Defending Against Application-Based DDoS Attacks with the Barracuda Web Application Firewall

White Paper

Executive Summary

In the past, DDoS attacks were largely volume-based with the intent to overwhelm the network using bogus UDP, TCP SYN, or ICMP traffic. Various vendors offered solutions against them including edge appliances and service providers such as ISPs, cloud, and CDN scrubbing platforms. However, today's attack platforms have evolved to include application-layer DDoS attacks that target web and domain name servers. According to Stratecast, application-specific DDoS attacks are increasing by triple digits annually,[1] and Gartner estimates that application-layer attacks will constitute 25% of all DDoS attacks in 2013.[2]

This is trending because organizations are ill-prepared to fight application DDoS. Many seek solutions from their existing edge firewalls, which have limited application-layer visibility. Further, from the attacker's perspective, application DDoS attacks require significantly fewer resources and can be stealthier. They can quietly render application services inaccessible while the network infrastructure may still be responsive.

Application-layer traffic visibility and control are key elements of a layered defense strategy to effectively combat multi-pronged DDoS attacks. Network-layer solutions that evolved with volumetric attacks are blind to the application-layer attacks. They do not have deep insight into application protocols. Nor do they terminate and actively seize control of the application sessions and sanitize them. The Barracuda Web Application Firewall provides an on-premise and virtualized application-layer solution that combines real-time situational insight and historical intelligence to mitigate application DDoS.

Botnets and Application-Layer DDoS

Botnets are networks of malware-infected machines that are commandeered by servers known as Command and Control (C&C) servers. Previously, mostly PCs were infected, however mobile devices and cloud-based machines are being increasingly targeted as well. Once a machine is infected by the malware, the victim becomes part of the botnet. Sophisticated botnet malware, such as Mebroot, takes complete control of the machine by replacing the Master Boot Record (MBR), which allows it to load before the OS and avoid detection by Antivirus tools.

Communication with the C&C servers is done over covert channels using proprietary encryption, but using common ports to traverse firewalls. The C&C servers employ evasion techniques such as domain fast flux and P2P hosting to cover their trails.

Criminals who operate botnets – known as botmasters – issue commands to the botnet via the C&C servers to carry out their nefarious tasks such as spam campaigns, DDoS attacks, click frauds, or harvesting personal information like bank credentials or credit card numbers. Lately, botnets are being commonly used for Advanced Persistent Threats and cyber warfare as evidenced by the FLAME, DUQU, and other malware attacks.

There is a flourishing underground market for either renting or creating your own botnets. The following screenshot of the DIY Zeus botnet dashboard displays the geographical distribution of the infected machines:

[1]Entering the Next Phase of DDoS Defense, April, 2012 - Stratecast

[2]Arming Financial and E-Commerce Services Against Top 2013 Cyberthreats (G00237376) - Gartner

