2014 THE DANGER DEEPENS

Neustar Annual DDoS Attacks and Impact Report

neustar®

Contents

Welcome to the 2014 DDoS Attacks and Impact Report

For the third consecutive year, Neustar surveyed hundreds of companies on distributed denial of service (DDoS) attacks. What were their experiences in 2013? The results suggest a more unstable and complex landscape.

DDoS Attacks: More Unpredictable than Ever

Over the last year, DDoS attacks evolved in strategy and tactics. We saw increased media reports of "smokescreening", where criminals use DDoS attacks to distract IT staff while inserting malware to breach bank accounts and customer data. More than half of attacked companies reported theft of funds, data or intellectual property. Such cyber attacks are intense but shorter-lived, more surgical than sustained strikes whose goal is extended downtime.

Neustar's survey reveals further evidence that the DDoS attack landscape is changing. The number of companies attacked is up, but attack duration is down. Larger attacks are more common, but most attacks are still less than 1 Gbps. Companies report a greater financial risk during a DDoS outage; however, most still rely on traditional defenses like firewalls, not purpose-built solutions like DDoS mitigation hardware or cloud services.

Companies understand the threat level is high.

It's a picture of uncertainty. But one thing is clear: businesses perceive the DDoS attack threat as real.

More than 47 percent view DDoS attacks as a greater threat than in 2012, while another 44 percent believe the problem is just as serious. In 2013, DDoS continued to cripple websites, shut down operations and cost millions of dollars in downtime, customer service and brand damage.

Report Methodology

Neustar surveyed nearly 450 companies in North America, across numerous industries: financial services, technology, retail, government/public sector, health care, energy/utility, telecommunications, e-commerce, Internet services and media.

Key questions revisited from 2012:

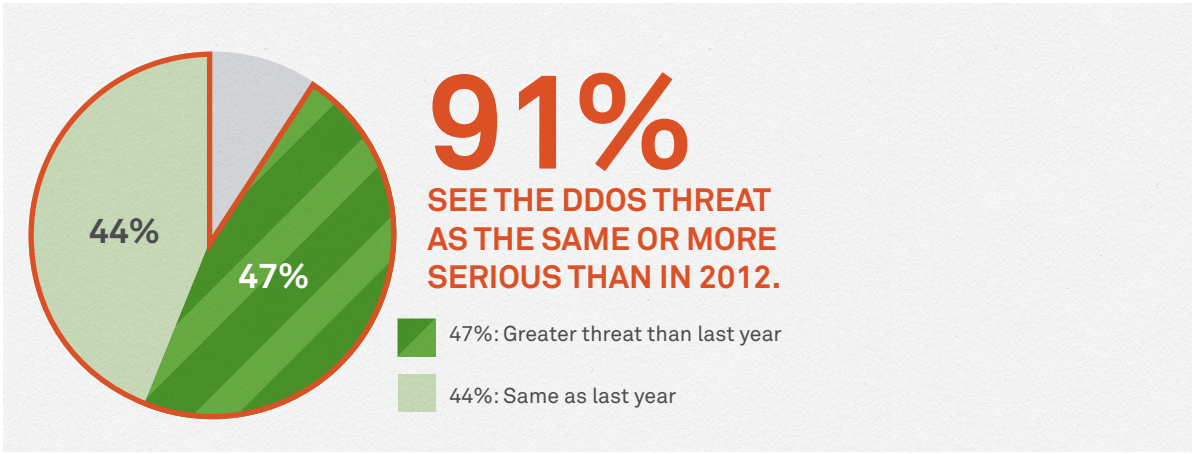
- How many companies were attacked?
- What are the costs of DDoS outages?
- What are the sizes and velocities of DDoS attacks?
- How long are DDoS attacks lasting?
- How many people are involved in attack mitigation?
- Which departments feel the greatest cost impact?
- What types of DDoS protection are businesses using?

New questions asked:

- Are DDoS attacks a bigger or smaller threat to your business versus a year ago?
- How often were you attacked?
- What were the impacts of data breaches that occurred during DDoS attacks?
- Which areas of your business did DDoS most affect?

Companies perceive the problem is growing.

