THE DOMAIN NAME INDUSTRY BRIEF

VOLUME 12 – ISSUE 1 – MARCH 2015

THE VERISIGN DOMAIN REPORT

AS A GLOBAL LEADER IN DOMAIN NAMES AND INTERNET SECURITY, VERISIGN REVIEWS THE STATE OF THE DOMAIN NAME INDUSTRY THROUGH A VARIETY OF STATISTICAL AND ANALYTICAL RESEARCH. VERISIGN PROVIDES THIS BRIEFING TO HIGHLIGHT IMPORTANT TRENDS IN DOMAIN NAME REGISTRATIONS, INCLUDING KEY PERFORMANCE INDICATORS AND GROWTH OPPORTUNITIES, TO INDUSTRY ANALYSTS, MEDIA AND BUSINESSES.

VERISIGN®

EXECUTIVE SUMMARY

The fourth quarter of 2014 closed with a base of 288 million domain name registrations across all top-level domains (TLDs), an increase of four million domain names, or 1.3 percent over the third quarter of 2014. Registrations have grown by 16.9 million, or 6.2 percent, year over year.[1]

Total country-code TLD (ccTLD) registrations were 134.0 million domain names, a 1.5 percent increase quarter over quarter, and an 8.7 percent increase year over year.

The .com and .net TLDs experienced aggregate growth, reaching a combined total of approximately 130.6 million domain names in the domain name base[2] in the fourth quarter of 2014. This represents a 2.7 percent increase year over year. As of Dec. 31, 2014, the base of registered names in .com equaled 115.6 million names, while .net equaled 15.0 million names.

New .com and .net registrations totaled 8.2 million during the fourth quarter of 2014. In the fourth quarter of 2013, new .com and .net registrations totaled 8.2 million.

The order of the top TLDs in terms of zone size changed slightly when compared to the third quarter, as .nl (Netherlands) moved up a ranking from the tenth-largest TLD to the ninth-largest TLD, resulting in .info moving down one ranking to the tenth-largest TLD. All other TLDs in the top 10 maintained their rankings.

At of the end of 2014, around

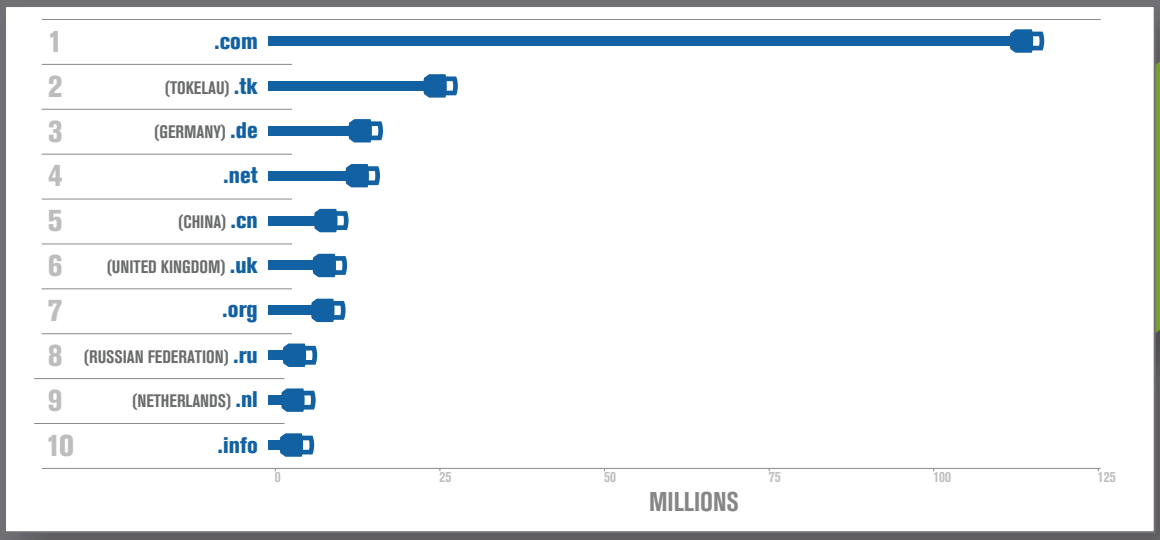
40

PERCENT

of the world population was connected to the Internet. In 1995, it was less than 1%.[4]

LARGEST TLDs BY ZONE SIZE

Source: Zooknic, Q4 2014; Verisign, Q4 2014; Centralized Zone Data Service, Q4 2014



The largest TLDs in order by zone size were .com, .tk (Tokelau), .de (Germany), .net, .cn (China), .uk (United Kingdom), .org, .ru (Russian Federation), .nl (Netherlands) and .info.[3]

1 The gTLD and ccTLD data cited in this report are estimates as of the time this report was developed, and is subject to change as more complete data is received. Totals include ccTLD Internationalized Domain Names.

