Domain Name Privacy Misuse Studies

Dave Piscitello and Steve Sheng

ICANN

INET Asia, Hong Kong 13 April 2010

Domain Name Privacy Conundrum

- Privacy is the ability to control what one reveals about oneself over the Internet and who can access that personal information
- Privacy controls for domain name registrations vary across registries and registrars
- Criminals exploit privacy controls that attempt to protect personal information associated with domain names to evade detection

Relevant prior studies

- *Prevalence of private registrations among malicious domains hosted at 3FN* (Oct 2009)
  - Population: concentration of alleged criminal activity
  - Result: 145 of 384 domains used in study were private domain registrations (38%)
- *NORC WHOIS data accuracy study* (Feb 2010)
  - General population, useful for determining validity of of subsequent studies into abuse of WHOIS services
  - 580 of 2352 domains used in the study were private or domain registrations (25%)

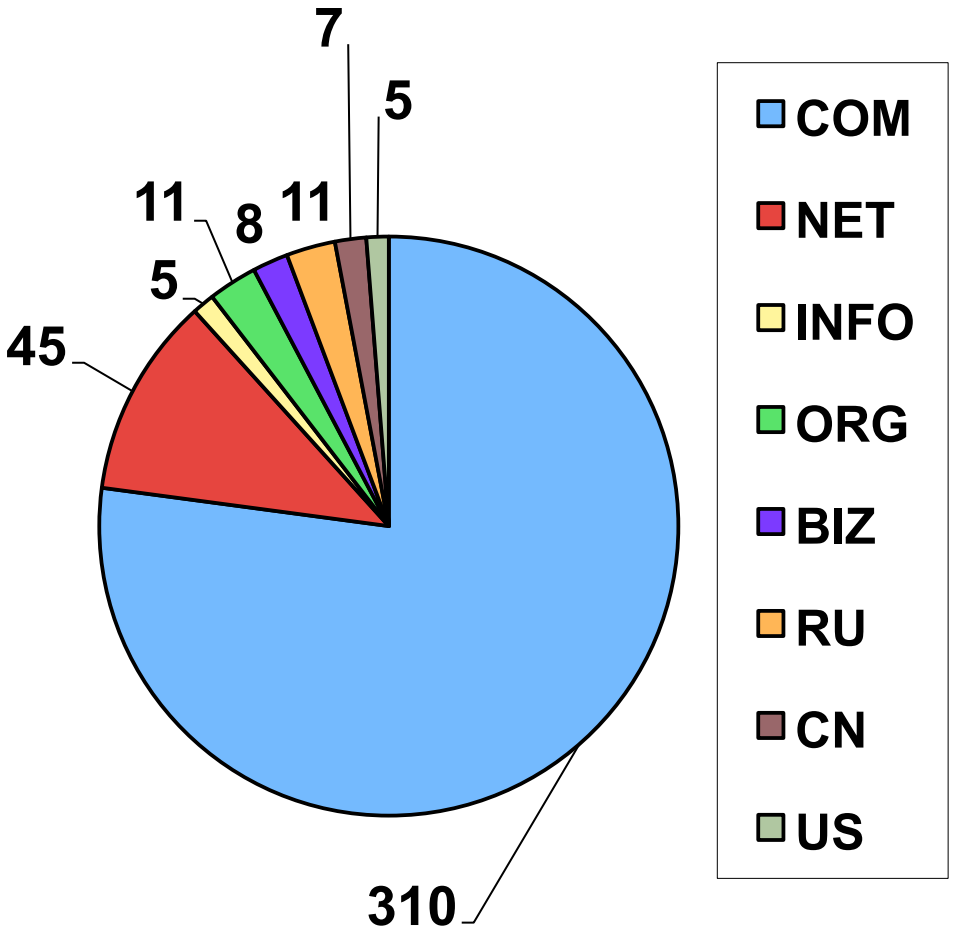
3FN Study

- 3FN Hosting: alleged locus of malicious domain activity
  - District court judge shuts 3FN service down at the request of the FTC (4 June 2009)
  - Domains hosted at 3FN used private registration services
  - Many block-lists have data associated with 3FN domains
- Opportunity to study private domain registrations to answer a specific question:
  - How many 3FN domains with privacy protection services allegedly host criminal or malicious content?

