Security Information Exchange
NANOG 44 Parlor Tricks

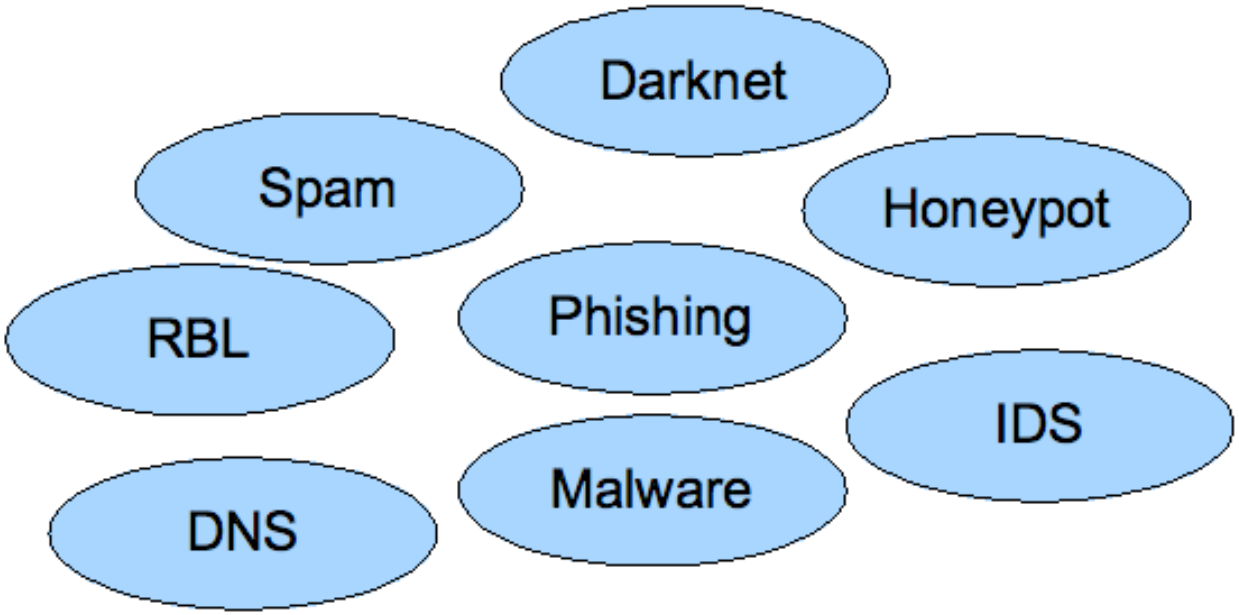
https://sie.isc.org

info@sie.isc.org

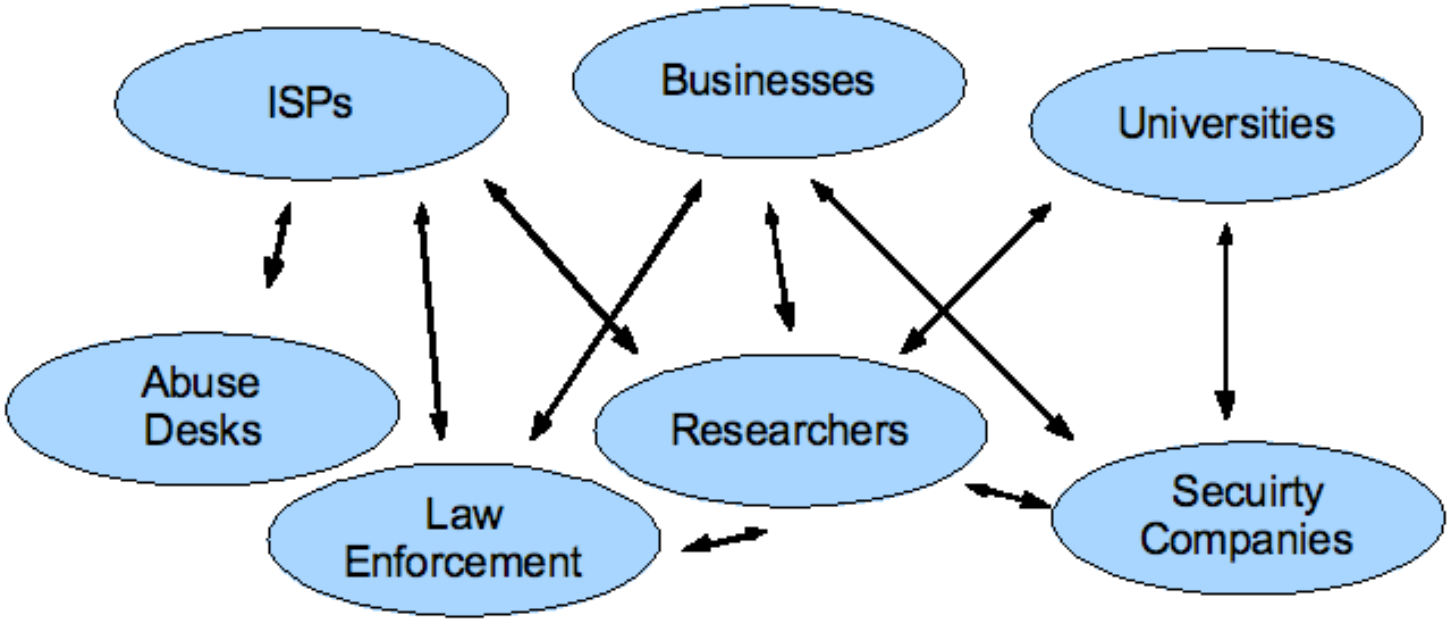
What we are solving

- Security industry is “stove piped”
  - Combined data => network effect
- No trust nor privacy framework
  - Common legal agreement - neutral carrier