2 Per the Verisign Q42014 Earnings announcement, starting in Q12015, the term "domain name base" will be defined as "the domain names that resolve in the zone, the domain names that are requested to be not configured for use in the top-level domain zone filed by the registrant, and those domain names on hold status.

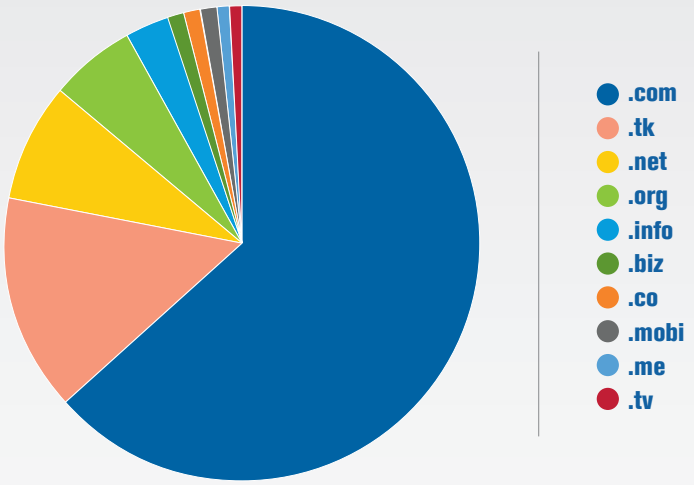
3 tk is a free ccTLD that provides free domain names to individuals and businesses. Revenue is generated by monetizing expired domain names. Domain names no longer in use by the registrant or expired are taken back by the registry and the residual traffic is sold to advertising networks. As such, there are no deleted .tk domain names. http://www.businesswire.com/news/home/20131216006048/en/Freenom-Closes-3M-Series-Funding#.UxeUGNJDv9s

4 http://www.internetlivestats.com/internet-users/

gTLD BREAKDOWN BY ZONE SIZE[5]

Largest gTLDs and ccTLDs Marketed as gTLDs by Zone Size

Source: Zooknic, Q4 2014; Verisign, Q4 2014; Centralized Zone Data Service, Q4 2014



Belgium had the highest IPv6 adoption rate

30.5
PERCENT
at the end of 2014.[7]

Some ccTLDs, including .tk, .co, .me and .tv are frequently used by registrants and treated by search engines as gTLDs.[6] This chart ranks the zone size of both gTLDs and ccTLDs marketed as gTLDs, as of Dec. 31, 2014, with that classification taken into account. The top 10 largest gTLDs and ccTLDs marketed as gTLDs by zone size were .com, .tk, .net, .org, .info, .biz, .co, .mobi, .me and .tv, as of Dec. 31, 2014, which account for 180.6 million domain name registrations, or 62.8 percent of the total global domain name registrations.

The top reported aftermarket domain sale in 2014 was z.com, at

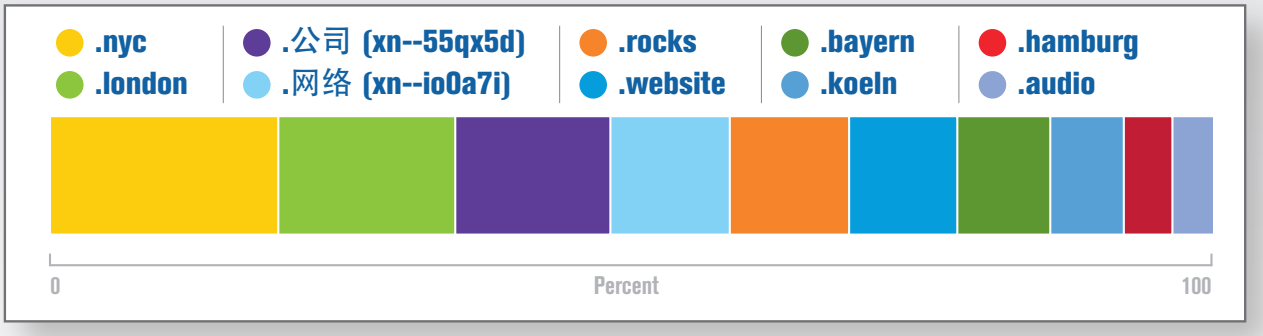
$6.78
MILLION USD[8]

