Open Meeting of the Security & Stability Advisory Committee

26 October 2009

Agenda

- Introduction – Steve Crocker, Chair, SSAC
- SSAC Retreat – Ram Mohan
- DNS Redirection – Ram Mohan
- Root Scaling Study –Ram Mohan
- Orphaned Name Servers – Dave Piscitello
- SSAC Activity: Follow Through and Outreach – Dave Piscitello

Introduction

- Security and Stability Advisory Committee
- Formed in 2001-2002
  - Decision to start: late 2001
  - First Operation: early 2002
- Provides guidance to ICANN Board, SO's and AC's, staff and general community
- Guidance areas are related to ICANN's missions, DNS, addressing, etc.

SSAC at Seoul

- Monday:
  - SSAC Open Meeting, 7:30 to 9:00 a.m.
  - Welcome Ceremony & President's Report, 8:30 to 10:00 a.m., Crystal A & B
  - Malicious Conduct and New gTLDs, 16:30 to 18:00, Crystal A
- Tuesday:
  - SSAC Closed Meeting, 9:00 to 10:30 AM
  - GAC Security Related Briefings, 10:30 am to 12:30 pm, Sapphire 1-3
  - Get to Know ICANN with Participation by SSAC 9:00 am to 12:30 pm, Crystal A

SSAC at Seoul

- Wednesday:
  - DNSSEC Workshop, 9:00 am to 12:00 noon, Sapphire 4
  - Root Scaling Study Results, 13:30 to 15:00, Crystal A
  - Internationalized Registration Information, 15:00 to 16:30 pm, Crystal A
  - SSAC Review -- Presentation of WG Draft Final Report, 14:00 to 15:30, Garnet
- Thursday:
  - ICANN Security, Stability, and Resiliency Activities Update session, 1700-1930, Crystal A
  - DNS Abuse Forum, 1500 to 1700, Crystal A
  -

SSAC Retreat

Ram Mohan

October 2009

SSAC Retreat

- 29 September to 01 October 2009
- Topics:
  - Registrant Protection and Abusive Behavior
  - DNS as an Attack Vector
  - How Robust is the Root Server System and What is Its Future?
  - Root Scaling Study: Briefing, Outcomes, Next Steps
  - SSAC Engagement with Other ICANN Bodies
  - SSAC Charter, Roles, Review, Workflow and Members

SSAC Retreat Preliminary Outcomes

- Recommendations Include:
  - Registrant Protection and Abusive Behavior
    - Identify a taxonomy of application threats that operators face.
  - DNS as an Attack Vector
    - Continue to emphasize the importance of requiring suppliers to provide source address validation.
  - Engagement with Other ICANN Bodies
    - Strengthen communications with other structures via inward and outward liaisons.
  - SSAC Review Outcomes
    - Address the issue of privacy/confidentiality in its requirements for membership.

Redirection & Synthesized DNS Responses in Top Level Domains – What Breaks?

Ram Mohan

October 2009

Redirection of DNS Responses @ TLDs

- **Issue**
  - – Wildcarding of DNS records at TLDs
  - – Provides “valid” address and routing even when domain names do not exist
- **Consequences**
  - – Breaks core DNS systems & legacy applications
  - – Erodes trust relationships
  - – Creates new opportunities for malicious attacks, without ability of affected parties to mitigate problem

Reference Document: SAC041

SSAC Advice:

Clear & Significant danger to security & stability of the DNS

Board Resolution (June 2009):

Take all available steps with appropriate entities to prohibit such use

Prohibit redirection/synthesis for all TLDs (gTLD & ccTLD, including IDN TLDs)

- Revise new gTLD Guidebook
- Consult with ccTLD community/GAC for new ccTLDs
- Revise existing gTLD agreements
- Add appropriate guidelines to existing ccTLD arrangements

Reference Document: SAC041

Problems Caused

- Architectural violation
- Impact on Internet protocols
- Single point of failure
- Reserved and blocked domains ‘appearing’ alive
- Privacy concerns
- Lack of choice for Internet users
- Poor user experience
- Impact on IDN TLDs

References: See list at end of presentation

Architectural Violation

- Redirection at the TLD level violates fundamental principles
  - DNS Protocol is neutral about what protocols to answer
  - Redirection assumes HTTP protocol (web browsing)
- All future protocols dependent on DNS affected by redirection
  - Unacceptable invasion of protocol boundaries
    - For example, HTTP could use DNS even though HTTP is a recent invention, due to clear layering