  - Common well-understood privacy framework
- Internet is not efficient nor reliable
  - Fast localized lossless switch backplane
- Not centralized
  - Common platform more efficient - real-time
  - Avoid duplication of effort (prod/consumer)

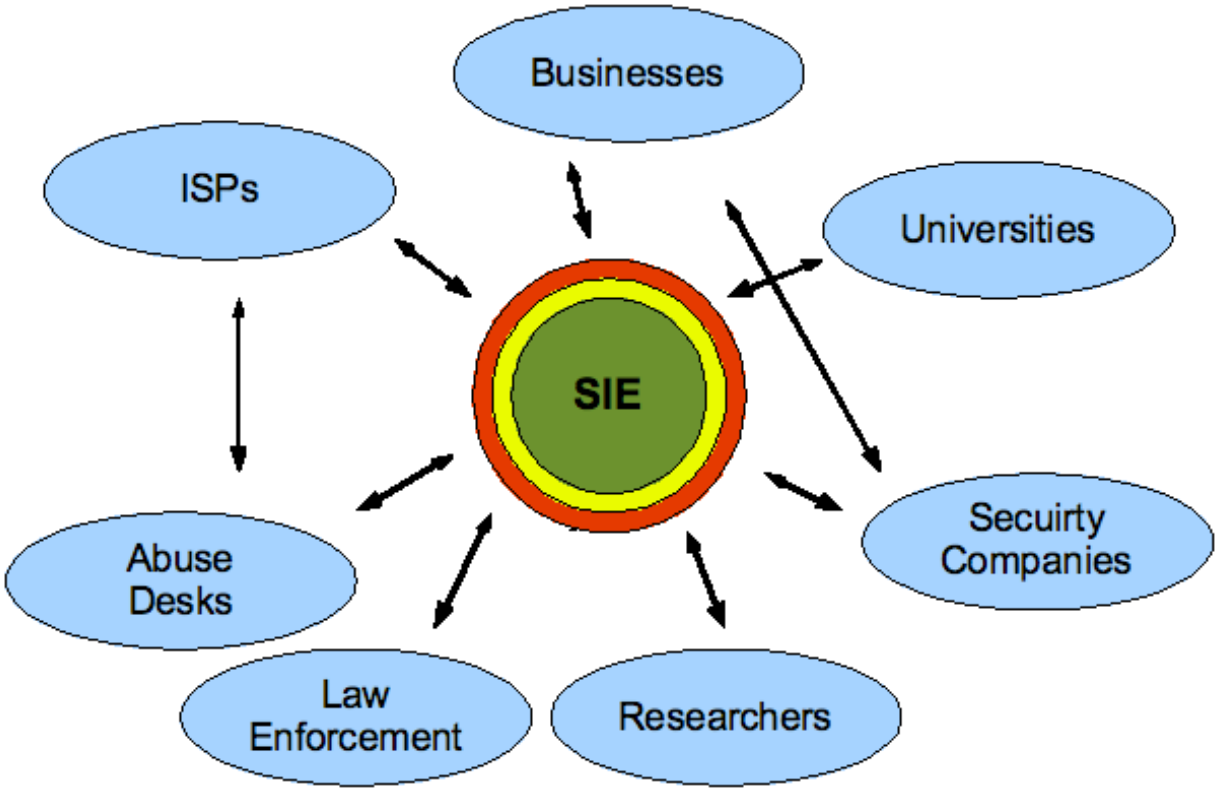
Problems (stove pipe)



Problem (not centralized)



Solution (centralized)