http://www.ftc.gov/opa/2009/06/3fn.shtm
http://blog.fireeye.com/research/

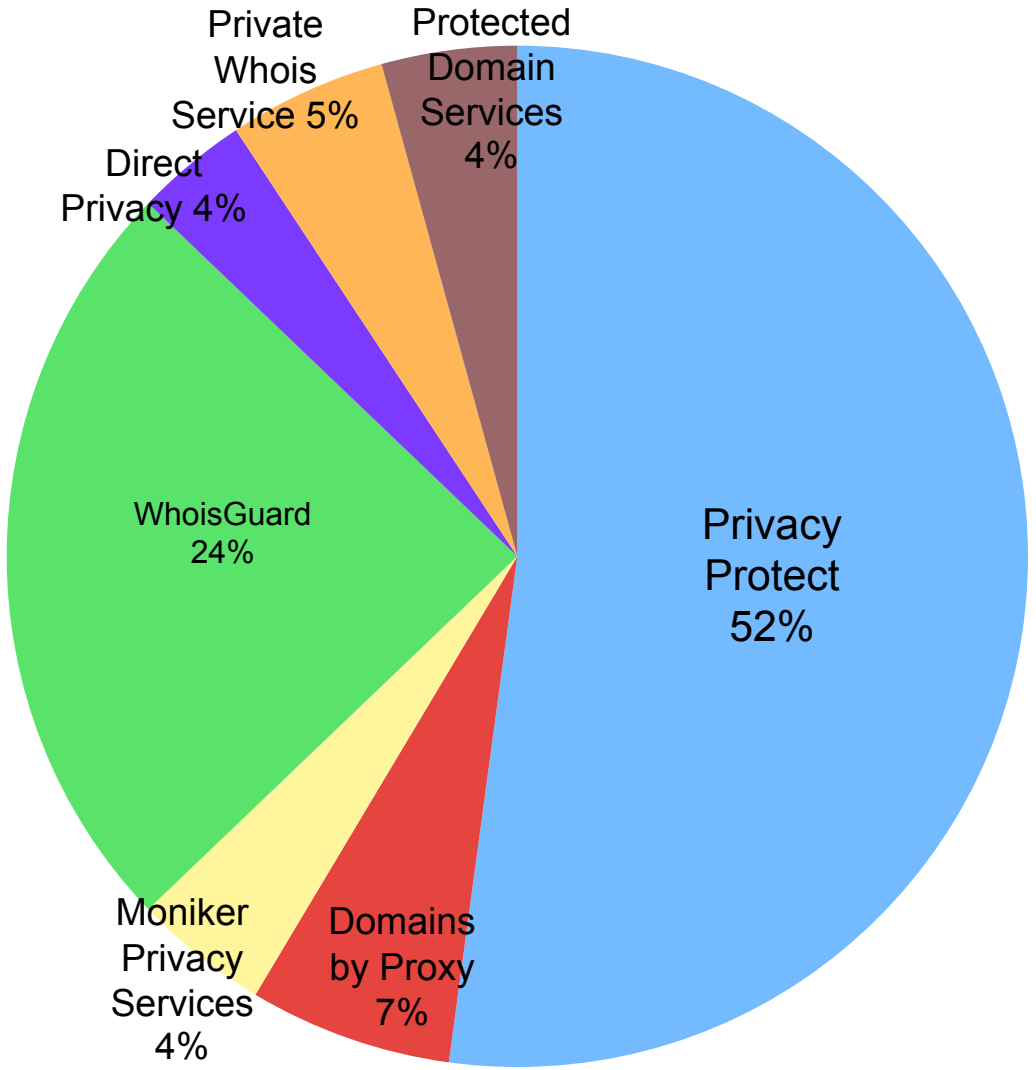
3FN sample: domains, TLDs

- 403 domains in data set
  - Included two CCTLDs
  - WHOIS not available
- Used 384 in study from
  - BIZ, COM, INFO, NET, ORG, US
  - WHOIS available



