ICANN Registry Services Technical Evaluation Panel

Report on Internet Security and Stability Implications

of the

Global Name Registry, LTD

Proposal for the Limited Release of Initially Reserved Two-Character Names

December 4, 2006

Preface

This report presents the findings of a technical evaluation of the proposal[1] by Global Name Registry, LTD for the limited release of initially reserved two-character Second Level Domain (SLD) names into the .name unsponsored generic Top-Level Domain (TLD).

On 8 November 2005 ICANN adopted[2] a consensus policy developed by its Generic Names Supporting Organization (GNSO) concerning the review and approval of requests by gTLD registry operators for new registry services.[3] This policy was implemented on 25 July 2006[4] as the Registry Services Evaluation Policy.[5] The policy provides for the evaluation of a proposed registry service by a team of experts selected from a standing Registry Service Technical Evaluation Panel (RSTEP)[6] when ICANN determines that the service could raise significant security or stability issues.

The process begins with a preliminary determination by ICANN that an RSTEP review is or is not required for a particular proposed registry service.[7] If ICANN determines that a review is required, an RSTEP review team investigates and evaluates the proposed service with respect to its potential impact on security or stability, as defined by the consensus policy:

> **Security**—An effect on security by the proposed Registry Service shall mean (a) the unauthorized disclosure, alteration, insertion, or destruction of Registry Data, or (b) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.
>
> **Stability**—An effect on stability shall mean that the proposed Registry Service (a) is not compliant with applicable relevant standards that are authoritative and published by a well-established, recognized, and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs sponsored by the IETF, or (b) creates a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems operating in accordance with applicable relevant standards that are authoritative and published by a well-established, recognized, and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs and

[1] http://www.icann.org/registries/rsep/GNR_Proposal.pdf

[2] http://www.icann.org/minutes/resolutions-08nov05.htm

[3] The ICANN Board resolution adopting the GNSO consensus policy (see footnote 2) specifies that implementation of the policy in contractual terms should be guided by the provisions of the .NET registry agreement (http://www.icann.org/tlds/agreements/net/net-agreement-new.html), which includes a precise definition of "Registry Services."

[4] http://www.icann.org/announcements/rsep-advisory-25jul06.htm

[5] http://www.icann.org/registries/rsep/rsep.html

[6] http://www.icann.org/registries/rsep/rstep.html

[7] The consensus policy also provides for the separate review of potential competition issues, which lie outside the scope of the RSTEP review.

relying on Registry Operator's delegation information or provisioning services.

The review team completes its evaluation within 45 days, and prepares a written report of its findings, containing:

(a) a detailed statement description of the technical issue(s) raised by the proposed registry service, and the assumptions, information,[8] analysis, reasons, and information reasoning upon which the review team's evaluation is based;

(b) the team's expert assessment of the potential impact of the proposed registry service on security or stability; and

(c) a response to any specific questions from ICANN that were included in the referral from ICANN staff in its request for the RSTEP review.

The review team's report is delivered to the ICANN Board as input to the Board's consideration of the proposed registry service and action on the registry operator's request to deploy the service within the context of its contract with ICANN.

It is important to recognize that the RSTEP review is a technical evaluation of a proposed registry service with respect to the likelihood and materiality of effects on security and stability, including whether the proposed registry service creates a reasonable risk of a meaningful adverse effect on security or stability. Because many other questions and issues may be relevant to the overall assessment of a proposed registry service, it is not a recommendation to the ICANN Board concerning whether or not the Board should approve or reject the registry operator's proposal.

[8] RSTEP review teams are expected to gather information from as many sources as necessary in order to conduct a thorough and comprehensive evaluation, including, but not limited to, information provided by the registry operator, by ICANN, and by contributors to the ICANN public comment forum that is associated with each registry service request.

Contents of the Report

1 Introduction

1.1 The Global Name Registry, LTD (GNR) Proposal

Global Name Registry Limited proposes the limited release of initially reserved two-character Second Level Domain names into the .name unsponsored generic Top-Level Domain. The proposal is not to delegate two character SLDs, *per se,* but to allow registrations at the third level under those SLDs, e.g., <somename>.li.name. GNR wishes to satisfy demand from persons with two-character family names, such as 'Li'.

According to GNR:
"In pure technical terms, Global Name Registry proposes to simply add and reserve for third level registrations, all two-character strings according to the current rules in the .NAME registry. The strings will be added to the already existing shared third-level namespace on the .name gTLD available to people worldwide through ICANN Accredited Registrars, and made available for registration on the third level on a first-come, first-served basis. All two-character names will be shared and not released directly on the second level.

"By way of background, since the inception of .name Global Name Registry has, per its Appendix K, initially reserved all two-character strings at the second level, such as xi.name, li.name, or ng.name.

"Technically, and in reference to the language of Appendix K, the proposed release is not a release of the two-character strings on the second level. Rather, the proposal is to share all such two-character names for third level registrations only.

"Also note that two-character names are existing on .COM today and are posing no problem to technical stability and security."

GNR proposes to avoid confusion with corresponding country codes with three measures: 1) no release on the second level, 2) seeking consent from ISO and as many ccTLD managers as possible, and 3) acting to increase general community awareness of .name as a space for personal names.

GNR also proposes staged testing and validation of relevant structures (e.g., two-character third reservation list), and including EPP command verification and toolkit interoperability testing, whois system validation, and real-world delivery verification.

Although GNR states that there are no technical problems associated with two-character names, they acknowledge that ccTLD manager DENIC has expressed concern regarding a problem cited in RFC 1535 in 1993, in which incorrect domain names could be returned from some resolvers. GNR believes that this problem is not unique to .name, and in any event is no longer relevant since it was due to old versions of software.

GNR asserts that the proposal would have no impact on the whois service. “The Limited Release of the two-character names will show in *Whois* in the same way as Shared Second Levels show today, e.g. for smith.name.”

1.2 RSTEP Process Summary

1.2.1 Activities

RSTEP evaluated the GNR proposal with respect to its potential impact on the security and stability of the Internet. In order to inform its work, the review team took advantage of previous analyses of the behavior of the DNS and consulted with outside experts.

During the period of the review team’s work (starting with the referral from ICANN to the Chair of the Registry Services Technical Evaluation Panel on October 20, 2006), the team took the following actions:

- Participated in 11 conference calls attended by the review team and the Chair of the Registry Services Technical Evaluation Panel;
- Reviewed the feedback of the open public comment process initiated by ICANN on 20 October 2006;
- Consulted with external experts in registry services related to security, stability, and the behavior of the DNS;
- Requested, collected and analyzed new data from external sources; and
- Performed a new experiment, and analyzed the resulting unique data.

1.2.2 Public Comments

ICANN opened a public comment forum for the GNR *two-character names* proposal on October 20, 2006. The comment period closed on November 20, 2006.

A total of ten comments were made in the forum by nine individual members of the community. No supporting organization or constituency within ICANN commented on the proposal. Abstracts of the public comments can be found in section B.1.6 of this report, “ICANN Public Comments on the GNR Proposal.”

1.2.3 Gathering of Supporting Material and Data

The RSTEP evaluation team decided early in the review to gather data to evaluate the relevance that problems described in RFC1535 currently have on Internet DNS traffic. As noted in the analysis of the data collected, in the case of the GNR proposal it is difficult, based on observed data, to determine if the relevant queries are coming from old and non-RFC compliant resolvers or from incorrectly typed queries.

The publicly available material is widely available and the References section of this document provides abstracts and, where available, URLs for the source documents that this team reviewed. Not all data that were available to the RSTEP review team are publicly available.

The RSTEP team gathered three types of data:

- Query data from authoritative name servers, on queries for SLDs under a TLD of the form *.<TLD>.<TLD>. These data were provided by Nominet, the registry for .uk, the second largest ccTLD and overall the third largest TLD.

- Data gathered from our own unique ‘honeypot’ experiment. The experiment set up web servers on several domains in order to receive traffic that could result from incorrect behavior by resolvers, as described in RFC 1535. The server collected the queries and we analyzed them in order to classify the requests.

- Statistics from IANA on the current existence of <TLD>.<TLD> registrations.

1.2.4 Discussions with GNR

The RSTEP process mandates that the proposing registry make itself available to meet with the review team in order to clarify the team’s understanding of specific aspects of the proposal. Such a meeting is solely at the discretion of the review team. The team did not have any questions, did not request a meeting, and no meeting was held.

1.3 Key Definitions

1.3.1 Security

An effect on security by the proposed Registry Service shall mean (A) the unauthorized disclosure, alteration, insertion or destruction of Registry Data, or (B) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards. (Definition comes from GNSO Recommendation, located at http://gnso.icann.org/issues/registry-services/final-rpt-registry-approval-10july05.htm#5 .)

1.3.2 Stability

An effect on stability shall mean that the proposed Registry Service (A) is not compliant with applicable relevant standards that are authoritative and published by a well-established, recognized and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs sponsored by the IETF or (B) creates a condition that adversely affects the throughput, response time, consistency or coherence of responses to Internet servers or end systems, operating in accordance with applicable relevant standards that are authoritative and published by a well-established, recognized and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs and relying on Registry Operator's delegation information or provisioning services. (Definition comes from GNSO Recommendation, located at http://gnso.icann.org/issues/registry-services/final-rpt-registry-approval-10july05.htm#5 .)

1.4 Members of the RSTEP Panel for this Proposal

The five members of the RSTEP Panel review team for the GNR *two-character names* proposal are:

- Rob Blokzijl (RIPE; The Netherlands)
- Jordyn Buchanan (Google; USA)
- Hiro Hotta (JPRS; Japan)
- Glenn Kowack (Consultant; USA; chair)
- Kurt Lindqvist (Internet Technology Advisors; Sweden)

The members of the review team were assisted in their work by the Chair of the Registry Services Technical Evaluation Panel:

- Lyman Chapin (Interisle Consulting Group; USA)

Staff support was provided to the panel by ICANN:

- Patrick Jones - Registry Liaison Manager

2 Summary of Findings

Global Name Registry Limited proposes the limited release of initially reserved two-character Second Level Domain names (SLDs) into the .name unsponsored generic Top-Level Domain (TLD).

The proposal is to not delegate two character SLDs, *per se*, but to allow registrations under those SLDs, e.g., <somename>.li.name. This would allow for registration of two-character family names that are currently blocked but are very common in certain cultures. Registering existing TLD labels under a TLD of the form <TLD>.<TLD> could potentially lead to the problems described in RFC1535.

With respect to technical feasibility, we believe that GNR could implement the service that they have proposed. The test plan and prior art appear adequate to ensure this.

Our technical evaluation of this proposed registry service with respect to the likelihood and materiality of effects on security and stability concludes that it does not create a reasonable risk of a meaningful adverse effect on security and stability. This report presents a detailed description of the technical issues raised by the proposed service, and the assumptions, information, and reasoning upon which our evaluation is based.

The principal findings that lead us to this conclusion may be summarized as follows:

- Nearly all TLDs today already allow registration of two-character domains under the TLD, many for years, and very few operational issues have ever been reported;
- Data from queries to a TLD that makes use of TLDs as SLDs show that the proportion of erroneous queries that are for *.<TLD>.<TLD> is very small; and
- Data gathered from a honeypot experiment indicates that misdirected queries represent a microscopic fraction of overall traffic.

This RSTEP review team finds that, taken in the context of our overall understanding, none of the observations point to the proposed release of two-character Second Level Domain having a material security or stability impact on the Internet.

3 Analysis of Security and Stability Issues

In order to assess the potential security and stability impact of introducing two-character SLDs into .name, the review team began by considering the current practices regarding two-character SLDs within various TLDs, as well as the presence of <TLD>.<TLD> combinations. The review team noted that there are a significant number of TLDs that allow the registration of TLDs as SLDs. A systematic walk through the DNS shows the following numbers:

Number of TLDs registered in the root zone	265
Possible <TLD>.<TLD> combinations	70225
<TLD>.<TLD> combinations with NS or A records	11592

In addition to considering the frequency of two-character SLDs and <TLD>.<TLD> combinations, the team reviewed known problems with <TLD>.<TLD> combinations. A recent overview of known problems with the DNS was presented at the RIPE53 meeting by Duane Wessels of The Measurement Factory/CAIDA. It recited a list of 32 known problems with the DNS, categorized as follows:

Protocol Issues	9
Implementation Issues	8
Operational Issues	10
Registry/Registrar Issues	5

Of the eight implementation issues, two were related to a combination of the presence of <TLD>.<TLD> domains and bad software behavior. The most significant of these problems is described in RFC 1535 and is discussed in detail in Section 3.1.1 below. The review team also conducted an exhaustive investigation of the potential security- and stability-related effects in each of the potential problem areas.

In addition, the review team conducted two kinds of analysis on the data collected from the behavior of actual DNS servers. First, we reviewed name server data from one of the .uk name servers. Second, we conducted an experiment in an attempt to produce the problems theoretically caused by <TLD>.<TLD> combinations.

We also considered special characteristics of the .name domain.

Taking these factors into consideration, the review team concludes that:

(1) Name server and experimental data reveal that inadvertent queries for <TLD>.<TLD> domains are fairly uncommon. More often than not, these queries seem to be the result of user error or temporary failures as opposed to software errors.

(2) <TLD>.<TLD> combinations are already extremely common, including combinations that seem far more likely to cause problems than two-character SLDs within .name, such as net.uk or de.com. The review team is not aware of any reports of problems attributed to existing <TLD>.<TLD> combinations.

(3) On balance, and taking into account theoretical security and stability effects as a result of the introduction of two-character SLDs within .name, these SLDs are unlikely to have any meaningful net increase in the level of these security or stability issues.

3.1 Theoretical Problems

The review team considered the types of problems that could potentially be caused by the introduction of <TLD>.<TLD> combinations within .name. Each of the potential problem areas is described below.

3.1.1 Incorrect Response to a Query for a Valid Domain Name

Perhaps the most dangerous possibility of allowing two character second level domains within .name (or of any <TLD>.<TLD> combinations) is that in some cases, improper behavior by DNS resolvers may cause information for an incorrect domain name to be returned in response to a query.

For example, a misconfigured resolver running on a host with a domain name in the .name TLD may incorrectly return DNS records for the domain "icann.ex.name" in response to a query for "icann.ex". RFC 1535 describes a situation in which a user types in a domain name and is inadvertently led to an incorrect destination. A user on "machine.xx.name" attempting to reach "host.yy" could find their request handled by a misconfigured resolver as follows, in this order:

host.yy.machine.xx.name.
host.yy.xx.name.
host.yy.name.
host.yy.

If “host.yy.name.” exists, the resolver would return the records for that domain name rather than “host.yy”, and an incorrect destination would be reached.

The problem described by RFC 1535 was a possible behavior of BIND 4.9.2 in 1993. RFC1535 and RFC1536 describe how to overcome this behavior by proper configuration of this BIND version.

The BIND 4 series has been deprecated since mid-1997. BIND 4 also has serious security vulnerabilities, and the Internet Systems Consortium, who develop and maintain BIND, strongly discourage administrators from using it. Newer versions of BIND do not exhibit this incorrect behavior. However, other software may also exhibit the incorrect behavior described in RFC1535.

3.1.2 Unexpected Response to a Query for a Non-Existent Domain Name

Section 3.1.1 describes the situation in which the user enters a valid domain name, but information for a different domain name is returned. Another problem that may occur as the result of <TLD>.<TLD> combinations is that when the domain name entered by the user does NOT exist, the user’s resolver or client software may attempt to find a related domain name by appending additional domain name(s) to the domain entered by the user. In some cases, this may result in an unexpected result being returned in response to the query.

3.1.2.1 Cause

3.1.2.1.1 Search Lists

Unlike the situation described in RFC 1535 in which the user enters a valid domain name, but is directed to another host, in some cases the domain name that the user is trying to reach may not exist, but the configuration of the resolver may incorrectly cause a domain within another TLD to be reached. This behavior is caused by a feature in many resolvers that allows a list of domains to be specified that the resolver will search through in order to resolve a domain name. If the initial lookup of the domain name fails, the resolver then consults the search list andbegins to append sequentially each of the domain names in the search list to the queried domain name. In the event that a successful lookup occurs, the resolver returns that result and no further entries in the search list are considered.

In a simple example, a user may have a search list with the following entries: example.com, subdomain.example.com, and otherdomain.com. The user may request that the resolver provide an IP address for the host name 'www'. The resolver would then attempt to resolve the following domains:

```
www.
www.example.com.
www.subdomain.example.com.
www.otherdomain.com.
```

In this example, valid DNS records may exist for both "www.example.com." and "www.otherdomain.com.". In this case, the record for "www.example.com." would be returned, because after failing to obtain a result for "www.", the resolver would receive a valid response for "www.example.com." and return the result. None of the other domains in the search list would be considered.

If a resolver were configured with the domain "name" in the search list, it is possible that the inclusion of two-character second level domains might cause some invalid domains to resolve as a result of the .name domain being appended to the user's query. As an example of this phenomenon, consider the case where the domain "example.li" does not exist while the domain "example.li.name" does. When a lookup is requested for the domain name "example.li", a resolver with the domain "name" in its search path would first attempt to resolve the domain "example.li" and, after that attempt failed, would resolve the domain "example.li.name" and return the DNS records to the client. In this case, the user would be directed to the site "example.li.name" although they had attempted to navigate to the nonexistent site "example.li".

3.1.2.1.2 Other Software

In some cases, after an initial DNS lookup failure, client software may attempt to append a domain name to the initial query and attempt to resolve the new domain name. For example, many web browsers attempt to add the string ".com" to the end of the domain name specified by the user if the initial DNS lookup fails.   If the user enters a string such as "icann", after receiving an initial DNS failure, the browser would issue a second DNS request for "icann.com". A client that appends ".name" to the user's requested domain name would cause the same problems as a resolver configured with the .name domain name in the search list, as described above.

3.1.3 User Confusion

It is possible that some users may simply be confused by the presence of two-character second level domains, believing that they are somehow related to ccTLDs. This concern was raised by some ccTLD operators in response to GNR’s proposal, but the review team is not aware of any specific instances or data that further elaborate on this potential for confusion.

There have been 18 UDRP[9] cases on two-character SLDs. They discussed the possibility of users confusing domain names with trademarks. No specific argument was made about confusing domain names with country codes.

