Hope is Not a Strategy

2012 Annual DDoS Attack and Impact Survey: A Year-to-Year Analysis

neustar®
Real Intelligence. Better Decisions.™

CONTENTS

Introduction

Last year, Neustar reported on the DDoS landscape during 2011. This year, we surveyed IT pros on their experiences in 2012. Did the threat of DDoS grow or shrink? What were the costs of downtime? In total, were companies better prepared to protect their websites and their brands?

In comparing threats to readiness, the answers aren't encouraging:

- DDoS attacks continue to grow in frequency and impact
- While a handful of massive attacks dominated the headlines – especially in the banking industry, where many suspect the hand of unfriendly nation-states – most DDoS attacks are less than 100Mbps in size
- As in 2011, over 1/3 of attacks lasted longer than 24 hours, extending downtime, customer complaints and mitigation costs
- Connecting the dots: it doesn't take a mega-attack to cause lasting damage, merely well-planned strikes on poorly defended websites
- While more companies are investing in some type of DDoS protection…
- Most still rely on firewalls and other traditional solutions that get bottlenecked during attacks and accelerate outages

Again, the data reported here is from a wide-ranging survey, not from Neustar's network monitoring or DDoS mitigation efforts. The data reflects the realities faced by diverse IT professionals across numerous industries, among companies large and small. It shows the real challenge most companies face today: how to gauge the threat clearly and respond within their means.

Survey Findings, 2012–2011

When DDoS attacks hit, organizations are thrown into crisis mode. From the IT department to call centers, to the board room and beyond, it's all hands on deck until the danger passes. In February 2013, Neustar surveyed IT professionals across North America to understand how companies are managing the crisis and to measure its business impact. Most respondents were network services managers, senior systems engineers, systems administrators and directors of IT operations. A total of 704 respondents shared details about attacks, defenses and financial losses. Of this group, 295 worked for ecommerce companies whose success depends on selling products or services online.

This report also compares 2012 results with survey findings from 2011, detailed in last year's Neustar report "When Businesses Go Dark." The 2012 findings outline the costs of DDoS attacks, how companies are responding to threats and the unique challenges for companies conducting ecommerce.

Key questions revisited from 2011 include:

- Who has been attacked and who hasn't?
- What are the costs of DDoS outages?
- How long have attacks lasted?
- What types of DDoS protection are people using?

Additionally, the survey asked:

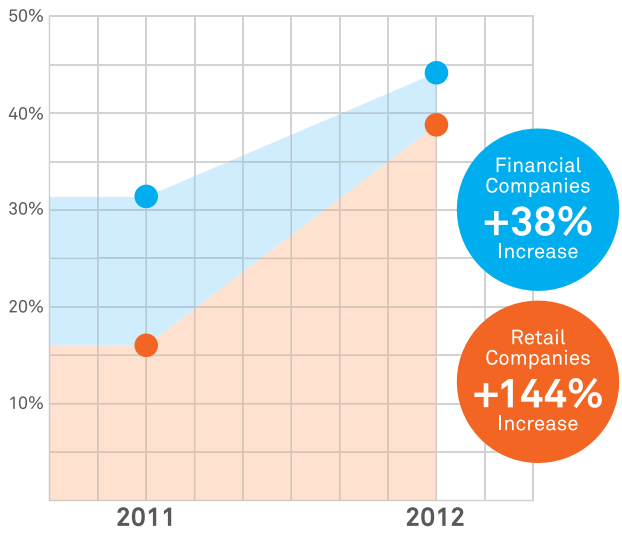
- What are the sizes of DDoS attacks?
- What are the velocities of DDoS attacks in packets per second?

The survey also examined the costs associated with DDoS attacks:

- How many people per organization are involved in DDoS responses?
- What areas of operation experienced the greatest cost increases in a DDoS attack?

Have you experienced a DDoS attack?

In 2012, 35% of companies experienced a disruptive attack. The retail sector showed the most alarming year-to-year increase. In 2011, only 16% of participating retailers reported being hit. In 2012, this increased by 144%: 39% of all retailers came under attack, along with 41% of ecommerce businesses.

