How to Use Policy Enforcement to Stop Abuse

RIPE
Anti-Abuse Working Group
Amsterdam, the Netherlands
May 2009
Dr. Robert Bruen

KnujOn's First Rule

It's all about the money

ICANN

Registrars

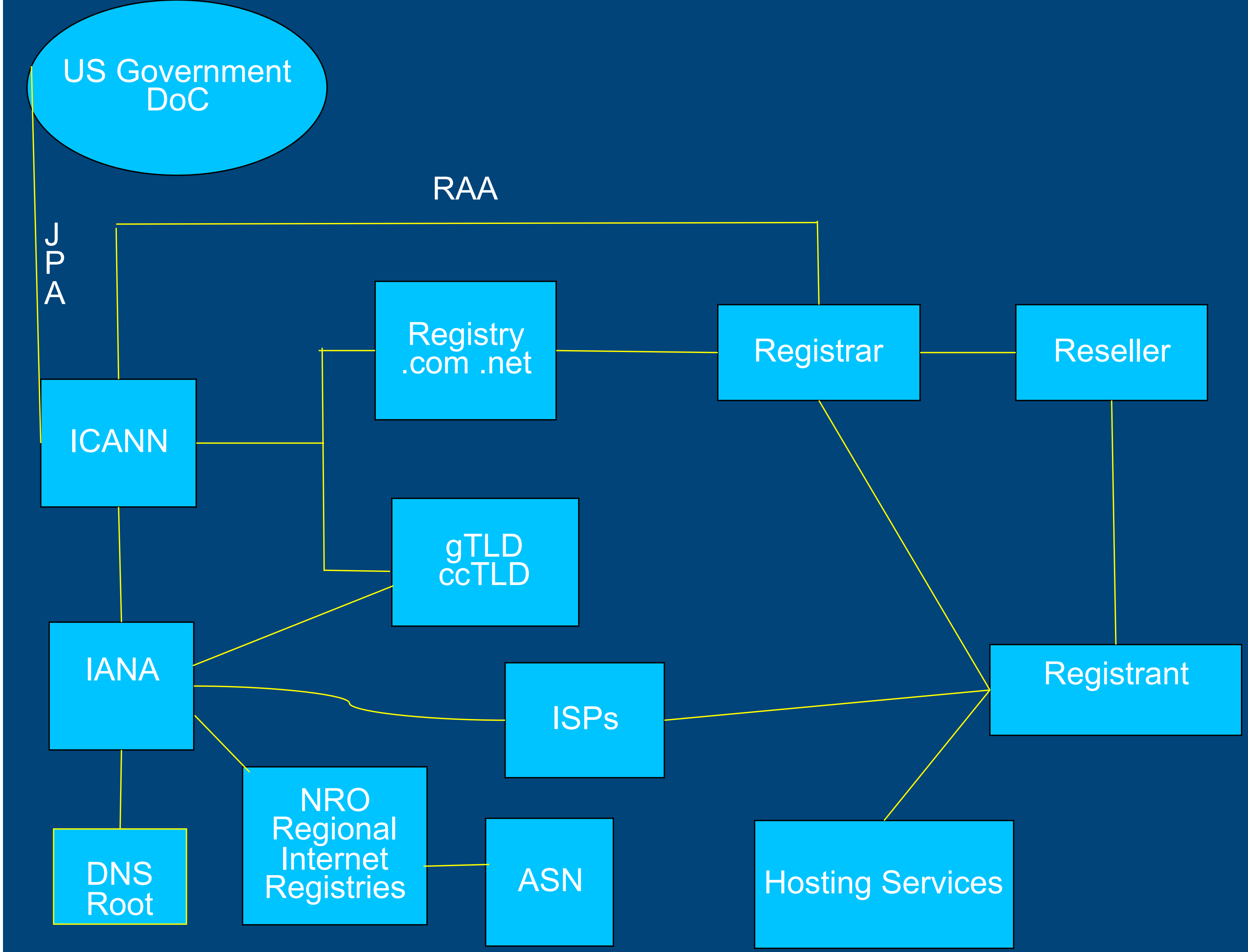
Resellers

ISPs

Criminals

Policies, Contracts, MoUs

- Policies are in contracts/agreements/rules
- Seek loopholes
- Whois data accuracy is one
- Follow the rule (loophole)



