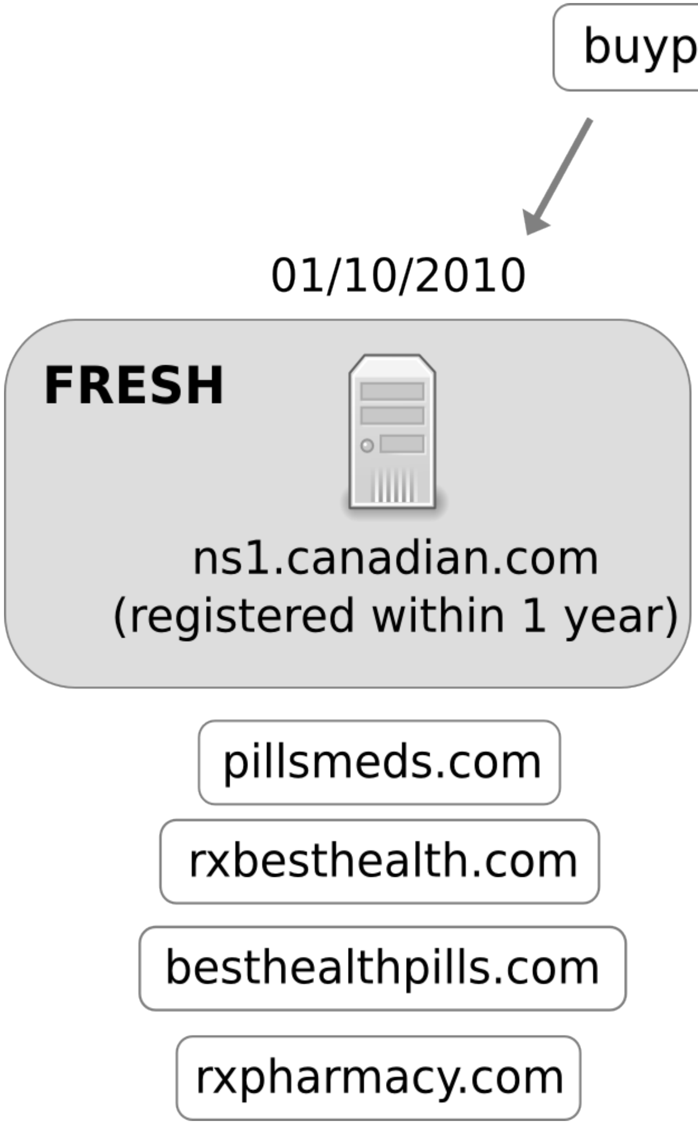
01/10/2010

FRESH

ns1.canadian.com
(registered within 1 year)

Name server features

.COM zone file - NS records



buypills.com

01/10/2010

FRESH

ns1.canadian.com
(registered within 1 year)

pillsmeds.com

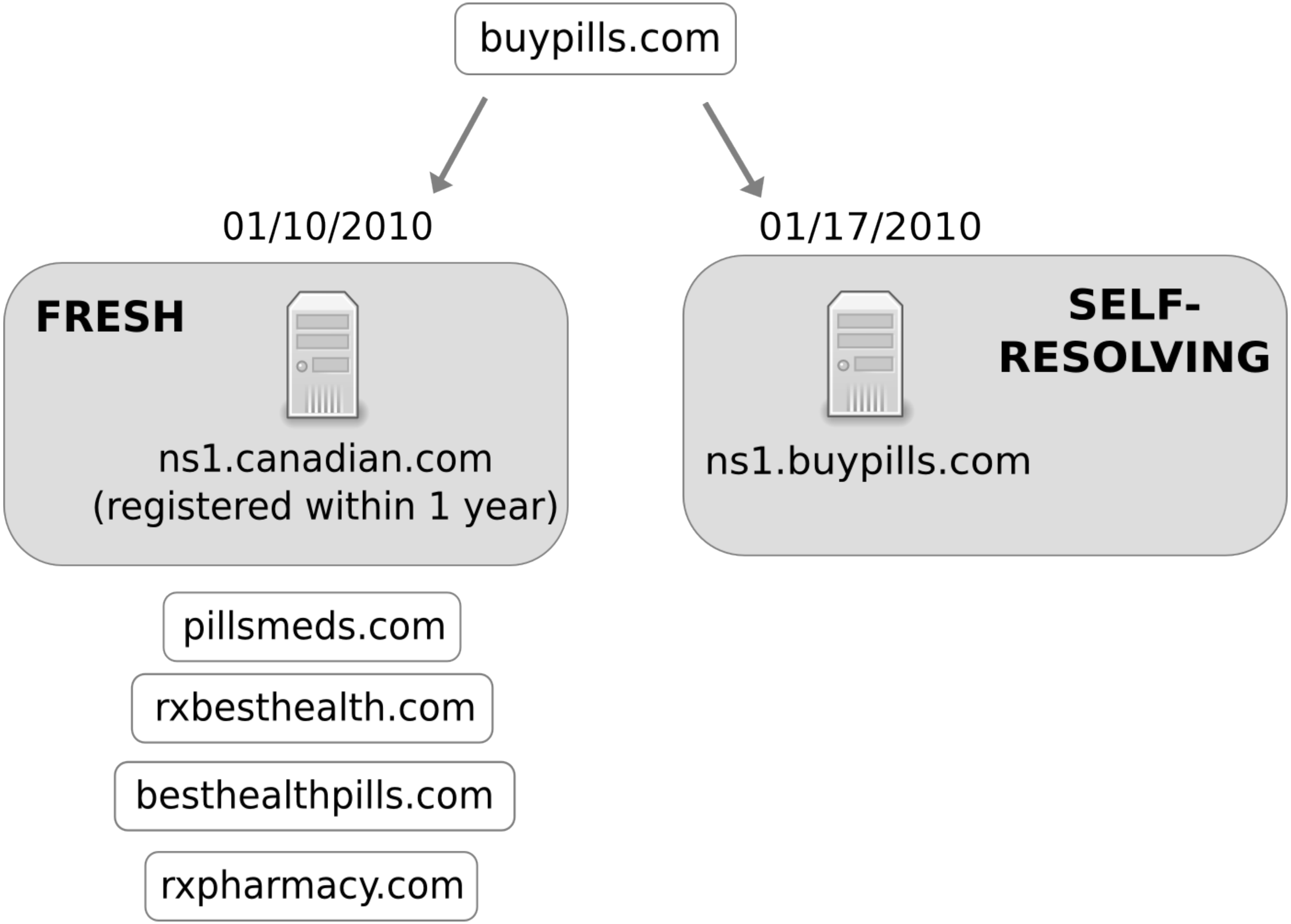
rxbesthealth.com

besthealthpills.com

rxpharmacy.com

Name server features

.COM zone file - NS records



buypills.com

01/10/2010

FRESH

ns1.canadian.com
(registered within 1 year)

