VERISIGN™

THE DOMAIN NAME INDUSTRY BRIEF

VOLUME 8 - ISSUE 2 - MAY 2011

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 A LEADING PROVIDER OF DIGITAL INFRASTRUCTURE FOR THE INTERNET, VERISIGN PROVIDES THIS BRIEFING TO HIGHLIGHT TO INDUSTRY ANALYSTS, MEDIA, AND BUSINESSES IMPORTANT TRENDS IN DOMAIN NAME REGISTRATION, INCLUDING KEY PERFORMANCE INDICATORS AND GROWTH OPPORTUNITIES.

VERISIGN™

EXECUTIVE SUMMARY

The first quarter of 2011 closed with a base of more than 209.8 million domain name registrations across all Top Level Domains (TLDs), an increase of 4.5 million domain names, or 2.2 percent over the fourth quarter. Registrations have grown by 15.3 million, or 7.9 percent over the past year.

The base of Country Code Top Level Domains (ccTLDs) was 81.7 million domain names, a 2.1 percent increase quarter over quarter, and a 5.1 percent increase year over year.[1]

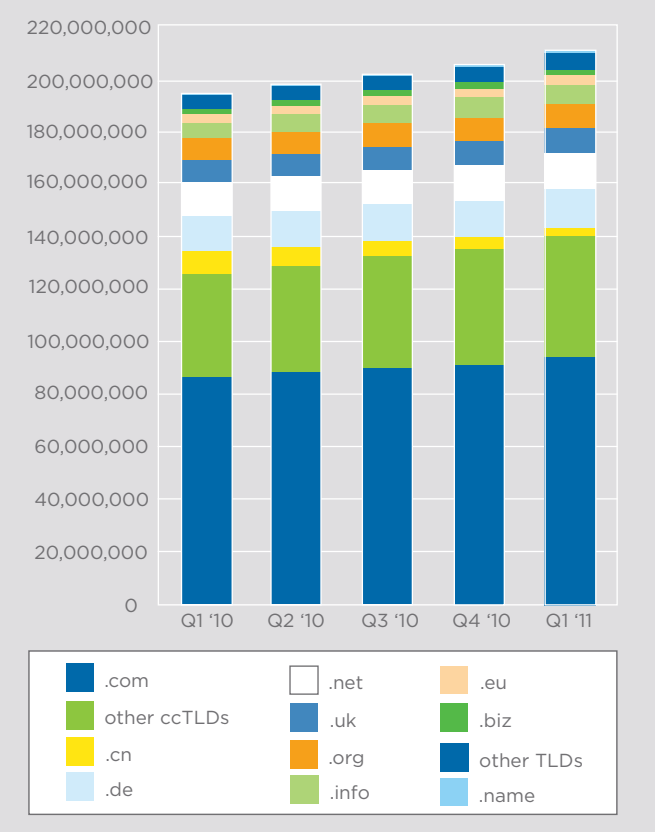
The .com and .net TLDs experienced aggregate growth in the first quarter, surpassing a combined total of 108 million names. New .com and .net registrations totaled 8.3 million during the quarter. This is a 9.2 percent increase year over year in new registrations, and 2.7 percent increase from the fourth quarter.

The order of the top TLDs in terms of zone size changed compared to the fourth quarter, as .uk (United Kingdom) moved from fifth to fourth largest TLD, dropping .org from fourth to fifth. Also, .cn (China) dropped from seventh to ninth largest which allowed .nl (Netherlands) and .eu (European Union) to move up one spot each to seventh and eighth largest, respectively.

The largest TLDs in terms of base size were, in order, .com, .de (Germany), .net, .uk, .org, .info, .nl, .eu, .cn and .ru (Russian Federation).