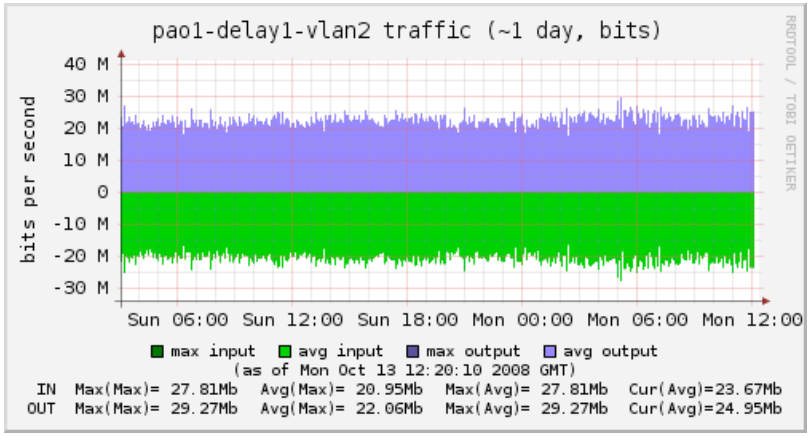


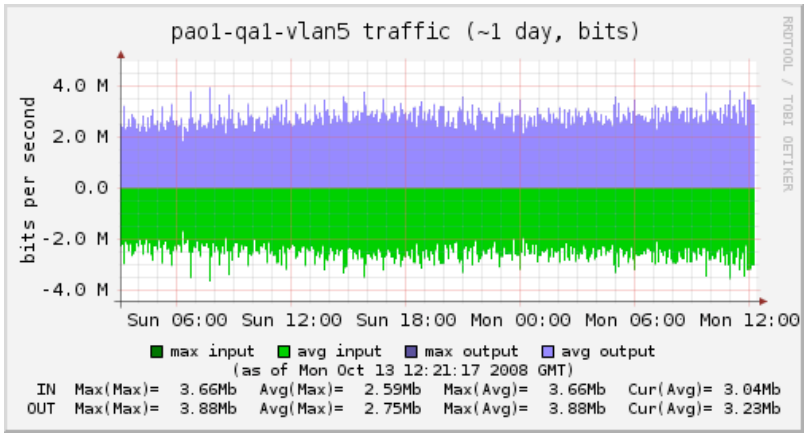
Channels

- Ch2 - Raw Passive DNS
- Ch5 - Dedupe Passive DNS
- Ch8 - Double Fast Flux DNS
- Ch9 - RBL-tagged DNS
- Ch3 - Authoritative queries
- Ch4 - Netflow
- Ch6 - Legacy root queries
- Ch7 - Queries (unicast)
- Ch10 - URL link pairs

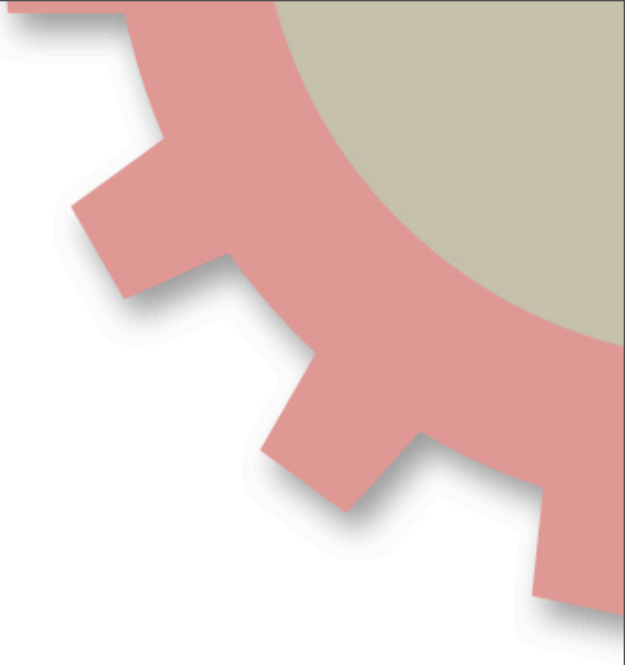
Data distilling

- can’t process with single box
- raw uploads -> ch2 (22 Mbps)
  - ch2 + dedupe module --> ch5 (4 Mbps)
    - ch5 + ns diff module --> ch8 (400 bps)
    - ch5 + CBL/SORBS lookups -> ch9 (300 Kbps)





Examples



- Phish damming
- Shooting phish in a barrel
- Web lookup tool
- Kaminsky attack detection

Phish damming

- Gov't researcher: -1 day phish
- Recipe
  - Start with passive DNS data ch5
  - Grep common phishing names
  - Compare A records to AS numbers
  - Pattern finds current phish site
  - Lookup reverse or nameserver info to find other yet-unused phishing domains BEFORE they ever send email
  - Subpoena -> takedown (ICANN help?)

Shooting phish in a barrel

- Recipe:
  - Grep double fast-flux DNS channel data for your trademarked name and find all the domain lookups that the phishers are using
  - ncaptool -l 169.254.8.255/7433 -mg - -e “ “ | egrep bankofamerica
  - Real time!
- General scanning:
  - Lots of false positives from CDNs
  - Compare to other data (eg: CBL/SORBS lookups)

Web lookup tool

- What domains does ns-ext.vix.com serve?
- What domains are hosted on 208.74.184.51?
- What else is on their net?

Kaminsky attack detection

- ncaptool + mod_urstate module
- ftp://ftp.isc.org/isc/ncap
- dns-oarc.net
- ICMP backwash from bad port selection
- recursor <-> auth server

Future channels

- ncaptool -> 2.0 (nmsg)
- Spam headers
- Malware metadata
- Phishing URLs
- Outgoing scan data
- Email reputation / spamassassin
- Darknet
- Pay per view (eg: flash-mob URL, ISC domain survey, bots!)
- Anonymized tattletale networks - real-time abuse consolidation

SIE - Out of darkness into light