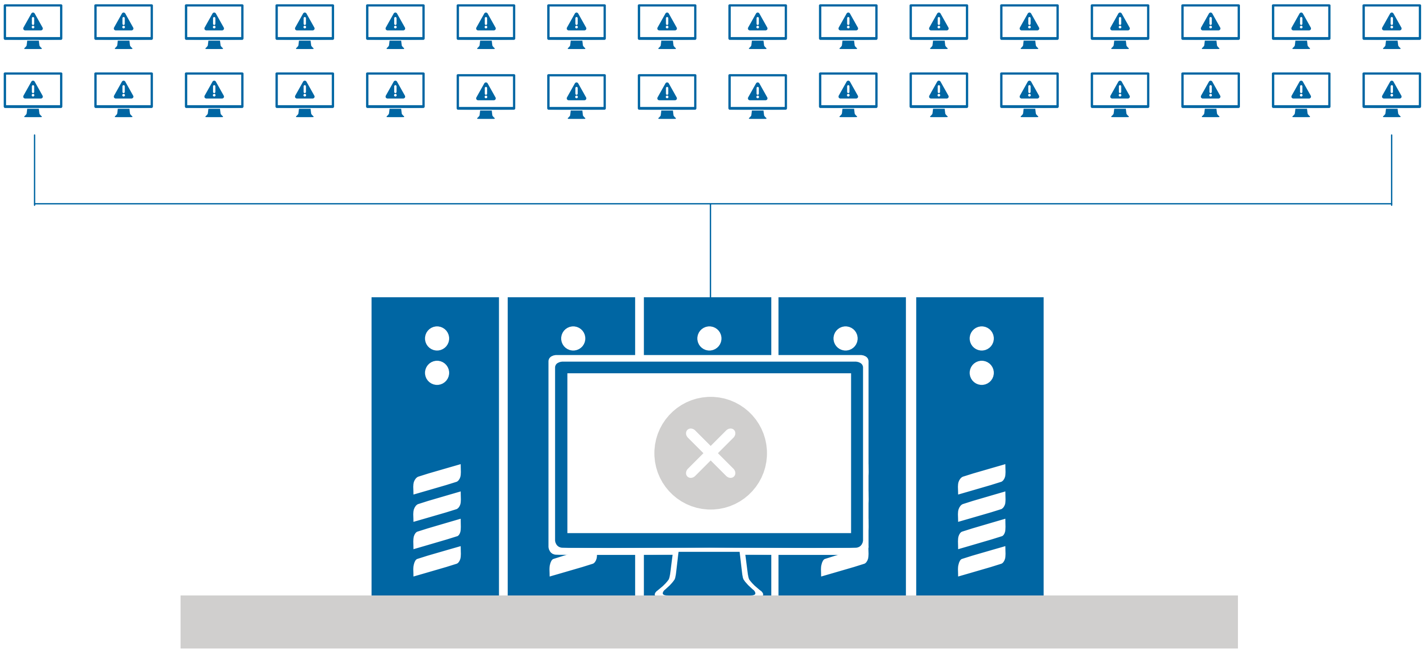

Introduction to DDoS

A guide to the causes, costs and consequences of distributed denial of service (DDoS) attacks

A white paper from Bell

What’s inside

Half of all organizations now see distributed denial of service (DDoS) attacks as the cyber threat that will do the most harm to their business. With these attacks becoming more common (and increasingly sophisticated), the first step toward protecting your organization is knowing exactly what you’re up against.

This white paper provides insights into how DDoS attacks work, why they’re becoming more prevalent, and the costs and consequences they can inflict on your organization’s bottom line and brand reputation.

Contents

A growing threat

While stolen credit card numbers and corporate data breaches may grab all the headlines, distributed denial of service (DDoS) attacks are just as likely to cause sleepless nights for many CIOs. In fact, half of all organizations now see DDoS attacks as the cyber threat that will do the most damage to their business.[1]

DDoS attacks are increasingly prevalent and can have a devastating impact on businesses of any size. At the highest level, their objective is simple: to stop legitimate user traffic from accessing an organization's online services or resources. They do this by taking websites offline and slowing servers to a crawl, severely limiting the organization's ability to do business and negatively affecting the customer experience.

