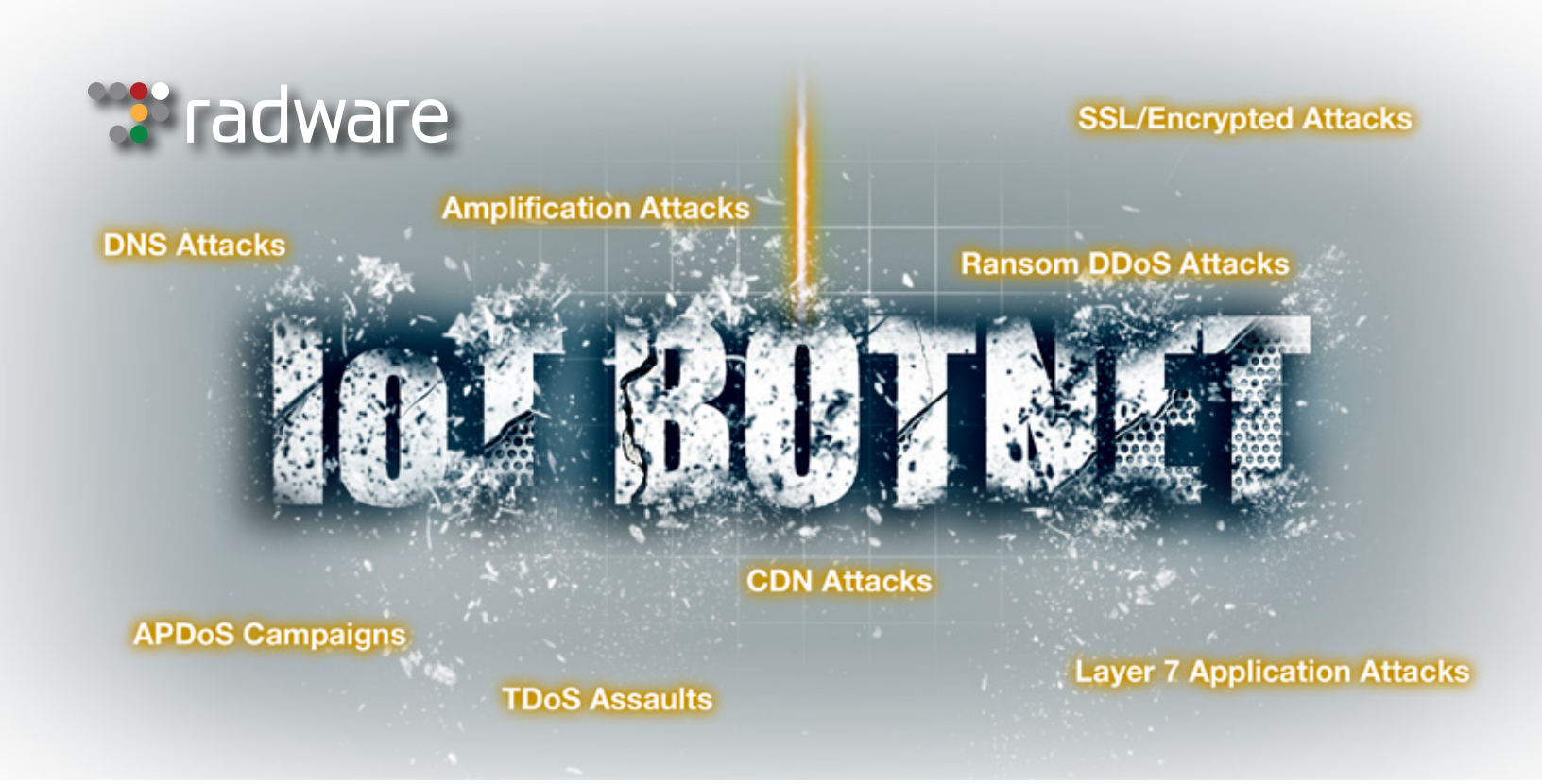

Top 9 DDoS Threats Your Organization Must Be Prepared For

New & Sophisticated DDoS Attacks Are Happening Daily. Are You Vulnerable?

DNS Water Torture attacks, SSL floods, ransom DoS assaults, Advanced Persistent DoS and application flood attacks – all are happening today. Is your organization prepared to detect and mitigate these threats? Is your organization a “botnet” killer?

Preparing for “common” DDoS attacks is no longer enough. Thanks to the growing array of online marketplaces, it is now possible for hackers to wreak havoc with virtually no knowledge of computer programming or networks. Attack tools and services are easy to access, making the pool of possible assaults larger than ever.

Leveraging burst attacks and Advanced Persistent DDoS campaigns, hackers launch multi-vector, blended campaigns that combine high volume network vectors with sophisticated application-layer attacks. In addition, recent IoT threats have spawned the largest DDoS attacks in history, propelling the market into the 1Tbps DDoS era.

