Neustar Global DDoS Report Reveals Seven Key Trends, Including Attacks Evolving from Disruptive to Continuous Threat

Sep 30, 2015

Hackers use smaller, more sustained attacks to cause distraction while malware is installed to steal company trade secrets and valuable data

Neustar, Inc. (NYSE: NSR), a trusted, neutral provider of real-time information services, today released the findings of its latest DDoS Attacks and Protection report, including seven key trends. The global research reveals more activity around targeted, smaller assaults aimed at distracting firms' IT departments while malware is installed to steal valuable corporate data.

Seven key findings from the research include:

1. 1 in 10 companies surveyed risked an **average of $1 Million or more** if website was down for one hour during peak revenue period.
2. **It's not if, not when, but how frequently:** 50 percent of companies suffered a DDoS attack and 8 in 10 of those struck were targeted more than once.
3. **Attackers infiltrate with purpose, using DDoS as a weapon of distraction:** when attacked, 50 percent of companies reported some form of theft (customer data, intellectual property, financial) and 36 percent of companies were infected with malware or viruses.
4. **When caught by surprise, brands lose credibility:** more than 1/3 of organizations hit learned of the attack from customers, partners, or other 3rd-parties. In EMEA, of those who learned via 3rd-party, 79 percent experienced some form of associated theft.
5. **"Slow and steady" have lasting repercussions:** rather than trying to overwhelm networks, attackers often use a "slow and low" strategy, deploying smaller attacks to disrupt and distract, install malware, steal data or funds, and tarnish the brand.
6. **Companies feel the sting in customer-facing areas:** once solely considered a security or IT problem, DDoS attacks now ripple through every part of the business. Top three areas affected by DDoS attacks are: **Customer Support** (41 percent), **Brand Damage** (35 percent), **Marketing/Online Promotional Spend** (25 percent).
7. **Companies realize the threat is valid:** 54 percent of companies are investing more in DDoS protection as compared to a year ago.

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.”

Attack methodology has evolved from singular incidents to repeated attack patterns with the majority causing a persistent threat to profitability and brand reputation. Attackers with malicious intent no longer need to be an expert to execute these destructive attacks; DDoS tools allowing anyone to take down online services are inexpensive and readily available.

“Organizations are often caught off guard during a DDoS attack and don’t realize they’ve been infected until alerted by their customers or a third-party said,” Christian Christiansen, Program Vice President for IDC's Security Products and Services group. “The consequences can be damaging creating a bad customer experience, which can increase costs and decrease revenue flow.”

In the wake of online attacks, organizations must consider the continuous risk to digital reputation – 33 percent of those surveyed discovered attacks from a third party, including customers and partners. Proactive protection is essential; statistics show once an organization is attacked the chances of experiencing a breach are more than 70 percent.

“Think about it: why saturate the pipes so that 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,” Tonnesen added.

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 Center, whose experts bring years of experience to blocking every attack.

The report was based on answers received from nearly 800 executives and professionals from the United

Kingdom, Europe the Middle East, Africa and the U.S. in the financial, retail, technology and healthcare sectors among others. It is available for download here: https://www.neustar.biz/lp/security/oct-ddos-report/index.php

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