BANFFCYBER
TECHNOLOGIES

# WebOrion$^{TM}$ Content Delivery Network (CDN) & DDoS Mitigation Service (DMS)

July 2017

WEBORION

**www.weborion.io**

# Introduction

This paper describes Distributed Denial-of-Service (DDoS) attacks, and aims to enable partners and customers to understand the types of attacks that WebOrion$^{TM}$'s Content Delivery Network (CDN) and other services are able to mitigate, as well as how the architecture of the services enables the mitigations to be performed.

# DDoS Attacks

A denial-of-service attack (DoS attack) is a form of cyber-attack whereby the attacker seeks to make a machine or network resource (e.g. website) unavailable to intended users of the service. In the context of a website or web service, the attacker can use various techniques e.g.:

- Sending the target website so much traffic that the connection of the website's web server to the internet is completely saturated, such that it cannot communicate to the intended users normally.
- Sending web requests that put a lot of load on the target web server, such that the web server is loaded e.g. high CPU usage, high memory usage, etc. and cannot process requests from intended users normally.
- Sending a web request that exploits a bug in the web server's software such that the web server stops responding.

*Figure 1: In a DoS attack, an attacker tries attack a server to make the server unavailable*

In the case of a ***distributed*** denial-of-service attack (***D***DoS attack), the attacker uses multiple sources – for example a large group of compromised computers – to attack the target concurrently. Each source sends some traffic to the target, which combine to saturate the internet connection of the target and/or overwhelm the target server.

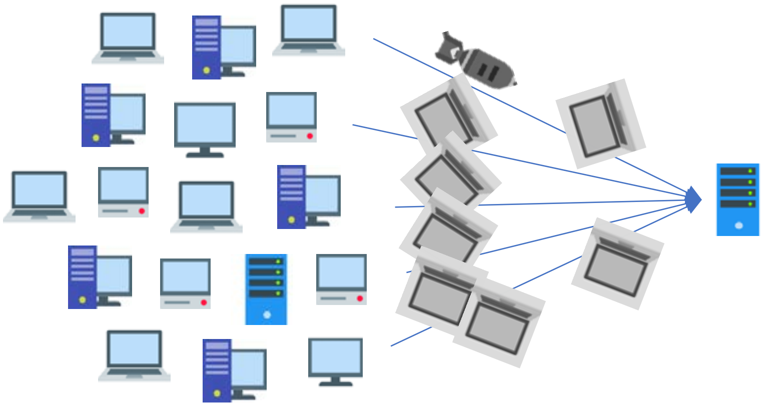

*Figure 2: In a DDoS attack, a large number of computers are used to attack a single target*

## Mitigation with WebOrion$^{TM}$ Business CDN Service

WebOrion$^{TM}$ offers a Content Distribution Network (CDN) service, which helps to improve the performance of websites by caching the contents of websites using the service at servers around the world, such that the website content is nearer to end-users.

While designed primarily for performance, the architecture of WebOrion$^{TM}$ CDN is also able to mitigate a wide range of DDoS attacks against web servers.

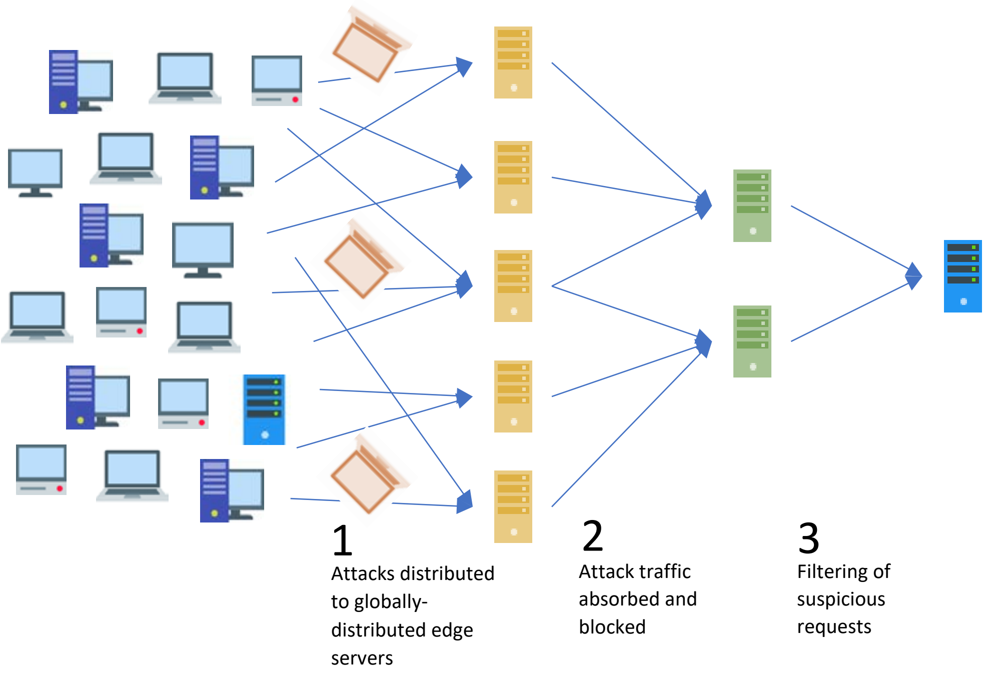
1
Attacks distributed to globally-distributed edge servers
2
Attack traffic absorbed and blocked
3
Filtering of suspicious requests

