AVAILABILITY IS EVERYTHING

What does availability mean to your business?

DDoS attacks bring significant risk to organizations that depend on their networks and websites as an integral part of their business. And these days, that's just about everyone. Think about online banking, retailing, travel reservations, medical patient portals, telecommunications, b-2-b e-commerce — virtually every business model today includes a significant online transactional component or, in some cases, has shifted online entirely.

We've all experienced the feeling of frustration, or even desperation, when the online services we expect are not available to us instantly when we want or need them.

Imagine that happening to thousands or even millions of customers worldwide, simultaneously, and you can understand the potential impact of a single DDoS attack on your organization. Maintaining availability of digital platforms, networks, applications and services is not simply a security issue — it is a business risk and continuity issue.

It doesn't take much to take down a fairly substantial section of the internet. In November 2016, an accidental misconfiguration at a major internet infrastructure company led to outages at several large carriers. Although the "route leak" was accidental and not malicious, the resulting 90-minute lack of availability was still painful for the carriers and their customers alike.

A concerted attack can have far more damaging consequences. Unlike advanced threats or data breaches, which are designed for stealth in order to exfiltrate data of value, a successful DDoS attack is instantly recognizable. The symptoms range from poor performance and intermittent outages, to a stream of customer complaints, all the way to sudden and complete unavailability. Whatever the motive, disruption or denial of service is the goal.

HAVE THREAT CAPABILITIES LEAPFROGGED YOUR PROTECTION CAPACITY?

DDoS attacks have been around just as long as e-commerce itself. Established organizations with a significant online presence have always taken measures to ensure availability. Ask yourself, however, if the protection you may have put in place several years ago is still adequate for a modern-day attack. DDoS threat capabilities have become more complex, dynamic and multi-vector. Increasingly, attackers employ a combination of attack methodologies, on the assumption that at least one will succeed while the others divert defenses. These attack types include:

- **Volumetric:** Large bandwidth-consuming attacks that essentially "flood" network pipes and router interfaces.
- **TCP State Exhaustion:** Attacks that use up all available transmission control protocol (TCP) connections in internet infrastructure devices such as firewalls, load balancers and web servers.
- **Application Layer:** "Low and slow" attacks indented to gradually wear down resources in application servers.

Moreover, attacks today are much easier for less sophisticated threat actors to launch, owing to the ready availability of inexpensive do-it-yourself attack tools and DDoS-for-hire services. The threat landscape has been further exacerbated by the rapid proliferation of inadequately secured Internet of Things (IoT) devices, which are being consumed into botnets and weaponized to launch multi-vector DDoS attacks.

EVALUATING RISKS AND DEFENSES

With the increase in multi-vector attacks, security experts agree that reducing the risk from DDoS attacks requires a defense-in-depth or layered approach utilizing multiple, synchronized mitigation approaches.

Firewalls have long stood as the first line of defense, as policy enforcement solutions designed to prevent unauthorized data access. Unfortunately, firewalls are not very effective when it comes to availability threats like the modern-day, multi-vector DDoS attack. Modern firewalls perform stateful packet inspection — maintaining records of all connections passing through the firewall. They determine whether a packet is the start of a new connection, part of an existing connection or invalid. But as stateful and inline devices, firewalls add to the attack surface and can be DDoS targets. They have no inherent capability to detect or stop DDoS attacks because attack vectors use open ports and protocols. As a result, firewalls are prone to become the first victims of DDoS as their capacity to track connections is exhausted. Because they are inline, they can also add network latency.

Finally, because they are stateful, they are susceptible to resource-exhausting attacks such as Transmission Control Protocol synchronous (TCP SYN) floods and spoofed Internet Control Message Protocol (ICMP) ping floods.

Intelligent DDoS Mitigation Solutions (IDMS) are purpose built for DDoS defense, they're stateless, deployed on-premise, in front of the firewall. These solutions can handle the majority of attacks, in fact, 80% of DDoS attacks are less than 1 Gbps in attack size. However, they are not adequate for the growing number of large-scale attacks intended to overwhelm internet bandwidth. These larger attacks are best mitigated in the cloud. Best practice defense today is intelligently integrated combination of on-premise and cloud-based solutions.

Recognizing that denial of availability is a business risk, it makes sense to undergo a risk analysis to assess your vulnerabilities, understand the impact of a DDoS attack under various scenarios, and determine the measures you need to have in place for optimal risk mitigation.

• • ○

Today's DDoS threat is not the same as it was ten or even five years ago. If availability is paramount to your business, then defenses need to be updated to match the threat.

NETSCOUT Guardians of the Connected World | Arbor

Corporate Headquarters
76 Blanchard Road, Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267 T +1 781 362 4300

North America Sales Toll Free +1 855 773 9200

Europe T +44 207 127 8147

Asia Pacific T +65 6664 3140

Latin & Central America T +52 55 4624 4842

www.arbornetworks.com

AI/AVAILABILITY/0318-LETTER