APPLICATION-LAYER DDoS ATTACKS: BAD THINGS COME IN SMALL PACKAGES

Distributed Denial of Service attacks come in many flavors. One of the more popular these days is the application-layer attack, sometimes called a Layer 7 attack because it targets the top layer of the OSI model, which supports application and end-user processes.

Unlike volumetric attacks, which overwhelm networks quickly by consuming high levels of bandwidth, application-layer attacks are more subtle and insidious – and much more difficult to detect and block. Posing as legitimate application users, attackers target specific resources and services, sending repeated application requests that gradually increase in volume and eventually exhaust the ability of the resource to respond. Widely regarded as the deadliest kind of DDoS attack, application-layer attacks can inflict significant damage with a much lower volume of traffic than a typical volumetric attack, making them difficult to detect and mitigate proactively with traditional flow-based monitoring solutions. While service providers can detect and block volumetric attacks as well as larger application-layer attacks, smaller application attacks can easily escape detection in the large ISP backbone, while still being large enough to cause a problem for the enterprise network or data center.

A GROWING THREAT

Application-layer attacks figure prominently in the DDoS threat landscape, according to NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report. Indeed, an estimated 88% of all DDoS attacks are smaller than two gigabits per second. Domain name system servers (DNS), the directories that route internet traffic to specific IP addresses, are the most common targets, cited by 81% of the report's respondents. HTTP and secure HTTPS services are also targeted frequently, rendering them unavailable to legitimate requests. In fact, many business-critical applications are built on top of HTTP or HTTPS, making them vulnerable to this form of attack even though they may not look like traditional public web-based applications. For a financial institution or online retailer that depends on its web presence to attract and serve customers, the impact can be catastrophic. Not only does the attack prevent the normal conduct of business, but it can also make a site invisible to search engines, or at least bump it from the front page of search results.

POTECTING APPS IS NOT ENOUGH

IT security teams are often under the mistaken impression that a web application firewall (WAF) provides adequate protection against application-layer attacks. Since applications are the targets, this seems logical on the surface. And WAFs are certainly necessary to filter or block attempts to gain access to servers or data. But they are vulnerable to state or resource exhaustion. The problem is that what starts as a trickle of legitimate-looking app service requests eventually turns into a flood, and application-level defenses won't recognize the flood of legitimate requests as an attack at all. Another problem is that the application-layer attack is often just part of a larger "blended" attack employing multiple attack methods, which may not be targeting the application layer that a WAF is analyzing.

For these reasons, a DDoS perspective is necessary to detect and thwart application-layer attacks. Without a dedicated DDoS solution, security teams may not even realize they are under attack when the site goes offline. They're left scrambling to restore service on the fly, diverting IT resources and eating up hours or even days that can translate into millions of dollars of lost business.

THE FIRST LINE OF DEFENSE

To effectively detect and mitigate this type of attack in real time, what's needed is an inline, always-on solution deployed on-premise as part of a best-practice, hybrid DDoS defense strategy combining cloud-based and on-premise mitigation. An intelligent on-premise system will have the visibility and capacity to quickly detect and mitigate these stealthy, low-bandwidth attacks on its own, early enough to avoid the need for cloud mitigation. Should the attack turn into a flood, the on-premise system can instantly activate cloud-based defenses through cloud signaling.

The best place to deploy application-layer DDoS detection and mitigation measures is at the traffic entry point at the edge of the enterprise data center or ISP infrastructure – ideally outside the firewall. Because of the small scale of these attacks, they are harder to detect and stop once they have worked their way into the data center or network. An edge-based DDoS protection system gives operators the ability to customize detection and mitigation for the specific applications running within the data center.

Some approaches to DDoS mitigation, such as cloud-based solutions, can have a false positive problem – blocking legitimate users while trying to block attacks. Having a dedicated, edge-based DDoS protection system allows you to tune the protections so that they won't block legitimate application traffic or have an impact on normal users, even during an attack.

Application-layer attacks contradict the perception of DDoS attacks as large-scale threats that overwhelm defenses and incapacitate networks through sheer brute force. Network guardians need to be on the lookout for these smaller but smarter threats that can work their way through the slightest openings. Fortunately, the on-premise component of a hybrid DDoS defense solution has the capability to mitigate the vast majority of application-layer attacks before they can do damage.

One final point, on-premise doesn't just mean the enterprise network itself. It's also about the migration to "the cloud", and the need to provide the same kind of on-premise protection for assets hosted in either public or private cloud environments, which have the same application layer vulnerability to DDoS that you have in the on-premise datacenter. Enterprises should make sure that as they move critical assets to the cloud, they are providing the same level of application protection there and not falling back to relying on WAF or other non-DDoS solutions for their DDoS protection there.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECA_004_EN-1801 08/2018