Welcome to the 2014 UK DDoS Attacks and Impact Report

For the second consecutive year, Neustar surveyed hundreds of companies in the United Kingdom 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 global reports of “smokescreening,” where criminals use DDoS attacks to distract IT staff while inserting malware to breach bank accounts and customer data. More than 40 percent 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 and so is attack duration, with nearly 30 percent of attacks lasting 1 to 2 days. The number of attacks over 1 Gbps in size skyrocketed—nearly 60 percent of all UK attacks now cross that threshold. While companies report a greater financial risk during a DDoS outage, 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 90 percent view the threat as greater or the same than in 2012. No wonder. 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 331 companies in the United Kingdom, 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.

Ninety-one percent of UK companies see DDoS attacks as a similar or bigger threat than in the previous year. Businesses believe the problem is not going away.

The next finding is one big reason why companies believe the threat is undiminished.
Nearly 1 in 3 businesses report being attacked.

In 2013, 30 percent of UK companies were DDoS-attacked, up from 22 percent experiencing a disruptive attack in 2012. Though 30 percent is half the number of North American companies attacked last year, UK firms saw greater growth in attack duration and size (p. 3 and p. 4).

69% of companies attacked were hit multiple times.

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

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Just once</td>
<td>31%</td>
</tr>
<tr>
<td>Monthly</td>
<td>2%</td>
</tr>
<tr>
<td>2-5 times</td>
<td>32%</td>
</tr>
<tr>
<td>Weekly</td>
<td>9%</td>
</tr>
<tr>
<td>6-10 times</td>
<td>16%</td>
</tr>
<tr>
<td>We lost count</td>
<td>10%</td>
</tr>
</tbody>
</table>

While 31 percent of these companies were DDoS-attacked just once, over 48 percent were targeted 2 to 10 times. Nine percent were targeted weekly, while over 10 percent lost count.

Nearly 30% of DDoS attacks last 1 to 2 days.

In 2013 there were a greater number of longer-lived attacks, with 28 percent lasting from 24 to 48 hours. Attacks lasting one week or longer fell, from 22 percent in 2012 to 9 percent in 2013.
Attacks over 5 Gbps more than doubled.

DDoS Attack Size in Bandwidth

Bandwidth is one way to measure DDoS attacks, including Layer 7 (application layer) attacks. The total number of attacks over 5 Gbps, including those higher than 20 Gbps, more than doubled. In 2013, just 40 percent of DDoS attacks were under 1 Gbps, down from 70 percent in 2012.

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 DDoS attacks up to 20 Gbps increased rapidly, it's also now common for attacks to reach 100 Gbps or higher. For example, as of April 2014 the Neustar Security Operations Centre has 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 in 2014 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. For 2013, UK companies report 32 percent of attacks in the 2–5 Mpps range, almost 3 times higher than for North American companies.
Smokescreening: A Growing Trend in DDoS Crime

Around the world in 2013, DDoS smokescreening became more popular. 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 U.S. Federal Deposit Insurance Corporation (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?”

### 2013: DDoS Attacks and Data Breaches*

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus or malware installed/activated</td>
<td>53%</td>
</tr>
<tr>
<td>Customer data theft</td>
<td>19%</td>
</tr>
<tr>
<td>Financial theft</td>
<td>14%</td>
</tr>
<tr>
<td>Loss of intellectual property</td>
<td>9%</td>
</tr>
</tbody>
</table>

*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 rose to 39 percent compared to 25 percent in 2012, a 56 percent increase. Furthermore, DDoS mitigation requiring more than 10 people doubled, from 12 percent in 2012 to nearly 24 percent in 2013.
32% estimate DDoS would cost over £240,000 per day.

In 2012, 17 percent of UK companies estimated they would lose over £10,000 in revenue per hour as the result of a DDoS outage. In 2013 this rose to 32 percent. That is, 1 in 3 would lose nearly a quarter of a million pounds (or more) per day.