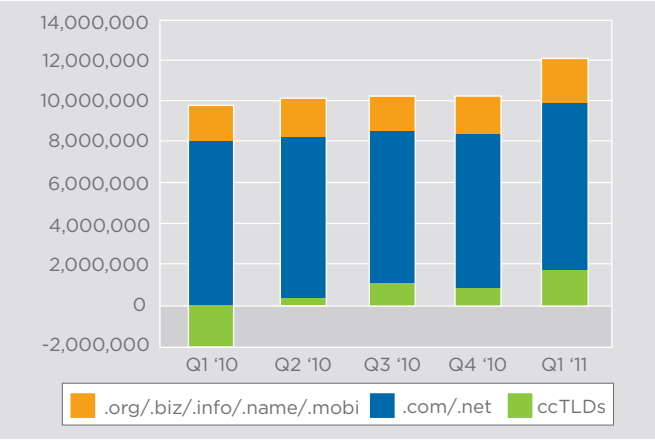
Total Domain Name Registrations

Source: Zooknic, April 2011; Verisign, May 2011



New Registration Growth

Source: Zooknic, April 2011; Verisign, May 2011; 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.

VERISIGN™

CCTLD BREAKDOWN OF ZONE SIZE

Total ccTLD registrations were approximately 81.7 million in the first quarter of 2011 with the addition of 1.6 million domain names, or a 2.1 percent increase compared to the fourth quarter. This is an increase of approximately 4.0 million domain names, or 5.1 percent from a year ago.[2]

Among the 20 largest ccTLDs, the Netherlands, Brazil, Italy, Australia, France, the United States and Canada each exceeded 4 percent quarter over quarter growth. Last quarter, four of the top 20 exceeded the same threshold.

Australia and Canada were the only top 20 ccTLDs exceeding 20 percent year over year growth. Last quarter, four of the top 20 exceeded this threshold.

There are more than 240 ccTLD extensions globally, with the top 10 ccTLDs comprising 61 percent of all registrations.

Top ccTLD Registries by Domain Name Base, First Quarter 2011

Source: Zooknic, April 2011

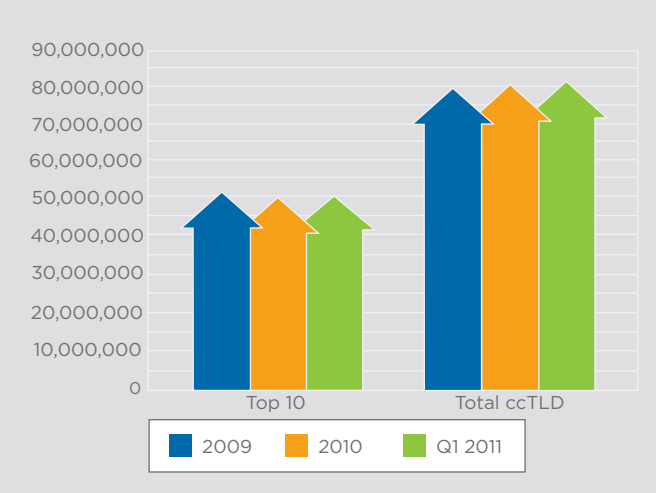
1.	.de	(Germany)	6.	.ru	(Russian Federation)
2.	.uk	(United Kingdom)	7.	.br	(Brazil)
3.	.nl	(Netherlands)	8.	.ar	(Argentina)
4.	.eu	(European Union)	9.	.it	(Italy)
5.	.cn	(China)	10.	.pl	(Poland)

.COM/.NET DYNAMICS

The .com/.net renewal rate for the first quarter of 2011 was 73.8 percent, up from 72.7 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.

