5 Things You Didn't Know About DDoS attacks

Even before the current pandemic, the types and speeds of distributed denial of service (DDoS) attacks are on the rise.

And with the architectural changes brought about by COVID-19 - such as more reliance on VPN gateways as more employees work from home - organizations are at greater risk of disruption. .

In fact, according to NETSCOUT's most recent threat report, DDoS attacks in 2020 were up 15% year-on-year in 2019 and up 25% from their pandemic peak. Currently, it is very likely that the world will experience more than 9 million attacks this year.

When organizations consider the steps necessary to mitigate the risks from DDoS attacks, and maintain resilience and readiness, the following 5 aspects should be kept in mind:

1. Pay attention to State-Exhaustion DDoS attacks

When it comes to DDoS attacks, most people immediately think of mass attacks. But State-Exhaustion DDoS attacks prevent state devices, such as firewalls, load balancers, and VPN concentrator (essentially a server), serving connections coming from legitimate clients as well. Negative impact on many critical applications, services, infrastructure, and data.

This problem is particularly serious nowadays, as people increasingly depend on remote connections through VPN concentrators. In order to protect against State-Exhaustion DDoS attacks, it is important to design the network infrastructure, including the applications and service delivery stacks, in order to minimize risk at risk. wherever possible.

There is a common misconception that firewalls are sufficient to protect against DDoS attacks. This is simply not true, as they are vulnerable to State-Exhaustion DDoS attacks. This is why best practices (even from firewall providers) recommend every company to deploy stateless DDoS protection against firewalls to protect them from State-Exhaustion attacks. DDoS.

2. Cloud-based protection is not enough

The most common form of DDoS attack protection is a cloud-based mitigation service, usually from ISPs or independent providers. And while such services are really important in preventing large-scale DDoS attacks, it's only part of a comprehensive protection strategy. For State-Exhaustion and Application Layer attacks, which are also very common, the best practice in the industry is an on-premises, stateless solution that can automatically detect and prevent such attacks.

3. Be mindful of the translation tactics

Many savvy DDoS attackers use attack performance management tools to monitor the effectiveness of their attack in real time. These tools help determine whether defenses are deployed when the attack vectors are altered. This can lead to launching multi-vector attacks, much more difficult to mitigate without the right solution.

4. Scale doesn't always matter

The majority of DDoS attacks today are not large-scale, but small-scale and short-lived. It's important to note that a DDoS attack doesn't need to be large and lengthy to have a negative impact. In fact, the majority of DDoS attacks last an hour or less (even nearly a quarter of them last less than 5 minutes). This means that organizations that need DDoS attack protection can detect and mitigate attacks immediately before any damage occurs.

5. Let's look at a fusion approach to protect against DDoS attacks

A combined method of protection against DDoS attacks is required. The cloud-based model, which relies on service providers to provide mitigating services against large-scale DDoS attacks, can be highly effective. However, to fully protect most organizations from smaller DDoS Application Layer attacks, you should strengthen DDoS protection in place. This allows organizations to quickly deploy custom DDoS protection as new applications or services are deployed.

The reality is, DDoS attacks can be mitigated, if you are prepared. An important part of that preparation lies in regularly reassessing your DDoS attack protection strategy. After all, today's DDoS attacks are ever-changing and traditional protection methods may not be enough. Organizations should stay up to date with the latest trends in DDoS attacks, know what are current best defense methods, and test those defenses on a regular basis.