VERISIGN™


# THE DOMAIN NAME INDUSTRY BRIEF

VOLUME 9 - ISSUE 2 - JULY 2012

## THE VERISIGN DOMAIN REPORT

AS THE GLOBAL REGISTRY OPERATOR FOR .COM AND .NET, VERISIGN REVIEWS THE STATE OF THE DOMAIN NAME INDUSTRY THROUGH A VARIETY OF STATISTICAL AND ANALYTICAL RESEARCH. AS THE TRUSTED PROVIDER OF INTERNET INFRASTRUCTURE SERVICES FOR THE NETWORKED WORLD, VERISIGN PROVIDES THIS BRIEFING TO HIGHLIGHT IMPORTANT TRENDS IN DOMAIN NAME REGISTRATION, INCLUDING KEY PERFORMANCE INDICATORS AND GROWTH OPPORTUNITIES, TO INDUSTRY ANALYSTS, MEDIA AND BUSINESSES.

VERISIGN™

## EXECUTIVE SUMMARY

The first quarter of 2012 closed with a base of more than 233 million domain name registrations across all Top-Level Domains (TLDs), an increase of 7.5 million domain names, or 3.3 percent, over the fourth quarter of 2011. Registrations have grown by 23 million, or 11 percent, since the first quarter of 2011.[1, 2]

The base of Country Code Top-Level Domains (ccTLDs) was 94.9 million domain names, a 4.8 percent increase quarter over quarter, and a 16.2 percent increase year over year in the base.[1, 2]

In the first quarter of 2012, Verisign began tracking the ccTLDs launched by ICANN through the IDN ccTLD Fast Track Process, which enabled countries and territories that use languages based on scripts other than Latin to offer users domain names in non-Latin characters. This additional tracking resulted in an additional 808,967 ccTLD names being reported in the first quarter that were not previously reported in prior periods. For further information on the Domain Name Industry Brief methodology, please refer to page 6 of the report.

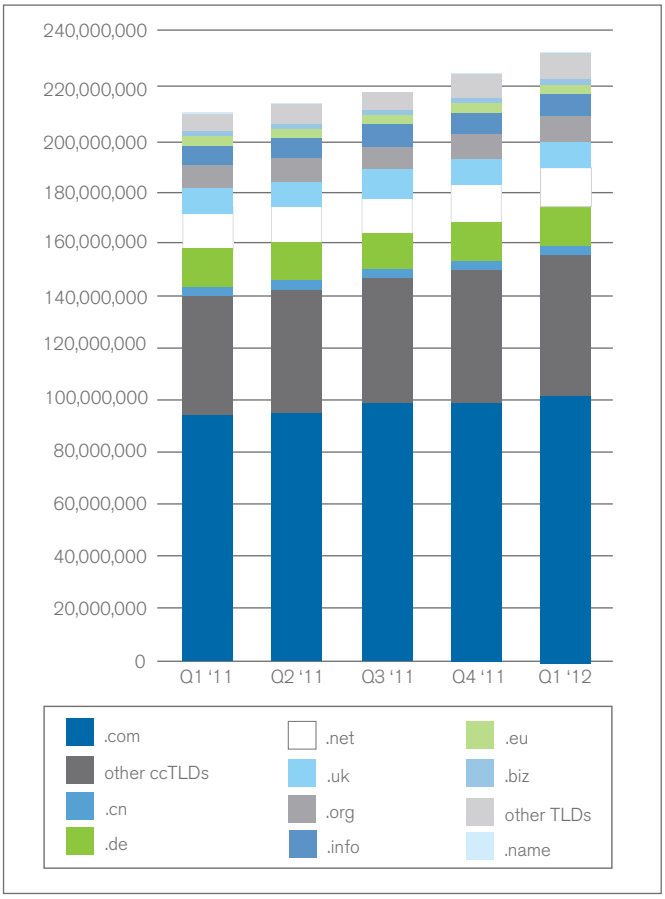
The .com and .net TLDs experienced aggregate growth, reaching a combined total of approximately 116.7 million domain names in the adjusted zone in the first quarter of 2012. This represents a 2.5 percent increase in the base over the fourth quarter of 2011 and an 8.1 percent increase over the first quarter of 2011. The .com registry also grew to more than 100 million domain names during the quarter.

New .com and .net registrations totaled 8.9 million during the first quarter of 2012. This reflects a 7.7 percent year-over-year increase in new registrations, and a 13.2 percent increase in new registrations from the fourth quarter.

The order of the top TLDs in terms of zone size did not change when compared to the fourth quarter. The largest TLDs in terms of base size were, in order, .com, .de (Germany), .net, .uk (United Kingdom), .org, .info, .tk (Tokelau), .nl (Netherlands), .ru (Russian Federation) and .eu (European Union).

