



C O M P A N Y P R E S S R E L E A S E

Press contacts:

Amanda Coolong / Noah Dye
LEWIS PR on behalf of CloudShield
+1 619 516 2559 / +1 619 708 7413
cloudshield@lewispr.com

Denial of Service Attacks Could Cause Super Bowl Slowdown, Warns CloudShield

Increasing size and complexity of attacks leave ISPs vulnerable

Sunnyvale, CA – January 23, 2007 – With the Super Bowl approaching, Internet Service Providers (ISPs) must be prepared to mitigate potential Denial of Service (DoS) attacks aiming to disrupt e-commerce sites around this major U.S. sporting event, warns CloudShield Technologies.

Worldwide, as many as 10,000 DoS attacks occur each day.¹ CloudShield Founder and CTO, Peder Jungck said: “Denial of service attacks are very difficult to stop because they can easily overrun an ISP’s defenses. For example, in one recent incident that CloudShield helped resolve, an ISP was facing a sustained attack against its DNS services exceeding one million requests per second – that’s roughly 100 times the capacity of typical DNS servers.” He continued: “The ease with which hackers and extortionists can launch such massive assaults is making DoS attacks increasingly popular, particularly those targeting e-commerce sites around peak traffic times like the Super Bowl.”

The Super Bowl is one of the biggest sporting events of the year, generating a massive spike in online gaming and merchandising. This year, PinnacleSports.com, which operates under license from the Netherlands Antilles, expects more Internet traffic on

¹ Cyber Extortion, A very Real Threat by Jose Nazario, IT Observer, June 7, 2006

February 5 than any other day of the year.² This necessitates adequate protection of e-commerce infrastructure to minimize any downtime due to DoS attacks.

“ISPs are unable to keep up with the increasing complexity and seriousness of today’s evolving DoS attacks, often leaving it to customers to protect themselves,” Jungck said. “Traditional security solutions like firewalls, routers and intrusion detection devices are not designed to protect against large-scale DoS attacks. All ISPs hosting and supporting online businesses must have the ability to quickly mitigate DoS attacks against their customer sites, and their own service infrastructures, or they risk not only lost revenues, but lost reputations as well.”

CloudShield has provided rapid response support to solve Distributed Denial of Service (DDoS) issues successfully with a number of customers since 2004. It also provides tailored DDoS mitigation services to prevent attacks, including real-time defense that supports millions of packets per second. With patented DPI techniques and high-performance attack traffic processing systems, CloudShield successfully protected several e-commerce sites that were attacked during the recent Christmas online shopping season. For further information on CloudShield’s DDoS attack mitigation capabilities please visit: http://www.cloudshield.com/solutions/ddos_mitigation.asp.

For more information on protecting operator and subscriber infrastructures against DoS attacks, contact CloudShield at stop_ddos_now@cloudshield.com.

About CloudShield

CloudShield solutions provide large network operators new levels of visibility *and* control of the traffic traversing their high-speed networks, providing opportunities to monetize network content and better manage their subscribers’ experiences. CloudShield systems enable controls to be customized to individual operator requirements, supporting unique service offerings and operator policies. Through its application and solution partners, CloudShield has helped deliver solutions to carriers in North America, Europe and Asia as well as many important U.S. federal government customers. More information about CloudShield can be found at www.cloudshield.com.

² <http://www.bankrate.com/brm/itax/news/20010122a.asp>

###