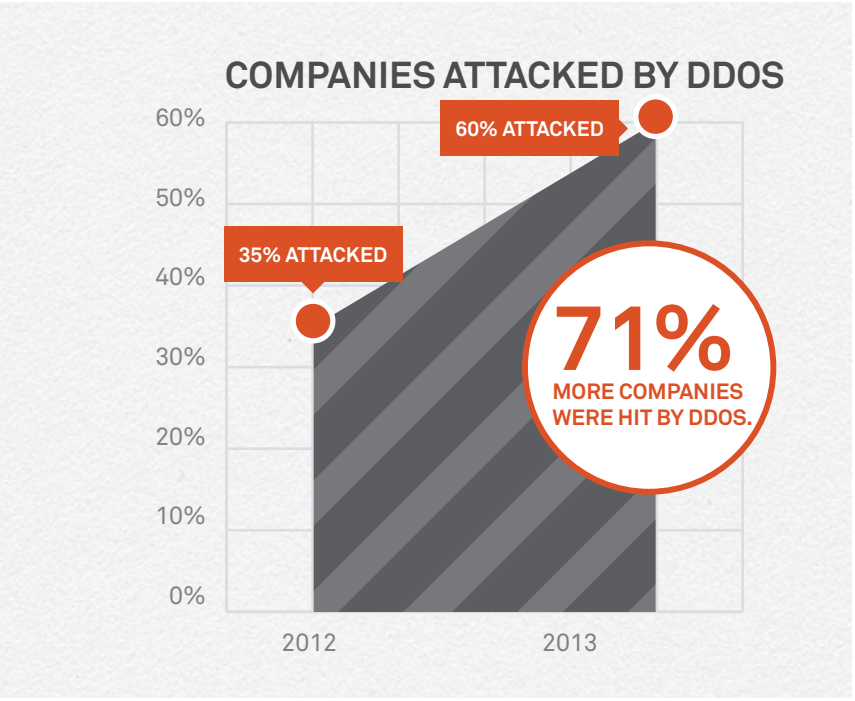
Over 90 percent of respondents see DDoS attacks as a similar or bigger threat than in the previous year. Businesses see that the problem is not going away.



The next finding is one big reason why companies believe the threat is undiminished.

Nearly twice as many businesses report being attacked.

In 2013, 60 percent of companies were DDoS-attacked, up from 35 percent experiencing a disruptive attack in 2012. With nearly twice as many targets, 2013 was a busy year for attackers.



87% of companies attacked were hit multiple times.

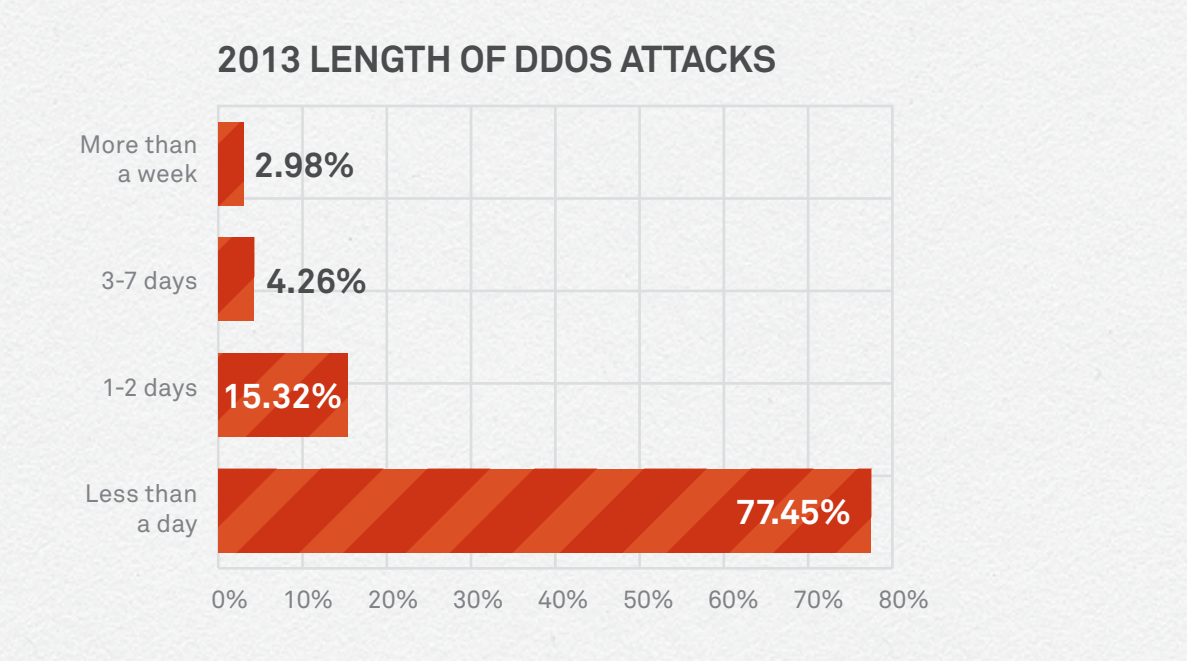
This year's survey asked companies that experienced DDoS attacks how often they occurred.

Just once: 12.88%
2-5 times: 34.09%
6-10 times: 12.5%
Weekly: 13.64%
Monthly: 9.47%
We lost count: 17.42%

Only 13 percent of these companies were attacked just once. Over 45 percent were targeted 2 to 10 times. Over 10 percent were targeted weekly, while over 15 percent lost count.

Attacks on average are shorter.

In 2012, 63 percent of companies reported that DDoS attacks lasted less than a day. In 2013, 77 percent reported the same. Moreover, last year, under 2 percent reported attacks lasting a week, while the previous year that number was 13 percent.