70
PERCENT
of consumers did their online shopping primarily on smartphones and tablets in the home stretch of the 2014 holiday shopping season.[9]

5 The total number of gTLDs and their registrations is published through the Centralized Zone Data Service. https://czds.icann.org/en
6 Google geotargetable domains. https://support.google.com/webmasters/answer/1347922?hl=en
7 https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption
8 http://www.dnjournal.com/archive/domainsales/2014/2014-top-100--sales-charts.htm
9 http://www.fluentco.com/the-fluent-2014-post-holiday-survey/

Largest New gTLDs Reaching Day 60 of General Availability in Q4, by Zone Size at Quarter's End

Source: Centralized Zone Data Service, Q4 2014



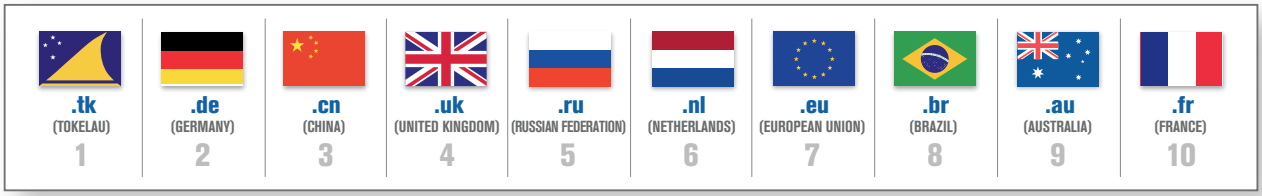
At the end of the fourth quarter of 2014, 478 new gTLDs were delegated into the root; 65 of which were delegated during the fourth quarter of 2014. New gTLD registrations totaled 3.6 million, or 2.3 percent of total gTLD registrations.[10]

The above chart captures the initial 60-day registration volume rank for those new gTLDs reaching 60 days of General Availability (GA) during the quarter. In the fourth quarter of 2014, 78 new gTLDs reached 60 days of General Availability; of those, the 10 largest new gTLDs, as measured by zone size at the end of the quarter, were .nyc, .london, .公司 (xn--55qx5d) (Chinese for "company"), .网络 (xn--io0a7i) (Chinese for "network"), .rocks, .website, .bayern, .koeln, .hamburg and .audio.[11]

ccTLD BREAKDOWN BY ZONE SIZE

Top 10 ccTLDs by Zone Size

Source: Zooknic, Q4 2014
For further information on the Domain Name Industry Brief methodology, please refer to the last page of this report.



Total ccTLD registrations were approximately 134.0 million in the fourth quarter of 2014, with the addition of 1.9 million domain names, or a 1.5 percent increase compared to the third quarter of 2014. This is an increase of approximately 10.8 million domain names, or 8.7 percent, year over year. Without including .tk, ccTLD quarter-over-quarter growth was 0.8 percent and year-over-year growth was 4.0 percent.

Among the 10 largest ccTLDs, .tk grew the fastest, with 4.0 percent overall quarter-over-quarter growth.