Private domain registrations in 3FN sample

- 3FN sample
  - 145 of 384 domains in the sample used privacy protection services (38%)

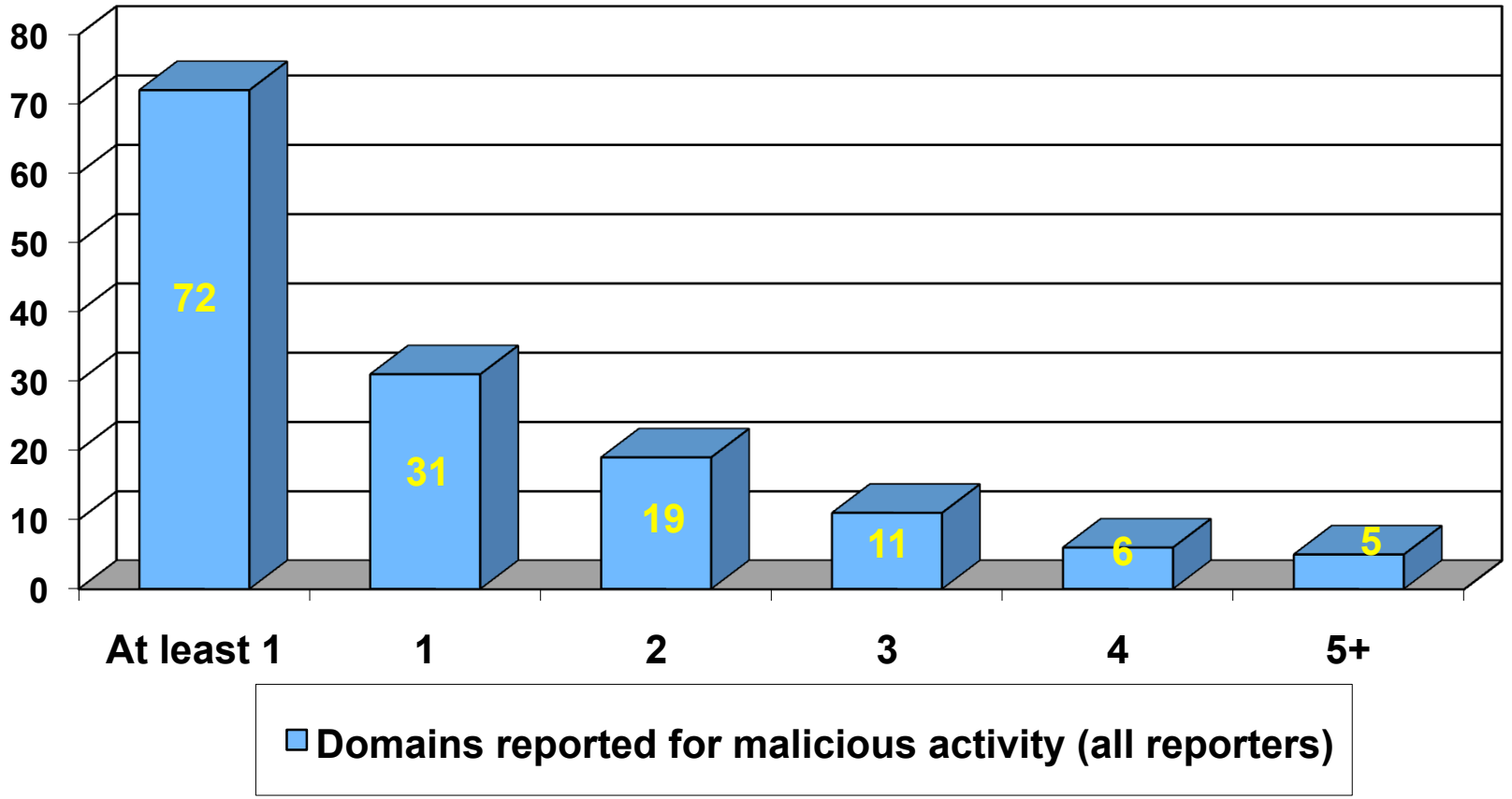


How do we classify private registrations as "allegedly hosting criminal or malicious content"?

