Survey

Incapsula Survey : What DDoS Attacks Really Cost Businesses

Incapsula
An Imperva Company

BY: TIM MATTHEWS

© Incapsula, Inc. 2014 All Rights Reserved

Contents

1. Report Introduction 01

2. Survey Methodology 02

3. How Widespread are DDoS Attacks? 03

4. Profile of an Attack 04

5. Business Impact 06

6. Mitigation and Preparedness 08

7. Learning More/Getting Prepared 09

01

Report Introduction

The impact of distributed denial of service (DDoS) attacks gets bigger and harder to ignore every year; 2014 is certainly no exception. But while such assaults are on the rise, many companies have been content to protect themselves with antiquated firewall-based solutions. Instead they should be investing in solutions providing true protection against unscheduled downtime and financial losses.

Current DDoS trends make it clear that yesterday's strategy is no longer defensible. Large-scale volumetric attacks are growing in size, requiring increased network capacity in order to keep up. In addition, new and more sophisticated DDoS varieties are emerging, requiring organizations to be both highly flexible and ready for anything that might come their way. Entities continuing to rely on existing protection solutions—or worse, no solution at all—should reassess their position in light of this pervasive threat.

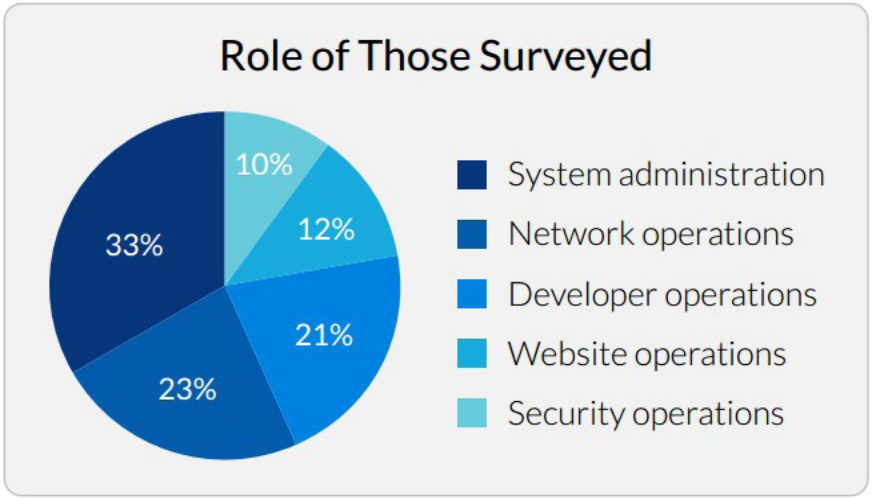
To determine real-world costs posed by DDoS attacks in 2014, Incapsula commissioned a survey to gauge real organizations' experiences with them. By compiling these statistics, we hoped to provide some perspective. Additionally, we wanted to underscore the importance of investing in a truly impenetrable mitigation solution.

02

Survey Methodology

Incapsula's survey data includes responses from 270 North American organizations.[1] These vary greatly in size—from as few as 250 employees to 10,000 or more—having a fairly even distribution between the two extremes.

Reporting organizations are also functionally diverse. When asked to describe the industry in which they primarily operate, responses such as software/technology, manufacturing, and banking/finance were cited. Respondents hold a variety of positions, from system administration to web, network, security, and developer operations. About 80% of the participants reported their company is headquartered in the U.S.



The survey provides valuable insights regarding the actual costs of DDoS attacks; these may prove informative to any organization having previously ignored DDoS protection or which continues to rely on antiquated methodologies.

The results are also useful in describing risks using common business terminology.

