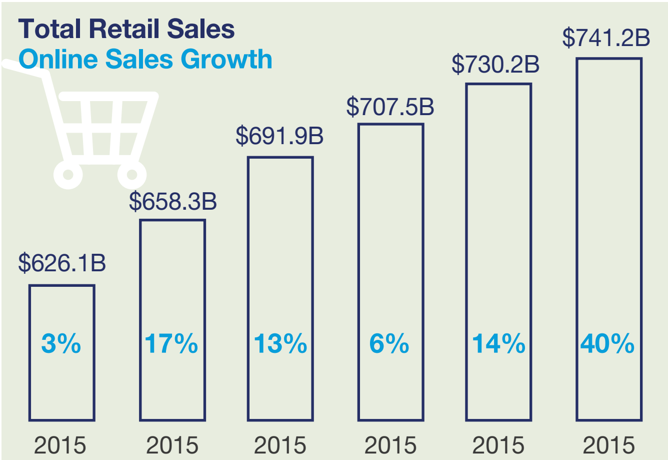
Most Vulnerable to DDoS Attacks

Background

Forrester predicts that by 2021, worldwide e-commerce sales will exceed $4.9 trillion, and retail sales are projected to reach $30 trillion by 2023. One of the triggers for this projection can be attributed to COVID-19. The pandemic has shifted consumer shopping patterns and forced greater adoption of e-commerce across all generations. As a result, the last quarter of 2020 is witnessing an upward shift with e-commerce exceeding pre-pandemic levels.



Source: National Retail Federation, CBRE Research, September 2020

However, even as consumers turn to online shopping, DDoS hackers are sharpening their wits to launch more sophisticated DDoS attacks. There were 4.83 million DDoS attacks in the first half of 2020 - a 15% increase. Attackers focused on COVID-era lifelines such as e-commerce, with complex, high-throughput attacks to overwhelm and take them down. More than 929,000 DDoS attacks occurred in May, representing the single largest number of attacks ever seen in a month and overall DDoS attack frequency jumped 25% during peak pandemic lockdown months.

DDoS attack traffic originates from many different sources – potentially thousands or more. These attacks are damaging as they come from so many sources it makes it highly difficult to stop them. It is also extremely difficult to distinguish legitimate user traffic from attack traffic. These potential DDoS vulnerabilities in any IT infrastructure, called DDoS mitigation gaps, take an immense toll on website resources and processing capabilities – causing websites to slow down or worse, crash.

DDoS Challenges for Retailers

Downtime Translates into Lost Business

For retailers, downtime translates into immediate lost business. The conversion rate for a leading online retailer peaked at 1.9% with an average page load time of 2.4 seconds. Only a one-second slower average page load time of 3.3 seconds led to a drop in the conversion rate by 27%. Google reported that site latency of 100 to 400 milliseconds has a measurable impact on consumer behavior and a site, which is slower by 250 milliseconds than a competitor's site, will be less visited.

The Rise of the Smaller and Stealthier DDoS Attacks

Neustar reveals a significant increase in small-scale DDoS attacks. The hacker aims to remain below the conventional 'detect and alert' threshold that could trigger a standard DDoS mitigation strategy. This ensures that an attack can continue unnoticed while specific areas of the target network are incapacitated. These smaller, stealthier DDoS attacks are designed to enable the perpetrator to get in and get out of a network unnoticed or allow the attack to continue for quite a long time undetected. Attacks target the bandwidth of e-commerce sites and are designed to disrupt business functions, severely damaging traffic and databases. As a result, a successful attack, well-timed to hit during a busy shopping period, for example, can lead to huge losses. Even a smaller attack that overloads servers and takes a site down for a few seconds could frustrate customers enough to shop elsewhere. Equally, attackers might seek to extort money from a retailer by simply threatening a DDoS attack.

DDoS Not Considered a Top Security Priority

DDoS threat requires a culture shift for many retailers as, until now, the focus has been on point-of-sale malware and online attacks targeting credit card data. However, 33% of all cyberattacks on retailers come from DDoS, making it the most common digital threat the sector currently faces. Research indicates that 72% of CTOs and CISOs of the retail industry are unprepared for DDoS attacks until they set in and by the time IT reacts, the stealthier threats could have penetrated the network.