3.2 Analysis

3.2.1 Presence of <TLD>.<TLD> combinations in other TLDs

Two-character SLDs appear in the vast majority of TLDs. In many cases, two-character SLDs do not overlap with the two-character codes used in ccTLDs. In cases where no such overlap occurs, there is no reason to believe that any of the problems described above would occur. However, many two-character SLDs do overlap with two-character ccTLD country codes, and some longer TLDs are also present as SLDs (for example, NET.TLD appears quite often). The meaning of these <TLD>.<TLD> combinations varies depending on the TLD in which they are contained. There are three general categories, which describe these <TLD>.<TLD> combinations:

(1) In many cases, where registrations are allowed directly on the second level, the <TLD>.<TLD> combination has no particular meaning. Rather, each <TLD>.<TLD> combination has been registered by an arbitrary third party and is used in whichever context the registrant believes is appropriate. For example, in the .com domain where all 265 possible <TLD>.<TLD> combinations have been registered, es.com is the website of Evans and Sutherland, a visual simulation technology company, and is not in any way associated with Spain, the country represented by the two-letter ISO 3166 code ES.

(2) Some TLDs that provide third level registrations have attempted to duplicate the gTLD naming structure. Many TLDs offer registration within COM.<TLD>, NET.<TLD> or ORG.<TLD> for commercial, networking or not-for-profit organizations, respectively. For example, in the .uk TLD Nominet (the registry operator for .uk) allows registration within .net.uk exclusively for

[9] ICANN’s Uniform Dispute Resolution Policy (UDRP) was developed specifically to deal with disputes involving domain names and trademarks.

Internet service providers[10] whereas org.uk is intended for not-for-profit entities[11].

(3) In some TLDs, the use of two-character codes is intended to provide meaning or categorize the registrations, but this meaning is distinct from the meaning of the related top-level domain. For example, several TLDs (including .UK and .NZ) use the second-level domain AC.<TLD> for the registration of academic institutions. This usage does not mirror the gTLD practice of registering educational institutions within the .EDU TLD nor does it reflect the association of the .AC TLD with the Ascension Islands. The operator of .aero allows registration of two-character SLDs by the airlines that have been assigned that particular two-character code by IATA. This categorization is distinct from the use of two-character strings to represent country codes. The proposed addition of two-character SLDs to .name is most similar to this last case—within .name the two-character strings at the second-level would represent last names rather than mirror the practice of using country codes for TLDs. A final example is the .US TLD, which is described in RFC 1480[12] and RFC 1591[13]; within .US second-level domain names are based on the two-character postal codes for states, but many of these two-character codes overlap with ISO 3166 country-codes used for ccTLDs (for example, CA is the two-character postal code for the state of California as well as the two-character country code for Canada[14]).

[10] http://www.nominet.org.uk/policy/consultations/netuk/

[11] http://www.nic.uk/registrants/legal/rules/

[12] RFC 1480, "The US Domain", A. Cooper, J. Postel, June 1993 (see http://www.isi.edu/in-notes/rfc1480.txt)

[13] RFC 1591, "Domain Name System Structure and Delegation", J. Postel, March 1994 (see http://www.isi.edu/in-notes/rfc1591.txt). It is interesting to note that, several months after the publication of RFC 1535, the principal caretaker of the Domain Name System felt no need to alter or restrict the use of two-character SLDs within .US, at a time when the resolver error described in RFC 1535 would have been far more common than it is today.

[14] A particularly interesting case is PR.US. In this case, PR is both the two-character postal code for Puerto Rico as well as the ISO 3166 country code for the same territory. As a result, the PR.US domain and the .PR domain both provide registration spaces relating to Puerto Rico, although they are operated by different registration authorities with distinct sets of DNS records.

Since 2001, ICANN has introduced ten new generic top level domain names (.aero, .biz, .cat, .coop, .info, .mobi, .museum, .name, .pro, and .travel). In most cases, the agreements between the registry operators and ICANN contain a similar prohibition on the registration of two-character second level domain names as is contained in the .name agreement. However, two of the new gTLDs currently allow resolutions of two-character second level domains:

(1) The .museum registry has included a wildcard A record within its zone file for approximately three years[15]. This wildcard record is intended to direct users to http://index.museum , which contains a listing of all second level domain names registered within the .museum TLD. Although Attachment 11[16] to .museum's registry agreement contains a provision reserving all two-character second level domain names (identical to the one contained in .name's Appendix K), the effect of the wildcard is that all domain names containing a two-character second level string resolve to the IP address of index.museum.[17]

(2) The .aero registry agreement contains a provision reserving two-character second level domain names (in an Attachment 11 identical to .museum's). However, Section 6 of Attachment 23[18] to the .aero agreement allows two-character registrations when they are used as "standard two-character airline designator codes". A number of airlines currently have delegations within the .aero zone on this basis. In some cases, (e.g., af.aero and ba.aero) these delegations overlap with ccTLD names. At the time of this report, 13 delegations were present in the .aero zone file that overlap with two letter country codes.

All told, of 70,225 possible <TLD>.<TLD> combinations, DNS records (either A or NS records) currently exist in 11,592 cases (in other words, 16.5 per cent of all possible <TLD>.<TLD> combinations exist). In many cases, these <TLD>.<TLD> domains represent combinations of some of the most popular top-level domains in the world (for example, de.com, com.cn, and net.uk and even the rather odd com.com). Despite the

[15] http://musedoma.museum/policy/wildcard
[16] http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-att11-20aug01.htm
[17] Cary Carp, the "curator" of .museum, recently announced that the registry intends to ask ICANN to suspend the operation of the wildcard record. (See http://forum.icann.org/lists/tralliance-comments/msg00014.html)
[18] http://www.icann.org/tlds/agreements/aero/sponsorship-agmt-att23-17nov01.htm#6

presence of these combinations in virtually all TLDs, the review team is aware of no significant impact on the security or stability of the Internet as a result. Given that GNR proposes to add a maximum of 265 additional <TLD>.<TLD> combinations (2.3% of the existing total), the operation of so many <TLD>.<TLD> combinations today with so little discussion of potential or actual problems as a result strongly indicates that these additional combinations would have little substantive effect on security or stability.

3.2.2 Analysis of DNS Data from .uk

The review team obtained access to data from Nominet's slave-servers for .uk covering one day (24 hours). These data can be found in Section 4.1. Based on these data, some numbers can be derived.

Name server:	ns1.nic.uk
Date:	01 11 2006
Total number of queries:	94.8M
Queries for .com.uk:	0.07M

.com.uk is not a delegated domain under .uk. Still 0.07% of all queries to .uk refer to it. Based on this we can make a few observations:

(1) The actual number of queries (0.07%) is quite small.

(2) Some of these queries may have been caused by users actually typing in a domain name such as host.com.uk.

(3) Some of these queries may have been caused by faulty resolver behavior as described above.

(4) The numbers above will effectively be upper bounds of the problem. The reason for this is that queries will be passed through resolvers from the clients. These resolvers will cache correct answers, but while they will also cache replies to erroneous queries, these have a much lower TTL. In our data source, .uk, valid replies have a cache TTL of 172800s while for NXDOMAIN the TTL is 300s. This caching means that the total query volume is probably higher, and the real number of total erroneous queries also is somewhat higher. Since the effect of the cache becomes bigger when the value of TTL is set bigger, the observed relation still is an upper bound and if we could measure the total number of queries we would probably see that erroneous queries are an even smaller percentage.

One may safely conclude that the size of the problem is below 0.07% in the case of .com and .com.uk. The .com domain. due to its nature and history, seems to have the largest potential for overlapping behavior as described in RFC1535, and the data above therefore seem reasonable to accept as the ‘worst case’.

Based on the data above the RSTEP team concludes that the overlap as described in RFC1535 seems small enough that it cannot be considered a risk to security or stability of the Internet in general or the DNS in particular.

3.2.3 Analysis of experimental data

The data described in Section 3.2.2, “Analysis of DNS Data from .uk”, were used to determine the number of DNS requests that seemed consistent with the problem described in RFC 1535. However, using DNS data alone provides no information about the reason that the DNS queries were generated. In addition to problems with resolver search order as described in RFC 1535, suspicious DNS queries could be generated from users incorrectly entering the domain name (either intentionally or unintentionally), or client software modifying the domain name entered by the user. In order to determine the cause for the DNS queries, it is necessary to correlate the DNS querying to the underlying user action.

In order to perform this correlation, the review team conducted a “honeypot” experiment by registering domain names that are likely to cause incorrect DNS lookups due to the behavior described in RFC 1535, and providing answers to those queries that direct the user to a server that logs the user's requested domain name. By comparing the user's request with the registered domain name, the review team could then analyze whether the user reached the site as a result of the type of incorrect DNS lookup described in RFC 1535, or as the result of some other cause.

A detailed description of the experiment is provided in Section 4.2. The key findings are summarized below.

The following table summarizes the number of queries received by the web server associated with each domain name. The third column (labeled “RFC 1535-type errors”) indicates the count of queries that were received in which the Host: header transmitted by the client does not include the domain’s TLD (e.g., a query for the domain name “golem.de.com” was received, but the browser sent the domain name “golem.de” in the host header). This mismatch between the domain name and HTTP Host: header is indicative of the type of problem described in RFC 1535.

Domain Name	# of queries	RFC 1535-type errors	Estimated total queries to real site
flurl.com.tw	242	11	57,000,000[19]
daum.net.nz	1	0	1,900,000,000[20]
golem.de.com	127	50	> 2,000,000[21]
photobucket.com.mx	65	1	56,000,000[22]

In some cases, many queries were received from the same originating IP address. For example, many of the queries received for the golem.de.com domain seem to be repetitive requests issued by RSS readers. In order to prevent repetitive requests from skewing the result set, a further analysis was peformed to count the number of unique IP addresses making requests in each domain. This analysis is summarized below:

Domain Name	# of unique IPs	IPs with RFC 1535-type errors
flurl.com.tw	146	4
daum.net.nz	1	0
golem.de.com	57	15
photobucket.com.mx	44	1

[19] Based on 19 days' traffic at 3 million page views per day. This estimate is based on http://www.primezone.com/newsroom/news.html?d=107516 ("…page views per month have grown over 500% since that date to over 100 million per month")

[20] Based on 19 days' traffic at 100 million page views per day. This estimate is based on http://www.asiamedia.ucla.edu/article.asp?parentid=26779 ("In the case of major portal www.daum.net, its news service's page views…soared to nearly 3.8 billion last month")

[21] A measure of golem.de's traffic was not readily available to the panel. In order to estimate the traffic for the site, the panel extrapolated based on Alexa traffic measurements (see http://www.alexa.com/data/details/traffic_details?url=golem.de) which show that approximately 75 out of every one million page views by Alexa users were to golem.de domains. Comparing this data with the Alexa data and known page view data of similar sites provides an estimated range of 100,000 to over 1,000,000 page views per day. Using the low end of that range for twenty days yields the total page views of 2,000,000 used in the chart above.

[22] Based on 8 days' traffic at 7 million page views per day. This estimate is based on http://blog.photobucket.com/archives/2005/03/fun_statistics.html

None of the domains in the honeypot attracted more than 12 hits a day on average, and few of the hits appeared to indicate RFC 1535 problems. One of the registered domains (daum.net.nz) did not generate any queries that appeared to be the result of RFC-1535 problems. Even the domain that generated the most RFC 1535-type errors (goelm.de.com) saw less than one unique IP address with the problem per day.

Given that the registered names were chosen to overlap with popular sites (many with millions of page views per day), the traffic reaching the honeypot represents an insignificant fraction of the total traffic for the site. In the extreme case, daum.net is a very popular Asian portal attracting over 100 million page views per day. In over two weeks, the experimental registration daum.net.nz attracted only a single hit (representing 0.00000006% of the site's total traffic). Even golem.com.de, the site with the greatest proportion of hits in the experiment relative to the target site's expected traffic (and using a very conservative extrapolation of golem.de's traffic) identifies only 127 hits for an estimated 2,000,000 page views for the golem.de site (representing 0.006% of the site's estimated traffic).

Because little of the traffic in the experiment seems to be associated with the type of query associated with RFC 1535, other possible explanations for the traffic include:

(1) Users may be entering the incorrect domain name into their client software.

(2) Client software may be altering the domain name entered by appending a TLD to the end. In some cases, this may be the result of a temporary DNS failure in resolving the original domain name entered by the user, which would then cause either the resolver or the client software to append strings to the end of the domain name in order to find a match.

(3) Other (unknown) software errors may cause the wrong domain name to be looked up.

Regardless of the cause, the level of traffic indicated by the experiment is so low as to pose a minimal risk to the security and stability of the Internet.

3.2.4 Characteristics Specific to the .name TLD

GNR has suggested that the .name TLD may be a special case in the sense that the second level domains under .name are not available for registration by the general Internet community. They are reserved by the registry, GNR, for shared use by third level domain names, which can be registered by the general Internet community. As an example:

ivanov.name

might be reserved by GNR, but

aleksandr.ivanov.name

and

fyodor.ivanov.name

might be registered by Aleksandr Ivanov and Fyodor Ivanov, respectively.

GNR argues that this gives a special status to second level domain names in .name, which in the case of two character names that coincide with two letter country codes, would diminish possible confusion.

From a technical point of view there is no special case for the .name SLDs. The special case is an administrative one that has no equivalent in the DNS protocol. In other words, there are no bits in the DNS protocol that support this assumption.

However, the problem described above in Section 3.1.2 relies on either the resolver or the user's client software appending a specific TLD (in this case .name) to the end of the user's query. This requires that the resolver or software be configured to append the TLD. However, these scenarios are quite unlikely because:

(1) It is unusual that resolvers would be configured with a top-level domain name in their search list. Typically, search lists include second or third level domains in order to allow easy navigation to hosts within an organization (for example, a company with host names such as "host1.corp.company.com" might configure its resolvers with "corp.company.com" in its search list to allow users to simply enter "host1" in order to reach the host).

(2) Generally, software that appends a TLD to the end of the user's query is assuming that the user neglected to include the TLD in their query and appends the most likely TLD. Many browsers, for example, append ".com" to the end of queries because .com is the largest TLD and many popular websites primarily use a .com domain name. Other software may attempt to append a ccTLD to the query, depending on the user's configuration (for example, by appending .cn for Chinese users). The review team is aware of no software that specifically appends ".name" to the end of domain names provided by users.

Finally, the review team notes that the association of the .name TLD with personal names may make it less likely that users will confuse two-character second level domains within .name with ccTLD country codes. It seems reasonable that a user seeing a domain such as hung.li.name are likely to understand that the string “li” represents a name as opposed to the country code for Lichtenstein.

4 Research Conducted by Review Team

The members of the RSTEP panel that carried out this Security and Stability implications analysis searched relevant literature and network sources concerning technical problems related to two-character second-level domain names (SLDs). However, this has not been an area of significant concern and there is only a very small amount of prior information available on this subject. Consequently, the review team found it necessary to obtain data not generally available from public domain sources. The team collected from cooperating organizations information that provides insights into the nature and magnitude of the problem. The review team also undertook new research in the form of a "honeypot" experiment. Those new data are assembled here. In those cases where data were collected from other organizations, the conclusions are our own, not necessarily those of the organization that provided the original data.

4.1 Nominet Data on observed requests for TLDs as SLDs

Nominet.UK, the Registry for the .uk Top level Domain, generously provided data relevant to the study of this review team. The actual data used can be found in the tables below. The conclusions drawn by the review team are our own, not necessarily those of Nominet.UK.

The following table lists the number of queries during 24hs for <something>.<tld>.uk, where <tld> is not a valid SLD under .UK.

<tld>	#	<tld>	#	<tld>	#
co	78865060	ni	39	ve	5
unknown	7065537	th	39	ws	5
org	5434328	lt	38	gd	4
net	2569880	id	36	gn	4
ac	698011	sg	32	la	4
gov	99656	ag	30	li	4
com	66932	cg	29	lu	4
uk	4147	fi	29	mg	4
mil	2694	lv	29	pg	4
edu	1803	sk	28	tc	4
om	1577	ua	23	um	4
cu	1215	arpa	22	af	3
au	677	kr	22	bm	3

ca	609	sd	22	er	3
cn	554	ms	21	ge	3
it	471	my	21	gm	3
de	421	bg	20	ir	3
so	416	bh	20	ke	3
ci	405	cf	20	ng	3
tr	344	mk	20	nr	3
as	316	ba	19	qa	3
br	316	hk	19	sm	3
sc	283	ee	18	tn	3
cc	269	mu	18	ug	3
in	251	nc	18	uz	3
fr	245	eg	17	zw	3
es	212	uy	17	bf	2
pl	205	gb	16	cy	2
ru	198	ph	16	et	2
jp	197	mo	14	fk	2
mx	185	pk	14	fm	2
do	178	vn	14	gg	2
nl	172	fo	13	gu	2
cm	165	ga	13	io	2
ar	155	mc	13	iq	2
ad	141	tj	13	jm	2
ch	126	az	12	kh	2
ec	113	cr	12	ki	2
il	102	gh	12	ls	2
pe	95	md	12	mz	2
info	94	an	11	na	2
se	93	tt	11	pa	2
biz	90	kw	10	sa	2
bo	88	mh	10	sl	2
cl	87	re	10	aero	1
za	87	vc	10	bi	1
ae	82	gt	9	bj	1
no	80	by	8	bz	1
ro	78	cx	8	dm	1
ne	75	hr	8	dz	1
ao	72	jo	8	gf	1
al	69	mr	8	gp	1
cz	69	tk	8	gy	1
to	69	yu	8	kg	1
us	63	coop	7	kn	1
sh	62	cv	7	kz	1
be	60	td	7	mm	1
ie	53	ai	6	mt	1
tw	53	bn	6	name	1
at	52	lb	6	np	1
dk	52	lk	6	pn	1
pt	52	mn	6	pr	1

gr	48	nu	6	py	1
bt	47	pro	6	sj	1
cd	45	si	6	sn	1
am	42	su	6	st	1
nz	41	vi	6	sv	1
ck	40	bb	5	tm	1
ma	40	gw	5	tp	1
tv	40	int	5	tz	1
hu	39	ky	5	vu	1
is	39	lc	5	wf	1
				zm	1

NXDOMAINs for valid .uk SLDs observed were:

<tld>	**#**
co	4723753
org	332543
sch	257875
net	37277
ltd	24729
me	10450
plc	9894
mod	9065
mil	2694
nic	426

4.2 Honeypot Experiment and Data

4.2.1 Experiment Objective

Some of the data collected by the review team were used to determine the number of DNS requests that appeared consistent with the problem described in RFC 1535. However, using DNS data alone provides no information about why the DNS queries were generated. In addition to problems with resolver search order as described in RFC 1535, suspicious DNS queries could be generated from users incorrectly entering the domain name (either intentionally or unintentionally), or client software modifying the domain name entered by the user. In order to determine the cause for the DNS queries, it is necessary to correlate the DNS querying to the underlying user action.

