NimbusDDOS

ARTICLE :

5 Common DDoS Misconceptions

Having been involved in the DoS (denial of service) attack landscape for 24 years, I've seen a broad array of changes. From the early days, of a simple ICMP flood on a hacked shell account, up through modern massively distributed IoT botnet attacks. Like many security professionals, I frequently talk to my clients about the emerging threats, and what the "next big thing" in DDoS might be. In cybersecurity we like to talk about the zero-day vulnerabilities, but with DDoS attacks the past is not as distant as it seems, and often just as relevant today as it was 24 years ago. Looking back over the last two decades, I see the same misconceptions emerge repeatedly across a diverse spectrum of organizations and industries. By avoiding these common pitfalls, you can set your organization on the right path to DDoS attack preparedness.

1. My Firewall Will Protect Me

At NimbusDDOS, this is the single most common misconception we see with new customers. Through a barrage of effective marketing, firewall vendors have convinced most IT organizations that all they need, to be secure, is a good corporate firewall. The corporate firewall is so ubiquitous today that I can't imagine an IT manager designing a network without one, and that's a good thing! But every day those same IT managers operate networks with no protection against DDoS attacks.

So what happened with DDoS protection? In the past, DDoS attacks were relatively rare except in certain high-risk industries (e-gaming, banking, adult industry, etc.). Since they weren't exposed to these attacks, most organizations just assumed that they were safe and that their expensive firewall was protecting them, just as it did in other areas. In reality, they were just lucky and had not been targeted. This would change abruptly in 2012 with the first major bitcoin/extortion motivated DDoS attacks appearing, and would abruptly change a few years later with the rise of IoT botnets fueling a DDoS- For-Hire marketplace. What this meant for the DDoS landscape, is a steady increase year-over-year in the frequency of attacks. More importantly for our IT manager, it also meant that organizations that had previously gone unnoticed by attackers were now in the crosshairs.

Recently at NimbusDDOS, we tested a customer that fit this stereotype almost perfectly. This particular customer operated a niche ecommerce site that had never been hit by a DDoS attack. With the increasing media attention surrounding DDoS attacks, the CIO had asked his team to test their defenses out of what he thought was an overabundance of caution. The IT team was confident that their modern next-gen firewall would shrug the attack off. As it turned out, a SYN flood completely crippled the environment. How did an attack from 1995 cause problems for a modern security appliance? The issue is that firewalls, by design, must track connection and session state for them to effectively block other security threats. This also is the same area that a SYN flood attempts to exploit by creating millions of sessions. The end result is that the firewall state tables fill up, and the firewall eventually tips over. This is just one of many DDoS attack vectors that we have seen challenge modern firewalls.

NimbusDDOS

2. DDoS Attacks are Easy to Detect

The classic image of a DDoS attack is an Internet circuit that is overfilled with junk traffic. Conceptually this is easy to understand, if the pipe is full of garbage data, then the good data can't get in. This is great for marketing materials, and the image is strengthened by media reports that describe volumetric DDoS attacks, but this oversimplification has lead to a persistent misconception that DDoS attacks are trivial to detect.

At the heart of a DDoS attack is the notion of impacting availability, but the mechanism for doing so is a bit arbitrary. At the highest level, DDoS attacks tend to be separated into three major categories; volumetric, protocol, and layer-7. Within each category there may be thousands of individual attack vectors. The classic image of the full Internet circuit is the volumetric attack category, where the sole purpose of the attack is to overwhelm the organizations circuits. However, Layer-7 and protocol attacks, don't follow this model. Instead, they attempt to overwhelm other components in the environment like firewalls, load balancers, application servers or databases. And unlike volumetric attacks, this can often be accomplished with a very small amount of traffic. A classic example of this is the Slowloris attack in which the attacker opens a large number of connections to a web server, and slowly sends data to the server in an attempt to exhaust connection resources on the target. During this specific attack, Internet circuit utilization will often drop so sharply that organizations frequently misdiagnose the attack as a server outage.