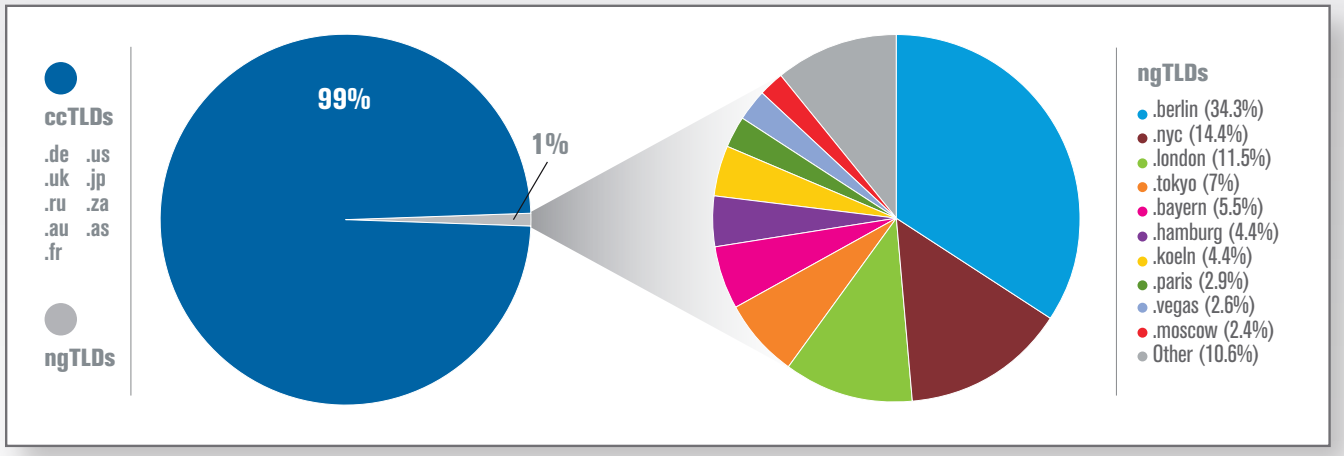
As of Dec. 31, 2014, there were 285 global ccTLD extensions delegated in the root (including Internationalized Domain Names), with the top 10 ccTLDs composing 67.2 percent of all ccTLD registrations.

10 The number of delegated new gTLDs is published by ICANN. http://newgtlds.icann.org//en/program-status/delegated-strings
11 The new gTLDs that reached 60 days of General Availability during the fourth quarter was determined using: http://ntldstats.com/launch?orderby=start&orderdir=asc&filterby=start&start=2014-02-01&end=2014-05-01&tld=&filter%5B%5D=4

Geographical New gTLDs as Percentage of Total Comparable Geographical gTLDs

Source: Centralized Zone Data Service, Q4 2014

Among the geographical new gTLDs that have been delegated, 22 have had more than 1,000 registrations since entering GA, as of the end of the fourth quarter of 2014. The following charts summarize approximate Q4 geographic new gTLD registrations as a percentage of total geographic gTLD registrations (ccTLD and ngTLDs combined):

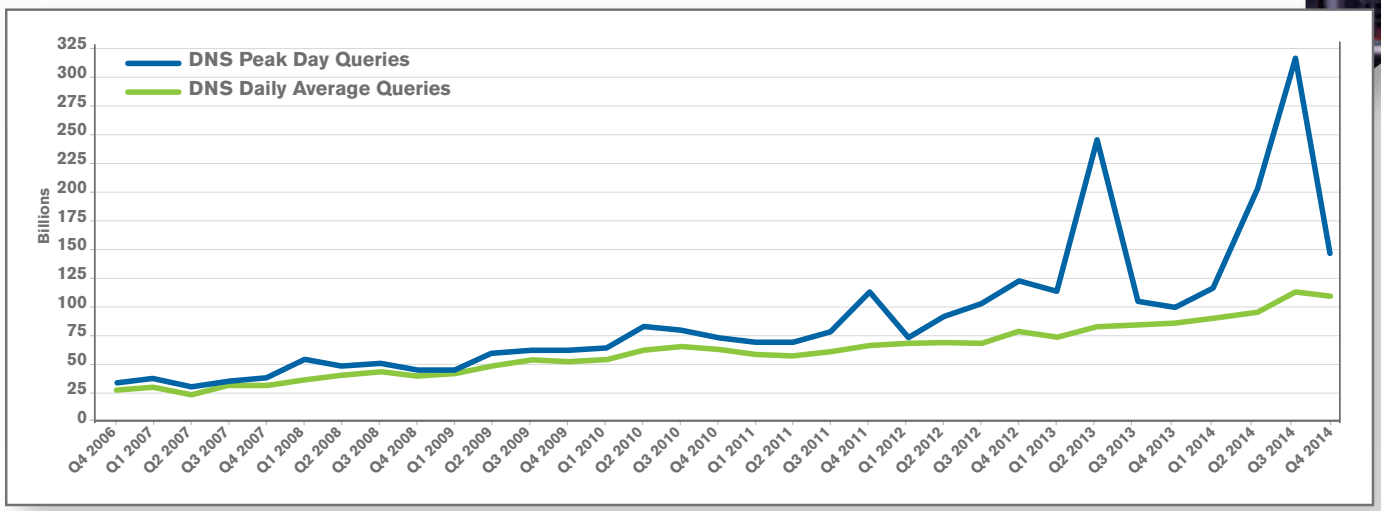


DNS QUERY LOAD

During the fourth quarter of 2014, Verisign's average daily Domain Name System (DNS) query load was 110 billion across all TLDs operated by Verisign, with a peak of 146 billion. Compared to the previous quarter, the daily average decreased 3.7 percent and the peak decreased 54.0 percent. Year over year, the daily average increased 33.5 percent and the peak increased 47.1 percent.