In this experiment, we registered domain names that are likely to cause incorrect DNS lookups due to the behavior described in RFC 1535, and provide answers to those queries which directs the user to a server that logs the user's requested domain name. By comparing the user's request with the registered domain name, we can analyze whether the user reached the site as a result of the type of incorrect DNS lookup described in RFC 1535, or as the result of some other cause.

Due to the small number of domain names used, and the relatively short duration, the experiment is not intended to provide statistically meaningful qualitative data concerning the incidence of the problem. Rather, the experiment is intended to determine (1) whether the problem can be observed in a real-world environment, and (2) whether the scope of the problem seems significant for the domain names selected.

4.2.2 Honeypot Methodology

There were four principal steps involved in the experiment:

(1) Selecting and registering domain names
(2) Creating DNS records
(3) Operating the web server
(4) Analyzing web server log data

Step 1: Selecting and Registering Domain Names

The problem described in RFC 1535 occurs only when the user attempts to reach a particular host, but:

(A) The user's resolver is running on a host in a domain name whose parent TLD includes <TLD>.<TLD> combinations.

(B) The combination targetdomain.targettld.parenttld must resolve. (For example, if the client is using a resolver on the host ns1.example.com and is attempting to access target.de, the name target.de.com must resolve.) Once a successful result is returned, the resolver accepts the result and no longer makes further attempts to determine the "correct" result for the domain name, including (in the case of the problem described in RFC 1535) the exact domain name entered by the user.

In selecting domain names for this experiment, a parallel set of constraints was created in order to identify domains where the type of problem described in RFC 1535 would be most likely to occur. This requires that the domain name cause a <TLD>.<TLD> overlap in a TLD that is likely to originate a large number of requests to a subdomain.

This concept may be easiest to demonstrate by example. The review team selected four names for the experiment:

Domain Name	Capture Queries Intended For…	…From Resolvers In
golem.de.com	golem.de	.com
photobucket.com.mx	photobucket.com	.mx
daum.net.nz	daum.net	.nz
flurl.com.tw	flurl.com	.tw

These domains were selected based on Alexa traffic rankings[23] in order to identify domains that were common targets from particular countries. For example, according to Alexa photobucket.com is the 27th most popular website visited by users in Mexico[24]. One of the domain names, photobucket.com.mx, was added approximately halfway into the experiment in order to obtain additional experimental data; any comparison made between the numerical results from each individual domain name should take this into consideration.

Selecting domain names in this manner should identify some of the most likely possible sources of the type of error described in RFC 1535. Most domain names would be far less likely to cause the problem, so this sample is somewhat skewed towards over representing potential problems caused by <TLD>.<TLD> combinations.

Step 2: Creating DNS Records

Once the domains were registered, DNS records were created in order to point clients to the target webserver. In order to log the largest amount of data possible, a wildcard A record pointing to the IP address of the webserver was created for each domain. In addition, a separate A record (also pointing to the IP address of the webserver) was created for the domain name itself. These records meant that any DNS query for the domain name, or any of its subdomains, would resolve to the IP address of the webserver.

Step 3: Operating the Web Server

The web server was configured to operate on the standard TCP port for HTTP traffic (80). No attempt was made to analyze traffic on other ports, including HTTPS traffic on port 443.

[23] http://www.alexa.com/site/help/traffic_learn_more

[24] http://www.alexa.com/site/ds/top_sites?cc=MX&ts_mode=country&lang=none

For each incoming request, the following information was logged:

- IP address of the request
- Date and time of the request
- HTTP request issued
- Host: header sent by the client
- User-Agent: header sent by the client

A simple page was returned to users indicating that they had likely reached the wrong destination. This page also provided a link to a truncated version of the domain name provided in the Host: header, with the TLD removed. (For example, if the Host: header was received with the domain "golem.de.com", a link was provided to "golem.de".) No attempt was made to analyze whether the user clicked on the provided link.

Step 4: Analyzing the Data

After two weeks, the log data gathered by the web server was collected and analyzed. In performing the analysis, the review team initially concentrated on identifying queries that seemed to be the result of the problem described in RFC 1535. In these cases, the Host: header logged by web server would not include the TLD that the web server’s domain was registered in. (For example, in the case of flurl.com.tw, the Host: header recorded would be “flurl.com”.) This initial analysis indicated that a relatively small proportion of the overall queries seemed to be a result of the problem described in RFC 1535.

In some cases, a single host performed a number of queries for the same domain name. For example, many of the queries for golem.de seem to be the result of RSS readers that periodically make queries for specific URLs. In order to prevent these hosts from having an overstated effect on the data, the review team conducted a further analysis considering the number of unique IPs issuing queries to the web server, as well as the number of unique IPs that generated queries that seemed to be the result of the problem described in RFC 1535.

The results of the analysis are laid out in Section 3.2.3 of this document.

4.2.3 Honeypot Data

In order to protect the privacy of the users that reached the honeypot, the third octet of the IP address in the table below has been removed.

Immediately following this table is a key that associates the index numbers listed in the "User-Agent" column with the value of the User-Agent: header received by the server.

IP Address	Date and Time	URL	User Agent	Target Host
84.129.X.103	09/Nov/2006:04:43:43	GET / HTTP/1.0	[1]	www.golem.de.com
84.56.X.148	09/Nov/2006:07:58:48	GET / HTTP/1.1	[2]	golem.de.com
84.56.X.148	09/Nov/2006:07:58:48	GET /favicon.ico HTTP/1.1	[2]	golem.de.com
66.194.X.76	09/Nov/2006:14:09:08	GET / HTTP/1.1	[3]	golem.de.com
84.191.X.165	10/Nov/2006:04:06:54	GET / HTTP/1.1	[4]	golem.de.com
84.191.X.165	10/Nov/2006:04:06:55	GET /favicon.ico HTTP/1.1	[4]	golem.de.com
66.194.X.81	10/Nov/2006:19:02:57	GET / HTTP/1.1	[5]	golem.de.com
80.126.X.166	11/Nov/2006:06:55:47	GET / HTTP/1.1	[6]	golem.de.com
80.126.X.166	11/Nov/2006:06:55:47	GET /favicon.ico HTTP/1.1	[6]	golem.de.com
66.194.X.75	11/Nov/2006:23:50:48	GET / HTTP/1.1	[7]	golem.de.com
84.169.X.92	12/Nov/2006:09:34:32	GET / HTTP/1.1	[8]	www.golem.de.com
84.169.X.92	12/Nov/2006:09:34:33	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
84.169.X.92	12/Nov/2006:09:34:41	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
84.57.X.83	12/Nov/2006:18:55:04	GET / HTTP/1.1	[8]	www.golem.de.com
84.57.X.83	12/Nov/2006:18:55:05	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
84.191.X.246	13/Nov/2006:03:06:54	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
84.191.X.246	13/Nov/2006:03:13:48	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
84.191.X.246	13/Nov/2006:03:18:49	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
84.191.X.246	13/Nov/2006:03:23:50	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
84.191.X.246	13/Nov/2006:03:28:51	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
84.191.X.246	13/Nov/2006:03:33:52	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
212.168.X.26	13/Nov/2006:03:50:21	GET / HTTP/1.1	[10]	www.golem.de.com
212.168.X.26	13/Nov/2006:03:50:21	GET /favicon.ico HTTP/1.1	[10]	www.golem.de.com
66.194.X.73	13/Nov/2006:04:23:02	GET / HTTP/1.1	[7]	golem.de.com
195.10.X.196	13/Nov/2006:13:30:53	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
211.239.X.59	13/Nov/2006:19:59:28	GET /phorum/bb_usage_stats/include/bb_usage_stats.php?phpbb_root_path=http://www.tunts.com.br/wmp/tk.txt? HTTP/1.1	[11]	forum.golem.de
84.191.X.175	14/Nov/2006:03:14:34	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
84.191.X.175	14/Nov/2006:03:19:35	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
66.194.X.70	14/Nov/2006:05:48:03	GET / HTTP/1.1	[12]	golem.de.com
195.10.X.196	14/Nov/2006:11:01:02	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
195.10.X.196	14/Nov/2006:12:00:53	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de

80.134.X.42	15/Nov/2006:01:28:18	GET / HTTP/1.1	[8]	www.golem.de.com
80.134.X.42	15/Nov/2006:01:28:18	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
80.134.X.42	15/Nov/2006:01:28:18	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
80.134.X.42	15/Nov/2006:01:58:11	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
217.173.X.3	15/Nov/2006:02:44:03	GET / HTTP/1.1	[13]	www.golem.de.com
217.173.X.3	15/Nov/2006:02:44:03	GET /favicon.ico HTTP/1.1	[13]	www.golem.de.com
84.191.X.114	15/Nov/2006:02:59:42	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
66.194.X.73	15/Nov/2006:08:03:06	GET / HTTP/1.1	[14]	golem.de.com
64.242.X.60	15/Nov/2006:09:46:13	GET /0601/42733.html HTTP/1.1	[15]	www.golem.de
64.242.X.60	15/Nov/2006:09:55:04	GET /0604/44772.html HTTP/1.1	[15]	www.golem.de
64.242.X.60	15/Nov/2006:10:01:05	GET /0501/35591.html HTTP/1.1	[15]	www.golem.de
212.87.X.182	15/Nov/2006:10:03:00	GET / HTTP/1.1	[16]	www.golem.de.com
195.10.X.196	15/Nov/2006:17:30:58	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
87.160.X.156	16/Nov/2006:02:58:56	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.156	16/Nov/2006:03:03:58	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.156	16/Nov/2006:03:08:59	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
195.10.X.196	16/Nov/2006:04:00:59	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
64.242.X.60	16/Nov/2006:08:52:34	GET /print.php?a=40956 HTTP/1.1	[15]	www.golem.de
64.242.X.60	16/Nov/2006:08:58:00	GET /0605/45292.html HTTP/1.1	[15]	www.golem.de
66.194.X.75	16/Nov/2006:09:59:31	GET / HTTP/1.1	[17]	golem.de.com
87.160.X.111	17/Nov/2006:03:05:45	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
213.199.X.149	17/Nov/2006:09:41:21	GET / HTTP/1.1	[18]	www.golem.de.com
213.199.X.149	17/Nov/2006:09:41:22	GET /favicon.ico HTTP/1.1	[18]	www.golem.de.com
66.194.X.72	17/Nov/2006:12:53:37	GET / HTTP/1.1	[19]	golem.de.com
195.10.X.196	17/Nov/2006:13:31:04	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
195.158.X.4	18/Nov/2006:14:58:25	GET / HTTP/1.1	[20]	www.golem.de.com
195.158.X.4	18/Nov/2006:14:58:25	GET /favicon.ico HTTP/1.1	[20]	www.golem.de.com
66.194.X.80	18/Nov/2006:16:13:58	GET / HTTP/1.1	[7]	golem.de.com
66.194.X.75	19/Nov/2006:22:56:04	GET / HTTP/1.1	[21]	golem.de.com
141.113.X.22	20/Nov/2006:02:06:24	GET / HTTP/1.1	[22]	www.golem.de.com
141.113.X.22	20/Nov/2006:02:06:25	GET /favicon.ico HTTP/1.1	[22]	www.golem.de.com
87.160.X.33	20/Nov/2006:02:49:23	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
80.136.X.185	20/Nov/2006:07:46:20	GET / HTTP/1.1	[8]	www.golem.de.com
80.136.X.185	20/Nov/2006:07:46:20	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
80.135.X.133	21/Nov/2006:01:17:24	GET / HTTP/1.1	[23]	www.golem.de.com
87.160.X.13	21/Nov/2006:03:02:39	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.13	21/Nov/2006:03:07:41	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.13	21/Nov/2006:03:12:42	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.13	21/Nov/2006:03:17:43	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.13	21/Nov/2006:03:22:44	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.13	21/Nov/2006:03:27:45	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
84.19.X.98	21/Nov/2006:06:27:06	GET / HTTP/1.1	[20]	www.markt.golem.de.com
84.19.X.98	21/Nov/2006:06:27:06	GET /favicon.ico HTTP/1.1	[20]	www.markt.golem.de.com
84.19.X.98	21/Nov/2006:06:27:08	GET /favicon.ico HTTP/1.1	[20]	www.markt.golem.de.com
66.194.X.79	21/Nov/2006:11:32:43	GET / HTTP/1.1	[24]	golem.de.com
87.160.X.102	22/Nov/2006:02:39:59	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de

87.160.X.102	22/Nov/2006:02:45:01	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.102	22/Nov/2006:02:50:02	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.102	22/Nov/2006:02:55:03	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.91	22/Nov/2006:05:17:03	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
62.2.X.78	22/Nov/2006:13:33:12	GET / HTTP/1.1	[8]	www.golem.de.com
84.135.X.2	22/Nov/2006:15:25:34	GET / HTTP/1.1	[25]	www.golem.de.com
84.135.X.2	22/Nov/2006:15:25:35	GET /favicon.ico HTTP/1.1	[25]	www.golem.de.com
213.39.X.243	22/Nov/2006:16:33:53	GET / HTTP/1.1	[20]	www.golem.de.com
213.39.X.243	22/Nov/2006:16:33:53	GET /favicon.ico HTTP/1.1	[20]	www.golem.de.com
213.39.X.243	22/Nov/2006:16:34:03	GET /favicon.ico HTTP/1.1	[20]	www.golem.de.com
66.194.X.75	22/Nov/2006:22:39:46	GET / HTTP/1.1	[26]	golem.de.com
82.135.X.132	24/Nov/2006:06:47:23	GET / HTTP/1.1	[8]	www.golem.de.com
82.135.X.132	24/Nov/2006:06:47:23	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
82.135.X.132	24/Nov/2006:06:47:23	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
82.135.X.132	24/Nov/2006:06:47:23	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
66.194.X.70	24/Nov/2006:09:56:15	GET / HTTP/1.1	[7]	golem.de.com
66.194.X.67	25/Nov/2006:22:11:01	GET / HTTP/1.1	[27]	golem.de.com
84.57.X.175	26/Nov/2006:07:56:49	GET / HTTP/1.1	[2]	golem.de.com
195.10.X.196	26/Nov/2006:10:50:42	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
195.10.X.196	26/Nov/2006:11:35:43	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
195.10.X.196	26/Nov/2006:16:20:48	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
87.160.X.137	27/Nov/2006:02:47:09	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
195.10.X.196	27/Nov/2006:03:50:49	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
195.10.X.196	27/Nov/2006:04:10:49	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
195.10.X.196	27/Nov/2006:04:25:41	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
195.10.X.196	27/Nov/2006:04:35:37	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
80.142.X.244	27/Nov/2006:07:48:38	GET / HTTP/1.1	[28]	www.golem.de.com
80.142.X.244	27/Nov/2006:07:48:38	GET /favicon.ico HTTP/1.1	[28]	www.golem.de.com
66.194.X.77	27/Nov/2006:09:34:30	GET / HTTP/1.1	[29]	golem.de.com
195.10.X.196	27/Nov/2006:10:55:42	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
87.160.X.50	28/Nov/2006:02:56:39	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
87.160.X.50	28/Nov/2006:03:09:23	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
62.153.X.138	28/Nov/2006:07:21:26	GET / HTTP/1.0	[8]	www.golem.de.com
62.153.X.138	28/Nov/2006:07:21:26	GET /favicon.ico HTTP/1.0	[8]	www.golem.de.com
84.146.X.37	28/Nov/2006:10:17:36	GET /0611/49148.html HTTP/1.1	[8]	www.golem.de.com
84.146.X.37	28/Nov/2006:10:17:37	GET /favicon.ico HTTP/1.1	[8]	www.golem.de.com
202.11.X.250	28/Nov/2006:10:24:14	GET / HTTP/1.1	[30]	golem.de.com
194.15.X.76	28/Nov/2006:10:24:28	GET / HTTP/1.1	[31]	www.golem.de.com
194.15.X.76	28/Nov/2006:10:24:32	GET /favicon.ico HTTP/1.1	[31]	www.golem.de.com
84.56.X.189	28/Nov/2006:13:12:59	GET / HTTP/1.1	[2]	golem.de.com
77.181.X.52	28/Nov/2006:16:59:07	GET / HTTP/1.1	[20]	www.golem.de.com
77.181.X.52	28/Nov/2006:16:59:07	GET /favicon.ico HTTP/1.1	[20]	www.golem.de.com
66.194.X.68	28/Nov/2006:21:22:20	GET / HTTP/1.1	[32]	golem.de.com
87.160.X.119	29/Nov/2006:02:54:50	GET /rss.php?tp=sec&feed=RSS1.0 HTTP/1.0	[9]	www.golem.de
62.245.X.62	29/Nov/2006:04:35:55	GET / HTTP/1.1	[20]	www.golem.de.com
62.245.X.62	29/Nov/2006:04:35:55	GET /favicon.ico HTTP/1.1	[20]	www.golem.de.com