US Government DoC

RAA

JPA

ICANN

Registry .com .net

Registrar

Reseller

gTLD ccTLD

IANA

ISPs

Registrant

DNS Root

NRO Regional Internet Registries

ASN

Hosting Services

Whois Data Accuracy

- Long and sordid history (1982-now)
- Registrars required to correct WI data (RAA)
- Still very controversial
- KnujOn cares about individual privacy
- Want commercial entities policy enforcement

Enforcing WI Data Accuracy

- KnujOn receives spam (anonymous & clients)
- Extract transaction sites
- Verify WI Data for each site
- Complain to ICANN (Policy Enforcement)
- Aggregate data & publish results (Sunshine)

Top Ten Worst Registrars May 08

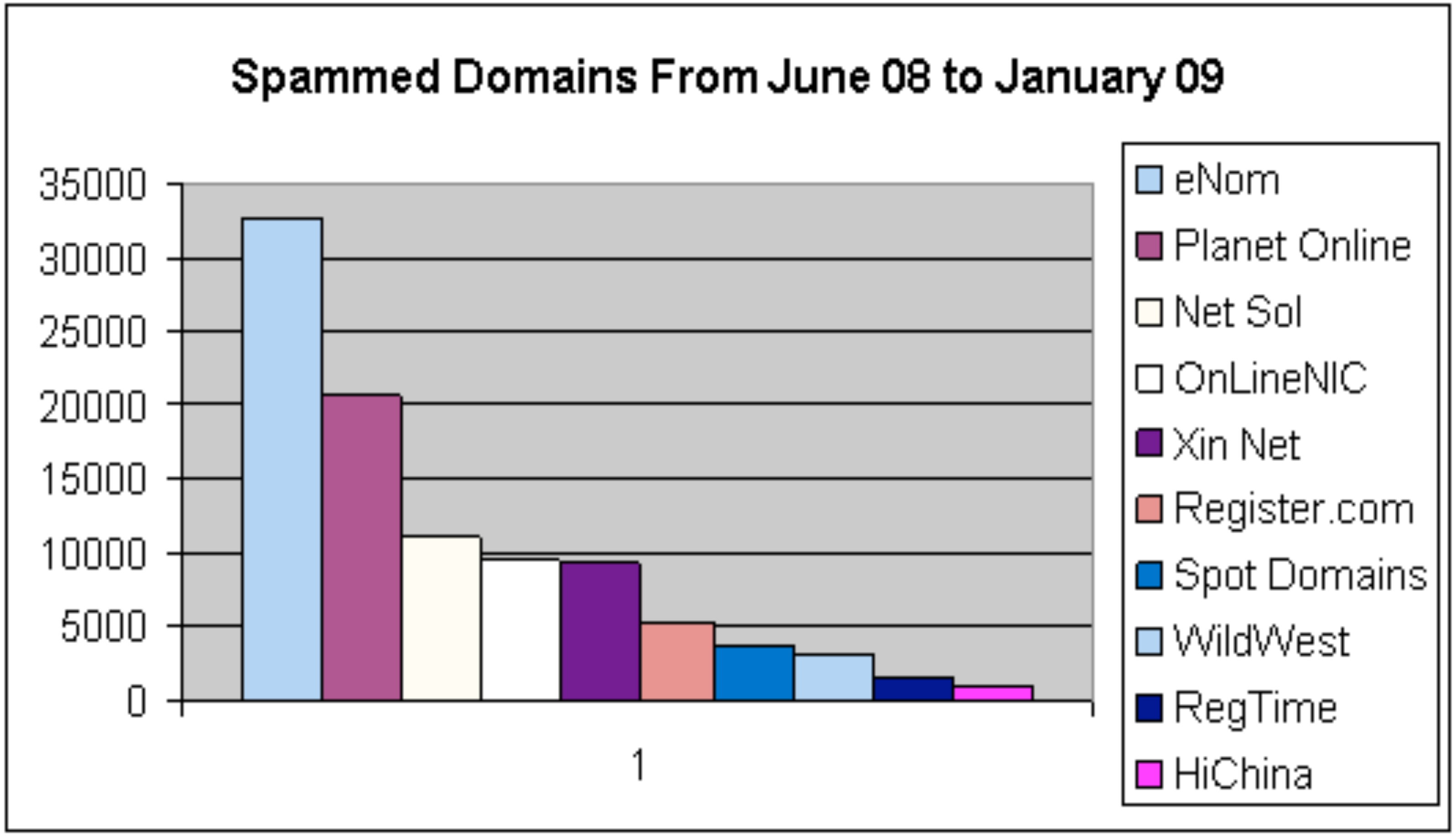
1. Xin Net Bei Gong Da Software
2. Beijing Networks
3. Todaynic
4. Joker
5. eNom, Inc.
6. MONIKER
7. Dynamic Dolphin
8. The Nameit Co/AITDOMAINS.COM
9. PDR (Directi)
10. Intercosmos/DIRECTNIC

