MAZEBOLT

The DDoS Handbook

for CISOs and Security Leaders

Table of Contents

A Changing Landscape 3

Deciphering the Anatomy of DDoS Attacks 4

Unveiling Modern DDoS Attacker Tactics 5

The Weakness of Existing DDoS Security Methods 6

The Incomplete Puzzle of DDoS Mitigation 7

The New Approach to DDoS Security 8

A Changing Landscape

According to a recent poll, 94% of CISOs are stressed at work. These stressors include everything from employee skills gaps and tight budgets to an inability to automate manual tasks and too many overlapping security technologies.

There's no doubt that being a CISO is a harder role than ever before, and a 200% rise in DDoS attacks is just one of many problems keeping them up at night.

Superheroes of the C-suite, the CISO is keeping risk at bay in every direction, ensuring 100% business continuity, securing sensitive enterprise data and customer PII, and protecting both service availability and business reputation – all as part of a day's work.

While most companies have DDoS mitigation and prevention solutions in their tech stack, attacks continue to rise, and the limitations and vulnerabilities inherent in existing tools are going undetected, unnoticed, or even ignored. Honestly, CISOs just want to consider the risk of DDoS attacks solved.

DDoS vulnerabilities may be inevitable but mitigating them proactively removes the fear of waiting for an attack, and then dealing with the fallout from a breach.

This eBook looks at:

1. The kinds of DDoS attacks and tactics most prevalent in today's cybersecurity landscape
2. The limitations of today's DDoS prevention technologies
3. A new approach to DDoS mitigation – proactive, continuous, and non-disruptive

Deciphering the Anatomy of DDoS Attacks

A DDoS attack is a simple yet fierce adversary, its strength stemming from a distributed attacker base. The attack originates from numerous source IP addresses, often spanning multiple geographical locations. Imagine hundreds or even thousands of source IPs converging to execute the attack, often controlled by one single entity. This provides the attacker with a distinct advantage, making it considerably more challenging for the target to withstand the onslaught.

DDoS attackers employ a legion of bots to overwhelm a network with internet traffic, eventually crashing the targeted website and/or online services - which leads to disruption to business continuity and downtime.

A dramatic

200% rise

in DDoS attacks emphasizes the escalating cyber threat landscape [1]

DDoS attacks are known to target all three critical levels of a website's infrastructure:

Layer 3 (Network): At this layer, DDoS attacks, such as IP/ICMP floods, aim to consume the bandwidth available to the target network. By sending a massive number of data packets to the network, attackers can saturate the bandwidth, causing legitimate requests to be dropped or significantly delayed. This level of attack can prevent access to websites hosted within the network.

Layer 4 (Transport): DDoS attacks at the transport layer, such as SYN floods exploit the TCP handshake process. Attackers send a flood of TCP/SYN requests with spoofed IP addresses to the server, which then allocates resources and waits for the acknowledgment that never arrives. This can exhaust the server's resources, making it unable to process legitimate requests.

Layer 7 (Application): Application layer attacks, such as HTTP floods, directly target the web application itself. These attacks mimic legitimate requests but are sent in such high volumes that the web servers or application resources (such as CPU and memory) become overwhelmed. Since these attacks mimic normal traffic, they can be harder to detect and mitigate. They can target specific website features, such as search functions or login pages, to consume more server resources.

1 https://www.zayo.com/newsroom/ddos-attacks-in-h1-2023-up-200-from-2022-according-to-new-zayo-data/

Unveiling Modern DDoS Attacker Tactics

In the connected realm of the digital world, DDoS attackers continually adapt and devise new strategies to disrupt their targets. In this section, we will explore the latest tactics employed by threat actors.

1 **WS-Discovery Attacks**

Attackers harness a protocol called WS-Discovery (WSD) that permits unauthenticated traffic to flow through, providing an avenue for attackers to amplify their attacks. This concept of amplification is not new and has previously appeared under names such as "Simple Network Management Protocol" & "Simple Service Delivery Protocol."

