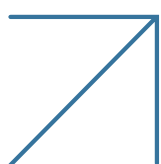


4 Signs You're in a Tsunami Attack



A Web DDoS Tsunami attack is an extreme form of HTTPS DDoS Flood designed to overwhelm and outmaneuver standard protection. Recognize the signs of attack so you can get the right kind of help—and avoid costly downtime.

1

High requests per second (RPS)

What to look out for:

Keep a watchful eye on your levels of RPS. Over the past year, the scale of these attacks has continued to reach new heights. Attacks have been observed at several million RPS, some with hours-long waves that go on for days.

Why it matters:

Any solution that is based on rate limiting, geo-blocking or other such mechanisms will not be able to accurately differentiate between legitimate and attack traffic at this scale and will end up blocking legitimate users.

2

Encrypted traffic

What to look out for:

Cybercriminals may increase your level of difficulty by adding encryption to the already daunting scale and sophistication of these attacks. Inspecting traffic becomes difficult and resource heavy as your defenses attempt to terminate and decrypt a staggering number of RPS.

Why it matters:

Post-encryption inspection and mitigation are heavy and expensive to maintain, especially at such high numbers.

3

Appears legitimate

What to look out for:

Once decryption is complete, these Layer 7 DDoS attacks appear to be legitimate HTTP/S requests and are constantly randomized (dynamic IPs and other parameters). No pre-defined signature or a rule-based mechanism can help because these “legitimate” requests do not contain any specific bad arguments.

Why it matters:

Only behavioral-based algorithms with self-learning and auto-tuning can cope with detecting and mitigating these attacks.

4

Randomizing attack techniques

What to look out for:

The dynamic nature of these new threats is unprecedented. They frequently change and randomize HTTP methods, headers, and cookies. They impersonate popular embedded third-party services, spoof IPs and more.

Why it matters:

To protect against these attacks, organizations need solutions that can quickly adapt in real time to the attack campaign. A standard on-prem or cloud-based WAF that is mostly based on pre-defined signatures will not be able to keep up with these randomized attacks.

Recognize these signs? Here's what to do:

Acknowledging a Web DDoS Tsunami attack is only the first step. Understanding that typical signature-based, network-layer protection won't help comes next. Radware's Cloud Web DDoS Protection solution is the only way to mitigate these attacks without affecting legitimate traffic.

Learn about [Radware's Cloud Web DDoS Protection](#).

Under attack right now?

Ask about Radware's emergency onboarding and mitigation services. [Get help](#).

