MAZEBOLT

WHITEPAPER

The CISO DDoS Handbook

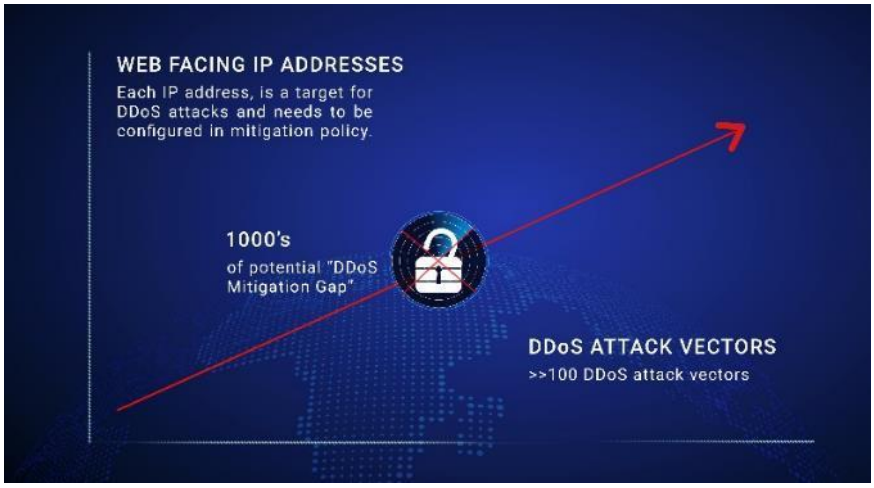
Table of Contents

Introduction

In the past, the threat of DDoS was low in comparison to the more complex cyber threats such as phishing, malware, social engineering, and ransomware. But that is no longer true, as DDoS has become one of the biggest cyber security concerns for CISO's worldwide. To understand the reasons for DDoS moving up the threat chain and the best ways to protect enterprises from DDoS attacks, requires an in-depth understanding of what DDoS is and a deep understanding of how mitigation solutions work, and their limitations.

DDoS and its Threat Landscape in a Digitally Transforming World

A DDoS ("Distributed Denial of Service") attack has a distributed attackers base, i.e., from many source IPs and generally multiple geo-locations. It can be hundreds or even thousands of source IPs from where the attack originates. This gives the attacker the advantage of making it more difficult for the targeted victim to mitigate the attack. DDoS attackers launch bots to cause downtime by sending internet traffic to a network in large numbers, eventually causing the site to crash.



DDoS attacks generally target all three levels of website infrastructure:

- **Layer 3 (Volumetric IP level),** which generates massive amounts of traffic, clogging the bandwidth, slowing the web or service performance, and ultimately preventing website access or the ability to access services.
- **Layer 4 (Volumetric IP level and Protocol Transport level),** which use up all the processing capacity by saturating an end server's CPU or connection table using a connection-oriented attack.
- **Layer 7 (Lower volume, higher connections, low and slow, application attacks)** exploit weaknesses in the application layer, overwhelming the database or server powering the application directly.

OSI Layer (#)	Attack Types
Network (3)	ICMP, Malformed IP, IP Fragmented
Transport (4)	SYN, UDP Flood, Empty Connection, PSH+ACK Flag, URG Flag
Application (7)	Brobot, SlowLoris, DNS Request, HTTPS, SSL Negotiation HULK

New DDoS Attacker Tactics in the Digital World

WS-Discovery Attacks

Attackers use a protocol called WS-Discovery (WSD) which allows unauthenticated traffic to flow through and amplify attacks. Amplification as a method is not new and has been used in the past under the names of Simple Network Management Protocol and Simple Service Delivery Protocol.

Multi-modal DDoS Attacks

Instead of just one single form of attack, multi-modal involves the launch of several different types of attacks at one point in time. For example, an attacker will launch one attack, and as the mitigation solution tries to mitigate it, another vector is launched, one which could penetrate the network.

Ransom DDoS Attacks

Ransom DDoS attacks or RDDoS as they are known are attacks which are launched with ransom demands as the underlying motive. Attackers launch small attacks with the promise of a larger attack on their web applications unless their demands are met.

Zero Day Attacks

These are attacks that involve vectors that haven't been previously used by attackers. As they are new and unknown, mitigation solutions are unaware of them, and therefore, blocking them is not possible. In parallel, they target unknown vulnerabilities in the network.

IoT DDoS Attacks

IoT devices are constantly increasing; there are thousands of them out there. As IoT devices are created to serve an array of purposes their manufacturers are not primarily concerned with ensuring security within these new devices. DDoS attackers are not interested in corrupting a single device. They on the other hand look to penetrate the network using the vulnerabilities in the IoT devices to launch DDoS attacks.

Low-rate attacks

Enterprises struggle to distinguish between low-rate attacks and legitimate traffic, and at the same time, find it difficult to maintain a low false-negative rate. Like the big attacks, small-size attacks can bring down the services rapidly and can create an equivalent impact on businesses; urging companies to be prepared and review their web security arrangements.