pillsmeds.com

rxbesthealth.com

besthealthpills.com

rxpharmacy.com

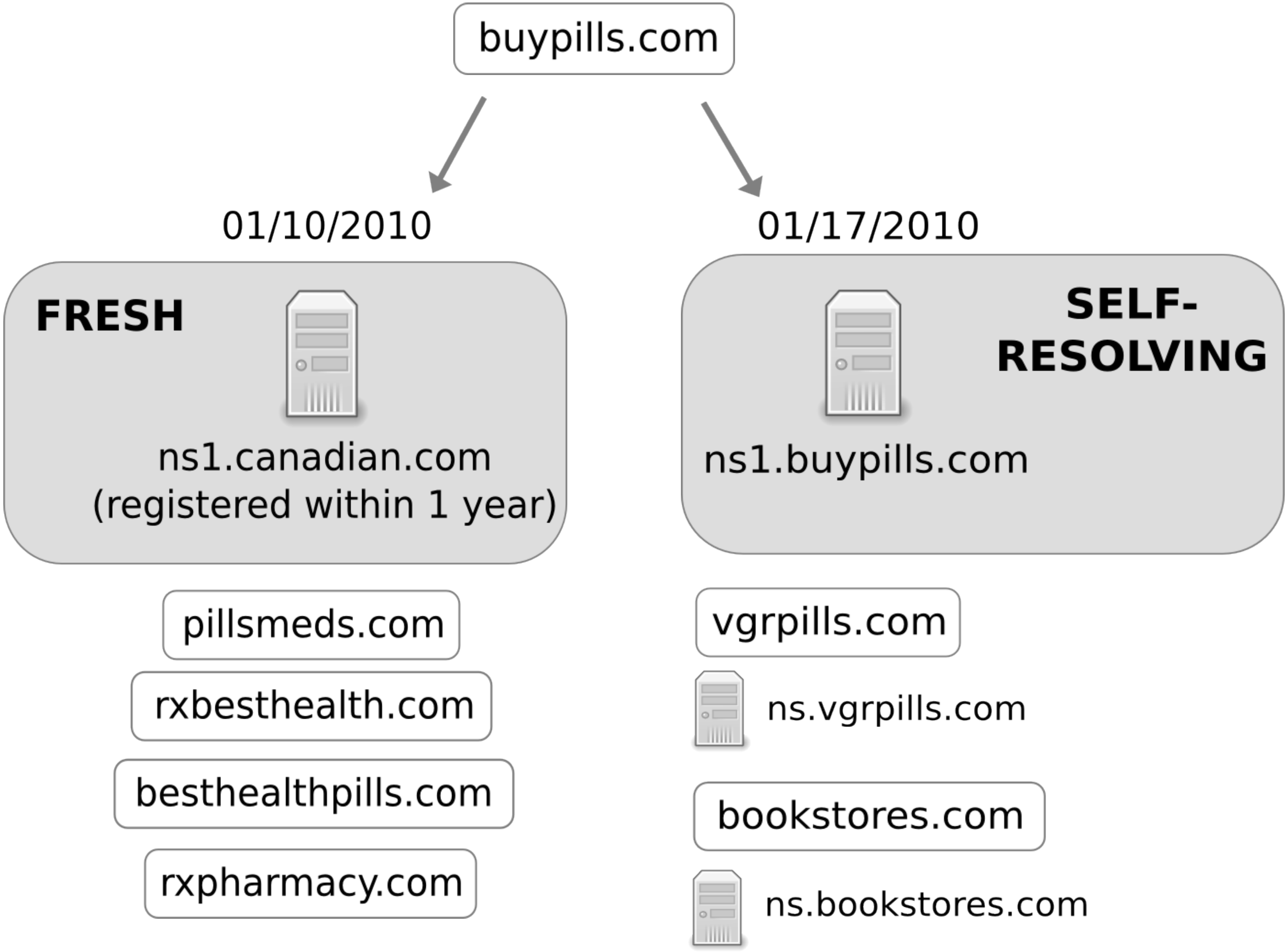
01/17/2010

SELF-RESOLVING

ns1.buypills.com

Name server features

.COM zone file - NS records



Registration features

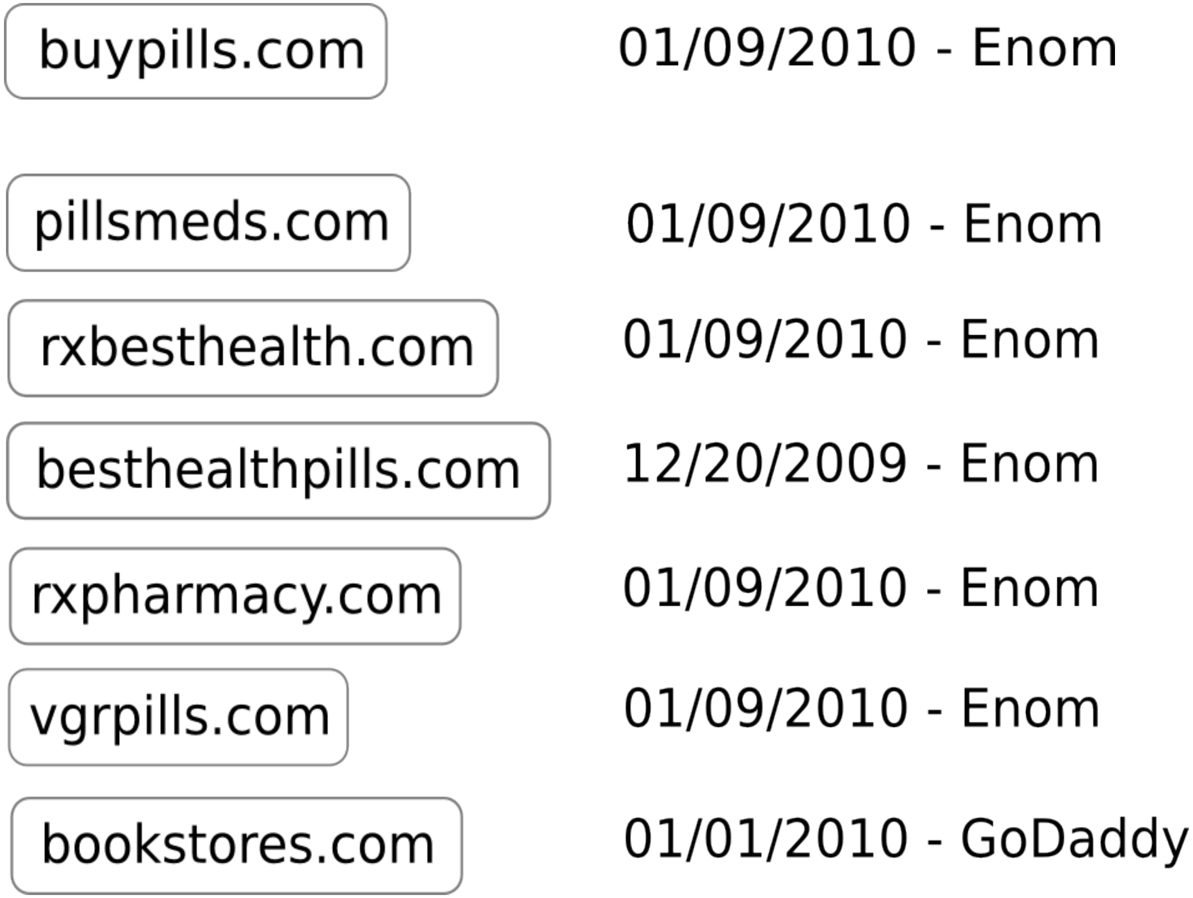
WHOIS registry records

buypills.com

01/09/2010 - Enom

Registration features

WHOIS registry records



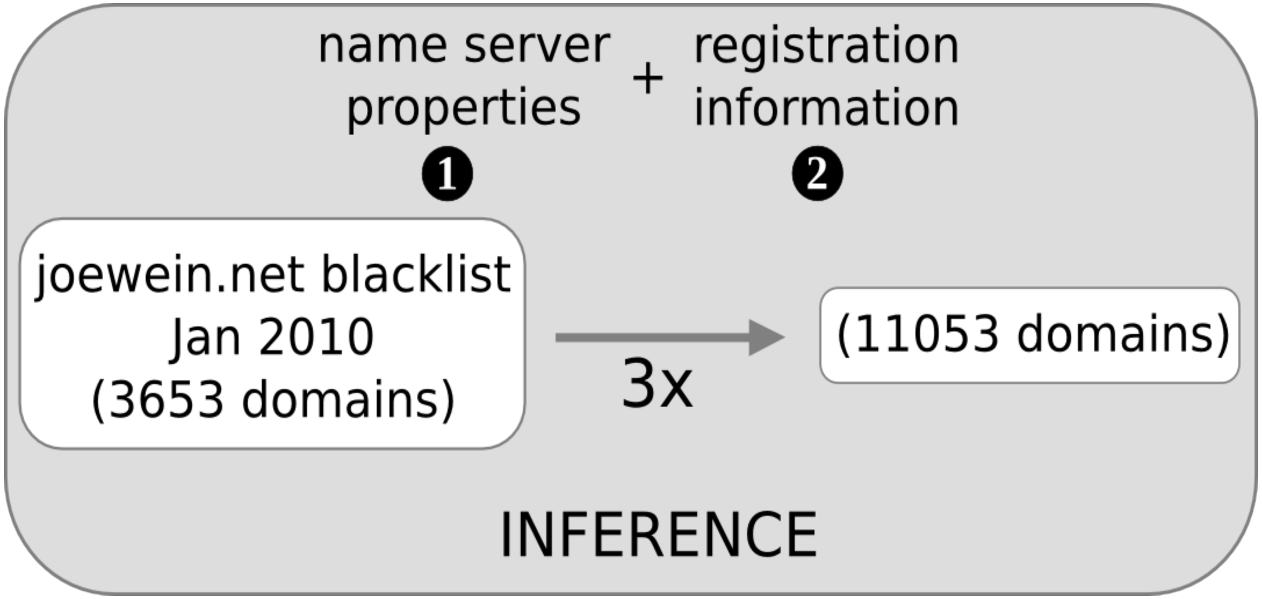
buypills.com	01/09/2010 - Enom
pillsmeds.com	01/09/2010 - Enom
rxbesthealth.com	01/09/2010 - Enom
besthealthpills.com	12/20/2009 - Enom
rxpharmacy.com	01/09/2010 - Enom
vgrpills.com	01/09/2010 - Enom
bookstores.com	01/01/2010 - GoDaddy

Registration features

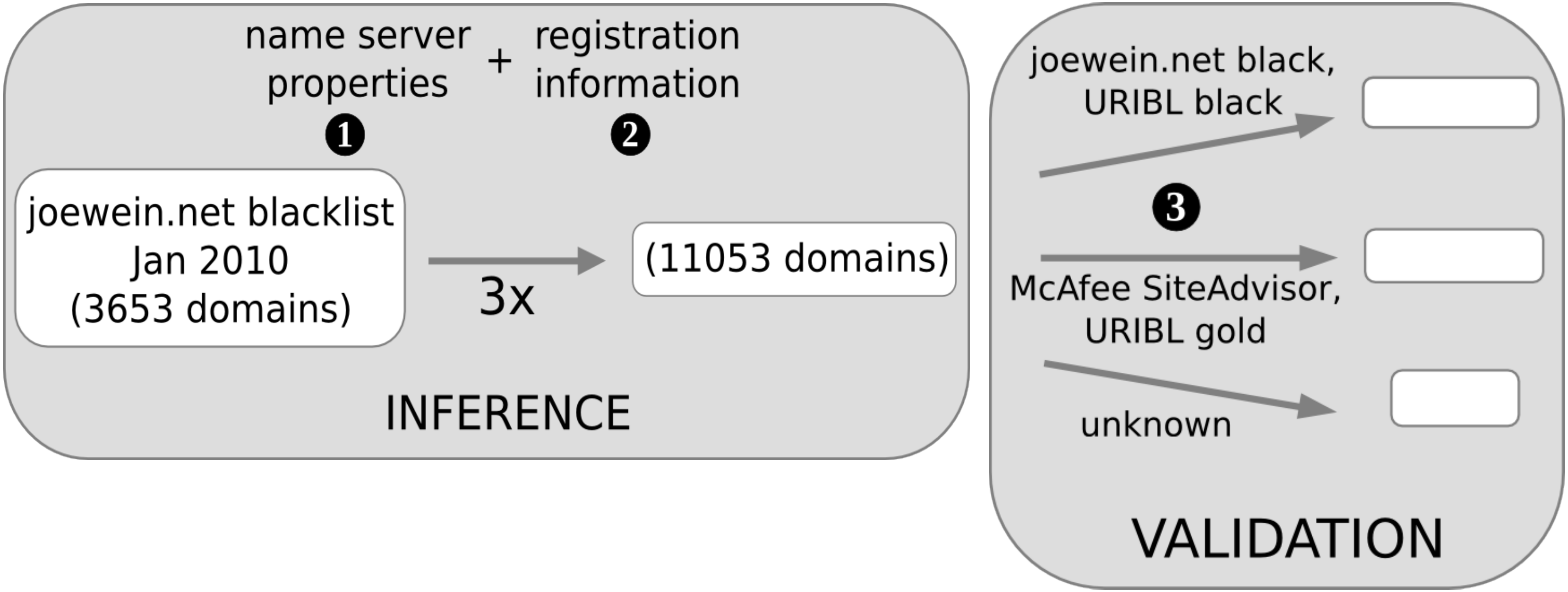
WHOIS registry records

buypills.com	01/09/2010 - Enom
pillsmeds.com	01/09/2010 - Enom
rxbesthealth.com	01/09/2010 - Enom
besthealthpills.com	12/20/2009 - Enom
rxpharmacy.com	01/09/2010 - Enom
vgrpills.com	01/09/2010 - Enom
bookstores.com	01/01/2010 - GoDaddy