In a recent survey by Radware of more than 300 companies around the world, 90 percent of respondents said they had experienced some sort of cyber attack in 2015, with more than half – 51 percent – reporting being hit by a DDoS attack.[2] And if recent trends are any indication, that number will climb even higher in the near term. Between the third and fourth quarters of 2015, reported DDoS attacks jumped by 39.9 percent; when comparing Q4 2014 to Q4 2015, the number of attacks increased by a staggering 148.9 percent.[3]

90% of respondents said they had experienced some sort of cyber attack in 2015, with more than half reporting being hit by a DDoS attack.[2]

The good news is there are strong defences against DDoS attacks. To understand how and why they are effective, though, it's important to know what happens during a DDoS attack.

How a DDoS attack works

Multiple targets, multiple paths

Most DDoS attacks take one of two main forms:

Volumetric attacks

Also known as network floods, these attacks use thousands of simultaneous information requests to clog the target's Internet 'pipe', congesting its network and making its website largely inaccessible. It's essentially massive online gridlock that forces multiple lanes of traffic into one. If you're trying to reach the affected website, it will take a very long time to get there (if you can at all).

Low-and-slow attacks

These rely on smaller volumes of carefully crafted information requests over a longer period of time which makes them harder to detect. They seek to consume the available memory or processing power of an application or server, gradually exhausting the computing resources of load balancers, servers and firewalls. Tied up by this illegitimate traffic, the IT infrastructure struggles to deal with genuine user requests – causing it to run inefficiently or even stop working altogether.

[1] Radware. *2015-2016 Global Application and Network Security Report*. Retrieved from https://www.radware.com/ert-report-2015.

[2] Radware. *2015-2016 Global Application and Network Security Report.* Retrieved from https://www.radware.com/ert-report-2015.

[3] Akamai. *Q4 2015 State of the Internet - Security Report*. Retrieved from https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.html.

Whether they take a volumetric or low-and-slow approach, DDoS attacks typically target two key areas of an organization's IT infrastructure: its network and its applications.[4]

Network-layer attacks

Network-layer attacks (*aka* layer 3-4 attacks) aim to overload network connections by driving up traffic volume and consuming massive amounts of bandwidth. While the largest attack can consume as much as 200 gigabits of bandwidth per second (Gbps), just 40 Gbps is sufficient to shut down most networks. This kind of attack can prevent access to servers and cause large data/bandwidth overage charges for the victim. Attackers target the network by exploiting vulnerabilities in areas such as user datagram protocol (UDP), network time protocol (NTP) and domain name systems (DNS). Network attacks currently account for 97 percent of all DDoS activity and show no sign of slowing down, with the number of reported attacks increasing by 42.4 percent between Q3 and Q4 2015.[5]

Application-layer attacks

Application-layer attacks (*aka* layer 7 attacks) are designed to overload a server by sending it a large number of requests that require resource-intensive handling and processing to complete. Anywhere from 50 to 100 requests per second is usually enough to severely impact or shut down the average website. This kind of attack targets application protocols that have exploitable weaknesses such as hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), file transfer protocol (FTP) and structured query language (SQL). The number of reported application-layer attacks is also rising, up 28.2 percent between Q3 and Q4 2015.[6]

Given that they're the most common targets of an attack, it's no surprise that the network and application layers are where most IT security spending is directed. These two layers received 30 percent and 19 percent, respectively, of the security funding budgeted or earmarked in 2015.[7]

An army of bots

DDoS attacks are called 'distributed' because the requests come from hundreds or even thousands of sources at once rather than from a single computer (as with a traditional denial of service attack). This approach typically relies on what's known as a 'botnet' – a network of malware-infected computers – to launch a coordinated assault on a particular target.

Most botnets are created through specially designed malware, which is spread to as many computers as possible through malicious file attachments, web scripts and other tools. Any computer that runs the malware inadvertently becomes another 'zombie' in the botnet, linked up to its command-and-control server and awaiting further instructions.

Because the malware comes to life only when directed by the command-and-control server, most people have no idea their computer is part of a botnet – to be leveraged at any time for malicious purposes. The U.S. Federal Bureau of Investigation (FBI) estimates some 500 million computers are infected globally each year, with 18 new bots created every second.[8]

500 million computers are infected globally each year, with 18 new bots created every second.[8]

[4] Incapsula. *Denial of Service Attacks*. Retrieved from https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html.

[5] Akamai. *Q4 2015 State of the Internet - Security Report*. Retrieved from https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.html.

[6] Akamai. *Q4 2015 State of the Internet - Security Report*. Retrieved from https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.html.

