Barracuda®

The Barracuda Web Application Firewall Versus Anonymous

Best Practices for Planning and Defending Against Attacks by Anonymous

White Paper

The security analysts at Barracuda Central have been continuously monitoring the recent state of distributed denial of service (DDoS) attacks launched by online criminals, hacktivists, and even nation states. This document profiles attacks that originate from hacktivists, including their preferred tools and attack methodology. It will then present best practices for defending against these attacks.

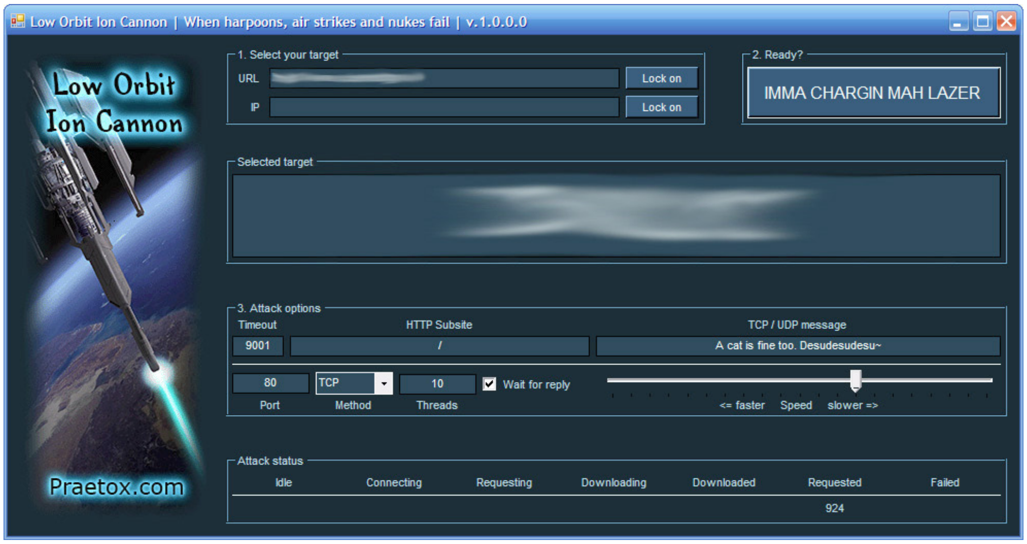
Introduction

Members of a loosely related ensemble of hacktivists call themselves Anonymous. Their preferred attack vectors are DDoS via the Low Orbital Ion Canon (LOIC) and SQL Injection attacks used for information extraction. They normally do not use traditional botnets for attacks. Details about Anonymous and their targets are well documented elsewhere so we will not go into those details here.

To counter these threats, the Barracuda Web Application Firewall provides a powerful proxy architecture WAF/ADC that can utilize its complete visibility into Layer 3 – 7 constructs to thwart such attacks.

LOIC

Anonymous uses LOIC as a tool to inflict DDoS attacks on victims' servers. The initiator of the attack recruits a large number of volunteers by various means (mainly through social networking) to participate in the attack. Volunteers either download the LOIC attack client or visit a web page, which has a JavaScript version of LOIC called JS-LOIC. The latter doesn't require installing anything on the client computer. The use of LOIC in both variants is becoming a preferred way of using nontechnical volunteers to magnify the intensity of attacks.



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

1. Select your target
URL [redacted]
IP

Selected target
[redacted]

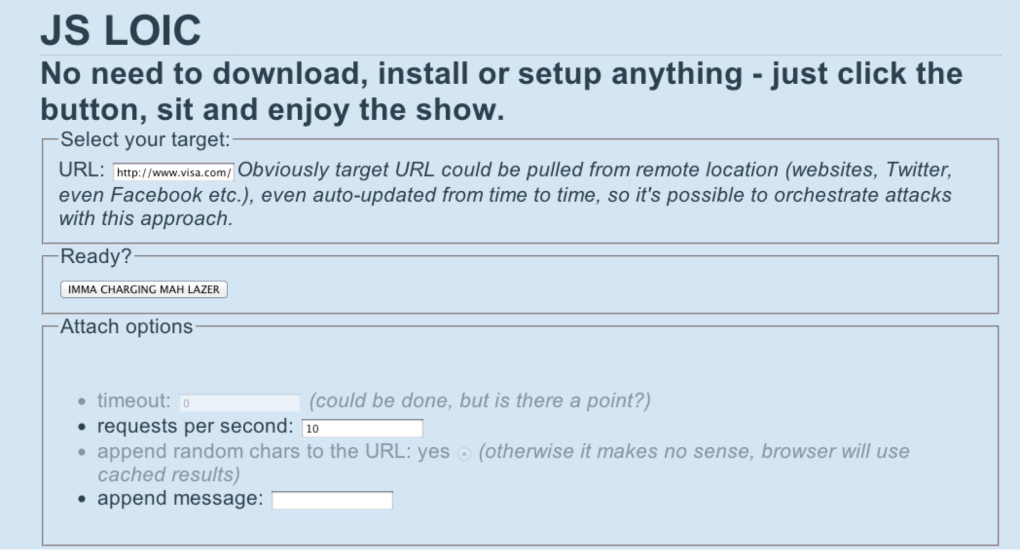
3. Attack options
Timeout: 9001
HTTP Subsite: /
TCP / UDP message: A cat is fine too. Desudesudesu~
Port: 80
Method: TCP
Threads: 10
☑ Wait for reply

Attack status
Requested: 924

Essentially, LOIC sends a continuous deluge of requests to the victim's server. These can be multiple HTTP, UDP packets, or TCP requests to the targeted servers.

