**ccNSO**
**Ad-hoc Wildcard Study Working Group**
**June 22, 2010**

# TABLE OF CONTENTS



# INTRODUCTION AND SUMMARY

## 1. Issue

On 10 June 2009, the Security and Stability Advisory Committee (SSAC) published and forwarded to the ICANN Board an advisory which determines that the redirection and

synthesizing of DNS responses by TLDs poses a clear and significant danger to the security and stability of the domain name system. At the ICANN Sydney meeting (June 2009) the ICANN Board requested the ccNSO to provide a report on mechanisms that could be employed to ensure that redirection and synthesis at the top level are effectively prohibited. At the Seoul ICANN meeting (October 2009) the ccNSO conducted an information session on redirection and synthesizing of DNS responses ("redirection"). At that session it was established that, with a few exceptions, most ccTLDs do not use redirection, and that more information was needed, both to understand the issues associated with redirection and the need for use of "redirection" by ccTLDs.

The ccNSO council resolved to establish a study group to provide to the ccTLD community and the ccNSO Council a comprehensive overview of the issues associated with redirection at country code Top Level Domains, and the need for and current use of redirection by country code Top Level Domains.

The study group undertook the following:

- Summarise the issues associated with "redirection" as identified by SSAC in its reports (see references);
- Liaise with SSAC to seek further clarification and input if considered needed and appropriate by the group, for example to better understand the threats that redirection creates for Internet users and related issues;
- Liaise with the Stability, Security and Resilience department of ICANN to seek further clarification and input if considered needed and appropriate by the group, for example to better understand the threats that redirection creates for Internet users and related issues;
- Liaise with the ccTLDs who are currently using "redirection" to solicit their views and perspective on "redirection" to provide a comprehensive overview on the backgrounds of their use of it;
- Prepare a session at a ccNSO meeting, either at the ICANN meeting in Nairobi or Brussels whichever is deemed to be more appropriate by the study group, or present and discuss the results of the study to the ccTLD community;
- Provide a final report of its findings to the ccNSO Council.

The study group did not consider the merits of wildcarding nor methods to engage ccTLDs who are using wildcards. The study group conducted anecdotal research and analysis and is providing the following report to the ccNSO. The research is not a scientific analysis of the issues, but rather an anecdotal examination of the issues.

## 2. Wildcarding Definition

Wildcarding is DNS redirection performed by the zone administrator or authoritative name service operator for all queried names that are not published in the zone file. RFC 1034 provides a definition of wildcards, and provides an overview of how wildcards work in DNS.

## 3. Study Group Recommendations

The study group recommends that the ccNSO council engage in further dialogue with ccTLDs engaged in DNS synthesis; that the ccNSO advise ICANN that clearer identification of ccTLDs engaged in wildcarding should be provided; and that the ccNSO council consider which harms are less desirable than others.

# WILDCARDING & HARMS

## 1. SSAC and ICANN staff advice

On 10 June 2009, the Security and Stability Advisory Committee (SSAC) published and forwarded to the ICANN Board an advisory which states that the redirection and synthesizing of DNS responses by TLDs (a.k.a. wildcarding) poses a clear and significant danger to the security and stability of the domain name system.

The June 2009 advisory (SAC041) recommends a prohibition on the use of redirection and synthesized responses by new TLDs.

1. Advises ICANN to take all available steps to prohibit redirection
2. Recommends ICANN communicate dangers
3. ICANN Board resolution during Sydney meeting June, 2009

A subsequent SSAC presentation to the ccNSO (28 Oct, 2009) outlined the following harms caused by wildcarding:

1. Architectural violation
2. Impact on Internet protocols
3. Single point of failure
4. Reserved and blocked domains 'appearing' alive
5. Privacy concerns
6. Lack of choice for Internet users
7. Poor user experience
8. Impact on IDN TLDs