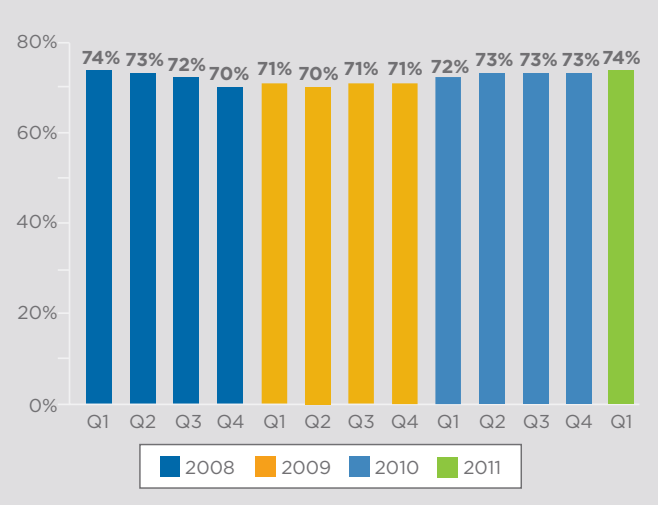
ccTLD Breakdown

Source: Zooknic, April 2011



.com/.net Registry Renewal Rates

Source: Verisign, May 2011

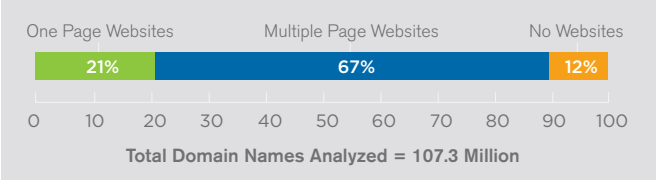


2 Some ccTLD registries ran promotional programs during the first quarter.

VERISIGN™

.com/.net Websites

Source: Verisign, May 2011



Whether a domain name resolves to a website is a key factor in the renewal rates 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.

Verisign's average daily Domain Name System (DNS) query load during the quarter was 57 billion, with a peak of 67 billion. Compared to the same timeframe in 2010, the daily average and the peak each grew 6 percent.

The ongoing growth of DNS query loads stems both from normal traffic drivers – most notably the continuing increase in global Internet usage – and from increasingly powerful distributed denial of service (DDOS) attacks leveled against all parts of the Internet's critical infrastructure. These increases, both from benign and malicious sources, require aggressive innovation and investment on the part of infrastructure operators to meet the growing demand. For Verisign, this means Project Apollo, which will grow capacity 1,000 times today's level of 4 trillion queries to manage 4 quadrillion queries per day by 2020.

NAVIGATING GROWING THREATS KEY FOR SUCCESS OF NEW TLDS

With all the excitement surrounding new generic Top Level Domains (gTLDs) and the expansion of the global Domain Name System (DNS), it is important that the global Internet community not lose sight of the very real and growing cyber threats facing that system. Successfully defending against these threats will be critical to ensuring the continued stability and growth of the DNS infrastructure.

For many years, the DNS has been ground zero in a high-stakes battle between cyber attackers and the technologists responsible for upholding the security and stability of the infrastructure. Combatants on both sides understand all too well that the DNS is the lynchpin of Internet communication. If it is compromised, the entire Internet is at risk.

In the past decade, the weapon of choice for cyber criminals – distributed denial of service (DDoS) attacks – has increased in both frequency and destructive payload.

DDoS attacks occur when attackers command unprotected PCs they have "enslaved" using malicious code to overload a single target with Internet traffic. What makes the attacks so insidious is that they often mimic normal traffic as they overload the capacity of their targets, effectively taking them offline. According to the Arbor Networks Worldwide Infrastructure Security Report VI, the Internet witnessed the first 100 gigabit-per-second (gbps) DDoS attack in 2010, compared to a high-water mark of 10 gbps in 2005.

To put that figure in perspective, 100 gbps is 10 times greater than the capacity of any single discrete IP backbone circuit, and is large enough to overwhelm all but a tiny handful of networks on the planet. This figure has not gone unnoticed by network administrators. Research on DDoS commissioned by Verisign and conducted in March 2011 found that nearly three in four IT decision makers working for companies without a DDoS mitigation solution plan to implement one in the next 12 months.