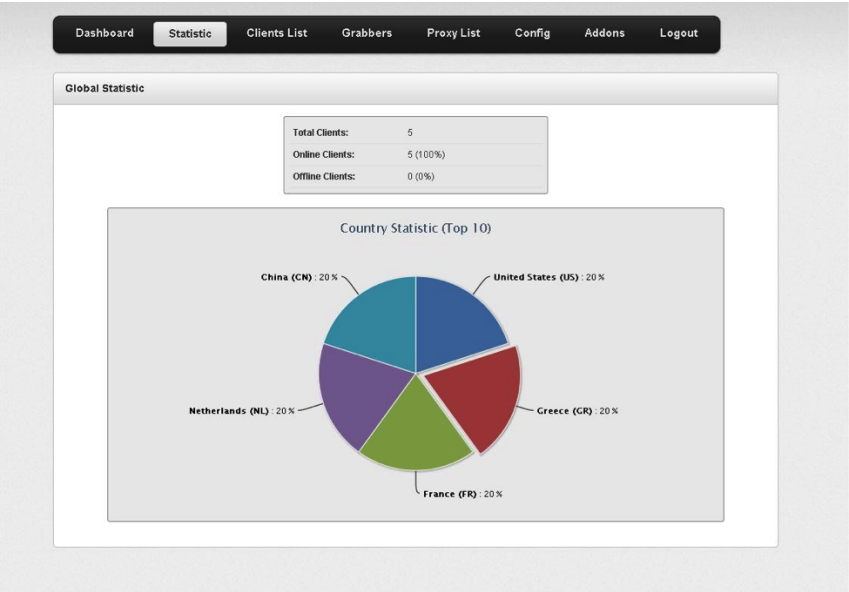


Figure 1: Screenshot of the Zeus botnet dashboard

Combating Application-Layer DDoS Attacks

Organizations have also been reluctant to adopt DDoS mitigation systems due to concerns over cost, effectiveness, and return on investment. The Barracuda Web Application Firewall is available as a hardware appliance or a virtualized application-layer solution. It combines real-time situational insights and historical intelligence to mitigate application DDoS. It can mitigate attacks based on application-centric thresholds, protocol checks, session integrity, active and passive client challenges, historical client reputation blacklists, geolocation, and anomalous idle-time detection. This is integrated into its hardened application firewalling platform, allowing for both functions in a consolidated offering with superior ROI and compliance benefits. Unlike service provider solutions that are priced by volume, mitigation is independent of attack volume and frequency, ensuring full-time protection with minimal costs.

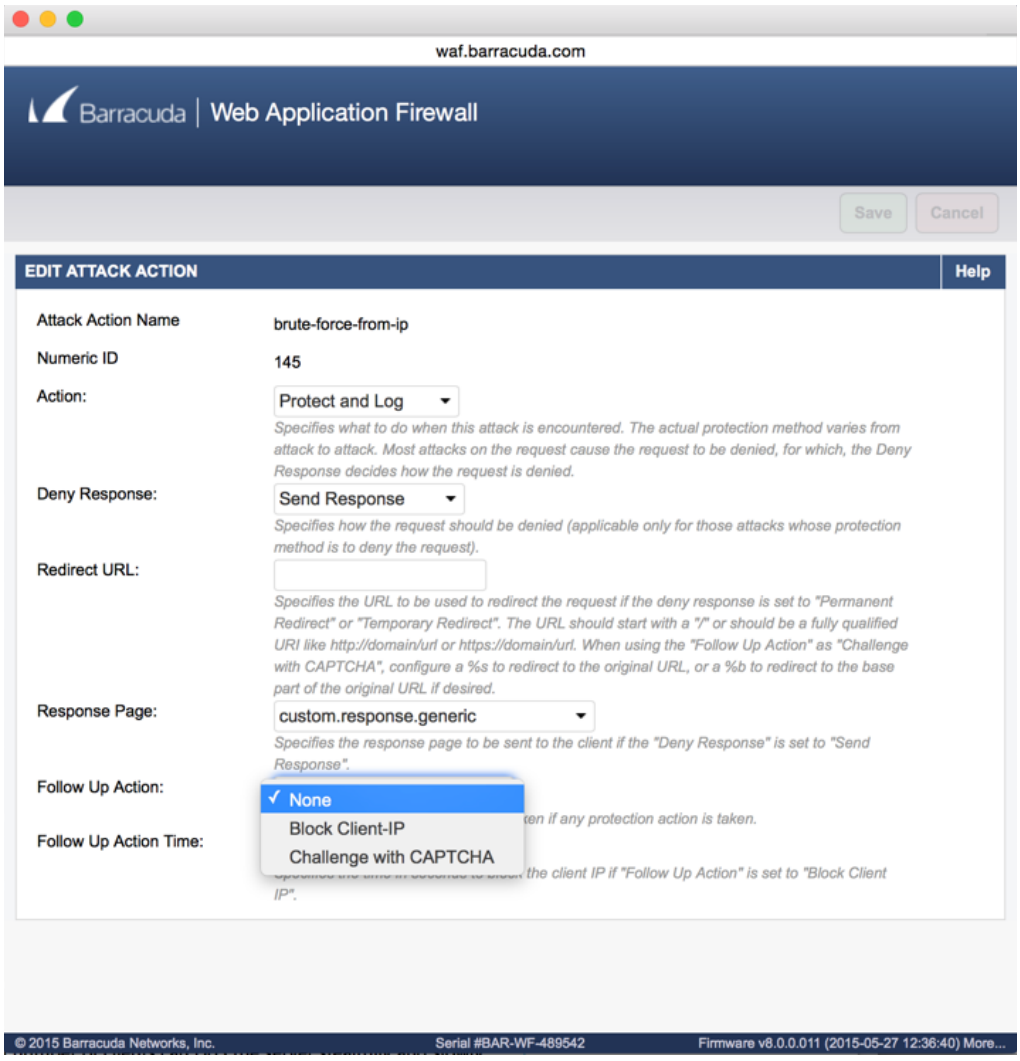
The Barracuda Web Application Firewall's Application-Based DDoS Protection
Protocol Anomaly Detection for HTTP
HTTP GET, POST Floods
HTTP "Slow Attacks" – Slowloris, R-U-Dead-Yet (RUDY), Slow Read Attack
LOIC, HOIC Protection
JS Challenges
CAPTCHA Challenges
Geolocation Controls
Filtering Anonymous Proxies
SSL Inspection Without Exporting Private Keys Off-Site
IP Reputation Feed
Building Excess Capacity
Session Rate Tracking
Automatic Signature and Firmware Updates
Vendor Agnostic SIEM Integration