*Figure 3: Web server protected by WebOrion$^{TM}$ CDN*

The following table shows attacks that WebOrion$^{TM}$ CDN is able to mitigate and the techniques employed:

| **Attack Category** | **Attacks** | **Mitigation Technique** |
|---|---|---|
| Bandwidth/ Network Depletion Attacks | • TCP Flood (TCP SYN, SYN/ACK, ACK+PSH, RST, FIN Floods)<br>• UDP Flood<br>• All UDP-based reflection and amplification attacks e.g. DNS reflection/amplification attack, SNMP reflection/amplification attack, NTP reflection/amplification attack, etc.<br>• ICMP Flood (reflected or otherwise)<br>• IGMP Flood<br>• Connection Flood<br>• Brute Floods (packets of all sorts)<br>• Zero-Day DDoS Attack<br>• Any combination of the above flood attacks | Globally-distributed edge nodes with multiple-terabits of network capacity. Edge nodes are full HTTP proxies that drop all traffic except valid HTTP or HTTPS traffic. |

| | | |
|---|---|---|
| Invalid/oversized packets | • Ping-of-death<br>• Fraggle attack<br>• Smurf attack<br>• Nuke attack<br>• Teardrop attack<br>• TCP Flag abuse (e.g. Christmas tree packets)<br>• IP Fragmentation Attacks | |
| Slow-rate attacks | • Slowloris/PyLoris<br>• RUDY attacks | |
| Application-level flooding/resource depletion attacks | • SSL Connection Flood and Renegotiation Attack<br>• HTTP Connection Flood<br>• HTTP GET flood<br>• HTTP POST flood | |
| Application-level malformed data | • HTTP Malformed Request<br>• Apache Killer | Edge nodes are full HTTP proxies that pass only valid HTTP requests. |
| Application-level exploits | • Buffer Overflows<br>• Fork Bombs<br>• XML DoS and Bomb<br>• Hash Flooding DoS<br>• SQL Injection<br>• Cross Site Scripting (XSS)<br>• Cross Site Request Forgery (XSRF)<br>• Session Hijack | Web Application Firewall with rules to filter common attacks. |
| Application-level DNS attacks | • Reflected DNS<br>• DNS Query flood<br>• DNS UDP flood<br>• DNS TCP flood<br>• Malformed DNS Query<br>• DNS Protocol and Vulnerability Exploitation DoS/DDoS | Globally-distributed WebOrion$^{TM}$ DNS name servers handle DNS queries, instead of customer's name server. |

## Architecture

The architecture of WebOrion$^{TM}$ CDN Service, while designed primarily for acceleration of websites, is also well-positioned to mitigate a DDoS attack.

Built upon the networks of >10Tbps of public-cloud operators and other partners, WebOrion$^{TM}$ CDN has a globally distributed network of edge nodes with huge network capacities that cache content nearer to users. These edge nodes are positioned to absorb a large amount of traffic and filter any packets that are not valid HTTP (web) or HTTPS traffic.

Valid HTTP and HTTPS traffic are then processed by a smaller cluster of nodes that perform more in-depth filtering of the HTTP/HTTPS traffic based on the data in the packets before the requests hit a website's origin web server.