Small Sized Attacks

Research confirms that large attacks of 100Gbps and above have fallen by 64% in 2019. However, there has been a startling 158% increase in attacks sized 5Gbps. or less. Enterprises struggle to distinguish between low-rate attacks and legitimate traffic, and at the same time, find it difficult to maintain a low false-negative rate. Like the big attacks, small-size attacks can bring down the services rapidly and can create an equivalent impact on businesses; urging companies to be prepared and review their web security arrangements.

DDoS Taking a Front Seat

DDoS risk is not static but a dynamic challenge with empowered mitigation solutions. The DDoS threat landscape is continuously shifting with new threats, new vulnerabilities, and new forms of attacks emerging almost on a day-to-day basis. For businesses, the impact of DDoS attacks is substantial in both the short and long-term. Short-term damages, for example, are costs associated with downtime/latency, and loss of immediate revenue, personnel costs associated with mitigating attacks. The long-term impact would be customer churn, regulatory repercussions, and compromised data.

Overall, enterprises engage sophisticated technologies to protect business assets and are committed to cybersecurity. Also, most enterprises remain confident that their mitigation solutions will ensure total protection from damaging DDoS attacks. The wake-up call comes when the organization is under attack and by then it is often too late. One of the key reasons for this is that enterprises expect their existing defense solutions to protect them without realizing that DDoS is a different type of threat altogether and needs to be handled differently.

Along with the large attacks, there were several more attacks of all sizes and durations that impacted companies across industry segments. Publicly available information (which is only an indication of the actual attacks) shows a barrage of major DDoS attacks on banking and financial services, government, and gaming. More details of these attacks can be found in our monthly DDoS Attack Round-ups.

For attackers, these are cheap attacks and can be obtained for as little as $10 per hour on the Dark Web. However, the impact on organizations can be devastating, costing the organization millions of dollars. Enterprises that have been attacked have suffered from loss of revenue from downtime, loss of customers from session disruption, and productivity loss.

Existing DDoS Prevention Methods:

- DDoS Testing
- DDoS Mitigation
- DDoS Simulation

DDoS Testing

DDoS attacks and the ensuing challenges such as downtime, loss of revenue, and customer goodwill, have created a niche for DDoS testing as an exclusive, mandatory security requirement.

The importance of DDoS testing can be understood in a blog that GitHub put out in 2014 after it suffered a massive DDoS attack that saw incoming traffic at a rate of 1.3 Tbps. The DDoS attack which went on for over 2 hours, made GitHub completely unreachable.

This painful attack, according to GitHub, was mitigated. However, the damage had been done despite mitigation postures. This paved the way for transformation, and GitHub investigated ways to simulate attacks in a controlled environment, to test their countermeasures. They invested in testing on a regular basis to build additional confidence in both their mitigation tools and to ensure improved response time going forward. To summarize, GitHub would rely on testing and automation to ensure resilient infrastructure.

Understanding why DDoS Testing could not prevent further attacks for GitHub requires a basic understanding of how DDoS testing works.

DDoS testing follows three steps:

Scoping: The Test Plan template is designed during this starting phase where all that needs to be protected including 3rd party applications are identified. The template includes necessary information about countermeasures and identifies roles and lines of responsibility. The template is circulated to all concerned.

Design: The targets are analyzed from the attacker's point of view and target profiles are created. This helps to uncover variations in attack format and helps to create the test plan.

Implementation: The tests are created in the testing platform and parameters will be entered and tested at low levels to ensure that all risk factors are considered.

So why is DDoS testing NOT a complete solution to ensure DDoS mitigation effectiveness?

Testing is invariably performed around twice a year. Static tests are done on dynamic environments that are constantly changing due to website upgrades, new applications, etc. hence their conclusions are not timely and do not hold well for extended periods of time (generally less than 1-2 months).

Some of the other challenging factors that need to be kept in mind are:

1. DDoS testing's capability to detect DDoS risks before attacks are limited.
2. During testing, there will be disruption to ongoing operations.
3. The number of DDoS attack vectors covered is less than 20.
4. Coverage of Web-facing IP Addresses is normally limited to around 4.
5. Vulnerability re-validation is limited to once a year, leaving the organization vulnerable for the rest of the time.
6. Finally, there is no proactive DDoS security.

Additionally, the key factor before or during an attack is the human factor. The security engineers, when busy battling an attack, will not be able to monitor other activities creating a `blind spot' which DDoS actors can exploit to penetrate the organization.

DDoS Mitigation

DDoS mitigation generally follows one of two approaches:

Reactive, "on demand" – Also known as Monitoring Mode does not block suspicious traffic automatically but monitors and waits for a block order. This is not always automated, which means by the time the mitigation provider discovers the problem – often reported via a client calling the customer service line – it is usually too late to prevent downtime.

Continuous, `always on' – goes into effect automatically. All traffic is inspected, and suspicious traffic is separated before it reaches the infrastructure, preventing it from going down.

Existing mitigation solutions can be categorized as follows:

Signature-based DDoS Mitigation as the name indicates identifies certain rates and strings in packets for Layers 3, 4, and 7 from SRC IPs. They generally do this by blocking or suspending SRC IPs. Specific mitigation mechanisms vary by vendor, but the approaches are similar. They do well with identified threats only.