Defending against HTTP GET and POST Floods

Applications often may have several resource-heavy pages or interfaces that invoke database, memory, or CPU-intensive operations, e.g., free text searches. Botnets frequently target such pages with a flood of requests to bring web applications down.

The first layer of protection here is to determine and enforce acceptable human browsing thresholds for a particular application. For example, users of a banking web application would click through a maximum of 10 pages per minute.[3] Moreover, human requests would contain valid client headers such as cookies and referrers.

The Brute Force Prevention Module of the Barracuda Web Application Firewall allows you to create and enforce such thresholds. Violating clients can either be blacklisted or challenged with a CAPTCHA to eliminate false positives.



It is possible for attackers to adapt their attacks by tuning the individual bots to stay below a certain threshold. However by reducing the number of requests per bot by a few orders of magnitude (i.e., from 1,000 to 10 request per minute), it will require attackers to increase the number of bots by a similar magnitude. This acts as a deterrent by greatly increasing the risk of discovery and the economic costs of launching a sustainable DDoS attack.

[3]For protection against the Anonymous group's Low Orbit Ion Cannon (LOIC) attacks, see Barracuda Web Application Firewall Defending Against Anonymous

Defending against HTTP "Slow Attacks"

Some attacks involve malicious clients that linger on with partial requests and responses, and indulge in minimum interaction to prevent server idle times from expiring. The attacks slow down applications by consuming system resources, leading eventually to an inability to handle server traffic. These are the "low and slow" attacks, as a relatively small number of clients can DoS the server stealthily and slowly, without consuming any significant bandwidth on the network. Such attacks are now common.

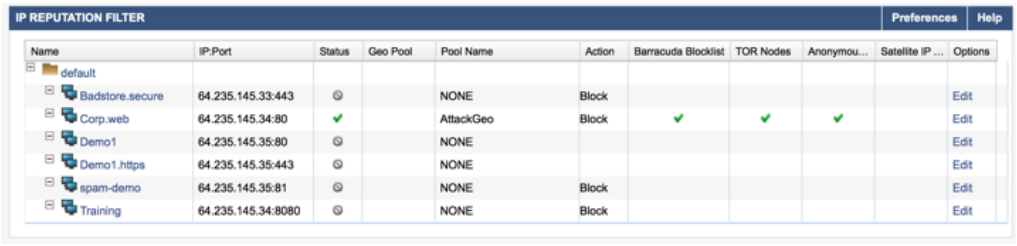
Slowloris is an example of a client initiating and sending HTTP headers repeatedly at regular intervals but never fully completing sending them. This keeps the server threads and network resources from being released, eventually leading to collapse. From a protocol compliance perspective, this is normal traffic that signature or blacklist-based devices cannot detect.

By virtue of its proxy architecture, protocol, and application awareness, the Barracuda Web Application Firewall can detect and block such anomalous traffic. It uses an adaptive algorithm that monitors incremental and aggregate communication thresholds to aggressively age and close malicious connections to prevent them from consuming system resources.