Every Current & Future Internet Application Is Affected

Impact & Side-Effects on:

- Every mail server, mail agent
- Every instant message program and agent
- Every VOIP server, proxy and user agent
- Every parental control system
- Every anti-virus system
- Every license management system
- Every software update system

i.e., Every Application On The Internet

Most Basic Internet Tools Break

- Systems that test for “existence” of a host fail
    - Spam filters stop working (all forged addresses now appear to be real)
    - URL link checkers will fail (all links appear to be valid)
- Systems that believe a host name is valid break
    - Mail to a mis-typed address will not bounce anymore
    - And, the mail is delivered to a different address, without any notification or choice by the e-mail sender
  - Search engines won’t be able to function as normal

- Applications that root operators, IANA and other organizations use to monitor TLD name service & zone composition might break

Impact on IDN TLDs

IDN TLD are deployed in <language>, but are represented on the DNS in ASCII

Wildcards for IDN TLD can cause unexpected behavior:

- Localization of content could break
  - User may request a web page in <language A> and get a different page in <language B>, with no choice

Reference document s

http://www.icann.org/committees/security/ssac-report-09jul04.pdf

http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html

http://www.icann.org/committees/security/sac041.pdf

http://www.icann.org/en/registries/rsep/tralliance_report.pdf

QUESTIONS?

Scaling the Root

Ram Mohan

October 2009

Main Points

- Sign the Root
  - This will be the biggest and most dynamic change. Get it done and see how things go.
- A few hundred new TLDs over two to three years is ok.
  - Not enough data available to feel comfortable to say more is ok.
- Next steps
  - Further study and modeling is needed
  - Information sharing and closer cooperation/ communication is needed
  - Put an early warning system in place; look for stress points

Main Points

- Some work for staff to do, but also much that involves others
- IDNs and IPv6 are not issues

Orphaned Name Servers

Dave Piscitello

ICANN Sr. Security Technologist

October 2009

The Problem Space

- What is an Orphan Name Server?
  - A name server record exists in a delegation
  - The parent domain name no longer exists
- How does an name server record become orphaned?

How a Name Server is Orphaned: Step 1

`example.TLD` and `example2.TLD` are registered in TLD

In the TLD zone file:

```
example.TLD     NS   ns1.example2.TLD
example.TLD     NS   ns2.example2.TLD
example2.TLD    NS   ns1.example2.TLD
Example2.TLD    NS   ns2.example2.TLD
.
.
.
ns1.example2.TLD    A    10.0.1.53
ns2.example2.TLD    A    10.0.2.53
```

How a Name Server is Orphaned: Step 2

`example2.TLD` is deleted from in NET

ın NET zone file:

```
example.TLD     NS   ns1.example2.TLD
example.TLD     NS   ns2.example2.TLD
~~example2.TLD    NS   ns1.example2.TLD~~
~~Example2.TLD    NS   ns2.example2.TLD~~
.
.
.
ns1.example2.TLD    A    10.0.1.53
ns2.example2.TLD    A    10.0.2.53
```

