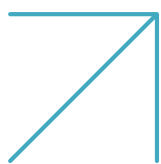# The Rise in Web DDoS Attacks and How To Stay Protected

Background: Evolution of the Latest Attack Campaigns

In 2026, we are witnessing an unprecedented surge in Web DDoS Tsunami attacks, driven by technological advancements and the widespread availability of AI tools. These tools, accessible to both cybercriminals and security professionals, enable the creation of highly sophisticated attack methods that can bypass common defenses.

AI-powered tools have revolutionized the cyber threat landscape by automating and enhancing the capabilities of attackers. These tools can generate complex, multi-vector attacks that are difficult to detect and mitigate. The use of machine learning and deep learning algorithms allows attackers to adapt their strategies in real-time, making traditional security measures less effective.

The tactics have evolved from high-volume network-based flood attacks to more complex multi-vector application-level attacks, making them harder to detect and mitigate.

Disruptive Web DDoS Tsunami Attacks

As seen in the recent attack campaigns, attackers are leveraging multiple types and vectors of attacks as part of one campaign, combining both network and application layer attack vectors and leveraging new tools to create sophisticated attacks that are harder, and sometimes impossible, to detect and mitigate with traditional methods.

Using these new attack tools, attackers generate new types of HTTPS Flood attacks— also referred to as Web DDoS Tsunami attacks—that are more sophisticated and aggressive. These unique attacks are higher in volume with very high requestspersecond (RPS). They are encrypted and appear as legitimate requests. They leverage sophisticated evasion techniques to bypass traditional app protections, such as randomizing HTTP methods, headers, and cookies, impersonating popular embedded third-party services, spoofing IPs, and other key targets. Among the application-level attack methods seen in these recent campaigns were HTTPS Get, Push and Post request attacks with changing parameters, behind proxies and dynamic IP attacks. All look like legitimate requests and API calls. In fact, most of the layer 7 DDoS attacks today are based on API-calls, which render the use of CAPTCHAs and other challenges futile.

HTTP/S Floods, and in particular Web DDoS Tsunami Attacks, are complex to mitigate. The attacks act at Layer 7 which means that most of the attack mitigation activities, and specifically inspecting the traffic, must be done after terminating the connection and inspecting the content. The attack mitigation processes that occur after the traffic are proxied and encrypted, and all are relatively heavy and expensive to maintain, especially at scale. This makes these attacks a very attractive technique for potential offenders to disrupt or impact online businesses and services.

Why Current Protections are Ineffective

The move towards encrypted attacks and the increase in the scale and sophistication of these attacks raises the bar needed for detection. These changes essentially render network-based DDoS mitigation tools, as well as traditional on-prem and cloud-based WAF solutions, ineffective against these attacks.

Network-based DDoS protection solutions are simply unequipped to detect and accurately mitigate application-layer DDoS attacks. Detecting and mitigating such attacks require decryption of the attack traffic and deeper inspection into the L7 headers. As such, these attacks would go undetected by network-based DDoS protection solutions.

A standard WAF—whether on-prem or cloud-based—is an effective tool to protect applications from standard web-based threats (mainly OWASP Top-10). That said, it is failing to protect against these L7 DDoS threats for the following reasons:

↗ **Scale:** The rate of some of these attacks, measured by Requests Per Second (RPS), is reaching new heights. Over the past year, several multi-million request per second (RPS) attacks were observed by multiple third parties and publicly disclosed. The rates and volume of traffic are multiple orders of magnitude above the capacity of the on-prem solution. In addition, if the on-prem WAF is actually an ADC with integrated WAF, then the task is even more complex. This is because the ADC will be maxed out by trying to terminate and decrypt millions of new requests per second, not to mention apply any security inspection. As a result, the WAF/ADC itself will be overwhelmed by the attack and ALL the services behind it will fail—not only the attacked URL/domain/application. In this case, adding more capacity to the WAF will not help the situation as the attackers can always gain more RPS power by various means available to them.