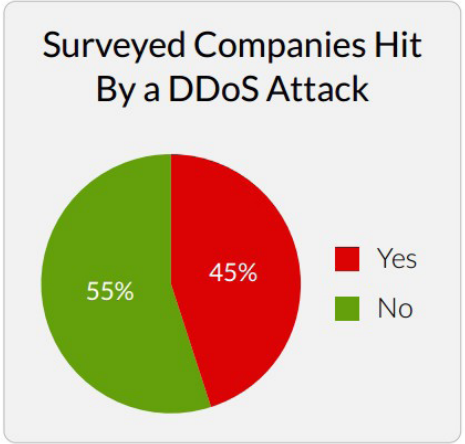
1 The Incapsula DDoS Attacks survey took place between August 4 and August 9, with a total of 270 information technology (IT) professionals participating. The survey was fielded online, and conducted by the Cicero Group, an independent third party marketing research firm. All participants were selected at random, from a variety of industries, across the U.S. and Canada. The survey has a confidence interval of approximately +/- 5.96% at a 95% confidence level.

03

How Widespread are DDoS Attacks?

DDoS assaults are common

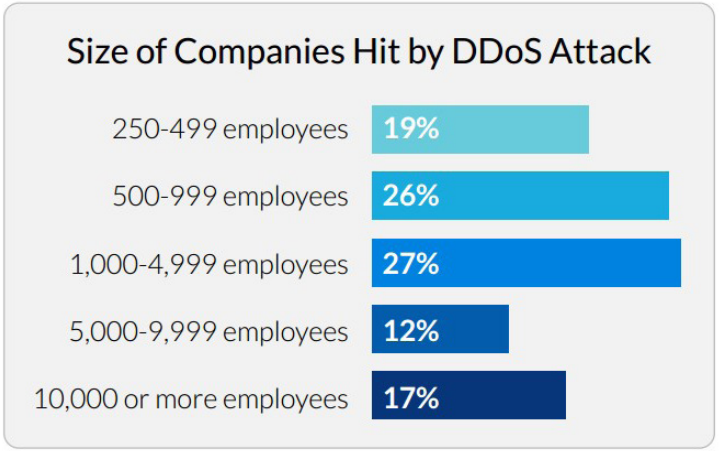
Almost half (45%) of the respondents indicated their organization had been hit at some point. Of these, almost all (91%) reported an attack during the last 12 months, and over two-thirds (70%) were targeted two or more times.



The data reflect that most organizations have at least some familiarity with DDoS threats. When asked to rate their understanding of them, including what they are and how they work, 98% of the participants declared they were either "somewhat familiar" or "very familiar." Further, their familiarity isn't merely based on theoretical knowledge—many indicated they have direct experience dealing with DDoS incursions.

While organizations of all sizes experience DDoS assaults, they are often worse for larger entities.

Those having 500 or more employees are most likely to experience a DDoS assault, incur higher attack costs, and require more employees to combat the threat.



04

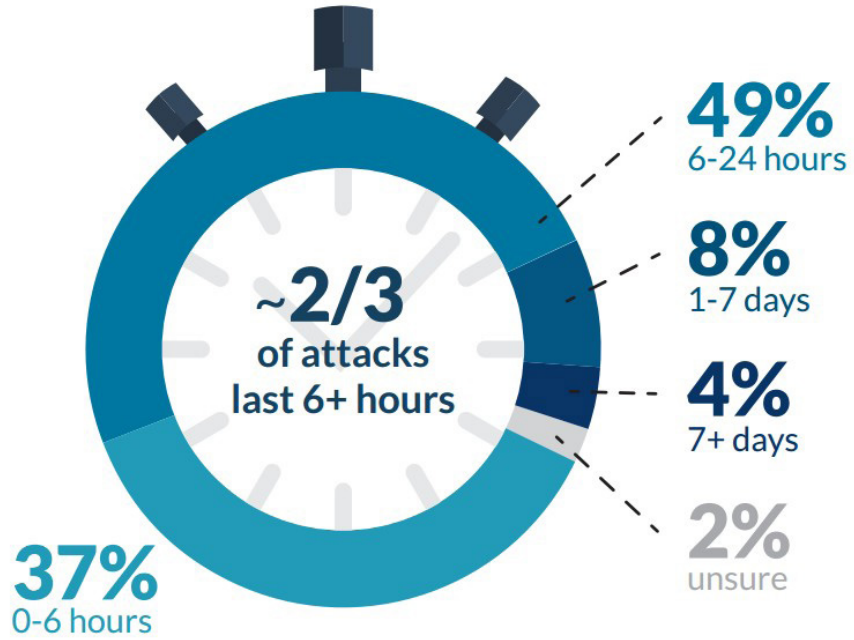
Profile of an Attack

DDoS assaults come in many shapes and sizes, so organizations must be prepared for anything in order to protect themselves

Participants offered a wide range of answers regarding DDoS duration, whether perpetrators used a ransom note to extort money, and what the primary tactic of each incursion appeared to be.

