ICANN

BRUSSELS

© vzw Atomium

No.38 | 20-25 June 2010

ICANN MEETING No. 38 | 20-25 June 2010

Open Meeting of the Security & Stability Advisory Committee (SSAC)

ICANN Meeting, Brussels, Belgium

22 June 2010

Agenda

1. Update on A Registrant's Guide to Protecting Domain Name Registration Accounts, Dave Piscitello, ICANN
2. Update on SSAC Work Party on Orphaned Name Servers, Jim Galvin, Afilias
3. SSAC Update on Root Scaling Issues, Ram Mohan, SSAC Liaison to the ICANN Board
4. SSAC Improvements Resulting from ICANN Board Review, Steve Crocker, SSAC Chair

Update on a Registrants Guide to Protecting Domain Name Registration Accounts

Dave Piscitello, ICANN

How to Protect Domain Registration Services Against Misuse

A guide for registrants

A complement to SAC040 (for registrars)

Best practices registrants should follow

How to make informed decision when choosing a registrar

Explain Why Measures Are Needed

Threat landscape

- Unauthorized access
- Malicious alteration of DNS
- Malicious alteration of contact information
- Unauthorized domain transfer
- Renewal issues

Assessment

Risk assessment

Business impact assessment

Identify Account Protective Measures

Protect account credentials

Use registrar correspondence to trigger internal checks and actions

Maintain proof of ownership

Manage (diversify) identities used as points of contact

Implement change controls

Maintain accurate external points of contact

Identify Proactive (Monitoring) Measures

WHOIS and DNS change activity

- Explain value (why)
- How to monitor, how to respond

How To Make Informed Decisions

Questions to ask prospective registrars

- Account management features
- Correspondence
- Security measures
- Reputation, track history, references

Questions?

Orphaned Name Server Work Party Update

Jim Galvin, Afilias

A Orphaned Record is

1) Address resource records sets (A/AAAA records);

2) that used to be glue records, but the delegation point name server records ("Delegated subzones") do not exist anymore, hence the name server software will treat them as authoritative address records and they will appear in the answer section of a response;

SSAC Research Plan

1. Empirical Study: measure the number of orphan records in gTLDs;
2. Empirical Study: Measure the extent orphan is used for abuse; and
3. Interview Study: semi-structured interview of gTLD operators on how they handle orphan records, problems if they are removed, and if any of the solutions affect cross TLDs.

Study 1: Measure the Number of Orphaned Records in gTLDs

Study Methodology

Use 5/16 snapshot of zone files from 11 gTLD registries;

Process the zone into three tables in a MYSQL database: glue_records, domain_records, domain_ns_records; and

Count all the entries in the glue records table whose parent domain does not exist in the domain records table.

Preliminary Results

Across all 13 gTLDs, there are a total of 20.4K orphan name servers, accounts for 0.8% of all gTLD glue records;

On gTLD by gTLD basis, the percentage of orphan name servers ranges from 0.00% - 6.17% (mean percentage: 2.13%, median: 1.43%); and

Overall, there are 53K gTLD domains that use these orphan name servers.

Study 2: Measure the Extent Orphaned Name Server Is Used for Abuse

Study Methodology

Take the 53K domains found in previous study that used orphan name servers and check against URL blacklists on 6/8:

- spamhaus domain blacklist (dbl.spamhaus.org)

- SURL multi domain blacklist (multi.surbl.org)

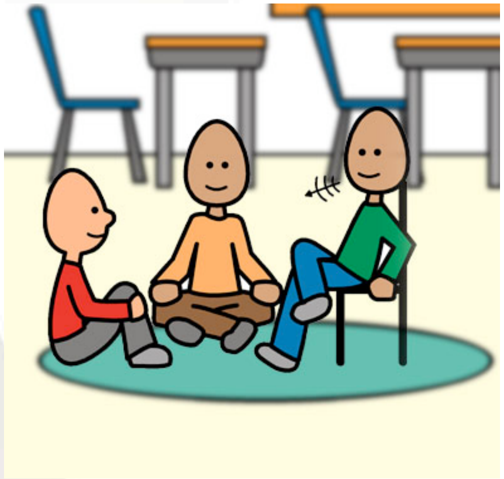
These lists have a wide coverage (40 – 70%), and low false positives (< 0.001%)

Preliminary Results

Of the 53K domains that use orphans:

-	On spamhaus domain blacklist : (dbl.spamhaus.org)	31%
-	On SURL multi domain blacklist: (multi.surbl.org)	28%

Discussions: Significance Test



Assuming that malicious domains account for 5% of the gTLD domains.

