beazley

Industry Insights

Don't let hackers spoil the season

December 10, 2023

As the holiday season approaches yearly, so does a wave of distributed denial-of-service (DDoS) attacks. Savvy threat actors know that the winter holidays mean that many organizations have fewer resources available to monitor their networks, creating opportunities for attack. This is especially true on e-commerce websites where traffic volume is at an all-time high, leaving those monitoring this traffic struggling to distinguish between legitimate and suspicious traffic.

How can organizations protect themselves from an influx of cyberattacks during the holidays? The first step is to identify all applications exposed to the Internet and reduce this surface area if possible. Any applications that are externally visible but do not require outside communication should be brought fully inside of the network. In addition, direct Internet traffic to those applications that need external availability can be better protected with firewall configurations.

The next step is for organizations to examine their bandwidth (i.e. transit) and server capacities to identify how to detect and mitigate a large-scale, volumetric DDoS attack. Regarding transit capacity, hosting providers should provide ample redundant Internet connectivity to allow an organization to handle large volumes of traffic and maintain ease of access for users. Additional options for web applications include Content Distribution Networks (CDNs) and Domain Name Service (DNS) resolution services that add extra layers of content service and DNS query resolution.

A DDoS attack’s power comes from devouring resources; this can be combatted by ensuring that resources can quickly scale up or down at a moment’s notice. Consider solutions like extensive networking that supports larger volumes and utilizes load balancers to continually monitor and shift loads between resources to prevent a singular resource from overloading.

Lodestone also recommends that organizations become familiar with their own traffic to detect what is normal and what is abnormal.

Establishing this baseline can help differentiate malicious traffic from waves of legitimate traffic that may be incoming because of the holiday season. Here, rate limiting can be employed to ensure that only the amount of traffic that would not affect the availability of the application is permitted. More advanced protection techniques can go further by analyzing packets themselves to identify legitimate activity. However, organizations must understand in detail the characteristics of “good” traffic typically received by the application or resource to provide a baseline for comparison.

WAFs can be deployed to defend against attacks that attempt to exploit vulnerabilities in applications themselves to create illegitimate requests. These may include SQL injection, cross-site request forgery, or requests from “bad” IP addresses disguised as “good” traffic.

Source: Lodestone

beazley