



Nimitz News Publications

#1

Title: The Cost of Denial

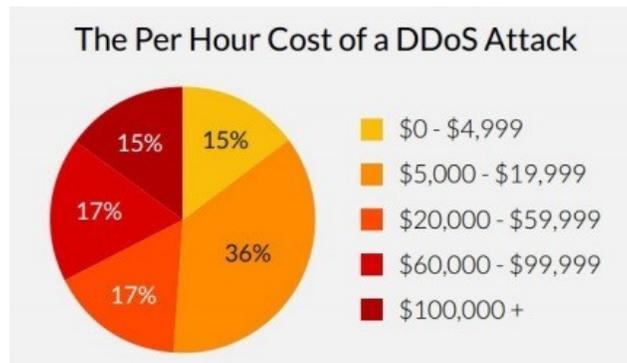
Author: Nimitz

Published: Oct 4th 2018

Updated: July 31st 2019

Distributed Denial of Service attacks (DDoS) are a method of exhausting a networks capabilities by attenuating available resources (e.g. bandwidth, routers, CPU, cache, ...) intended for legitimate traffic. This results in either complete downtime or reduced operational capacity for both service providers and users. They are often caused by a malicious agent(s), who's goal is to intentionally cause some form of harm towards the intended victim(s).

In 2014 [Incapsula](#) performed a North American survey looking into the frequency and consequences of DDoS attacks across a range of industries, varying in size from small (250-499 employees) to enterprise (>10,000 employees). From those surveyed, 45% of respondents indicated that they had experienced an attack. Of which 49% lasted between 6-24 hours with an average estimated cost of ~\$40,000 per hour.



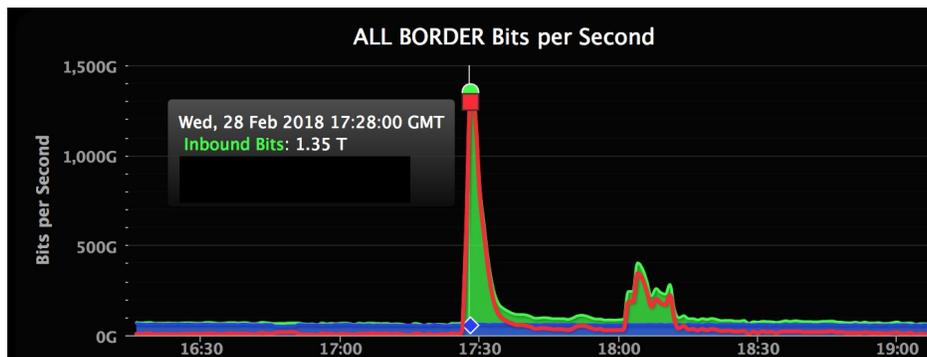
These costs can often fall under one of two categories. Those associated with the initial onset and duration of an attack or those that followed its termination as a consequence of remediation and future provisioning.

During:	After:
<ol style="list-style-type: none"> 1. Loss of payments 2. ↓ customer service 3. ↓ worker productivity 4. Loss of physical data 5. Compromised network security 6. Cost of emergency CyberSecurity reponse 7. Damage to physical networking infrastructure 8. etc... 	<ol style="list-style-type: none"> 1. ↓ consumer trust 2. ↓ brand recognition/ reliability 3. ↑ cost of remediation to restore trust 4. ↑ cost of hiring addition IT security personel 5. repairing/ upgrading physical infrastructure to accomodate attacks 6. etc...

As of 2017 it is estimated that 99% of organizations have taken some form of initiative towards mitigating the effects of DDoS attacks. Reports from [Neustar](#) suggest that of those 99%, 90% are investing more than years prior with 33% feeling that the increases are insufficient.

["99% of organizations have DDoS-specific defenses in place, nine in ten are investing more than they did just 12 months ago. Even then, more than 1/3 believe that the increases are still insufficient" -Neustar](#)

On February 28th 2018 [Github](#) was hit by the largest DDoS attack ever recorded, reaching a peak inbound traffic of 1.35Tbps (126.9 million packets per second). Only to be exceeded five days later by a 1.7Tbps attack on a unidentified customer of U.S based service provider, [Arbor Networks](#). Even though attacks such as these are uncommon they are becoming more likely to occur as technology continues to advance and the cost of doing business increases. Data published by [Trend Micro Inc](#) showed that DDoS attack services can be purchased for as little as \$150 per week. Showing that it does not take much to cause some form of harm.



Research done by [Corero Network Security](#) indicated that 94% of attacks that have occurred in 2018 (Q1, Q2) so far were <5Gbps with 81% <1Gbps and could not be completely countered with traditional methods. Now that we are nearing the end of 2018, the frequency of DDoS attacks is continuing to rise (Q4/2017 < Q1/2018 [53%](#) < Q2/2018 [35%](#)), with no end in site businesses are scrambling to find a solution that is both cost efficient and effective.

Resources:

- [1] <http://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf>
- [2] https://www.discover.neustar/201705-Security-Solutions-DDoS-SOC-Report-LP.html?utm_medium=web%2520referral&utm_source=blog-security&utm_campaign=201705-securitysolutions-ddos-ddossocreportblogsecurity&ucid=7013900001bbzpa2
- [3] <https://githubengineering.com/ddos-incident-report/>
- [4] <http://www.enterpriseitworld.com/index.php/q1-2018-observes-53-increase-in-ddos-attack-number-from-q4-2017/>
- [5] <http://www.itnext.in/article/2018/10/04/ddos-attacks-increase-q2-2018-study>
- [6] <https://asert.arbornetworks.com/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon>
- [7] <https://www.helpnetsecurity.com/2018/09/13/ddos-attack-frequency-grows/>
- [8] <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>
- [9] <https://www.corero.com/resources/reports/h1-ddos-trends-report/>
- [10] <https://nimitz.ca/>