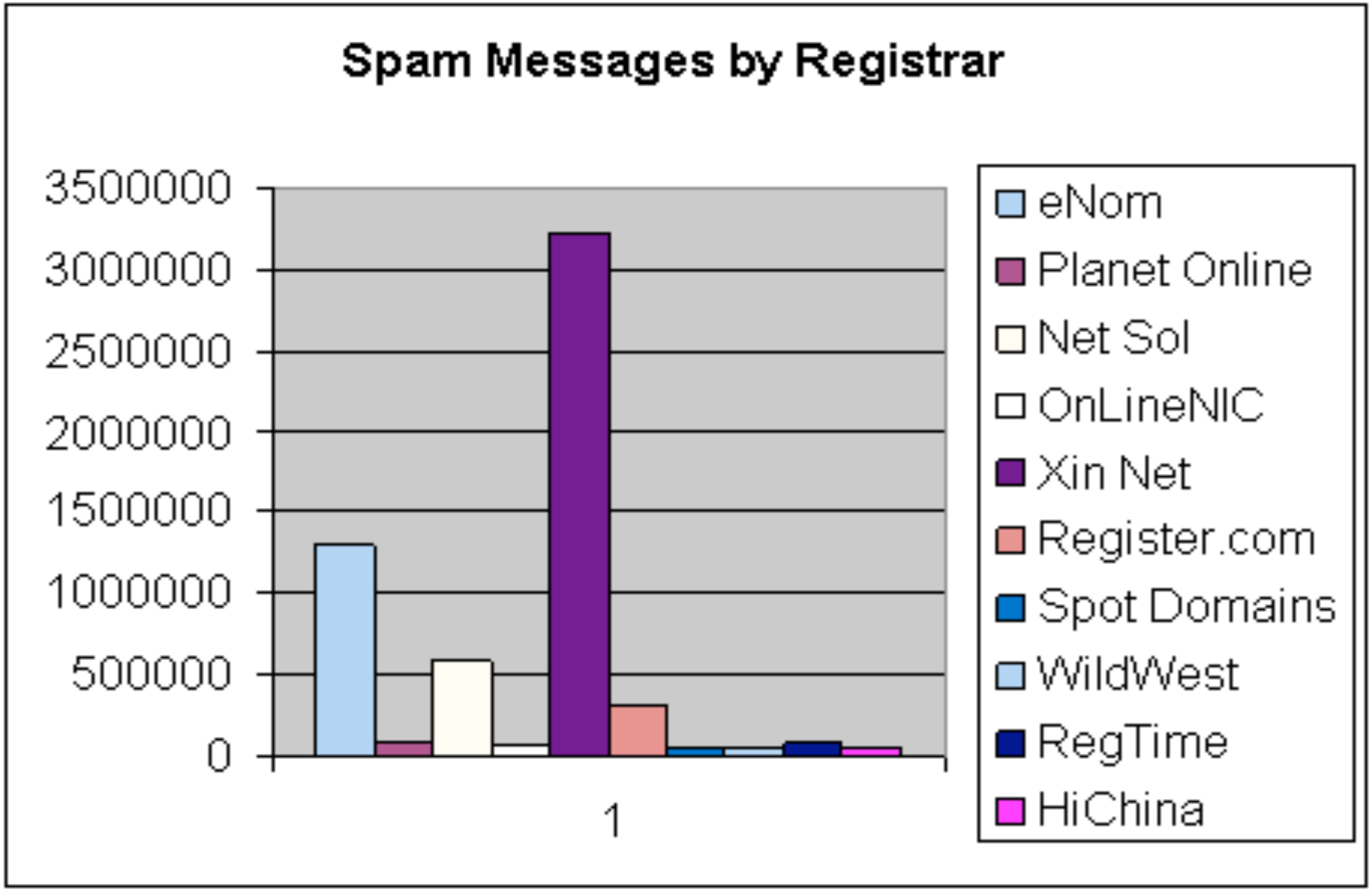
Top Ten Worst Registrars Feb 09

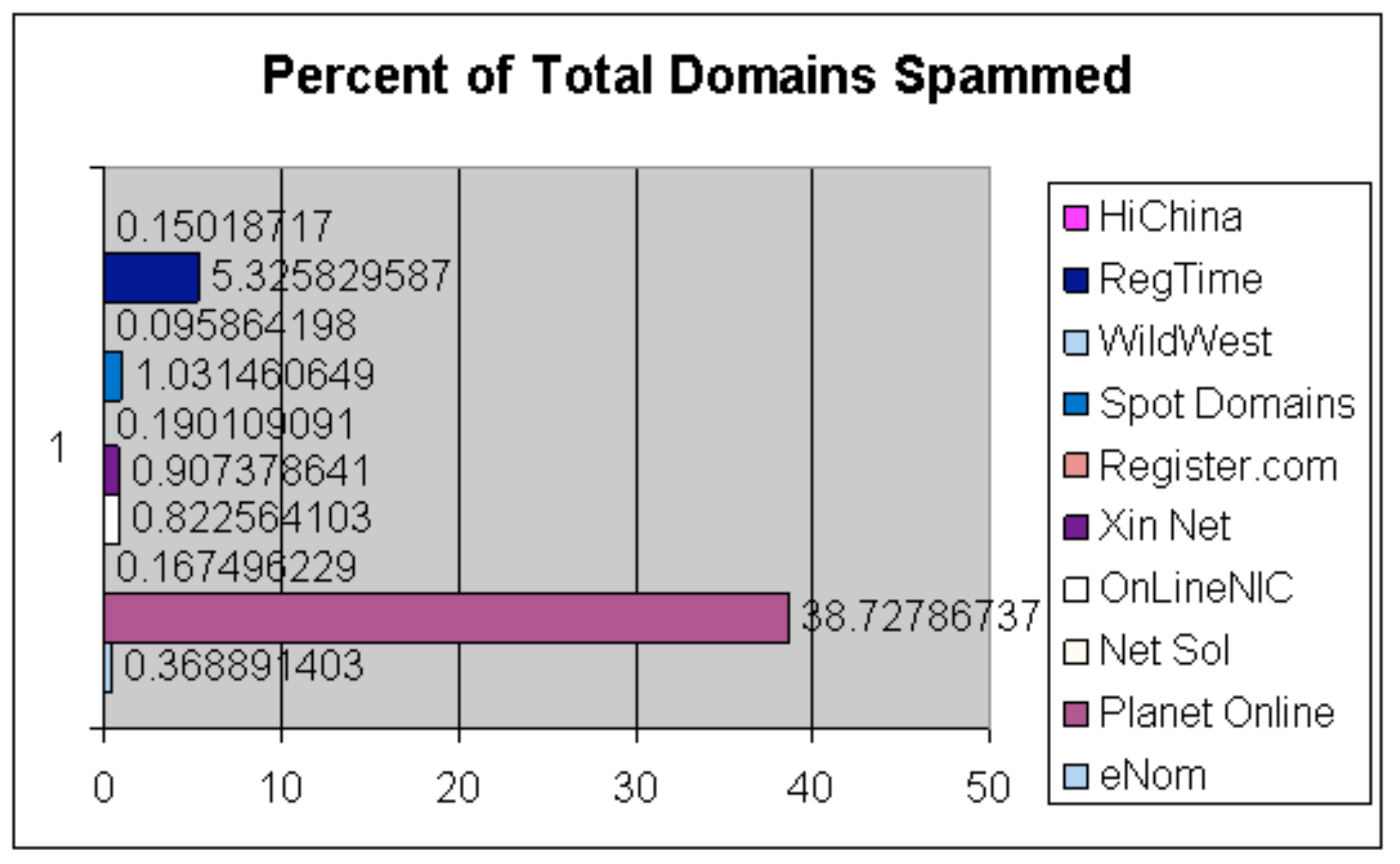
1. Xin Net
2. eNom
3. Network Solutions
4. Register.com
5. Planet Online
6. RegTime - 1st Russian registrar to make the list
7. OnlineNIC
8. Spot Domain/Domainsite
9. Wild West Domain
10. HiChina Web Solutions

