Community Response to Inter-network Abuse

NANOG 37
June 2006, San Jose, CA

Rick Wesson
Support Intelligence
rick@SupportIntelligence.org

Problem Statement

- Identifying abuse on your network is hard
- Frequently involves another network
- Most customers are unaware they are compromised, and the number is huge
- Once identified, how to communicate abuse across separately managed networks is unclear

Identifying Abuse

- Realtime DNS Black Lists
- IP Based
  - SpamHaus, SORBS, WPBL, etc
- RHS (name) based
  - URIBL, SURBL, etc

Identifying Abuse (cont)

- Spam Traps
- Proxy Lists, Proxy Hunters
- Honey pots (http,socks{4,5})
- DNS (fast flux/hopping glue)

Spam Traps

- Uses special MX server for 10K domains
- Implements EVIL-SMTP
- Filters mail, dynamic feedback, automated RBL promotion
- 1.5M messages/day (< 2msg per ip)

Bots and Proxies

- Web search for “open proxy”
- Proxy hunters now pay for proxy lists
- Proxy forums and lists, irc channles
- Proxies (open or closed) used in click fraud
- Botnets used as computing platform

Honey Pots

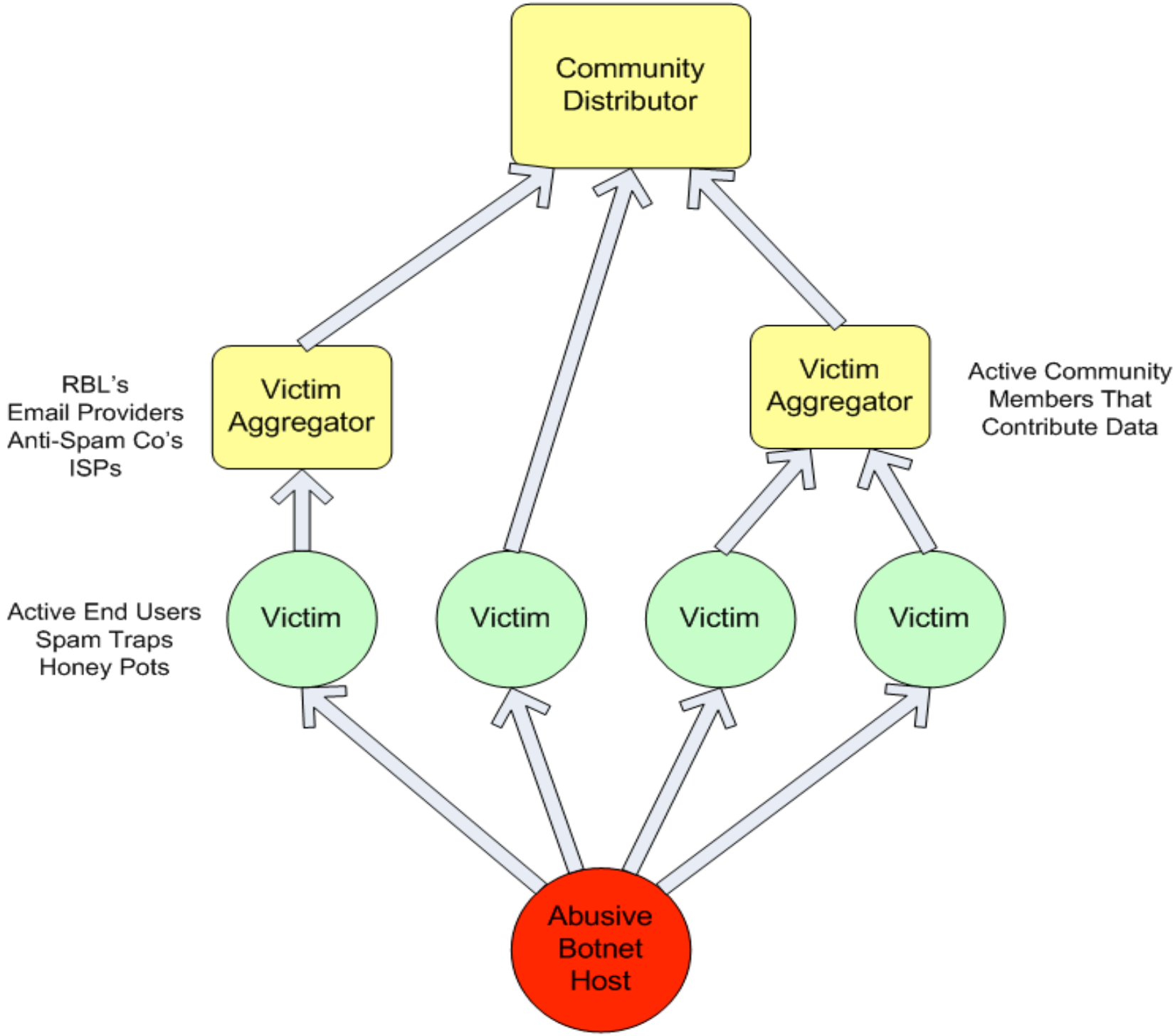
- Hosting Services to mine their abuse
- DNS Hosting (dynDNS)
- Domain Registration (Registrar)
- Proxy Pots (building open proxies)

