ONZRA

Recursive DNS Cache Auditing

Jose Avila III
Founder, ONZRA

Who Am I?

- One of the founders of ONZRA
- Security Researcher
- Previous Lead Developer at NeuStar for the Managed Internal DNS and SiteBacker2 products

N Z R A

ISC OARC

Cache Poisoning Is Not New!

- We find out we were poisoned when services start failing!
- There is a need for a notification system
- Why aren't there solutions to detect this?

Where Does ONZRA Fit In?

- Developing a Cache Verification Tool
  - Verifies changes seen in cache
  - Alert on potential Cache Poisoning Events
  - Similar to DoX concept

How Does It Work?

- Takes a dump of the in-memory cache
- Finds differences with an old dump
- Verifies the changes
  - Checks authoritative servers
  - Checks peer recursive servers
- Alerts if results could not be verified

Features

- Recordset comparison
- Content Delivery Network detection
- Record type based comparison
- Threshold based peer approval
- History tracking
- Alerting based on percentage of change

Content Delivery Network Detection

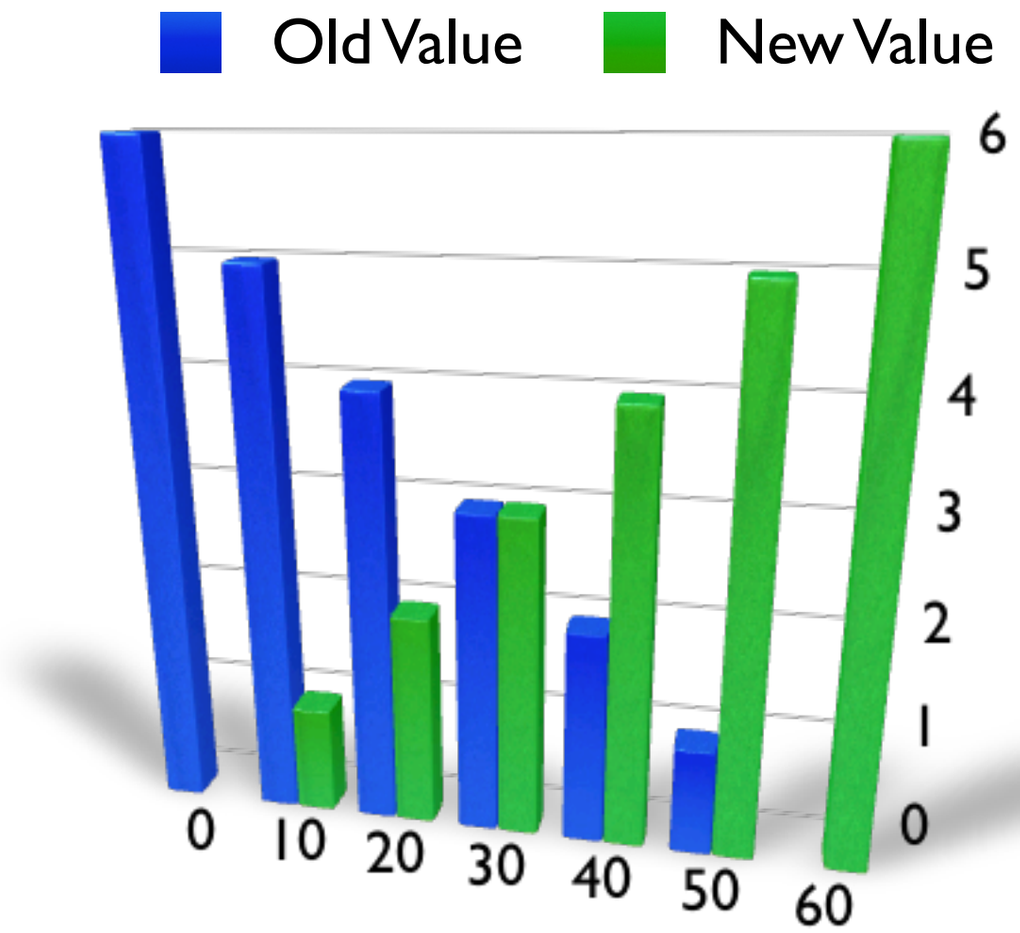
- Detected by comparing the record sets amongst the peers
- Can lower the alert level

Record Comparison

- Ordering of records does not matter
- We don't have to verify everything
- What we do not verify:
  - MX Record: Preference
  - SOA Record: Serial, etc.

Threshold Based Peer Approval

- Based on the threshold of required peers we need to alter our probing interval.
- If too much time passes we will not be able to verify with peers



Probe Interval

- Verify Freq. = TTL-(THRESHxTTL/PEERS)
- Verifying against:
  - 20 Peers
  - 10% Threshold
  - 120s Min TTL
- Need to verify cache every 108 seconds

History Tracking

- Stores a history of prior record sets
- If the record is not verified by peers its verified against historic values

NZRA

ISC OARC

Detecting Fast Flux

- Value changing quicker than the TTL
  - Peers will have multiple values represented
    - Screws up prior formula
- How can we verify these?
  - Shared DB of historic data?

Tool Components

- TCP Daemon (Listens for Cache Dumps)
- Cache Dump Parsers
- Cache Compare
- Application Cache
- CDN / Fast Flux Detection
- Alerter (Currently only SYSLOG)

What Resolvers Are Supported?

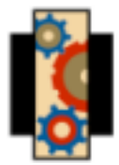
- Currently Supported
  - Microsoft DNS
  - Bind
- Supported eventually
  - DJB DNS w/ custom Patch
  - PowerDNS

Future Features

- Cache Verification Service?
  - More Research Data
- Multiple Query Nodes
  - Better CDN Detection
- Use peer cache dumps instead of querying
- Interaction with other DNS Projects

Questions?

Jose.Avila@ONZRA.com
Keith.Myers@ONZRA.com



ISC OARC