Neustar Second Annual DDoS Survey Finds 35% of Businesses Experienced a DDoS Attack in 2012

Apr 24, 2013

Three-Quarters of Respondents Reported DDoS Outages Could Cost up to $250k Per Day

STERLING, Va. – When DDoS (Distributed Denial of Service) attacks hit, organizations are thrown into crisis mode. From the IT department to call centers, to the boardroom and beyond, it's all hands on deck until the danger passes. In February 2013, Neustar, a trusted, neutral provider of real-time information and analysis, surveyed 704 IT professionals across North America to understand how companies are managing the crisis around DDoS attacks and measuring the impact on their businesses.

Among the key findings from the survey, 35% of organizations experienced a disruptive DDoS attack in 2012. Of those surveyed, a staggering 39% of retailers and 41% of ecommerce businesses experienced an attack last year. Additionally, more than a quarter of respondents (26%) indicated a DDoS outage could cost between $50-100k per hour, further showcasing the need for a strategy around DDoS protection and mitigation.

"Preparation is key: The consequences of being unprepared to mitigate a DDoS attack can be crippling to businesses," said Alex Berry, Senior Vice President, Enterprise Services, Neustar. "It isn't just about possible revenue loss – it's about erosion in trust, brand value and reputation."

Additional survey findings include:

- Key sectors reported higher rates of attack: The number of retailers experiencing an attack increased by 144 % from 2011 levels to reach an overall level of 39% in 2012; financial organizations experienced a 38% increase in attacks year-to-year with 44% of financial organizations being victimized in 2012.
- Though more companies are deploying DDoS protection—only 8% had no protections in place compared to 25% in 2011—few have invested in purpose-built hardware or third-party expertise.
- The latter is alarming; while 66% of companies use firewalls, routers and switches for DDoS protection, these networking products create bottlenecks that actually aid attackers.

As DDoS attacks continue to become both more frequent and complex, it's important that organizations adopt the right mix of people, processes and technologies to fight these attacks and quickly eliminate downtime. A critical aspect in getting this right is ensuring resources are in place to both monitor and mitigate. The survey found a 10% increase year-to-year in the use of firewalls, switches and routers as defensive mechanisms, but the reality is that these means can compound the effects of DDoS attacks by bottlenecking the traffic.

According to Christian A. Christiansen, Chris Liebert and Charles J. Kolodgy of IDC Research, in a February 2013 report, entitled *The Business Value of Hybrid Cloud-based Compromise Intelligence Monitoring and Threat Mitigation*, “Given the complex nature of today's threats, enterprises can achieve a strategic advantage by employing a new layer of security that is services based. Cloud-based services are an important aspect of this approach to security and provide always-on monitoring without the added expense of buying and maintaining on-premise equipment.”

Download a copy of the full survey here.

About Neustar

Neustar, Inc. is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, information services, financial services, retail, media and advertising sectors. Neustar applies its advanced, secure technologies in location, identification, and evaluation to help its customers promote and protect their businesses. More information is available at www.neustar.biz