When asked how long an average assault lasts, they report a higher number of shorter attacks, with 86% reporting an average of 24 hours or less.

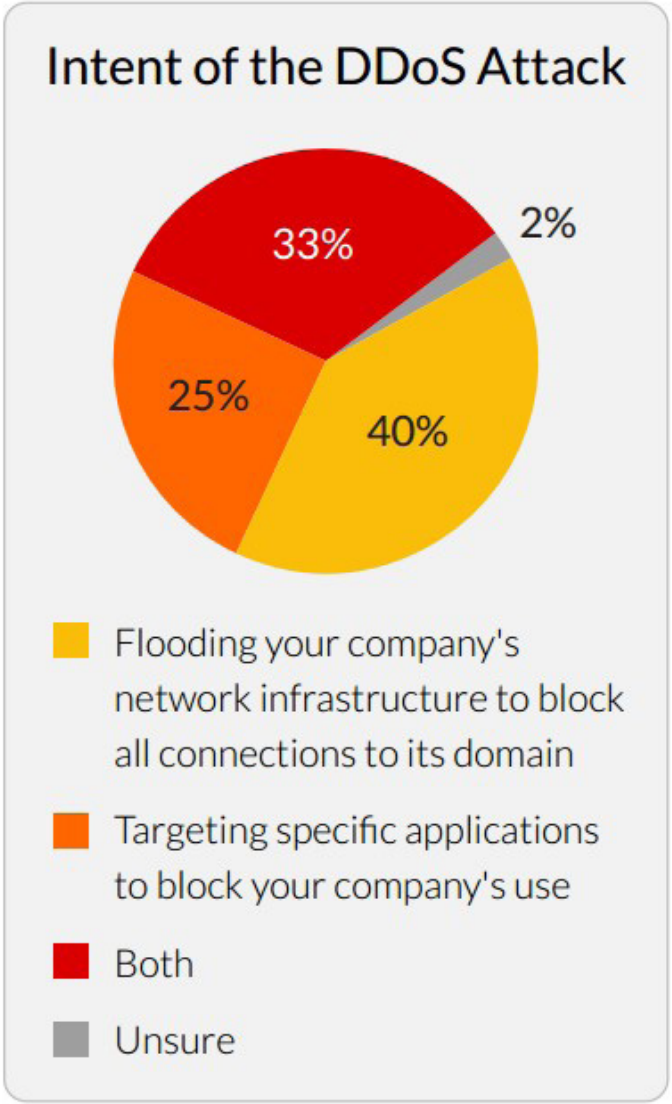
However, upon closer examination, the data reveals there are no predictable patterns as to how long an assault will last. 37% of organizations reported an average of six hours or less, 31% cited 6 to 12 hours, and 18% claimed 13 to 24 hours. While the trend seems to point toward shorter durations, average attack lengths of days—or even more than a week—are also reported.



In part, NTP amplification attacks can be massive because the underlying UDP protocol does not require two-way handshaking.

There seems to be no unified motive behind attacks, either. Respondents were evenly divided in answering whether they had ever received a ransom note from a DDoS perpetrator: 46% indicated they had, while 45% had not. This reveals an even mix of those motivated by financial gain and others who attack for different reasons.