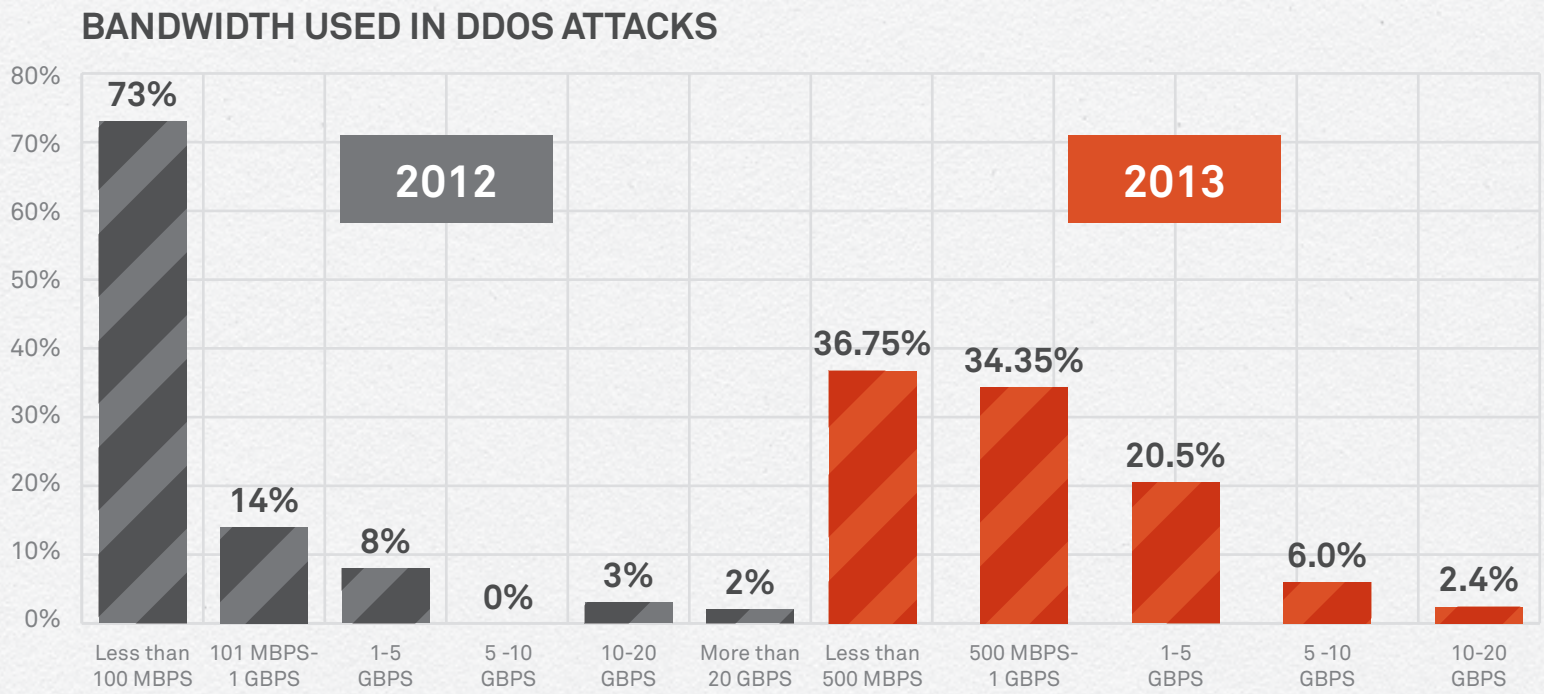


Attacks between 1-5 Gbps almost tripled.

DDoS Attack Size in Bandwidth

Bandwidth is one way to measure DDoS attacks, including Layer 7 (application layer) attacks. In 2013, 73 percent of DDoS attacks were under 1 Gbps—down from 87 percent in 2012, but still representing nearly three out of four attacks. Attacks between 1-5 Gbps grew by 150 percent, from 8 percent in 2012 to over 20 percent in 2013. Notably, DDoS attacks over 10 Gbps dropped by half, from 5 percent in 2012 to 2.4 percent in 2013.

The graph below compares DDoS attack size in bandwidth from 2012 to 2013. The scale was adjusted in 2013 to reflect the growing size of attacks over 1 Gbps.