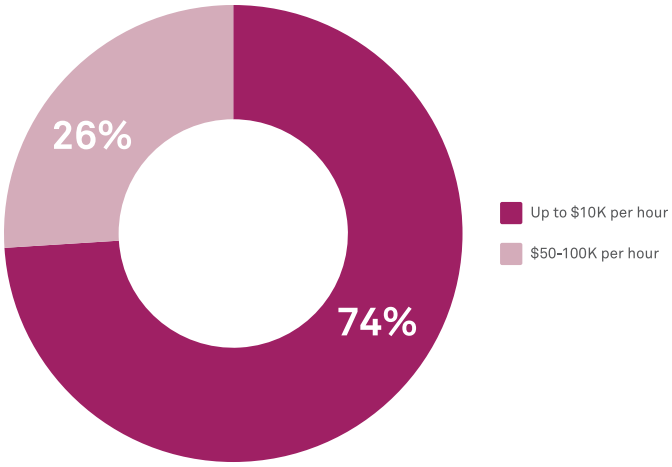


As in 2011, financial and ecommerce businesses were the most frequent DDoS victims. Last year, 32% of financial organizations reported being attacked. In 2012, the number increased to 44%. Starting in Q3 2012 and continuing to the present, banks in particular have suffered large, disruptive attacks, with specialized botnets such as "itsoknoproblembro" amplifying the destructive impact.

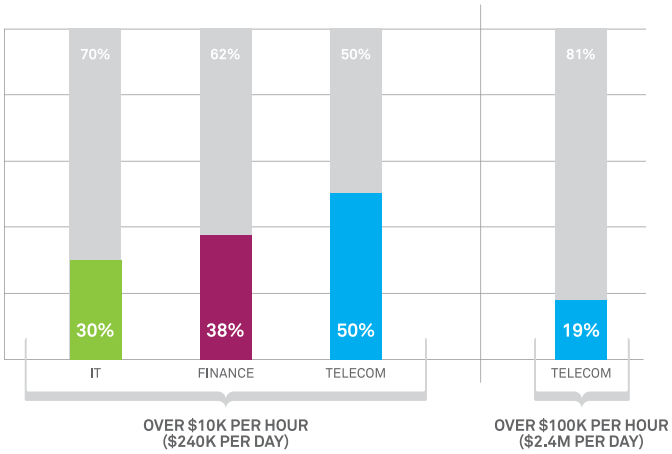
The number of DDoS attacks in the IT and telecom industries remained relatively unchanged from 2011. 42% of government agencies reported being victimized. The 2011 survey did not include this industry.

What is the financial impact of a DDoS attack?

A DDoS attack can inflict a grave toll on revenues. Overall, the reported revenue risk was slightly lower than in 2011, owing to the increased investment in DDoS protection solutions (see p. 6). Even so, more companies in 2012 (74% vs. 65% in 2011) said a DDoS outage would cost them up to $10K per hour, potentially almost a quarter of a million dollars a day. 26% reported revenue risks at $50–100K per hour.



Among key industries, financial services, telecom and IT projected the highest DDoS related bottom-line risks.



Ouch!

1 in 5 financial companies estimated outages would drain their revenues by $50K per hour. CNBC reports that in early 2013 U.S. banks, targets of the largest wave of DDoS ever, were knocked offline a total of 249 hours. 249 x 50,000 = $12,450,000. And that's just revenue. Resource allocation and loss of brand equity/ consumer trust should be factored in too.

Beyond immediate loss of revenue, DDoS exacts costs that are difficult to measure: erosion of brand value, reputation and customer trust. From a product page that won't load to a ticket purchase that can't be confirmed, short-term inconveniences become long-term PR problems. Far worse than unsold shoes that remain in inventory are customers left wondering what happened to their purchases. Did they complete the process? Are their credit card numbers safe? As call center lines become overloaded and hold times increase, the chance to salvage the customer relationship dims. In an instant, a positive shopping experience becomes an urgent complaint.

Are customers willing to forgive and trust the company next time? If yes, will they purchase at their previous levels? These questions are difficult to answer. Even if they could, many companies would be unwilling to reveal such information.

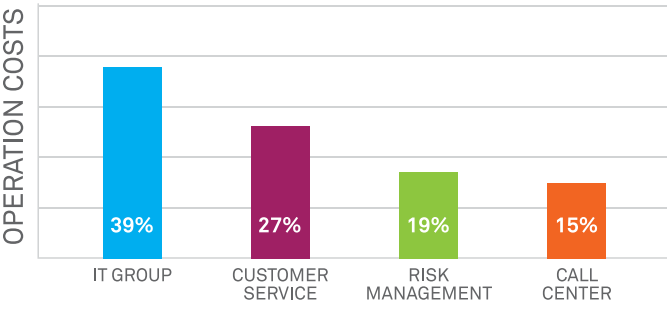
To identify the costs related to DDoS protection, including those specifically associated with attacks, the 2012 survey asked several new questions. The first addressed staffing levels for attack mitigation.

