
Neustar DDoS Attack Study Quantifies Cost of Attacks

Apr 21, 2015

April 21, 2015 – Sterling, Va. - [Neustar, Inc.](#) (NYSE: [NSR](#)), a trusted, neutral provider of real-time information services and analytics, today announced findings from its [2015 North American Denial of Service \(DDoS\) Attacks & Impact Report](#). The study interviewed 510 North American companies, with nearly one-third earning more than \$1 billion in annual revenue, and underscores the devastating financial consequences of a DDoS attack on a company and its revenues.

Key findings:

- 32 percent of companies would lose more than \$100k in revenue per hour of attack
- 31 percent say their longest attacks last more than one day
- 30 percent of respondents are attacked more than 10 times per year
- 26 percent report DDoS attacks adversely affect customer trust and brand reputation

“These findings begin to quantify the financial damage that a DDoS attack leaves in its wake,” said Margee Abrams, CISSP, director of security services at Neustar. “With the rise of DDoS for-hire websites and increased levels of hacktivism (a cyber-display of disobedience), businesses and the information they possess are attractive targets for nefarious activities,” she added.

While the costs associated with a successful DDoS attack are high in North America, a Neustar study of 250 businesses in Europe and the Middle East and Africa shows that 40 percent of companies in estimate hour losses near \$150,000 – a 470 percent increase from last year.

“The global results make it clear that DDoS attacks are being used as tools for weaponization and smokescreening (a process where a DDoS attack is launched as a diversionary tactic). Businesses, regardless of their industry and location, need to be prepared to defend against DDoS attacks as well as other signs of potential compromise,” said Abrams.

To combat DDoS attacks, Abrams recommended the use of hybrid protection in addition to traditional firewalls and routers.

Hybrid, a highly recommended approach that allows companies to mitigate DDoS attacks by combining on-site hardware and cloud-based solutions, has increased by 20 percent internationally as companies bolster their

defenses against DDoS attacks.

“The increased hybrid adoption reflects the growing need for companies to have immediate, on-premises DDoS defense capabilities along with the capacity to surge defenses in response to larger attacks,” said Abrams.

“Companies continue to rely on layered traditional perimeter defenses including firewalls, routers and switches as well as DDoS mitigation services. But when revenues and brand reputation are at risk, deploying a hybrid solution offers the best of both worlds: immediate on-premises protection with the capacity that only cloud providers can offer.” she added.

From April 20-24, Neustar will have representatives available at the RSA Conference in San Francisco to discuss survey findings. To learn more, RSA visitors are encouraged to visit Neustar at booth number S2520.

About Neustar, Inc.

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.