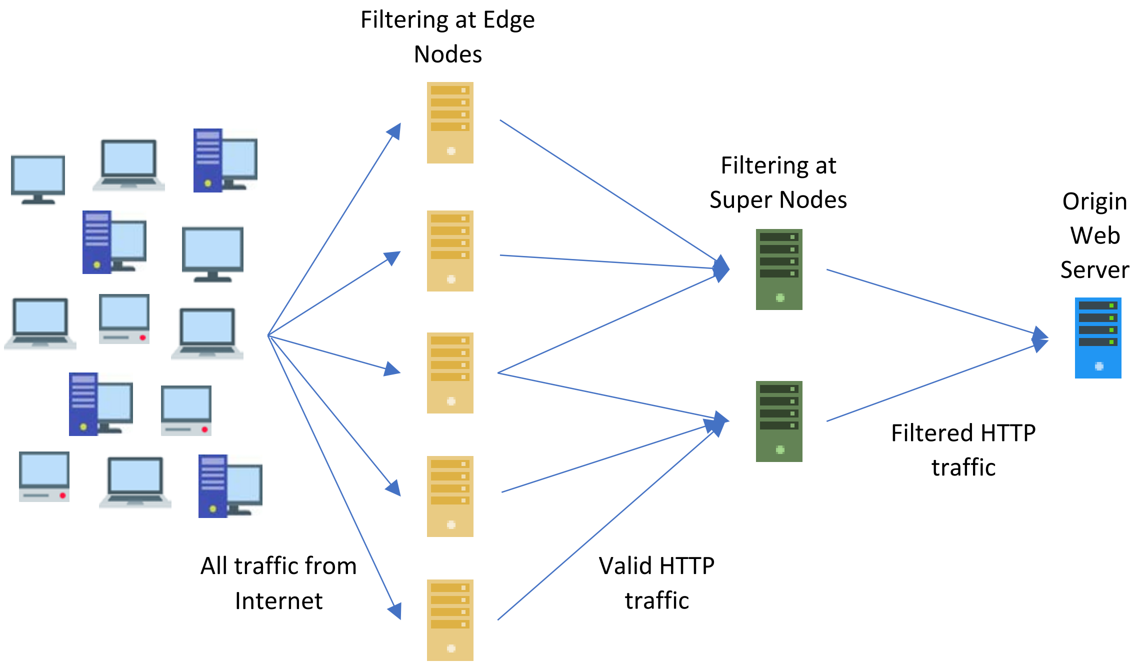

*Figure 4: Approximate architecture of WebOrion Business' CDN Service. Note that the number of nodes shown is not representative of the number of nodes used by the service*

## First Level Filtering: Edge Nodes

When a request is made for a website that uses the service, the packets first arrive at our edge nodes that perform the first stage of filtering and caching.

As WebOrion$^{TM}$ CDN is designed specifically for Website Acceleration, content that is marked as cacheable by the origin web server will be cached in the edge nodes.

Only TCP connections containing valid HTTP or HTTPS traffic is processed, all other packets (e.g. UDP, ICMP, IGMP, etc.) are dropped.

Furthermore, the edge servers are full HTTP-level proxies and as such, all IP packets are reassembled at the edge, and all TCP connections and terminated at the edge. Therefore, malformed IP or TCP packets are also dropped.

If there is a HTTP(S) flood, requests for the same resource (same URL) can be responded with the edge's cache if the content is cached.

In addition, the edge servers are also capable of performing IP blacklisting.

With multi-terabit network capacity globally distributed at the edge nodes, this stage has the capacity to mitigate most forms of network layer DDoS attacks.

By blocking most DDoS traffic at the edge, this design effectively limits the impact of a DDoS to the rest of WebOrion$^{TM}$ network and to the origin web server.

## Second Level Filtering: Super Nodes

After filtering by the edge nodes, HTTP and HTTPS traffic is sent to our "super nodes" that perform more in-depth analysis and filtering of the HTTP traffic.

The super nodes look at the traffic to detect suspicious web requests using a Web Application Firewall (WAF). Using rules that detect common attacks against web applications, WebOrion$^{TM}$ is able to block suspicious HTTP traffic.

## DNS DDoS Mitigation

Other than protecting the web server, DDoS attacks can also target the nameserver of a website. The nameserver is part of the domain name system (DNS) that matches the domain name that the user types into their web browser (e.g. www.example.com) to an IP address.

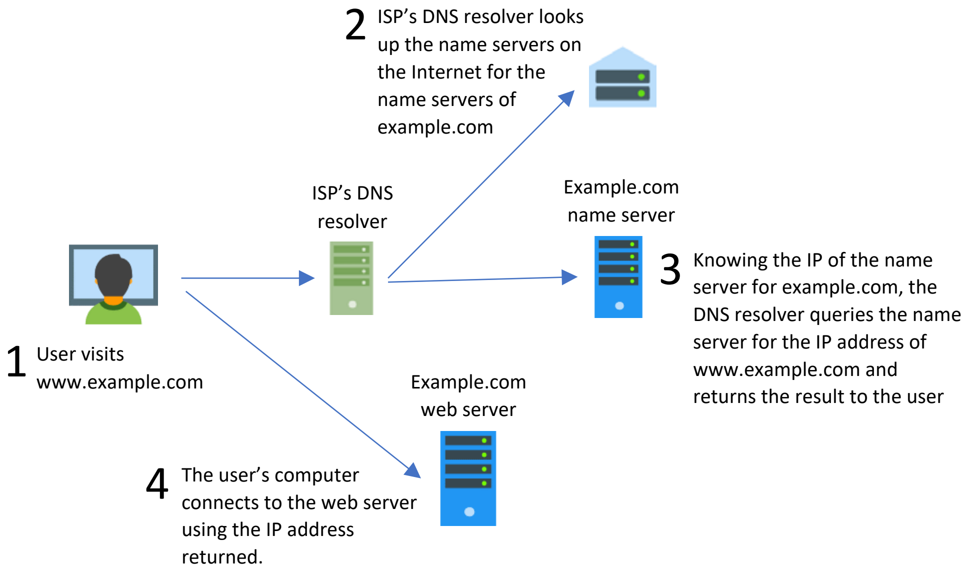
2 ISP's DNS resolver looks up the name servers on the Internet for the name servers of example.com
ISP's DNS resolver
Example.com name server
3 Knowing the IP of the name server for example.com, the DNS resolver queries the name server for the IP address of www.example.com and returns the result to the user
1 User visits www.example.com
Example.com web server
4 The user's computer connects to the web server using the IP address returned.