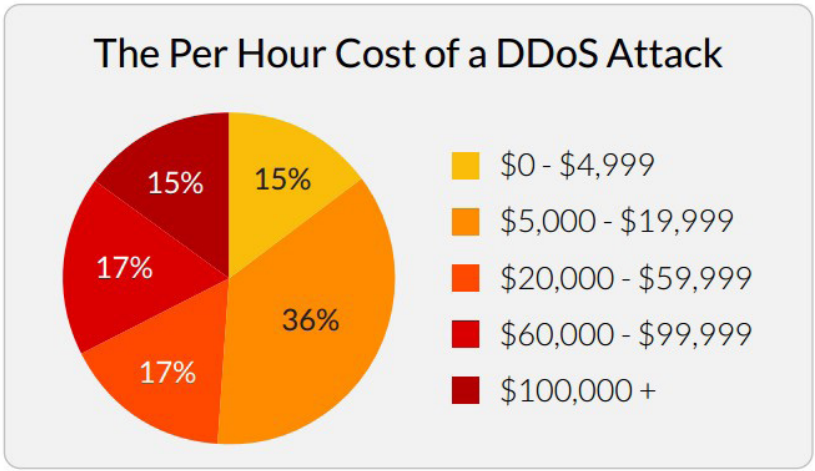
Here 40% of participants believe perpetrators were attempting to flood their organization's network, 25% surmised they were trying to cause an outage by targeting specific applications, and 33% believe both were the motivating factors. The tally shows that there is also a fairly even distribution of attack types used by offenders



05

Business Impact

49% of DDoS attacks last between 6-24 hours. This means that with an estimated cost of $40,000 per hour, the average DDoS cost can be assessed at about $500,000—with some running significantly higher. Costs are not limited to the IT group; they also have a large impact on units such as security and risk management, customer service, and sales.



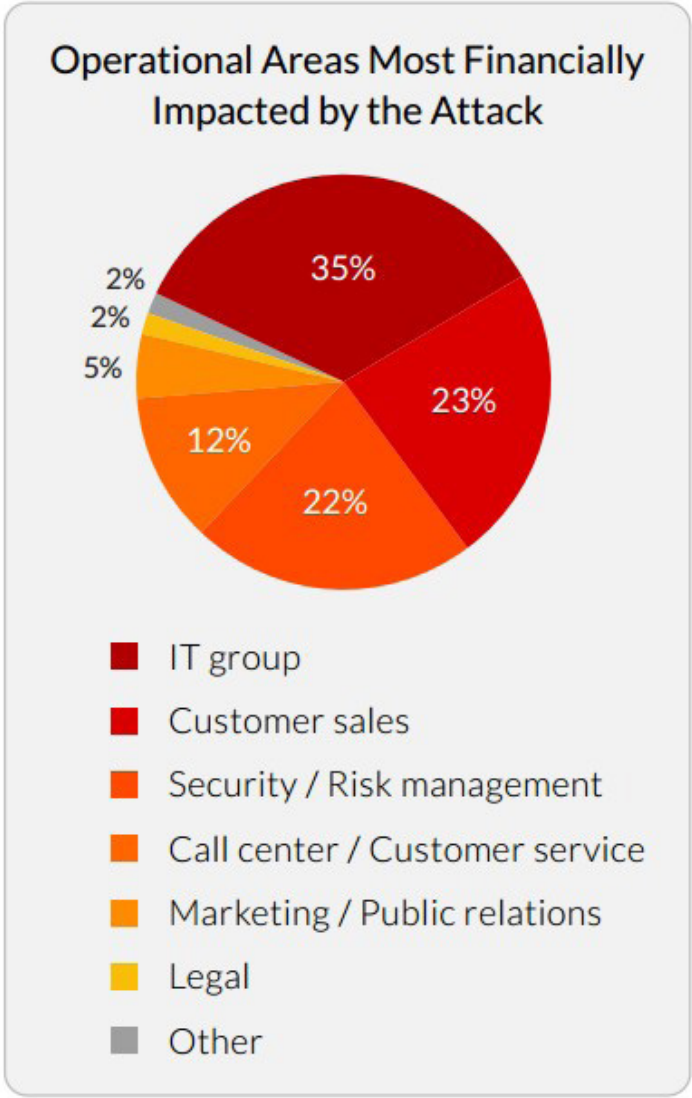
Additionally, most respondents who had been targeted experienced a variety of non-financial costs. 87% experienced at least one non-financial consequence, such as loss of customer trust, loss of intellectual property, and virus/malware infection, while 60% incurred two or more.