Behavioral-based DDoS Mitigation - Based on the vendor, these mechanisms use various proprietary algorithms to identify malicious DDoS traffic, such as measuring the normal baseline rate and comparing it against IPs that deviate from that rate.

Challenge-based DDoS Mitigation - This mitigation defense may issue a challenge to specific or all new connecting IPs when an anomaly has been discovered to determine whether the traffic is legitimate. This challenge may be Layer 7 or Layer 4: a SYN cookie challenge, DNS challenges, JS/302 redirect challenges, etc.

Out-of-state Packet DDoS Mitigation - Some DDoS mitigation devices in certain deployments may enforce stateful sessions or deliver partial enforcement for TCP traffic.

Rate-based/Geo-blocking DDoS Mitigation - When no other option is available, these primitive fallback methods are used. They are false-positive prone, so they may cause more problems than they solve; however, most vendors offer rate-limiting options. When you have no option, some false positives may be better than a complete site outage.

Botnet-detection DDoS Mitigation - Botnet-detection DDoS mitigation generally involves applying a known list of attacking IPs to perimeter defenses. It is only part of a wider toolbox for mitigating attacks because it's only as good as the quality of the list. It may also introduce some level of false positives, and it will never find zero-day attacks. The lists also vary by vendor, so some IPs on one list may not be on another.

So why is DDoS Mitigation NOT a complete solution to ensure DDoS mitigation effectiveness?

- → DDoS mitigation is not an IT issue limited to bandwidth and networking. It is a global concern that affects business continuity, reputation, and customer loyalty, and therefore requires the complete engagement and involvement of business leaders.

- → Even with the most sophisticated DDoS mitigation and testing solutions deployed, most companies are left with major DDoS vulnerabilities. DDoS Mitigation security policies don't adapt to dynamic changes happening in the network, leaving around 50% of DDoS vulnerabilities undetected and therefore unprotected. Furthermore, mitigation solutions & infrequent Red Team DDoS testing are reactive, rather than automatically and continuously detecting and closing vulnerabilities.

- → DDoS attacks are getting smarter and sneakier, and companies aren't sufficiently prepared to dodge devious threats. In 2020, successful DDoS attacks witnessed a 200% growth. From Netflix to Twitter, Wikipedia to international banks, gaming and gambling sites, DDoS attacks have spared no industry segment. Although the statistics may exhibit that the attacks target `certain types' of enterprises, in reality, 9 out of 10 businesses have claimed to experience an attack, with an average downtime of 30 minutes. Gartner estimates that a single minute of downtime costs most businesses $5,600, or more than $300,000 per hour. The aftermath of a DDoS

attack leads to monetary loss, operational challenges and loss of customer trust. Ironically, enterprises who believe they are safe from web attacks are the ones who suffer the most debilitating threats because they are unprepared.

→ Currently, mitigation solutions are inept to re-configure and fine-tune their DDoS mitigation policies, leaving their ongoing visibility limited, and forcing them to troubleshoot issues at the very worst possible time, i.e. when a successful DDoS attack brings down systems. These solutions are all reactive, reacting to an attack, and not closing DDoS vulnerabilities before an attack happens. All existing solutions, whether they are testing, or mitigation are all reactive in nature which is what makes DDoS the single biggest threat to enterprises worldwide.

The Only Complete DDoS Protection for the Digital World

Simulate DDoS attacks with no downtime

To effectively block complex and intermittently changing threats, enterprises should continuously validate and remediate the entire dynamic attack surface in peaceful times and fix known areas of weaknesses proactively as there is no time to do this when an attack starts.

Break complex attacks into individual attack vectors to ensure protection automatically against mixed vector attacks.

DDoS Simulation - MazeBolt's RADAR™ technology

MazeBolt's RADAR™ testing is the only 24/7 automatic solution testing DDoS attacks across your live environment with zero operational downtime. It automatically detects, analyses, and prioritizes the remediation of DDoS vulnerabilities in any mitigation system. Raising the efficiency of your mitigation solution for a healthy DDoS mitigation posture.

This new technology enables:

Vulnerability Identification across the complete attack surface, automatically running thousands of non-disruptive smart attack simulations against protections in place to identify the entire vulnerability landscape.

Guided Remediation Process and Revalidation of specific network vulnerability intelligence collection throughout the process creates a personalized remediation plan, guiding customers in closing vulnerabilities in the most accurate and effective manner.

Finally, the system immediately revalidates the protection level, ensuring the highest level of protection is achieved.

About MazeBolt

MazeBolt is pioneering a new standard in testing DDoS vulnerabilities that provides enterprises with full visibility into their dynamic DDoS attack surface. Its vulnerability solution, RADAR™ testing, continuously observes tens of thousands of potential DDoS attack entry points, identifying how attackers succeed in bypassing existing mitigation systems. The solution's autonomous risk detection allows cybersecurity teams to go beyond traditional DDoS testing by continuously detecting, analyzing, and prioritizing remediation across the network with zero operational downtime. Global enterprises, including financial services, insurance, and governments rely on MazeBolt for full visibility into their DDoS security posture. For more information, visit https://www.mazebolt.com or email info@mazebolt.com