Lodestone

DECEMBER 2022

STATE OF CYBER

monthly newsletter

DDOS DEFENSE: DON'T LET HACKERS SPOIL THE SEASON

As the holiday season approaches yearly, so too 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. Defending against cyberattacks such as DDoS is critical during this time of year, as downtime can result in especially significant consequences like lost customers, high recovery costs, or reputational damage.

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. When it comes to 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 being overloaded.

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 through. 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.

Web Application Firewalls (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" Internet Protocol (IP) addresses disguised as "good" traffic. WAFs provide additional support in understanding resource traffic patterns and creating highly customized protections for an organization's environment.

WARNING: NEW RAPPERBOT CAMPAIGN AIMS TO LAUNCH DDOS ATTACKS AT GAME SERVERS

Cybersecurity researchers have identified samples of malware that is being used to build a botnet capable of launching DDoS attacks against game servers. Known as RapperBot, this campaign is designed to brute force Secure Shell (SSH) servers used to accept password authentication. Fortinet has stated that this malware is designed to target appliances that run on the following architectures: ARM, MIPS, PowerPC, SH4, and SPARC.

KMSDBOT – MALWARE WITH DDOS AND MINING COMBO ATTACKS

A new piece of malware known as KmsdBot is targeting SSH connections that use weak login credentials with the goal of entering systems and launching DDoS attacks and crypto mining operations. This malware includes specific, targeted attacks as well as general Layer 4 and Layer 7 DDoS attacks. It sends TCP, UDP, HTTP POST, or GET requests with command and control (C2) commands to overwhelm a target's resources and hamper its ability to process and respond to requests.

CYBER ATTACKS DURING THE HOLIDAYS: WHY THE SPIKE?

Threat actors see the holiday season as the perfect opportunity to launch attacks – ransomware attacks increase by 30% during this time of year. Increased traffic and personnel out of the office can make networks more vulnerable to DDoS and ransomware attacks, and threat actors rely on urgency and lack of availability to make organizations feel increased pressure to pay ransoms. Organizations must ensure that systems and networks are well-defended, and that cybersecurity stays in mind during the winter holidays.

DDOS ATTACKS IN Q3 2022

Kaspersky examines common trends in DDoS attacks over the past quarter, including the significant rise in such attacks in comparison to Q2 of 2022. Organizations can use this information to remain abreast of what industries were most targeted, possible motivations, and which threat actor groups currently present the greatest threat.

Contact Us: 320 East Main St, Lewisville, TX 75057. Tel: 1-203-307-4984. www.lodestone.com