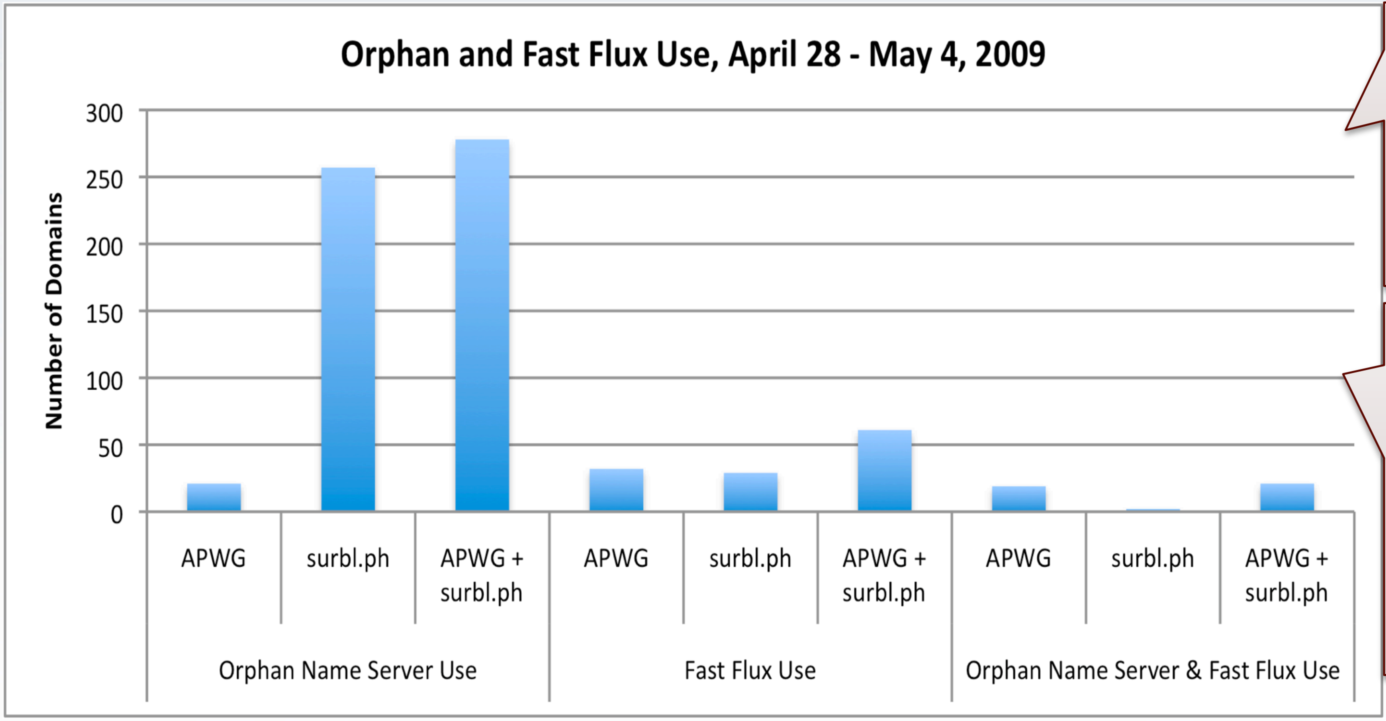
These resource records are removed by the registry when label is deleted

These resource records remain even though parent domain name no longer exists – these name servers are **orphans**

Not all registries have policies to unilaterally remove the glue – other domains may be using the same name server Identifying orphans and removing glue is harder when parent and delegation are not in same TLD

Does DNS Abuse Result From Orphaned Name Servers?

- APWG study conducted by Internet Identity and Karmasphere
  - Correlate incidence of orphaned name servers among a sample set of domains against domains used in fast flux attack networks



3.4% of all malicious domains from APWG input list used orphan name servers

59% of the malicious domains associated with FF attack networks used orphaned name servers

October 2009

Initial Findings, Next Steps

- Registry action to remove glue records for deleted domains may strip miscreants of an evasion and persistence tool
- Considerable cooperation across TLDs is needed
- Further study is needed before specific recommendations can be made
  - SSAC to collaborate with APWG
  - Kudos to Karmasphere and Internet Identity for initial study and preliminary results

SSAC Activity, Follow Through, and Outreach

Dave Piscitello

Julie Hedlund

October 2009

SSAC Activity: Follow Through

- SSAC reports and advisories are being considered in the following study areas:
  - WHOIS studies - SAC 27, 33, 37, 38, 40
  - GNSO IRTP - SAC007, 040
  - GNSO RAP - SAC025, 040
  - New TLD Applicant Guide - SAC038, 041
  - Compliance's RAA amendments - SAC038, 040
  - GNSO, ALAC, CCNSO, GAC - SAC037 (Internationalized Registration Data Working Group)
  - Malicious conduct report - SAC038, 040
  - Highly secure registry verification program - SAC038, 040, 041

SSAC Activity: Follow Through

- Related Meetings:
  - Monday:
    - Trademark Protection and Malicious Conduct – New gTLD Program Proposed Path Forward, 1530 to 1800, Crystal A
    - DNS Abuse Forum, 1500 to 1700, Crystal A
  - Wednesday:
    - Root Scaling Study Results, 13:30 to 15:00, Crystal A
    - Internationalized Registration Information, 15:00 to 16:30 pm, Crystal A
    - Registration Abuse Policies Working Group, 1400-1530, Sapphire 4

SSAC Activity: Outreach

- At Seoul:
  - Tuesday, 27 Oct: Get to Know ICANN with Participation by SSAC 9:00 am to 12:30 pm, Crystal A
  - At Registration: One-page information pieces on SSAC and DNSSEC
- Other Outreach:
  - Participate in joint workshops on hot issues
  - Refine processes of engagement
  - Strengthen communications with other structures via inward and outward liaisons.

감사합니다

Thank you!