↗ **Attack Sophistication:** These Layer 7 DDoS attacks appear as legitimate traffic requests and are constantly randomized (dynamic IPs, and other parameters). As such, there is no pre-defined signature or a rule-based mechanism to provide based on a connection because the requests appear legitimate and do not contain any specific bad arguments. Therefore, only behavioral-based algorithms with self learning and auto-tuning can cope with detecting and mitigating such attacks.

↗ **Morphing Attacks:** The dynamic nature of these new threats—the frequency in which they change and randomize vectors, source IPs, and other parameters, and sustain these changes over a long period of time—is unprecedented. To protect against such attacks, organizations need solutions that can quickly adapt in real time to the attack campaign. A standard on-prem or cloud-based WAF is not able to provide that.

↗ **The Human Factor:** The sophistication of attack campaigns requires having security experts that can handle the complexity of the attacks and ensure the quality of protection is not compromised during an attack. Self-managed teams, limited in personnel, tools, and budgets cannot cope with a 24x7 attack campaign. Also, on-prem tools are mainly rule-based and require definition of new rules for mitigation. The time it takes to analyze the attack and deploy a rule means significant downtime—lasting from minutes to hours—in every iteration of the attack. All of this and the continuous morphing of the attack result in continuous downtime.

a Standard bot manager - whether standalone or incorporated into a WAF most bot managers also deem ineffective as they rely on serving challenges such as CAPTCHA to the end users which present three problems:

↗ **API-based attacks:** Most web DDoS attacks are actualy API based and cannot be served challanges.

↗ **Challenge Bypass:** even in the case of web requests based attacks, Challenges are not full proof anymore as many of the new bot scripts and DDoS attack tools can bypass those challenges

↗ **Bad User Experience:** Serving interactive challenges on such large scale can also end up blocking legitimate users as well as imapct their user experience

On top of this, additional traditional mitigation methods will not be successful in mitigating these attacks. Solutions that leverage rate-limiting techniques will not be able to accurately distinguish attack traffic from legitimate traffic and will block legitimate traffic. Similarly, blocking traffic based on the geographic location of its source (also known as geo-blocking) would be ineffective as the attacks leverage botnets that are globally distributed and often placed in the same country as the target itself.

What You Need to Stay Protected

Comprehensive 360-Degree Application Protection

To protect against these new campaigns, organizations need to opt for a comprehensive, adaptive application protection service—one that keeps them protected against threat vectors as the business grows and applications evolve, while eliminating management overhead and enabling the fastest time to protection. Radware's Cloud Application Protection Service provides a best-of-suite, one-stop shop for all your application protection needs. It combines best-of-breed WAF, bot management and Account Takeover (ATO) Protection, API protection, client-side protection, and Web DDoS protection in a single solution. Radware's Cloud Application Protection Service is backed by Radware's 24/7 Emergency Response Team (ERT) to provide fully managed, comprehensive protection when under attack.

Figure 1:

Radware
360-Degree
Cloud Application
Protection Service
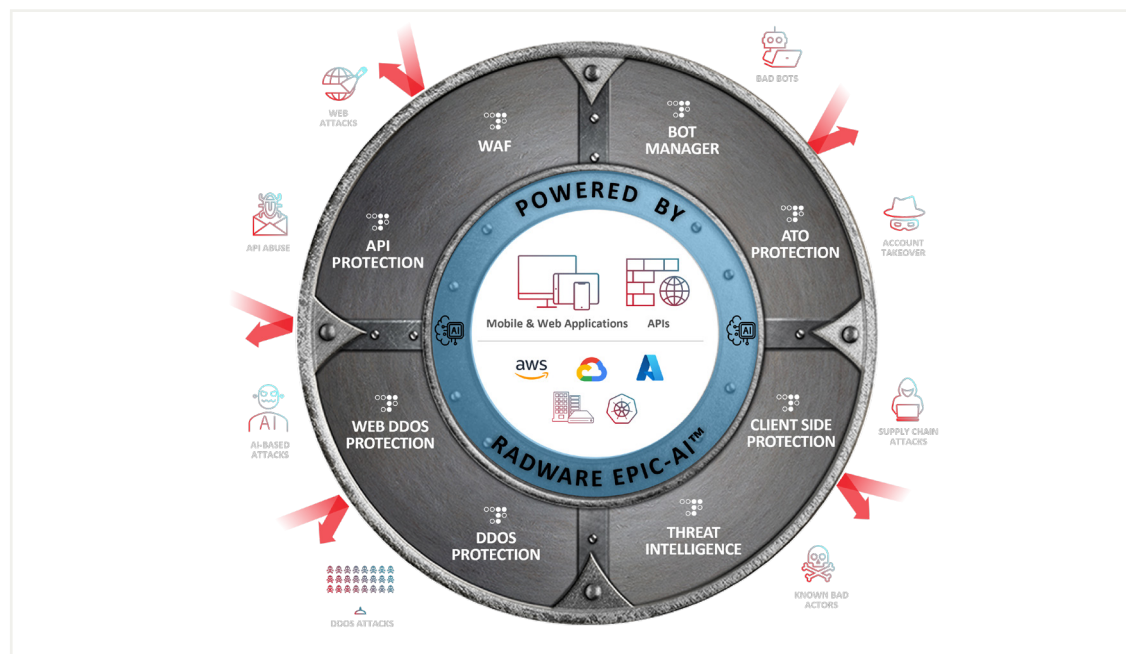
New Advanced Protection against Web DDoS Attacks

Radware's new Web DDoS Protection solution is uniquely designed to protect against high-scale, newly emerging Web DDoS Tsunami attacks and provide customers with advanced protection at the scale needed to combat these threats. The solution provides:

1. **Industry-First Encrypted Traffic Protection Without Decryption**

   Radware sets a new standard with the first cloud-based Web DDoS protection that accurately defends encrypted traffic without TLS certificate sharing: preserving privacy, ensuring compliance, and delivering high-accuracy protection at scale.

2. **Automated, Accurate Detection and Mitigation with Minimal False Positives**

   The solution leverages dedicated, behavioral-based algorithms with advanced learning capabilities designed to quickly detect and surgically block L7 DDoS attacks while minimizing false positives and not blocking legitimate traffic. In contrast to the common volumetric approach of most vendors, Radware's L7 behavioral-based protection can accurately distinguish between a legitimate surge in traffic (aka flash crowd) and a flood of attack traffic generated by adversaries and ensure that only malicious traffic is blocked—even during Web DDoS Tsunami attacks it does so by automatically generating granular signatures of the attack traffic in real-time and adapting them as the attack changes.

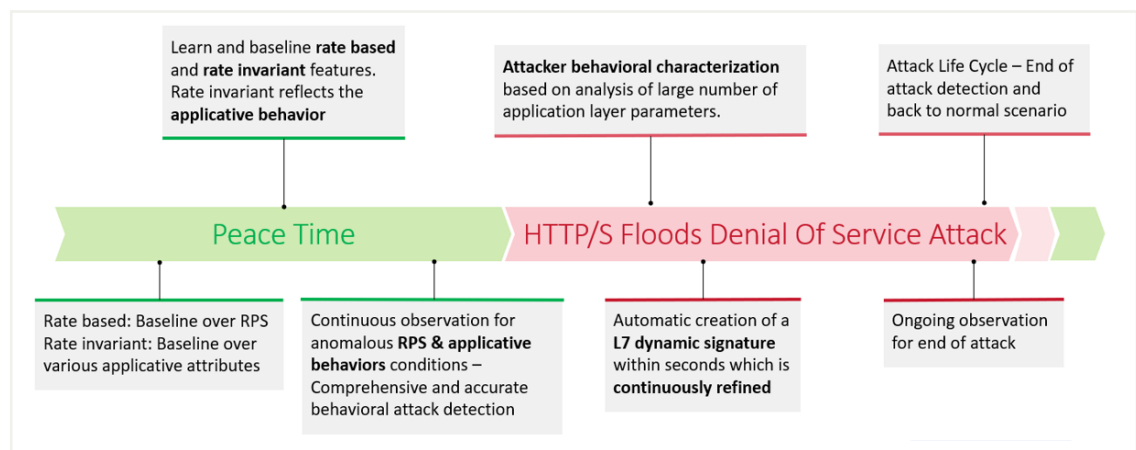3. **Widest Attack Coverage Protecting from the Most Advanced, Zero-Day Attacks**