A Nov. 2009 ICANN Staff document lists the following harms

- Architectural implications
- Impact on Internet protocols
- Single point of failure
- Reserved and blocked domains appear alive
- Fragmentation of the DNS ecosystem
- Privacy concerns
- Lack of choice for Internet users
- Poor user experience (e-mail)
- Use of privileged position

## 2. Summary

We compiled a single harms list from both documents with references to all other related

documents in order to clearly summarize the consensus on the harms associated with wildcarding.

| | **Harm** | **References** | **Short description** |
|---|---|---|---|
| 1. | Architectural violation | [2], [3], [9] | Violation of the layered protocol design of the Internet: DNS query is protocol neutral, while the IP address given back is targeted for HTTP |
| 2. | Impact on Internet protocols | [1], [2], [9] | NXDOMAIN responses is eliminated for affected DNS type (e.g., A, AAAA, MX); that is something on which an application may depend |
| 3. | Single point of failure | [1], [9] | Redirection service can result in a centralized point being accessed for the traffic of uninstantiated domains |
| 4. | Reserved and blocked domains appear alive | [1],[3],[9] | Unregistered/undelegated domains can look as if they were delegated/existent from an end-user point of view. |
| 5. | Fragmentation of the DNS ecosystem | [5],[9] | Some users may want to reverse the effect of the changes and they could take action to implement workarounds, e.g., filters to the server redirection, patches to DNS resolvers, etc. |
| 6. | Privacy concerns | [1],[2],[3],[9] | Some data from various Internet protocols may arrive at the redirection server's network against the intention of the sender |
| 7. | Lack of choice for Internet users | [1],[2],[3],[4],[5],[9] | Local settings of various user applications may became ineffective because of unexpected DNS response |
| 8. | Poor user experience | [1],[9] | No immediate negative response from application (for example from e-mail client) |
| 9. | Use of privileged position | [5],[9] | Registry is making use (and perhaps profit) from all or a subset of the uninstantiated domains without having registered or paid for them; another organization would have to invest a considerable amount of money |
| 10. | Impact on IDN TLDs | [8] | 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 |
| 11. | Erosion of trust relationships | [6],[7],[8] | Redirecting can create security issues for domain registrants. In particular, trust relationships between a parent domain and its subdomains cannot be assured |
| 12. | New opportunities for attacks | [6],[7],[8] | New opportunities for malicious attacks without ability of affected parties to mitigate problem |

List of references

[1] IAB. (2003, September 19). Architectural Concerns on the use of DNS Wildcards. Retrieved from http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html

[2] RSTEP. (2006, November 2). Report on Internet Security and Stability Implications of the Tralliance Corporation search.travel Wildcard Proposal. Retrieved from http://www.icann.org/en/registries/rsep/tralliance_report.pdf

[3] SSAC. (2004, July 9). SAC006: Redirection in the COM and NET Domains. Retrieved from http://www.icann.org/en/committees/security/ssac-report-09jul04.pdf

[4] SSAC. (2006, November 10). SAC015: Why Top Level Domains Should Not Use Wildcard Resource Records. Retrieved from http://www.icann.org/en/committees/security/sac015.htm

[5] R. Levien, S. R. Austein, B. M. Stanley, B. L. Christine, C. Timothy, D. Hugh, et al. Signposts in Cyberspace. The Domain Name System and Internet Navigation. National Research Council of the National Academies. Section 4.4 Responding to Domain Name Errors. The National Academies Press. Washington, D.C., US. 2005.

[6] SSAC. (2008, June). SAC032: Preliminary Report on DNS Response Modification. Retrieved from http://www.icann.org/en/committees/security/sac032.pdf

[7] SSAC. (2009, June 10). SAC041: Recommendation to prohibit use of redirection and synthesized responses by new TLDs. Retrieved from http://www.icann.org/en/committees/security/sac041.pdf

[8] SSAC (2009, October 28). SSAC Meeting with ccNSO on Redirection http://sel.icann.org/meetings/seoul2009/ssac-ccnso-redirection-28oct09-en.pdf