195.243.X.34	29/Nov/2006:07:06:40	GET / HTTP/1.0	[33]	www.golem.de.com
195.243.X.34	29/Nov/2006:07:06:41	GET /favicon.ico HTTP/1.0	[33]	www.golem.de.com
66.194.X.71	30/Nov/2006:09:01:57	GET / HTTP/1.1	[24]	golem.de.com
195.10.X.196	30/Nov/2006:15:15:47	GET /rss.php?feed=ATOM0.3 HTTP/1.0	[9]	rss.golem.de
222.152.X.87	24/Nov/2006:13:56:14	GET / HTTP/1.1	[34]	daum.net.nz
140.126.X.45	10/Nov/2006:01:00:45	GET / HTTP/1.1	[35]	www.flurl.com.tw
59.120.X.128	10/Nov/2006:01:18:20	GET / HTTP/1.1	[35]	www.flurl.com.tw
58.169.X.140	10/Nov/2006:08:13:56	GET / HTTP/1.1	[34]	www.flurl.com.tw
59.113.X.253	10/Nov/2006:13:23:01	GET / HTTP/1.1	[36]	www.flurl.com.tw
59.104.X.231	10/Nov/2006:19:36:52	GET / HTTP/1.1	[37]	www.flurl.com.tw
59.104.X.231	10/Nov/2006:19:36:53	GET /favicon.ico HTTP/1.1	[9]	www.flurl.com.tw
220.130.X.187	11/Nov/2006:00:01:51	GET / HTTP/1.1	[38]	www.flurl.com.tw
220.140.X.18	11/Nov/2006:01:02:36	GET / HTTP/1.1	[39]	www.flurl.com.tw
220.140.X.18	11/Nov/2006:01:02:38	GET /favicon.ico HTTP/1.1	[39]	www.flurl.com.tw
125.228.X.207	11/Nov/2006:06:09:06	GET /item/wmv_u_194268 HTTP/1.1	[34]	www.flurl.com.tw
125.228.X.207	11/Nov/2006:06:09:06	GET /favicon.ico HTTP/1.1	[34]	www.flurl.com.tw
125.228.X.207	11/Nov/2006:06:09:07	GET /favicon.ico HTTP/1.1	[34]	www.flurl.com.tw
218.161.X.223	11/Nov/2006:06:58:50	GET / HTTP/1.1	[40]	www.flurl.com.tw
218.168.X.121	11/Nov/2006:10:33:01	GET / HTTP/1.1	[41]	www.flurl.com.tw
220.137.X.102	11/Nov/2006:11:06:57	GET / HTTP/1.1	[40]	www.flurl.com.tw
220.143.X.177	11/Nov/2006:12:24:45	GET / HTTP/1.1	[41]	www.flurl.com.tw
210.200.X.228	11/Nov/2006:13:38:59	GET / HTTP/1.1	[42]	www.flurl.com.tw
218.166.X.23	12/Nov/2006:04:14:03	GET / HTTP/1.1	[41]	www.flurl.com.tw
218.160.X.20	12/Nov/2006:06:15:50	GET / HTTP/1.1	[43]	www.flurl.com.tw
218.160.X.20	12/Nov/2006:06:15:51	GET /favicon.ico HTTP/1.1	[43]	www.flurl.com.tw
61.223.X.197	12/Nov/2006:07:40:20	GET / HTTP/1.1	[44]	www.flurl.com.tw
219.79.X.180	12/Nov/2006:09:51:32	GET / HTTP/1.1	[40]	www.flurl.com.tw
218.168.X.7	12/Nov/2006:14:33:56	GET /item/Kliederen_met_verf_u_201985 HTTP/1.1	[40]	www.flurl.com.tw
218.168.X.7	12/Nov/2006:14:33:56	GET /favicon.ico HTTP/1.1	[40]	www.flurl.com.tw
59.105.X.163	12/Nov/2006:19:27:38	GET / HTTP/1.1	[45]	www.flurl.com.tw
210.200.X.227	12/Nov/2006:21:27:44	GET / HTTP/1.0	[40]	www.flurl.com.tw
59.112.X.102	13/Nov/2006:03:05:14	GET / HTTP/1.1	[46]	www.flurl.com.tw
210.6.X.76	13/Nov/2006:06:00:18	GET / HTTP/1.1	[23]	www.flurl.com.tw
140.128.X.111	13/Nov/2006:06:50:41	GET / HTTP/1.1	[47]	www.flurl.com.tw
163.19.X.54	13/Nov/2006:10:36:51	GET / HTTP/1.1	[23]	www.flurl.com.tw
61.59.X.152	13/Nov/2006:11:46:30	GET / HTTP/1.1	[48]	www.flurl.com.tw
125.233.X.146	13/Nov/2006:12:46:34	GET / HTTP/1.1	[40]	www.flurl.com.tw
59.113.X.179	13/Nov/2006:14:03:14	GET / HTTP/1.1	[36]	www.flurl.com.tw
59.115.X.202	13/Nov/2006:14:35:22	GET /showthread.php?t=1119 HTTP/1.1	[23]	forums.flurl.com
59.115.X.202	13/Nov/2006:14:35:24	GET /showthread.php?t=1119 HTTP/1.1	[23]	forums.flurl.com
59.115.X.202	13/Nov/2006:14:35:28	GET /showthread.php?t=1119 HTTP/1.1	[23]	forums.flurl.com
59.115.X.202	13/Nov/2006:14:35:30	GET /showthread.php?t=1119 HTTP/1.1	[23]	forums.flurl.com
211.75.X.144	14/Nov/2006:01:32:21	GET / HTTP/1.1	[23]	flurl.com.tw
220.133.X.92	14/Nov/2006:05:19:49	GET / HTTP/1.1	[49]	www.flurl.com.tw
59.116.X.164	14/Nov/2006:08:33:19	GET / HTTP/1.1	[50]	www.flurl.com.tw
218.169.X.112	14/Nov/2006:09:13:12	GET / HTTP/1.1	[51]	www.flurl.com.tw
218.169.X.112	14/Nov/2006:09:13:13	GET /favicon.ico HTTP/1.1	[51]	www.flurl.com.tw
218.169.X.112	14/Nov/2006:09:13:22	GET / HTTP/1.1	[51]	www.flurl.com.tw
61.228.X.59	14/Nov/2006:12:51:59	GET / HTTP/1.1	[52]	www.flurl.com.tw
61.228.X.59	14/Nov/2006:12:52:00	GET /favicon.ico HTTP/1.1	[52]	www.flurl.com.tw
218.167.X.252	14/Nov/2006:14:18:31	GET / HTTP/1.1	[53]	www.flurl.com.tw
125.233.X.100	14/Nov/2006:22:43:29	GET / HTTP/1.1	[54]	www.flurl.com.tw
60.248.X.115	15/Nov/2006:00:27:12	GET / HTTP/1.1	[47]	www.flurl.com.tw
202.42.X.194	15/Nov/2006:02:56:03	GET / HTTP/1.1	[40]	www.flurl.com.tw

```
61.230.X.112    15/Nov/2006:04:29:04   GET / HTTP/1.1                [23]   www.flurl.com.tw
61.224.X.167    15/Nov/2006:08:38:48   GET / HTTP/1.1                [55]   www.flurl.com.tw
61.224.X.167    15/Nov/2006:08:38:49   GET /favicon.ico HTTP/1.1     [55]   www.flurl.com.tw
61.224.X.167    15/Nov/2006:08:38:49   GET /favicon.ico HTTP/1.1     [55]   www.flurl.com.tw
61.224.X.167    15/Nov/2006:08:40:33   GET / HTTP/1.1                [55]   www.flurl.com.tw
201.253.X.246   15/Nov/2006:10:31:57   GET / HTTP/1.1                [36]   www.flurl.com.tw
66.249.X.161    15/Nov/2006:11:09:01   GET /robots.txt HTTP/1.1      [56]   www.flurl.com.tw
66.249.X.161    15/Nov/2006:11:09:01   GET / HTTP/1.1                [56]   www.flurl.com.tw
61.58.X.156     15/Nov/2006:16:38:52   GET / HTTP/1.1                [23]   www.flurl.com.tw
218.164.X.158   15/Nov/2006:22:34:15   GET / HTTP/1.1                [57]   www.flurl.com.tw
59.120.X.205    15/Nov/2006:23:32:54   GET / HTTP/1.1                [34]   www.flurl
59.120.X.205    15/Nov/2006:23:33:05   GET / HTTP/1.1                [34]   flurl
59.112.X.105    16/Nov/2006:04:13:13   GET / HTTP/1.1                [23]   www.flurl.com.tw
59.112.X.105    16/Nov/2006:04:13:15   GET /favicon.ico HTTP/1.1     [58]   www.flurl.com.tw
124.8.X.34      16/Nov/2006:10:26:25   GET / HTTP/1.1                [34]   www.flurl.com.tw
124.8.X.34      16/Nov/2006:10:26:26   GET /favicon.ico HTTP/1.1     [34]   www.flurl.com.tw
124.8.X.34      16/Nov/2006:10:26:26   GET /favicon.ico HTTP/1.1     [34]   www.flurl.com.tw
210.200.X.226   16/Nov/2006:12:25:14   GET / HTTP/1.0                [47]   www.flurl.com.tw
61.229.X.205    17/Nov/2006:03:27:19   GET / HTTP/1.1                [35]   flurl.com.tw
61.229.X.205    17/Nov/2006:03:27:27   GET / HTTP/1.1                [35]   www.flurl.com.tw
220.137.X.54    17/Nov/2006:04:46:16   GET / HTTP/1.1                [36]   www.flurl.com.tw
163.15.X.31     17/Nov/2006:11:46:48   GET / HTTP/1.0                [40]   www.flurl.com.tw
163.15.X.31     17/Nov/2006:11:46:49   GET / HTTP/1.0                [40]   www.flurl.com.tw
220.131.X.70    17/Nov/2006:12:04:01   GET / HTTP/1.0                [40]   www.flurl.com.tw
220.131.X.70    17/Nov/2006:12:04:02   GET /favicon.ico HTTP/1.0     [40]   www.flurl.com.tw
61.223.X.113    17/Nov/2006:16:35:47   GET / HTTP/1.1                [23]   www.flurl.com.tw
59.112.X.238    17/Nov/2006:19:03:04   GET / HTTP/1.1                [40]   www.flurl.com.tw
59.112.X.238    17/Nov/2006:19:03:04   GET /favicon.ico HTTP/1.1     [40]   www.flurl.com.tw
61.228.X.84     17/Nov/2006:19:42:59   GET / HTTP/1.1                [23]   www.flurl.com.tw
218.172.X.224   17/Nov/2006:20:29:00   GET / HTTP/1.1                [40]   www.flurl.com.tw
220.136.X.169   17/Nov/2006:22:37:23   GET / HTTP/1.1                [59]   www.flurl.com.tw
220.136.X.169   17/Nov/2006:22:37:23   GET /favicon.ico HTTP/1.1     [59]   www.flurl.com.tw
220.136.X.169   17/Nov/2006:22:37:24   GET /favicon.ico HTTP/1.1     [59]   www.flurl.com.tw
203.75.X.63     18/Nov/2006:06:11:15   GET / HTTP/1.1                [39]   www.flurl.com.tw
219.68.X.250    18/Nov/2006:06:33:43   GET / HTTP/1.1                [47]   www.flurl.com.tw
218.168.X.215   18/Nov/2006:07:18:12   GET / HTTP/1.1                [23]   www.flurl.com.tw
220.141.X.235   18/Nov/2006:09:23:14   GET / HTTP/1.1                [40]   www.flurl.com.tw
218.162.X.221   18/Nov/2006:12:14:26   GET / HTTP/1.1                [34]   www.flurl.com.tw
140.138.X.110   18/Nov/2006:12:26:50   GET / HTTP/1.0                [60]   www.flurl.com.tw
140.138.X.10    18/Nov/2006:12:26:51   GET /favicon.ico HTTP/1.0     [60]   www.flurl.com.tw
140.138.X.110   18/Nov/2006:12:26:51   GET /favicon.ico HTTP/1.0     [60]   www.flurl.com.tw
140.138.X.110   18/Nov/2006:12:26:51   GET /favicon.ico HTTP/1.0     [60]   www.flurl.com.tw
210.192.X.200   18/Nov/2006:18:15:19   GET / HTTP/1.1                [1]    www.flurl.com.tw
61.223.X.143    18/Nov/2006:18:17:17   GET / HTTP/1.1                [44]   www.flurl.com.tw
220.134.X.208   18/Nov/2006:19:48:13   GET / HTTP/1.1                [43]   www.flurl.com.tw
220.134.X.208   18/Nov/2006:19:48:14   GET /favicon.ico HTTP/1.1     [43]   www.flurl.com.tw
219.69.X.35     18/Nov/2006:20:15:17   GET / HTTP/1.1                [34]   www.flurl.com.tw
218.172.X.158   18/Nov/2006:21:50:38   GET / HTTP/1.1                [40]   www.flurl.com.tw
218.172.X.158   18/Nov/2006:21:50:40   GET /favicon.ico HTTP/1.1     [40]   www.flurl.com.tw
218.170.X.189   18/Nov/2006:23:51:15   GET / HTTP/1.1                [61]   www.flurl.com.tw
218.170.X.189   18/Nov/2006:23:51:16   GET /favicon.ico HTTP/1.1     [58]   www.flurl.com.tw
60.248.X.131    19/Nov/2006:00:47:27   GET / HTTP/1.1                [1]    flurl
218.168.X.145   19/Nov/2006:01:25:13   GET / HTTP/1.1                [43]   www.flurl.com.tw
218.164.X.32    19/Nov/2006:01:55:09   GET / HTTP/1.1                [40]   www.flurl.com.tw
61.225.X.207    19/Nov/2006:01:59:48   GET / HTTP/1.1                [62]   www.flurl.com.tw
61.225.X.207    19/Nov/2006:01:59:48   GET /favicon.ico HTTP/1.1     [62]   www.flurl.com.tw
61.225.X.207    19/Nov/2006:01:59:49   GET /favicon.ico HTTP/1.1     [62]   www.flurl.com.tw
61.225.X.207    19/Nov/2006:01:59:49   GET /favicon.ico HTTP/1.1     [62]   www.flurl.com.tw
59.113.X.198    19/Nov/2006:03:08:18   GET / HTTP/1.1                [40]   www.flurl.com.tw
124.8.X.156     19/Nov/2006:04:26:21   GET / HTTP/1.1                [23]   www.flurl.com.tw
220.131.X.47    19/Nov/2006:05:08:58   GET / HTTP/1.1                [40]   www.flurl.com.tw
61.231.X.121    19/Nov/2006:05:22:45   GET / HTTP/1.1                [23]   www.flurl.com.tw
```

```
61.231.X.121    19/Nov/2006:05:22:46   GET /favicon.ico HTTP/1.1             [23]   www.flurl.com.tw
61.58.X.156     19/Nov/2006:15:11:58   GET / HTTP/1.1                        [23]   www.flurl.com.tw
66.249.X.7      19/Nov/2006:17:12:07   GET /robots.txt HTTP/1.1              [56]   www.flurl.com.tw
66.249.X.7      19/Nov/2006:17:12:07   GET / HTTP/1.1                        [56]   www.flurl.com.tw
140.118.X.246   19/Nov/2006:20:50:33   GET / HTTP/1.1                        [63]   www.flurl.com.tw
60.52.X.248     19/Nov/2006:21:15:40   GET / HTTP/1.1                        [64]   www.flurl.com.tw
60.52.X.248     19/Nov/2006:21:15:41   GET /favicon.ico HTTP/1.1             [64]   www.flurl.com.tw
210.208.X.230   19/Nov/2006:21:51:48   GET / HTTP/1.1                        [40]   www.flurl.com.tw
163.23.X.62     19/Nov/2006:22:03:51   GET / HTTP/1.1                        [65]   www.flurl.com.tw
75.11.X.160     19/Nov/2006:22:21:46   GET / HTTP/1.1                        [41]   www.flurl.com.tw
71.249.X.99     19/Nov/2006:22:46:56   GET / HTTP/1.1                        [40]   www.flurl.com.tw
218.162.X.160   20/Nov/2006:01:21:23   GET / HTTP/1.1                        [40]   www.flurl.com.tw
218.166.X.139   20/Nov/2006:04:53:33   GET / HTTP/1.1                        [1]    www.flurl.com.tw
125.231.X.220   20/Nov/2006:05:00:34   GET / HTTP/1.1                        [23]   www.flurl.com.tw
125.231.X.220   20/Nov/2006:05:02:54   GET / HTTP/1.1                        [23]   www.flurl.com.tw
61.221.X.76     20/Nov/2006:06:24:33   GET / HTTP/1.1                        [61]   flurl.com.tw
61.221.X.76     20/Nov/2006:06:44:17   GET / HTTP/1.1                        [61]   www.flurl.com.tw
218.210.X.131   20/Nov/2006:20:30:27   GET / HTTP/1.1                        [35]   www.flurl.com.tw
60.49.X.145     20/Nov/2006:22:41:53   GET / HTTP/1.1                        [34]   www.flurl.com.tw
                                       GET /item/wmv_u_150266
163.21.X.253    21/Nov/2006:02:46:21   HTTP/1.1                              [1]    www.flurl.com.tw
163.21.X.253    21/Nov/2006:02:46:30   GET /item/ HTTP/1.1                   [1]    www.flurl.com.tw
220.137.X.156   21/Nov/2006:04:35:18   GET / HTTP/1.1                        [36]   www.flurl.com.tw
125.231.X.203   21/Nov/2006:05:23:19   GET / HTTP/1.1                        [23]   www.flurl.com.tw
222.166.X.189   21/Nov/2006:06:19:01   GET / HTTP/1.1                        [66]   www.flurl.com.tw
222.166.X.189   21/Nov/2006:06:19:02   GET /favicon.ico HTTP/1.1             [66]   www.flurl.com.tw
220.142.X.13    21/Nov/2006:08:23:06   GET / HTTP/1.1                        [67]   www.flurl.com.tw
220.142.X.13    21/Nov/2006:08:23:06   GET /favicon.ico HTTP/1.1             [67]   www.flurl.com.tw
125.232.X.81    21/Nov/2006:16:35:58   GET / HTTP/1.1                        [39]   www.flurl.com.tw
163.27.X.251    22/Nov/2006:01:29:55   GET / HTTP/1.1                        [68]   www.flurl.com.tw
163.27.X.251    22/Nov/2006:01:29:57   GET /favicon.ico HTTP/1.1             [58]   www.flurl.com.tw
59.124.X.52     22/Nov/2006:03:32:47   GET / HTTP/1.1                        [69]   www.flurl.com.tw
59.124.X.52     22/Nov/2006:03:32:48   GET /favicon.ico HTTP/1.1             [69]   www.flurl.com.tw
59.117.X.183    22/Nov/2006:06:42:35   GET / HTTP/1.1                        [34]   www.flurl.com.tw
61.229.X.182    22/Nov/2006:07:35:22   GET / HTTP/1.1                        [34]   www.flurl.com.tw
61.229.X.182    22/Nov/2006:07:35:24   GET /favicon.ico HTTP/1.1             [34]   www.flurl.com.tw
220.142.X.139   22/Nov/2006:09:27:42   GET / HTTP/1.1                        [67]   www.flurl.com.tw
220.142.X.139   22/Nov/2006:09:27:43   GET /favicon.ico HTTP/1.1             [67]   www.flurl.com.tw
137.132.X.11    22/Nov/2006:12:52:14   GET / HTTP/1.1                        [23]   www.flurl.com.tw
61.64.X.211     22/Nov/2006:14:05:38   GET / HTTP/1.1                        [70]   www.flurl.com.tw
59.114.X.109    23/Nov/2006:00:32:33   GET / HTTP/1.1                        [71]   www.flurl.com.tw
                                       GET /item/wmv_u_19782
61.57.X.249     23/Nov/2006:04:46:16   HTTP/1.1                              [72]   www.flurl
220.143.X.130   23/Nov/2006:05:40:53   GET / HTTP/1.1                        [40]   www.flurl.com.tw
218.163.X.166   23/Nov/2006:09:25:15   GET / HTTP/1.1                        [46]   www.flurl.com.tw
210.200.X.228   23/Nov/2006:12:14:01   GET / HTTP/1.1                        [73]   www.flurl.com.tw
                                       GET
                                       /item/mr_lung_film_1612_u_15840
218.170.X.158   23/Nov/2006:14:24:44   7 HTTP/1.1                            [34]   www.flurl.com.tw
218.170.X.158   23/Nov/2006:14:24:47   GET / HTTP/1.1                        [34]   www.flurl.com.tw
218.170.X.158   23/Nov/2006:14:28:40   GET / HTTP/1.1                        [34]   www.flurl.com.tw
61.225.X.49     23/Nov/2006:21:54:07   GET / HTTP/1.1                        [23]   www.flurl.com.tw
59.120.X.205    23/Nov/2006:23:25:17   GET / HTTP/1.1                        [23]   flurl
218.166.X.199   24/Nov/2006:02:49:20   GET / HTTP/1.1                        [1]    www.flurl.com.tw
59.117.X.204    24/Nov/2006:07:59:47   GET / HTTP/1.1                        [40]   www.flurl.com.tw
66.249.X.7      24/Nov/2006:11:11:39   GET /robots.txt HTTP/1.1              [56]   www.flurl.com.tw
66.249.X.7      24/Nov/2006:11:11:39   GET / HTTP/1.1                        [56]   www.flurl.com.tw
59.112.X.48     24/Nov/2006:19:33:03   GET / HTTP/1.1                        [23]   www.flurl.com.tw
59.112.X.48     24/Nov/2006:19:33:04   GET /favicon.ico HTTP/1.1             [23]   www.flurl.com.tw
59.112.X.48     24/Nov/2006:19:33:07   GET / HTTP/1.1                        [23]   www.flurl.com.tw
220.139.X.243   24/Nov/2006:22:11:35   GET / HTTP/1.1                        [74]   www.flurl.com.tw
124.8.X.11      25/Nov/2006:03:55:36   GET / HTTP/1.1                        [23]   www.flurl.com.tw
```

```
59.117.X.58     25/Nov/2006:08:58:07   GET / HTTP/1.1                       [75]   www.flurl.com.tw
60.50.X.155     25/Nov/2006:11:14:23   GET / HTTP/1.1                       [23]   www.flurl.com.tw
210.200.X.228   25/Nov/2006:11:27:40   GET / HTTP/1.1                       [76]   www.flurl.com.tw
210.200.X.228   25/Nov/2006:11:33:37   GET / HTTP/1.1                       [76]   www.flurl.com.tw
210.200.X.228   25/Nov/2006:11:43:41   GET / HTTP/1.1                       [76]   www.flurl.com.tw
210.200.X.228   25/Nov/2006:12:01:43   GET / HTTP/1.1                       [76]   www.flurl.com.tw
210.200.X.228   25/Nov/2006:12:35:58   GET / HTTP/1.1                       [76]   www.flurl.com.tw
66.180.X.88     25/Nov/2006:14:04:13   GET / HTTP/1.1                       [77]   www.flurl.com.tw
210.64.X.12     25/Nov/2006:14:04:13   GET / HTTP/1.1                       [23]   www.flurl.com.tw
210.200.X.228   25/Nov/2006:16:47:15   GET / HTTP/1.1                       [76]   www.flurl.com.tw
210.200.X.228   25/Nov/2006:20:19:33   GET / HTTP/1.1                       [76]   www.flurl.com.tw
220.142.X.83    25/Nov/2006:20:36:43   GET / HTTP/1.1                       [40]   www.flurl.com.tw
220.142.X.83    25/Nov/2006:20:36:43   GET /favicon.ico HTTP/1.1            [40]   www.flurl.com.tw
210.64.X.53     26/Nov/2006:00:22:36   GET / HTTP/1.1                       [23]   www.flurl.com.tw
220.140.X.87    26/Nov/2006:02:11:05   GET / HTTP/1.1                       [78]   www.flurl.com.tw
220.140.X.87    26/Nov/2006:02:11:07   GET /favicon.ico HTTP/1.1            [78]   www.flurl.com.tw
210.200.X.228   26/Nov/2006:03:31:04   GET / HTTP/1.1                       [76]   www.flurl.com.tw
220.229.X.19    26/Nov/2006:04:29:30   GET / HTTP/1.1                       [23]   www.flurl.com.tw
210.200.X.227   26/Nov/2006:05:44:32   GET / HTTP/1.0                       [79]   www.flurl.com.tw
58.214.X.218    26/Nov/2006:07:49:32   GET / HTTP/1.1                       [23]   www.flurl.com.tw
220.229.X.19    26/Nov/2006:08:13:42   GET / HTTP/1.1                       [23]   www.flurl.com.tw
219.68.X.137    26/Nov/2006:10:12:21   GET / HTTP/1.1                       [47]   www.flurl.com.tw
59.105.X.22     26/Nov/2006:10:31:21   GET / HTTP/1.1                       [23]   www.flurl.com.tw
                                       GET
                                       /item/Bali_Rodriguez_photo_shoot_
61.70.X.118     26/Nov/2006:10:52:50   u_205942 HTTP/1.1                    [47]   www.flurl.com.tw
210.200.X.228   26/Nov/2006:12:53:09   GET / HTTP/1.1                       [76]   www.flurl.com.tw
61.221.X.91     26/Nov/2006:22:05:37   GET / HTTP/1.1                       [35]   www.flurl.com.tw
61.221.X.91     26/Nov/2006:22:09:51   GET / HTTP/1.1                       [35]   www.flurl.com.tw
61.221.X.91     26/Nov/2006:22:13:01   GET / HTTP/1.1                       [35]   www.flurl.com.tw
61.221.X.91     26/Nov/2006:22:14:32   GET / HTTP/1.1                       [35]   www.flurl.com.tw
61.221.X.91     26/Nov/2006:22:15:12   GET / HTTP/1.1                       [35]   www.flurl.com.tw
61.221.X.91     26/Nov/2006:22:16:06   GET / HTTP/1.1                       [35]   www.flurl.com.tw
61.221.X.91     26/Nov/2006:22:16:52   GET / HTTP/1.1                       [35]   www.flurl.com.tw
61.221.X.91     26/Nov/2006:22:17:36   GET / HTTP/1.1                       [35]   www.flurl.com.tw
61.221.X.91     26/Nov/2006:22:18:15   GET / HTTP/1.1                       [35]   www.flurl.com.tw
59.126.X.228    26/Nov/2006:22:59:18   GET / HTTP/1.1                       [23]   www.flurl.com.tw
59.120.X.205    26/Nov/2006:23:19:25   GET / HTTP/1.1                       [23]   flurl
61.229.X.228    27/Nov/2006:00:48:56   GET / HTTP/1.1                       [43]   tw.flurl.com.tw
124.155.X.214   27/Nov/2006:00:50:12   GET / HTTP/1.1                       [47]   www.flurl.com.tw
124.155.X.214   27/Nov/2006:00:50:12   GET /favicon.ico HTTP/1.1            [47]   www.flurl.com.tw
124.155.X.214   27/Nov/2006:00:50:12   GET /favicon.ico HTTP/1.1            [47]   www.flurl.com.tw
71.80.X.62      27/Nov/2006:01:09:11   GET / HTTP/1.1                       [1]    www.flurl.com.tw
125.231.X.253   27/Nov/2006:04:39:21   GET / HTTP/1.1                       [23]   flurl.com.tw
125.231.X.253   27/Nov/2006:04:39:58   GET / HTTP/1.1                       [23]   www.flurl.com.tw
125.231.X.253   27/Nov/2006:04:56:06   GET / HTTP/1.1                       [23]   www.flurl.com.tw
220.134.X.208   27/Nov/2006:05:45:56   GET / HTTP/1.1                       [43]   www.flurl.com.tw
220.134.X.208   27/Nov/2006:05:45:56   GET /favicon.ico HTTP/1.1            [43]   www.flurl.com.tw
61.216.X.158    27/Nov/2006:09:34:32   GET / HTTP/1.1                       [80]   www.flurl.com.tw
61.216.X.158    27/Nov/2006:10:09:02   GET / HTTP/1.1                       [80]   www.flurl.com.tw
219.81.X.162    27/Nov/2006:11:10:51   GET / HTTP/1.1                       [40]   www.flurl.com.tw
219.81.X.162    27/Nov/2006:11:10:52   GET /favicon.ico HTTP/1.1            [40]   www.flurl.com.tw
219.81.X.162    27/Nov/2006:11:10:52   GET /favicon.ico HTTP/1.1            [40]   www.flurl.com.tw
219.81.X.162    27/Nov/2006:11:10:52   GET /favicon.ico HTTP/1.1            [40]   www.flurl.com.tw
59.120.X.205    27/Nov/2006:23:18:25   GET / HTTP/1.1                       [23]   flurl
61.217.X.102    28/Nov/2006:01:33:47   GET / HTTP/1.1                       [81]   www.flurl.com.tw
210.200.X.228   28/Nov/2006:10:40:22   GET / HTTP/1.1                       [76]   www.flurl.com.tw
24.83.X.131     28/Nov/2006:22:46:47   GET / HTTP/1.1                       [59]   www.flurl.com.tw
24.83.X.131     28/Nov/2006:22:46:47   GET /favicon.ico HTTP/1.1            [59]   www.flurl.com.tw
203.186.X.70    29/Nov/2006:04:48:02   GET / HTTP/1.1                       [82]   www.flurl.com.tw
218.163.X.119   29/Nov/2006:07:12:37   GET / HTTP/1.1                       [23]   www.flurl.com.tw
218.168.X.193   29/Nov/2006:07:14:01   GET / HTTP/1.1                       [40]   www.flurl.com.tw
```

