Three-Quarters of IT Professionals Fear Negative Brand Impact or Customer Experience as a Result of DDoS Attacks

May 15, 2012

By unleashing extremely high volumes of malicious Internet traffic or surgically targeting Web applications, hackers seek to shut down a company's Web resources – typically websites, but

also email servers. When hackers unleash a DDoS attack, it carries the potential to exert lasting damage to customer service, online revenue streams and brand reputation.

Neustar Survey Results:

Executed in Q1 2012, the survey garners responses of IT professionals in more than 25

industries such as finance and banking, retail, telecommunications, travel and IT. Notable

findings include:

- More than 300 respondents reported they had been attacked

- The top concern was the impact attacks have on customer service – with 51percent

  listing it as their greatest concern associated with the attacks

- 35 percent of those attacked said the attacks lasted more than 24 hours – with 11percent

  of attacks lasting more than a week

- Specific to retailers, 67 percent who had experienced a DDoS attack pegged the costs of

  website outages at more $100,000 per hour – equating to loses of $2 million a day

“The potential negative implications of DDoS attacks can be devastating for both marketers and IT professionals,” said Alex Berry, senior vice president, Enterprise Services, Neustar. “Many companies have been hit hard - with consequences lasting far longer than the attacks themselves. It’s important that companies are proactive about protecting their online presence,

as well as their customers, to ensure the constant delivery of online services and necessary

brand vigilance.”

Overall, the survey shows that a significant number of companies face the risks of DDoS

attacks, yet few have solutions designed specifically to combat attacks, with many relying

solely on firewalls and intrusion detection systems. Less than 5 percent of respondents have a

purpose-built DDoS mitigation solution, for example, an on-premise DDoS mitigation appliance.

This explains why so many attacks last days – in fact, 35 percent respondents experienced

attacks that lasted more than 24 hours. Without adequate protection, companies are unable to prevent losses from adding up. While many respondents are aware of the risks to their customer experience and public trust, they haven’t taken the next step to safeguard their reputation.

To download a copy of the report, please

visit: http://hello.neustar.biz/rs/neustarinc/images/neustar-insights-ddos-attack-survey-

q1-2012.pdf

Neustar, Inc., (NYSE: NSR) is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, entertainment and marketing industries throughout the world. Neustar applies its advanced, secure technologies in routing, addressing and

authentication to its customers' data to help them identify new revenue opportunities and network efficiencies, and institute cybersecurity and fraud protection measures. More information is available at www.neustar.biz.