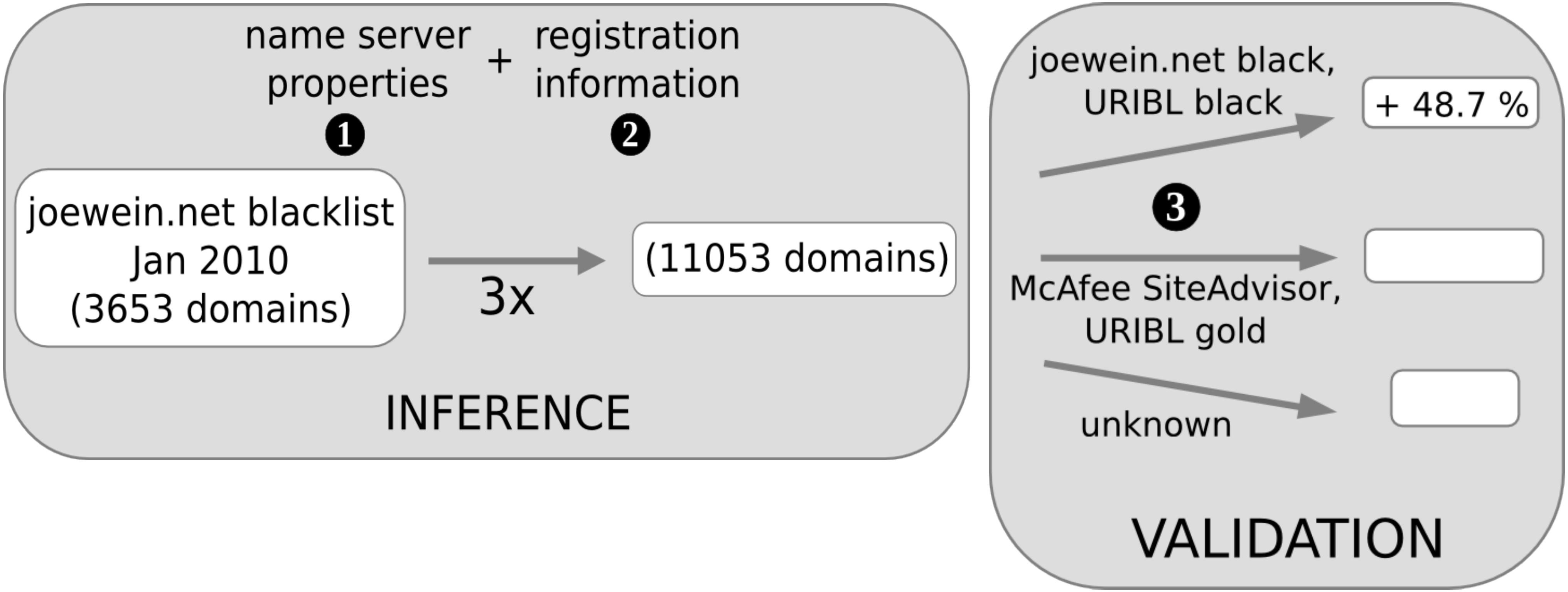
Evaluation


name server properties
+
registration information
1
2
joewein.net blacklist Jan 2010 (3653 domains)
3x
(11053 domains)
INFERENCE

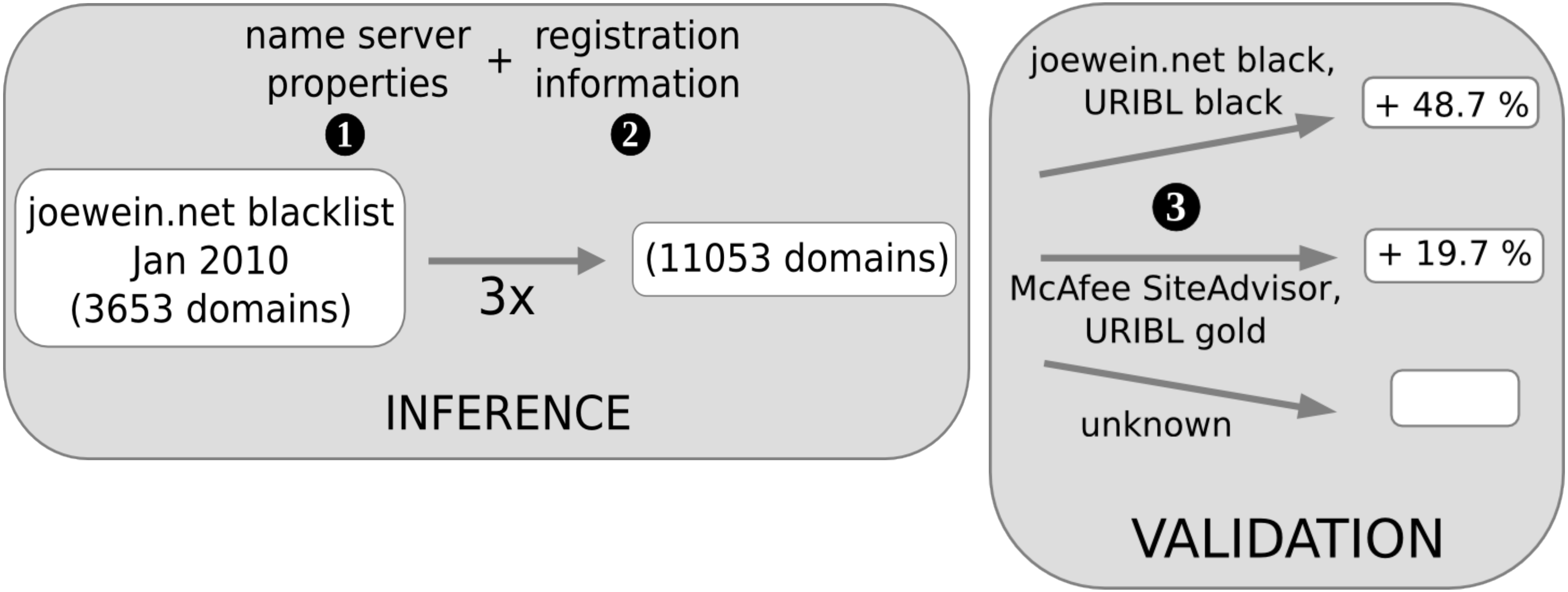
Evaluation


name server properties
+
registration information
❶
❷
joewein.net blacklist
Jan 2010
(3653 domains)
3x
(11053 domains)
INFERENCE
joewein.net black,
URIBL black
❸
McAfee SiteAdvisor,
URIBL gold
unknown
VALIDATION

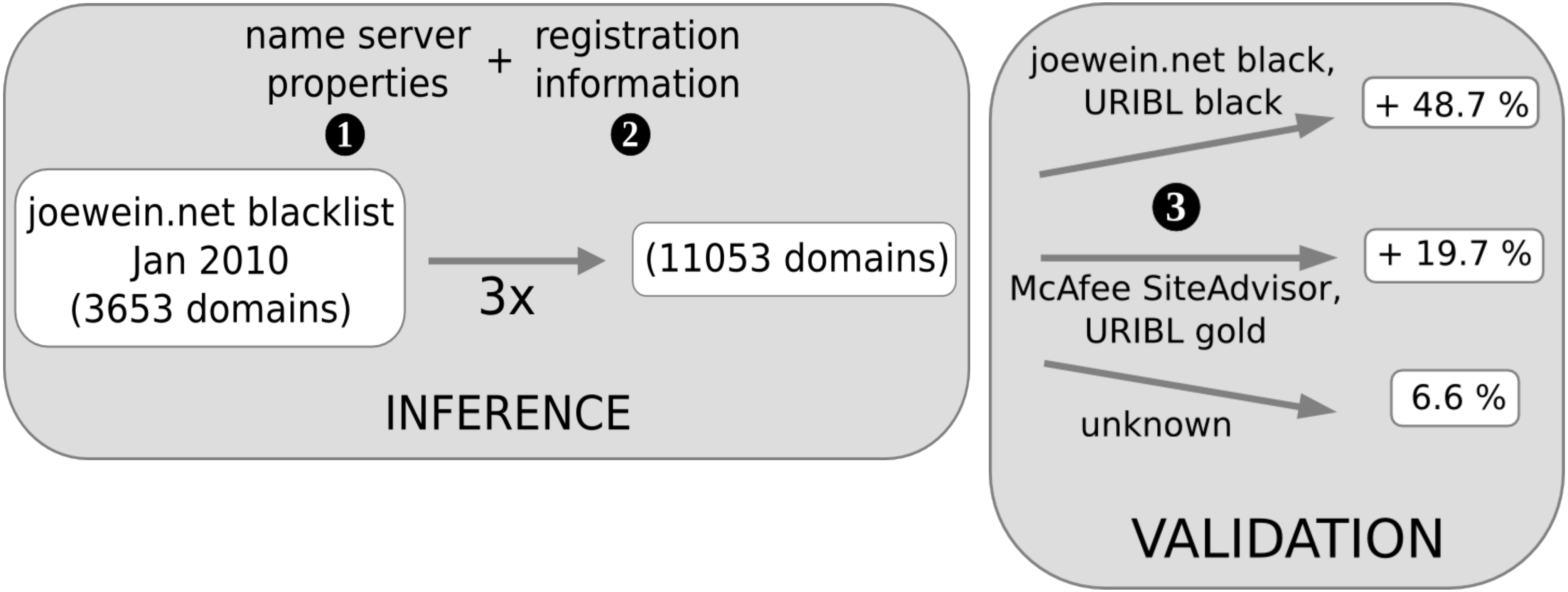
Evaluation


name server properties
+
registration information
❶
❷
joewein.net blacklist Jan 2010 (3653 domains)
3x
(11053 domains)
INFERENCE
joewein.net black, URIBL black
+ 48.7 %
❸
McAfee SiteAdvisor, URIBL gold
unknown
VALIDATION

Evaluation


name server properties
+
registration information
❶
❷
joewein.net blacklist Jan 2010 (3653 domains)
3x
(11053 domains)
INFERENCE
joewein.net black, URIBL black
+ 48.7 %
❸
+ 19.7 %
McAfee SiteAdvisor, URIBL gold
unknown
VALIDATION

Evaluation



name server properties + registration information

❶ ❷

joewein.net blacklist Jan 2010 (3653 domains)

3x

(11053 domains)