- Query 13 block- and black-lists for reports against
  - Domain name
  - IP address while hosted at 3FN
  - New IP address (if domain remains hosted)
- Spam/malware feed data (courtesy of FireEye)
- Count domains with 1+ reports of malicious activity

- Malicious activities reported among lists include:
  - Spam hosting
  - Phishing
  - Child pornography✪
  - Malware hosting
  - Search or click fraud
  - Illegal pharma
  - Digital rights infringements (illegal MP3 downloads)
  - Hosting DNS for any of above activities

How many "3FN" domains with private domain registrations are *reported* as hosting criminal or malicious content?



3FN Study Findings

- Privacy protection services are used by registrants of domains who host commercial content
  - All 3FN domains hosted commercial content
  - Finding debunks myths regarding who uses private domain registrations
  - Finding is statistically significant using two proportion test in conjunction with NORC general population ($p < 0.01$)
- Privacy protection services are used by registrants of domains that appear on public lists of "domains used to host or support malicious activity"
  - 49% of 3FN-hosted domains that used privacy protection services were reported for 1+ malicious activities

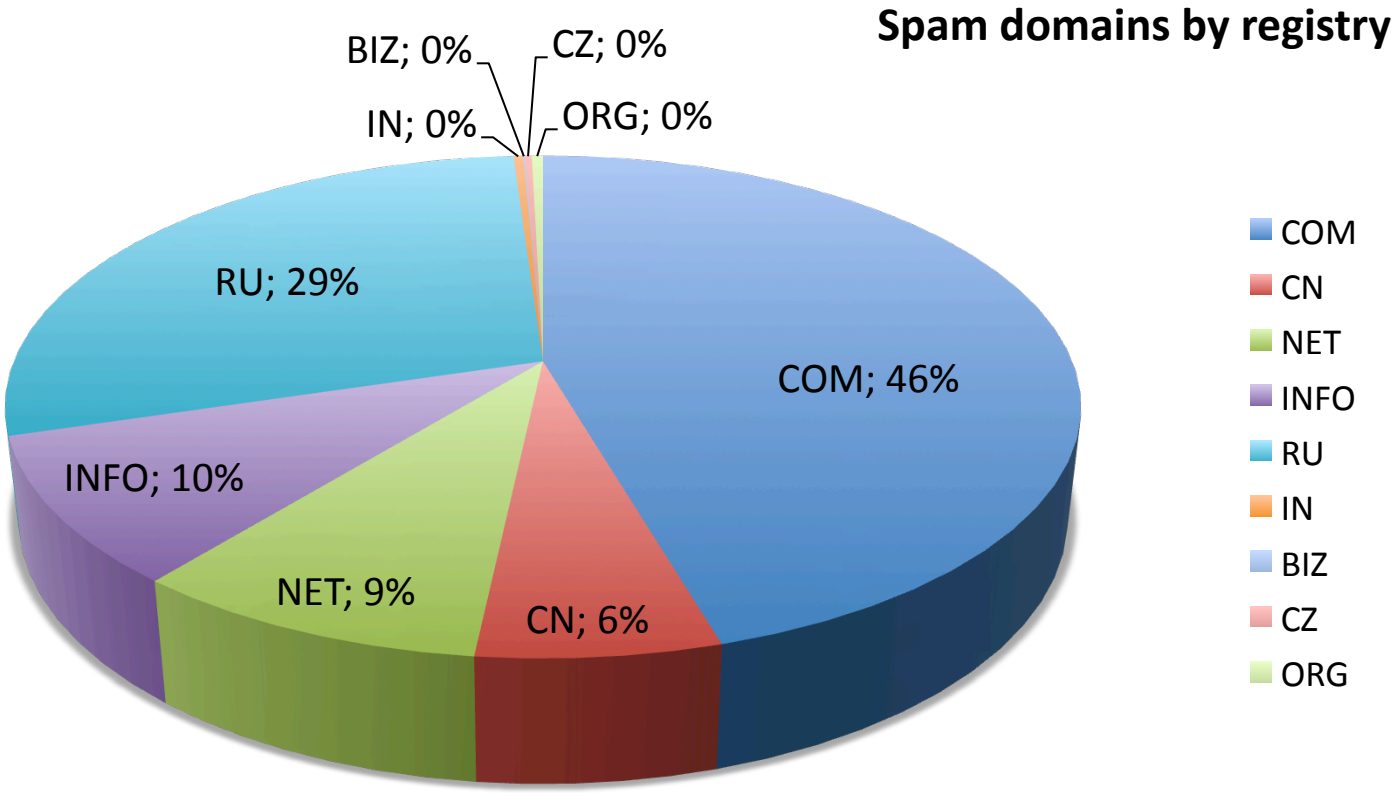
Next steps

- Study a larger, statistically meaningful sample
  - Should (can) we assure a similar concentration of bad actors in the sample?
    - Sources of alleged malicious domains are easy to find