[9] ICANN (2009, November 24). Harms Caused by NXDOMAIN Substitution in Toplevel and Other Registry-class Domain Names http://www.icann.org/en/topics/new-gtlds/nxdomain-substitution-harms-24nov09-en.pdf

# WILDCARDING CCTLDS

When the study group set out to examine wildcarding among ccTLDs, we were informed by ICANN that the following 11 ccTLDs were engaged in wildcarding:

.CG
.KR
.NU
.PH
.PW
.RW
.ST
.TK
.VG
.VN
.WS

However, after this list was raised, the study group was made aware by a member of the community that another ccTLD ( .CO) had once engaged in a form of redirection and had recently stopped. The study group thought it would be useful to find out from this ccTLD the reasons for no longer engaging in the practice, and the reasons are summarized below.

As well, over the course of time several of these ccTLD's indicated they no longer engage in wildcarding. The final list used during the study group's analysis was therefore the following:

.KR
.PH
.PW
.ST
.TK
.VN
.WS

**1. Identification of ccTLDs using wildcards**

By the end of the study group's work, thanks to different tests run by different community members, it became clear that other ccTLDs, not on this list, were exhibiting some kind of selective synthesis behaviours outside the scope of "wildcards" as described in RFC 1034, which requires that this specific kind of synthesis involve a "*" record in a zone, and responds to all non-existent labels with the contents of that record.

Although the RFC 1034 section 4.3.3 recommends to query label '*' in a domain to test wildcarding, not all TLDs follow this rule. Some of the TLDs positively answer A type query for *.<TLD> however they answer negative to a query <random string>.<TLD> (e.g.

sdfasfhaksjfhask.tw). On the other hand some of these TLDs answer to IDN like queries in a form xn--<random string>.<TLD> or sometimes even xn--*.<TLD> (e.g. xn—sdfsdfsdjlk.cn or xn--*.tw). We found three methods for identifying ccTLD engaged in synthesis or redirection.

Below we provide each method and the resulting list of ccTLDs.

| **Method 1**<br><br>***.<TLD>** | **Method 2**<br><br>**<random string>.<TLD>** | **Method 3**<br><br>**<xn—randomstring>.<TLD>** |
|---|---|---|
| .CN<br>.KR<br>.PH<br>.PW<br>.ST<br>.TK<br>.TW<br>.VN<br>.WS | .KR<br>.PH<br>.PW<br>.ST<br>.TK<br>.VN<br>.WS | .CN<br>.KR<br>.MP<br>.PH<br>.PW<br>.ST<br>.TK<br>.TW<br>.VN<br>.WS |

(All tests were done on June 19 2010)

The tests reveal that there are different levels of DNS response synthesis and there also can be other types that those tests did not find. TLDs that are on some of these three lists but are not in all of them somehow violate DNS related RFCs. This violation could be a potential blocker in future advancement of DNS, for example, in deployment of DNSSEC. (In DNSSEC all items in the zone are signed. That means either all possible combination of xn--<random string>.<TLD> would be either generated into or every answer would be signed in time of a query. Both variants are technically almost impossible.

## 2. Reasons for using Wildcards

A number of ccTLDs engaging in DNS redirection provided the study group with the reasons or justification for engaging in the practice. The following summarises the responses received from those ccTLDS.

### .VN (Vietnam)

Thuan Nguyen of the Vietnam Internet Network Information Center ("VNNIC") explained that VNNIC is charged with managing, allocating, supervising and promoting the use of Internet domain name, address, autonomous system number in Vietnam. Their primary mandate is to

support and develop the use of the internet in Vietnam with a particular focus on the Vietnamese ccTLD and promote adherence to the policies which govern the use of the internet. They engage in wildcarding in order to address the following:

- Many internet users in Vietnam are not familiar with the registration process, especially in rural and underserved regions; and
- Many internet users in Vietnam cannot access or locate the regulations on internet content and use. Therefore, certain users will unwittingly violate relevant internet law.