INFERENCE

joewein.net black, URIBL black

+ 48.7 %

❸

+ 19.7 %

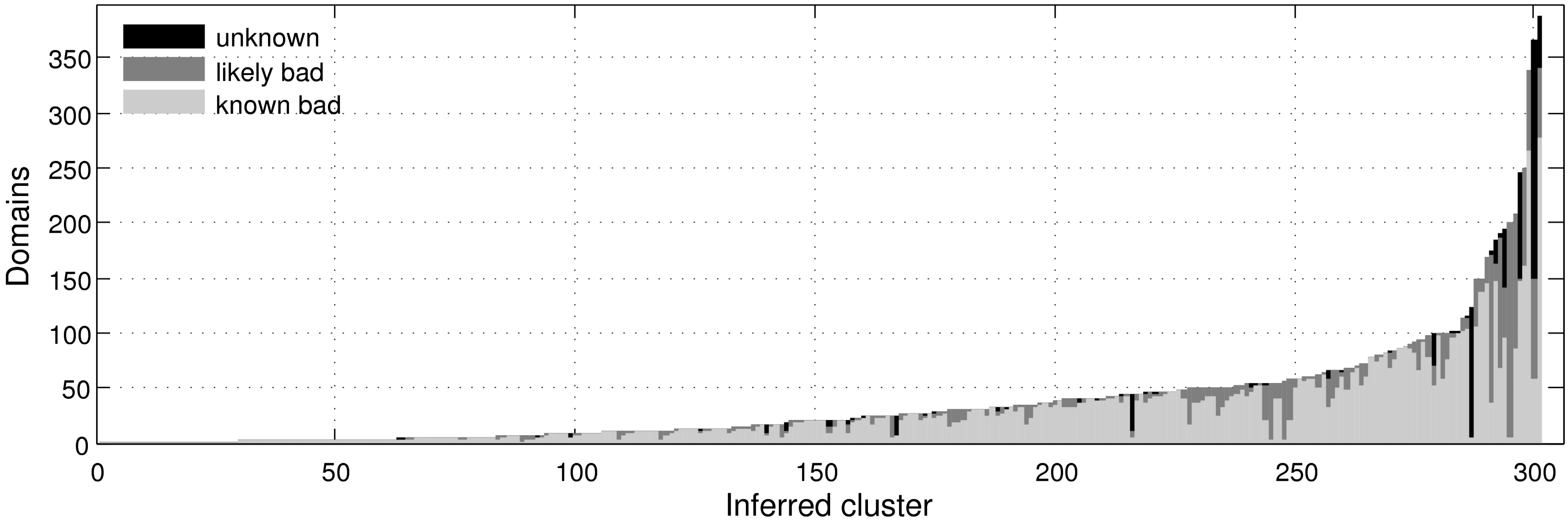
McAfee SiteAdvisor, URIBL gold

unknown

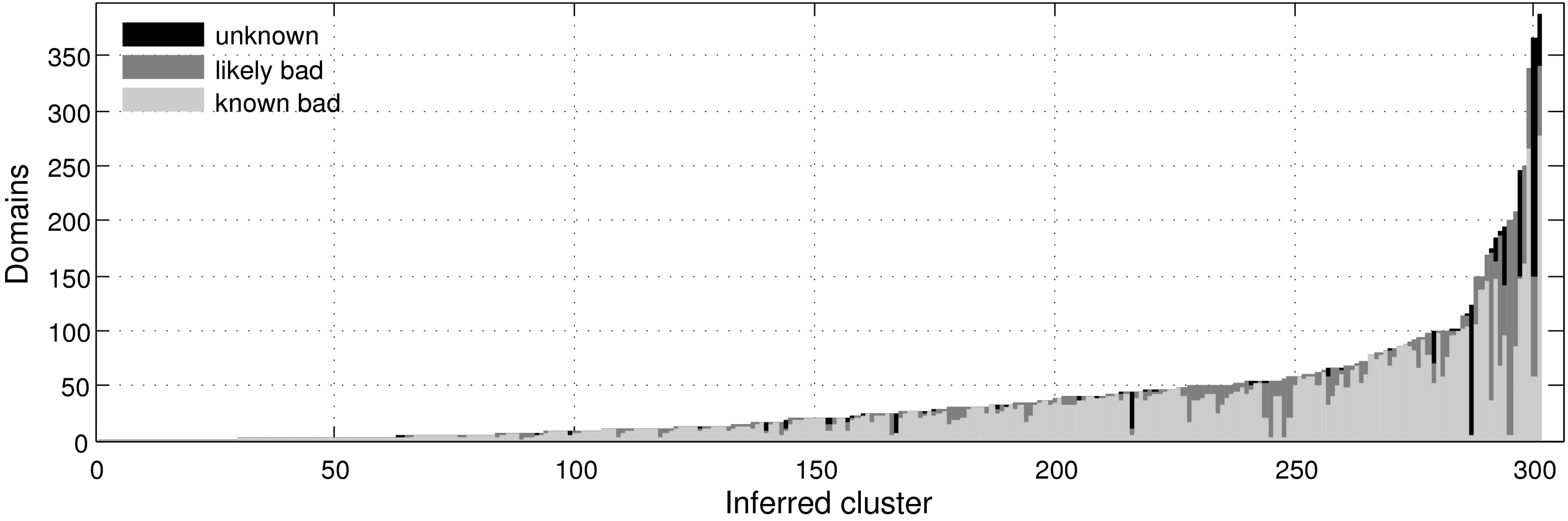
6.6 %

VALIDATION

Prediction accuracy



Prediction accuracy



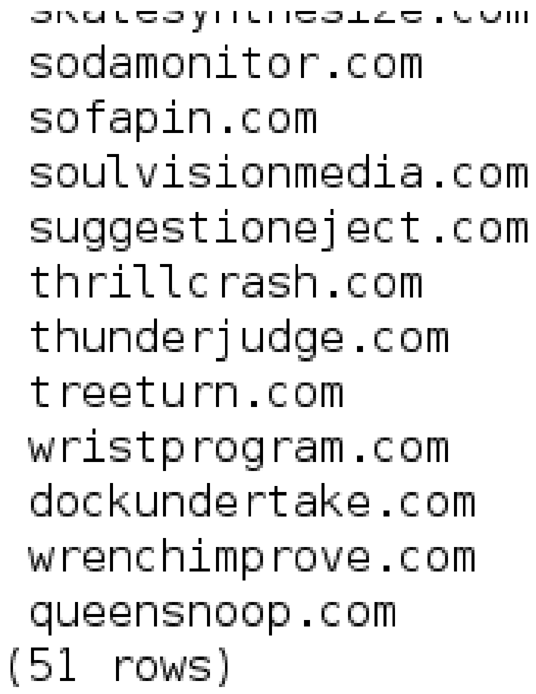
- good true positive rate, only few false positives
- # of false positives vary across clusters
  - 84% of clusters have no potential FPs (unknown)

A note on false positives

- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains

A note on false positives

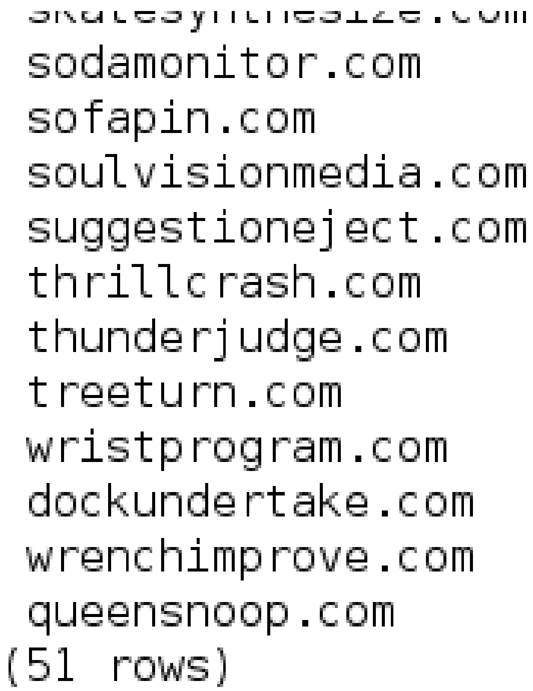
- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains



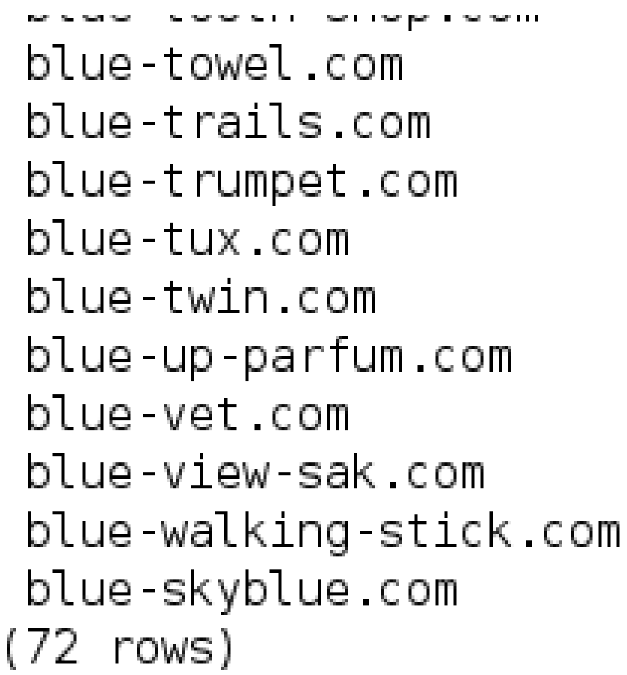
```
 skatesynthesize.com
 sodamonitor.com
 sofapin.com
 soulvisionmedia.com
 suggestioneject.com
 thrillcrash.com
 thunderjudge.com
 treeturn.com
 wristprogram.com
 dockundertake.com
 wrenchimprove.com
 queensnoop.com
(51 rows)
```

A note on false positives

- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains



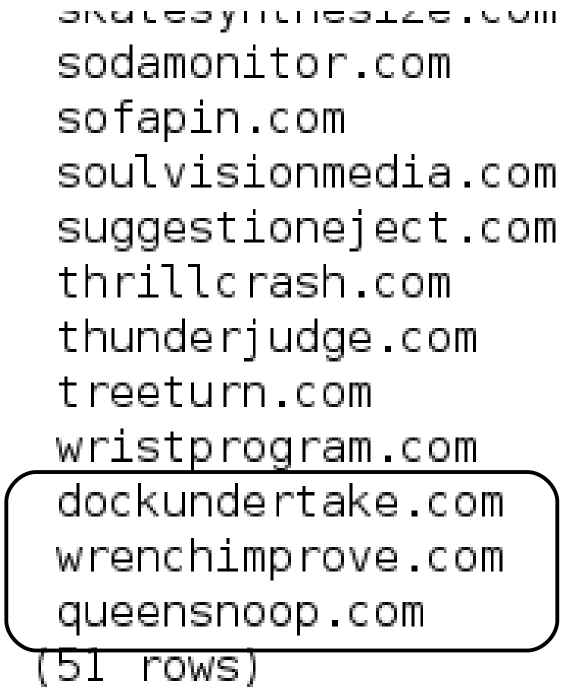
```
 skatesynthesize.com
 sodamonitor.com
 sofapin.com
 soulvisionmedia.com
 suggestioneject.com
 thrillcrash.com
 thunderjudge.com
 treeturn.com
 wristprogram.com
 dockundertake.com
 wrenchimprove.com
 queensnoop.com
(51 rows)
```



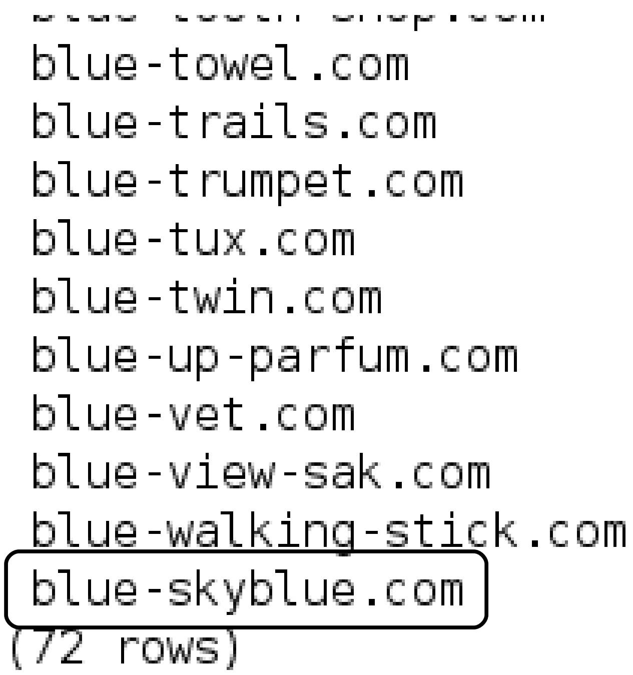
```
 blue-tooth-shop.com
 blue-towel.com
 blue-trails.com
 blue-trumpet.com
 blue-tux.com
 blue-twin.com
 blue-up-parfum.com
 blue-vet.com
 blue-view-sak.com
 blue-walking-stick.com
 blue-skyblue.com
(72 rows)
```