How many people are involved in DDoS mitigation?

Overall, companies reported that 45% of attacks involved 2 to 5 people in mitigation; 33% required more than 6 people. As expected, ecommerce companies needed more staff to handle attacks.

To clarify the impact on operational costs, the 2012 survey asked respondents to identify the two areas of their organization with the highest related costs. The IT group was the leading area at 39%, with customer service second at 27%.

Areas of greatest cost increases in a DDoS attack

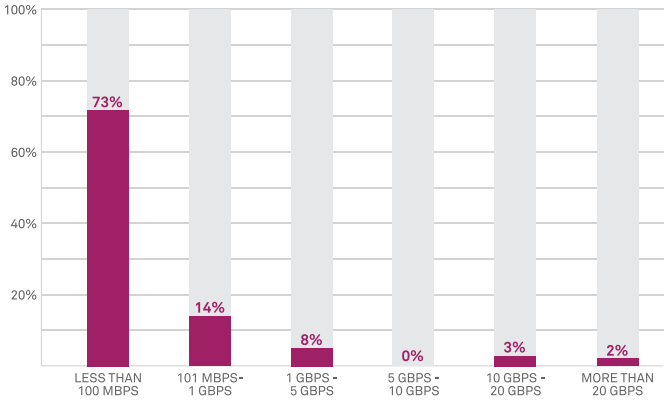


How big were DDoS attacks in 2012?

In 2012, the survey expanded to reveal information about the size of attacks as measured in bandwidth and packets per second.

Attacks Measured in Bandwidth

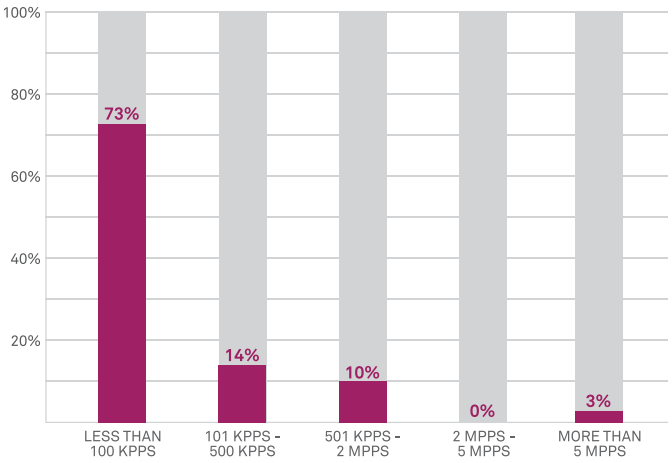
Any attack, including Layer 7 application attacks, can be measured in terms of bandwidth. Following is a breakdown of attacks by bandwidth size.



Industry experts agree that a well-crafted, multi-vector attack as small as 2 Gbps, a common attack size, can take down a site.

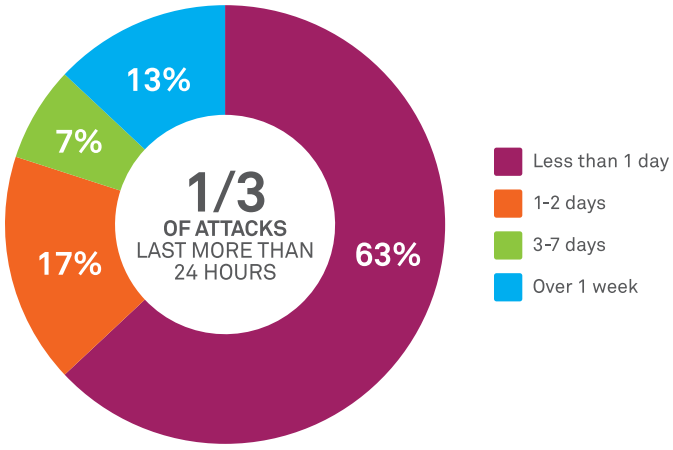
Attacks Measured in Packets Per Second

The survey also looked at the size of Layer 3 network attacks as measured in packets per second, a standard measurement of traffic flowing through network routers.



