Neustar Research Reveals 92 Percent of Brands Attacked with DDoS Just Once Suffer Theft

Oct 11, 2017

Survey data shows hackers are getting higher yields from targeted, determined attacks

Neustar, Inc., a trusted, neutral provider of real-time information services, today released its bi-annual Global DDoS Attacks and Cyber Security Insights Report, affirming DDoS attacks continue to be an effective means to distract and confuse security teams while inflicting serious damage on brands. The report highlights that brands experienced a **27 percent increase** in the number of breaches per DDoS attack, despite suffering similar attack levels in the same time period last year.

Data from the report shows attackers are achieving higher levels of success against brands they only hit once: 52 percent of brands reported a virus associated with a DDOS attack, 35 percent reported malware, 21 percent reported ransomware and 18 percent reported lost customer data. Over a twelve-month period, **75 percent** of respondents recorded multiple DDoS attack attempts following an initial assault on their brand's network. The resulting breach ratio increases as the number of DDoS attacks increases, but the net result is it only takes one attack to breach a brand's defenses. Findings suggest that cybercriminals are focused on taunting defenses, probing network vulnerabilities and executing more targeted strikes, instead of making noise with a singular, large attack.

"Not only are hackers becoming craftier and more dangerous, but they're also becoming more opportunistic," said Nicolai Bezsonoff, Vice President, Neustar Security Solutions. "The importance of always-on vigilance and investment in DDoS security technology is essential for brands looking to adapt and evolve their defenses. Protecting a brand's infrastructure and customer data against threats is paramount in the current digital landscape."

Key findings from the report include:

- Brands have a lot to lose – even if attacked only once
    - 92 percent of those attacked just once reported theft of intellectual property, customer data and/or financial assets and resources
    - 89 percent acknowledged some form of associated activity, including data theft, dangerous ransomware, and network compromise with DDoS attacks
    - 36 percent saw malware activation during DDoS attacks as part of multi-tactic assaults
- Internet of Things (IoT) devices remain a tempting target for DDoS attacks

    - 76 percent of brands that have IoT devices in active operation were attacked
    - Of those 76 percent, nearly one-third suffered network compromises or damage to physical equipment
    - 40 percent of respondents are actively focused on finding ways to prevent IoT devices from becoming compromised
- Attacks and breach activities were not contained to large brands
    - Over 50 percent of mid-sized brands encountered an average of three breach incidents (malware, ransomware, virus, etc.)
    - Mid-sized brands were hit the hardest with 60 percent experiencing an attack
    - On average, DDoS attacks caused brands $4.3M in revenue generation risk

Brands are continuing to make DDoS protection a budget priority, with layered defenses and web application firewalls (WAFs) listed as a top investment. Respondents noted that on average their brands have at least two components of DDoS protection that can include appliance hardware, cloud services, and hybrid deployments. Notably, protection against application layer threats has increased significantly with WAF solution deployments nearly tripling in the past year. Using web application firewalls to protect the most exploited layer in the network stack reflects a brand's drive for the right combination of defenses in an effort to protect against growing concerns associated with DDoS attacks.

Top motivators for increased budget spend on DDoS protection include:

- Preserving customer confidence and brand reputation
- Prevention of associated attacks, including ransomware
- Proactively strengthen existing protection

"Brands need to continuously diversify their security strategy for DDoS – it's no longer 'good enough' to accept a pre-packaged solution as the cornerstone of your security portfolio," said Barrett Lyon, Vice President of Research and Development, Neustar Security Solutions. "Writing application code is difficult, but it is also fraught with security failings and attackers know this. Brands are making investments in layered protection, including the deployments of WAF solutions, to level the playing field and decrease the time cybercriminals will have to execute a successful attack."

Methodology: Neustar and Harris Interactive conducted the global, independent research of 1,010 directors, managers, CISOs, CSOs, CTOs, and other C-suite executives to find out how DDoS attacks affect their brands and what measures are in place to counter these threats. The respondents span many industries, including technology, financial services, retail, healthcare and energy.

Join Neustar on October 24 for the first International DDoS Awareness Virtual Conference to learn how brands can protect themselves against cyber threats and fight DDoS attacks.

The full Global DDoS Attacks and Cyber Security Insights report can be downloaded here.