Guide

Top DDoS Attacks To Prepare For

DNS Water Torture attacks, SSL Floods, ransom DoS assaults and Layer 7 application attacks – DDoS and network-layer attacks are as diverse as they are sophisticated. Thanks to the growing array of online marketplaces, it is now possible for hackers to wreak havoc with little to no knowledge of networks and cyberattacks. Attack tools and services are easy to access, making the pool of possible assaults larger than ever.

Now more than ever, it's critical that your DDoS mitigation solution provides comprehensive protection from a broad array of DDoS assaults. Here are eight of the most common, and sophisticated, DDoS attacks your organization should be prepared to stop.

1 Burst Attacks

Burst Attacks and advanced persistent denial-of-service (APDoS) campaigns include short bursts of high-volume attacks at random intervals as well as attacks that can last weeks, involving multiple vectors aimed at all network layers simultaneously. These types of attacks tend to cause frequent disruptions to network performance and SLAs, preventing legitimate users from accessing services.

2 DNS Attacks

DNS Attacks are still highly attractive to attackers, as they require relatively few resources and can cause severe damage to the DNS critical infrastructure. Sophisticated attackers take advantage of DNS protocol weaknesses to generate more powerful attacks, including DNS Water Torture and DNS Recursive attacks. Mitigating these attacks requires tools that can learn and gain a deep knowledge of the DNS traffic behavior.

3 Dynamic Content and CDN-Based Attacks

Organizations often use Content Delivery Network (CDN) providers to support global site and application performance. The problem is that CDNs provide a particularly insidious cover for attacks, as organizations cannot block traffic coming from the CDN's IP addresses. Malicious

actors have made an art form out of spoofing IP addresses to not only obfuscate their identity but also masquerade as seemingly legitimate users based on geolocation or positive reputational information about the IP addresses they are able to compromise. Dynamic content attacks further exploit CDN-based protection by overloading origin servers with requests for noncached content that the CDN nodes simply pass along.

4 IoT Botnets

While robotic process automation and other good bots help accelerate productivity and business processes, such as data collection and decision-making, malicious bots can create a large-scale DDoS attack on your network and services. Organizations continue to rely on conventional security solutions to assess bot traffic. Today's sophisticated bad bots can mimic human behavior and bypass CAPTCHAs and other older technologies and heuristics.

5 Layer 7 (L7) Application Attacks

Application DoS attacks target resource exhaustion by using the well-known Hypertext Transfer Protocol (HTTP) as well as HTTPS, SMTP, FTP, VOIP and other application protocols that possess exploitable weaknesses, allowing for DoS attacks. Much like attacks targeting network resources, attacks targeting application resources come in a variety of flavors, including floods and "low and slow" attacks.

Download ***Layer 7 DDoS Attacks to Prepare for & Mitigation Capabilities*** to Learn More

Guide
radware
Layer 7 DDoS Attacks To Prepare for
& Mitigation Ca... to Stop Them

6 Ransom DDoS Attacks (RDoS)

Ransom DDoS Attacks are where perpetrators send an email threatening to attack an organization – rendering its business, operations or capability unavailable – unless a ransom is paid by the deadline. These attacks are growing annually and typically take the form of a volumetric DDoS attack. RDoS attacks are particularly insidious because they do not require the attacker to hack into the target's network or applications.

7 Reflection/Amplification Attacks

Reflection/Amplification Attacks take advantage of a disparity of request and response ratios in certain technical protocols. The attackers send packets to the reflector servers with a source IP address spoofed to their victim's IP, therefore indirectly overwhelming the victim with the response packets. At high rates, these responses have generated some of the largest volumetric DDoS attacks to date. A common example is a reflective DNS response attack.

8 SSL/TLS And Encrypted Attacks

Attackers use SSL protocols to mask and further complicate attack traffic in both network- and application-level threats. Many security solutions use a passive engine for SSL attack protection, meaning they cannot effectively differentiate encrypted attack traffic from encrypted legitimate traffic while only limiting the rate of request.

Download the ***SSL/TLS Cyberattacks eBook*** to Learn More

Stopping assaults like these requires DDoS mitigation that combines automated, machine-learning based detection and mitigation capabilities with comprehensive protection for any infrastructure: on premise, private cloud and public cloud.

Stopping assaults like these requires DDoS mitigation that combines automated, machine-learning based detection and mitigation capabilities with comprehensive protection for any infrastructure

Learn More

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for Phone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.