May 25, 2011

Internet Adds 4.5 Million Domain Names in First Quarter of 2011

DULLES, VA (Marketwire) - Four and a half million domain names were added to the Internet in the first three months of 2011, according to the latest Domain Name Industry Brief published by VeriSign, Inc. (NASDAQ: VRSN), the trusted provider of Internet infrastructure services for the networked world.

The first quarter of 2011 closed with a base of more than 209.8 million domain name registrations across all Top Level Domains (TLDs), or a 2.2 percent increase over the fourth quarter of 2010. Registrations grew by 15.3 million, or 7.9 percent year over year.

Verisign's combined base of .com and .net domain names experienced aggregate growth in the first quarter of 2011, surpassing a total of 108 million names. New .com and .net registrations totaled 8.3 million during the first quarter. The total represents a 9.2 percent increase year over year in new registrations, and a 2.7 percent increase from the fourth quarter. The .com/.net renewal rate for the first quarter was 73.8 percent, up from 72.7 percent from the fourth quarter.

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.

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.

DNS Integrity, Availability and the Growing Threats Facing New TLDs

The latest Domain Name Industry Brief also highlights the security considerations for new generic TLD (gTLD) operators -- along with the importance of improving integrity and availability in combating security threats. As the DNS expands to make room for more TLDs, it is vital to remain vigilant against cyber threats that increasingly target the DNS. If the DNS is compromised, the entire Internet is at risk.

In the past decade, distributed denial of service (DDoS) attacks have increased in both frequency and severity. A weapon of choice for cyber criminals, DDoS attacks occur when hackers use malicious code to "enslave" unprotected PCs and cause them to overload a single target with Internet traffic, effectively taking the target offline. Bringing down a TLD can simultaneously wreak havoc on millions of sites and hundreds of millions of users. 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.

One essential safeguard against threats to the DNS itself is DNS Security Extensions (DNSSEC). Now being deployed 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 TLDs like .com, .net, .org and many others, the integrity of the DNS has taken a step forward. But as important as integrity is to the smooth and reliable operation of the DNS, another crucial element 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. Everything else must be put on hold until it can be brought back online. This makes upholding availability a 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.

Verisign recently commissioned a market research report surveying 225 IT decision-makers in the U.S. from large and medium-sized businesses, which revealed that nearly two-thirds (63 percent) of respondents who reported experiencing a DDoS attack in the past year, sustained more than one attack. Eleven percent of surveyed businesses were hit six or more times.

In this rapidly evolving threat environment, 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 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.

Verisign publishes the Domain Name Industry Brief to provide Internet users throughout the world with significant statistical and analytical research and data on the domain name industry and the Internet as a whole. Copies of the 2011 first quarter Domain Name Industry Brief, as well as previous reports, can be obtained at: http://www.verisigninc.com/en_US/why-verisign/research-trends/domain-name-industry-brief/index.xhtml.

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.

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.