Percentage of malicious domains that use orphans = Total malicious orphan domains / Total malicious domains = 30% * 53K / (118 million * 5%) = 0.27%

Percentage of legitimate domains that use orphans = Total legitimate orphan domains / Total legitimate domains = 70% * 53K / (118 million * 95%) = 0.03%

Open Questions

Definition of Orphan:

Should name servers that are out of zone but still in registry be counted as orphans?

Are there any legitimate use of orphans?

Next steps

1. Resolve open questions;

2. Complete interview Study of gTLD operators on how they handle orphan records, problems if they are removed, and if any of the solutions affect cross TLDs; and

3. Draft report.

Questions?

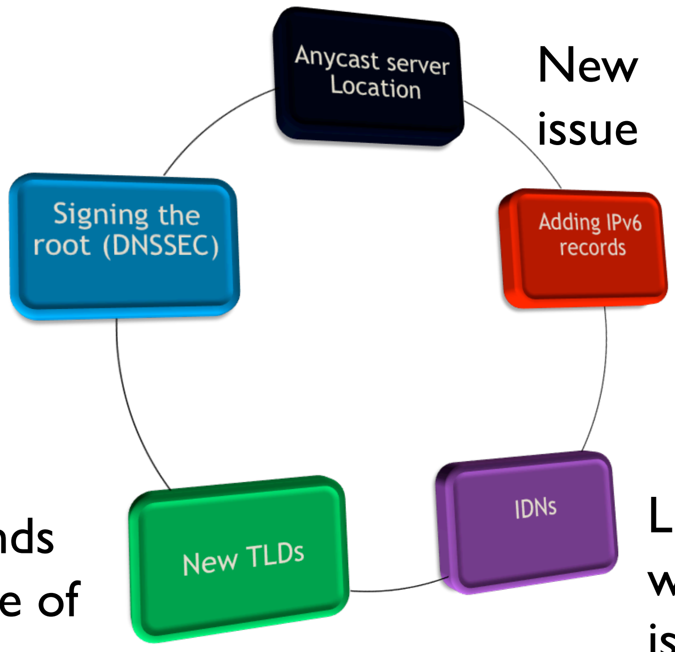
SSAC Update on Root Scaling Issues

Ram Mohan, SSAC Liaison to the Board

Background

- February 2009: ICANN Board asks SSAC and Root Server System Advisory Committee (RSSAC) to co-ordinate a study:
  - To consider the potential impact on the stability of the root when adding:
    - DNSSEC
    - IPv6 address records
    - Internationalized Domain Name top level domains (IDN TLDs), and
    - New TLDs
- September 2009: SSAC began consideration of two reports: the Root Scaling Study Team’s (RSST) Report and the TNO Report; and
- June 2010: SSAC has reviewed both reports and is considering recommendations.

Multiple Changes, Some Large, Some Small



Anycast server Location

New issue

Adding IPv6 records

Small impact

IDNs

Like new TLDs, but with some special issues

New TLDs

Depends on rate of change

Signing the root (DNSSEC)

Big Change

Signing the Root (DNSSEC) - A Big Change

Signing the root (DNSSEC)

- Signing the Root is underway
- Anticipated to be in full operation in July
- Lots of testing in progress
  - Some of the root servers have the signed zone with the test key;
  - Large responses are being returned;
  - Nothing bad has happened; and
  - This appears to be moving along smoothly.
- Conclusion: Among the multiple factors, this was clearly the largest. If this continues to proceed smoothly, we’re in good shape.

New TLDs - Depends on Rate of Change

New TLDs

- Will the addition of new TLDs overwhelm any part of the root server system?
  - If so, how many?
  - When?
  - How will we know?
- ICANN preparing to ramp up capacity to evaluate and approve new TLDs to a max of 924 per year, a year or more after the initiation of the new gTLD program.
  - However, it is not clear that the legal department, the Board or the US Government can accommodate that many contract actions.
- Can the Root Server Operators accommodate that many new TLDs?
  - Probably, but might depend on rate of change.

IDN TLDs - New TLDs with Special Situations

IDNs

- Adding IDN TLD to the root is a non-issue
  - Extensive testing was completed a long time ago
  - Adding an IDN TLD is exactly the same as adding a non-IDN TLD
- **<u>Except</u>**: There are requests for IDN TLD variants to be delegated to the root zone
- Technical and operational issues not yet thoroughly worked out:
  - Methods to ensure variants point to the same locations.
- This issue is separable from the scaling issues.
- But wrong approach can cause stability issues.

