May 6, 2010

VeriSign Report Details Five Ways to Arm Against Latest Wave of DDoS Attacks

New Report Outlines Best Practices for Defending Sites as Distributed Denial-of-Service Attacks Grow Larger, Stealthier and More Sophisticated

MOUNTAIN VIEW, CA (Marketwire) - VeriSign, Inc. (NASDAQ: VRSN), the trusted provider of Internet infrastructure services for the networked world, today released a new report aimed at helping online businesses and other enterprises protect themselves against distributed denial-of-service (DDoS) attacks.

"DDoS Mitigation: Best Practices for a Rapidly Changing Threat Landscape," a new white paper available today, describes how hackers are employing larger and stealthier techniques to outmaneuver such traditional DDoS defense tactics as bandwidth over-provisioning, firewalls, and intrusion prevention systems (IPS). DDoS attacks use multiple hosts, such as compromised PCs, to flood and overwhelm a target site or application with traffic. Successful attacks can bring down sites for hours or even days, causing businesses to suffer losses in the millions and damaging a company's brand and customer relationships.

The paper cites Forrester survey data showing that 74 percent of IT decision-makers reported experiencing one or more DDoS attacks in the past year. In nearly one out of every three attacks, hackers were successful in disrupting service, even though these organizations had in place security measures designed to thwart DDoS attacks.

One reason, the report notes, is that DDoS methods have evolved rapidly in the past year. More and more, hackers are preying on specific targets by dispatching hundreds of thousands of custom bots to directly flood a target site with traffic. Or they amplify their attacks with reflection flood techniques that use recursive Domain Name System (DNS) servers to bounce attacks to their victims. Or they execute subtle application-level attacks that are harder to detect because they mimic legitimate traffic. Even budget-minded amateurs can spawn successful attacks by renting botnets for as little as $200 for 24 hours.

Five Best Practices from an Expert in DDoS Defense
VeriSign has successfully defended its global DNS infrastructure against DDoS and other attacks for more than a decade, while maintaining 99.99 percent availability of its critical infrastructure. VeriSign also has maintained 100 percent availability of its .net and .com infrastructure, even as it resolves more than 50 billion DNS transactions per day.

Drawing on this success and VeriSign's hands-on customer engagements, the white paper identifies a set of best practices that enables organizations to keep pace with DDoS attacks while minimizing impact on business operations. (For a much more detailed explanation of these best practices, download the paper.)

1. Centralize data gathering and understand trends. It's vital to understand what normal network traffic looks like, and to identify anomalies quickly and accurately. By working with expert security researchers, organizations can better track trends and threats. And they can implement effective DDoS-specific alerting, logging and reporting systems.
2. Define a clear escalation path. A fast and effective response is key to mitigating DDoS attacks, so enterprises need systematic processes and methodologies in place. For instance, defining incident response teams and preparing for downtime before an attack occurs can restore operations sooner, with less devastating effects.
3. Use layered filtering. Even as unwanted network traffic is blocked, legitimate traffic must be allowed through with minimal latency. Filtering traffic in layers, rate-limiting traffic, and enhancing rule sets over time all are key to achieving this.
4. Build in flexibility and scalability. A scalable, flexible infrastructure helps ensure systems function properly under attack conditions. IT managers should: test the limits of IT components to know their breaking points; enforce hardware and software diversity so an attack targeting one platform doesn't bring down the entire network; and

```
    do what it takes to provide on-demand capacity within a load-balanced
    infrastructure.
5.  Address application and configuration issues. With DDoS attacks evolving
    from brute force traffic floods to subtle infiltrations of the
    application layer, organizations need better insight into application
    thresholds and vulnerabilities. Among the paper's suggestions: Address
    simplistic configurations and common application vulnerabilities.
```

The Growing Need for Managed Services
The picture that emerges may be worrisome for organizations attempting to protect themselves with on-premise DDoS detection and protection technologies. Implementing these best practices can be complex, time-consuming, and resource-intensive, involving not only human expertise, but also state-of-the-art technology and military-grade network operations centers (NOCs).

For a growing number of organizations, the most cost-effective and comprehensive solution is managed DDoS mitigation services. As the VeriSign paper explains, managed DDoS mitigation services provide benefits in-house solutions cannot, including:

- The ability to "scrub" packets and divert malicious traffic while still in the cloud
- An inherently larger capacity to handle traffic and efficiently divert malicious traffic
- Built-in massive bandwidth and multiple NOCs for redundancy and high availability
- DDoS mitigation expertise and around-the-clock staffing
- A more global view of Internet traffic, threats and attack trends
- Carrier and ISP neutrality, enabling equal levels of protection across all the carriers and ISPs an organization uses worldwide

"If the past year has shown us anything, it's that DDoS threats represent a moving target -- one that is growing more sophisticated and difficult to defend against, even as the attacks themselves grow more frequent," said Ken Silva, VeriSign CTO. "We published this white paper as a blueprint for organizations looking to stay ahead of this rapidly evolving threat to revenues, operations, customer loyalty and network reliability. And because in-house mitigation is often too expensive or labor-intensive to remain effective, the paper also provides tips on what organizations should look for when choosing a managed DDoS mitigation services provider."

The paper leverages insights and experience gathered via the VeriSign® Internet Defense Network, a massively fortified, comprehensive service that can effectively and efficiently mitigate the world's largest DDoS attacks. The service addresses the facets of DDoS mitigation -- from assessment, monitoring, detection, and reporting to DDoS source analysis. The Internet Defense Network helps protect organizations from catastrophic DDoS attacks by detecting and filtering malicious traffic upstream of the organization's network. An international team of security experts staffs the globally distributed network operation centers and is available 24/7 to monitor, detect, analyze, and respond to malicious traffic.

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 engage in communications and commerce with confidence. Additional news and information about the company is available at www.verisign.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 and Section 21E of the Securities Exchange Act of 1934. 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 the inability of VeriSign to successfully develop and market new products and services and customer acceptance of any new products or services, including VeriSign Internet Defense Network; the possibility that VeriSign's announced new services may not result in additional customers, profits or revenues; and increased competition and pricing pressures. 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, 2007 and quarterly reports on Form 10-Q. VeriSign undertakes no obligation to update any of the forward-looking statements after the date of this press release.