*Figure 5: Illustration of the workings of the Domain Name System (DNS)*

If an attacker attacks the nameservers of example.com, then a user wanting to visit the website will not be able to translate www.example.com to the IP address of the web server (step 3 in Figure 5 will fail). As a result, the website will be inaccessible to the intended users, even though the web server is still working.

To mitigate this, WebOrion$^{TM}$ also offers a nameserver service to customers on our **Bespoke** service plan. The service is designed to be highly available and scalable, comprising many globally-distributed servers. Anycast is also used to ensure that a request to the name server (using one IP address) actually reaches one of many servers, spreading out the effect of a DDoS attack and increasing availability of the system.

The customer simply needs to copy the existing records in their name server to the WebOrion$^{TM}$ nameserver service, and switch their domain name to point to the nameservers provided by WebOrion$^{TM}$.

## Other Best Practices

While WebOrion$^{TM}$ CDN is able to mitigate attacks against websites and web services, there are some best practices that customers should also try to follow to minimize the impact of a DDoS attack.

### Hiding the Origin

The DDoS mitigation capabilities of WebOrion$^{TM}$ CDN work only in the case where attacker traffic goes through WebOrion$^{TM}$ CDN instead of targeting the website's origin web servers directly.

Therefore, customers should try to prevent leaking the IP address of the origin. For example, some blogs may perform “pingbacks” that send a request to notify the target website of a link when a link is posted in a blog post. Or, some servers may send email directly from the server itself. These actions can leak the IP address of the origin, as outbound requests and email do not pass through the CDN infrastructure.

If possible, customers should try to change their IP addresses after on-boarding to WebOrion$^{TM}$, as there are services that archive DNS records, from which attackers may be able to discover the IP of the origin server before the DNS records are changed to use WebOrion$^{TM}$.

### Protecting the Origin

In the event that the attacker targets the origin IP address, the origin web server may be affected and unable to respond to requests that are forwarded by WebOrion$^{TM}$ CDN.

In such cases, WebOrion$^{TM}$ offers another service, the WebOrion$^{TM}$ Enterprise Restorer. The WebOrion$^{TM}$ Enterprise Restorer periodically crawls a website and keeps a copy of the public content, which can be used when the origin web server is unavailable.

Customer may also consider checking that incoming requests are from WebOrion$^{TM}$ CDN. Filtering the requests before further processing will allow the web servers to handle a lot more requests than otherwise, thus reducing the impact of an attack against the origin.

Customers may also look for solutions from their Internet Service Provider that block unauthorized requests further upstream of their internet connection, at the ISP level. As the ISP has bigger bandwidth than the customer, the ISP is usually able to handle larger volumes of traffic and block packets before they saturate the customer’s Internet connection.

As such, WebOrion$^{TM}$ CDN can work together with the ISP’s service since WebOrion$^{TM}$ CDN distributes traffic globally and provides caching and other services.

### Attack Service Reduction for Other Servers

Most websites and web services today have dependencies on other servers, for example, database servers, application servers, etc. In most cases, there is no need for these other servers to be exposed to the Internet. For example, in a typical two or three-tier web application, the web server communicates with the application and database servers, but these other servers do not directly connect to the Internet.

Not exposing these servers to the Internet prevents a DDoS attack on these servers.

## Conclusion

DDoS attacks are an increasingly common occurrence today, and organizations should take precautions against these attacks. Using WebOrion$^{TM}$ Content Delivery Network (CDN), along with other WebOrion$^{TM}$ services such the nameserver service and WebOrion$^{TM}$ Enterprise Restorer, will help to mitigate a wide variety of DDoS attacks against your website.