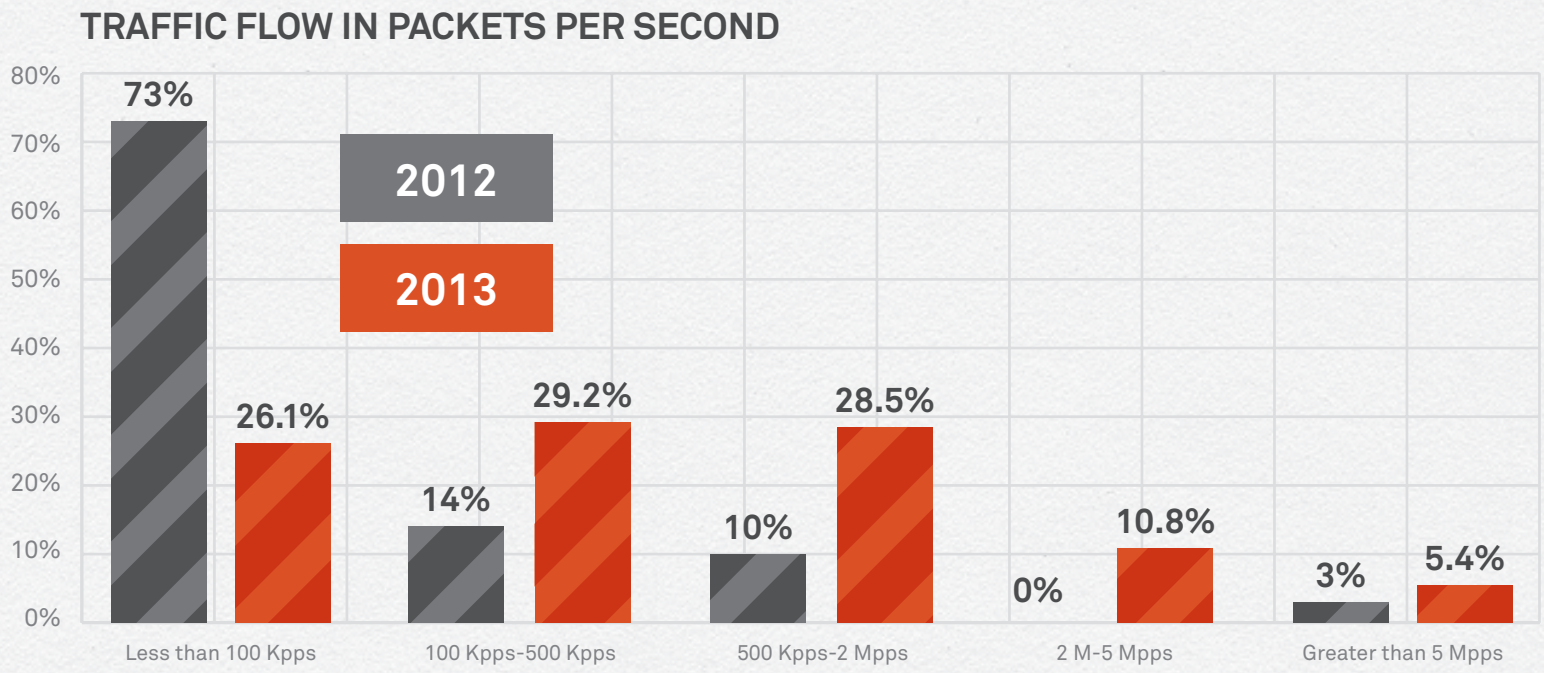
WHAT ABOUT SUPER-SIZED ATTACKS?

While most DDoS attacks are small, less than 1 Gbps, it's not uncommon for attacks to reach 100 Gbps or higher. For example, as of April 2014 the Neustar Security Operations Center has already mitigated more than twice as many 100+ Gbps attacks versus all of last year.

One reason: the rise in DNS and NTP amplification attacks. In launching these, attackers send UDP packets to vulnerable DNS/NTP servers with the spoofed IP addresses of the targeted servers. The vulnerable server sends an amplified response to the target IP address. These attacks can easily add up to enormous bandwidth. One amplification attack this year measured 400 Gbps.

DDoS Attack Size in Packets per Second

Packets-per-second is a standard measurement of the rate at which network traffic flows through routers. The graph below compares traffic flow in packets per second from 2012 and 2013. Companies reported a more even distribution of attacks by packets per second last year. More attacks occurred in the 100 Kpps-500 Kpps range, fewer at less than 100 Kpps and substantially more between 500 Kpps and 2 Mpps. Attacks greater than 5 Mpps increased from 3% in 2012 to 5.4% in 2013.



SPOTLIGHT

Smokescreening: A growing trend in DDoS crime.

Our survey shows a trend towards shorter DDoS attacks, but also more attacks from 1 Gbps to 5 Gbps—that is, quicker, more concentrated strikes. While it's too soon to say for sure, this could stem from a highly damaging tactic, DDoS smokescreening.

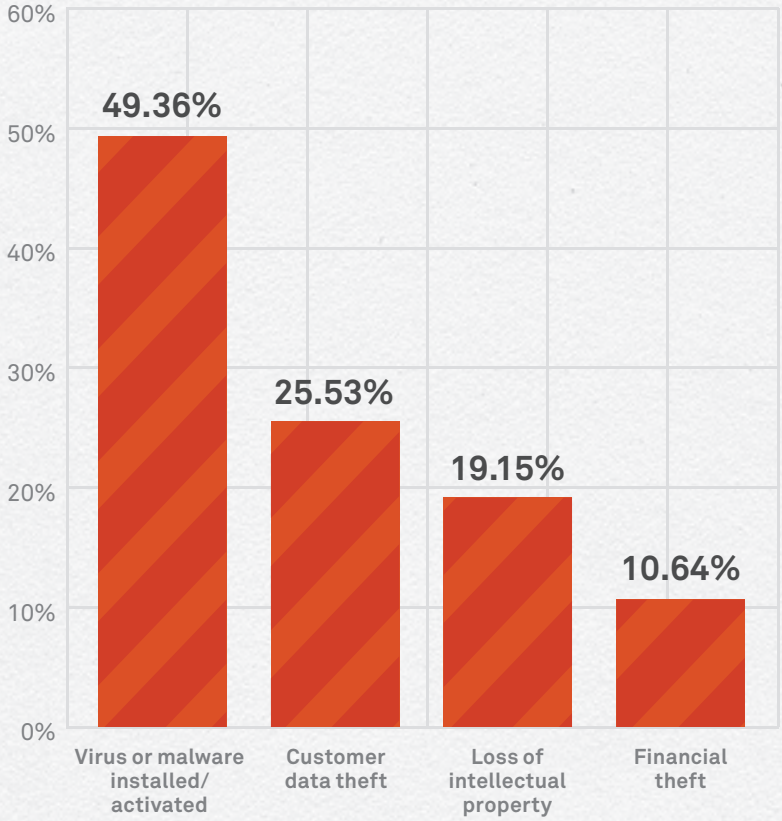
What exactly is smokescreening? While IT and security teams are fully distracted by a DDoS attack, criminals grab and clone private data to siphon off funds, intellectual property and more. In one case, crooks used DDoS to help steal bank customers' credentials and drain $9 million from ATMs in just 48 hours. Such incidents have caused the FDIC to warn about DDoS as "a diversionary tactic."