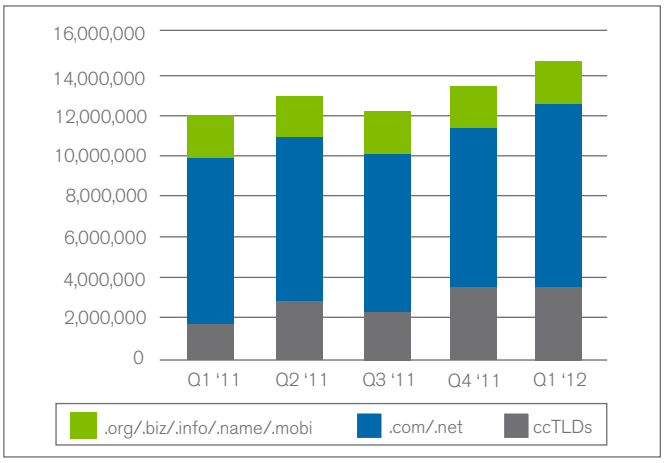
### Total Domain Name Registrations

Source: Zooknic, April 2012; Verisign, April 2012




### New Registration Growth

Source: Zooknic, April 2012; Verisign, April 2012; ICANN Monthly Reports






1 The gTLD and ccTLD data cited in this report are estimates as of the time of this report and subject to change as more complete data is received.
2 Total includes additional tracking of ccTLD internationalized domain names.

## CCTLD BREAKDOWN OF ZONE SIZE

Total ccTLD registrations were approximately 94.9 million in the first quarter of 2012 with the addition of 4.3 million domain names, or a 4.8 percent increase compared to the fourth quarter. This is an increase of approximately 13.2 million domain names, or 16.2 percent from a year ago.

Among the 20 largest ccTLDs, Tokelau, France, India, the Republic of Korea and the Russian Federation each exceeded 4 percent quarter-over-quarter growth. Last quarter, four of the top 20 exceeded the same threshold.

There are more than 290 ccTLD extensions globally (including Internationalized Domain Names), with the top 10 ccTLDs comprising 60 percent of all registrations.

### Top ccTLD Registries by Domain Name Base, First Quarter 2012

Source: Zooknic, April 2012

| | | | | | |
|---|---|---|---|---|---|
| 1. | .de | (Germany) | 6. | .eu | (European Union) |
| 2. | .uk | (United Kingdom) | 7. | .cn | (China) |
| 3. | .tk | (Tokelau) | 8. | .br | (Brazil) |
| 4. | .nl | (Netherlands) | 9. | .ar | (Argentina) |
| 5. | .ru | (Russian Federation) | 10. | .au | (Australia) |

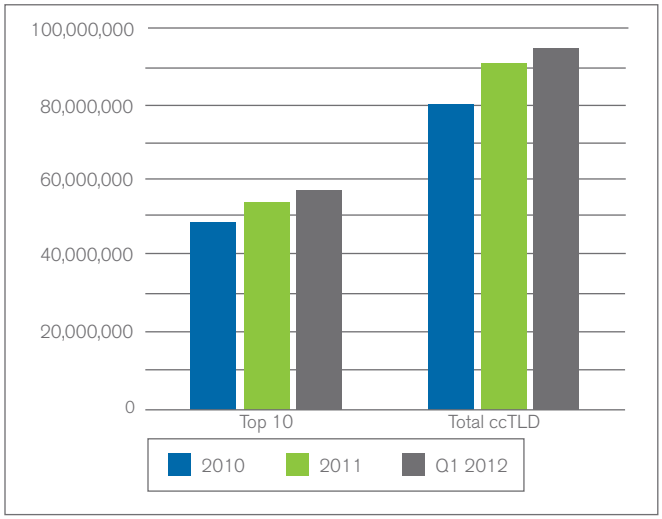
## .COM/.NET DYNAMICS

The .com/.net renewal rate for the first quarter of 2012 was 73.9 percent, up from 73.5 percent for the fourth quarter. Renewal rates vary quarter over quarter based on the composition of the expiring name base and the contribution of specific registrars.

Whether a domain name resolves to a website is a key factor in determining the renewal rate since domain names that resolve to websites are more likely to be renewed. Verisign estimates that 88 percent of .com and .net domain names resolve to a website, meaning that an end user visiting that domain name would find a website. These websites can be further described as those having multiple pages or as one-page websites. One-page websites include under-construction, brochure-ware and parked pages in addition to online advertising revenue-generating parked pages.