DNS Query Load by Quarter

Q4 2006 – Q4 2014



FEATURED ARTICLE

UNDERSTANDING AND ENABLING THE FULL BENEFITS OF DNSSEC

The Domain Name System (DNS) enables nearly all Internet transactions today. Its operation and inherent systemic dependencies are critical yet commonly overlooked when calculating an organization's attack surface and conducting risk management and mitigation activities. Understanding the implications of the DNS control plane and the full benefits of DNS Security Extensions (DNSSEC) can help to minimize your attack surface and enhance your security posture.

In mid-2008, new attack techniques were discovered that have made DNS cache poisoning much easier to adversaries. The new attack vectors permitted an adversary to redirect clients that used the DNS to servers of their choosing. The ease of remote exploitation of this vulnerability super-charged the adoption of DNSSEC because DNSSEC was specifically designed to mitigate cache poisoning attacks. DNSSEC's design accomplishes this by adding incrementally deployable authentication and object-level integrity validation functions to the DNS.

Established top-level domains (TLDs) such as .com, .net and .gov have been DNSSEC-enabled for many years, as well as the root, which was fully DNSSEC-enabled nearly half a decade ago, in July of 2010. However, DNSSEC has recently become operationally relevant, with over 75 percent of all TLDs being DNSSEC-enabled. Further, with the rapid introduction of a large number of new gTLDs in the root zone last year and by requiring that new gTLDs be DNSSEC-enabled out of the gate, considerable thrust was provided to the global rollout.

DNSSEC, however, provides more than a single advantage. While cache poisoning is the most evangelized problem that it helps resolve, there are an array of other benefits that DNSSEC provides, which range from obvious to more nuanced. For example, one of the more interesting, but under-marketed benefits of DNSSEC is its ability to address issues with transitive trust and ever-expanding attack surfaces in the DNS. The term "transitive trust" refers to the fact that, when a single DNS zone is accessed, a web of other zones (TLDs and others) supports that access and must also be trusted. The larger this web of other servers, the larger the attack surface.

In a nutshell, the two key components of DNSSEC encompass DNSSEC enablement at the authoritative level of the DNS (e.g., at a TLD registry), and the validation of that DNSSEC information by DNS resolvers (e.g., a validating recursive name server). Typically, people focus on the role of DNSSEC enablement at the authoritative level (e.g., the 75 percent of TLDs mentioned above). The utility of this component (alone) is essentially like installing a tamper-resistant seal on a bottle; making it visibly obvious if someone has opened the bottle (and possibly tainted its contents) after having been produced and packaged at the source. If the seal weren't there, any distributor or other party in the distribution path could taint the contents prior to receipt and consumption by a consumer. As such, the consumer must take action to verify that the seal has not been tampered with in order for the safeguard to be of benefit. In the DNS, validation of that DNSSEC information by resolvers must occur for the benefits of DNSSEC to be fully realized.

At each level of the DNS, including the root, names that belong to the same operational entity are called zones. Each zone is served by a set of authoritative name servers, but for ease of operation, zones are often configured at, and maintained by, a single master authoritative name server and one or more secondary authoritative name servers (which simply serve the zone contents that the master server has specified). While all authoritative name servers for a zone (e.g., example.com) can distribute responses with authority for the zone, the zone file is normally produced and distributed to the other servers via the master authoritative name server. Just as is the case with the seal protecting the contents of the bottle, DNSSEC allows consumers to know that the contents that are authored at a master name server have not been tampered with on a secondary authoritative name server or an intermediate system such as a recursive DNS resolver. However, it's important to recognize that this creates a dependency on the master server for accurate, uncontaminated DNSSEC information that must be preserved through secondary name servers and the rest of the DNS system.

In order to calculate the transitive trust for a given zone and get an idea of the number of potential systems that could be attacked in order to affect a given Internet DNS presence, one

must look at all the authoritative name servers for the zone in question, as well as for any parent zones (e.g., the TLD or root zone), as well as all other zones that enable those servers.

