Neustar's Third DDoS Survey Finds Attacks Unrelenting in 2015 with 73% of Global Brands & Organizations Attacked

Apr 26, 2016

- *82% of corporations were attacked repeatedly; 57% suffered subsequent theft*
- *IoT opens up new threat vectors – 63% have IoT deployed and of those – 4 out of 5 have been hit with DDoS attacks*

Neustar, Inc. (NYSE:NSR), a trusted, neutral provider of real-time information services, today released the findings from its third global DDoS Attacks and Protection Report titled *The Threatscape Widens: DDoS Aggression and the Evolution of IoT Risks*. The April 2016 report follows a survey of over 1,000 IT professionals across six continents, and reveals that few organizations globally are being spared DDoS attacks. With the bombardment fairly constant throughout 2015, it is no longer a matter of if or when attacks might happen, but how often and how long the attack will last. Faced with this ongoing onslaught, the report demonstrates that increasingly DDoS-defense savvy organizations are now arming themselves accordingly.

The research results show that although revenue loss caused by a DDoS related outage is usually the main concern, 57% of all breaches involved some sort of theft including intellectual property and customer data as well as financial information. More troubling, following the initial breach, 45% of organizations reported the installation of a virus or malware - a sign that attackers are interested in causing ongoing harm.

The research highlights that although DDoS attack tactics continue to evolve from single large attacks intended to take a website offline to the multi-vector attacks we are seeing today, organizations are fighting back. The good news is 76% of companies are investing more in DDoS protection than in 2014 and 47% of the attacked organizations are participating in security consortiums to share information on threats and counter measures.

Headline findings from the research include:

- 73% (7 in 10) of global brands and organizations were attacked, which should put virtually every organization with a digital presence on notice.
- 82% of organizations experiencing a DDoS attack were then attacked repeatedly, with 45% reporting they were attacked 6 or more times. In EMEA, 47% of organization have been struck more than 5 times.
- More than half (57%) of organizations reported theft after attack, including loss of customer data, finances or intellectual property.
- 50% of organizations would lose at least $100,000 per hour in a peak-time DDoS related outage (33% would lose more than $250,000 per hour), and 42% needed at least three hours to detect that they were under DDoS attack.
- 76% of organizations are investing more than last year in response to the DDoS threat.
- 71% of financial services firms attacked experienced some form of theft and 38% found viruses or

malware activation after an attack. With big money, customer trust and regulatory implications on the line, 79% of financial services organizations are investing more this year than last.

“The findings of our most recent report are clear: attacks are unrelenting around the world but organizations are now recognizing DDoS attacks for what they are - an institutionalized weapon of cyber warfare – and so are protecting themselves,” says Rodney Joffe, Head of IT Security Research at Neustar. “We present the data from our third DDoS survey as a means to inform the public of the dangers associated with DDoS attacks, and advance a conversation about the importance of multi-layered cybersecurity. This should be a discourse that reaches from security through to marketing, as when a DDoS attack hits, the reverberations are felt like a domino effect throughout all departments.”

Why IoT offers a second chance to improve security

In addition to examining the DDoS trends of 2015, for the first time the survey also asked respondents to consider what the future portends for companies deploying IoT connected devices, providing insight into why security needs to be a central tenet for devices in the future. The survey found that while 63% of companies have IoT devices already deployed only 34% have security measures in place, indicating the IoT is opening up new threat vectors but too few organizations are focused on preventing connected devices from being compromised.

Hank Skorny, Neustar IoT expert, comments on security and IoT: “Although IoT is already here, the Internet was never built with security in mind; ease of use and convenience were paramount. By 2017, 81% of organizations will have devices deployed to collect and analyze data so today, we have the opportunity to learn from our mistakes and make security a cornerstone of every IoT device moving forward. From design conception, every IoT device, sensor, and software system needs a multi-tiered security driven approach, including timely patches and updates. Just as important, or perhaps more so, is for security to be an intrinsic part of every network. Every IT professional knows it can take just one successful hack on an IoT device to access and compromise an entire network. As IoT devices continue to become ingrained into our electrical grid, hospitals, assembly lines and other essential areas of life, the stakes are simply too high to leave security to chance.”

The Neustar April 2016 DDoS Attacks and Protection Report: *The Threatscape Widens: DDoS Aggression and the Evolution of IoT Risks* is based on answers received from over 1,000 directors, managers, CISOs, CSOs, CTOs and other security directors from six continents in the technology (18% of respondents), financial services (16%), retail (12%), and government (8%) sectors and others.