218.175.X.173	29/Nov/2006:08:30:57	GET / HTTP/1.1	[67]	www.flurl.com.tw
218.175.X.173	29/Nov/2006:08:30:58	GET /favicon.ico HTTP/1.1	[67]	www.flurl.com.tw
59.115.X.116	29/Nov/2006:11:53:39	GET / HTTP/1.1	[83]	www.flurl.com.tw
220.134.X.208	29/Nov/2006:12:03:47	GET / HTTP/1.1	[43]	www.flurl.com.tw
220.142.X.163	29/Nov/2006:21:40:56	GET / HTTP/1.1	[40]	www.flurl.com.tw
220.142.X.163	29/Nov/2006:21:40:56	GET /favicon.ico HTTP/1.1	[40]	www.flurl.com.tw
125.232.X.116	30/Nov/2006:02:15:13	GET / HTTP/1.1	[84]	www.flurl.com.tw
125.232.X.116	30/Nov/2006:02:15:13	GET /favicon.ico HTTP/1.1	[84]	www.flurl.com.tw
163.13.X.12	30/Nov/2006:02:37:31	GET / HTTP/1.1	[23]	www.flurl.com.tw
163.13.X.12	30/Nov/2006:02:37:32	GET /favicon.ico HTTP/1.1	[23]	www.flurl.com.tw
125.231.X.2	30/Nov/2006:06:19:48	GET / HTTP/1.1	[23]	www.flurl.com.tw
220.142.X.62	30/Nov/2006:09:34:29	GET / HTTP/1.1	[67]	www.flurl.com.tw
220.142.X.62	30/Nov/2006:09:34:30	GET /favicon.ico HTTP/1.1	[67]	www.flurl.com.tw
69.229.X.59	21/Nov/2006:17:57:21	GET / HTTP/1.1	[85]	photobucket.com.mx
69.229.X.59	21/Nov/2006:17:57:21	GET /favicon.ico HTTP/1.1	[85]	photobucket.com.mx
201.132.X.95	21/Nov/2006:19:56:01	GET / HTTP/1.1	[86]	www.photobucket.com.mx
201.130.X.213	21/Nov/2006:21:56:56	GET / HTTP/1.1	[1]	www.photobucket.com.mx
201.130.X.213	21/Nov/2006:21:56:56	GET /favicon.ico HTTP/1.1	[1]	www.photobucket.com.mx
189.169.X.88	22/Nov/2006:12:26:10	GET / HTTP/1.1	[40]	photobucket.com.mx
189.143.X.143	22/Nov/2006:15:27:10	GET / HTTP/1.1	[40]	www.photobucket.com.mx
201.141.X.213	22/Nov/2006:21:37:31	GET / HTTP/1.1	[87]	www.photobucket.com.mx
201.141.X.213	22/Nov/2006:21:37:31	GET /favicon.ico HTTP/1.1	[87]	www.photobucket.com.mx
201.141.X.213	22/Nov/2006:21:37:31	GET /favicon.ico HTTP/1.1	[87]	www.photobucket.com.mx
189.131.X.26	23/Nov/2006:12:54:58	GET /webhp?hl=es HTTP/1.1	[23]	www.photobucket.com.mx
189.131.X.26	23/Nov/2006:12:55:01	GET /webhp?hl=es HTTP/1.1	[23]	www.photobucket.com.mx
189.140.X.108	23/Nov/2006:14:46:51	GET / HTTP/1.1	[23]	www.photobucket.com.mx
189.143.X.172	23/Nov/2006:15:18:29	GET / HTTP/1.1	[67]	www.photobucket.com.mx
189.166.X.36	23/Nov/2006:17:11:42	GET / HTTP/1.1	[88]	photobucket.com.mx
189.166.X.36	23/Nov/2006:17:11:42	GET /_vti_bin/owssvr.dll?UL=1&ACT=4&BUILD=6254&STRMVER=4&CAPREQ=0 HTTP/1.1	[88]	photobucket.com.mx
189.166.X.36	23/Nov/2006:17:11:46	GET /MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=6254&STRMVER=4&CAPREQ=0 HTTP/1.1	[88]	photobucket.com.mx
148.243.X.3	23/Nov/2006:18:20:27	GET / HTTP/1.1	[40]	www.photobucket.com.mx
189.147.X.226	23/Nov/2006:22:53:59	GET / HTTP/1.1	[23]	photobucket.com.mx
189.146.X.69	24/Nov/2006:13:59:28	GET / HTTP/1.1	[40]	www.photobucket.com.mx
189.146.X.69	24/Nov/2006:14:22:57	GET / HTTP/1.1	[40]	www.photobucket.com.mx
200.77.X.6	24/Nov/2006:14:27:01	GET / HTTP/1.1	[40]	www.photobucket.com.mx
189.156.X.91	24/Nov/2006:16:12:32	GET / HTTP/1.1	[89]	photobucket.com.mx
189.148.X.82	24/Nov/2006:17:45:01	GET / HTTP/1.1	[40]	www.photobucket.com.mx
189.144.X.125	25/Nov/2006:00:19:34	GET / HTTP/1.1	[72]	www.photobucket.com.mx
189.142.X.85	25/Nov/2006:18:21:18	GET / HTTP/1.1	[90]	photobucket.com.mx
189.142.X.85	25/Nov/2006:18:21:18	GET /favicon.ico HTTP/1.1	[90]	photobucket.com.mx
201.141.X.90	25/Nov/2006:22:37:53	GET / HTTP/1.1	[91]	www.photobucket.com.mx
201.141.X.90	25/Nov/2006:22:37:54	GET /favicon.ico HTTP/1.1	[91]	www.photobucket.com.mx
148.240.X.81	25/Nov/2006:22:45:06	GET / HTTP/1.0	[23]	photobucket.com.mx
200.77.X.77	26/Nov/2006:10:32:36	GET / HTTP/1.1	[91]	www.photobucket.com.mx
200.77.X.77	26/Nov/2006:10:32:36	GET /favicon.ico HTTP/1.1	[91]	www.photobucket.com.mx
189.142.X.85	26/Nov/2006:19:40:07	GET / HTTP/1.1	[40]	photobucket.com.mx
201.132.X.60	27/Nov/2006:00:33:30	GET / HTTP/1.1	[23]	photobucket.com.mx
200.66.X.61	27/Nov/2006:01:32:25	GET / HTTP/1.1	[34]	photobucket.com.mx
189.164.X.124	27/Nov/2006:11:38:34	GET /albums/j262/snchzgris/ELI.jpg HTTP/1.1	[68]	www.i82.photobucket.com.mx
70.137.X.247	27/Nov/2006:12:09:46	GET / HTTP/1.0	[1]	photobucket.com.mx
148.204.X.169	27/Nov/2006:15:50:14	GET / HTTP/1.1	[23]	www.photobucket.com.mx
201.132.X.10	27/Nov/2006:17:28:26	GET / HTTP/1.1	[92]	www.photobucket.com.mx
189.141.X.251	27/Nov/2006:18:54:37	GET / HTTP/1.1	[93]	www.photobucket.com.mx
189.155.X.132	27/Nov/2006:19:30:27	GET / HTTP/1.1	[34]	www.photobucket.com.mx

```
189.142.X.170   27/Nov/2006:23:17:41   GET / HTTP/1.1                 [23]   www.photobucket.com.mx
189.156.X.196   28/Nov/2006:09:13:52   GET / HTTP/1.1                 [94]   photobucket.com.mx
189.142.X.193   28/Nov/2006:14:59:18   GET / HTTP/1.1                 [23]   www.photobucket.com.mx
201.148.X.61    28/Nov/2006:17:32:28   GET / HTTP/1.0                 [13]   www.photobucket.com.mx
201.148.X.61    28/Nov/2006:17:32:29   GET /favicon.ico HTTP/1.0      [13]   www.photobucket.com.mx
201.143.X.243   28/Nov/2006:21:21:27   GET / HTTP/1.1                 [23]   photobucket.com.mx
189.163.X.10    29/Nov/2006:10:57:42   GET / HTTP/1.0                 [23]   www.photobucket.com.mx
189.144.X.188   29/Nov/2006:13:14:47   GET / HTTP/1.1                 [40]   www.photobucket.com.mx
189.144.X.188   29/Nov/2006:13:14:47   GET /favicon.ico HTTP/1.1      [40]   www.photobucket.com.mx
200.76.X.3      29/Nov/2006:13:41:28   GET / HTTP/1.1                 [13]   www.photobucket.com.mx
200.76.X.3      29/Nov/2006:13:41:28   GET /favicon.ico HTTP/1.1      [13]   www.photobucket.com.mx
189.167.X.222   29/Nov/2006:16:26:47   GET / HTTP/1.1                 [90]   www.photobucket.com.mx
189.167.X.222   29/Nov/2006:16:26:47   GET /favicon.ico HTTP/1.1      [90]   www.photobucket.com.mx
189.171.X.192   29/Nov/2006:17:24:17   GET / HTTP/1.1                 [87]   www.photobucket.com.mx
189.171.X.192   29/Nov/2006:17:24:17   GET /favicon.ico HTTP/1.1      [87]   www.photobucket.com.mx
189.134.X.131   29/Nov/2006:21:45:17   GET / HTTP/1.1                 [87]   www.photobucket.com.mx
189.134.X.131   29/Nov/2006:21:45:18   GET /favicon.ico HTTP/1.1      [87]   www.photobucket.com.mx
201.170.X.32    29/Nov/2006:22:27:44   GET / HTTP/1.1                 [40]   photobucket
189.160.X.113   30/Nov/2006:09:25:31   GET / HTTP/1.1                 [47]   www.photobucket.com.mx
189.140.X.20    30/Nov/2006:14:09:50   GET / HTTP/1.1                 [23]   www.photobucket.com.mx
189.140.X.20    30/Nov/2006:14:21:33   GET / HTTP/1.1                 [23]   www.photobucket.com.mx
189.142.X.75    30/Nov/2006:15:26:16   GET / HTTP/1.1                 [95]   www.photobucket.com.mx
189.142.X.75    30/Nov/2006:15:26:16   GET /favicon.ico HTTP/1.1      [95]   www.photobucket.com.mx
189.142.X.75    30/Nov/2006:15:26:16   GET /favicon.ico HTTP/1.1      [95]   www.photobucket.com.mx
```

The following table is a key that associates the index numbers listed in the "User-Agent" column of the table above with the value of the User-Agent: header received by the client.

