# Neustar Security Report Shows Increased Use of Dangerous Multi-Vector DDoS Attacks Targeting Companies

Mar 31, 2016

**Report Identifies Tactics Deployed by Sophisticated Veteran and Novice Hackers; Offers 5 Key Takeaways for CIOs**

Neustar, Inc. (NYSE: NSR), a trusted, neutral provider of real-time information services, today released its first report from the Neustar Security Operations Center (SOC) that shares technical insights gained from the distributed denial of service (DDoS) attacks mitigated by the company in 2015.

The DDoS attack vectors of 2015 ranged from using DNS (Domain Name System) as a reflection source, one of the oldest types of UDP (User Datagram Protocol) amplification attacks, to targeted strikes using DNSSEC (Domain Name System Security Extensions) signed zones. The company also saw an uptick in attacks using multiple vectors that probed defenses and persisted until they succeed. For companies that are not prepared, the impact of a DDoS attack can cost a company up to US$1 million per hour that the website is down.[1]

"In recent years, DDoS attacks have evolved from a small nuisance to a stealth weapon capable of crippling digital infrastructures," said Brian Foster, Senior Vice President of Information Services for Neustar. "The DDoS attacks of 2015 were persistent, with 32 percent of attacks occurring in Q4 and in time for Cyber Monday. Already in 2016, we are seeing an expansion of the use of DDoS attacks, whether for solo attacks or in conjunction with other sinister activity, including extortion and intrusion."

## Multi-Vector Mayhem

One of the most alarming trends noted in the findings is the rise of multi-vector attacks. Rather than just use one style of method to breach a company's infrastructure, attackers are increasingly turning to multi-vector attacks to exhaust defenses.

"Multi-vector attacks show a higher level of sophistication on behalf of the hackers," said Foster. "Anybody can go to a stressor website and buy a cheap DDoS service, but with multi-vector attacks, the hacker is exhibiting a familiarity with attack methods and determination to potentially cause real damage."

Statistics from Neustar's Security Operations Center uncovered:

- 47 percent of all multi-vector attacks occurred in the fourth quarter
- 17 percent of attacks involved multiple vectors
- 57 percent of all multi-vector attacks involved reflection attacks

"Rather than just hit with a massive DDoS strike, multi-vector attacks are more alarming because they require dexterity, familiarity with attack methods, and they can also be used as a smokescreen to insert malware and sneak out sensitive company information," Foster added.

**Five Key Takeaways**

At this point, it is not a question of "if" there will be an attack but rather "when" a DDoS attack will strike. Hackers, whether sophisticated veterans or solo novices, are determined to do damage with increasingly powerful and easy-to-use array of tools. Based on Neustar's 2015 SOC findings, Foster calls out the following five key takeaways for CIOs:

- **Sometimes A Single Vector Attack Just Will Not Do.** If at first they do not succeed, attackers will try again. Motivated by money and aware that all it takes is one successful breach, attackers are continually working to penetrate defenses through different attack methods.
- **Death by a Thousand Cuts.** Not every attack is intended to cause an outage. By using smaller, pointed assaults, attackers can fly under the radar and avoid network-level DDoS detection. These "low and slow" attacks can disrupt the network and set the stage for exfiltration opportunities.
- **They Are the Most Dangerous Times of the Year.** Attackers chose high-volume transaction periods – such as the tax return period and Q4 for some of their most vicious strikes.
- **Defend your DNS.** Attacks on DNS skyrocketed in Q4. As the layer of the Internet that is initially most critical for a company's digital presence, DNS is often the first target of a DDoS attack, and the least protected. No DNS = no website.
- **The Combat Continues.** DDoS attacks are inevitable. As too many companies, organizations and governments found out, it is no longer a matter of if or when, but how often the attacks will occur. As hackers continue to innovate ways to attack, the best defense remains an active, vigilant defense.

The full Neustar Security Operations Center report details attack sizes, strategies, and stories from the SOC. The report is comprised of attacks that Neustar has defended on behalf of its clients in 2015. To protect customer privacy and security, no client names or identifying information are provided in the report.

Download the Neustar Security Operations Center report here.

**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.