VNNIC has therefore developed the default web page for non-existent .vn domain names in an attempt to address the above outlined issues. The default page informs the visitor that the domain name may be open for registration and assists them in both checking the availability of the domain name and provides tools for registration. Further, it brings them to the VNNIC website which provides them with access to all regulations on the use of internet resources. While this may not be a permanent solution, VNNIC anticipates that this method will help them better grow and manage the Internet in the near and mid-term. They have chosen the current strategy as the best balance for the time being and will monitor the overall impact of this program on the Vietnamese internet.

**.PW (Palau)**

Tom Barrett of the .PW Registry stated .PW no longer uses a wildcard, but a recent (April 21 2010) check by IANA verified that the wildcard is still being used, and the study group's anecdotal research also revealed that .PW uses a wildcard.

**.PH (Philippines)**

Joel Disini of .PH states that the registry has been wildcarding for 8 years, and states that they receive 1.5M unique visitors monthly on the wildcard site, 7M page views (one of top 10 most trafficked sites in the Philippines). The stated reason for using wildcarding is to provide a service to the user providing service to the user. The position on wildcarding is that it is a tremendous resource, providing information about the status of the domain is more useful for the domain registrant. Wildcarding provides interesting statistics on browser usage, for example. As well, .PH's point of view is that harms of wildcarding are minimal, the response time is very fast, and if a protocol were to be written that "broke" because of wildcarding, it would be simple enough for all gTLDs and ccTLDS (that choose to wildcard) to install a handler (on the wildcard server) for each protocol.

**.NU (Niue)**

While .NU was on the original wildcarding list, this registry has since stopped wildcarding. However, Bill Semich of .NU pointed out that in his view wildcarding is considered acceptable by technical authorities. For example, .NU engaged in significant consultations with in-house technical staff, experienced independent technical consultants, advice and guidance of Paul Mockapetris, former chairman of the IETF and author of RFC 1034 and RFC 1035, which set the standards for the DNS. As well, Mr. Semich stated that Paul Mockapetris' opinion was that .nu's use of the wildcard was acceptable and permissible under IETF standards and would cause no harm to the Internet or the DNS. He went to explain that IETF RFC 4592 which updated the definition of the wildcard protocol described in RFC 1034 stated that the document "avoids

specifying rules for DNS implementations regarding wildcards." His position is that the IETF RFC 1034 and the RSSAC's report in 2009, "Harms and Concerns Posed by NXDOMAIN Substitution" present two conflicting sets of Internet standards regarding wildcarding and puts the TLD managers and operators in a potentially untenable conundrum. He suggested that the IETF and the RSSAC should reach an understanding about who is responsible for which standards on the Internet, and for the IETF to make a definitive statement on the matter.

**.KR (Korea)**

.KR has been redirecting queries in order to assist IE6 users correctly resolve IDN.kr queries of second-level IDNs. The IDNA standards applied to IDN.kr can function properly only if the browser supports the IDNA standard. However, IE6 does not support the IDNA standard, and KISA therefore provides redirection services in order to provide .kr users with optimal IDN.kr browsing experience while complying with the IDNA PUNYCODE standards. .KR emphasizes that .kr's redirection service is a temporary service due to the high percentage of IE6 users in Korea. It does not engage in wildcarding of queries resulting in the normal 'page not found' response.

KISA reported June 22, 2010 that the percentage of IE6 users has recently been decreasing at a faster rate than in previous years. Approximately 80% of the internet users in Korea were using IE6 in 2003 but the percentage of IE6 users had decreased to 50% in February, 2010, and decreased even further to 40% in May, 2010. KISA is also continuously encouraging Internet users in Korea to start using IDN supported browsers. KISA plans to stop the redirection service when the number of IE6 users decreases to a non-significant level.

**.CO (Colombia)**

The Ministerio de Comunicaciones of Columbia does not allow wildcarding, taking into account the international best practices and interpreting those practices in a way that does not isolate .co from the global domain name system.