2 **Multi-Vector DDoS Attacks**

Instead of relying on a single type of attack, some DDoS attackers involve the simultaneous launch of multiple attack vectors. For instance, an attacker initiates one assault, and as the DDoS protection provider attempts to mitigate it, another vector is unleashed, potentially penetrating the network's defenses.

3 **Ransom DDoS Attacks (RDDoS)**

Ransom demands are the primary motive behind RDDoS attacks. Attackers initiate small-scale attacks and threaten larger ones on web applications unless their demands are met. RDDoS attacks are a severe menace to organizations worldwide, and in many cases – organizations feel they have no choice but to pay the ransom.

4 **Zero Day Attacks**

Zero Day attacks exploit vectors that are new – previously unused by attackers, and unknown vulnerabilities within the network. As mitigation providers do not know about these vectors and vulnerabilities, defense is virtually impossible. After all, you can't block what you don't know about.

5 **IoT DDoS Attacks**

As Internet of Things (IoT) devices become increasingly common, attackers have begun leveraging IoT as a new avenue for exploitation. Smart TVs, smart speakers such as Google Home, toys, wearables, and even smart appliances are all potential attack vectors. IoT device manufacturers often prioritize functionality over security, leaving vulnerabilities, and opening doors for DDoS attackers to infiltrate networks using these IoT device weaknesses as launch points for their attacks.

6 **Low-Rate Attacks**

Enterprises often face the challenge of distinguishing between low-rate DDoS attacks and legitimate traffic. Maintaining a low false-negative rate becomes equally complicated. Despite their smaller size, these attacks can swiftly disrupt services and exert a significant impact on businesses. Often seen as an invisible killer, these attacks often fail to trigger protections at the ISP level, and are a challenge to differentiate from legitimate traffic.

The Weakness of DDoS Protection Methods

The landscape of DDoS attacks is anything but static. It's a dynamic challenge that continually tests the limits of even sophisticated DDoS mitigation solutions. The DDoS threat evolves with new threat actors, vulnerabilities, and attack vectors emerging almost daily. The truth is that many security leaders tend to overestimate their existing DDoS protection solutions, assuming they provide a complete safeguard against destructive DDoS attacks and the associated damaging downtime.

There are two main areas of concern with existing DDoS mitigation platforms, the way they test against vulnerabilities, and how they practically prevent DDoS attacks.

The Importance of DDoS Testing and Simulations

DDoS attacks, with their grim consequences including downtime, revenue loss, and tarnished reputational damage, have thrust DDoS testing into the limelight as a mandatory security requirement for governance, risk and compliance (GRC).

From the largest enterprises to the smallest businesses, when companies are hit by a DDoS attack, it underscores the necessity for further testing of their defenses. One example is Microsoft, who was hit by a DDoS attack in June 2023, and publicly shared that "Microsoft consistently reviews the performance of its hardening capabilities and incorporates learnings into refining and improving their effectiveness."

As well as being an important part of incident response, thorough testing is also a critical element of compliance regulations such as HIPAA, GDPR, DORA, and PCI-DSS. Additionally, it has often become a prerequisite for obtaining cyber insurance.

Currently, the majority of enterprises use red team testing and manual simulations to complete DDoS testing. There are many limitations to consider with this approach:

Relevance: DDoS testing typically occurs once a year because it is intrusive and disrupts ongoing production and business activities. It scrutinizes dynamic environments that change and evolve due to website upgrades, new applications, and more. Consequently, DDoS testing's conclusions often lack timeliness and are relevant for only brief periods, typically less than 1-2 months.

Scope: Traditional DDoS testing is also limited in detecting DDoS risks before attacks occur, with a restricted number of DDoS attack vectors covered (typically less than 20), limited coverage of web-facing IP addresses (typically around 4), annual vulnerability re-validation, and a lack of proactive DDoS security measures.

Risk: The human element plays a crucial role before and during a DDoS attack: Security engineers busy battling an ongoing attack may inadvertently create a blind spot that DDoS threat actors will exploit to infiltrate the organization - and create even more downtime.