Adding IPv6 Records - Small Impact

Adding IPv6 records

- IPv6 records have been added at a slow, steady rate;
- Impact on the size of the root zone is very small;
- This is business as usual without any issue at all; and
- There is no reason to interrupt future requests for new IPv6 records.

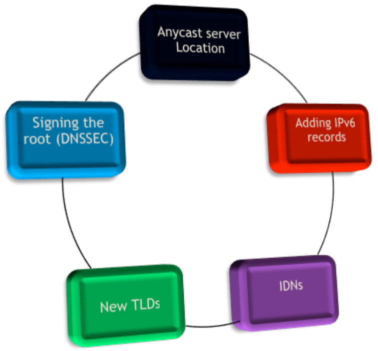
Location of Anycast Servers - New Issue

Anycast server Location

- Possibility that remote location of Anycast instances of the root might inhibit the growth of the root zone;
- This would be a new consideration, not previously explicit;
- The Root Server Operators have not spoken clearly on this;
- Some Root Server Operators say this is not a problem at all; and
- Conclusion: Some straightforward discussion with the Root Operators is needed.

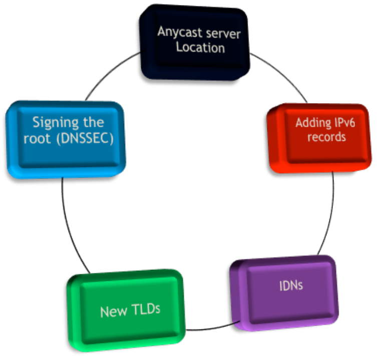
Status and Conclusions to Date

- The RSST Report and TNO report are not sufficient to conclude the Root Scaling Study.
- Several issues that may potentially impact the scaling of the root, including placement of Anycast instances.
- Further work:
  - May not be required to <u>start</u> new TLD delegations; but
  - Could be required to <u>continue</u> new TLD delegations.



Status and Conclusions to Date, Cont.

- Targets
  - It is expected that a report will be delivered 3Q 2010.
    - The report will take into account that some of the concerns originally expressed about the impact of the signing of the root are now overtaken by the experience gained with DNSSEC implementation, and that some of the concerns about the potential for a very, very large root zone are diminished because the maximum rate of change has now been published.
  - Initiate Root Scaling Study v2 3Q 2010.
  - Initiate Root Scaling End-User Impact Study 4Q 2010.



Questions?

SSAC Improvements Resulting from ICANN Board Review

Steve Crocker, SSAC Chair

Background

- In 2009, the ICANN Board appointed an SSAC Review Working Group (WG);
- The Board appointed JAS Communications as consultants for the independent review of the SSAC and in November 2008 they began their review with input from the ICANN community and released a report on 17 February 2009 followed by a Public Comment period;
- The SSAC review WG engaged in extensive consultations with the SSAC community and produced a draft report on 18 September 2009 followed by a Public Comment period; and
- The SSAC review WG released its final report on 08 February 2010.

SSAC Review WG Report Highlights

- The SSAC should:
  - Maintain its fundamental identity as an Advisory Committee chartered by and reporting to the ICANN Board;
  - Undertake a lightweight planning process to determine the research and publication agenda, membership strategy, and resource requirements;
  - Keep and publish meeting minutes (but not transcripts as such) on the SSAC web site in a timely manner;
  - Endeavor to keep its web site current to include work in progress and work planned; and
  - Appoint members for three-year terms renewable by the Board, not impose a limit on the number of terms served, and stagger member terms.

SSAC Review WG Report Highlights, Cont.

- The SSAC should:
  - Adopt a default confidentiality policy;
  - Produce a yearly report of activities to the Board and for publication;
  - Include sections in its reports to record member dissents and abstentions;
  - Develop and post a conflicts of interest policy based on the ICANN Board policy; and
  - Develop and post a conflicts of interest policy based on the ICANN Board policy

SSAC Improvements

- Establish initial membership term lengths of current members of no more than three years to be renewed by the SSAC Chair indefinitely;
- Request a change to the ICANN Bylaws to accommodate initial membership term lengths, which will be published for public comment before adoption;
- Institute a procedure for SSAC members to affirm confidentiality and non-disclosure of proprietary information; and
- Institute a procedure to notify SSAC members that they may have to sign a non-disclosure agreement before accessing proprietary information.

Thank you and Questions