May 9, 2011

Businesses Lack Safeguards Against DDoS Attacks and DNS Failures, New Research Shows

At Interop Las Vegas, Verisign Spotlights Two Studies That Illustrate the Urgent Need to Maximize Network Security, Availability and Performance

LAS VEGAS, NV (Marketwire) - **INTEROP LAS VEGAS** -- A significant percentage of organizations are ill-equipped to prevent and respond to web infrastructure failures caused by distributed denial of service (DDoS) attacks and Domain Name System (DNS) failures, according to two new research studies commissioned by VeriSign, Inc. (NASDAQ: VRSN), the trusted provider of Internet infrastructure services for the networked world.

As networking executives from around the world convene this week at Interop's annual flagship event, Verisign is spotlighting research findings that underscore the urgent need for robust DDoS protection, reliable and secure DNS infrastructure, and advanced threat intelligence.

"This research illustrates the dire costs of insufficient web and network protection to businesses spanning all industries. When a DDoS attack or DNS failure hits a website or network, companies are losing significant revenue and employee productivity, and are likely seeing decreasing customer satisfaction and loyalty," said Ben Petro, senior vice president of Verisign's Network Intelligence and Availability Group. "Businesses are facing a number of threats in today's economy. Implementing Verisign's suite of trusted network intelligence and availability services will help ensure that DDoS attacks and DNS failures are not among them."

DDoS Protection: Vital, as frequency and strength of DDoS attacks are predicted to grow
Verisign commissioned a market research report from Merrill Research to investigate the level of concern IT decision makers have with the growing threat of DDoS attacks in today's ever evolving cyber landscape. An online survey of 225 IT decision-makers in the U.S. from large and medium-sized businesses revealed that 78 percent are extremely or very concerned about DDoS attacks, and more than two-thirds (67 percent) expect the frequency and strength of DDoS attacks to increase or stay the same over the next two years. Nearly nine in 10 respondents (87 percent) view DDoS protection as very important for maintaining availability of websites and services. Moreover, seven in 10 (71 percent) respondents who reported a lack of DDoS protection said they plan on implementing a solution in the next 12 months.

Research Highlights:

- **DDoS attacks are widespread:** Nearly two-thirds (63 percent) of respondents who reported experiencing a DDoS attack in the past year said they sustained more than one attack. Eleven percent were hit six or more times.
- **More sites will soon be protected:** Of the respondents who currently lack DDoS protection, 71 percent plan to implement a solution in the next 12 months -- 40 percent plan to outsource their DDoS protection, 31 percent plan to implement an in-house solution, and 29 percent are still undecided on their approach for protection.
- **Leaving web infrastructures unprotected is too risky:** More than half (53 percent) of the respondents said they experienced downtime in the past year, with DDoS attacks accounting for one-third (33 percent) of all downtime incidents.
- **Downtime impacts customers and revenue:** More than two-thirds (67 percent) said their downtime impacted customers and half (51 percent) reported they lost revenue. Considering 60 percent of the respondents rely on their websites for at least 25 percent of their annual revenue, downtime can have significant and lasting impacts.
- **Threats extend beyond DDoS attacks:** The study also found that nine in 10 respondents rate "access to threat and vulnerability data" as very important and nearly three-fourths (73 percent) are "concerned with DNS failures" -- suggesting a significant need for ongoing threat intelligence and managed DNS services, in addition to DDoS protection and mitigation.

DNS Availability Lower for Internally Managed Sites
A separate study commissioned by Verisign sheds light on the need for solutions that ensure DNS availability -- a crucial requirement for the reliable operation of websites, network services, and online communications. The study, which is highlighted in the inaugural issue of the Verisign State of DNS Availability Report, found that in the first quarter of 2011, DNS availability was a problem for even the highest ranked e-commerce sites.

Using proprietary technology, ThousandEyes, a company that provides application performance analytics, calculated the minimum availability, maximum availability, and average availability of the Alexa 1,000 websites in the first quarter of 2011 to illustrate the state of global DNS availability.

The research revealed some stark differences between sites with internally managed DNS and those that employ third-party managed DNS services. In particular, the study revealed that minimum DNS availability on average dropped to 90.13 percent for sites that host their own DNS, while sites using third-party managed DNS services averaged a minimum DNS availability rate of more than 98 percent. When examining minimum availability overall, the research showed that some sites with internally managed DNS had total outages, while sites with third-party DNS management never went below 50 percent availability. Similarly, average downtime for sites that host their own DNS is twice that of those that use a third party (99.7 percent versus 99.85 percent).

This dramatic difference is most likely attributed to the fact that most third-party DNS providers use an anycast resolution service, meaning there is always a server available somewhere to respond to DNS queries. This allows end users to experience less impact even if a few physical anycast servers fail or are unreachable. Verisign has taken DNS resolution a step further by implementing a unique hybrid model of anycast and unicast resolution into its Managed DNS service, which provides the optimal combination of performance and reliability for responding to DNS queries. Most enterprises do not have the resources and expertise to set up such extensive systems for their internally managed DNS, which may make them more vulnerable to availability problems.

Verisign at Interop Las Vegas:
Verisign will showcase its suite of network intelligence and availability services in Booth 1221 at Interop Las Vegas this week. These services include DDoS monitoring and mitigation, Verisign Managed DNS®, and Verisign iDefense® Security Intelligence Services.

Also at Interop, Sean Leach, vice president of technology for Verisign's Network Intelligence and Availability Group, will give a 45-minute presentation exploring how organizations can leverage recent advances in Internet infrastructure, such as DNSSEC and IPv6, to provide greater protection from the ever evolving cyber threat landscape, while managing the growing complexity of their network infrastructure.

The session, titled: "The Yin-and-Yang of Internet Infrastructure: Balancing New Opportunities with Growing Threats and Increased Risk," is on Tuesday, May 10, 2011 at 12:15 p.m. PT at Mandalay Bay L at the Mandalay Bay Convention Center.

Limited-Time Promotion:
Verisign is currently offering the Verisign Uptime Bundle, which combines the Verisign Managed DNS service with threat intelligence services and protection from DDoS attacks -- all in one competitively priced suite starting at just $495. To learn more about Verisign's solutions and the Verisign Uptime Bundle, please visit www.verisigninc.com.