But why does it matter? Put simply, if you expect a certain behavior then you will be blind to alternatives. Recently we performed a test for one of our SaaS customers that exemplified this. To protect their environment from DDoS attacks, they had configured their alerting system to trigger a DDoS attack incident response if certain bandwidth and packet-per-second thresholds were exceeded. During volumetric attacks this worked well, with their SOC quickly responding and activating mitigation strategies. Then we switched to a "low and slow" layer-7 attack. The attack was only about 50 Mbps, which was nearly undetectable against their legitimate traffic. As a result, their alerting didn't detect the anomaly, and incident response procedures were never activated.

3. My Company is Too Small to be Targeted

The common perception is that only large companies need to worry about DDoS attacks, and that small organizations are somehow immune. While it is true that media reports tend to focus on large companies impacted by DDoS attacks, the reality is that small companies and even individuals are regularly targeted by DDoS attacks. To understand this, we need to consider the motivations of an attacker.

Why would an attacker target a small organization? The motivations of an attacker can often be nebulous, but there are a few common threads that have emerged:

- Personal Vendettas : This is one of the oldest motivations for a DDoS attack. Some of the earliest attacks in the 90s where fueled by animosity between individuals or small groups within gaming and chat communities. This behavior continues to this day, with the well-known example of the security researcher Brian Krebs who was personally targeted.
- Easier Extortion Targets : In many cases, smaller organizations are less prepared for a DDoS attack. For an attacker attempting to extort a ransom, it's often more rewarding to target numerous small companies than one well-prepared large company.
- Business Rivals : Although not common, businesses within some industries and specific geographic locations have been targeted by competitors.

NimbusDDOS

It's important to understand that risk and business size are not directly connected, and that decisions on preparedness should be driven by risk level and tolerance. As an example, we had the operator of a small Forex market contact us while under attack. Although they were a small organization, their risk level was significantly higher than similarly sized businesses. This elevated risk level was primarily driven by the real-time transactional nature of their business, but was also heavily influenced by the loose regulatory environment in which they operated that made them targets of competitors. Unfortunately for them, they had fallen into the pitfall of thinking they would fly under the radar of DDoS attacks.

4. We are Safe Because We Pentest

Organizations that are security aware generally perform regular penetration testing and vulnerability scanning (monthly, quarterly, annually). These regular scans produce reports that detail the areas of vulnerability within the environment, and is indisputably a good best practice. However, they have an unintended side-effect in that most organizations misinterpret the results to indicate that they are secure against all cybersecurity threats. Although some scanners may detect specific software bugs that could cause a DoS, they fail to detect the vast majority of DDoS risk areas.

Why is DDoS special? The areas of security that are tested with traditional pen-testing and vulnerability scanning are generally looking to exploit weaknesses in software and configurations to gain access to specific data or escalate privileges. DDoS attacks, however, aren't dependent on a software or configuration error, and may simply exploit a capacity limitation of the environment. A good example of this is a classic HTTP GET request flood, in which the attacker's botnet simply submits a large number of legitimate web requests to the target site. The impact is that the application server is overwhelmed by the flood of traffic. In this attack, there was no weakness in the webserver or the application code, they just didn't have the capacity to handle the volume of requests. In this scenario, the webserver would have passed their periodic vulnerability scans, yet remained susceptible to a DDoS attack.

5. A DDoS Attack Wouldn't Impact My Business

As mentioned earlier, there are certain high-risk industries that are prone to DDoS attacks. The commonality amongst these targets is that they have a strong reliance on their online presence for revenue generation. For these industries, the need for DDoS attack preparedness is obvious since it can be directly tied to revenue. At the other end of the spectrum there are businesses that have very little reliance on their online presence, which often leads them to the misconception that a DDoS attack wouldn't effect their business.

What are the true costs of a DDoS attack?

- Direct Revenue Loss : This is the obvious loss for businesses that depend on their website like e-commerce or SaaS vendors.
- Human Resource Cost : Often overlooked is the productivity losses within an organization due to a DDoS attack. These certain include IT teams, but can often extend to other areas of the business as well.
- Reputation Damage : A DDoS attack that is in the public eye can cause reputation damage that easily surpasses direct revenue loss in scale. This loss can continue well beyond the time of the attack and may effect a business for months or years.
- Data Loss : DDoS attacks are being used to conceal data theft. The time and monetary cost associated with a data theft or breach can be immense.