Data Sheet

FLASHBOX DDoS PROTECTION: Application-Layer Attacks

Protect and secure your business against DDoS attacks.

Definition of an Application-Layer DDoS Attack

A DDoS (distributed-denial-of-service) attack is one of the most significant and popular kinds of cybersecurity threats, aimed at preventing or significantly slowing access to your network. There are three main kinds: application-layer, volumetric or protocol attacks.

Application-layer attacks exploit a weakness in the Layer 7 protocol stack and target web application packets to disrupt the communication of data between hosts. Attack types include HTTP floods, GET/POST floods, SQL injections and low-and-slow attacks. Attack magnitude is measured in Requests per second (Rps).

The most sophisticated kinds of application-layer attacks are often highly effective and can prove difficult to mitigate. Their requests appear to be legitimate, but the goal of these kinds of attack is to crash the web server and prevent legitimate traffic from reaching their target.

Application-layer attacks account for around 17% of all reported DDoS attacks. They are often used in combination with other kinds of attack vectors to compromise a single target, and can be highly effective.

What are Multi-Vector Approaches?

Increasing numbers of DDoS attacks use a multi-vector approach, combining different kinds of DDoS attack. This kind of approach is appealing to an attacker as it can lead to the most significant damage to an enterprise or organization. This tactic can increase the chances of success by either simultaneously targeting several different types of network resources, or using one attack vector as a smokescreen while another more powerful vector is deployed as the main weapon. According to Imperva Incapsula, 81% of attacks are multi-vector.

Common Application-Layer Attack Types

HTTP Flood
HTTP Floods are the most common type of application-layer attack. They use numerous infected machines to force a target to expend significant resources in order to respond to a flood of HTTP requests.

GET/POST Flood
An HTTP request can either be "GET" or "POST". The GET request is used to retrieve static content such as images. The POST request usually involves some kind of processing. HTTP Floods can focus on one kind of request. POST flood attacks tend to more easily exhaust server resources.

Low-and-Slow Attack
This type of attack aims at denial-of-service through deploying extremely slow HTTP or TCP traffic to target application and/or server resources. Low-and-slow attacks are notoriously challenging to detect.

"The application layer is the hardest to defend. The vulnerabilities encountered here often rely on complex user input scenarios that are hard to define with an intrusion detection signature. This layer is also the most accessible and the most exposed to the outside world." - Security Intelligence

Mitigating Application-Layer DDoS Attacks

Application-layer, or layer 7 attacks are often smaller than the other kinds of DDoS and can be unnoticed until it is too late. As application requests appear to be legitimate traffic from users, it is often only once services have become overburdened and unable to respond that this style of DDoS is detected.

Flashbox counters application-layer attacks by continuous monitoring of the traffic to your site, allowing us to detect and mitigate both large and small attacks that specifically target your application layer. We immediately troubleshoot visible security issues by, for instance, blocking known malicious bots, and challenging unknown or suspicious actors with JS Test and CAPTCHA or Cookie challenges.

Why Flashbox for your Comprehensive DDoS Protection?

With proactive monitoring, precise threat assessments and timely responses, Flashbox has only one mission: to keep your data safe and secure, 365/24/7. We offer four comprehensive deployment options:

CLOUD PROTECTION

We offer two kinds of cloud protection: DNS redirect and BGP redirect. Whether you are relocating, rightsizing, upgrading, or outsourcing – we can help. As leading infrastructure experts, our Flashbox team will engineer an agile and scalable custom data center and/or cloud solution that grows with your business.

ON PREMISES PROTECTION

The best on-premises DDoS protection solutions provide real-time, 365/24/7 threat detection and in-line mitigation. There is zero latency and all kinds of DDoS threat can be accurately diagnosed and removed.

HYBRID PROTECTION

We can help you secure the most comprehensive service, providing on-premises protection at the appliance level combined with cloud-based protection. Flashbox will help design a hybrid protection service that offers DDoS and web application protection at scale.

PROFESSIONAL PLANNING & MANAGEMENT SERVICES

This service is for customers who want Flashbox to manage their on-premises boxes, cloud-based protection solutions and/or their hybrid package. Our team has decades of security experience and will work with you to provide top-level security and professional services.

Key Benefits of Flashbox Protection

- Comprehensive DDoS Protection
- 365/24/7 Monitoring & Visibility
- Real-time Threat Detection
- Multivector Protection
- Timely Deployment
- Critical Expertise
- Fully Managed Services

FLASHBOX

NETWORKS

CORPORATE HEADQUARTERS

660 4th Street #621
San Francisco, CA 94107 USA

www.flashbox.net