Business continuity: Scheduling red team tests during weekends, typically when production is slower, requires consideration of staffing and productivity losses, as well as revenue losses where applicable – for example in eCommerce and financial services.

Visibility: Red team testing provides insights into only a small fraction of an organization's DDoS attack surface, averaging about 0.01%. This represents a significant blind spot, as most

The Incomplete Puzzle of DDoS Mitigation

DDoS mitigation generally follows one of two approaches. Either the solution works reactively, simply monitoring traffic and waiting for a block order, or all traffic is monitored, and suspicious behavior is automatically blocked based on pre-defined rules. These rules could be based on identifying signatures of known threats, detecting unusual behavior against a baseline, or applying a list of known attacking IPs to perimeter defenses, as just three examples.

So, why does DDoS mitigation fall short when it comes to ensuring complete and automated protection?

Despite deploying DDoS protections, companies experience a

40-75%

exposure to DDoS attacks, revealing gaps in current mitigation techniques [2]

Existing mitigation solutions and bi-annual (at best) DDoS testing methods are typically reactive, responding to attacks rather than proactively identifying and addressing vulnerabilities. It's true that DDoS protection providers include SLAs to mitigate DDoS attacks and remediate vulnerabilities – but these usually only come into play once an attack has occurred.

And once an organization is already under attack, it may be too late to prevent severe damage and downtime.

Even with sophisticated DDoS protection and mitigation solutions in place which act automatically to prevent attacks, many companies are left with 75% online exposure of their online services, as security policies often fail to adapt to dynamic environment changes. Mitigation solutions often lack the ability to reconfigure and fine-tune their policies, leaving visibility limited. They can also quickly become vulnerable due to outdated settings, patches, and misconfigurations that arise as the last service maintenance window fades into the distant past.

All this leads inevitably to an elevated risk of service interruption that will require emergency response scenarios, creating a heavy reliance on reactive actions.

As DDoS attacks become increasingly sophisticated, resulting in a 200% increase in DDoS attacks in 2023, no industry is immune.

Without an automated DDoS protection solution that tests for vulnerabilities, where DDoS mitigation platforms fall short, organizations must deal with the immediate costs tied to DDoS attacks, including service downtime, latency, and revenue loss, as well as the resources associated with incident response. In the long-term, consequences extend further, contributing to customer churn, reputational damage, regulatory ramifications, and compromised data security.

2 MazeBolt RADAR testing results

The New Approach to DDoS Security

There's no doubt that DDoS mitigation solutions are often reactive and always vulnerable. With the realization that DDoS vulnerability testing is now a cyber necessity, and that DDoS mitigation has its inherent limitations, organizations must adopt a new approach to DDoS security: Proactive and automated protection.

1 MazeBolt RADAR™ is the only solution that identifies and enables the elimination of DDoS vulnerabilities ahead of time, without a disruption to business continuity so that organizations can stay protected without experiencing maintenance windows or service downtime.

2 RADAR automates DDoS security by performing non-disruptive and continuous DDoS simulations on live, production services. RADAR's autonomous risk detection allows cybersecurity teams to reinforce their existing DDoS protection systems by continuously detecting vulnerabilities and misconfigurations, analyzing traffic data, and prioritizing remediation for DDoS readiness.

3 RADAR requires zero operational downtime, and identifies Layer 3, 4, and 7 DDoS vulnerabilities, with over 150 DDoS attack vectors checked. RADAR identifies volumetric, low and slow, carpet bombing, and multi-vector attacks, prioritizes and manages the remediation and validation of DDoS vulnerabilities, and provides full online services coverage – validating all targets and services, against all known attack vectors to identify all vulnerabilities.

! MazeBolt RADAR is the only solution that **identifies and enables** the elimination of DDoS vulnerabilities ahead of time, without disruption to business continuity.

Identify your DDoS vulnerabilities with our free DDoS Threat Rating tool

Learn more