1	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
2	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Arcor 5.004; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.2)
3	Mozilla/5.0 (compatible; Konqueror/3.1-rc4; i686 Linux; 20020319)
4	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)
5	Mozilla/5.0 (compatible; Konqueror/3.0-rc4; i686 Linux; 20020822)
6	Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en) AppleWebKit/418.9 (KHTML, like Gecko) Safari/419.3
7	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312468)
8	Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1) Gecko/20061010 Firefox/2.0
9	-
10	Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.0.7) Gecko/20060909 Firefox/1.5.0.7
11	libwww-perl/5.79
12	Mozilla/5.0 (compatible; Konqueror/3.1-rc4; i686 Linux; 20020203)
13	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
14	Mozilla/5.0 (compatible; Konqueror/3.1-rc1; i686 Linux; 20021002)
15	Mozilla/4.0 compatible ZyBorg/1.0 (wn-14.zyborg@looksmart.net; http://www.WISEnutbot.com)
16	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.2)
17	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312464)
18	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.03)
19	Mozilla/5.0 (compatible; Konqueror/3.1-rc6; i686 Linux; 20020618)
20	Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.8
21	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312467)
22	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1) Gecko/20061010 Firefox/2.0
23	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
24	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312460)
25	Mozilla/5.0 (Windows; U; Windows NT 5.0; de; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.8
26	Mozilla/5.0 (compatible; Konqueror/3.0-rc4; i686 Linux; 20020421)
27	Mozilla/5.0 (compatible; Konqueror/3.1-rc2; i686 Linux; 20020614)
28	Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.1) Gecko/20061025 BonEcho/2.0
29	Mozilla/5.0 (compatible; Konqueror/3.0-rc4; i686 Linux; 20020211)
30	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; i-NavFourF; .NET CLR 1.1.4322)
31	Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418.9 (KHTML, like Gecko) Safari/419.3
32	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312463)
33	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; InfoPath.2)
34	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
35	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
36	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; FDM)
37	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; mxie; .NET CLR 1.1.4322; InfoPath.1)
38	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; KKman3.0; .NET CLR 1.1.4322; InfoPath.1)
39	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
40	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
41	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; mxie; .NET CLR 1.1.4322)
42	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; KKman3.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
43	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; mxie)
44	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon; .NET CLR 1.1.4322)

45 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; mxie; .NET CLR 1.1.4322; .NET CLR 2.0.50727)

46 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; KKman3.0; .NET CLR 1.1.4322)

47 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1)

48 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; mxie; KKman2.0; KKman3.0)

49 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; InfoPath.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)

50 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; KKman3.0; InfoPath.1; .NET CLR 1.1.4322)

51 Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-TW; rv:1.8.0.7) Gecko/20060909 Firefox/1.5.0.7

52 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; FunWebProducts; .NET CLR 1.1.4322)

53 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; mxie; InfoPath.1; .NET CLR 1.1.4322)

54 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; KKman3.0)

55 Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-TW; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.8

56 Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

57 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1)

58 Mozilla/5.0 (compatible; Google Desktop)

59 Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-TW; rv:1.8.1) Gecko/20061010 Firefox/2.0

60 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; ezPeer+ v1.0 (0.5.0.06); .NET CLR 2.0.50727)

61 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar)

62 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1.1.4322)

63 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; MyIE2; Maxthon; .NET CLR 1.1.4322)

64 Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.1) Gecko/20061010 Firefox/2.0

65 Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)

66 Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; FDM; InfoPath.2)

67 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.1)

68 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)

69 Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.8

70 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; mxie; KKman3.0; .NET CLR 1.1.4322; InfoPath.1)

71 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Alexa Toolbar; mxie; SV1; KKman3.0)

72 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)

73 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; KKman3.0; .NET CLR 2.0.50727)

74 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; FunWebProducts)

75 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; mxie; Alexa Toolbar)

76 Mozilla/4.0 (compatible;)

77 Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)

78 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Alexa Toolbar; mxie; (R1 1.5))

79 Mozilla/4.0 (compatible; MSIE 5.5; Windows 98; Win 9x 4.90)

80 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Alexa Toolbar; mxie; .NET CLR 1.1.4322)

81 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; mxie; MODA3.0; FDM; .NET CLR 1.1.4322; .NET CLR 2.0.50727)

82 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; (R1 1.5))

83 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar; mxie; Alcohol Search; KKman3.0; .NET CLR 1.1.4322; InfoPath.1)

84 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Badongo 2.0.0)

85 Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; FunWebProducts; IEMB3; IEMB3)

86 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Alexa Toolbar)

87 Mozilla/5.0 (Windows; U; Windows NT 5.1; es-AR; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.8

88 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; FunWebProducts)

89 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.1; MEGAUPLOAD 1.0)

90 Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.8.1) Gecko/20061010 Firefox/2.0

91 Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418.8 (KHTML, like Gecko) Safari/419.3

92 Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Win 9x 4.90)

93 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; TISA; .NET CLR 1.1.4322)

94 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; FunWebProducts; ZangoToolbar 4.8.2)

95 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20060912 Netscape/8.1.2

4.3 <TLD>.<TLD> Combinations

On the request of the review team, IANA performed a systematic walk through the DNS in order to count the number of <TLD>.<TLD> occurrences. The analysis of these data appears in Section 3.2.1. All combinations of <TLD>.<TLD> have been tested for occurrence in the DNS. Since there are 265 delegations in the root zone (http://data.iana.org/TLD/tlds-alpha-by-domain.txt), there are 70,225 combinations. Among them, there are 11,592 combinations having A record or NS records, as shown in the table below.

It is possible that other <TLD>.<TLD> combinations exist with other types of resource records (e.g. MX or TXT), however no attempt was made to query for these other resource records. As a result, the number of <TLD>.<TLD> combinations identified represents a lower bound of the total number of <TLD>.<TLD> combinations with any type of DNS records.

TLD	Existing <TLD>.<TLD>
AC	AERO.AC, ARPA.AC, AX.AC, BIZ.AC, CAT.AC, CD.AC, and 24 others
AD	INFO.AD
AE	AC.AE, AD.AE, AE.AE, AF.AE, AG.AE, AM.AE, and 84 others
AERO	AC.AERO, AE.AERO, AF.AERO, BA.AERO, CAT.AERO, CI.AERO, and 12 others
AF	COM.AF, EDU.AF, EU.AF, GL.AF, GOV.AF, NET.AF, and 2 others
AG	AERO.AG, AF.AG, AI.AG, AN.AG, AS.AG, AT.AG, and 58 others
AI	AD.AI, AI.AI, AM.AI, BIZ.AI, BM.AI, COM.AI and 11 others
AL	COM.AL, EDU.AL, GOV.AL, MIL.AL, NET.AL, ORG.AL, and 2 others
AM	AX.AM, BE.AM, BIZ.AM, CAT.AM, DE.AM, DJ.AM, and 18 others
AN	GOV.AN, IT.AN, MIL.AN
AO	AT.AO, GOV.AO
AQ	AG.AQ
AR	BA.AR, COM.AR, EDU.AR, GOV.AR, INT.AR, MIL.AR, and 2 others
AS	AERO.AS, CAT.AS, GOV.AS, MOBI.AS
AT	AC.AT, AERO.AT, BIZ.AT, CAT.AT, CO.AT, COOP.AT, and 8 others
AU	COM.AU, EDU.AU, GOV.AU, ID.AU, INFO.AU, NET.AU, and 2 others
AW	SI.AW, UA.AW
AX	AE.AX, FK.AX, MUSEUM.AX
AZ	BR.AZ, GOV.AZ, MOBI.AZ, MS.AZ, TRAVEL.AZ
BA	BIZ.BA, CO.BA, COM.BA, COOP.BA, EDU.BA, GOV.BA, and 7 others
BB	CO.BB, COM.BB, EDU.BB, FM.BB, GOV.BB, JOBS.BB, and 4 others
BD	AC.BD, COM.BD, EDU.BD, GOV.BD, MIL.BD, ORG.BD
BE	AC.BE, AE.BE, AERO.BE, AF.BE, AG.BE, AI.BE, and 216 others
BF	AN.BF, GA.BF, GOV.BF
BG	INFO.BG, JOBS.BG, TRAVEL.BG
BH	BI.BH, CC.BH, CO.BH, COM.BH, EDU.BH, GOV.BH, and 2 others
BI	CO.BI, COM.BI, IS.BI, ORG.BI, SJ.BI, TO.BI

BIZ	CAT.BIZ, JOBS.BIZ, MOBI.BIZ, TRAVEL.BIZ
BJ	COM.BJ, ORG.BJ
BM	BM.BM, BS.BM, BT.BM, BV.BM, CC.BM, CL.BM, and 15 others
BN	COM.BN, EDU.BN, GOV.BN, MIL.BN, NET.BN, ORG.BN
BO	INFO.BO
BR	AM.BR, BN.BR, COM.BR, COOP.BR, EDU.BR, FM.BR, and 7 others
BS	MS.BS, NO.BS, TRAVEL.BS
BT	COM.BT, EDU.BT, GOV.BT, NET.BT, ORG.BT, TRAVEL.BT
BW	AC.BW, BT.BW, CO.BW, GOV.BW, INFO.BW, IS.BW, and 3 others
BY	AC.BY, AD.BY, AERO.BY, AF.BY, AG.BY, AL.BY, and 92 others
BZ	AC.BZ, AD.BZ, AERO.BZ, AI.BZ, AM.BZ, AU.BZ, and 37 others
CA	AC.CA, AD.CA, AE.CA, AERO.CA, AF.CA, AG.CA, and 215 others
CC	AC.CC, AD.CC, AE.CC, AERO.CC, AF.CC, AG.CC, and 254 others
CD	AC.CD, CAT.CD, EDU.CD, GH.CD, GOV.CD, INFO.CD, and 5 others
CG	AC.CG, AD.CG, AE.CG, AERO.CG, AF.CG, AG.CG, and 258 others
CH	AERO.CH, AG.CH, AI.CH, AM.CH, AR.CH, ARPA.CH, and 30 others
CI	AC.CI, CO.CI, COM.CI, EDU.CI, ET.CI, FR.CI, and 5 others
CL	AERO.CL, AF.CL, AG.CL, AI.CL, AL.CL, AM.CL, and 169 others
CM	AC.CM, AD.CM, AE.CM, AERO.CM, AF.CM, AG.CM, and 256 others
CN	AC.CN, AQ.CN, BB.CN, BJ.CN, CAT.CN, COM.CN, and 41 others
CO	UK.CO
COM	AC.COM, AD.COM, AE.COM, AERO.COM, AF.COM, AG.COM, and 259 others
COOP	TRAVEL.COOP, UK.COOP
CU	CC.CU, CO.CU, COM.CU, EDU.CU
CV	BI.CV, BN.CV, GOV.CV, IE.CV, MY.CV, TC.CV, and 1 others
CX	AC.CX, AD.CX, AG.CX, AI.CX, AL.CX, AM.CX, and 157 others
CY	AC.CY, BIZ.CY, COM.CY, GOV.CY, NAME.CY, NET.CY, and 2 others
CZ	AC.CZ, AD.CZ, AE.CZ, AERO.CZ, AF.CZ, AG.CZ, and 234 others
DE	AERO.DE, BIZ.DE, CAT.DE, COOP.DE, INFO.DE, JOBS.DE, and 5 others
DJ	AF.DJ, BIZ.DJ, CO.DJ, DJ.DJ, EU.DJ, INT.DJ, and others 2
DK	AC.DK, AD.DK, AE.DK, AERO.DK, AF.DK, AG.DK, and 253 others
DM	AI.DM, CO.DM, COM.DM, EDU.DM, GOV.DM, INFO.DM, and 2 others
DO	COM.DO, EDU.DO, GOV.DO, MIL.DO, NET.DO, ORG.DO
DZ	CAT.DZ, COM.DZ, CV.DZ, EDU.DZ, GOV.DZ, INT.DZ, and 2 others
EC	CAT.EC, COM.EC, EDU.EC, GOV.EC, INFO.EC, INT.EC, and 5 others
EDU	AC.EDU, AI.EDU, AU.EDU, BD.EDU, BI.EDU, BW.EDU, and 55 others
EE	AC.EE, AD.EE, AE.EE, AERO.EE, AF.EE, AG.EE, and 157 others
EG	COM.EG, EDU.EG, GOV.EG, MIL.EG, NET.EG, ORG.EG
ER	COM.ER, EDU.ER, GOV.ER, MIL.ER, NET.ER, ORG.ER
ES	AERO.ES, ARPA.ES, BT.ES, CAT.ES, COM.ES, EDU.ES, and 5 others
ET	BIZ.ET, COM.ET, EDU.ET, GOV.ET, INFO.ET, NAME.ET, and 2 others
EU	AERO.EU, ARPA.EU, COOP.EU, EDU.EU, INFO.EU, INT.EU, and 7 others
FI	AERO.FI, ARPA.FI, AX.FI, CAT.FI, EDU.FI, INFO.FI, and 10 others
FJ	GOV.FJ
FM	AC.FM, AERO.FM, AL.FM, AM.FM, AT.FM, BE.FM, and 42 others
FO	AT.FO, BB.FO, BG.FO, BR.FO, CH.FO, DE.FO, and 25 others
FR	AERO.FR, BIZ.FR, CAT.FR, COM.FR, COOP.FR, INFO.FR, and 5 others

GA	AM.GA, CO.GA, GT.GA, ORG.GA
GD	CO.GD, DE.GD, EDU.GD, GOV.GD, ORG.GD
GE	BIZ.GE, COM.GE, EDU.GE, GOV.GE, INFO.GE, INT.GE, and 8 others
GG	AT.GG, BE.GG, CA.GG, CH.GG, CN.GG, CZ.GG, and 21 others
GH	COM.GH, EDU.GH, GOV.GH, IT.GH, MIL.GH, NET.GH, and 1 others
GI	COM.GI, EDU.GI, GOV.GI, JOBS.GI, ORG.GI
GL	AC.GL, AE.GL, AG.GL, AT.GL, BIZ.GL, CAT.GL, and 33 others
GM	GOV.GM, MS.GM
GOV	AG.GOV, AL.GOV, AR.GOV, ARPA.GOV, AZ.GOV, CA.GOV, and 27 others
GP	BD.GP, COM.GP, NET.GP
GR	AE.GR, AERO.GR, ARPA.GR, BD.GR, BI.GR, BIZ.GR, and 34 others
GS	AD.GS, AE.GS, AG.GS, AI.GS, AN.GS, AQ.GS, and 106 others
GU	COM.GU, EDU.GU, GOV.GU, NET.GU, ORG.GU
GY	CO.GY, COM.GY, EDU.GY, GOV.GY, NET.GY, ORG.GY
HK	AX.HK, COM.HK, EDU.HK, GOV.HK, JOBS.HK, MOBI.HK, and 4 others
HM	AN.HM, AO.HM, AT.HM, AU.HM, AX.HM, AZ.HM, and 39 others
HN	AM.HN, AT.HN, BA.HN, BIZ.HN, CA.HN, CAT.HN, and 25 others
HR	BIZ.HR, COM.HR, HT.HR, INFO.HR, IT.HR, KZ.HR, and 6 others
HT	COM.HT, COOP.HT, EDU.HT, INFO.HT, NET.HT, ORG.HT, and 1 others
HU	AD.HU, AERO.HU, AF.HU, AI.HU, AL.HU, AM.HU, and 238 others
ID	AC.ID, CO.ID, MIL.ID, NET.ID
IE	BIZ.IE, CAT.IE, EDU.IE, GOV.IE, JOBS.IE, MUSEUM.IE, and 2 others
IL	AC.IL, CO.IL, GOV.IL, NET.IL, ORG.IL
IM	AT.IM, BI.IM, CAT.IM, CK.IM, CN.IM, CO.IM, and 18 others
IN	AC.IN, CAT.IN, CO.IN, EDU.IN, GOV.IN, JOBS.IN, and 4 others
INFO	CAT.INFO, INFO.INFO, JOBS.INFO, MOBI.INFO, TRAVEL.INFO
INT	EU.INT
IO	AERO.IO, ARPA.IO, AX.IO, BIZ.IO, BT.IO, CAT.IO, and 17 others
IR	AC.IR, CO.IR, GOV.IR, ID.IR, MOBI.IR, NET.IR, and 1 others
IS	AC.IS, AD.IS, AE.IS, AF.IS, AG.IS, AI.IS, and 172 others
IT	AG.IT, AL.IT, AN.IT, AO.IT, AQ.IT, AR.IT, and 73 others
JE	AC.JE, AT.JE, BE.JE, CF.JE, CH.JE, DE.JE, and 11 others
JO	CG.JO, COM.JO, EDU.JO, GOV.JO, IO.JO, IT.JO, and 10 others
JOBS	COM.JOBS, JOBS.JOBS
JP	CAT.JP, MOBI.JP, TRAVEL.JP
KE	AC.KE, CO.KE, NE.KE, SC.KE
KG	AC.KG, AR.KG, AT.KG, BA.KG, BIZ.KG, BR.KG, and 40 others
KH	COM.KH, EDU.KH, GOV.KH, NET.KH, ORG.KH
KI	BIZ.KI, CO.KI, COM.KI, DE.KI, EDU.KI, EU.KI, and 6 others
KN	CAT.KN, CO.KN, COM.KN, EDU.KN, GOV.KN, HK.KN, and 2 others
KR	AC.KR, CO.KR, ES.KR, KG.KR, MIL.KR, MS.KR, and 4 othres
KW	COM.KW, EDU.KW, GOV.KW, MIL.KW, NET.KW, ORG.KW
KY	CD.KY, CN.KY COM.KY, DE.KY, EDU.KY, GOV.KY, and 12 others
KZ	AC.KZ, AE.KZ, AERO.KZ, AF.KZ, AI.KZ, AL.KZ, and 157 others
LA	AC.LA, AERO.LA, AF.LA, AG.LA, AL.LA, AM.LA, and 139 others
LB	COM.LB, EDU.LB, GOV.LB, NET.LB, ORG.LB
LC	COM.LC, EDU.LC, GOV.LC, ORG.LC
LI	AERO.LI, BIZ.LI, CAT.LI, COM.LI, COOP.LI, EDU.LI, and 8 others