How long did DDoS attacks last?

Tracking with last year's results, over a third of all DDoS attacks lasted more than 24 hours: 37% in 2012 versus 35% in 2011.



How big is big enough?

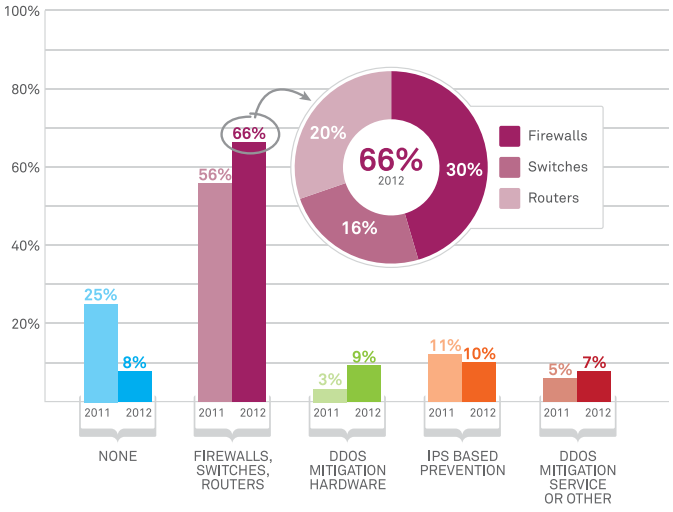
In early 2013, the news was filled with massive, high-profile DDoS attacks. The attack that shut down Spamhaus, the well-known spam tracker, was reportedly measured at 300+ Gbps. Some attacks on major banks may have reached over 150 Gbps.

But while industry reports estimate that DDoS attacks increased in size an average of 27% – from 1.23 Gbps in 2011 to 1.56 Gbps in June 2012 according to Arbor Networks – successful attacks typically use less than 2 Gbps per second. It's useful to remember that many experts believe a nation-state is behind the attacks on U.S. banks. The DDoS attackers most businesses face, whether extortionists or mercenaries hired by competitors, lack the resources (or indeed, the need) to unleash a tidal wave. With basic tools and modest bandwidth, they can launch a DDoS attack big enough to cripple the average business site.

Some attacks stretched out for several days or even longer. In fact, 20% of attacks lasted between 3 days and 7+ days. The longest attacks, those lasting over a week, increased from 10% in 2011 to 13% in 2012.

What kind of DDoS protection was used?

If there was a glimmer of good news in 2012, it was the rise in DDoS protection. In 2011, fully 25% of companies reported having no DDoS protection in place. Just one year later that number dropped to only 8%. There was a 10% increase in the use of firewalls, switches and routers; a 6% increase in DDoS mitigation hardware; and a 2% increase in other protection measures.



While this would seem like a positive trend, it's important to note the distinction between network protection solutions and DDoS protection solutions. Firewalls, routers and switches can protect against intrusive attacks at Layer 3 (to some extent) but compound the effects of DDoS attacks by bottlenecking traffic. In fact, attackers often hit both the network and application layers. Routers are not effective against Layer 7 application attacks.

More respondents used on-premise hardware to mitigate attacks in 2012, 9% versus 3% in 2011. Larger organizations with specialized IT staff are best equipped to do this.

"For those organizations that determine they are most at risk and have made the decision to invest budget in a comprehensive DDoS strategy, IDC finds it should include the following: A mix of on-premise and cloud monitoring and mitigation managed internally or externally or a combination of the two."

– IDC Worldwide DDoS Prevention Products and Services 2013-2017 Forecast, doc #239954, March 2013

Intrusion detection systems saw a 1% decline in use. Like a firewall, an IDS becomes a bottleneck during DDoS attacks. It can, however, help defend against growing two-pronged attacks, in which DDoS is a distraction while the attacker breaches the system, aiming to steal customer data, government secrets or intellectual property.

Survey Conclusions

For most businesses, DDoS attacks are either a reality or an impending threat, one that outpaces protection solutions currently in place.

