
DDoS attacks pose biggest threat yet to European businesses

Mar 31, 2015

Survey shows more than half of companies attacked have critical data stolen as a result of DDoS

MARCH 31, 2015 – LONDON, UK – [Neustar](#). Inc. (NYSE: NSR), a trusted, neutral provider of real-time information services and analytics, has today announced findings from its third annual DDoS Attacks & Impact Report.

2015: The Rise of Hybrid Prevention Strategies to Outperform Attackers, is a survey of IT professionals from across the United Kingdom, Europe and the Middle East and Africa (EMEA) to understand the impact of Distributed Denial of Service (DDoS) attacks on business, ways in which companies are managing the crisis, and how attitudes towards DDoS attacks have changed over the past year.

Among the key findings from the survey, a staggering 40 percent of companies estimate hourly losses of over £100,000 at peak times during a DDoS outage, a 470 percent rise since the last Neustar survey almost a year ago. Multiple attacks are also becoming more prevalent and are lasting even longer than those recorded in the last survey, with more than a third of attacks affecting businesses for more than 24 hours. Additionally, 52 percent of companies attacked find themselves the victims of theft, with 24 percent more businesses reporting loss of customer data, intellectual property or money during a DDoS attack compared to last year.

“Businesses need to become more strategic in their approach to fighting these attacks,” said Rodney Joffe, Senior Vice President and Technology Fellow at Neustar. “The use of website stressor services such as Lizard Squad, which lets anyone take down a website for as little as six dollars (four pounds) a month, has become a major source of irritant attacks, with the sizes jumping during 2014,” added Joffe.

Companies, however, are fighting back and a third of all EMEA businesses are now using Hybrid DDoS protection, combining the best of on-premise hardware and cloud-based solutions to tackle these attacks. In the financial sector in particular, the figure of those using a Hybrid Solution jumps to around 40 percent; a reaction to high profile and repeated targeting of financial institutions. According to the survey, 69 percent of financial institutions reported more than six DDoS attacks per year by hackers making a political statement, and thieves targeting money rich resources. Where big money is involved, for example where a DDoS attack could cost over £100,000 per hour, the survey indicates a massive 80 percent of financial institutions deploying a hybrid DDoS

solution.

“These improvements won’t happen overnight or solve everything, but they could make a significant and positive difference,” explained Joffe.

“The online community needs to develop industry-based mitigation technologies that incorporate mechanisms to distribute attack source information into ISPs, so they can squelch the attacks closer to the source. It needs to improve visibility and understanding of activities in the criminal underground, so their command and control structures can be disabled rapidly. Finally, it’s important to improve attribution and law enforcement actions to identify perpetrators and bring them to justice,” he added.

To establish a thorough insight into the impact of these attacks, Neustar surveyed 250 companies in the United Kingdom and throughout the EMEA region, across a diverse range of industries including financial services, technology, retail, government & public sector, health care, energy & utility, telecommunications, e-commerce, Internet services and media. The report revealed that 84 percent of businesses across these sectors use up to 10 staffers to mitigate when attacked, which opens the door to further attacks because when more people focus on a DDoS attack, fewer eyes are watching for other threats like malware or virus installation.

To mitigate DDoS attacks, Neustar blends expertise, proven responses and diverse technologies. Neustar SiteProtect, our DDoS mitigation service, offers: options to meet level of risk, budget and technical environment; cloud-based protection; on-premise, always-on hardware; or a hybrid of both, all of which is fully managed by Neustar. SiteProtect is backed by the Neustar Security Operations Center experts who bring years of experience to blocking DDoS attacks.

Download a copy of the full survey [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.