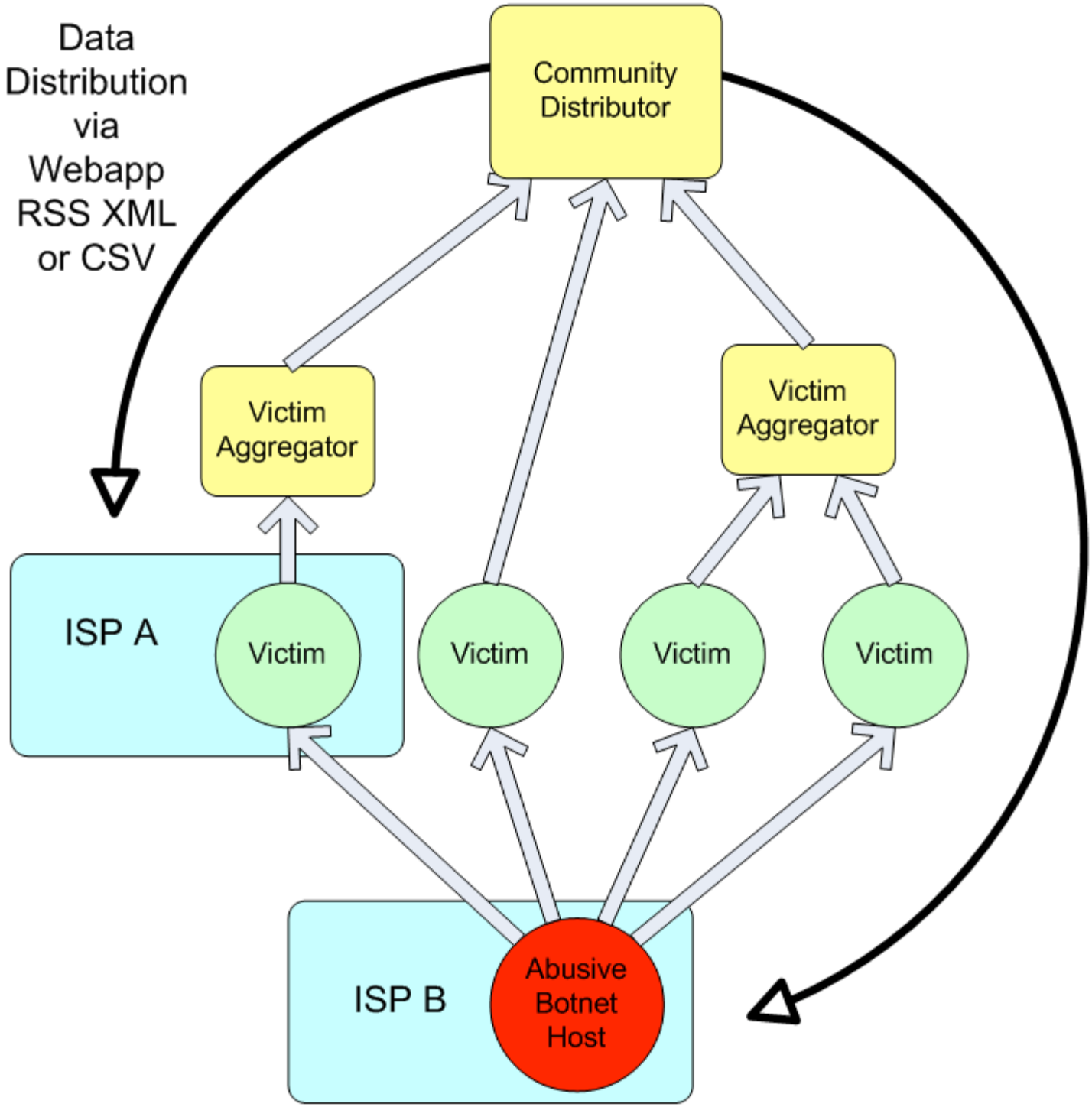
Mining the DNS

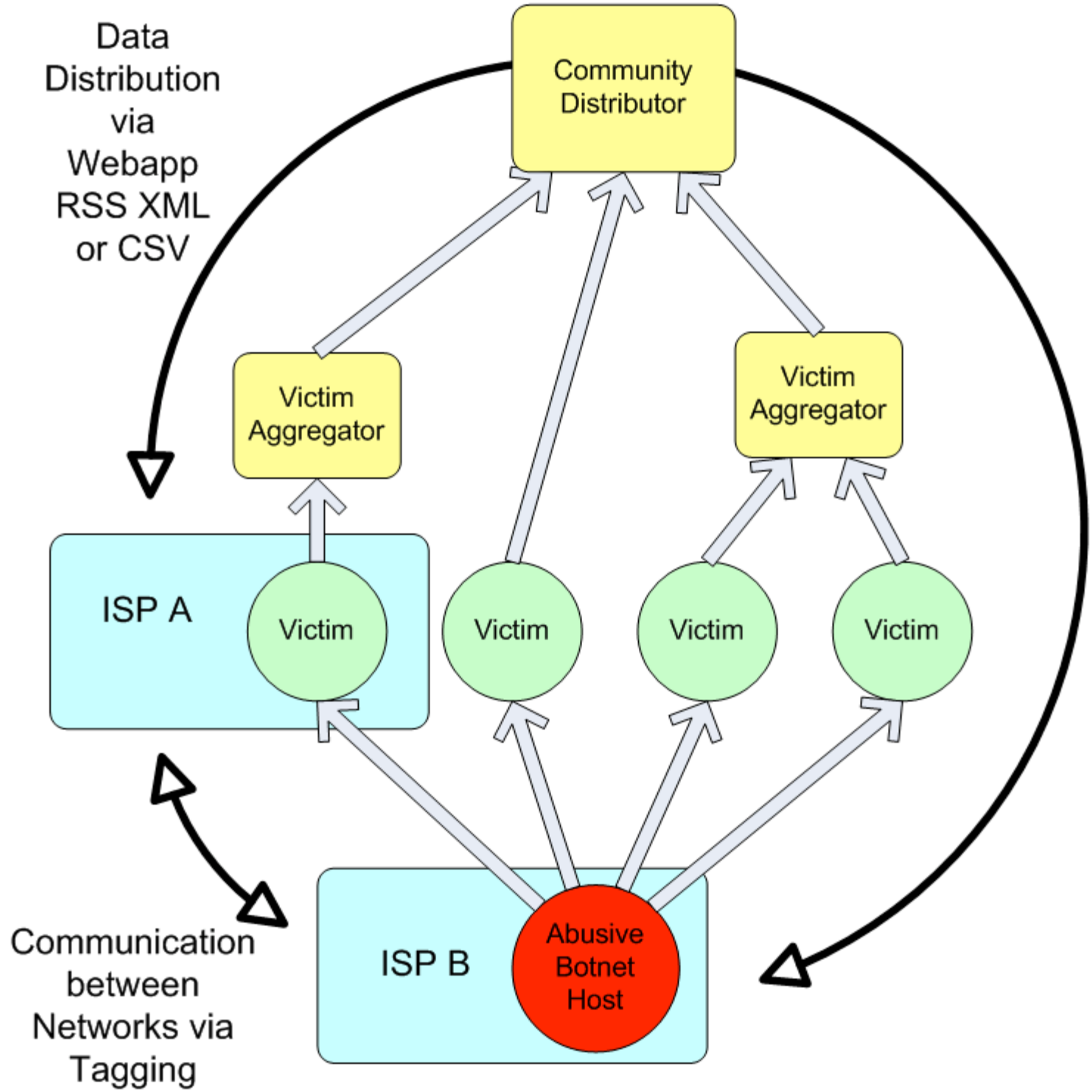
- Hosting dns RBLs Mirrors
- Hosting DNS
- Fast Flux and Hopping Glue (fast moving NS glue)

