ISC SIE

Internet Systems Consortium
Security Information Exchange

Exchange Concepts

- Operator is a neutral trusted intermediary
- Participants are often direct competitors
- Examples
  - Internet traffic (PAIX, Equinix)
  - Equity/futures (NYSE, NASD, CMOT)
  - Telco/MMR (TelX, CRG West)

Security Information

- Raw captured data, for baseline characterization
  - may also include evidence of malfeasance
- Reprocessed data, with value added
  - duplicate suppression? format conversion?
- Directed observations
  - honeypot and spamtrap droppings
- ...all having one universal property:
  - "this would be more valuable if more folks knew it"

Sharing Sensitive Information?

- Nondisclosure agreements with one's customers
- Implied, pass-through, or other liability
- Privacy laws in origination and collection locales
- Loss of prospective competitive advantage
- Public relations nightmare (AOL search results?)
- Audit costs for data sharing agreements
- Leak to malfeasants (sensor illumination)

ISC SIE (1)

- Secure datacenters (at ISC HQ, and soon PAIX)
  - Private LAN switch, channelized using VLANs
  - Switch connections managed/vetted by ISC staff
  - Connected devices audited/monitored by ISC staff
- Rules on subscribers are set by sensor operators
  - “No backhauling the raw data, do all analysis locally”
  - “Anonymize sensor operators and sensor locations”
  - “Report back anything interesting you discover”

ISC SIE (2)

- ISC also has some rules for subscribers
  - no direct monetization – you can use SIE in conjunction with other data, to enhance products or services, but you can't build a product/service out of it
    - that's an activity ISC reserves for itself, to fund SIE
  - respect end user privacy – you can't use SIE to improve the quality of advertising activities or cookie tracking; nor do direct or indirect targeted marketing of end user security products and services
    - basically this means “don't annoy people”

Current Lineup

- Existing channels
  - vlan 2: authoritative DNS responses heard by recursive servers as a result of cache misses
    - note: we don't collect rcode=3 (NXDOMAIN)
    - February 2008: about 8 MBit/sec
  - vlan 3: DNS queries heard by authority servers as a result of cache misses
    - most of this is RBL lookups given our current sensors
    - February 2008: about 20 MBit/sec

Coming Soon or Someday

- The Malware Channel
  - {*md5,sha1,URI*}
    - “hash of a honeypot turd, dowload at *URI*”
- The Phishing Channel
  - {*URI1,rating,URI2*}
    - “spam contained *URI1*, see the body at *URI2*”
- Premium/payperview?
  - channels could be sponsored by participants, with access control by private bilateral agreements
- Reprocessing?
  - duplicate suppression?

Non-packet-related services

- VLANs, UDP, broadcasts, binary – yikes!
- Some suitably anonymized derivatives can be downloaded from ISC under separate agreement
  - example: list of domain names seen in a day
- Some suitably anonymized views can be queried by a web browser (under a separate agreement)
  - example: fast flux DNS history

Demo, first cut, whois

```
% whois -h ::1 'address-associations 198.63.208.223'
           xowner           |          rdata
----------------------------+--------------------------
 114.239.65.58.in-addr.arpa | 58-65-239-114.myrdns.com
 5yearscontract.com         | 58.65.239.114
 bulletproofstuff.com       | 58.65.239.114
 deluxenote.com             | 58.65.239.114
 faxmonitoring.com          | 58.65.239.114
 itsnotjoke.com             | 58.65.239.114
 medicasntred.com           | 58.65.239.114
 mynameisseller.com         | 58.65.239.114
 ns1.crewsins.com           | 58.65.239.114
 polanddreams.com           | 58.65.239.114
 toneandpulse.com           | 58.65.239.114
 tredinsa.com               | 58.65.239.114
 vertuslkj.com              | 58.65.239.114
 warinmyarms.com            | 58.65.239.114
(14 rows)
```

Ideal Sensor Operators

- Busy recursive nameservers
  - ISP/MSP
  - Education
  - Mid/large enterprise
- Busy authority nameservers
  - Managed DNS hosting including ISP/MSP
  - TLD or mid/large SLD
  - *no root nameservers, not even f-root!*

Ideal Participants/Subscribers

- High-end internet security companies (eg, Arbor)
- Nonprofit publicbenefit projects (eg, CastleCops)
- Law enforcement or L.E. support (eg, CERT)
- ISP abuse desks
- Industrial research
- Academic research
- *Basically anyone who's wanted to use or build a passive DNS system or anything like RUS-CERT's*

Fees

- Noncommercial public benefit use might be free
  - big universities or LEOs can't really cry poverty
- Other use is by annual subscription
  - fees for switch port, download, and/or online access
  - big discount for anyone who also supplies data
  - moderate discount for members of OARC, ISC BIND Forum, ISC DHCP Forum
- *Keep in mind ISC is a 501(c)(3) – if we make extra money from this we'd spend it on BIND 10.*

Moral Imperative

- Internet makes communication easier for everybody, including thieves, attackers, snoops
- Organized criminals now prefer the Internet to guns, it's safer and more profitable for them
- Why purse snatch when you could key log?
- The innovators who helped create and expand the Internet have therefore made the world less safe
- We must now start fixing what we've broken