[7] Ponemon Institute. *2015 Cost of Cyber Crime Study: Global*. Retrieved from http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf.

[8] Federal Bureau of Investigation. (2014). *Taking Down Botnets*. Retrieved from https://www.fbi.gov/news/testimony/taking-down-botnets

No experience necessary

DDoS attacks are on the rise partly because the tools needed to launch them are more accessible and less expensive than ever before. Just as anyone can now purchase cloud-based software-as-a-service or infrastructure-as-a-service, the same is true for DDoS attacks. As a result, people who would normally have no idea how to create or distribute the malware needed to build up a botnet can now easily buy what they need – or hire someone to do it for them.

Several DDoS-for-hire services (also known as 'stressers' or 'booters') have emerged in recent years. These allow potential cyber criminals to rent existing botnet infrastructures or even pay someone to launch an end-to-end attack on their behalf against a target of their choosing.

The costs associated with 'DDoS-as-a-service' are startlingly low. For example, one hacking group offers eight different DDoS subscription packages, with the most affordable starting at just $6 per month. That option provides access to a botnet that can bring down a website for 100 seconds. Those who pay $130 a month can take a site offline for more than eight hours.[9] And when these services are paid for through alternative payment systems such as Bitcoin, it becomes extremely difficult to trace a particular attack back to any one person.[10]

Those who pay **$130** a month can take a site offline for more than eight hours.[9]

With such a low barrier to entry, anybody with a credit card and a motive can quickly and easily initiate a DDoS attack. Consider the 17-year-old Idaho teen who paid a third-party DDoS provider to launch multiple attacks against the state's largest school district. Internet connectivity across 52 schools was disrupted for more than a week, causing test results to be lost, making online classes and texts inaccessible, and affecting administrative and payroll systems.[11]

What's the motive?

With the ability of low-cost DDoS attacks being launched with very little preparation, it has become clear that any organization can be attacked at any time. But what motivates an attacker? The reasons can include: [12, 13]

Hacktivism

DDoS is often used as a form of protest against governments and corporations whose actions are 'wrong' from the attacker's point of view. Hacktivism can range from the political and ethical (such as attacks by groups like Anonymous against organizations ranging from Islamic State to the FBI) to the personal and petty (like when online game servers are taken down by players upset over recent changes to the game).

Vandalism

sometimes a website is taken down just to prove that it can be done – or for no other reason than to 'troll' an online community. These kinds of attacks are attributed to so-called 'script kiddies' due to the childish motivations; they do it simply for the adrenaline rush or to get the attention of their peers.

Competition

if one company's website goes down, that's good news for its competitors. Not only will the affected company lose sales, its reputation will also take a hit – and its customers may flock to the competition instead. These kinds of attacks seem to be common practice in cutthroat industries such as online gambling.

[9] PCMag. (2014). *Lizard Squad Offers $6 DDoS Attack Tool*. Retrieved from http://www.pcmag.com/article2/0,2817,2474386,00.asp.

[10] National Crime Agency. (2015). *Operation Vivarium Targets Users of Lizard Squad's Website Attack Tool*. Retrieved from http://www.nationalcrimeagency.gov.uk/news/691-operation-vivarium-targets-users-of-lizard-squad-s-website-attack-tool.

[11] KTVB. (2015). *Student Accused of Cyber Attack on West Ada District*. Retrieved from http://www.ktvb.com/news/crime/student-accused-of-cyber-attack-on-west-ada-district/175763447.

[12] Incapsula. *Denial of Service Attacks.* Retrieved from https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html.

[13] Brain Stuff. (2014). *Why Do People Perform DDoS Attacks?* Retrieved from http://www.brainstuffshow.com/blogs/why-do-people-perform-ddos-attacks.html.

Extortion

knowing how damaging a DDoS attack can be to a business, the mere threat of one can be used to extort money from a victim. Unless the ransom is paid, the attack will go ahead as planned (or if it is already in progress, it won't be called off until the money is received).

Diversion

DDoS can also be used as a 'smokescreen' to hide the true target of a cyber attack. With IT teams sidetracked by the website or server outage, it can be easier to sneak into a company's network to steal its customer or financial data.

From simple to sophisticated

DDoS attacks aren't just becoming more common and accessible. They're also becoming more complex, making it harder for security professionals to detect, prevent and resolve them.

While traditional DDoS attacks relied on just a single attack vector, multi-vector attacks that use a combination of volumetric, low-and-slow, network-layer and application-layer attacks are quickly becoming the norm.

