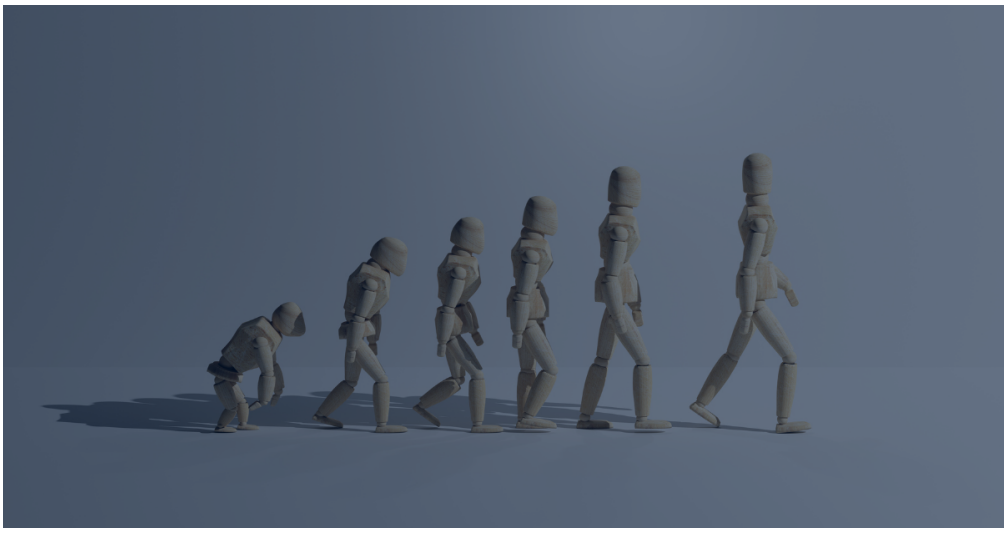
How Have DDoS Attacks Evolved Over The Last 10 Years?

by Steve Mulhearn



DDoS attacks have been a persistent and challenging security threat for many years. In this article, I will explore the evolution of DDoS attacks over the last decade and how attackers have adapted their methods to overcome defense systems.

Plainly speaking, we must accept that for an attack method that is over 20 years old, it is still one of the most difficult security challenges for service providers to deal with. The major target of these original attacks was the infrastructure. In particular, attackers focused on the weaker, lower performance elements of the network, such as the switches and the routers. These devices lacked performance when put under pressure and would stop working.

Early Targets and Defense Options

The DDoS defense product market at that time really only offered their customers two options: They could go granular or go scalable. Scalability was the chosen focus as the target market for these solutions were large, global Tier 1 and transit providers. To do this, they used Netflow/Cflowd/Sflow to take accounting records in and analyse up to Layer 4. These accounting systems were not designed to give detailed data analysis but rather to simply provide billing records to the service provider. Nevertheless, by capturing this information, they were able to gain visibility of traffic behaviour for further analysis.

Adapting to Defense Systems

Much like any other security system, attackers meticulously analysed them to understand exactly how they worked, adapting their methods to deploy low and slow attacks. These attacks were focused on particular servers/services and designed to fly under the detection radar. These infrastructure protection systems came with some other limitations:

- ✔ The response time was the first drawback. It would take minutes for these systems just to detect an attack, let alone start mitigating it.
- ✔ The mitigation techniques deployed by these systems were, at best, rather crude and cumbersome. In worst-case scenarios, they inadvertently took the very systems under attack offline whilst attempting to prevent collateral damage to other services.

Understanding Attackers' Motivations

Often, organisations overlook a crucial aspect: understanding the motivations driving criminals. To effectively counter them, you really do have to get inside their minds, subscribing to the notion that to beat a criminal you have to think like one.

A common, albeit naive, perception among many organisations is that the perpetrators of these attacks are mere 'script kiddies' or 'eco warriors' championing a 'noble' cause against corporations and governments. Whilst it's a comforting thought for some idealists, it's far from the truth, potentially misdirecting defences to incorrect areas of operations. It's vital for defenders to grasp that attackers have a defined objective. This objective is quite straightforward – to maximise profits in the shortest time, with the least effort, and minimal risk.

Evolution of DDoS Protection

As we celebrate the 10th anniversary of our SmartWall solution this year, we're proud of all the feedback we receive from our satisfied customers. Throughout this time, our threat intelligence and SOC teams have developed a deep understanding of attackers' motivations and techniques, which has directly guided the evolution of our DDoS protection platform.

The Future of DDoS Attacks

What sets SmartWall One apart is its automatic detection capabilities. Our threat research team constantly monitors SOC data for the latest DDoS techniques and trends, creating protection that is immediately rolled out to customers. Our approach is to be more than just a DDoS protection provider; it's to be a trusted partner to our customers, providing advanced technology and solutions tailored to the needs of each.

Staying ahead of evolving DDoS threats is key for any business. As attackers constantly develop new techniques to disrupt systems, defenders must consider every possible target of a DDoS attack, from the network layer to the application layer. My advice? Work with a partner that lives and breathes DDoS protection and lean on their experience battling the latest threats. By investing in advanced

protection solutions like SmartWall One, organizations can navigate the ever-evolving digital threat landscape and ensure the continuity of their online operations.

Find out more about how our approach to DDoS protection can help protect your organization by scheduling time to speak with an expert today.

Posted in Blog Posts Tagged ddos attack evolution