New DDoS Tactics Expose Businesses to Data Theft

Sep 15, 2015

Rise of repeated 'low and slow' DDoS attacks places sustained pressure on companies' security infrastructure

Neustar, Inc. (NYSE: NSR), a trusted, neutral provider of real-time information services, today released the Europe, Middle East and Africa findings from its DDoS attacks and protection report titled *North America and EMEA: The Continual Threat to Digital Brands for 2015*. The report reveals a significant change in the nature of DDoS attacks that is leaving businesses exposed to data breaches and malware.

The research shines a light on the changing tactics being employed in DDoS attacks, with smaller but more repeated attacks undertaken to distract firms' security and IT teams while malware is installed to steal trade secrets or valuable data. Around 40 percent of attacks are relatively small at less than 5 Gbps.

Such attacks designed to take websites offline are available from hacker groups "for hire" costing as little as €5.29 **(**£3.88) a month. In the wake of online attacks, 36 percent of executives surveyed discovered malware installed in their systems and 25 percent revealed that data or funds had been stolen. In the Financial Services sector the results were even more damaging, with 54 percent of attacks being less than 5 Gbps in strength but 43 percent of all attacks leaving malware or viruses.

Headline findings from the research include:

- DDoS attacks have moved from singular to repeated attack patterns. Half of all surveyed companies suffered a DDoS attack in 2014 and early 2015, with more than 4 out of 5 of those suffering numerous attacks over the period and 54 percent of companies being hit at least six times.
- The duration of DDoS attacks is increasing and causing a sustained threat to businesses' profitability and brand reputation – more than 4 out of every 10 attacks last longer than an entire day, with 10% lasting around a week.
- In the EMEA region, 40 percent of companies' losses due to a DDoS attack occurring during peak hours are greater than €100,000 per hour of downtime.
- 90 percent of the executives and professionals surveyed viewed the threat from DDoS attacks as being greater than or equal to that of last year, with concern focusing on the need to protect against data breaches.

In the report, Mark Tonnesen, CIO and CSO for Neustar, elaborates on this shifting trend of smaller attacks as a cloak for data-mining malware.

“If the attacker’s goal isn’t to cause an outage but to disrupt, he doesn’t need to craft an attack of extra-large proportions. A Syn Flood attack is a good example. The attacker sends enough SYN requests to a company’s system to consume server resources and stall legitimate traffic. It’s a kind of ‘low and slow’ DDoS attack—steady and problematic, though not tsunami-like,” Tonnesen explains. “In launching such an attack, the attacker accomplishes several things: he disrupts operations, distracts the website and security teams, and makes sure the target network is still operational—that is to say, accessible. Now the attacker can go in and plant malware or a virus, setting the stage for data theft, siphoning funds, or whatever else.”

“Think about it: why saturate the pipes if you can’t access the network? Doing the reverse lets attackers harass a target and set the stage for exfiltration. In this sense, a so-called smaller attack can be more dangerous than a huge one that knocks you offline but may not result in a data breach,” he added.

This changing nature of DDoS threats and the rising cost of failing to properly prepare is driving businesses to take steps to mitigate against this risk. More than half of all the executives surveyed had over six staff members dedicated to IT security and DDoS protection, with 55 percent of businesses investing more in DDoS security than last year and 67 percent of attacked companies in the EMEA region now using hybrid protection.

To defend against DDoS attacks, Neustar combines expertise, reliable responses, and diverse technologies. Neustar SiteProtect, a DDoS mitigation service, offers options to meet any businesses level of risk, budget, and technical environment, through cloud-based protection; on-premises, always-on hardware; or a hybrid of both, fully managed by the Neustar Security Operations Centre, whose experts bring years of experience to blocking various attacks.

The report was based on answers received from almost 800 executives and professionals from the United Kingdom, Europe, the Middle East, Africa, and the U.S. in the financial, retail and technology sectors, among others.

About Neustar

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services, 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 https://www.neustar.biz