To make matters worse, TLDs have always been – and will always be – both targets and potential conduits for some of the most serious cyber attacks. Bringing down or manipulating a TLD can wreak havoc on millions of sites, and hundreds of millions of users at once. And attacks on specific Country Code TLDs can cripple entire nations, a dangerous tactic for both state-sponsored cyber terrorists and other cyber criminals.

These are the realities that all TLD operators – even those that are small and new – face as they work to serve the registrars, registrants, and consumers who rely on them.

STRENGTHENING THE PILLARS OF AVAILABILITY AND INTEGRITY

Of the three pillars of information security – confidentiality, integrity and availability – the greatest focus of the DNS community has recently been on integrity, with the deployment of DNSSEC around the world. DNSSEC addresses the problem of so-called "man-in-the-middle" attacks – in which attackers spoof DNS data – by allowing for the authentication of that data. As DNSSEC gets deployed more extensively throughout the Internet, these types of attacks should decline significantly.

With DNSSEC implemented at the root-server level, and in leading gTLDs and ccTLDs, such as .com, .net, .org and many others, DNS integrity has taken a step forward. But as important as integrity is to the smooth and reliable operation of the DNS, another pillar of information security – availability – may be even more critical.

When a network or TLD becomes unavailable – even for a short time – it has a trickledown effect, as once it becomes non-responsive to queries, the doors to the store are closed and consumers could go elsewhere. For this reason, upholding availability must always be a top priority – especially for TLD operators. And while there are many issues that can cause network downtime, DDoS attacks are one of the most significant and unpredictable. The DDoS research cited above found that almost nine in 10 respondents (87 percent) rated DDoS protection as very important to maintain availability.

Today, there are many known countermeasures for DDoS attacks (rate limiting, firewalls, "blackhole" routing, etc.) that range in effectiveness and efficiency. Often, the first line of defense – particularly for TLD operators, who can ill-afford the time it takes to mitigate a DDoS attack after it happens – is "over-provisioning," or building additional network bandwidth and transaction-servicing capacity to help withstand the exponential spikes in volume experienced during a DDoS attack.

Over-provisioning is necessary, but does not – in itself – represent a complete DDoS mitigation program. Ideally, TLD operators will seek to develop the ability to quickly detect and mitigate attacks in the cloud before they reach their networks.

With the extraordinary and rapid changes in DDoS attacks we're seeing today, traditional DDoS mitigation tactics such as bandwidth over-provisioning, firewalls and intrusion prevention system (IPS) devices are no longer solely sufficient to protect networks, applications and services. For many TLD operators, third-party DDoS mitigation services from specialized experts should help bridge the technology gap in defending their networks from an ever-widening array of threats and challenges.

One of the ways that Verisign is working to help network operators address these challenges is through Verisign DDoS Protection Services. Based on the company's

VERISIGN™

expertise in successfully defending its global DNS infrastructure against DDoS and other attacks for more than a decade, Verisign DDoS Protection Services are cloud-based, network and hardware agnostic DDoS monitoring and mitigation services that detect and filter malicious traffic in the cloud so it never reaches the network. This approach enables IT teams to keep critical online applications and services available without requiring large investments in infrastructure or over-provisioning.

As in all things related to launching a new gTLD, strong technical partners and a firm understanding of the threat landscape will be critical to success and stability in the emerging market.

LEARN MORE

To subscribe or access the archives for the Domain Name Industry Briefs, please go to http://www.verisigninc.com/en_US/why-verisign/research-trends/domain-name-industry-brief/index.xhtml. 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 to connect online with confidence. Additional news and information about the company is available at www.VerisignInc.com.

Zooknic Methodology
For gTLD data cited with Zooknic as a source, the 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.

VerisignInc.com

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; the sluggish economic recovery; 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; new or existing governmental laws and regulations; changes in customer behavior, Internet platforms and web-browsing patterns; the inability of Verisign to 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; and the uncertainty of whether Project Apollo will achieve its stated objectives. 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, 2010, 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.