56% **of all DDoS attacks in the fourth quarter of 2015 leveraged multiple attack vectors.**[14]

The multi-vector approach gives attackers a greater chance of success. They can target different resources simultaneously or even use one type of attack as a decoy for another. When security professionals don't know where attacks will be coming from or what they'll be targeting, planning for, managing and mitigating them becomes much more difficult.

Attackers are further improving their odds by changing the way they launch their DDoS attacks. Rather than focusing on the traditional, large-scale attacks that run persistently over a very long timespan, some attackers are now turning to what are known as 'burst' or 'hit-and-run' attacks. Generating large volumes of traffic over a short period of time, they last just long enough to bring down a server or website (between 20 minutes and an hour) – and then are repeated again and again over several days or even weeks.

This kind of attack was developed specifically to counter traditional IT security measures designed for prolonged and persistent attacks. By the time the anti-DDoS systems and protocols are manually triggered the burst attack has already run its course, wasting IT time and resources while disrupting the entire organization.[15]

How a DDoS attack affects your business

An immediate impact on your bottom line

The ultimate goal of a DDoS attack is to affect an organization's customer experience by:

- Taking its website completely offline so that no legitimate traffic can get through
- Causing its server to become so slow and unresponsive that even if customers can access the site, they can't do anything on it

[14] Akamai. *Q4 2015 State of the Internet - Security Report.* Retrieved from https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.html .

[15] Incapsula. (2013). *Hit and Run DDoS Attack.* Retrieved from http://www.incapsula.com/blog/hit-and-run-ddos-attack.html.

Any eCommerce business whose website grinds to a halt will suffer immediate consequences in terms of lost sales. Consider what happened to Amazon in August 2013: when its site went down for just 40 minutes, it lost approximately $5 million.[16]

Even organizations that don't sell products online can suffer if their websites are critical sources of information or services. When the network or servers are under attack, customers can no longer access the support they need. This can lead to a flood of calls or emails, bogging down lines of communication that might otherwise be used in more productive ways.

The high cost of remediation

Stopping a DDoS attack also comes with a potentially high price tag – second only to cyber crimes caused by malicious insiders.[17] How many people will need to divert their attention from their regular tasks to fight the attack? How long will it take to reboot applications or servers – and then test them to ensure they're working correctly? What if data is lost? If a server crashes while a transaction is being completed, for example, the entire disk could become corrupted due to a read/write error – potentially requiring you to re-create all transactions made since your last backup.

Depending on the timing and nature of the attack, getting a downed website or server back up and running could take hours or even days.

Some estimates say the average DDoS attack takes up to 90 days to resolve completely.[18]

In a Forrester Research survey of Canadian decision-makers directly involved with customer-facing systems, 35 percent said it would cost between $10,000 and $100,000 to resolve a DDoS attack. Another 25 percent said it would cost anywhere from $100,000 to $1 million.[19] But that's a drop in the bucket compared to what Sony experienced in 2011: when its PlayStation Network was hit by a series of DDoS attacks and data breaches, it reportedly spent more than $250 million over two years to address the immediate impacts of the attacks and then reinforce its defences.[20]

A direct hit to your reputation

None of the numbers above include the costs associated with the potential damage to reputation, customer retention or customer acquisition. If your website is your product or if the performance of your product depends on the availability of your server, your customers could be denied services they've already paid for. This can provoke anger and frustration, potentially affecting your brand image. Customers who have a bad experience are likely to spread the word, especially over social media. This means that even after the DDoS attack is resolved, the impact on your reputation can affect your sales for weeks or even months down the line.

[16] VentureBeat. (2013). *Amazon Website Goes Down for 40 Minutes, Costing the Company $5 Million*. Retrieved from http://venturebeat.com/2013/08/19/amazon-website-down/#YrOqv7cqKgylGzWm.99.

[17] Ponemon Institute. *2015 Cost of Cyber Crime Study: Global*. Retrieved from http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf.

[18] Ponemon Institute. *2015 Cost of Cyber Crime Study: Global.* Retrieved from http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf.

[19] Forrester Research. (2014). *Protecting Customer Experience Against Distributed Denial of Service (DDoS).* Retrieved from https://business.bell.ca/shop/enterprise/forrester-network-ddos-security-white-paper.

[20] Fortune. (2014). *Why Sony Didn't Learn from Its 2011 Hack.* Retrieved from http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack.