A note on false positives

- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains



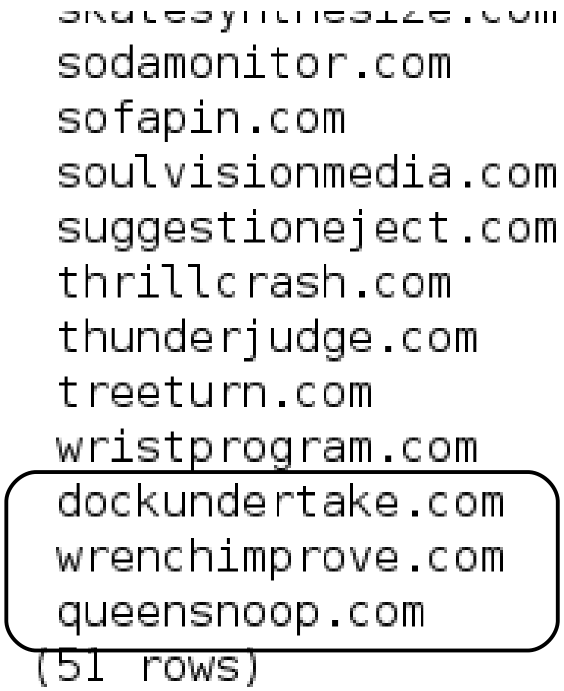
```
 skatesynthesize.com
 sodamonitor.com
 sofapin.com
 soulvisionmedia.com
 suggestioneject.com
 thrillcrash.com
 thunderjudge.com
 treeturn.com
 wristprogram.com
 dockundertake.com
 wrenchimprove.com
 queensnoop.com
(51 rows)
```



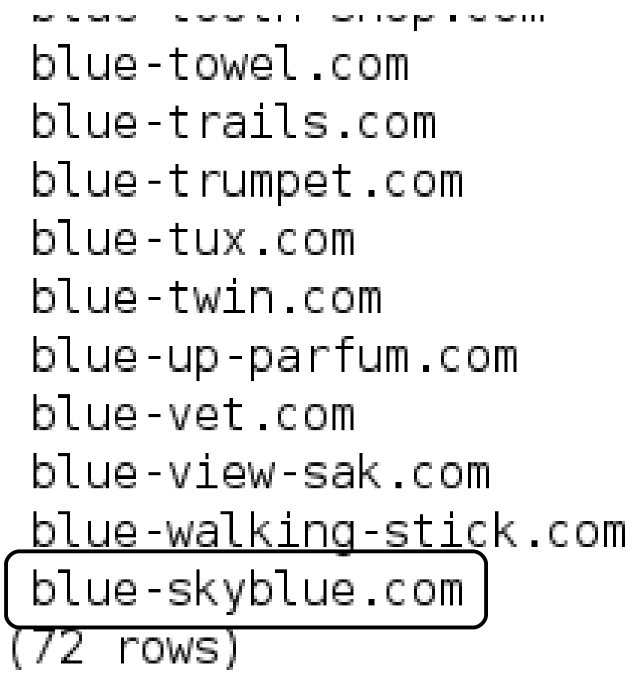
```
 blue-tooth-shop.com
 blue-towel.com
 blue-trails.com
 blue-trumpet.com
 blue-tux.com
 blue-twin.com
 blue-up-parfum.com
 blue-vet.com
 blue-view-sak.com
 blue-walking-stick.com
 blue-skyblue.com
(72 rows)
```

A note on false positives

- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains



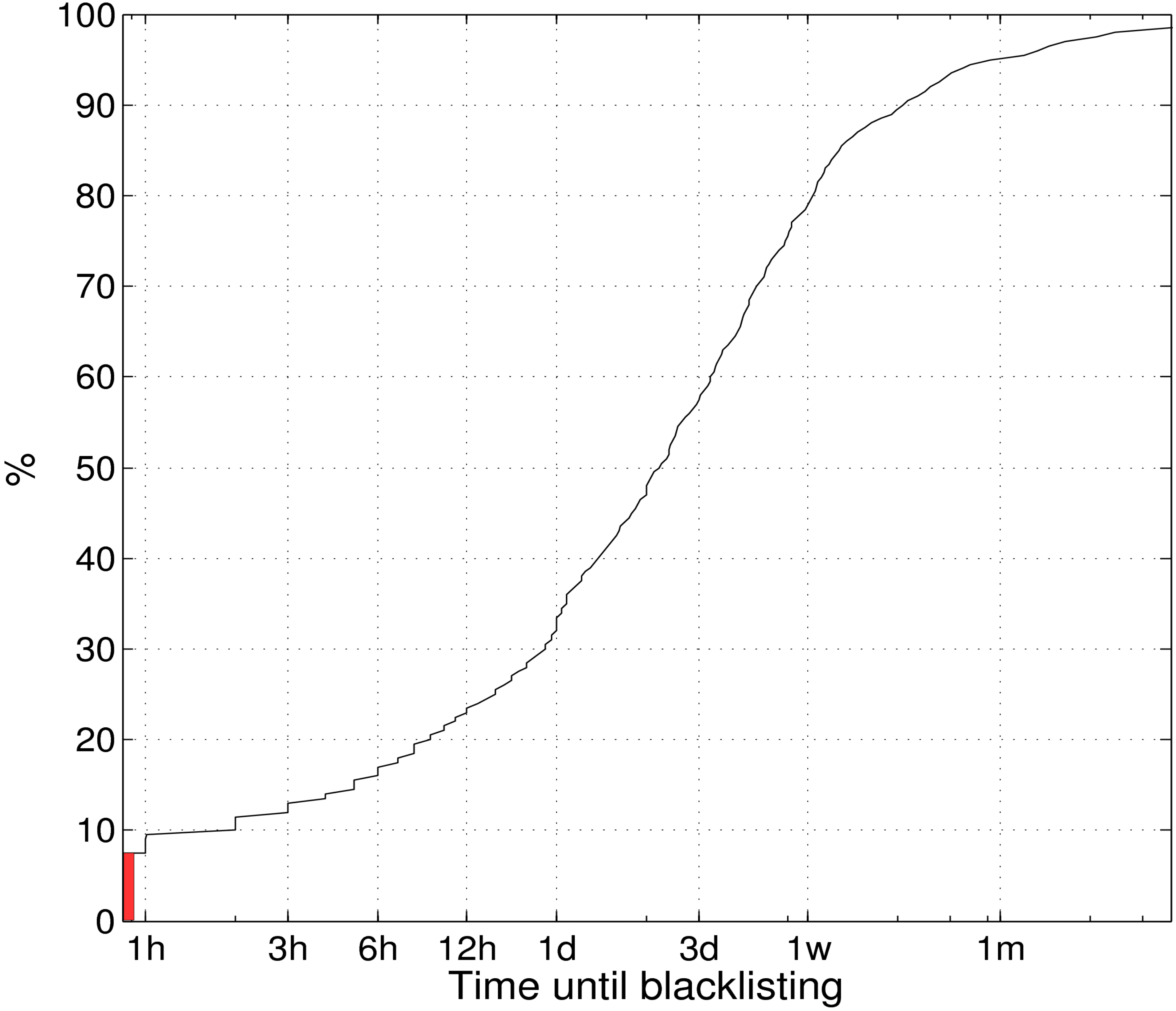
```
 skatesynthesize.com
 sodamonitor.com
 sofapin.com
 soulvisionmedia.com
 suggestioneject.com
 thrillcrash.com
 thunderjudge.com
 treeturn.com
 wristprogram.com
 dockundertake.com
 wrenchimprove.com
 queensnoop.com
(51 rows)
```



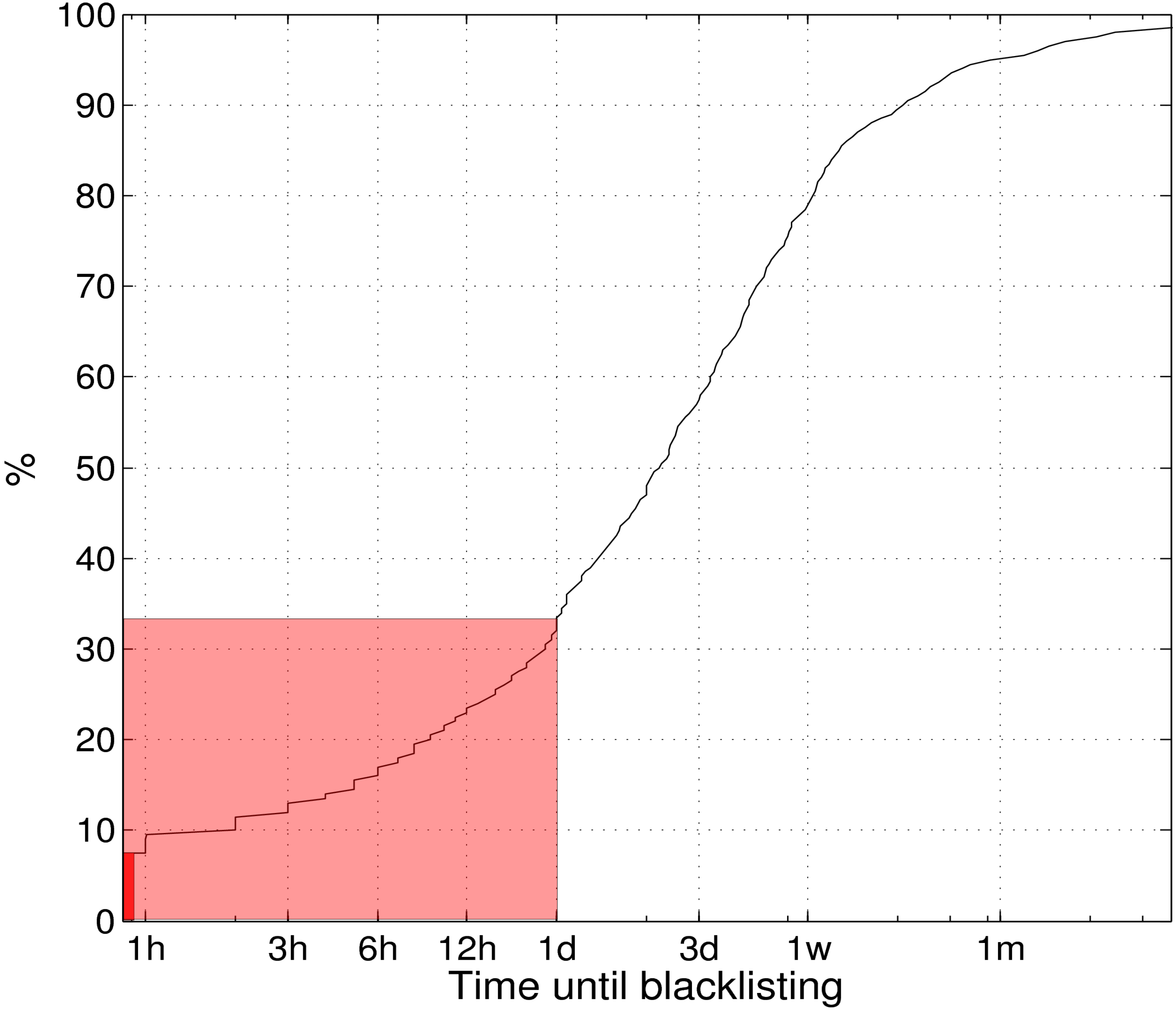
```
 blue-tooth-shop.com
 blue-towel.com
 blue-trails.com
 blue-trumpet.com
 blue-tux.com
 blue-twin.com
 blue-up-parfum.com
 blue-vet.com
 blue-view-sak.com
 blue-walking-stick.com
 blue-skyblue.com
(72 rows)
```