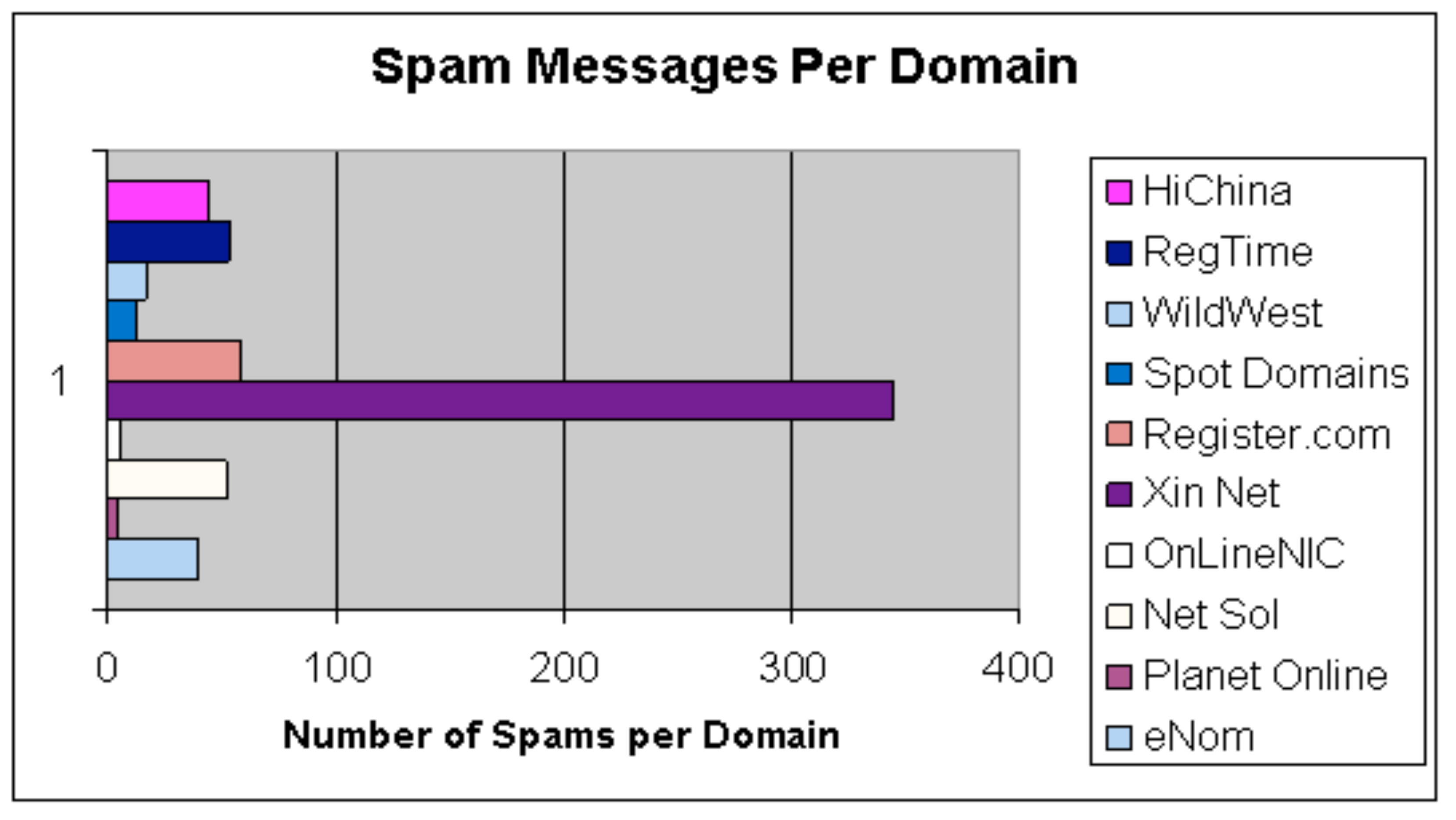
KnujOn’s Top 10 Criteria

- The raw number of domains held by the Registrar advertised in spam
- The number of spam messages used to advertise those domains
- The percentage of the whole Registrar portfolio that the spammed domains represents
- The rate of spam messages per spammed domain
- SUBJECTIVE: Is the Registrar Cooperating?


Spammed Domains From June 08 to January 09
35000
30000
25000
20000
15000
10000
5000
0
1
eNom
Planet Online
Net Sol
OnLineNIC
Xin Net
Register.com
Spot Domains
WildWest
RegTime
HiChina


Spam Messages by Registrar
3500000
3000000
2500000
2000000
1500000
1000000
500000
0
1
eNom
Planet Online
Net Sol
OnLineNIC
Xin Net
Register.com
Spot Domains
WildWest
RegTime
HiChina


Percent of Total Domains Spammed
0.15018717
5.325829587
0.095864198
1.031460649
0.190109091
0.907378641
0.822564103
0.167496229
38.72786737
0.368891403
1
0
10
20
30
40
50
HiChina
RegTime
WildWest
Spot Domains
Register.com
Xin Net
OnLineNIC
Net Sol
Planet Online
eNom


Spam Messages Per Domain
1
0
100
200
300
400
Number of Spams per Domain
HiChina
RegTime
WildWest
Spot Domains
Register.com
Xin Net
OnLineNIC
Net Sol
Planet Online
eNom

Use of English – Whois Record

- Common Language Use vs. Domination
- Historically true – Latin, French, English
- Future – Who knows? Maybe Chinese.
- Also historical – Whois record in English
- Change by replacement vs. addition = problem

New Whois Registrar Problem

- Chinese registrars are using Chinese characters
- *Registrar name, registrant, not address*