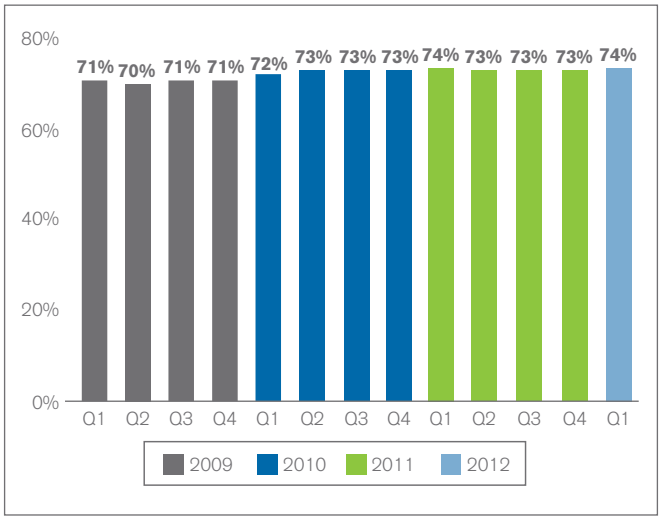
### ccTLD Breakdown

Source: Zooknic, April 2012
For further information on the Domain Name Industry Brief methodology, please refer to the page six of the report.



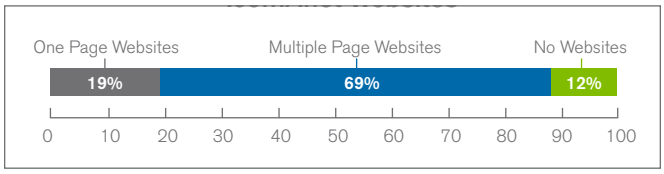

### .com/.net Registry Renewal Rates

Source: Verisign, April 2012



### .com/.net Websites

Source: Verisign, April 2012




Verisign's average daily Domain Name System (DNS) query load during the first quarter of 2012 was 66 billion, with a peak of 74 billion. Compared to the previous quarter, the daily average increased 4 percent and the peak decreased 37 percent. Year over year, the daily average increased 16 percent and the peak increased 10 percent.

## IPV6 AND SECURITY

On June 6, 2012, more than 2,000 websites, ISPs, and home router vendors from more than 100 countries around the globe marked their commitment to move to a global IPv6-enabled Internet by turning on their IPv6 capabilities permanently. Known as World IPv6 Launch, this event marked a major milestone in Internet history as IPv6 is critical for the continued growth and innovation of the Internet.

The benefits of IPv6 have been well documented. As almost all available IPv4 addresses within the Internet Assigned Numbers Authority (IANA) block have been depleted, and Regional Internet Registries (RIRs) will begin to exhaust their IPv4 address pools at varying rates in the near future, this should provide the impetus for widespread adoption of IPv6. Coupled with the continued deployment of DNS Security Extensions (DNSSEC), IPv6 should ultimately provide the stable and secure base for the next generation of Internet evolution.

Responsibility for making that happen lies among all Internet stakeholders. To support a smooth IPv6 transition, everyone from infrastructure operators and service providers to application developers and users will have to work together to support and develop IPv6 capabilities by debugging issues with new software and applications that are IPv6 only, and refining interworking and transitional co-existence with IPv4. But most importantly, Internet stakeholders should focus on security.

IPv6 presents an interesting security paradox. The capabilities IPv6 provides will enhance online security, but they may also present risks if not properly managed.

Historically, security was largely an afterthought for the early Internet, as its primary purpose was to facilitate open, end-to-end, any-to-any communications and information exchange for bridging and accelerating research efforts. Today, we have a much more complex Internet ecosystem that spans billions of users and devices across the globe and serves not only as an engine for e-commerce, but as an engine for all commerce.

In addition to being the de facto standard for global Internet services and consumers, the Internet protocol suite also serves as a near ubiquitous substrate for running critical network infrastructure and applications: Transportation, financial systems, emergency services, utilities and government applications are just a few examples of services that need absolute availability and robust security.

At the micro level, the migration of personally identifiable information (PII) and proprietary intellectual property online has influenced IPv6 protocol architects to include additional security mechanisms natively. However, if network operators do not properly manage IPv6 – and recognize that it's enabled "out of the box" in most devices today – this will have a substantial impact on their security posture. One of the biggest, but arguably easiest to remedy, pitfalls is that an increasing array of networking equipment and end systems today are shipped with IPv6 enabled by default. This would be ideal in an Internet environment with no bad actors, however, if network administrators are not ready for IPv6 in their operating environments, from a security and operational perspective, then they will need to either disable IPv6 entirely or deploy it in a very calculated manner.

