
Neustar 2014 'DDoS Attacks and Impact Report' Finds Unpredictable DDoS Landscape

Apr 22, 2014

Attacks Becoming Quicker and More Concentrated, Pointing to Growing "Smokescreening" Trend as 55 Percent of DDoS Targets Report Theft

STERLING, Va. – [Neustar, Inc.](#) (NYSE: NSR), a trusted, neutral provider of real-time information and analytics, today released its third annual "DDoS Attacks and Impacts Report," delivering key insights on Distributed Denial of Service (DDoS) attacks and the business impact of these incidents. The survey reveals that DDoS attacks are now more unpredictable and damaging than ever, crippling websites, shutting down operations, and costing millions of dollars in downtime, customer support and brand damage. Nearly twice as many businesses surveyed suffered a DDoS attack last year and more than 40 percent estimated DDoS losses at more than \$1 million per day.

Other key findings include a growing trend toward quicker, more concentrated attacks, suggesting a spurt in "smokescreening" – where criminals use DDoS attacks to distract IT staff while inserting malware to breach bank accounts and customer data. In fact, 49 percent of businesses who suffered a DDoS attack and a breach in 2013 reported that a virus or malware was installed or activated and 55 percent of DDoS targets reported that they were also victims of theft. Attackers stole funds, customer data and intellectual property.

"DDoS attacks create an 'all hands on deck' mentality, and the potential for damage is high as criminals take advantage of the distraction to grab and clone private data to tap into funds, intellectual property and more," said Rodney Joffe, senior vice president and senior technologist at Neustar. "Businesses should look out for shorter, more intense attacks without the traditionally expected extortion or policy demands. It is critical that they protect themselves by dedicating staff to watch entry systems during attacks, making sure everything is patched and having dedicated DDoS protection."

Additional insights from the survey include:

- Almost 90 percent of companies attacked were hit repeatedly
- Larger attacks almost tripled. The number of attacks between 1-5 Gbps in size grew by 150 percent

-
- DDoS attacks are consuming more manpower. Attacks requiring more than 10 people to put out the fire more than doubled compared to 2012
 - The costs of DDoS attacks were not only higher, but were felt more widely across the enterprise. Non-IT/security departments absorbed more than 50 percent of attack-related costs and customer support felt the impact most acutely at 63 percent of companies
 - There are now very few companies (under five percent) with no DDoS protection in place. Of the vast majority with protection, most still use traditional solutions like firewalls, switches and routers

Neustar surveyed nearly 450 North American companies in the financial services, technology, retail, government/public sector, health care, energy, telecommunications, e-commerce, Internet services and media industries. The full report, including comprehensive results from the survey and best practices from Neustar's DDoS experts, may be found [here](#).

###

About Neustar

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services and data analytics, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at www.neustar.biz.