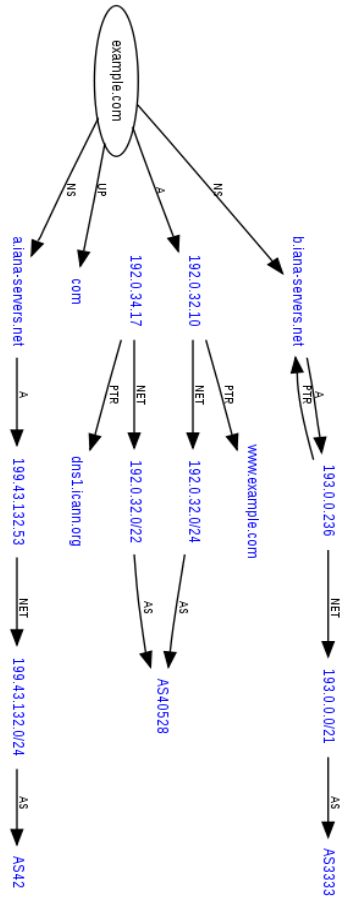
DNS Zone Risk Analysis

Dave Piscitello, ICANN

Background

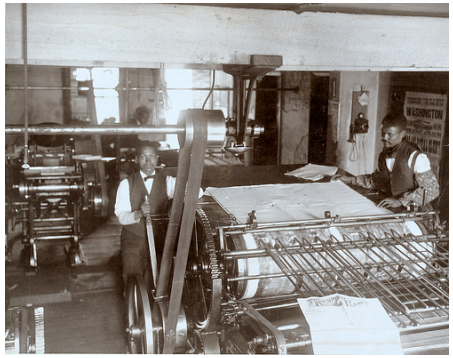
- Domain name resolution is based on zone file data:
  - Resource records in a zone file define bindings between names, addresses, services
- Authoritative name servers “host” zone files.
- Recursive name servers ask authoritative name servers for resource records.

Who Provides Authoritative NS?



- The registrant;
- Authorized 3rd parties:
  - A DNS hosting provider;
  - A registrar (reseller) who offers DNS hosting;
  - An ISP;
  - A web hosting provider; and
  - A managed service provider.

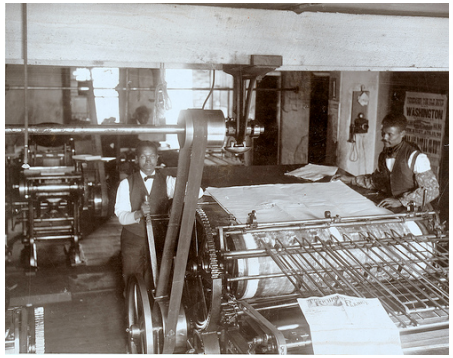
How Does a Registrant Publish a Zone File?



- Composes zone, publishes it on own host.
- Composes and sends complete zone to DNS hosting provider.

In these scenarios the registrant knows all resources and bindings.

How Does a Registrant Publish a Zone File?



- Registrant provides some zone data to DNS hosting provider:
  - Out of band, or through a DNS hosting provider's submission form.
- DNS hosting provider provides remainder of zone data and publishes zone.

In these scenarios the registrant may not know all resources and bindings.

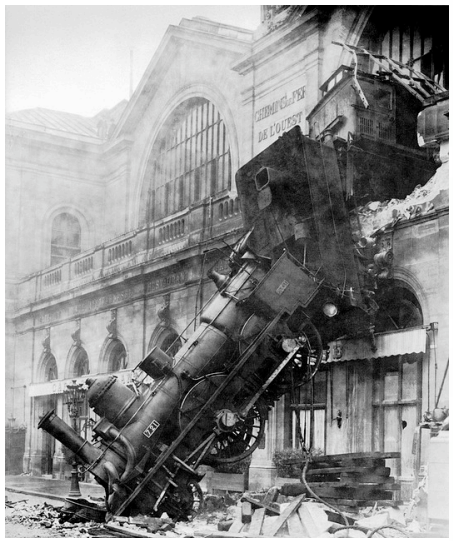
Problem Definition

A registrant who does not have complete knowledge of the information used to create the zone file for a domain is at risk of having name resolution interrupted without the ability to restore name service.

Why Is This Important?

- Name resolution is an essential and critical service.
- Your Internet presence relies on users being able determine the IP addresses of the names of your {web, email…} servers.
- Any circumstance where name resolution is interrupted is a threat.

Threat Landscape



- Technical or business failure of any DNS hosting provider:
  - Temporary or permanent, resulting in loss of original data.
- Account compromise (intentional misconfiguration resulting in loss of original data.
- Unintentional misconfiguration resulting in loss of original data.

Mitigating This Risk

- Document your DNS architecture and operations.
- Design for resiliency.
- Actively manage zone data.
- Implement appropriate defenses against attack.
- Proactively monitor name service.

Thank You


in San Francisco ▪ 13-18 March 2011
ICANN
SILICON
VALLEY
Meeting

One World

One Internet

Questions