- In key sectors, approximately 40% of companies reported being attacked, including retail and ecommerce, telecom, financial services and government
- The potential cost of DDoS attacks continues to be a concern, with downtime costs estimated as high as $100K per hour.
- DDoS increases the cost of business operations, particularly among IT and customer service departments.
- In the vast majority of cases, DDoS attacks were under 100Mbps. While they grab more attention, mega-attacks are rare. Modest-sized attacks can inflict sufficient pain.
- Though more companies are deploying DDoS protection – only 8% had none in place compared to 25% in 2011 – few have invested in purpose-built hardware or third-party expertise.
- The latter is alarming; while 66% of companies use firewalls, routers and switches for DDoS protection, these networking products create bottlenecks that actually aid attackers.

Clearly, many companies are hoping traditional defenses will suffice. Given the evidence, such hopes are badly misplaced.

Neustar SiteProtect

Neustar SiteProtect offers intelligent DDoS protection, blending the people, processes and technologies to stop today's complex attacks. Using battle-tested procedures and best-of-breed equipment, the experts in the Neustar Security Operations Center work swiftly to eliminate downtime and protect your brand.

Based in the cloud, SiteProtect offers 24/7 on-demand traffic scrubbing. Immediately accessible through DNS or BGP re-direction, it provides instant relief from DDoS attacks involving network Layer 3, application Layer 7, IPv6 and/or encrypted traffic – or any combination of these takedown methods. SiteProtect reroutes traffic to unclog your network, filters malicious traffic and permits valid traffic to return to your infrastructure.

Built on a dedicated, globally distributed Anycast network, SiteProtect can be instantly deployed and remains activated until the danger is gone. With SiteProtect handling the DDoS, your responses remain nimble and in sync with customer requests. Online business continues even as the attack unfolds.

For larger organizations, SiteProtect is an ideal complement to in-house mitigation hardware. As a cloud-based failover solution, SiteProtect provides the bandwidth to absorb malicious traffic and enables you to launch counter-measures in real time. Using a hybrid approach, you can leverage your investments in DDoS detection and alerting, avoid outages and minimize disruptions.

When it comes to DDoS protection, we've got you covered. Learn more at www.neustar.biz/enterprise.

Appendix: DDoS and Ecommerce

With so much on the line, website outages from DDoS attacks are especially painful for ecommerce companies.

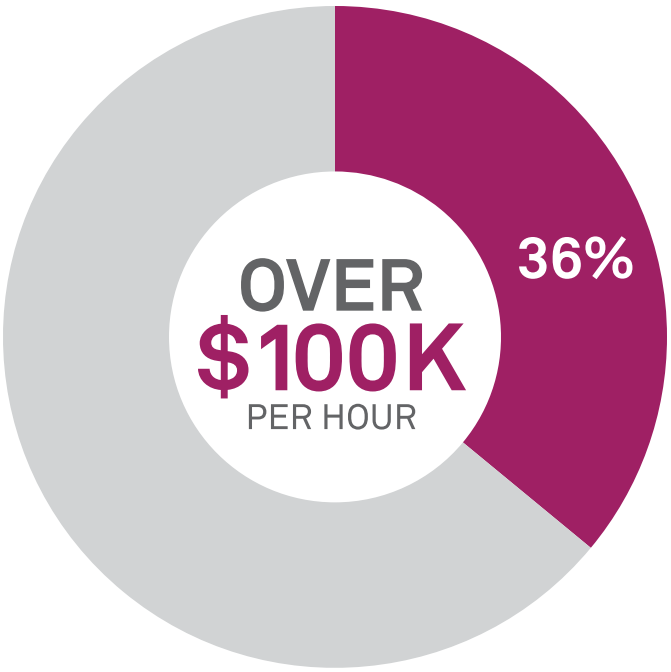
Have you ever been DDoS-attacked?

In 2012, 45% of ecommerce businesses reported being attacked.

What is the financial impact of a DDoS attack?

Companies in ecommerce face the greatest potential DDoS costs: 40% reported in 2012 that a DDoS outage would cost them over $10K per hour and 20% projected losses over $50K per hour. 12% said losses would reach over $100K per hour.

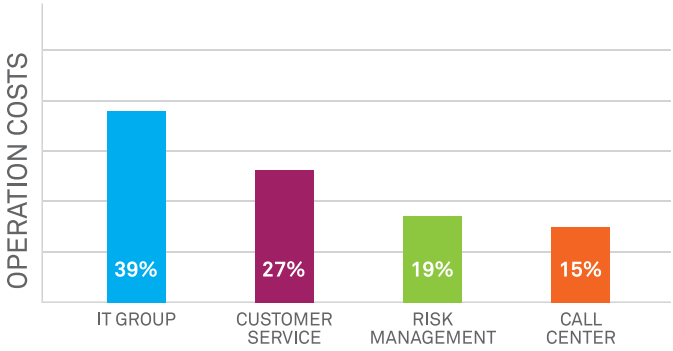
In the retail ecommerce sector, the risks were especially steep: 36% projected outage losses at over $100K per hour.



