KnujOn

RIPE
Amsterdam, the Netherlands
May 2009

Dr. Robert Bruen

KnujOn

- Dr. Bob and son Garth
- Started with fighting spam (90/10 inversion)
- Spam is the gateway for crime
- Policy Enforcement and sunshine
- Using whois data accuracy
- Registrars are the key – Domain Names

KnujOn's First Rule

It's all about the money

ICANN

Registrars

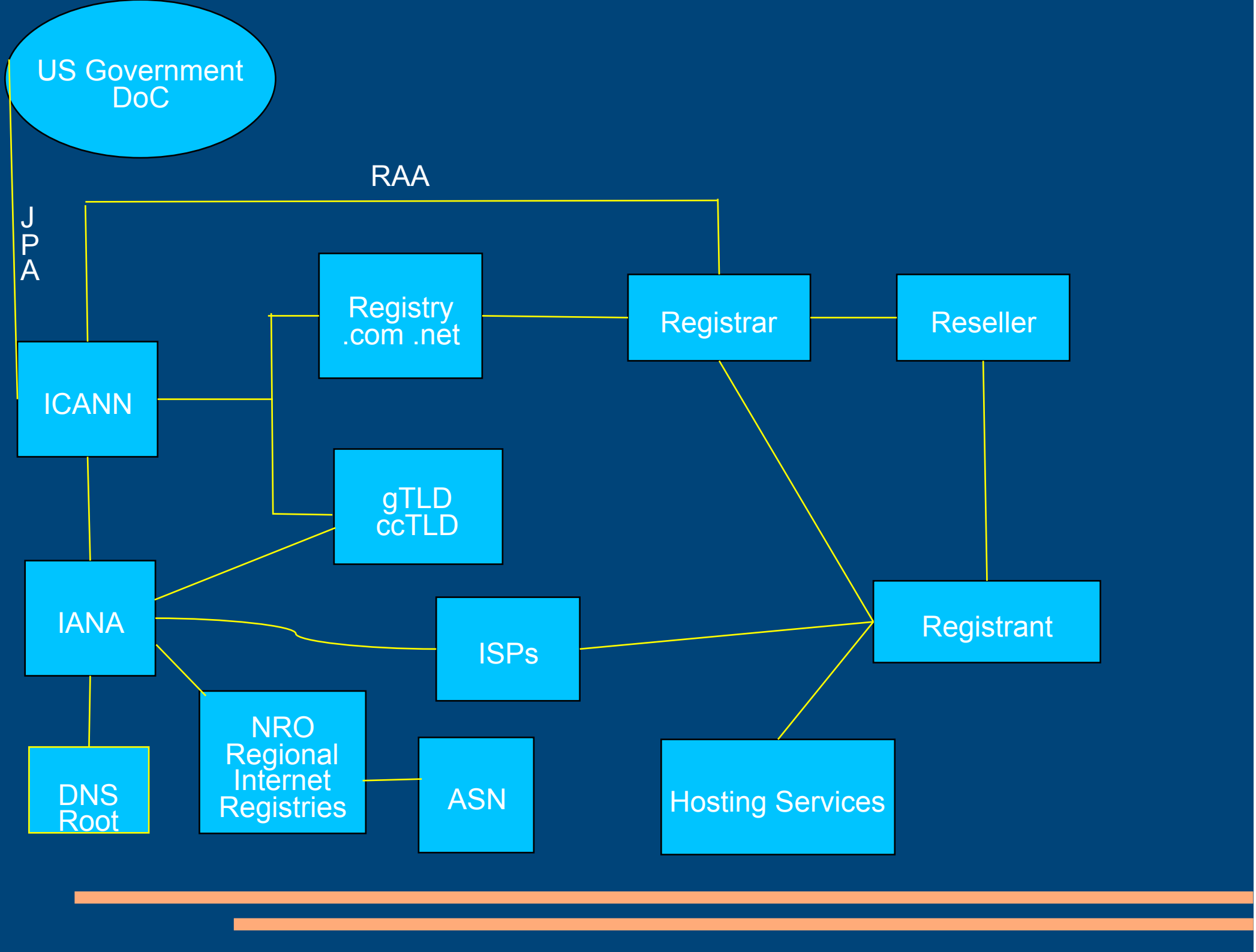
Resellers

ISPs

Criminals

Policies and Contracts

- Policies are in contracts/agreements/rules
- Critical that Policies are well constructed
- Bad policy creates problems
- Good policy helps decisions in novel situations