Review of last work

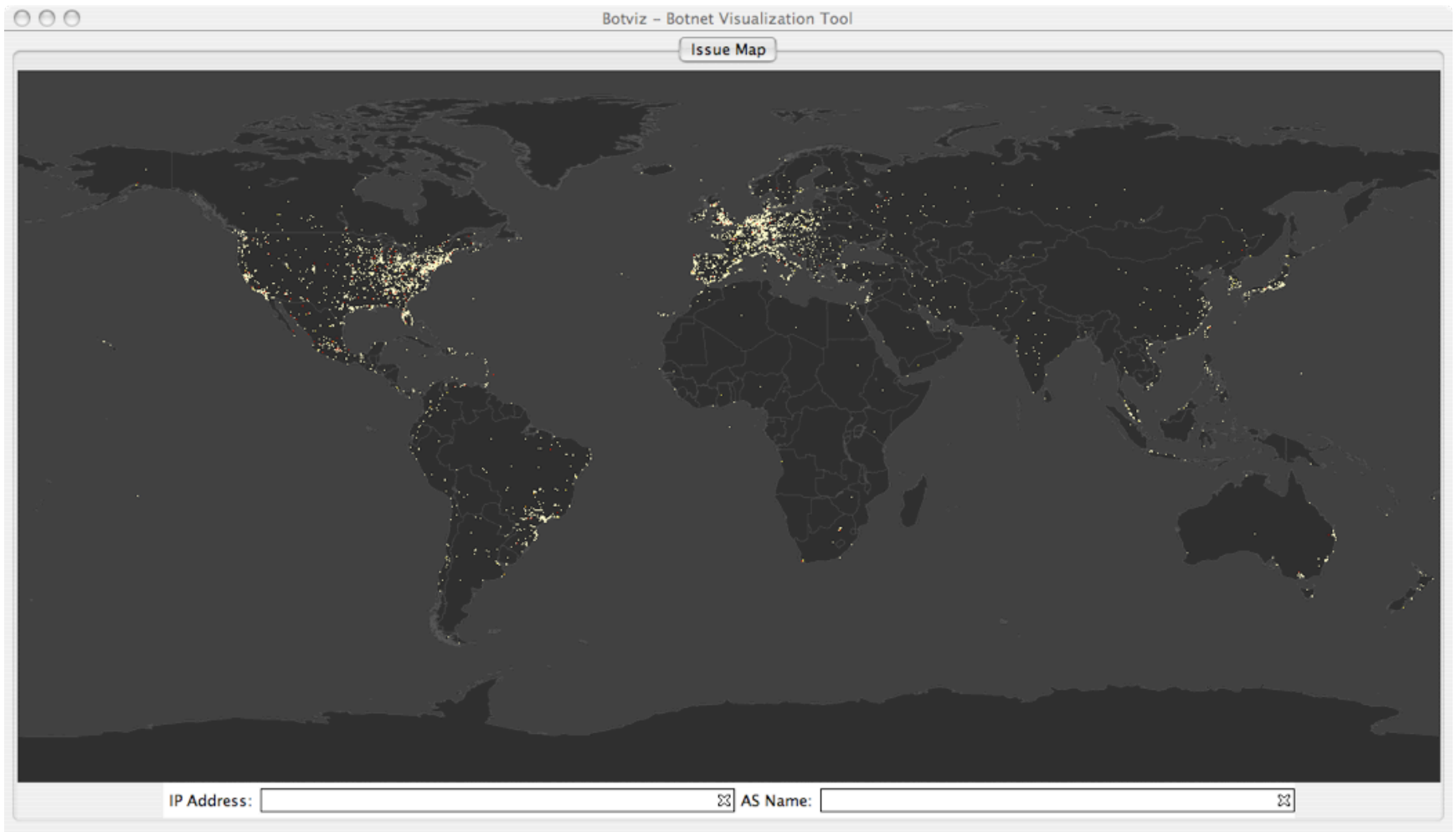
- Simple email Reporting on ASNs
- Basic aggregation of 6 RBLs
- Hard to get timely data out of the system
- Difficult to measure effectiveness