VERISIGN™

### Key Security Considerations

As an industry, we have already observed IPv6 being used to compromise systems "under the radar" of IPv4-only sensors, and several organizations have reported IPv6 being expressly enabled by miscreants in order to ex-filtrate data, facilitate malware propagation, and enable distributed denial of service (DDoS) attacks. Other security considerations include:

- Translating IPv4 to IPv6 (because it will take some time before all systems are running on IPv6) itself can be a pitfall. Because IPv4 and IPv6 are not perfectly compatible, translating traffic from IPv4 to IPv6 will inevitably result in intermediate nodes mediating transactions as they move through the network. During that process, an opportunity might arise for a poor implementation or a bad actor to trigger or exploit a potential vulnerability.
- Unlike IPv4's variable header size, IPv6 has a 40-byte fixed header, but introduces add-on "extension headers" that may be chained and require complex processing by various systems. Such processing could overwhelm firewalls and security gateways. It could even introduce router forwarding performance degradation and be a potential vector for DDoS and other attacks.
- During a long period of "transitional coexistence," IPv6 adoption may require large network address translation, protocol translation devices, end system or intermediate translation devices and protocols. But these devices complicate the network and operations, and could break useful functions like geo-location or tools that security administrators use to identify and mitigate malicious network behaviors (e.g., blacklists and traffic filters).
- Because of IPv6's sparse address space, active scanning of infrastructure for unauthorized or vulnerable systems is much more complex than with IPv4. These capabilities need to be augmented with network access controls and active measurement systems that trigger vulnerability scanning of active systems once access has been granted.
- While IPSec is mandatory to implement in IPv6, it is not mandatory to use and continues to suffer from nearly all of the adoption challenges that IPSec in IPv4 encountered. These include key management and distribution mechanisms that are challenging to implement and operate at scale.

### IPv6 Migration Steps

To help ensure a smooth IPv6 transition and eliminate security pitfalls, there are several steps organizations can take to protect their systems, including:

- Begin monitoring networks for IPv6 traffic, especially if there are IPv6-enabled devices, operating systems and transitional configurations on the network.
- Turn off "IPv6 everywhere" to ensure that there are not any unknown paths through the network.
- Begin thinking about what is required to build the security needed to use IPv6 within the application layer and various software systems in the operating environment.
- Conduct an IPv6 pilot on a small portion of the network, potentially using a transitional technology.
- Develop a plan to transition an entire network to IPv6 incrementally.
- Execute the plan once ready, but execute quickly once committed; the number of vulnerabilities on an organization's network will only increase as organizations linger.
- Acquire and test IPv6-aware monitoring and assessment tools.

IPv6 signals a new era for the Internet, a fundamental change that will alter the technology that has become an essential part of our lives. Verisign's role in operating and securing the .com and .net infrastructure caused the company to be an early adopter of IPv6 in every aspect of our operations. As with DNSSEC, we have focused on our core responsibility of being a responsible steward of the Internet infrastructure we manage by being ready, informed and engaged. Verisign will continue to work with the Internet community to make IPv6 the de facto standard for all Internet operations.

VERISIGN™

## LEARN MORE

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

## ABOUT VERISIGN

VeriSign, Inc. (NASDAQ: VRSN) is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day, Verisign helps companies and consumers all over the world connect between the dots. Additional news and information about the company is available at www.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 all 290 ccTLDs 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 www.zooknic.com. Information on or accessible through this website is not part of this report.

ICANN's 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 is the first quarter that we have reported on these TLDs that have been delegated into the root zone, including Russian Federation, Thailand, Jordan, Palestinian Territories, Saudi Arabia, Serbia and Sri Lanka. This additional tracking resulted in an additional 808,967 ccTLD names being reported. 97.7 percent of these names (790,447) came from the Russian Federation (.рф). 1.61 percent (13,014) of these names came from Thailand (.ไทย).

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.





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 Verisign's 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 future revenue and profitability and potential fluctuations in quarterly operating results due to such factors as increasing competition, pricing pressure from competing services offered at prices below our prices and changes in marketing practices including those of third-party registrars; challenging global economic conditions; challenges to ongoing privatization of Internet administration; the outcome of legal or other challenges resulting from our activities or the activities of registrars or registrants, or litigation generally; new or existing governmental laws and regulations; changes in customer behavior, Internet platforms and web-browsing patterns; the uncertainty of whether Verisign will successfully develop and market new services; the uncertainty of whether our new services will achieve market acceptance or result in any revenues; system interruptions; security breaches; attacks on the Internet by hackers, viruses, or intentional acts of vandalism; the uncertainty of the expense and duration of transition services and requests for indemnification relating to completed divestitures; the uncertainty of whether Project Apollo will achieve its stated objectives; the impact of the introduction of new gTLDs and whether our gTLD applications or the applicants' gTLD applications for which we have contracted to provide back-end registry services will be successful; and the uncertainty of whether the .com Registry Agreement renewal will occur on or before November 30, 2012, if at all. More information about potential factors that could affect the Company's business and financial results is included in Verisign's filings with the Securities and Exchange Commission, including in the Company's Annual Report on Form 10-K for the year ended December 31, 2011, 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.