Filtering Botnet Traffic Based on Client-side Integrity Checks

The vast majority of web application traffic on Internet-facing websites is accessed by human browsers, with the exclusion of search engine indexers like Google and Yahoo. Most of the web traffic originates from humans using a common browser platform like Internet Explorer, Firefox, Chrome, or Safari. Traffic originating from bots often consists of automated scripts that do not have the rich browsing capabilities of clients using a browser. Consequently, it is possible to distinguish human traffic from bot traffic using a few heuristic algorithms.

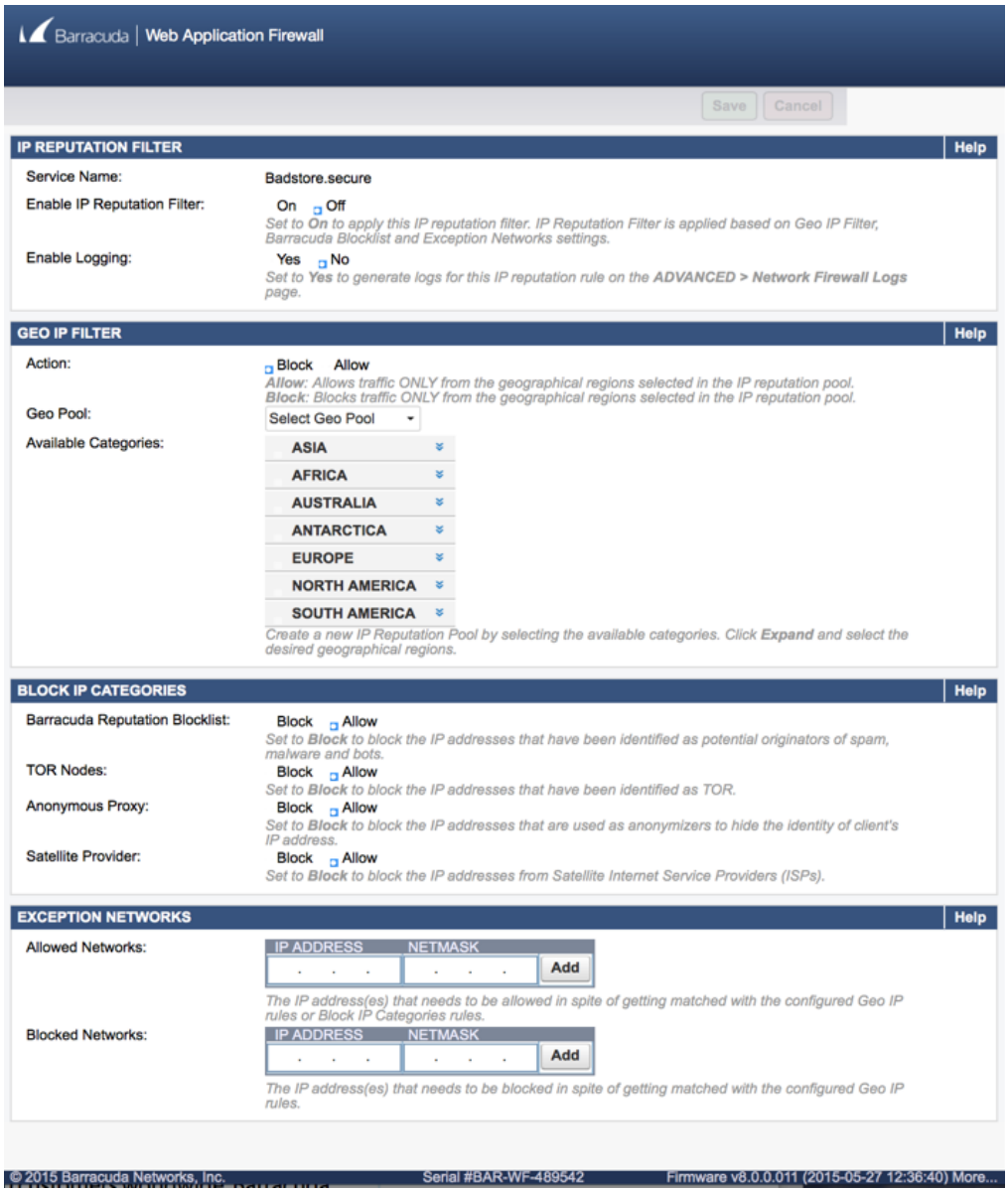
The Barracuda Web Application Firewall provides two mechanisms to detect and filter such traffic sources. First, it detects suspicious clients by injecting client-side controls to evaluate the web browser and application session. This is a passive challenge-response mechanism that is non-obtrusive to human-generated traffic, but can detect and block bot-generated traffic. The second mechanism is to issue active challenges – CAPTCHA images for verifying human clients. This can be done without any modification of the backend web applications.