"Here's an analogy," says Rodney Joffe, Neustar Senior Vice President and Senior Technologist. "When there's a tremendous storm, you run around your house making sure all the windows are closed and you've got the flashlights ready. You're not worried about anything else. DDoS attacks are similar. They create an all-hands-on-deck mentality, which is understandable but sometimes dangerous."

The potential for damage has experts like Joffe worried. "The stakes are much higher," he notes. "If you're a criminal, why mess around with extortion when you can just go ahead and steal—and on a much greater scale?"

55% OF DDOS TARGETS WERE ALSO VICTIMS OF THEFT. ATTACKERS STOLE FUNDS, CUSTOMER DATA AND INTELLECTUAL PROPERTY.

2013: DDOS ATTACKS AND DATA BREACHES*



*Multiple responses allowed.

Watch for these warning signs:

- **Shorter, more intense attacks.**

  If the aim is to steal money, customer data or intellectual property, it's not necessary to knock your business offline for days at a time.

- **No extortion or policy demands.**

  The absence of a ransom note or socio-political ultimatum could indicate a hidden agenda. It should give you pause.

Adhere to these best practices:

- **Don't assign all resources to DDoS mitigation.**

  Dedicate at least some staff to watching entry systems during attacks.

- **Make sure everything is patched.**

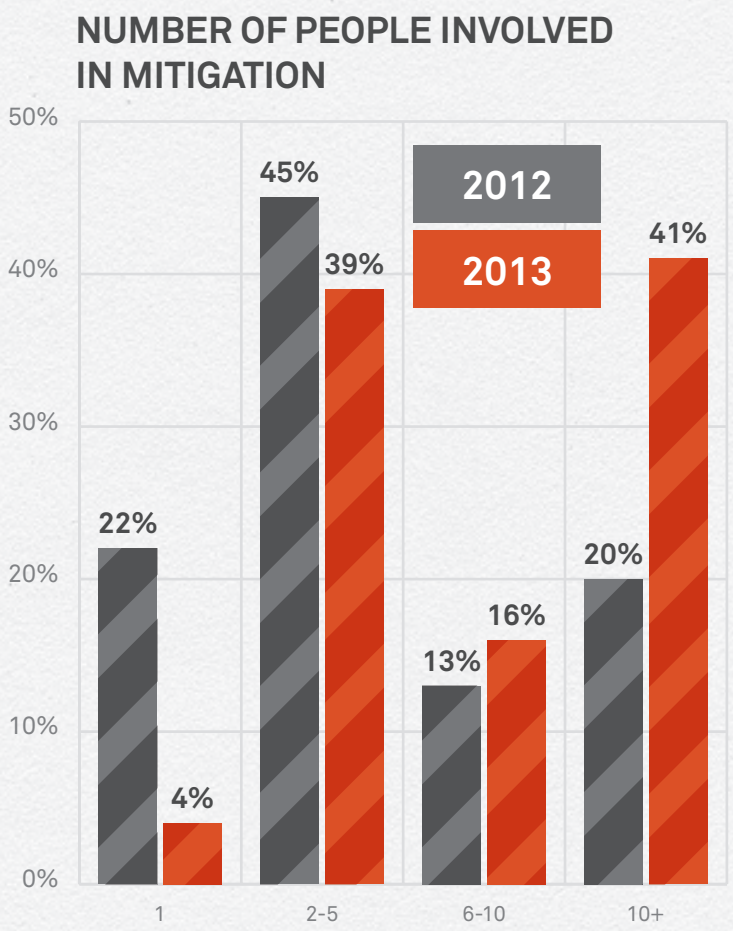
  Keep your security up to date.

- **Have dedicated DDoS protection.**

  Scrambling to find a solution in the midst of an emergency only adds to the chaos—and any intended diversion.

DDoS attacks are consuming more manpower than ever.

In 2013, attacks requiring more than 6 people to mitigate nearly doubled to 56 percent compared to 33 percent in 2012. Furthermore, DDoS attacks requiring more than 10 people to put out the fire more than doubled, increasing from 20 percent in 2012 to nearly 41 percent in 2013.