LK	AC.LK, CF.LK, CH.LK, CI.LK, DE.LK, EG.LK, and 6 others
LS	AC.LS, CO.LS, GOV.LS, NET.LS, ORG.LS
LT	AD.LT, AERO.LT, AL.LT, AM.LT, AS.LT, BA.LT, and 72 others
LU	AL.LU, BIZ.LU, CAT.LU, CC.LU, CU.LU, GOV.LU, and 11 others
LV	AC.LV, AD.LV, AF.LV, AI.LV, AM.LV, AR.LV, and 149 others
LY	AC.LY, AR.LY, AT.LY, BB.LY, BE.LY, BG.LY, and 38 others
MA	AC.MA, AD.MA, AERO.MA, AG.MA, AL.MA, AM.MA, and 69 others
MC	COM.MC, TM.MC
MD	AC.MD, AD.MD, AM.MD, AR.MD, AS.MD, AT.MD, and 64 others
MG	CO.MG, COM.MG, EDU.MG, GOV.MG, MIL.MG, NET.MG, and 1 others
MH	GF.MH
MIL	AF.MIL, ARPA.MIL, NG.MIL, SD.MIL
MK	IN.MK
ML	AC.ML, CO.ML, COM.ML, EDU.ML, GOV.ML, NET.ML, and 2 others
MN	AM.MN, AT.MN, AZ.MN, BD.MN, BM.MN, BT.MN, and 33 others
MO	COM.MO, EDU.MO, GOV.MO, INFO.MO, NET.MO, ORG.MO
MP	CO.MP, EDU.MP, GOV.MP, NET.MP, ORG.MP
MR	GOV.MR
MS	AC.MS, AD.MS, AE.MS, AERO.MS, AF.MS, AG.MS, and 231 others
MT	COM.MT, EDU.MT, GOV.MT, NET.MT, ORG.MT
MU	AC.MU, AD.MU, AE.MU, AERO.MU, AF.MU, AG.MU, and 157 others
MUSEUM	AC.MUSEUM, AD.MUSEUM, AE.MUSEUM, AERO.MUSEUM, AF.MUSEUM, AG.MUSEUM, and 259 others
MV	COM.MV, EDU.MV, GOV.MV, NET.MV, ORG.MV
MW	AC.MW, AERO.MW, BB.MW, BIZ.MW, CC.MW, CD.MW, and 32 others
MX	CAT.MX, COM.MX, EDU.MX, NET.MX, ORG.MX
MY	COM.MY, EDU.MY, GOV.MY, MIL.MY, NAME.MY, NET.MY, and 2 others
MZ	AC.MZ, CO.MZ, GOV.MZ, NET.MZ, ORG.MZ
NA	BIZ.NA, CO.NA, COM.NA, EDU.NA, GOV.NA, IN.NA, and 4 others
NAME	CAT.NAME, JOBS.NAME, MOBI.NAME TRAVEL.NAME
NC	PA.NC
NET	AC.NET, AD.NET, AE.NET, AERO.NET, AF.NET, AG.NET, and 259 others
NF	AC.NF, AT.NF, CH.NF, CO.NF, COM.NF, DE.NF, and 9 others
NG	AC.NG, COM.NG, EDU.NG, GOV.NG, NET.NG, ORG.NG
NI	AC.NI, BIZ.NI, CO.NI, COM.NI, EDU.NI, IN.NI, and 5 others
NL	AC.NL, AD.NL, AE.NL, AERO.NL, AF.NL, AG.NL, and 258 others
NO	AC.NO, AD.NO, AE.NO, AERO.NO, AF.NO, AG.NO, and 246 others
NP	COM.NP, EDU.NP, GOV.NP, MIL.NP, NET.NP, ORG.NP
NR	AT.NR, BIZ.NR, CO.NR, COM.NR, DE.NR, EDU.NR, and 5 others
NU	AD.NU, AE.NU, AERO.NU, AF.NU, AG.NU, AI.NU, and 257 others
NZ	AC.NZ, CO.NZ, MIL.NZ, NET.NZ, ORG.NZ
OM	BIZ.OM, CO.OM, COM.OM, EDU.OM, GOV.OM, NET.OM, and 1 others
ORG	AD.ORG, AE.ORG, AERO.ORG, AF.ORG, AG.ORG, AI.ORG, and 248 others
PA	AC.PA, COM.PA, EDU.PA, NET.PA, ORG.PA
PE	COM.PE, EDU.PE, MIL.PE, NET.PE, ORG.PE
PF	BT.PF, COM.PF, EDU.PF, GOV.PF, HM.PF
PH	AC.PH, AD.PH, AE.PH, AERO.PH, AF.PH, AG.PH, and 259 others
PK	AERO.PK, JOBS.PK, MOBI.PK

PL	AC.PL, AD.PL, AE.PL, AERO.PL, AF.PL, AG.PL, and 253 others
PN	AT.PN, AU.PN, BIZ.PN, CA.PN, CC.PN, CH.PN, and 23 others
PR	AC.PR, BD.PR, BIZ.PR, CAT.PR, COM.PR, EDU.PR, and 7 others
PRO	JOBS.PRO, MOBI.PRO, TRAVEL.PRO
PS	AL.PS, CAT.PS, CO.PS, COM.PS, CU.PS, EDU.PS, and 13 others
PT	BB.PT, BN.PT, CAT.PT, CL.PT, CO.PT, EDU.PT, and 10 others
PW	AC.PW, AD.PW, AE.PW, AERO.PW, AF.PW, AG.PW, and 254 others
PY	COM.PY, EDU.PY, GOV.PY, MIL.PY, NET.PY, ORG.PY
QA	COM.QA, EDU.QA, FM.QA, GOV.QA, MIL.QA, NAME.QA, and 4 others
RE	MOBI.RE, TRAVEL.RE
RO	AC.RO, AD.RO, AERO.RO, AF.RO, AI.RO, AM.RO, and 196 others
RU	AC.RU, AD.RU, AE.RU, AERO.RU, AF.RU, AG.RU, and 252 others
RW	AC.RW, AD.RW, AE.RW, AERO.RW, AF.RW, AG.RW, and 257 others
SA	COM.SA, EDU.SA, GOV.SA, NET.SA, ORG.SA
SB	COM.SB, EDU.SB, GOV.SB, NET.SB, ORG.SB
SC	AERO.SC, BIZ.SC, CAT.SC, COM.SC, EDU.SC, GOV.SC, and 12 others
SD	BIZ.SD, COM.SD, EDU.SD, GOV.SD, INFO.SD, JOBS.SD, and 3 others
SE	AD.SE, AE.SE, AERO.SE, AF.SE, AL.SE, ARPA.SE, and 89 others
SG	AE.SG, AI.SG, AM.SG, AR.SG, AT.SG, BS.SG, and 50 others
SH	AERO.SH, ARPA.SH, AX.SH, CAT.SH, CD.SH, CO.SH, and 25 others
SI	AERO.SI, ARPA.SI, CAT.SI, GOV.SI, JOBS.SI, KI.SI, and 3 others
SK	AC.SK, AERO.SK, AX.SK, CAT.SK, COOP.SK, EDU.SK, and 15 others
SL	TRAVEL.SL
SM	ARPA.SM, CC.SM, ES.SM, GOV.SM, PA.SM, SH.SM
SN	CAT.SN, SR.SN
SR	CC.SR, CH.SR, CO.SR, COM.SR, DE.SR, EDU.SR, and 9 others
ST	AD.ST, AE.ST, AERO.ST, AF.ST, AG.ST, AI.ST, and 244 others
SU	CAT.SU, JOBS.SU, MOBI.SU, TRAVEL.SU
SY	AD.SY, AM.SY, CO.SY, COM.SY, CV.SY, DM.SY, and 10 others
SZ	GOV.SZ
TC	AC.TC, AD.TC, AE.TC, AERO.TC, AG.TC, AI.TC, and 131 others
TF	AT.TF, BE.TF, BG.TF, BY.TF, CA.TF, CC.TF, and 24 others
TG	CAT.TG, CR.TG
TH	AC.TH, CO.TH, IN.TH, NET.TH
TJ	JOBS.TJ, TRAVEL.TJ
TK	AC.TK, AD.TK, AE.TK, AERO.TK, AF.TK, AG.TK, and 257 others
TL	AG.TL, AI.TL, AM.TL, AR.TL, AT.TL, AU.TL, and 49 others
TM	AERO.TM, ARPA.TM, AX.TM, BIZ.TM, CAT.TM, COOP.TM, and 11 others
TN	COM.TN, GOV.TN, INFO.TN, NET.TN, ORG.TN, TT.TN
TO	AD.TO, AE.TO, AERO.TO, AF.TO, AI.TO, AL.TO, and 178 othera
TP	AR.TP, AT.TP, AU.TP, BIZ.TP, BR.TP, CA.TP, and 26 others
TR	BIZ.TR, COM.TR, EDU.TR, GOV.TR, INFO.TR, MIL.TR, and 4 others
TRAVEL	TRAVEL.TRAVEL
TT	AT.TT, AU.TT, BE.TT, CA.TT, CAT.TT, CC.TT, and 14 others
TV	AC.TV, AD.TV, AERO.TV, AF.TV, AG.TV, AI.TV, and 247 others
TW	COM.TW, EDU.TW, GOV.TW, MIL.TW, NET.TW, ORG.TW
TZ	AC.TZ, CO.TZ, MIL.TZ, NE.TZ
UA	AC.UA, AG.UA, AU.UA, BIZ.UA, BM.UA, BT.UA, and 56 others

UG	TRAVEL.UG
UK	AC.UK, CO.UK, GOV.UK, MIL.UK, NET.UK, ORG.UK
US	CAT.US, JOBS.US, MOBI.US
UY	COM.UY, EDU.UY, MIL.UY, NET.UY, ORG.UY
UZ	AS.UZ, AT.UZ, BIZ.UZ, BY.UZ, CC.UZ, CD.UZ, and 48 others
VC	AC.VC, AD.VC, AE.VC, AF.VC, AG.VC, AI.VC, and 104 others
VG	AC.VG, AD.VG, AE.VG, AERO.VG, AF.VG, AG.VG, and 226 others
VI	CO.VI, COM.VI, GOV.VI, NET.VI, ORG.VI
VN	AC.VN, BIZ.VN, CAT.VN, COM.VN, COOP.VN, EDU.VN, and 10 others
VU	AG.VU, AT.VU, AU.VU, BIZ.VU, BZ.VU, CH.VU, and 31 others
WS	AC.WS, AD.WS, AE.WS, AERO.WS, AF.WS, AG.WS, and 257 others
YE	COM.YE, EDU.YE, GOV.YE, MIL.YE, NET.YE, ORG.YE
YU	AC.YU, CG.YU, CO.YU, EDU.YU, GOV.YU, MN.YU, and 2 others
ZA	AC.ZA, CO.ZA, EDU.ZA, GOV.ZA, MIL.ZA, ORG.ZA, and 1 others
ZM	AC.ZM, CO.ZM, COM.ZM, EDU.ZM, GOV.ZM, MIL.ZM, and 3 others
ZW	AC.ZW, CO.ZW, GOV.ZW, MIL.ZW, ORG.ZW

Appendix A: Specific Security and Stability Scenarios

The review team conducted an extensive analysis of the potential security and stability implications of each of the issues described in Section 3.1. As indicated above in Section 3.2, we conclude that the addition of <TLD>.<TLD> combinations within .name would not cause any meaningful security or stability problems. This section describes the theoretical problems that <TLD>.<TLD> combinations could cause. However, we believe that the risk of these issues is either extremely low, or that the addition of two-character SLDs in .name does not meaningfully add to the risk already present in today's Internet naming system. This survey of problems is not intended to be exhaustive, but identifies the types of issues that could occur as the result of the presence of <TLD>.<TLD> combinations.

A.1 Scenarios Associated with Incorrect Responses to a Valid Domain Name

A.1.1 Security Issues

A.1.1.1 Pharming

Pharming is a common technique (related to phishing) used to obtain confidential or personal information from the user by presenting a web page that masquerades as a website that the user would trust. At the time of this report, Wikipedia[25] described Pharming as follows:

> "Pharming is a hacker's attack aiming to redirect a website's traffic to another (bogus) website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses — they are the "signposts" of the Internet. Compromised DNS servers are sometimes referred to as "poisoned". The term pharming is a word play on farming and phishing. The term phishing refers to social engineering attacks to obtain access credentials such as user names and passwords. In recent years both pharming and phishing have been used to steal identity information. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-

[25] http://en.wikipedia.org/wiki/Pharming

> pharming are required to protect against this serious threat.”

Resolvers returning incorrect DNS information as described in RFC 1535 expose users to Pharming attacks by directing the user to a different domain than the one that they entered. (For example, an attacker could register a domain such as example.li.name and hope to attract users who had entered “example.li” into their web browser. By presenting a site that appears to be similar to the actual example.li, the attacker could hope to obtain confidential information, such as the user’s password for the authentic example.li website.)

A.1.2 Stability Issues

A.1.2.1 Ability to Deploy a Secure DNS

The data and protocol extensions to add security to the DNS (DNSSEC) are defined in RFCs 4034[26] and 4035[27], respectively. Two-character labels are not treated specially in any way in the DNSSEC protocols, and the review team does not believe that allowing the inclusion of two-character SLDs within .name would have any effect on the ability to deploy a secure DNS.

At the same time, the review team notes that deployment of DNSSEC does nothing to solve the problem described in RFC 1535. Although the user’s initial query is for a different domain name than the domain name finally returned, the resolver appends the incorrect domain name prior to issuing the query to remote DNS servers, and the signatures returned on the zone data would be valid under the DNSSEC protocols.

A.1.2.2 Web Browsing

A.1.2.2.1 Side Effects on Web Browsing

More and more, the web is a portal to applications such as email, spreadsheets, and other services that are effectively outsourced applications. Many of these services make use of AJAX technology, which at the time of this report was defined by Wikipedia[28] as follows:

> “Ajax, shorthand for Asynchronous JavaScript and XML, is a web development technique for creating interactive

[26] RFC 4034, “Resource Records for the DNS Security Extensions”, R. Arends, et al, March 2005, http://www.ietf.org/rfc/rfc4034.txt

[27] RFC 4035, “Protocol Modifications for the DNS Security Extensions”, R. Arends, et al, March 2005, http://www.ietf.org/rfc/rfc4035.txt

[28] http://en.wikipedia.org/wiki/Ajax_%28programming%29

> web applications. The intent is to make web pages feel more responsive by exchanging small amounts of data with the server behind the scenes, so that the entire web page does not have to be reloaded each time the user makes a change."

All of these services will see the same set of issues as applications running directly on hosts. Having an AJAX transaction access the incorrect domain name rather HTTP point of access that was planned might lead to very unpredictable results in the JavaScript engine as well as in the user interface.

A.1.2.2.2 HTTP vs. HTTPS

Although the client application would receive the same (incorrect) data in preparing to make either an HTTP or HTTPS connection, typical browser behavior for HTTPS connections provides some protection for users in situations where incorrect DNS information is used to make the connection.

When the user of a browser types a URL such as:

https://icann.ex.name/index.html

the browser must first resolve "icann.ex.name". In the problematic case being discussed here, the IP address of the host icann.ex would actually be returned. However, immediately after opening the connection to the host icann.ex, one of the first steps in establishing the secure session is for the browser and the server to exchange digital certificates. The server's digital certificate contains information including the "Common Name" of the server, which is typically the host's domain name (in this case, icann.ex). In order to prevent man-in-the-middle attacks the browser compares the Common Name on the digital certificate to the domain name entered by the user; if the two strings do not match, a warning is displayed to the user. In our scenario, because the user entered the domain name "icann.ex.name" and the Common name contained in the certificate is "icann.ex", the browser will recognize the mismatch and warn the user. As a result, the user may realize that an error has occurred and be cautious about providing confidental information on the site.

However, in some cases the user may not understand the warning or may simply ignore it as an inconvenience rather than a potential security issue. Many users, when encountering messages they do not understand simply click "OK" in order to allow them to continue to the website. In cases in which users do not understand or choose to ignore the warning message, this layer of protection is of limited value.

A.1.2.3 SMTP

Internet mail service depends heavily on DNS for routing messages. The bulk of Internet mail is transferred using the (Extended) Simple MailTransfer Protocol ((E)SMTP) according to RFC 2821 and its predecessors, primarily RFCs 821 and 974 (full standard and historic, respectively).

SMTP uses DNS and its mail routing capabilities to reach a mail server closer to the destination. In order to determine the proper server to deliver an e-mail message to, the originating mail server consults the DNS to locate MX records (or, if MX records are not available, A records) for the domain name on the right hand side of the e-mail address. The information contained in the DNS is used to identify and connect to a mail server for the domain name.

If the resolver returns information for the incorrect domain name, an SMTP connection will be attempted to the incorrect server and mail will not be delivered properly. In many cases, the message will immediately be rejected (and an error message will be provided to the sender) because the mail server will not recognize the destination domain name. In these situations, the sender would immediately be aware that a problem had occurred. However, there are two possible configurations on the server receiving the misdirected message that would result in different outcomes:

(1) The mail server may be configured to attempt to deliver messages addressed to unknown domains to a mail server responsible for that domain. In this case, after receiving the message, the mail server would perform a second DNS lookup to obtain the MX records for the domain. Assuming that the mail server was not configured in a manner to reproduce the DNS problem[29] that caused the mail to be misdirected in the first place, it would obtain the proper information and then attempt to pass the information along to the correct mail server. In this case, the message would likely be delivered correctly[30], although

[29] In the unlikely event that both the sending and receiving mail servers used resolvers that were misconfigured and as a result obtained DNS records indicating (incorrectly) that the receiving mail server was the intended destination for the mail message, it is likely the message would be rejected. Most mail server software recognizes situations in which DNS records indicate that the mail server should be responsible for a particular domain name but the mail server's configuration does not include information about the domain; the usual behavior in these cases is to reject the message and generate an error message to the sender.

[30] Some anti-spam tools, such as Sender Policy Framework (SPF), limit the servers from which mail with a From: address in a particular domain

the delivery process would take longer and consume unnecessary resources in the intermediate host. Because the message would be delivered properly, it is possible that this situation might persist undetected for an extended period of time.