Since CAPTCHA challenges can be considered obtrusive, organizations can utilize both passive and active detection algorithms to only use CAPTCHAs for suspicious clients after administering the passive client tests.

Mitigation Using Geo-location Controls

Botnets are widely distributed globally with a bias for regions with high computer and broadband penetration. The Barracuda Web Application Firewall has a built-in GeoIP module that can map the attacking IP address to its geographic location. During an attack, this allows traffic originating from outside a company's core geography and markets to be blocked.



Depending on the botnet global footprint, about 30-70% of the attack traffic can be eliminated just by using geolocation ACLs. Not only does this allow you to continue serving genuine clients, it also frees up compute and network capacity.

Filtering Botnet Traffic Using Client IP Reputation Feed

Botnets have evolved to become extensible, generic frameworks that can be used for banking Trojans, spam, DDoS attacks, click fraud, APTs, etc. Because Barracuda Networks provides security solutions that span email, web, network, and web applications to more than 150,000 customers worldwide, Barracuda has an industry-leading reputation database that categorizes numerous threat vectors and malicious IPs. This infrastructure is known as the Barracuda Reputation Block List (BRBL) and is maintained by Barracuda Labs.

The Barracuda Web Application Firewall integrates with BRBL to provide protection from bots. During a sustained DDoS attack, this provides a great tool to detect and block botnet traffic that may be targeting your servers. Additionally, the Barracuda Web Application Firewall has the ability to block anonymous and open proxies and Satellite ISPs – commonly used by hackers for reconnaissance and carrying out Advanced Persistence Threats (APTs).

All of this infrastructure is automated and new definitions are automatically pushed to appliances in the field using Energize Updates (EU) so there is no need for administrator intervention.

Protecting Application Servers from Becoming Botnet Nodes

While it's important to protect against application DDoS, it is equally critical to ensure that your own application server and network resources do not become unwitting participants of a botnet or a C&C server. Herding application servers is very attractive to botmasters, as servers afford them significantly larger attack resources, as well as an excellent platform to further their botnet recruitment.

Application servers may have custom, legacy, or third party applications. Any zero-day vulnerability in these can lead to an attack and recruitment of your server and bandwidth for botnet activities. The Barracuda Web Application Firewall provides strong security against malware uploads, OS command injections, directory traversals, or any such reconnaissance or attacks that capture application servers.

Summary

The trend toward application-layer DDoS is likely to accelerate. Gartner research indicates that hackers now use DDoS attacks to distract security staff so that they can steal sensitive information or money from accounts. Verizon's Data Breach Investigations Report 2012 confirms such attacks to be "more frightening than other threats, whether real or imagined." Internet-connected devices, social-networking, and cloud computing have fueled new attack vectors as well. Botnets targeting mobile platforms are now common. The evolution of browser-as-a-platform and HTML5 will likely open new bot-herding avenues. Access to botnet kits and rentals is easier than ever.

As the value and criticality of organizations' websites increase, they cannot afford to become botnet targets or tolerate extended disruptions of their web-based services. Botnets can cause significant erosions in revenue, operations, brand, and consumer trust. Lack of an international mitigation strategy makes it harder to fight botnets. Fortunately, the Barracuda Web Application Firewall provides a robust solution against application-based DDoS attacks that neutralizes the negative effects of such an attack.

To learn more about the Barracuda Web Application Firewall, please visit http://www.barracuda.com/waf or call Barracuda Networks for a free 30-day evaluation at 1-408-342-5400 or 1-888-268-4772. For more information on our other security and productivity solutions, please visit http://www.barracuda.com/products.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com