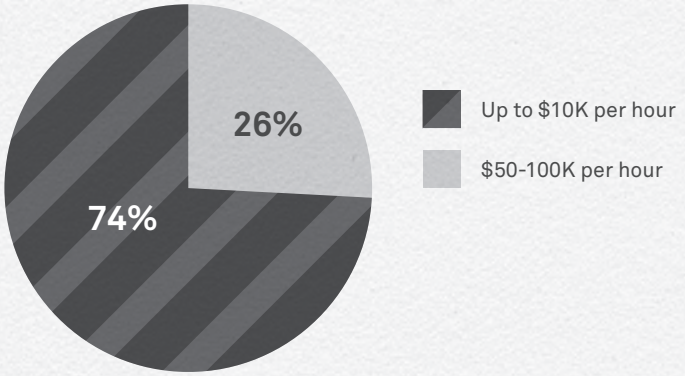
SPOTLIGHT

More than 40% estimate DDoS losses at $1M+ per day.

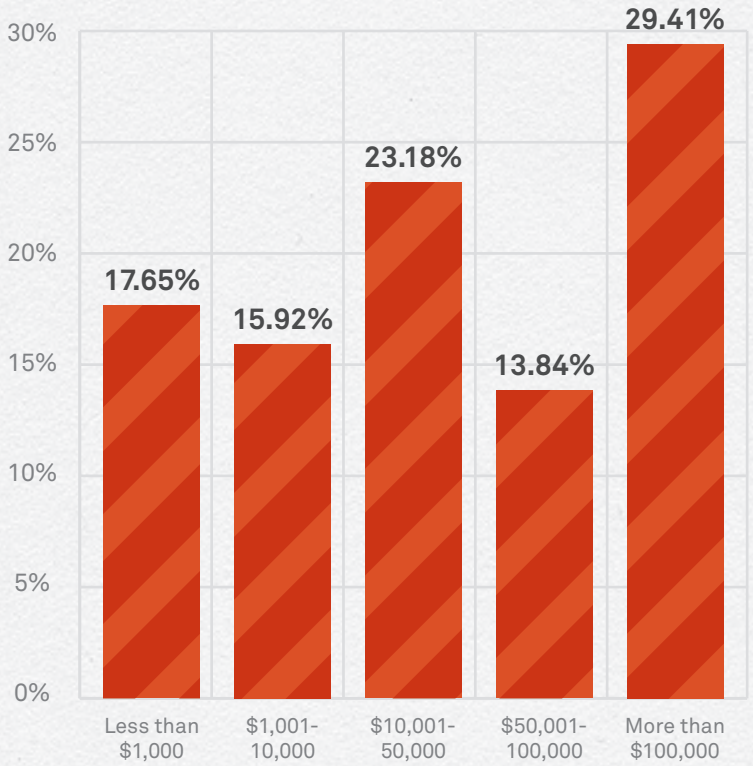
In 2013, 14 percent of companies said that a DDoS outage would mean losses of $50K - 100K per hour, while 29 percent reported $100K+ per hour.

Though attacks on the whole got shorter last year, nearly 40 percent of companies reported being attacked for a day or more—a considerable amount of time when a DDoS attack of just a half day costs one-third of companies $500,000. Bottom line: if DDoS attacks are shorter but more revenue is at stake, losses can still add up.

2012 COSTS PER HOUR



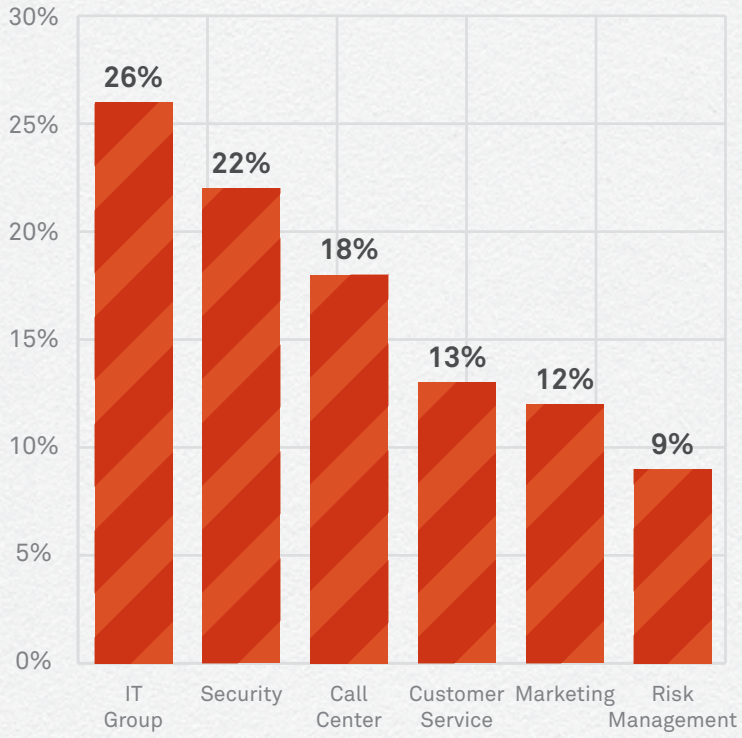
2013 COSTS PER HOUR



Non-IT/security departments absorb over 50% of DDoS attack-related costs.

Surprising, perhaps, but true. Collectively, customer-facing areas like call centers, customer service and marketing take a big hit, along with risk management and compliance. Why? Unhappy customers flood the call center when your site goes down. Customer service is overwhelmed and marketing/PR goes into overdrive.