52% had to replace hardware or software, 50% had a virus or malware installed/activated on their network, and 43% experienced loss of consumer trust. Furthermore, 33% acknowledged customer data theft, and 19% suffered intellectual property loss.

There is much more than meets the eye in relation to DDoS dangers and costs. This is illustrated by participants' answers when asked to describe which operational area takes the largest financial hit during an assault. As you might expect, at 35% IT was the most-cited answer.

However, responses were fairly distributed among all options, with 23% naming sales, 22% identifying security and risk management, and 12% citing customer services. Marketing and legal were also listed, revealing that very few departments are completely safe from DDoS carnage.

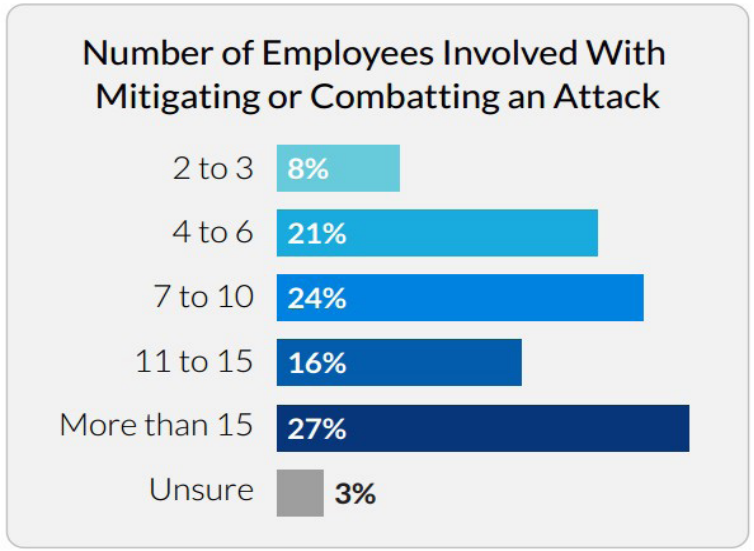
Recovering from attack damage can also take months or years. Over half of the respondents (52%) reported their organization had to replace software/hardware, or that it had lost revenue. An additional 43% confirmed that their organization lost consumer trust. Each example reveals DDoS aftermath to be long-term.



06

Mitigation and Preparedness

Many of those surveyed work for organizations lacking an effective plan to prepare for, and mitigate, targeted DDoS penetrations. When participants were asked to describe how many people are typically involved in mitigating an incursion, the numbers tend to be higher. 27% reported their organization used 15 or more people, while no one works for an entity where its response could be managed by a single person



These numbers emphatically demonstrate there is room for improvement when it comes to efficiently thwarting DDoS attacks. Ideally, an organization should be able to quickly respond with as few employees as possible.

Statistics regarding measures taken to protect themselves are equally discouraging. Over half of all respondents acknowledge that their firm continues to rely on web application firewalls or traditional network firewalls—partial solutions that are vulnerable on their own.

A respectable 43% reported that their organization uses a purpose-built DDoS protection solution. This is a good sign. Ideally, however, all organizations should avail themselves of the latest mitigation technologies. These provide a level of defense that traditional firewalls can never match.

Learning More/Getting Prepared

Our *2014 DDoS Impact Report* data demonstrate an alarming trend—intrusions are becoming more prevalent, more sophisticated, and more costly. At the same time, many organizations aren't taking appropriate measures to protect themselves.

The survey reveals that many organizations continue to haphazardly respond to attacks, relying on the same firewall solutions they've been using for years. In today's world, where DDoS attacks are increasingly common and can easily cost an organization hundreds of thousands of dollars, this is no longer tenable.

If you want to be more proactive about combating DDoS attacks, then the data from this survey will help you to convince your CEO/CTO/CFO that steps need to be taken. After all, the numbers don't lie. To learn what your company should do next, download our free *DDoS Response Playbook*.

Try a Two-Week Free Trial

- No software to download or equipment to hook up
- Getting started is easy and requires only a DNS change
- Includes load-balancing and web application acceleration

Get Started Today

Questions? Contact us.