  - What affect would a randomized sampling of domains have on findings?
    - Percentage of bad actors may change dramatically
    - Percentage of commercial actors may not change

Current study

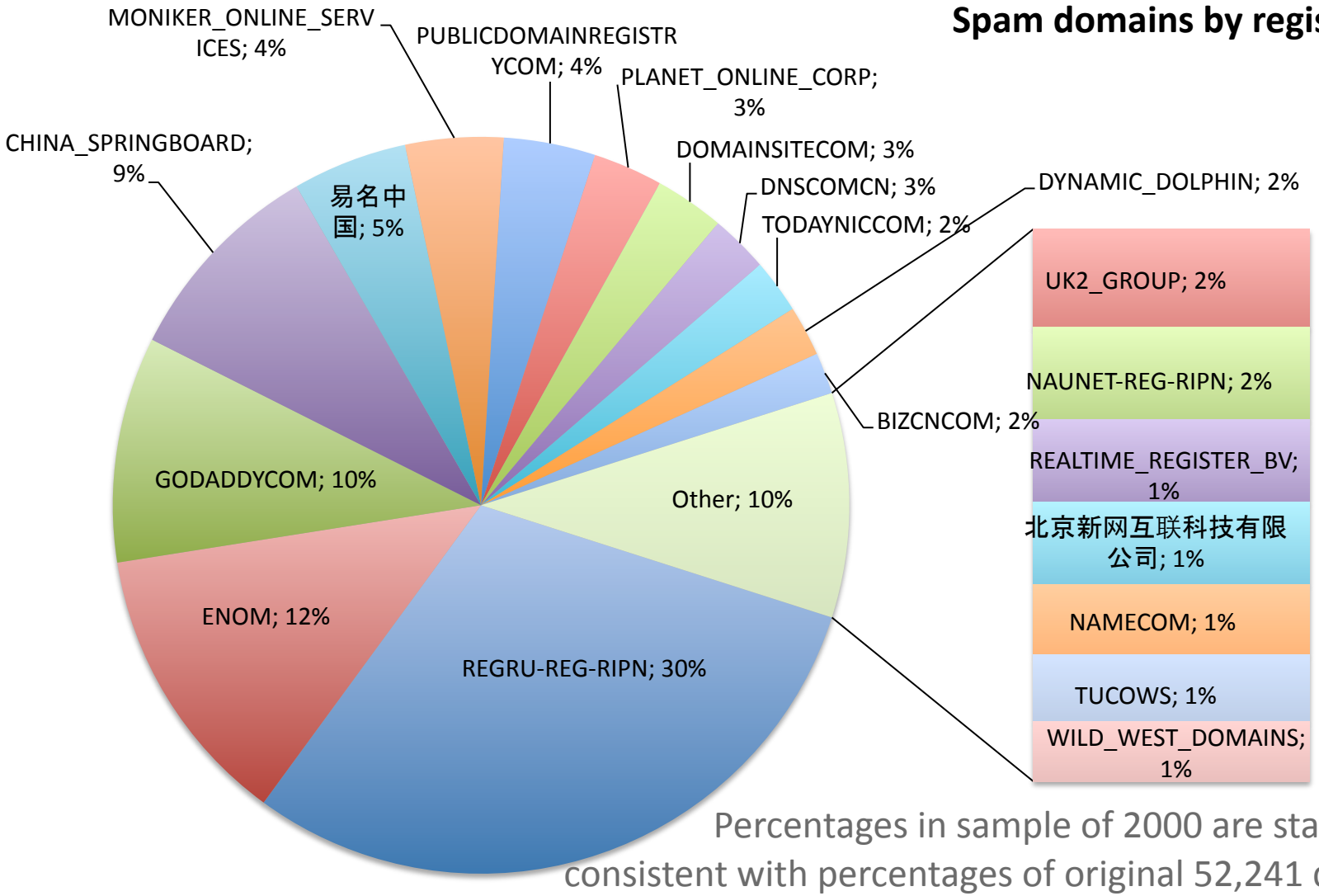
- Leverage data collection by trusted monitors of malicious activity to obtain data set
  - 54,809 domains identified as hosting spam from SpamHaus Domain Block List (DBL) (March 17 – 23),
  - Able to retrieve 52,241 of 54,809 Whois records
- Use a statistically meaningful sample size
  - 2000 domains randomly extracted from 52,241
- Automate to make study repeatable
  - SQL database of domains registered in gTLDs
  - Considerable variation among WHOIS data stores is noteworthy inhibitor