2013: WHICH AREA OF YOUR BUSINESS BEARS THE GREATEST COST INCREASE IN A DDOS ATTACK?



The impact of DDoS attacks is felt most acutely in customer service.

Sixty percent of companies say customer service takes the largest hit. Only 32 percent cite revenue loss as the biggest impact, notable given that revenue (as reported on page 8) can fly out the door at an alarming rate during a DDoS attack. Brand damage was a close second in DDoS-related fallout.

Biggest Impact of DDoS outages:

Customer support: 63.40%

Brand/customer confidence: 56.60%

Lost revenue: 32.34%

Theft: 23.40%

Lost online promotional spend/marketing : 20.85%

*Multiple responses allowed.

Most companies are fighting attacks with tools not designed for DDoS.

Approximately two-thirds of companies use traditional solutions like firewalls, switches and intrusion prevention systems (IPS) to defend against DDoS attacks. While it's common for companies to use a combination of protection tools, traditional technologies are not designed for DDoS. They can actually accelerate an outage by bottlenecking traffic when a DDoS attack overwhelms your bandwidth. It's like trying to fit a size eight foot into a size five shoe.

The good news: more companies are embracing purpose-built DDoS solutions. Also, companies with no protection dropped from 8 percent to less than 5 percent.

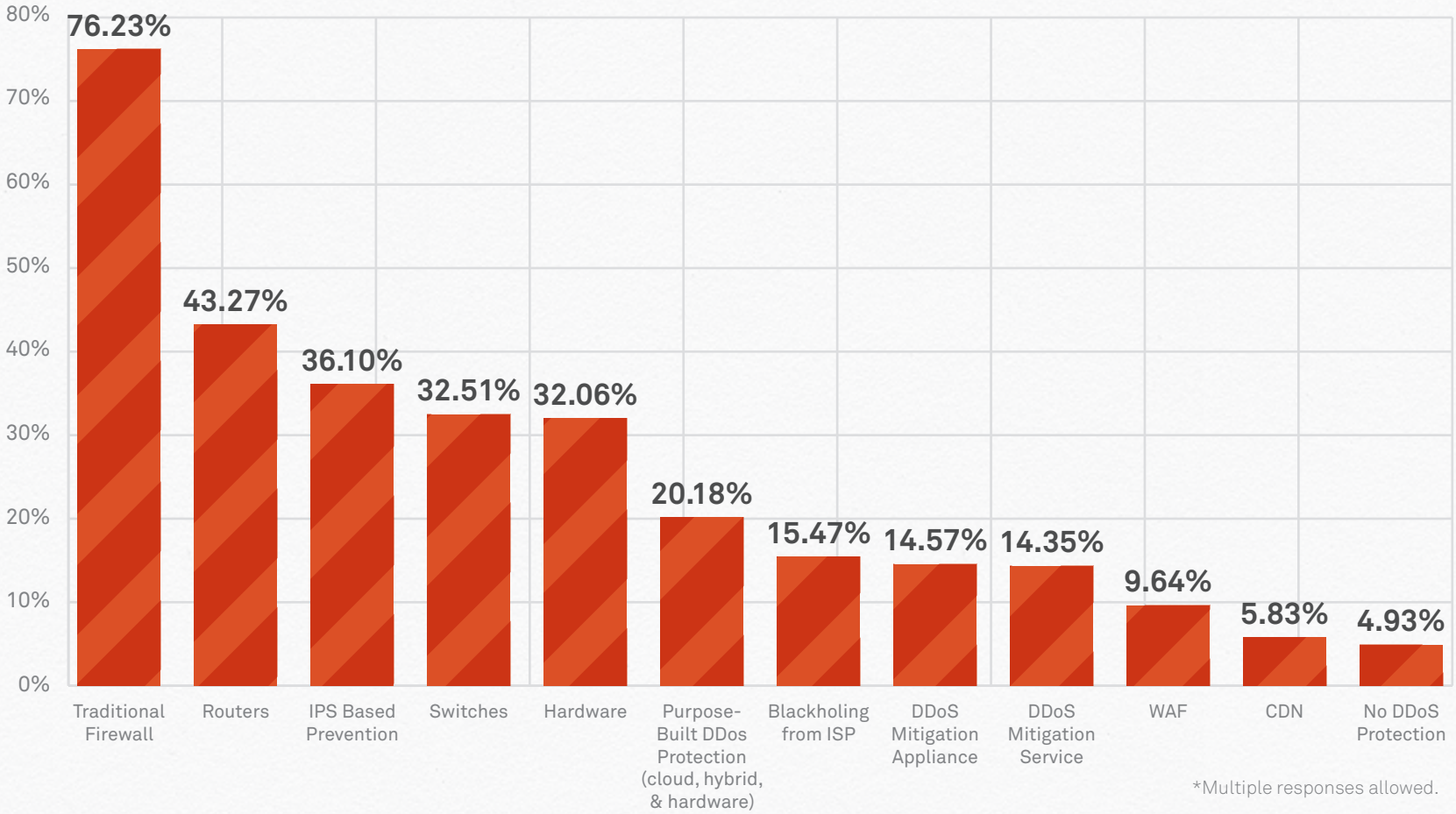
DDoS protection tipping point: losses of $50K per hour.