# ANECDOTAL EVIDENCE OF HARMS (MAPPING)

The study group looked at whether and how each of the harms listed by SSAC and ICANN staff could be identified at each individual country code engaged in wildcarding, including protocol tests where appropriate. It should be noted that this was not done on a scientific basis nor is the claim that the tests are exhaustive. The mapping is intended to understand the impact of the use of wildcards by ccTLDs and link the observed phenomena to the harms list ( see section 2). The examined country codes were based on the original list, removing the names of those cc's which indicated they no longer engage in this practice (and testing if this was accurate by typing non-existent domain names in our browsers). As well, we provide below a brief description of the landing pages for each cc below.

1. KR : Korea. "Page not found" in Korean.
2. PH : Philippines. dotPH Page stating that requested (non-existent) domain is available. Page contains information about services offered by .ph as well as external advertising.
3. PW : Palau. A .pw page promoting the use of .pw services.
4. ST : Sao Tome and Principe. Nic.st landing page indicating requested (non-existent domain name) may be available.
5. TK : Tokelau. Page contains several links to unrelated websites (external advertisements). No reference to registry.
6. VN : Viet Nam. Page referring user to info.vn, a portal site providing news, legal issues relating to use of .vn, and indicating that the requested (non-existent) domain name may be available.
7. WS : Samoa. Global Domains International Inc. page contains a 4 minute video promoting the use of .ws and a method for earning income by encouraging others to acquire .ws names.

Given that the following table provides an objective classification of the harms provided on the harms lists and technical classification, it is not intended to reflect, nor did the study group consider, whether the harms or reason for use of wildcards are desirable or undesirable.

| **Harm** | **Country Code** | **Protocol Tests** |
|---|---|---|
| Architectural violation | This harm applies to all cc's engaging in wildcarding. | NA |
| Impact on Internet protocols | This harm applies to all cc's engaging in wildcarding | NA |
| Single point of failure | This harm applies to all cc's engaging in wildcarding | NA |
| Reserved and blocked domains appear alive | (note: We may need to know the policies on reserved/blocked names of each cc to know whether this harm would apply)<br><br>This may apply to .tk and .ph, as it appears as though any domain is alive.<br><br>This may not apply to the other cc's, as the unregistered domains do not appear alive. | NA |
| Fragmentation of the DNS ecosystem | This harm applies to all cc's engaging in wildcarding | NA |
| Privacy concerns | This harm applies to all cc's who engage in wildcarding. | TLD\Protocol SMTP SUBMISSION HTTP HTTPS<br>KR refuse refuse connect refuse<br>PH connect refuse connect refuse<br>PW refuse refuse timeout connect |

| | | |
|---|---|---|
| | | ST connect refuse connect connect<br>TK connect timeout connect refused<br>VN connect refuse connect refuse<br>WS timeout timeout connect timeout<br><br>Those ccTLDs whose SMTP servers accept wildcards (i.e. .ph, .st, .tk, .vn) may have more privacy concerns than those who do not. However, this is assuming that there is no expectation of privacy for data sent over the other servers. |
| Lack of choice for Internet users | This harm applies to all cc's who engage in wildcarding | NA |
| Poor user experience | While the term "poor user experience" may not apply to all of these cc's, since many of them are attempting to make the user experience better, the description provided (in column at left) applies to all cc's who engage in wildcarding.<br><br>Some ccTLD (e.g. .ph) prevent the harm of not receiving bounced e-mail notices, by returning the e-mail immediately with a clear message that the user sent an e-mail to a wrong address.<br><br>However, despite the fact that .ph attempts to correct the poor user experience of not receiving bounced e-mail notifications, the message is in English only, which negatively impacts the non-English speaking user experience. | The following table demonstrates how long (numbe of seconds) the domain name will stay in DNS cache servers. The user's experience is worsened the longer the domain name is cached.<br><br>TLD\TTL A AAAA NS MX<br>KR 1800 - - -<br>PH 300 - - -<br>PW 600<br>ST 600 - - -<br>TK 300 - - 86400<br>VN 1 - - -<br>WS 10800 - - - |
| Use of privileged position | This harm applies to .tk and .ph. The other cc's are not engaging in external advertisements. | NA |
| Impact on IDN TLDs | For those cc's which offer IDN domains, this could be an issue if the landing page is in one | NA |