- large cluster: 1746 domains
  - part of a set of 80k domains
  - registered under a single name in Albania in Jan and Feb 2010

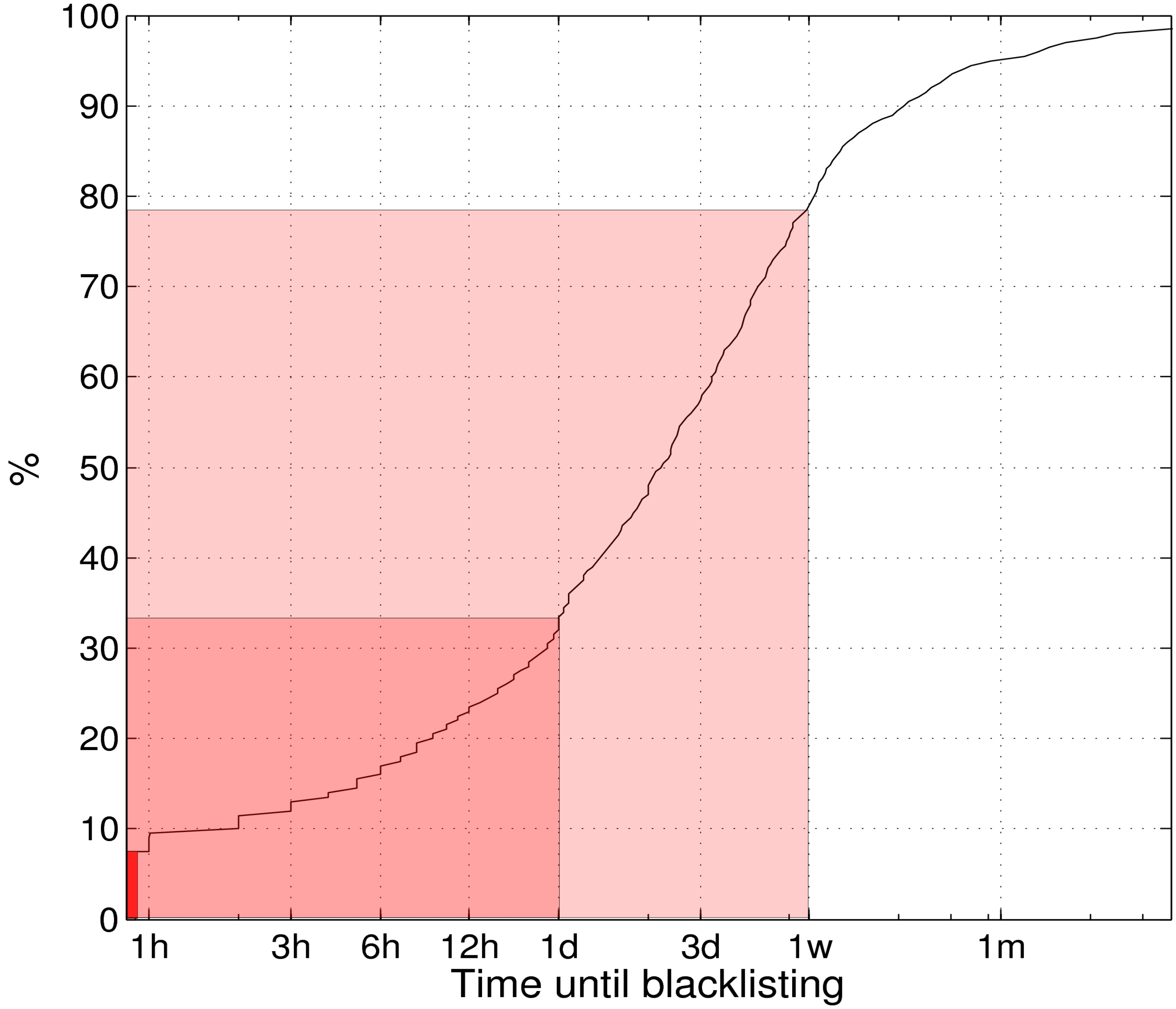
Time to blacklisting



Time to blacklisting



Time to blacklisting



Summary

- domains registered and used in clusters

Summary

- domains registered and used in clusters
- more malicious domains based on a few seeds and domain registry information

Summary

- domains registered and used in clusters
- more malicious domains based on a few seeds and domain registry information
- good accuracy
  - 73% of inferred domains on blacklists
  - 93% of domains are suspicious
  - false positives are often true positives

Summary

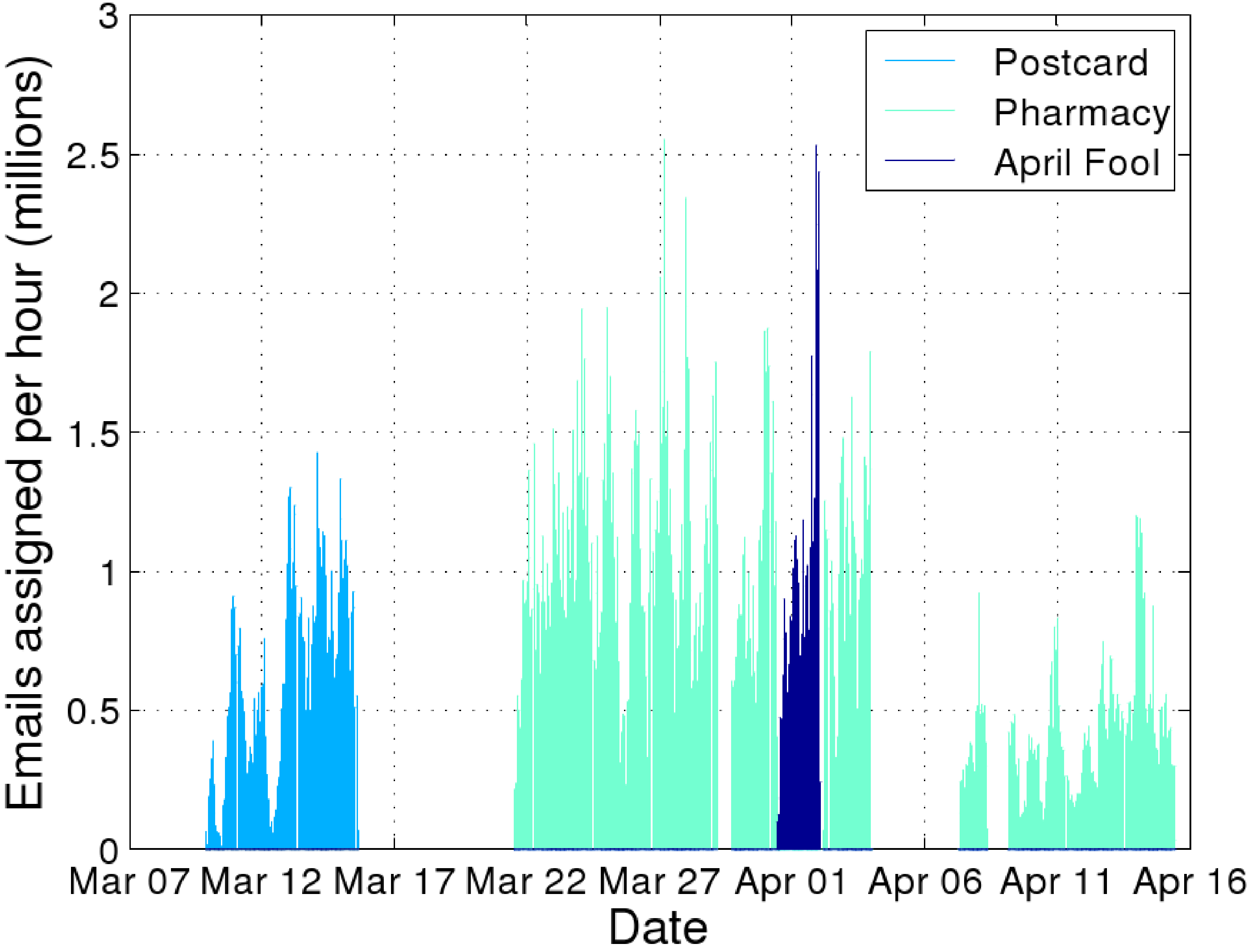
- domains registered and used in clusters
- more malicious domains based on a few seeds and domain registry information
- good accuracy
  - 73% of inferred domains on blacklists
  - 93% of domains are suspicious
  - false positives are often true positives
- faster than blacklists for 92% of the inferred malicious domains

Summary

- domains registered and used in clusters
- more malicious domains based on a few seeds and domain registry information
- good accuracy
  - 73% of inferred domains on blacklists
  - 93% of domains are suspicious
  - false positives are often true positives
- faster than blacklists for 92% of the inferred malicious domains

