Reputational DNS

with an

Introduction to

DNS Response Policy Zones

João Damas, ISC

Background

- Concept of DNS reputation isn't new
  - Used today in virtually all email (SMTP) servers to curtail spam
  - Some Recursive DNS providers do it today
- What is new
  - Response Policy Zones announced by ISC in late July
    - A common framework for DNS reputation
  - A blog post by Paul Vixie to facilitate awareness and debate

http://www.circleid.com/posts/20100728_taking_back_the_dns/

What is RPZ

- DNS policy information inside a specially constructed DNS zone
- Enables producers of domain name reputation data and consumers to cooperate in the application of such policy to real time DNS responses
- It turns a recursive DNS server into a powerful security tool!

Example Uses of DNS RPZ

- Block or redirect malicious sites
- Block ability of bots to find the Command&Control
- Walled garden treatment for infected clients
- IP address reputation can also map into here

Pro Perspective

- Modern malware is agile and sophisticated but … traditional defences are not
  - Based on signatures
  - Lag time between zero-day of exploit and the deployment of an AV update (if there is one)
- There are roadblocks for domain take downs at the domain authorities
  - Inability of Registries to act or react quickly
    - Due to policy, resources, risk of liability
  - Reluctance of Registrars to act or react quickly
    - Due to risk of liability, resources, loss of revenue

Pro Perspective

- RPZ provides a fast, effective and scalable solution for remediation
- DNS is ubiquitous – no need for a new system
- Puts domain reputation in the hands of the security experts
- Buys time for AV companies to update their software
- Minimizes spread of infections
  - Can block would-be fly-by infections
- Can inform victims (bots) of their infection while rendering the botnet beign