Now more than ever, it’s critical that your DDoS mitigation solution protect your organization and customers from today and tomorrow's most sophisticated attacks.

Hackers Find New Attack Types and Threats to Breach Existing Mitigation Technologies

IoT Botnets have earned their "right" as one of the top threats for organizations given the dramatic increase in the use of IoT devices to create powerful botnets. Most notable is the Mirai botnet, used to carry out the largest DDoS attack in history in the fall of 2016. This botnet utilized 60+ factory default credentials found on BusyBox-based IoT devices and created the most powerful botnet seen to date. Mirai introduced new and sophisticated attack vectors including the Generic Routing Encapsulation (GRE) flood attack and DNS Water Torture attack. With additional botnets uncovered in 2017, including Hajime and BrickerBot, it is clear that the impact botnets will have in cyber security has just begun.

DNS Attacks: DNS is a critical infrastructure component for any organization. While organizations and service providers take security measurements to protect the DNS infrastructure, attackers are generating more sophisticated attacks, with increased impact on the service. Sophisticated attackers take advantage of the DNS protocol behavior 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.

Burst Attacks and Advanced Persistent Denial-of-Service (APDoS) campaigns include short bursts of high-volume attacks in random intervals and attacks that can last weeks, involving multiple vectors aimed at all network layers simultaneously. These type of attacks have a tendency to cause frequent disruptions in a network server's SLA and can prevent legitimate users from accessing services.

SSL/Encrypted Attacks: With 10% year-over-year growth[1], attackers are using SSL protocol to mask and further complicate attack traffic and malware detection 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 and can only limit the rate of request.

Layer 7 Application Attacks: With the incarnation of IoT botnets, Layer 7 attacks have leveled their prevalence to the one of network attacks (64% of organizations)[2]. These attacks come in two varieties: application DoS attacks that target resource exhaustion by using the well-known Hypertext Transfer Protocol (HTTP), as well as HTTPS, DNS, 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.

Ransom DDoS Attacks: In 2016, ransom was the primary attack motivation, accounting for 41% of all cyber-attacks that year.[3] Ransom denial-of-service (RDoS) attacks are one form of ransom-based attacks, 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 have increased yearly since 2010 and typically come in 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.

Reflection/Amplification Attacks: Reflection and amplification attacks take advantage of a disparity of request and response ratios in certain technical protocols. For instance, the attacker could use a router as an amplifier, taking advantage of the router's broadcast IP address feature to send messages to multiple IP addresses in which the source IP (return address) is spoofed to the target IP. At high rates, these responses have generated some of the largest volumetric DDoS attacks to date.

Telephony DoS (TDoS) Attacks involve launching high volume of calls against the target network, tying up the system from receiving legitimate calls. In recent years, these attacks have targeted various businesses and public entities, including the financial sector and other public emergency operations interests. In its *2016-2017 Global Application & Network Security Report*, Radware predicted that TDoS attacks would rise in sophistication and importance, catching many by surprise.

Dynamic Content and CDN-based Attacks: Organizations often use Content Delivery Network (CDN) providers to support global site and application performance. Trouble is, 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 to possibly masquerade as seemingly legitimate users based on geolocation or positive reputational information about IP addresses they are able to compromise. Dynamic content attacks further exploit CDN-based protection by overloading origin servers with requests for non-cached content that the CDN nodes passes along.

Without Cutting-Edge Technology, Companies Don't Stand a Chance

When choosing a DDoS protection solution, make sure it can protect from these threats. This requires a dynamic solution that can keep up with constant changes in attack types and provides full coverage from all forms of DDoS attacks.

Radware's new DefensePro product line is the **ultimate IoT-bot-killer platform**, the industry's most advanced, automated protection from fast moving threats including from recent IoT-based attacks such as Mirai. It is uniquely built to overcome both the complexity and scale of today's sophisticated IoT-based botnets by providing:

- New, first-in-class behavioral-based algorithms to protect from known and unknown DNS flood attacks in the most cost effective way and includes an innovative positive DNS security model to protect from DNS Water Torture attacks and more.
- New in-the-box, patented SSL attack mitigation that provides the lowest latency, most efficient SSL attack protection with the widest coverage from SSL-based DDoS attacks.
- New burst attack protection to provide detection and mitigation from one of today's top threats.

DefensePro is based on industry-leading technologies, including behavioral-based detection and real-time signature creation, that work together to provide a wide range of protections at high capacity. It has the ability to automatically mitigate unknown attacks and minimize impact on legitimate traffic.

Radware's new line of DefensePro provides the most advanced DDoS protection available in the market that is built future-proof to fight today and tomorrow's sophisticated, automated attacks.

1, 2, 3 2016-2017 Global Application & Network Security Report by Radware