Passive DNS and ISC SIE

Paul Vixie, ISC

Passive what?

- When a “full resolver” (caching, recursive) gets a question it cannot answer from cache
  - query is forwarded to the best known authority (root, TLD, SLD, etc)
  - response is eventually received, cached for reuse, and sent back to original asker
- In “Passive DNS”, these responses from authority servers are also collected, stored, and analyzed
  - no “personally identifiable information” here

Uses for Passive DNS

- Detect security problems
  - known-bad address used under a new name
  - known-bad name has a new address
  - many other exotic possibilities
- Analyze and characterize the D. N. System
  - what is it really being used for?
  - what does it really contain?
- Reconstruct the visible parts of distant zones
  - look, ma! no zone transfers!

History

- Florian Weimar invented this concept
- Implementation in academia
  - GNU ADA, Berkeley DB
  - Sensors in European ISPs & Universities
  - Original intent: zone content recovery
- Used today by world wide LEO community
- “Inverse directory” & botnet hunting
  - what names map to “this” address?
  - when was “this” name first used and by whom?
  - who has looked up “this” botnet C&C name?

Upcoming Alternatives

- April Lorenzen, sponsored by ISC
  - Implemented in Perl & PostgreSQL on FreeBSD
  - Uses NSF funded hardware (OARC)
  - Text-y, emphasis is on web GUI
- Florian Weimar (redux)
  - Wants to try SQL (vs. Berkeley DB)
  - Strong non-text-y schema
  - Emphasis on performance

Hazards of Decentralization

- Every new passive DNS effort has to solicit sensors (instrumented recursive NS)
- Due to ops+BW costs, few sensors can feed more than one passive DNS system
- Thus, sensor population is heavily diluted
- ➔ Perhaps a central solution is warranted?

Hazards of Commercialization

- Huge datamining opportunity for spammers
- There might be some problems, though:
  - National privacy laws
  - ISP privacy policies
  - Competitors getting hold of it
- Perhaps a trusted nonprofit could help?

Proposed Solution: ISC SIE

- PCAP-based data capture tool (NCAP)
  - similar to tcpdump and dnscap
- Lightweight relationship for sensor operators
  - get and install the free/open sensor software
  - exchange security keys
  - upload batches using SSH/SFTP
- Central collector operated by ISC
  - receives batches, rebroadcasts on a LAN
  - each passive DNS project sits on that LAN

Roles and Responsibilities

- Sensor operator – instruments a nameserver to collect incoming authoritative responses and share them via ISC SIE
- ISC Security Information Exchange – receive collected response data and share it in real time with Passive DNS projects
- Passive DNS projects – get to hear all kinds of interesting collected response data, and study/analyze it

Future of ISC SIE – Security Information Exchange

- Passive DNS is the first thing to be carried by the ISC Security Information Exchange
  - conceptually, this is an “easy sell”
  - Passive DNS created earlier by Florian Weimar
- Syslog is the next frontier
  - information about rejected spam e-mail
  - information about failed SSH logins
- Selection criteria for future data types:
  - more interesting by daylight than by flashlight
  - time-value is steep – must be shared in real time