Community Distributor
Victim Aggregator
Victim Aggregator
RBL's
Email Providers
Anti-Spam Co's
ISPs
Active Community
Members That
Contribute Data
Victim
Victim
Victim
Victim
Active End Users
Spam Traps
Honey Pots
Abusive Botnet Host


Data
Distribution
via
Webapp
RSS XML
or CSV
Community
Distributor
Victim
Aggregator
Victim
Aggregator
ISP A
Victim
Victim
Victim
Victim
ISP B
Abusive
Botnet
Host

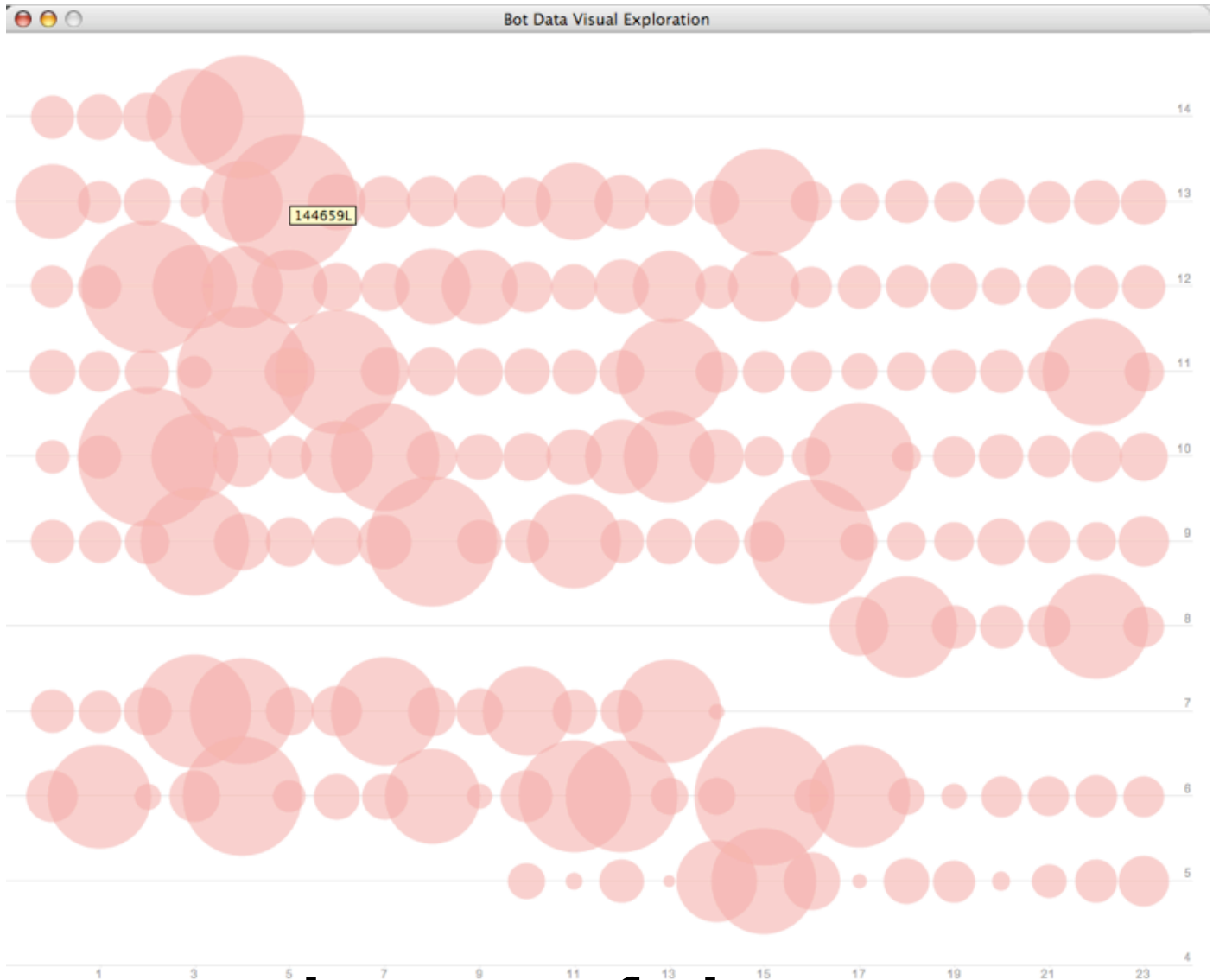

Data Distribution via Webapp RSS XML or CSV
Community Distributor
Victim Aggregator
Victim Aggregator
ISP A
Victim
Victim
Victim
Victim
Communication between Networks via Tagging
ISP B
Abusive Botnet Host

Visualizing the problem



5pm to 6pm PST Feb 8th 2006

Event Clusters



Day of Month

hour of day

Daily Stats

- New Issues per day 1.2M unique
- Spamvertisements 6K unique URIs
- Phish and Malware 50-100 Domains
- 50-75 Active Hoping Glue Name Servers

REACTb Tool

- REACTb
  - Response
  - Environment for
  - Accountability, Cooperation, Trust
  - and Beer