- Clearly hiding who they are
- Much of the whois record is in English
- No one else using their native language, yet

Policy Reform

- Transparency, stability and security
- More cooperation
- WI verification at registration
- Better control of resellers

Fake Online Pharmacies

- Controversial
- Not the same approach as Whois data accuracy
- KnujOn & LegitScript believe it is obvious
  - In the USA: no license, no prescription = no sale
  - Support of illegal activity against RAA
  - Income supports the criminal ecosystem
- Talking with Pharmaceutical industry (EU &US)

Fake Pharmacies

- *Pumped Up on the Internet* - LegitScript/Knujon Report
- Starting with steroids
- Branching out to all illicit pharmacy site
- Registrars have already shutdown hundreds of thousands of sites using our data

Views of Criminal Ecosystem

- Two Main Views
  - Law Enforcement (LE) view - Handcuffs
  - KnujOn View -Policy

- LE = Details (Lots...)
  - Financial theft & fraud, key loggers, hijacks,botnets
  - Arrest the Criminals
  - Blocklists
  - Spam filter & block

- KnujOn = It looks the same as legitimate activity
  - Fast Flux, domain resellers, DNS, Pharmacies
  - Fix and Enforce Policy

More Reform

- Make everyone obey the laws
- No need to disrupt privacy
- Registrars in transition to institutions
- Resisting, of course, but in the end…

Any Questions?

- Bob Bruen
  - bob.bruen@coldrain.net
  - http://www.coldrain.net/bruen
- Garth Bruen
  - garth.bruen@coldrain.net
  - http://www.knujon.com