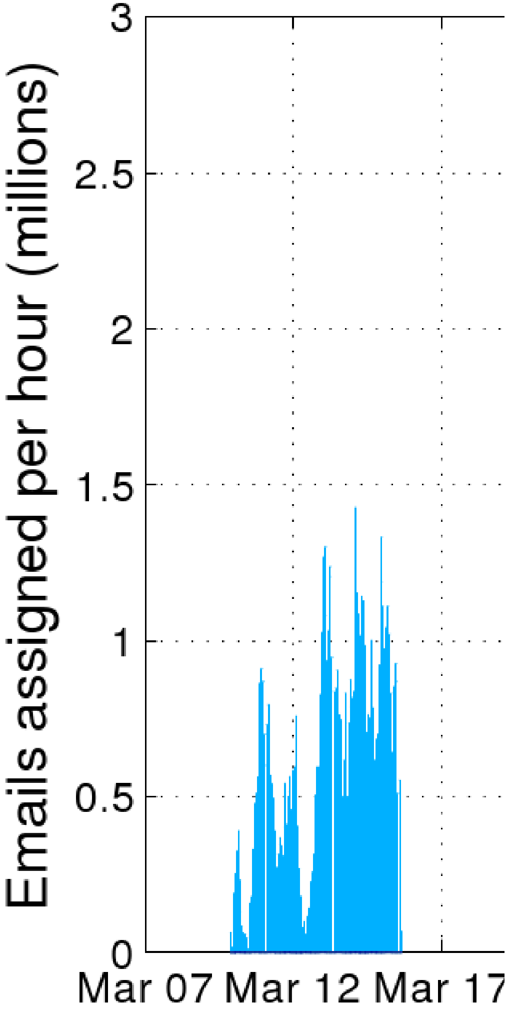
early response to spam

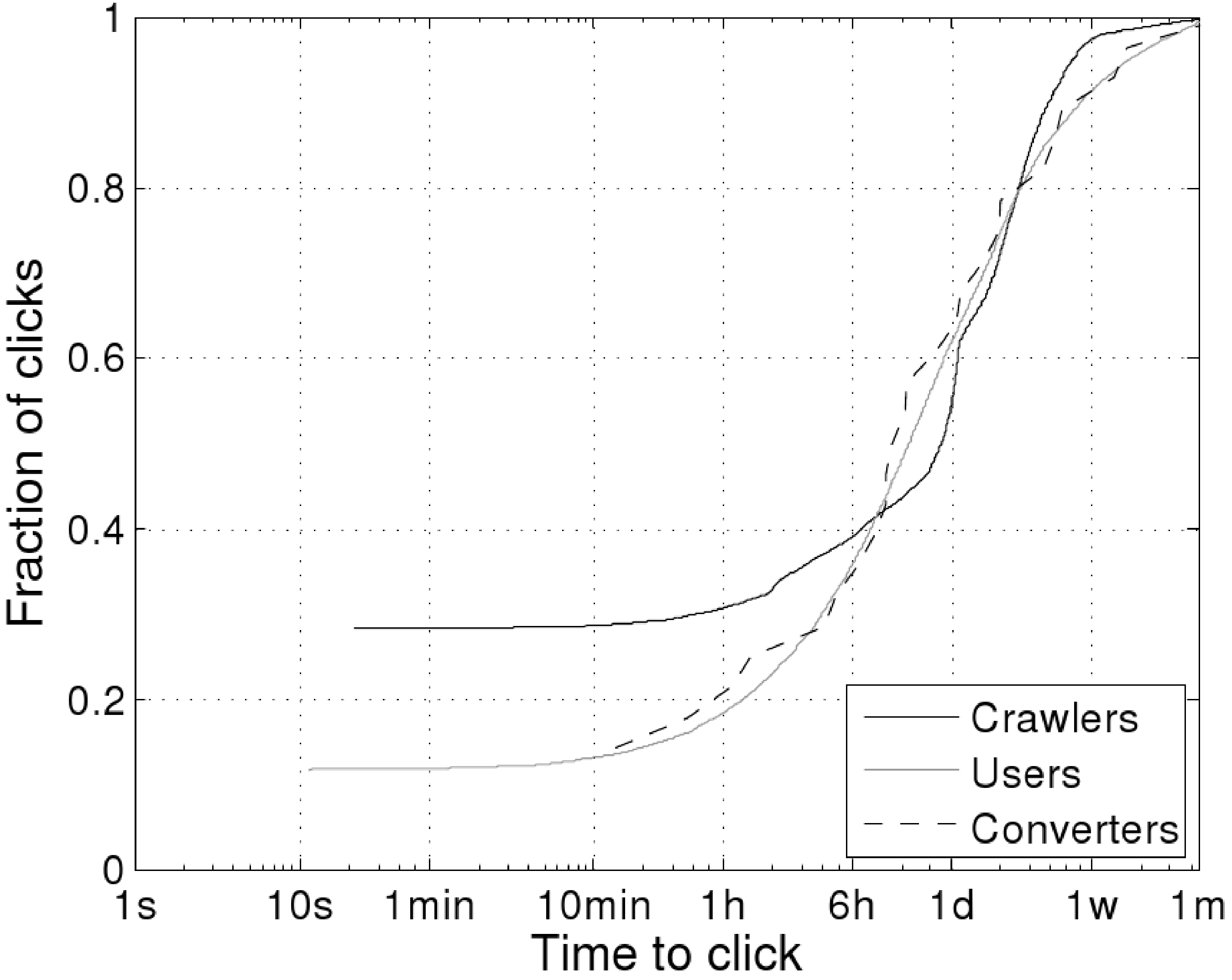
Spam and click volumes



Kanich et al., “Spamalytics: An empirical analysis of spam marketing conversion” CCS 2008
(CCIED: The Collaborative Center for Internet Epidemiology and Defenses)

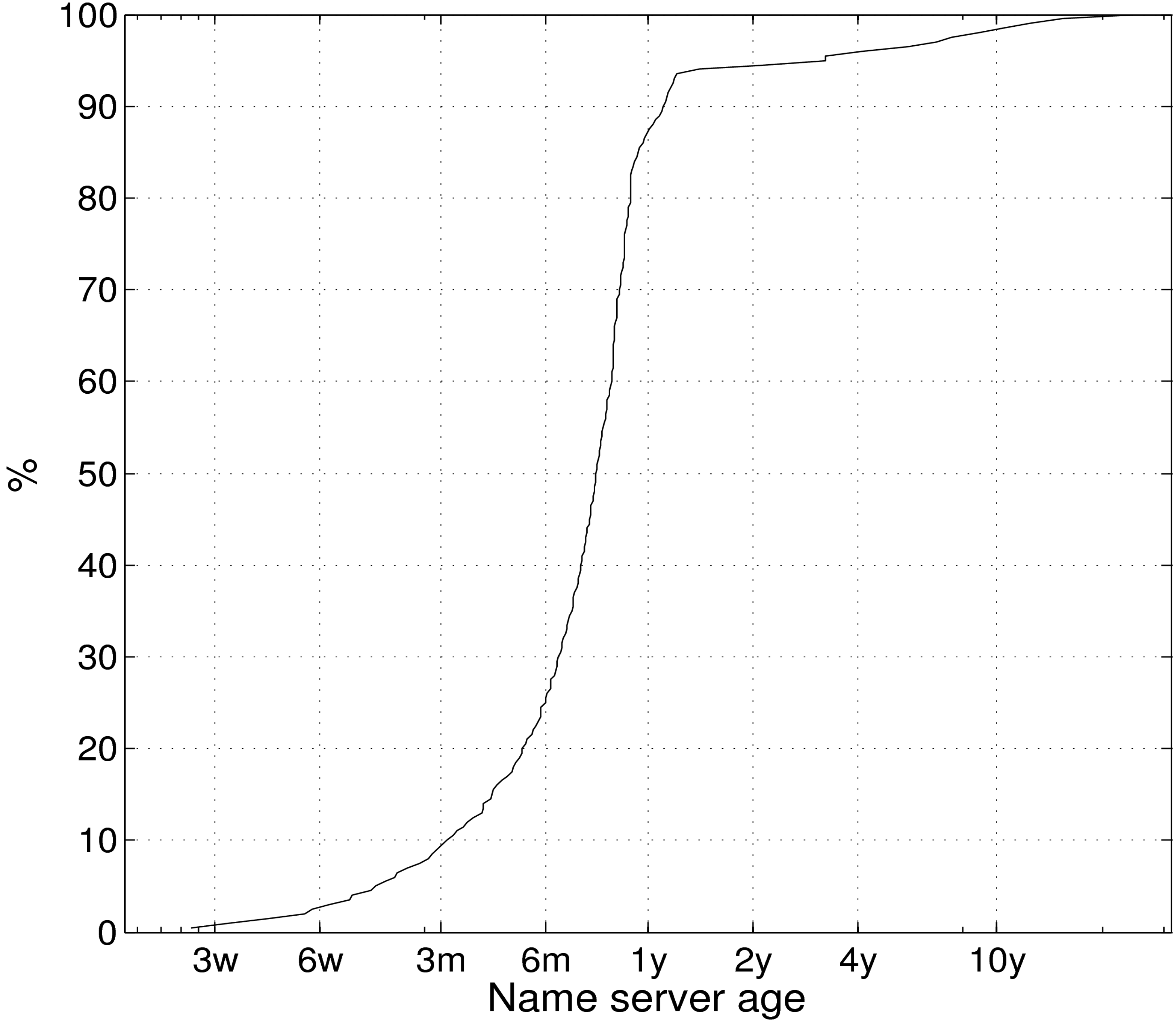
Spam and click volumes





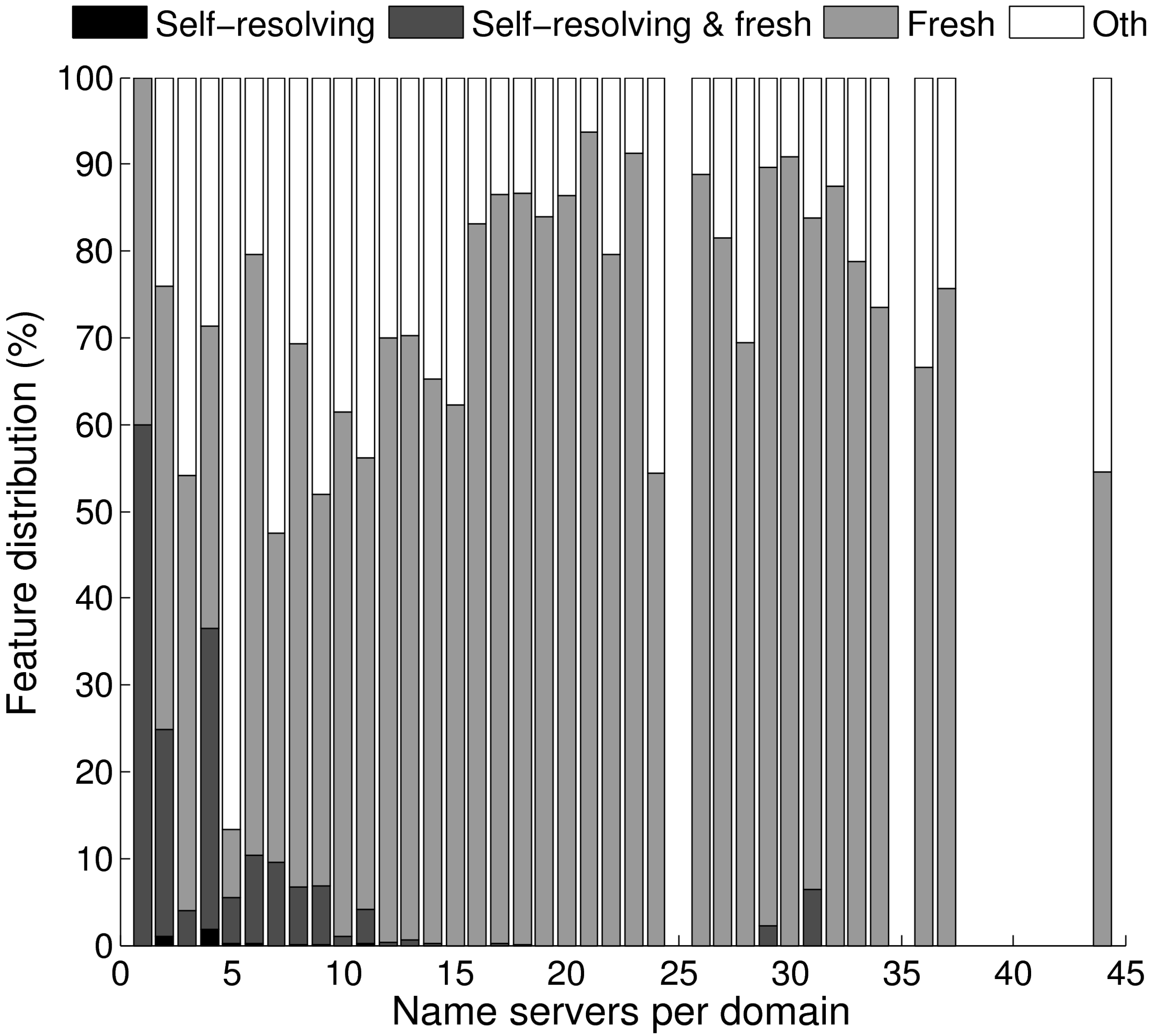
Kanich et al., “Spamalytics: An empirical analysis of spam marketing conversion” CCS 2008
(CCIED: The Collaborative Center for Internet Epidemiology and Defenses)