   Unique algorithms provide protection from a wide range of L7 DDoS threats including smaller-scale, sophisticated attacks, new L7 attack tools and vectors, and large-scale, sophisticated Web DDoS Tsunami attacks including attacks on API-based applications. The solution analyzes the advanced threats as well as their numerous variants, and it adapts to any attack patterns, randomization methods, and attack techniques (using proxies, impersonating legitimate bots, etc).

4. **Best Protection for the High-Scale Web DDoS Tsunami Attacks**

   A combination of automated algorithms and high-scale infrastructure is needed to accurately protect against these high-RPS (requests per second) sophisticated L7 DDoS threats.

Figure 2:

Radware's Web DDoS Protection Attack Mitigation Lifecycle

Learn and baseline **rate based** and **rate invariant** features. Rate invariant reflects the **applicative behavior**

Attacker behavioral characterization based on analysis of large number of application layer parameters.

Attack Life Cycle – End of attack detection and back to normal scenario

Peace Time

HTTP/S Floods Denial Of Service Attack

Rate based: Baseline over RPS Rate invariant: Baseline over various applicative attributes

Continuous observation for anomalous **RPS & applicative behaviors** conditions – Comprehensive and accurate behavioral attack detection

Automatic creation of a **L7 dynamic signature** within seconds which is **continuously refined**

Ongoing observation for end of attack

Summary

Web DDoS attacks are increasing in scale and sophistication. As observed in the recent attack campaigns, attack tactics start with high-volume network-based flood attacks, and then evolve to more sophisticated multi-vector application-level attacks that are hard to detect and mitigate.

These new types of Web DDoS Tsunami Floods are harder to detect and mitigate, making them extremely attractive techniques for potential offenders who want to disrupt or impact online businesses and services. Traditional WAF, bot manager, or network-based DDoS protection solutions are incapable of mitigating these L7 DDoS threats.

To protect against these new campaigns, organizations need to opt for a comprehensive, adaptive cloud application protection service that keeps them protected against threat vectors as the business grows and applications evolve, while eliminating management overhead and enabling the fastest time to protection.

Radware's Web DDoS Protection solution is uniquely designed to block these attacks – leveraging dedicated, AI-powered behavioral-based algorithms to quickly detect and surgically block L7 DDoS attacks while not blocking legitimate traffic. Radware is the only vendor that can automatically generate new highly granular signatures in real-time for all type of attack traffic including API based DDoS attacks.

Radware expands its Web DDoS Protection with enhanced deployment flexibility and integration options, allowing customers to choose the approach that best fits their environment. Organizations can deploy cloud based protection with or without decryption through Radware's Cloud Security Platform, use on prem Web DDoS protection with Radware DefensePro, integrate protection into the application delivery layer with Alteon Protect, or secure modern containerized applications with industry first Web DDoS protection for Kubernetes through Radware's Kubernetes WAAP.

↗ **Comprehensive Protection:** A one-stop shop for application protection solutions: WAF, API protection, Client-side protection, ATO protection.

↗ **State-of-the-art Security:** The widest coverage against known threats and zero-day attacks based on advanced, patented, machine-learning-based behavioral analysis technology that is implemented on L3 through L7 threats.

↗ **Reduced Overhead:** Adaptive protection with automatic policy generation and 24x7 support through Radware's ERT.

↗ **Centralized Management and Reporting:** One place to manage and monitor the security of your applications, no matter where they are deployed.