A closer look at the 2013 results shows that when companies lose $50K per hour in DDoS attacks, it's the tipping point for deploying purpose-built protection.

FINANCIAL SERVICES LEAD THE WAY IN PURPOSE-BUILT DDOS PROTECTION

Given the attacks on the financial industry during the past 15 months, financial institutions are far more likely to have DDoS-specific protection than companies in other industries. This industry's adoption rate is 25 percent higher than average. No wonder. Forty-two percent would stand to lose more than $100K per hour if their site was down, compared to 29 percent of companies overall.

WHAT PROTECTION DOES YOUR BUSINESS USE?



*Multiple responses allowed.

Q&A: A professional DDoS responder's insights.

Neustar's professional DDoS fighters (Security Operations Center) are first responders when businesses are hit by DDoS attacks. We asked one member of the team to walk us through the crucial early stages of DDoS mitigation.

When a business makes a DDoS "911" call to you, what typically happens?

The caller is always stressed. Many companies still wait to get attacked before deploying protection, so they have to decide on the spot: are we purchasing a solution, and if so from whom?

It's a big decision to have to make on the fly, which compounds the anxiety of being under attack. Assuming callers want a solution, an experienced mitigation team can start to onboard them to a platform right away.

How long does it take to begin DDoS mitigation?

If you already have an always-on appliance-based solution in place, you're already mitigating. However, these appliances max out at some point, so if an attack becomes large you might call a provider for cloud failover.

If you already have a cloud solution, your provider should help launch mitigation in under five minutes. If you have no solution in place, it can easily take four hours to provision your defenses.

What are the basic "first responder" steps?

They're similar for all attacks and we carry them out in a just a few minutes. First responders examine any alerts or notifications. Then we analyze your traffic step by step. Once the analysis is clear, we can determine the type of attack and use precise countermeasures. Again, this all happens very quickly at the onset of an attack.

If you're an existing customer with a protection provider, they have baseline data on your traffic. They're able to compare attack traffic to everyday traffic, which is extremely useful in crafting the response.

Any advice for businesses who still want to go it alone?

It's smart to "know your normal." What does your traffic usually look like? Knowing this will help you identify and mitigate attacks faster.

Also, set your DNS TTL (time to life) low, especially A records that are likely to become targets.

Work with your upstream provider to see what they can block through their access control lists (ACL).

And a final piece of more general advice: have some protection and plans in place. It's the same thing any type of first responder would tell you.

Final Thoughts

DDoS attacks are evolving in complex, dangerous ways. Companies assessing their risk and protection should consider:

- Nearly twice as many companies (60 percent) report being attacked in 2013.
- Almost 90 percent of those attacked were hit repeatedly.
- 55% of DDoS targets were victims of theft: funds, customer data or intellectual property.
- Though attack duration is down, the number of attacks between 1–5 Gbps shot up nearly three times.
- DDoS drains manpower: over half of businesses (57 percent) need 6 or more people to mitigate DDoS attacks.
- Risks of $1M a day (estimated outage losses) are common: 4 in 10 companies would suffer this much or more.
- DDoS is costly across the enterprise. Customer service and other public-facing areas now take as large a hit as IT/Security.

In protecting against DDoS attacks, companies must ask: What do they stand to lose if they're hit hard? Rigorous risk, threat and cost analysis is in order. Predicting DDoS is as slippery as the attacks themselves.

CASE STUDY

To win real-life battles, this gaming company chose Neustar DDoS protection.

Gamers have plenty of options, so when a game is unavailable due to a DDoS attack, they take their highly developed opposable thumbs elsewhere. It's a nightmare, of course, for the company whose site is down for an hour. Or two or three or 12. Or sometimes all day.

A developer of free-to-play games has avoided such disaster by taking proactive action. The company creates award-winning games, along with supporting platforms and technologies. The games generate huge traffic, which needs to be protected. When the company got word that someone was planning to attack them, effective mitigation became an urgent matter.

The company's goals:

- Block DDoS attacks quickly
- Ensure their games are available to millions of players worldwide
- Protect the gaming experience
- Protect their good name within the gaming community

To achieve these objectives, the company now relies on Neustar SiteProtect cloud-based mitigation. It filters their traffic through DNS redirection before clean traffic proceeds to the site. On-demand activation and a return to normal traffic happen in just minutes. By controlling mitigation, the company also controls costs.

The gaming industry is ultra-competitive and a frequent target of DDoS. Within the past year, multiple platforms have been hit simultaneously, some by new types of DDoS specially crafted to take down games. Outside of gaming, many firms face similar threats. The smart ones are following this company's lead and preparing in advance.

Neustar SiteProtect

To mitigate DDoS attacks, Neustar blends expertise, proven responses and technologies. Neustar SiteProtect, our DDoS mitigation service, offers options to fit your needs: cloud-based protection, on-premise, always-on hardware or a hybrid of both, fully managed by us. SiteProtect is backed by the Neustar Security Operations Center, whose experts bring years of experience and proven responses to blocking every attack.

For more information on DDoS, please visit **www.ddosattacks.biz.**

About Neustar

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services and data analytics, 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 **www.neustar.biz.**

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

neustar®