Spam domains (sample of 2000)



SPAM DOMAINS IN CCTLDs	710
DEACTIVATED DOMAINS	4
TOTAL USABLE SAMPLE DOMAINS	1286

Sponsoring registrars (sample of 2000)



Percentages in sample of 2000 are statistically consistent with percentages of original 52,241 domains

DBL Study Results

SPAM DOMAINS IN CCTLDs	710
DEACTIVATED DOMAINS (NO WHOIS AVAILABLE)	4
TOTAL USABLE SAMPLE DOMAINS	1286
PERCENT OF SPAM DOMAINS USING PRIVACY/PROXY services	31%

Spam domains have higher percentage of privacy protection services than regular domains (statistically significant)

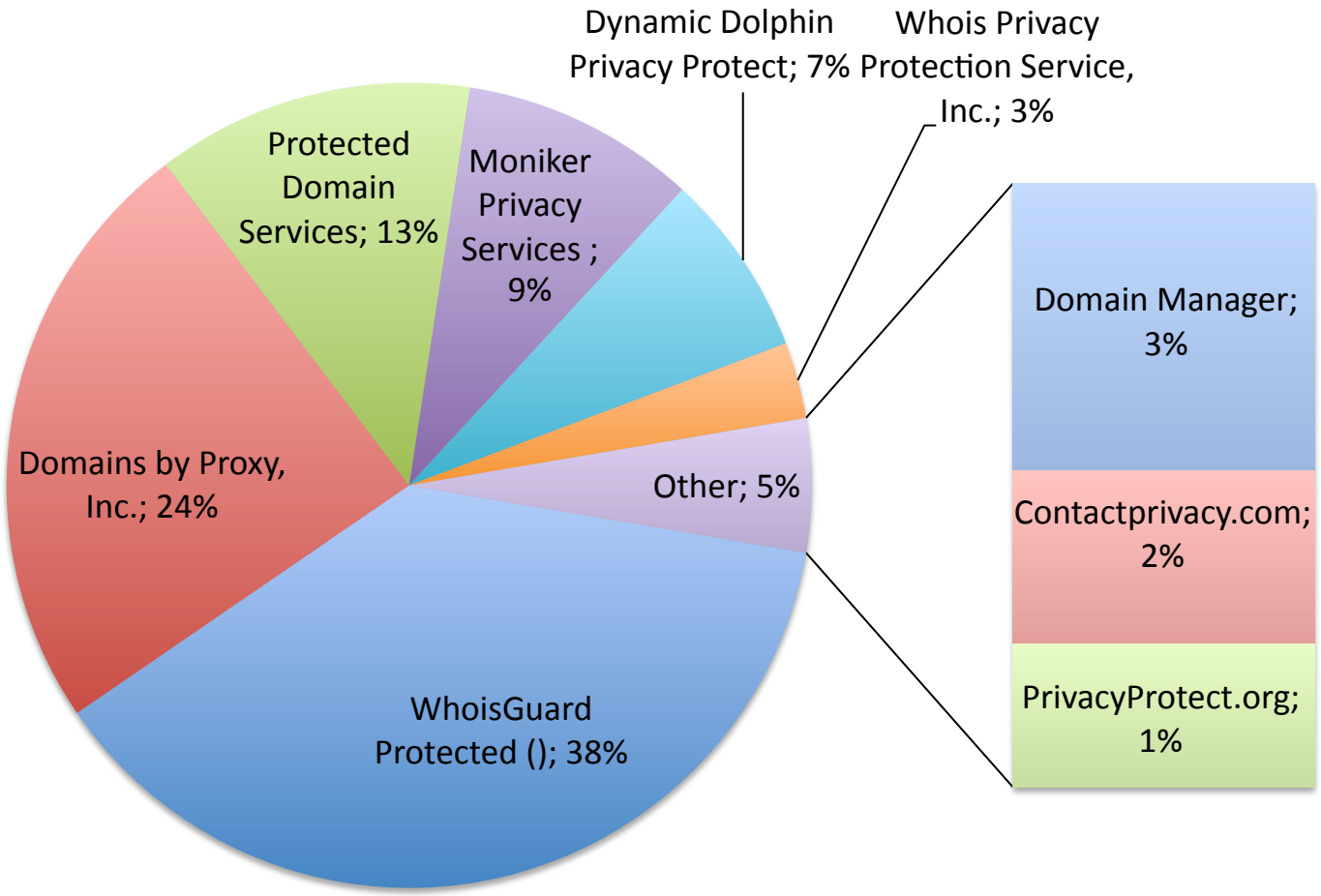
Two Proportions Test

- Confidence Level: 95%
  - NORC study size: 2352
  - Proportion: 588 (25%)
  - DBL study size:1286
  - Proportion: 397 (30.87%)
  - $p < 0.01$