As expected, ecommerce companies require more staff to respond to DDoS attacks.

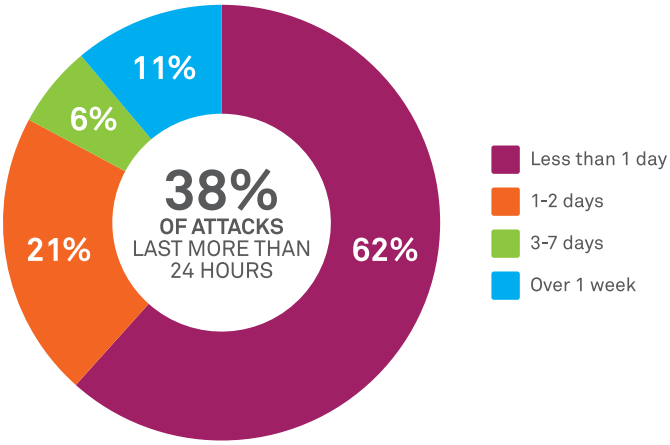
42% reported that 6 or more people were involved in mitigation, while 26% utilized teams of 10 people or more.

The impact of attacks was felt across various departments.



How long do DDoS attacks last?

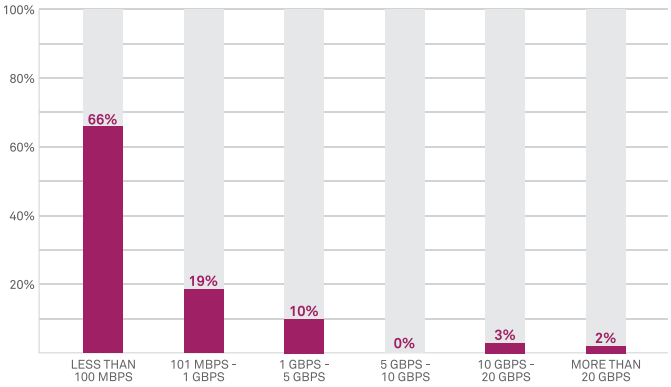
38% of ecommerce companies experienced attacks lasting more than 24 hours. In fact, 17% reported attacks lasting from 3 days to 7+ days.



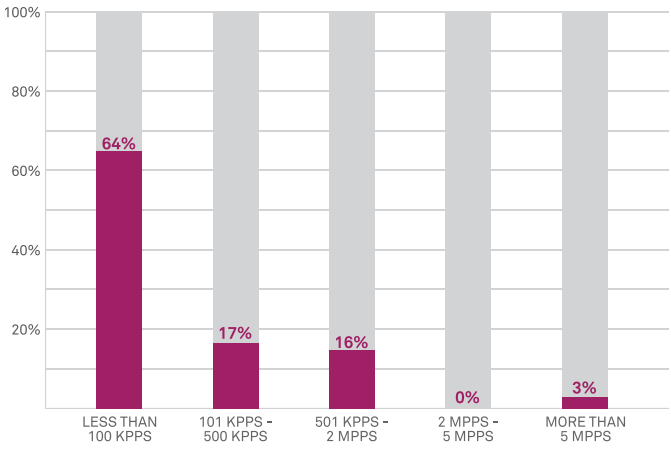
How big were DDoS attacks in 2012?

In ecommerce, DDoS attack sizes were similar to those in other sectors.

Attacks Measured in Bandwidth



Attacks Measured in Packets Per Second



FOR MORE INFORMATION

Visit **www.neustar.biz/enterprise**

About Neustar

Neustar, Inc., (NYSE: NSR) is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, information services, financial services, retail, media and advertising sectors. Neustar applies its advanced, secure technologies in location, identification, and evaluation to help its customers promote and protect their businesses. More information is available at **www.neustar.biz.**

21575 Ridgetop Circle, Sterling, VA 20166
+1 571 434 5400 / www.neustar.biz

V1-04/23/2013

neustar®
Real **Intelligence.** Better **Decisions.**™