Let's look at example.com, a second-level domain (SLD) operated by the Internet Corporation for Assigned Names and Numbers (ICANN), to illustrate this. At the second level, there are only four authoritative name server delegations within .com for example.com ([a-c].iana-servers.net and ns.icann.org) and the attack surface calculation would certainly include those four named servers. However, one must also consider all the other servers that help enable resolution. Because example.com is within .com, all the .com authoritative name servers (13 named servers, [a-m].gtld-servers.net) must be considered, as well as all the root name servers (13 named servers, [a-m].root-servers.net).

Additionally, because three of the authoritative servers for example.com reside within .net, all of the .net name servers must be included – fortunately, .com and .net are operated on the same 13 named servers, so additional servers are not actually added. However, the fourth authoritative name server, ns.icann.org, is within .org, so six .org authoritative named servers need to be included. But wait, because three of the six authoritative name servers in .org are located within .info, the .info name servers must be added, and so on for the corresponding second- and third-level domains of those servers, until the fully qualified domain names (FQDNs) of each named server are resolved.

Each of these names is associated with one or more IPv4 addresses (A records) and/or one or more IPv6 addresses (AAAA records), each of which may reside in different autonomous systems (ASes) / networks as well. All told, example.com's transitive trust graph includes 62 named nodes, 54 unique IPv4 addresses and 35 unique IPv6 addresses, all distributed across 30 different ASes. That's a lot of points for potential compromise without the added object-level security DNSSEC provides. Verisign Labs has developed a Transitive Trust and DNS Dependency Graph Portal[12] openly available for anyone to plot transitive trust graphs to see what the DNS transitive trust plot for any domain name looks like, and subsequently, to help understand and manage its attack surface. It's important to note that the tool does not include anycasted instances of a given IP address or name, and it also doesn't reflect geographical location data of the nodes in question (See Operational Implications of the DNS Control Plane as it relates to transitive trust for more detail on the topic), so things like resiliency aren't accurately reflected.

By simply enabling DNSSEC within a given zone, object-level integrity protection is achieved, effectively shrinking that zone's integrity attack surface from all the authorities in the zone (i.e., the 13 root name servers and all the hundreds of anycasted instances) to the single master publication point (e.g., where the root zone is periodically minted and distributed to all the other root servers). To fully protect a given domain, you would need to ensure DNSSEC is enabled for every zone within your transitive trust graph, but that's perfectly feasible in today's environment, and this information should be readily available.

Now, as discussed above, the other thing that needs to be done is to ensure that folks are using the integrity information that's being published with the zone to validate the integrity of the responses they receive, which mostly just means enabling DNSSEC validation on recursive name servers, or using name servers that have it enabled already. For example, Verisign's open recursive name servers perform DNSSEC validation by default, as well as those operated by Comcast and Google.[13] Even U.S. federal government regulations call for both DNSSEC signing of .gov zones and DNSSEC validation for Internet names.

With this in mind, we recommend that all domain holders / registrants consider the implications of transitive trust and the DNS control plane on your attack surface, and consider how DNSSEC protections will add another layer of defense to your Internet presence. Furthermore, you need to ensure that your recursive name servers are performing DNSSEC validation, leveraging the work that's been done to fortify the DNS in order to ensure the responses you receive from the DNS are the ones that were intended by the domain administrator.

12 http://trans-trust.verisignlabs.com/
13 For more information on Verisign's Recursive DNS Service, please visit http://www.verisigninc.com/en_US/website-availability/recursive-dns/index.xhtml.

LEARN MORE

To subscribe to or access the archives for the Domain Name Industry Brief, please go to VerisignInc.com/DNIB. Email your comments or questions to domainbrief@verisign.com.

ABOUT VERISIGN

Verisign, a global leader in domain names and Internet security, enables Internet navigation for many of the world's most recognized domain names and provides protection for websites and enterprises around the world. Verisign ensures the security, stability and resiliency of key Internet infrastructure and services, including the .com and .net domains and two of the Internet's root servers, as well as performs the root-zone maintainer functions for the core of the Internet's Domain Name System (DNS). Verisign's Network Intelligence and Availability services include intelligence-driven Distributed Denial of Service Protection, iDefense Security Intelligence and Managed DNS. To learn more about what it means to be Powered by Verisign, please visit VerisignInc.com.