US Government
DoC
RAA
J
P
A
Registry
.com .net
Registrar
Reseller
ICANN
gTLD
ccTLD
IANA
ISPs
Registrant
NRO
Regional
Internet
Registries
ASN
DNS
Root
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)

KnujOn's Data Collection

- Not interested in personal information
- Publish reports daily for clients (web pages)
- Keep databases of emails
- Send all image spam to a researcher
- Keep data on registrars

Working with ICANN

- “You [KnujOn] are casting a big shadow”
  - Steve Crocker. ICANN BoD
- KnujOn now an ICANN ALAC ALS
- Garth co-chaired ICANN E-Crime Summit in March
- Contributed to RAA recommendations for change
- Contributed to ICANN's new WDPRS

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

What Happened

- EstDomains lost accreditation
  - Domains transferred to Directi
- PDR (Directi) – cooperating
- Intercosomos/Directnic - improving
- Joker – breach notice - improving
- Beijing Networks – breach notice - improving
- Moniker – Market losses improving
- Dynamic Dolphin – Market losses & lawsuits
- Parava networks recently deaccredited

On Top of That...

- Atrivo/Intercage report by HostExploit.com
  - ISPs stopped doing business with them
  - A/I never recovered
- McColo report by HostExploit.com
  - ISPs stopped doing business with them
  - McColo never recovered completely
  - Spam has only reached bottom of previous range
- Ukranian takedown UkrTeleGroup Ltd. 30Jan09
  - Spam levels drop dramatically, like McColo
  - Within a day, backup to highest since McColo

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?

Policy Works

- The struggle against spam has been long
- Success has been hard to come by
- This past year has been the best so far
- The bad guys keep coming back, of course
- We know it can be done

KnujOn and the ICANN WDPRS

- New ICANN complaint system in place
- One time complaints and Bulk complaints
- Greater capacity & Better design
  - 3 orders of magnitude problem
- Password protected (Bulk)

Registrars

- Lots of pushback
- Deny responsibilities
- Some success with Fake Pharmacies
- Reseller issues
- In dire need of reform

Attacks on Registars

- Recent
  - DomainTheNet Israel Jan 2009 “Team Evil”
  - NetSol/CheckFree Dec 2008
  - Comcast May 2008
- Not really that new
- SSAC Report: Domain Name Hijacking 2005
  - panix.com
  - hushmail.com (NetSol)
  - HZ.com
  - Etc.

Wholesale Registrars

- Registrars who use resellers, some exclusively
- Examples: Tucows, NetSol, eNom
- Has legitimate purpose
- Also has problems:
  - New attacks on registrars
  - Resellers not held accountable by registrars
  - Used as a channel by the bad guys

New Whois Registrar Problem

- Chinese registrars are using Chinese
- Registrar name, registrant
- Clearly hiding who they are
- Much of the whois record is in English
- No one else using their native language, yet

Registrar Reform

- Transparency
- More cooperation
- WI verification at registration
- Better control of resellers
- Perhaps Open International Organization

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

Fake Pharmacy Notes

- Most registrars have some Fakes Pharmacies
- Worst registrars concentrated to 20 or so
- Top 5 each have 1000 or more domains
- Bottom 5 each have about 200 domains
- Fast Flux Misuse

Beyond Fake Pharmacies

- Anything to take your money
- Charity Fraud, Identity Theft
- Credit card theft, Mortgage Fraud
- Phishing of all sorts
- Malware of all sorts

Criminal Ecosystem Evolving Always

- World wide, distributed system
- Getting more organized every day
- Code writers getting smarter
- Architecture becoming more robust
- Happy to sacrifice low level workers
- Attacking all parts of the Infrastructure

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

Any Questions?

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