
Neustar Reports Rampant Growth of DDoS Attacks in 2016

Dec 19, 2016

Mitigation of Multi-vector DDoS Attacks Has Increased 322 Percent in 2016;

IoT Botnets, DNS-based Attacks and Conventional DDoS Attacks Present On-going Risk

December 19, 2016 – STERLING, Va. – [Neustar](#), Inc. (NYSE: NSR), a trusted, neutral provider of real-time information services, today announced the publication of “[DDoS & Cyber Security Insights](#),” an in-depth research report that provides statistical analysis of the distributed denial of services (DDoS) attack and mitigation data collected through Neustar SiteProtect. The report examines the growth of DDoS attacks during 2016, providing specific insight into multiple attack vectors, such as DNSSEC amplification and Internet-of-things (IoT) botnets.

“The DDoS attack landscape has become increasingly complex in 2016 because there is no singular goal behind these attacks; some seek to disrupt services, while others serve as smokescreens to breach data,” said Rodney Joffe, SVP and Fellow, Neustar. “Organizations must remain vigilant against conventional attacks, even as new threats are realized today and in 2017.”

“DDoS & Cyber Security Insights” analyzes attack and mitigation data collected through Neustar SiteProtect, a global DDoS mitigation network, from January 1, 2016 through November 30, 2016. Key findings include:

- **Increasing Frequency of DDoS Attacks** – The frequency of DDoS attack mitigations by Neustar has increased 40 percent compared to the same period of time in 2015.
- **Eruption of Multi-vector Attacks** – Multi-vector attacks, which combine attack vectors to confuse defenders and supplement attack volume, increased 322 percent and accounted for 52 percent of the attacks mitigated by Neustar. UDP, TCP and ICMP comprise the three most popular attack vectors, which were leveraged in more than 50 percent of attacks.
- **Vulnerability of DNS and DNSSEC** – DNS-based attacks increased 648 percent with many attackers leveraging DNSSEC amplification to generate massive volumetric pressure. Previous Neustar research, “[DNSSEC: How Savvy DDoS Attackers Are Using Our Defenses Against Us](#),” determined that the average DNSSEC amplification factor for a DNSSEC signed zone was nearly 29 times greater than the initial query.
- **IoT Botnets Emerge as DDoS Attack Tools** - The threat of IoT botnets was realized in 2016, which was popularized by Mirai. Mirai and similar types of malware compromise IoT device credentials to enroll them into botnets, which are activated by command and control servers. As these code assemblies are published, new developments continue to emerge, such as persistent device enrollment, which enables botnet operators to maintain control of a device even after it is rebooted.

“Mirai signals a watershed moment for DDoS attacks, where the bad guys finally turned the Internet back on its users,” said Joffe. “It is imperative to invest in effective DDoS protection now because the threat landscape has fundamentally changed.

For more information about “Neustar Customer Security Operations Report,” please visit <https://hello.neustar.biz/2016-soc-report-security-lp.html>

About Neustar

Every day, the world generates roughly 2.5 quadrillion bits of data. Neustar (NYSE: NSR) isolates certain elements and analyzes, simplifies and edits them to make precise and valuable decisions that drive results. As one of the few companies capable of knowing with certainty who is on the other end of every interaction, we’re trusted by the world’s great brands to make critical decisions some 20 billion times a day. We help marketers send timely and relevant messages to the right people. Because we can authoritatively tell a client exactly who is calling or connecting with them, we make critical real-time responses possible. And the same comprehensive information that enables our clients to direct and manage orders also stops attackers. We know when someone isn’t who they claim to be, which helps stop fraud and denial of service before they’re a problem. Because we’re also an experienced manager of some of the world’s most complex databases, we help clients control their online identity, registering and protecting their domain name, and routing traffic to the correct network address. By linking the most essential information with the people who depend on it, we provide more than 12,000 clients worldwide with decisions—not just data. More information is available at <https://www.neustar.biz>

Neustar Media Contact

Clinton Karr

Clinton.karr@neustar.biz

(415) 590-4611