METHODOLOGY

The data presented in this report for ccTLDs, including quarter-over-quarter and year-over-year metrics, reflects the information available to Verisign at the time of this report and may incorporate changes and adjustments to previously reported periods based on additional information received since the date of such prior reports, so as to more accurately reflect the growth rate of the ccTLDs. In addition, the data available for this report may not include data for the 283 ccTLD extensions that are delegated to the root, and includes only the data available at the time of the preparation of this report.

For gTLD and ccTLD data cited with Zooknic as a source, the Zooknic analysis uses a comparison of domain name root zone file changes supplemented with Whois data on a statistical sample of domain names which lists the registrar responsible for a particular domain name and the location of the registrant. The data has a margin of error based on the sample size and market size. The ccTLD data is based on analysis of root zone files. For more information, see ZookNIC.com. Information on or accessible through this website is not part of this report.

The Internet Corporation for Assigned Names and Numbers' IDN ccTLD Fast Track Process enables countries and territories that use languages based on scripts other than Latin to offer users domain names in non-Latin characters. The first quarter of 2012 was the first quarter that Verisign reported on the IDN ccTLDs which were delegated in the root zone at that time.

Recognizing that this growth did not all occur in the first quarter of 2012, the changes in domain name registrations for each new TLD were phased in beginning with the quarter that the IDN.IDN variants were initially launched, in order to more closely model the changes in the worldwide domain name growth. Following the initial launch, the quarterly growth rate for previous TLD launches was applied to determine the domain base. These adjustments resulted in a growth curve for each TLD that is typical of historic TLD introduction lifecycles.

INDUSTRY EVENTS

Upcoming industry events through June 30, 2015:

- IETF 92: March 22-27, 2015, Dallas
- Domaining Europe: April 23-25, 2015, Valencia, Spain
- ICANN 53: June 21-25, Buenos Aires, Argentina

Statements in this announcement other than historical data and information constitute forward-looking statements within the meaning of Section 27A of the Securities Act of 1933 as amended and Section 21E of the Securities Exchange Act of 1934 as amended. These statements involve risks and uncertainties that could cause our actual results to differ materially from those stated or implied by such forward-looking statements. The potential risks and uncertainties include, among others, the uncertainty of the impact of the U.S. government's transition of key Internet domain name functions [the Internet Assigned Numbers Authority ("IANA") function], whether the U.S. Department of Commerce will approve any exercise by us of our right to increase the price per .com domain name, under certain circumstances, the uncertainty of whether we will be able to demonstrate to the U.S. Department of Commerce that market conditions warrant removal of the pricing restrictions on .com domain names and the uncertainty of whether we will experience other negative changes to our pricing terms; the failure to renew key agreements on similar terms, or at all; the uncertainty of future revenue and profitability and potential fluctuations in quarterly operating results due to such factors as restrictions on increasing prices under the .com Registry Agreement, changes in marketing and advertising practices, including those of third-party registrars, increasing competition, and pricing pressure from competing services offered at prices below our prices; changes in search engine algorithms and advertising payment practices; the uncertainty of whether we will successfully develop and market new products and services, the uncertainty of whether our new products and services, if any, will achieve market acceptance or result in any revenues; challenging global economic conditions; challenges of ongoing changes to Internet governance and administration; the outcome of legal or other challenges resulting from our activities or the activities of registrars or registrants, or litigation generally; the uncertainty regarding what the ultimate outcome or amount of benefit we receive, if any, from the worthless stock deduction will be; new or existing governmental laws and regulations; changes in customer behavior, Internet platforms and web-browsing patterns; system interruptions; security breaches; attacks on the Internet by hackers, viruses, or intentional acts of vandalism; whether we will be able to continue to expand our infrastructure to meet demand; the uncertainty of the expense and timing of requests for indemnification, if any, relating to completed divestitures; and the impact of the introduction of new gTLDs, any delays in their introduction, the impact of ICANN's Registry Agreement for new gTLDs, and whether our new gTLDs or the new gTLDs for which we have contracted to provide back-end registry services will be successful; and the uncertainty regarding the impact, if any, of the delegation into the root zone of over 1,300 new gTLDs. More information about potential factors that could affect our business and financial results is included in our filings with the SEC, including in our Annual Report on Form 10-K for the year ended Dec. 31, 2014, Quarterly Reports on Form 10-Q and Current Reports on Form 8-K. Verisign undertakes no obligation to update any of the forward-looking statements after the date of this announcement.