Unfortunately, these cost estimates typically include only considerations around lost sales. With more companies engaging partners, customers and employees online, the impact goes beyond a day of lost revenue. Additionally, industry analysts estimate a company spends 2 percent of revenues on digital marketing. The loss of landing pages and website presence is equivalent to throwing pounds out the window.
Non-IT/security departments absorb over 40% of DDoS attack-related costs.

Following the IT group and security, customer-facing areas like call centres, customer service and marketing take a big hit, along with risk management and compliance. Why? Unhappy customers flood the call centre when your site goes down. Customer service is overwhelmed and marketing/PR goes into overdrive.

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

So says over 95 percent of companies. Nearly 90 percent cite brand and customer confidence as the biggest impact of DDoS outages. Just over 80 percent say revenue loss is the biggest impact, reasonable given that revenue (as reported on p. 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: 96%
- Brand/customer confidence: 89%
- Lost revenue: 82%
- Theft: 55%
- Lost online promotional spend/marketing: 30%

*Multiple responses allowed.*

### 2013: Areas of Greatest Cost Increases in a DDoS Attack

<table>
<thead>
<tr>
<th>Area</th>
<th>Cost Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Group</td>
<td>37%</td>
</tr>
<tr>
<td>Security</td>
<td>20%</td>
</tr>
<tr>
<td>Customer Service</td>
<td>20%</td>
</tr>
<tr>
<td>Risk MGMT./Compliance</td>
<td>9%</td>
</tr>
<tr>
<td>Call Centre</td>
<td>8%</td>
</tr>
<tr>
<td>Marketing</td>
<td>6%</td>
</tr>
</tbody>
</table>
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 8 foot into a size 5 shoe.

The good news: more companies are embracing purpose-built DDoS solutions. Also, companies with no DDoS protection dropped from 20 to 12 percent.

**WHAT PROTECTION DOES YOUR BUSINESS USE?**

<table>
<thead>
<tr>
<th>Protection Type</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Firewall</td>
<td>58%</td>
</tr>
<tr>
<td>Routers</td>
<td>26%</td>
</tr>
<tr>
<td>Hardware</td>
<td>23%</td>
</tr>
<tr>
<td>IPS-Based Prevention</td>
<td>20%</td>
</tr>
<tr>
<td>Purpose-Built DDoS Protection</td>
<td>18%</td>
</tr>
<tr>
<td>Switches</td>
<td>17%</td>
</tr>
<tr>
<td>DDoS Mitigation Appliance</td>
<td>11%</td>
</tr>
<tr>
<td>DDoS Mitigation Service</td>
<td>11%</td>
</tr>
<tr>
<td>Blackholing from ISP</td>
<td>10%</td>
</tr>
<tr>
<td>WAF</td>
<td>4%</td>
</tr>
<tr>
<td>CDN</td>
<td>4%</td>
</tr>
<tr>
<td>No DDoS Protection</td>
<td>12%</td>
</tr>
</tbody>
</table>

*Multiple responses allowed.*
Q&A: A professional DDoS responder’s insights.

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

When a business makes a DDoS “999” 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 DDoS 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 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 5 minutes. And 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 analyse 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 DDoS 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:

- Thirty percent of UK companies report being attacked in 2013. Almost 70 percent of those attacked were hit repeatedly.
- 42% of DDoS victims suffered cyber theft, with attackers pilfering funds, customer data or intellectual property.
- In general, businesses are seeing longer and larger DDoS attacks. Nearly 1 in 3 attacks last 24 to 48 hours and attacks over 1 Gbps in size are now the majority. Attacks over 5 Gbps more than doubled.
- DDoS drains manpower: Nearly 40 percent of UK businesses need 6 or more people to mitigate DDoS attacks.
- The financial risks are high. Over 30 percent of companies estimate daily DDoS outage losses at £240,000 per day or more.
- DDoS is costly across the enterprise. Customer service and other areas now take a significant hit along with 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 2 or 3 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 Centre, 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.