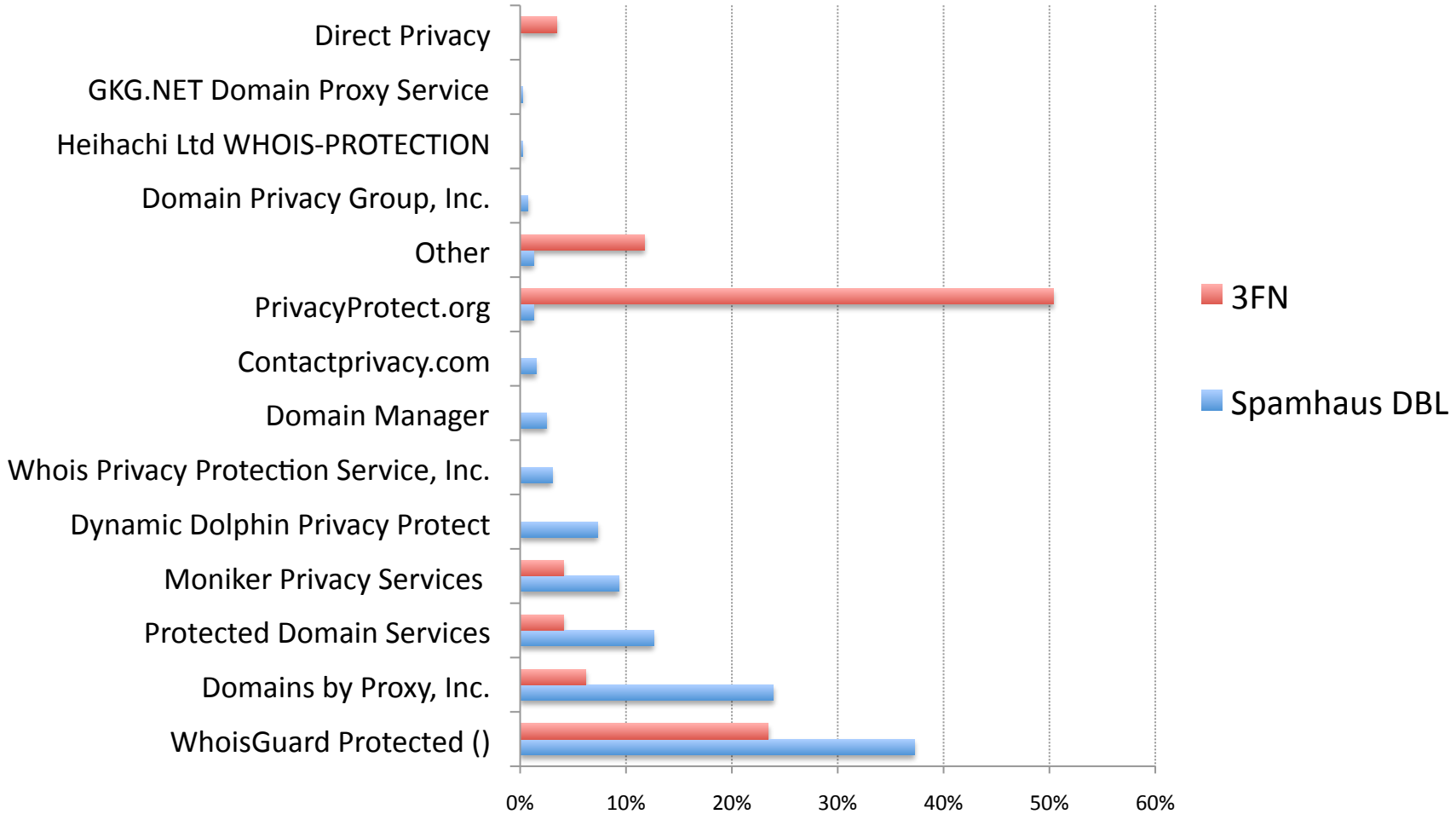
Confidence Level: 95%

Sample Size: 1286
Observed Results: 30.87% (397 frequency)
Confidence Interval: ± 2.52%
True Population Proportion Range: 28.35% to 33.39%

Spam domains in DBL sample that use privacy or proxy registrations



Do targets shift over time?



Some targets change… not all results are statistically significant, need more samples

What other questions should we study?

- What attracts spammers to a particular registrar?
- Do spammers flock to registrars or privacy protection services, or is the attraction entirely opportunistic?
- Do targets shift over time? What causes shifts?

Conclusion

Both case studies confirm that *a higher percentage of malicious domains use privacy protection registration services than the general population*

How can we reduce or mitigate abuse?

- Possible option: guidelines for private registrations
  - Exempt commercial use from private domain registration
  - Establish criteria registrants must meet to use private registrations
- Possible requirements for privacy protection services
  - Proof: party satisfies criteria for privacy protection; for example, party is a natural person, not engaged in commercial activity…
  - Enforcement: Terms of Service includes suspension when abuse or misrepresentation is reported and confirmed
- Are privacy protection services for natural persons only?
  - Should protection registrations only protect privacy of individuals or should parties operating legitimately with need for anonymity qualify? (e.g., "rights advocacy" group)?

Thank you

Contact information

- Dave Piscitello
  dave.piscitello@icann.org
- Steve Sheng
  steve.sheng@icann.org