In the Forrester Research survey of IT decision-makers mentioned earlier, Canadian businesses ranked the indirect impacts of losing their website for an hour or more as follows:[21]

67%

state there is a negative impact to customer satisfaction

56%

feel it critically impacts the brand

52%

State customer acquisition is at risk

55%

are concerned with negative effects on customer retention

Every sector is at risk

No industry is immune to the possibility of a DDoS attack. Certain kinds of organizations, however, are more likely targets, such as government departments, online gaming and gambling companies, and Internet service providers. The online gaming sector was hit particularly hard in the fourth quarter of 2015, accounting for 54 percent of all DDoS attacks during that period. When looking specifically at application-layer attacks, the retail sector remains the most popular target, receiving 59 percent of all attacks during that same quarter.[22]

Still, many other types of organizations face substantial risk, including those in the financial, education, healthcare, energy/utility and legal sectors. In fact, 2015 saw such an increase in the number of attacks against schools and other educational websites that it prompted Radware to move those organizations from medium to high risk.[23]

While DDoS attacks typically make the news only when governments, banks or multinational corporations are targeted, the reality is that organizations of all sizes are affected. In the financial sector, for example, smaller credit unions and brokerage houses have also been targeted by DDoS attacks.[24]

Conclusion

Even though they're at risk, many organizations think they're not big enough or have a sufficient online presence to be targeted. As a result, they're less likely to invest in advanced DDoS protection – and that plays right into the hands of potential attackers. For smaller or less visible organizations especially, even a single prolonged outage can result in an irreversible loss in sales or consumer confidence.

One of the keys to protecting your organization is the ability to recognize a DDoS attack before it takes place. But even though a sudden surge in bandwidth consumption is typically the first warning sign of a DDoS attack, not every organization is able to detect such changes in real time.

In one survey of IT professionals, 21% of respondents said customer complaints were the primary indicator of an attack – and nearly half could respond only reactively, recognizing and working to stop an attack well after the damage had already been done.[25]

[21] Forrester Research. (2014). *Protecting Customer Experience Against Distributed Denial of Service (DDoS).* Retrieved from https://business.bell.ca/shop/enterprise/forrester-network-ddos-security-white-paper.

[22] Akamai. *Q4 2015 State of the Internet – Security Report*. Retrieved from https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.html.

[23] Radware. *2015-2016 Global Application and Network Security Report*. Retrieved from https://www.radware.com/ert-report-2015/.

[24] Credit Union Times. (2014). *DDoS Takes Aim at Vulnerable Credit Unions*. Retrieved from http://www.cutimes.com/2014/10/03/ddos-takes-aim-at-vulnerable-credit-unions?page=1.

[25] Corero Network Security. (2015). *Corero Network Security Finds Degradation of Customer Confidence and Lost Revenues are the Most Damaging Ramifications of DDoS Attacks.* Retrieved from https://www.corero.com/company/newsroom/press-releases/corero-network-security-survey-finds-degradation-of-customer-confidence-and-lost-revenues-are-the-most-damaging-ramifications-of-ddos-attacks-/.

These numbers underscore the importance of using a proactive, always-on IT security service. Many such services exist, including on-premises solutions, cloud-based solutions and combinations of the two. And the good news is that you don't have to be a global organization with a giant IT team to implement them. Bell Network DDoS Security Service, for example, is an affordable, fully managed service that automatically detects, mitigates and filters DDoS attacks before they can reach your corporate network, preventing malicious traffic from interrupting your operations.

Visit our website for more information about Bell Network DDoS Security. If you'd like to learn more about how Bell can protect your organization against all kinds of cyber attacks, please contact your Bell representative. We'll help you find the most appropriate security solution for your business needs.

About Bell

Businesses that demand a reliable, highly secure IT infrastructure choose Bell. Bell is an integral part of Canada's critical infrastructure, and also delivers advanced threat detection, mitigation and prevention expertise.

By owning and operating Canada's largest voice and data network, Bell has a significant scope of visibility into potential threats against your business. We can aggregate massive amounts of data and correlate traffic patterns to proactively detect and mitigate malicious traffic – and reduce response times when incidents do occur. Plus, with a team of more than 300 security professionals holding advanced security certifications including CIPPIC, CISA, CISM, CISSP and OSSTMM, we have the experience and insight to help you plan, design, build and manage and end-to-end security solution that's right for your organization.