Name server ages

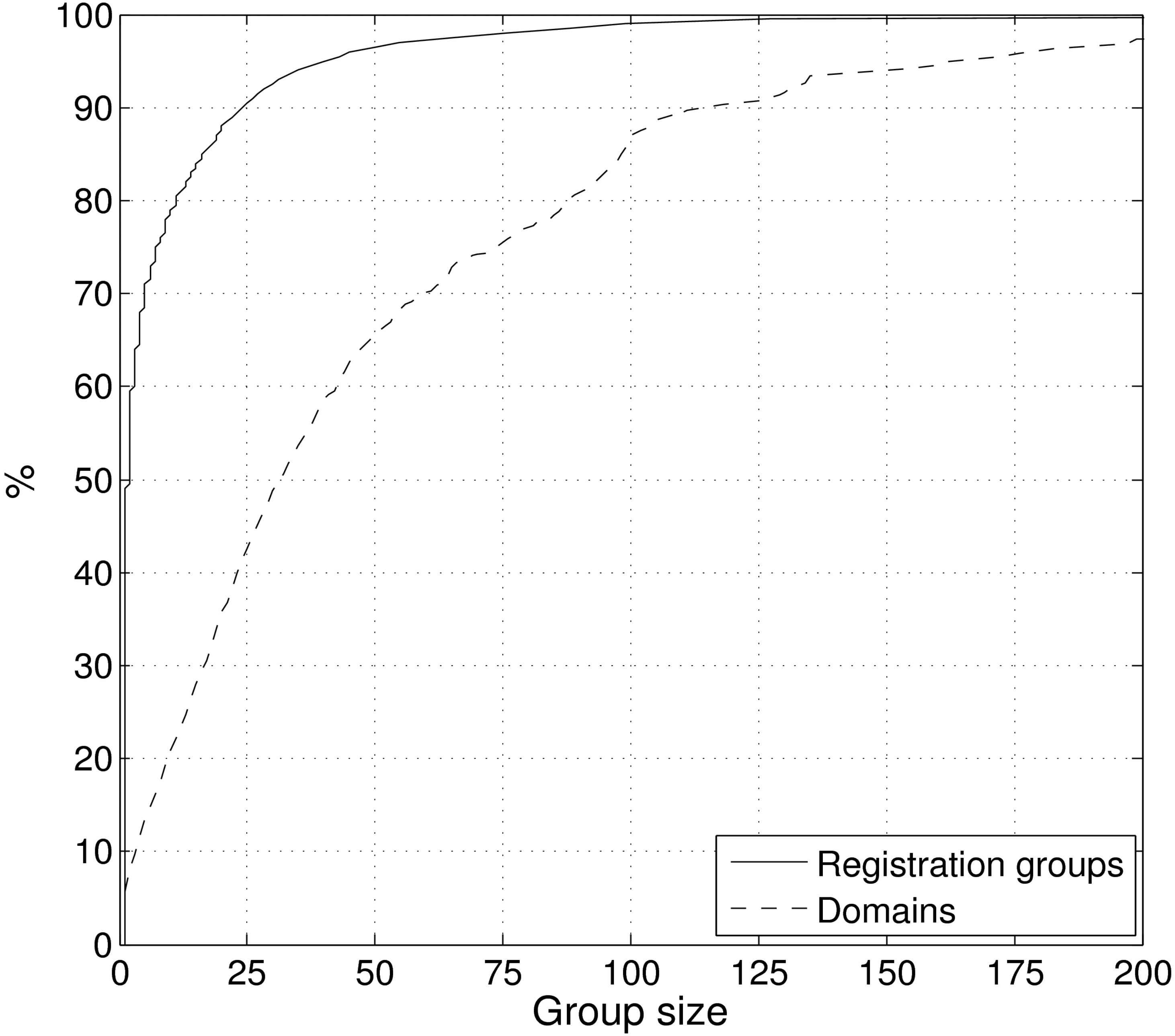


NS features

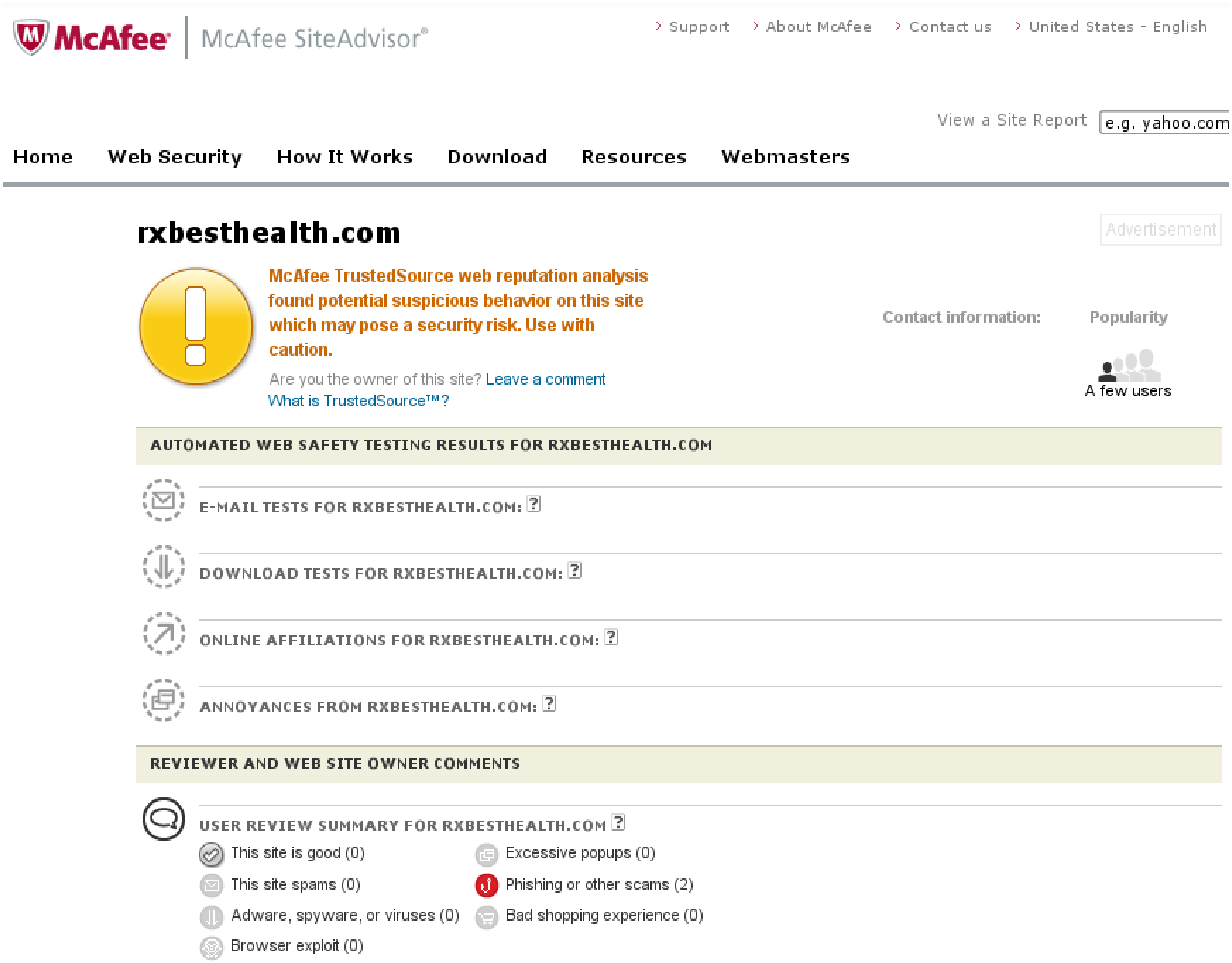
- 82.2% of domains encounter fresh name servers



Registration clusters



McAfee SiteAdvisor



McAfee | McAfee SiteAdvisor®

› Support › About McAfee › Contact us › United States - English

View a Site Report e.g. yahoo.com

Home Web Security How It Works Download Resources Webmasters

Advertisement

rxbesthealth.com

McAfee TrustedSource web reputation analysis found potential suspicious behavior on this site which may pose a security risk. Use with caution.

Are you the owner of this site? Leave a comment

What is TrustedSource™?

Contact information:

Popularity

A few users

AUTOMATED WEB SAFETY TESTING RESULTS FOR RXBESTHEALTH.COM

E-MAIL TESTS FOR RXBESTHEALTH.COM: ?

DOWNLOAD TESTS FOR RXBESTHEALTH.COM: ?

ONLINE AFFILIATIONS FOR RXBESTHEALTH.COM: ?

ANNOYANCES FROM RXBESTHEALTH.COM: ?

REVIEWER AND WEB SITE OWNER COMMENTS

USER REVIEW SUMMARY FOR RXBESTHEALTH.COM ?

This site is good (0)	Excessive popups (0)
This site spams (0)	Phishing or other scams (2)
Adware, spyware, or viruses (0)	Bad shopping experience (0)
Browser exploit (0)	