Goals

- How long do malicious domain names live?
- How many IP addresses do malicious domains resolve to, and how often do they change?
- Can lifecycle properties help correlate domains that are part of the same criminal network?

Approach

Distributed DNS lookup utility, called Digger:
- Hadoop nodes as VMs on commodity hardware.
- Distributed Hadoop nodes hosted by collaborators around the world.
- Mapper tasks query domains using priority queues ordered by TTL.
- Set of geographically diverse resolvers including public RDNS servers and resolvers local to each node.

Ongoing Work

- Long-term data collection using Digger.
- Develop metrics for Authoritative NS reputations.
- Remediation strategies.

Preliminary Results

Newly blacklisted domains per day.

Distribution of IPs per domain.