(2) Some mail servers are configured with “catchall” capabilities, where messages addressed to unrecognized e-mail addresses (and even unrecognized domain names) are delivered to one or more mailboxes on the server instead of being rerouted or rejected. In this situation, the mail message would be delivered to the wrong recipient. This instability can also be used to cause insecurity: if the message contained personal or confidential information, this (admittedly unlikely) scenario may expose the information to third parties. It is possible that an attacker could register a domain name and configure a catchall mail server to specifically target mail delivered to another related domain (e.g. registering example.li.name in order to attempt to intercept mail addressed to example.li).

A.1.2.4 Other Services

Returning DNS information for the incorrect domain name can redirect traffic for virtually any Internet service to the wrong host. This, in turn, will cause one of several problems. For example, imagine the user correctly types the domain name of his intended destination at the command line:

```
% ssh host.foo.ex
```

Instead of a login prompt, the user will see something like:

```
ssh: connect to host host.foo.ex.name port 22:
Connection refused
```

A user reading the error carefully may notice that the domain name of the host ssh tried to connect to is not the domain name he intended. However, many users wouldn't notice that subtlety. Moreover, many programs don't produce output this clear.

If the user does not realize that data from the wrong domain name have been returned, or the domain name is contained in a configuration file where the user does not see any direct feedback as a result of accessing the domain name information, the program will obtain the incorrect

may be sent. In this case, because the message is passing through an untrusted intermediary, it may be rejected by anti-spam software.

information from the resolver and connect to the wrong host. Depending on the nature of the program, this may expose sensitive data to eavesdropping, either by the maintainers of the alternative host or by someone with access to an intermediate network.

A.2 Scenarios Associated with Unexpected Responses to a Query for a Non-Existent Domain Name

A.2.1 Security Issues

A.2.1.1 Pharming

As described in section 3.1.2.1 above, an attacker could register a domain name that the user would reach if their resolver used .name in its search list, or if the user's browser automatically appended ".name" to the end of the domain name. However, this attack is less likely to be successful because (absent the type of problem described in RFC 1535) if the domain name entered by the user actually exists the user will successfully reach that site. In other words, this type of attack would work only if a user accidentally entered a domain name that did not exist, but which matched a subdomain within .name.

As an example, consider the possibility that the .ex domain allows registrations only at the third level in specific subdomains (e.g., com.ex or org.ex). A user might try to navigate to icann.ex, not realizing that they needed to type icann.org.ex. An attacker could register the name icann.ex.name in the hope that the user's resolver was configured with .name in its search list or that the user's browser would append .name to the end of the domain name.

A.2.2 Stability Issues

A.2.2.1 DNS

A.2.2.1.1 Impact on redirection NX Domains

There are some services that depend on an NXDOMAIN error being generated in response to a user query for an invalid domain name. These services include:

(1) Some web browser designers and Internet Service Providers have introduced services that direct the user to a "search page" or an "approximate match" to the user's result if the original query fails. These services typically use the domain name entered by the user as input to a search engine or some other tool to direct the user to information related to their original query.

(2) A common feature of modern browsers is to allow for the use of local languages in the display of menus, toolbars and error messages. Two crucial customizations are possible: a version of the browser whose application tools (menus and dialog boxes, etc.) have been adapted to a local language; and a version of the browser that adapts content in the document window to a local language.

When a browser adapts content based on a user's language preferences it can display text in an alternative character set—possibly rendering the content more usable. This clearly optimizes the browsing experience for the user. This customization is also usually extended to displaying traditional HTTP error messages in the language of the user's choice.

If, rather than receiving an NXDOMAIN error, the user is directed to an alternative domain name, neither of the above mechanisms can function correctly. Rather than seeing a search web site or an error message displayed in the user's preferred language, the user would be directed to another website altogether. This is likely a less than optimal experience for the user.

A.2.2.1.2 Ability to Deploy a Secure DNS

As described in Section 1.2.1 above, the inclusion of two-character second level domains within any particular TLD does not negatively impact the deployment of DNSSEC. At the same time, however, DNSSEC does not provide protection against unexpected response data being returned as the result of a resolver traversing its search list or client software appending a TLD to the end of the domain name entered by the user.

A.2.2.2 Web Browsing

A.2.2.2.1 Side Effects of Web Browsing

AJAX and other web applications
As described in Appendix A.1.2.2.1, AJAX applications that rely on reaching particular domain names may behave unexpectedly in situations in which they inadvertently contact the incorrect server because DNS resolution returns data applying to a different domain name.

Links vs. typed names

Much web navigation is achieved via clicking on links as opposed to using explicitly typed URLs. In cases where these are set up incorrectly, if the resolver still returns valid data (but for a different domain name), the recognition of the problem can be delayed, causing continuing errors and problems.

A.2.2.2.2 HTTP versus HTTPS

As described in Section 1.2.2.2 above, in situations where the user is directed to a different domain name than the one they entered, their browser may provide a warning to the user because the Common Name on the digital certificate provided by the server would not match the domain name entered by the user.

In the case where the user reaches an unexpected host as a result of the browser appending a TLD to the end of the domain name entered by the user, this warning would not be generated. In this case, the browser would recognize the certificate as matching the domain name that it had attempted to reach by appending the TLD to the end of the domain.

A.2.2.3 SMTP

As described in Section 1.2.3 above, the SMTP protocol used to deliver mail depends on DNS in order to identify the mail server to transmit the message to. In some cases, the resolver's search list may cause an alternative domain name to be returned which will cause the message to be delivered to the wrong server.

In addition, the SMTP protocol makes two other uses of DNS:

Use 1: Verify Sender Domain

There is another case in which the mail server makes intelligent use of DNS. The SMTP standard has the concept of an "envelope sender." This corresponds to the address on the reverse side of the paper envelope, to which the postal service will return the paper message if it is undeliverable. The function is exactly the same in the electronic version: this is the address to which an error message should be sent, if there is a need to send one.

The envelope sender is the first useful thing a sending mail server tells its recipient counterpart. The reason is that among the first things the recipient server wants to do, is to make sure it can return an error message to the sender, if there is the need to send one. Hence, when the recipient mail server hears this envelope sender address, it will immediately (before continuing the transaction) look up the mail domain of this address, to make sure it can reach the sender. This is done in the same fashion as described above (it "pretends" to send an error report, and performs all the corresponding lookups). If the mail domain doesn't exist, it will reject the incoming message on the basis that it will be unable to send an error report back to the sending user, if need be, and leaves it up to the sending mail server (which has obviously accepted the message, and hence has a way to report back to the user) to send an error report back.

If the message is sent from a non-existent mail domain, in some cases the mail server's resolver may fall back to its search list and return results from an alternative domain in a different zone. If it seems to exist, the recipient mail server will accept the message, and if it later is unable to forward the message appropriately, it will be unable to send an error report back (quite possibly wasting additional resources trying to do so).

This method of verifying the return path also has a limiting effect on unsolicited commercial email (UCE, or "spam"), which is often produced to seem to come from mail domains that do not exist. If the recipient mail server is unable to verify the sender's mail domain, it will reject the message. A parallel domain returned by the resolver will make the fake domain name seem to exist, and hence cause the spam message to be accepted.

Use 2: Find Submission Mail Server.

DNS is also used in another part of mail handling, when a mail user agent (MUA, the program that is used for reading and writing mail messages) needs to find its mail server(s). The MUA will typically be configured with the name of a mail server to which it will submit outgoing mail messages. It will look up the address of this mail server in DNS. If the domain name of the mail server is mistyped, it will normally be noticed immediately when the MUA tries to send a message, but if the resolver's search list causes DNS information for another domain to be returned, the mail server will seem to exist, and the MUA will attempt to submit its message to it. This may either succeed or not, again depending on whether a mail server is operated on this host. The error message to the user will again be unclear and misleading.

A.2.2.4 Other Services

As described in section 1.2.4, if the resolver returns DNS records for a different domain than the one entered, the user may connect to a different host. Depending on the nature of the program, this may expose sensitive data to eavesdropping, either by the maintainers of the alternative host or by someone with access to an intermediate network.

A.3 Scenarios Associated with User Confusion

A.3.1 Security Issues

A.3.1.1 Phishing

Similar to Pharming (described in Section 3.1.2.1 above), Phishing is a type of attack intended to obtain confidental information from a victim through social engineering. At the time of this report, Wikipeda[31] described Phishing as:

> "…a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well[1]. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures."

Phishing attacks depend, by their very nature, on user confusion. In order to be successful, the user must believe that they are providing information to a trusted party. As with Pharming attacks, the attacker will generally construct a website that is similar in appearance to a trusted website operated by the third party. The user is directed to the website through a means such as e-mail. In order to appear more legitimate, attackers will sometimes attempt to use a URL that appears to be associated with the third party. An attacker could conceivably use a domain name in a two-character SLD within .name in order to trick a user into thinking that the website was associated with the operator of the website within a ccTLD. For example, if there were a website famouswebsite.li, an attacker might register famouswebsite.li.name and create a page that looks very similar to the original web site at this domain. Users directed to this site might be fooled by the domain name in the URL into thinking that the attacker's site was legitimately associated with the famouswebsite.li domain and as a result be willing to provide confidential information (such as their famouswebsite.li password).

[31] http://en.wikipedia.org/wiki/Phishing

Appendix B: References

The members of the RSTEP panel that carried out the Security and Stability implications analysis searched relevant literature and network sources regarding technical problems relating to two-character second-level domain names (SLDs). It has not been an area of significant concern, and there is only a very small amount of prior information available on this subject.

It is not the intent of the review team to duplicate or restate any of the reports, analysis or guidelines provided by previous parties. However, as a service to the ICANN Board as it considers the GNR proposal and to members of the Internet community considering two character SLDs, the review team has collected and annotated the references that it found useful during its work in October, November, and December of 2006.

These references include the material that is specific to the GNR application for implementation of a new registry service. They also include references that are germane to the discussion of security and stability implications of adding two-character SLDs.

The review team has provided brief annotations on the material provided in this reference so that the reader may understand how the source material was used during the review team's work.

B.1 Material Specific to this Application

B.1.1 GNR Application to ICANN for New Registry Service

Document metadata:

- Dated: 2006-10-02
- Author: Global Name Registry, Limited
- Length: 15 pages (printed from Web page)
- URL: http://www.icann.org/registries/rsep/GNR_Proposal.pdf

This is the document that GNR sent to ICANN to request that a new registry service be approved. It contains a description of the service, how it will be implemented, the benefits proposed and a discussion of the contractual implications of the proposal. This document is in a standard format supplied by ICANN.

B.1.2 ICANN Notice of Referral to GNR

Document metadata:

- Dated: 2006-10-17
- Author: Patrick Jones

- Length: 2 pages
- URL: http://www.icann.org/registries/rsep/icann-to-gnr-17oct06.pdf

ICANN is required by its Registry Services Evaluation Policy to notify any applicant for new registry services if the application is to be referred to RSTEP. This process gives the applicant a chance to confirm that they wish to proceed with the process and discusses the process by which the review team will be selected.

B.1.3 GNR Response to ICANN

Document metadata:

- Dated: 2006-10-19
- Author: Håkon Haugnes
- Length: ~2 pages (E-mail without explicit pagination)
- URL: http://www.icann.org/registries/rsep/gnr-to-icann.htm

This letter states GNR's intent to continue with the New Registry Service process and asserts that: "RFC1535 is not specific to two-character domains or subdomains. It describes bad resolver behaviour, not normal resolver behavour"; "RFC1536, released at substantially the same time (in 1993), describes how to fix this bad resolver behaviour."; "The behaviour described in RFC1535 was fixed in release 4.9.2 of BIND in 1993"; "The BIND 4 resolver is officially deprecated"; "less than 0.02% of all resolvers use version BIND 4.8 or lower."; and "There are already far larger domains active on the Internet today, domains which would be affected and unstable if RFC1535 was a real issue. For example: li.com, ng.net, co.kr, name.com, name.de, com.au….."

B.1.4 Referral of GNR Request from ICANN to RSTEP

Document metadata:

- Dated: 2006-10-20
- Author: Patrick Jones
- Length: 9 pages
- URL: http://www.icann.org/registries/rsep/icann-to-rstep20oct06.pdf

This letter to the chair of the RSTEP provides notification that ICANN is going to use the 45-day process of technical evaluation for the GNR proposal. It outlines the timetable for the RSTEP process and provides the starting impetus for the technical evaluation.

B.1.5 DENIC Letter to ICANN

Document metadata:

- Dated: 2006-10-6
- Author: Stephan Welzel
- Length: 1 page

- URL: http://www.icann.org/registries/rsep/denic-to-icann-06oct06.pdf

This letter expresses DENIC's concern that "domain names following the model <TLD>.<TLD> (like de.name) cause technical problems as described in RFC 1535." They further state that "we did some checks on this the other day and found that these problems do still occur."

B.1.6 ICANN Public Comments on the GNR Proposal

Document metadata:

- Dated: October 20, 2006 through November 20, 2006.
- Author: Various postings from 9 separate authors
- Length: 10 separate forum postings
- URL: http://forum.icann.org/lists/gnr-proposal-comments

ICANN opened a public forum for comment on the GNR proposal on October 20, 2006. The public forum was open for a month and saw ten separate postings, two of which are from the same individual. Specific comments generally divided into two groups. The first group consisted of technical comments primarily citing RFC 1535. The second group consisted of non-technical points, which are outside the scope of this review. The members of the review team used the following abstract to help guide their reading of the public comments.

[#1] Stephen Hecker (http://forum.icann.org/lists/gnr-proposal-comments/msg00000.html) argues, in reference to spam, "Rather than increase the complexity (or length) of end user domain names, some thought should be put into ways to reduce this increasingly serious threat to the Internet." This comment has no technical content and is outside the scope of this review.

[#2] Guanghao Li (http://forum.icann.org/lists/gnr-proposal-comments/msg00001.html) states "We too have received requests from GNR about opening the two-character names, and we decided not to support this action. We are concerned that it may have negative impact on the DNS system and confuse users. We recommend that all ccTLDs' (or ISO 3166 list) two-character names should be remain reserved." However, no technical basis for this position is provided.

[#3] Jeremy Mathieux (http://forum.icann.org/lists/gnr-proposal-comments/msg00002.html) urges dropping the two-character reservation clause from all ICANN registry contracts for reasons, among others, of equal treatment and human rights. There were no significant technical arguments in this posting.

[#4] 'Jenny' (http://forum.icann.org/lists/gnr-proposal-comments/msg00003.html) would like to provide two-character names to customers, pointing out that two-character names in China are very common. There was no technical content in this posting.

[#5] Bob Steinbruckner (http://forum.icann.org/lists/gnr-proposal-comments/msg00010.html) advocates release of 2-character names, saying that people should not be restricted from registering due to the length of their names. This posting had no technical content.

[#6] Thorsten Smeets (http://forum.icann.org/lists/gnr-proposal-comments/msg00009.html) makes an argument similar to that of Bob Steinbruckner, adding that shared second level names are not new.

[#7] Marilyn Cade (http://forum.icann.org/lists/gnr-proposal-comments/msg00007.html) makes an extensive posting summarized by her statements: "I ask that ICANN not approve the proposal by .name registry until there is further discussion and consideration of the political and public policy issues that are involved in the question of the use of two-character names/otherwise known as 'two letter names'." and "ICANN should not be addressing the use of two letter names in a 'one off' manner….." Her posting included no technical arguments.

[#8] Tommy Ho (http://forum.icann.org/lists/gnr-proposal-comments/msg00006.html) supports GNR's proposal, arguing that two-character SLDs provide a value to persons with two-character surnames, such as himself. There was no technical content in this posting.

[#9] Håkon Haugnes (http://forum.icann.org/lists/gnr-proposal-comments/msg00012.html) makes a lengthy reply to Marilyn Cade, making points seen in the GNR proposal (including technical points), and also stating that, since .name is unique, a general 2-character SLD policy is not required and that there will be no 'landrush' for SLDs since they will not be released. In a second posting (http://forum.icann.org/lists/gnr-proposal-comments/msg00011.html), he again argues that it is "right and fair" that these names should be available to individuals worldwide.

B.1.7 Current .name TLD Registry Agreement

On 1 August 2001, ICANN and Global Name Registry entered into an Unsponsored TLD Agreement under which Global Name Registry operates the .name top-level domain. The agreement and the appendices were examined by the review team during its evaluation of the proposed Registry Service. The registry agreement can be found at http://www.icann.org/tlds/agreements/name

B.2 Supporting Material and Reports

In addition to the documents directly related to GNR’s proposal, the RSTEP review team made use of other existing reference materials and reports. Since two-character SLDs have been of only limited interest in the past, only a small body of material was available for the review team to consider in tandem with the request materials.

What follows is a summary of the public materials that this RSTEP review team used during its consideration of GNRs proposal. This list is not exhaustive since the RSTEP review team was able to take advantage of materials not in the public domain and materials subject to non-disclosure.

B.2.1 RFC 1535, A Security Problem and Proposed Correction With Widely Deployed DNS Software

Document metadata:

- Dated: 1993-10
- Author: Ehud Gavron
- Length: 5 pages
- URL: http://www.ietf.org/rfc/rfc1535.txt

This document discusses a flaw in some of the name resolver clients in distribution in 1993. The flaw exposes a security weakness related to the search heuristic invoked by these same resolvers when users provide a partial domain name, and which is easy to exploit (although not by the masses). This document points out the flaw, a case in point, and a solution.

B.2.2 RFC 1536, Common DNS Implementation Errors and Suggested Fixes

Document metadata:

- Dated: 1993-10
- Author: Anant Kumar, et al
- Length: 12 pages
- URL: http://tools.ietf.org/html/rfc1536

This memo describes common errors seen in DNS implementations in use in 1993 and suggests some fixes. Where applicable, violations of recommendations from STD 13, RFC 1034 and STD 13, RFC 1035 are mentioned. The memo also describes, where relevant, the algorithms followed in BIND (versions 4.8.3 and 4.9 which the authors referred to) to serve as an example.

B.2.3 Known Problems with the DNS

Document metadata:

- Dated: 2006-10-3

- Author: Duane Wessels, The Measurement Factory/CAIDA
- Length: 41 pages
- URL: http://www.ripe.net/ripe/meetings/ripe-53/presentations/whats_wrong_with_dns.pdf

A recent overview of most well known problems with the DNS system can be found in this presentation. It shows 32 known problems, of which only 2 are correlated to the existence of <TLD>.TLD names. It also states that these can be easily avoided.

B.2.4 Governmental Advisory Committee - Communique

Document metadata:

- Dated: 2000-3-8
- Author: Government Advisory Committee
- Length: 1 page
- URL: http://gac.icann.org/web/communiques/gac5com.htm

The source of the request for the reservation of ISO 3166-1 2-letter codes in gTLDs can be seen in the communique from the Governmental Advisory Committee Meetings in Cairo, 7-8 March 2000. The communique did not cite any technical basis for the request.