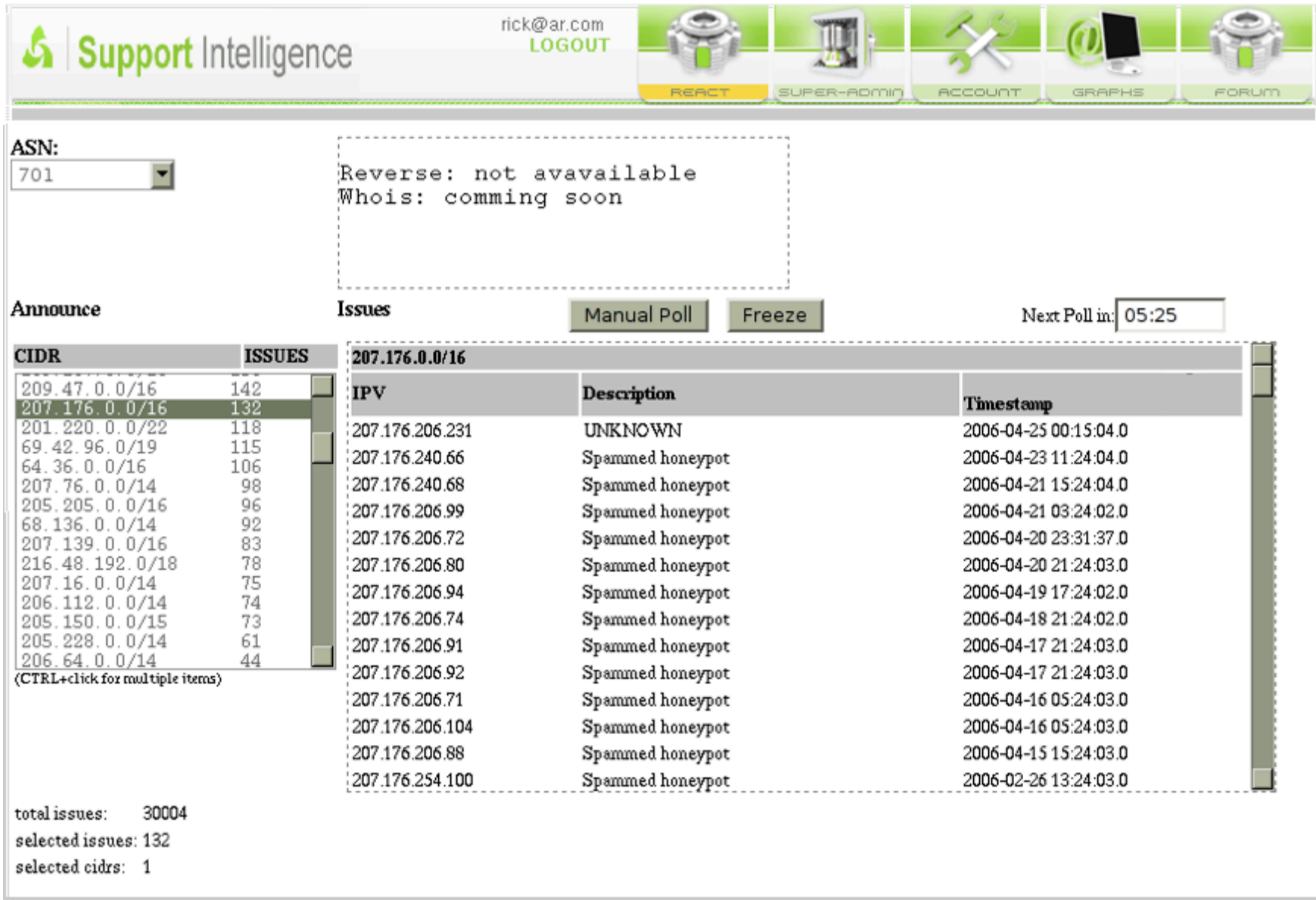
How to Use REACT

- Web based tool for the introspection of BGP announcements and abuse
- Many way to copy data out using CSV, XML, or RSS
- Authenticated logins with sub delegated accounts

Signup Process

- see http://Support-Intelligence.com/
- register, list at least one ASN
- We verify POC is in-fact the correct POC for the resource using whois information, telephone (inoc-dba) or the postal mail
- Your account is then authorized or denied

Demo Screenshot



Available Data Feeds

- XML formatted streams
- Jabber (XMPP) clients
- eMail Alerts

Submitting Data

- Simple XML or Text Formats
- Rsync or scp pickup
- HTTP REST API

Feature Roadmap

- RSS everywhere
- Trend and History Reporting
- Graphs and Visuals
- Public and Private Tagging
- Time and Relevance navigation
- geo IP Maps
- more dns/domain views

Next Steps

- continue to seek vet and incorporate new data sources.
- seek and obtain additional funding sources (no vc please, its a lifestyle company)
- acquire feedback and improve tools

Special Thanks to the Following

- SpamHaus, URIBL, SURBL (RBL mirrors)
- Paul Vixie and Bill Woodcock (BGP feeds)
- David Ulevitch, Freedom Networks (hardware donation)
- Aaron Hoover - UC Berkeley (GeoIP Issue Mapping Tool)
- Registrars, gTLD Registries (DNS meta data)

Thanks

see http://Support-Intelligence.com

rick@Support-Intelligence.com

adam@Support-Intelligence.com