Redns

Matthew Faltys
IASC 4580 - 5.4.17

Goals

- Build a free and open tool
- Easy to set up (features ‘sane-defaults’)
- Able to leverage public malicious domain lists
- Low footprint
- Fast

User Stories

- As an administrator, I want to add new blacklisted domains to keep my clients safe.
- As an end-user, I want non-intrusive malware indicators so I am not distracted.
- As an administrator, I want to stop malicious intent to keep my users safe.
- As an administrator, I want to follow traffic on a per-ip basis to track down malicious software swiftly.
- As an organizational manager, I want an indicator of compromise(IOC) deployed rapidly to cut down on man-hour costs.

Architecture

- Redns Server
  - DNS listener: responds to ipv4 and ipv6 requests
  - Web listener: hosts a ‘Access denied’ page
- Redns CLI Tool
  - List all clients
  - Get client history/traffic
  - Add/Remove malicious domains from database

Testing and Distribution

- CI with Travis
- Travis builds binaries on every commit
- Public ACI (rkt) images
- Docker

Demo

Questions

- Thanks Dr. Hale for the sweet name

https://github.com/mfaltys/redns
https://mfaltys.github.io/redns_docs/
https://github.com/mfaltys/redns_docs
https://travis-ci.org/mfaltys/redns
https://trello.com/b/5KMHrR6L/redns
https://cryo.unixvoid.com/redns
https://hub.docker.com/r/mfaltys/redns