| | | |
|---|---|---|
| | language only.<br>The following cc's offer their landing page in one language only: .kr; .ws; .ph; .pw; .st; and .tk.<br>In the case of .kr, while the localization of content is not broken, since the landing page is in Hangul, the choice of non-Korean speakers is limited.<br><br>If the other cc's offer IDN domain names this harm would apply, since the landing page is offered in English only. | |
| Erosion of trust relationships | This harm applies to all cc's who engage in wildcarding | NA |
| New opportunities for attacks | This harm applies to all cc's who engage in wildcarding | NA |

# RECOMMENDATIONS

The study group has come up with the following recommendations. The recommendations are within the mandate of the ccNSO study group and therefore do not address the ICANN Board's request of the ccNSO to provide a report on mechanisms that could be employed to ensure that redirection and synthesis at the top level are effectively prohibited.

**1. Dialogue**

Following our analysis and liaising with the many interested parties (ccTLDs, ICANN) we came to the conclusion that full and frank dialogue on the use of redirection by ccTLDs should be fostered. By ensuring the harms and reasons for use are well understood, a solution is more likely to be arrived at sooner rather than later. This dialogue, however, will only succeed if judgement on reasons for use is suspended.

**2. Identification of cc's using wildcarding**

As mentioned, it was determined that in fact a number of other ccTLDs engage in redirection of sorts even though the behaviours are not captured by RFC 1034. We therefore recommend that the ccNSO advise ICANN that, prior to taking further steps, ICANN and the broader community consider either more clearly delineating which behaviours it is targeting or develop systemic methods to identify (cc)TLDs who are engaged in synthesis.

**3. Differentiate between harms**

It became clear during the group's work that different harms were exhibited by different ccTLD's depending on the manner in which the registry use redirection. The group attempted to remain objective and not determine in this exercise which harms are more or less harmful than others. However, we recommend that the council consider determining which harms or behaviours are more harmful than others.

# PROCESS

The following provides a brief outline of the study group's activities.

**1. Purpose**

The Ad-hoc Wildcard Study Working Group was established by the ccNSO Council to provide to the ccTLD community and the ccNSO Council a comprehensive overview of the issues associated with "redirection" at level of Top Level Domains, and the need for and current use of "redirection" by country code Top Level Domains.

**2. Scope of activities**

The Scope of the Study Group was as follows:

a. Summarize the issues associated with "redirection" as identified by SSAC in its reports
b. Liaise with SSAC to seek further clarification and input if considered needed and appropriate by the group
c. Liaise with the ccTLDs who are currently using "redirection" to solicit their views and perspectives on "redirection"
d. Prepare a session at a ccNSO meeting either at the ICANN meeting in Nairobi or Brussels to present and discuss the results of the study to the ccTLD community.
e. Provide a final report of its findings to the ccNSO council

The Study Group members undertook the following activities in attempting to fulfill its mandate:

a. Corresponded with ccTLDs who engage in wildcarding in an effort to collect their reasons for doing so.
b. Summarize independent findings
c. Compared SSAC and ICANN staff harms lists and compile one list for analysis
d. Provided short description of each harm
e. Independent review of the types of redirection
f. Assessed redirection results, resolution time, and IANA database on registry
g. Mapped the cc's according to the 'harms' list

**3. Membership and chairs**

**Co-Chairs:**

Young Eum Lee
Ondrej Filip

**Members:**
Wali Berjasta. .af
Keith Davidson, .nz
Joel Disini, .ph
Afaf El Maayati, .ma
Khaled Esheh, .ly
Patrick Hosein, .tt
Erick Iriarte, LACTLD (observer)
Rungang Mo, .cn
Kathryn Reynolds, .ca
Yoshiro Yoneya, .jp