DDoS Mafia

In the past DDoS was primarily used for pranks and petty mischief, but it is now increasingly used by organized cyber-criminals to threaten retailers' operational and financial security. When executing a DDoS attack, hackers set their sights on any organization that relies heavily on its website to generate revenue.

Implications of DDoS Attacks for Retailers

Estimated Costs

Neustar's most recent study indicates that nearly half of the enterprises (49%) estimated their hourly revenue risk at US$250,000 or higher. When considering that mitigating DDoS attacks takes 45% of enterprises between 3 hours, to more than 24 hours, that amounts to significant financial losses.

Session Disruption

Finding customers who buy online, keeping in mind the severe competition, and then losing them to a DDoS attack is unimaginable. 20 DDoS attacks in 30 days can degrade customer web traffic by 35%. Relatively speaking, a 35% degradation in traffic equates to a 60% drop in online purchases and a 40% increase in abandoned shopping carts.

Productivity Losses

The average cost of network downtime is around $300,000 per hour. Along with the time required to get the network up and running, it takes an average of 23 minutes to get refocused on one's prior task. According to a Carnegie Melon University study, cognitive function can decrease by 20 percent after an interruption.

IT Staff Time and its Impact on Security

In the world of digital transformation, IT manpower is a key contributor to business revenue. Their responsibilities stretch beyond setting up hardware and network to ensuring seamless communication channels. As key contributors to the business's revenue, locking them up in managing an attack can impact the overall smooth functioning of the IT organization and thereby impact revenue numbers.

What Can Retailers Do?

Even retailers who diligently prepare for peak season may run into problems that can come from unexpectedly high levels of traffic caused by DDoS attacks. Every retailer should have a plan in place for what it will do in the event its e-commerce site is slowed down during a peak period.

DDoS attacks are smart, sneaky, and stealthy in their methods. And waiting for an application or the website to come down before reacting is already too late. Continuous monitoring is required to recognize an attack before it happens.

Mitigation solutions are reactive - springing into action after an attack has been initiated. This is the reason why even with the most sophisticated DDoS mitigation and DDoS testing deployed, most companies are left with a staggering 48% DDoS vulnerability level. This gap allows damaging DDoS traffic to penetrate the target network, causing system disruption and downtime.

Introducing RADAR™ - detecting open vulnerabilities in real-time

RADAR™ analyzes the target network attack surface exactly as a hacker would. By simulating known attacks against all web facing IP's targets without any downtime, RADAR™ detects open vulnerabilities in the target network. RADAR ™ clearly identifies the attack surface risks (DDoS vulnerabilities) automatically as they are generated across live production web-facing IP's. Then it prioritizes the vulnerabilities by the number of targets found prone to and details the nature of those vulnerabilities through unprecedented information. This information enables proper mitigation and remediation setup. Once the remediation is completed RADAR™ validates the remediated vulnerabilities ensuring the remediation process was successful.

- Differentiate between legitimate traffic and DDoS attacks - RADAR™ continuously & without disruption, detects DDoS risks before an attack happens, not after, thereby ensuring that all three layers, i.e., layers 3, 4, and 7 are continuously checked.

- Prevent the risk of DDoS attacks - Working as a top layer on any mitigation solution, RADAR™ eliminates in advance any chance of downtime if attacked.

- Safeguards applications from insidious attacks - By taking a DDoS risk-based approach it prioritizes vulnerabilities to reduce the time and effort needed to close the highest risk vulnerabilities.

- Reduce the burden on existing IT staff – by detecting and eliminating DDoS threats before an attack and not during or after.

- Business as usual - continuously & without any downtime, RADAR™ detects all DDoS vulnerabilities on an ongoing basis. Working as a top layer on any mitigation system to provide end to end full DDoS coverage.

About MazeBolt

MazeBolt is an innovation leader in cybersecurity and part of the DDoS mitigation space. Offering full DDoS risk detection and elimination and working with any mitigation system to provide end to end full coverage. Supporting organizations in avoiding downtime and closing DDoS vulnerabilities before an attack happens.

For more information,
please visit: www.mazebolt.com
or e-mail: info@mazebolt.com