JS LOIC

This is the JavaScript version of LOIC. To use it, a user has to simply visit the URL of a page that hosts the JavaScript version of the LOIC. Users are informed of the URL through social media channels. Once the user is on that URL, the JavaScript is automatically retrieved by the browser and executed. At the time of this writing, the JS version of the LOIC is limited to only carrying out HTTP attacks.



JS LOIC

No need to download, install or setup anything - just click the button, sit and enjoy the show.

Select your target:

URL: http://www.visa.com/ *Obviously target URL could be pulled from remote location (websites, Twitter, even Facebook etc.), even auto-updated from time to time, so it's possible to orchestrate attacks with this approach.*

Ready?

Attach options

- timeout: 0 *(could be done, but is there a point?)*
- requests per second: 10
- append random chars to the URL: yes ● *(otherwise it makes no sense, browser will use cached results)*
- append message:

This attack vector is potentially very dangerous since anyone with any sort of browser on any device such as a PC, laptop, Mac, smartphone, or tablet can become part of the attack.

Best Practices for Defending Against Anonymous Attacks

To protect against such attacks, the main goal is to distinguish genuine users of websites from the attackers. In order to provide needed "friend-or-foe" recognition, the Barracuda Web Application Firewall provides several layers of defense against such attacks, which are outlined below:

Step 1: Validate Protocol Basics

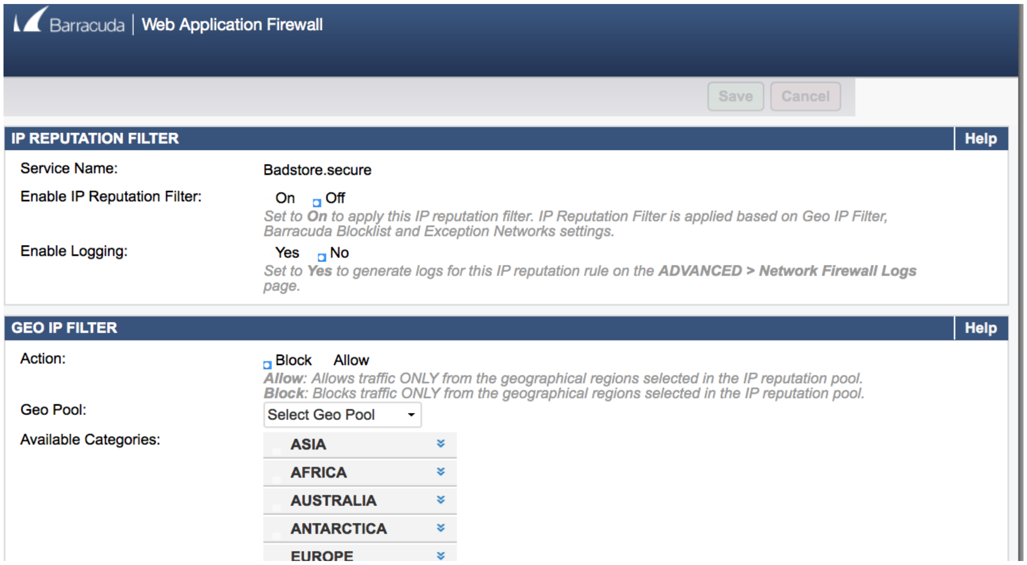
Standard browsers have implemented the HTTP protocol for a long time. They ensure that they follow the basics of the protocol. Additionally, many of the tools used during attacks do not go into enough detail of the HTTP protocol to get them right. The basic protocol validation engine of the Barracuda Web Application Firewall detects these discrepancies and uses them to stop the attacks even before they begin.

Step 2: Employ GeoIP Intelligence

In attacks by Anonymous, the participants are often located globally, regardless of whether the attack has regional or global significance. For example, the participants in the Visa/MasterCard attacks were distributed across the globe.

Since Anonymous directs their anger towards all state actors and large corporations irrespective of nationality, people from across the world join in. A simple and effective way to deflate such an attack is to block client traffic from regions that are not the core audience of your web application.

The Barracuda Web Application Firewall has a built-in GeoIP module that can map the attacking IP address to its geographic location. Around 30-70% of attack traffic can be blocked just by using GeoIP control.



IP REPUTATION FILTER | Help

Service Name:	Badstore.secure
Enable IP Reputation Filter:	○ On ● Off *Set to **On** to apply this IP reputation filter. IP Reputation Filter is applied based on Geo IP Filter, Barracuda Blocklist and Exception Networks settings.*
Enable Logging:	○ Yes ● No *Set to **Yes** to generate logs for this IP reputation rule on the **ADVANCED > Network Firewall Logs** page.*

GEO IP FILTER | Help

Action:	● Block ○ Allow ***Allow**: Allows traffic ONLY from the geographical regions selected in the IP reputation pool.* ***Block**: Blocks traffic ONLY from the geographical regions selected in the IP reputation pool.*
Geo Pool:	Select Geo Pool
Available Categories:	ASIA AFRICA AUSTRALIA ANTARCTICA EUROPE

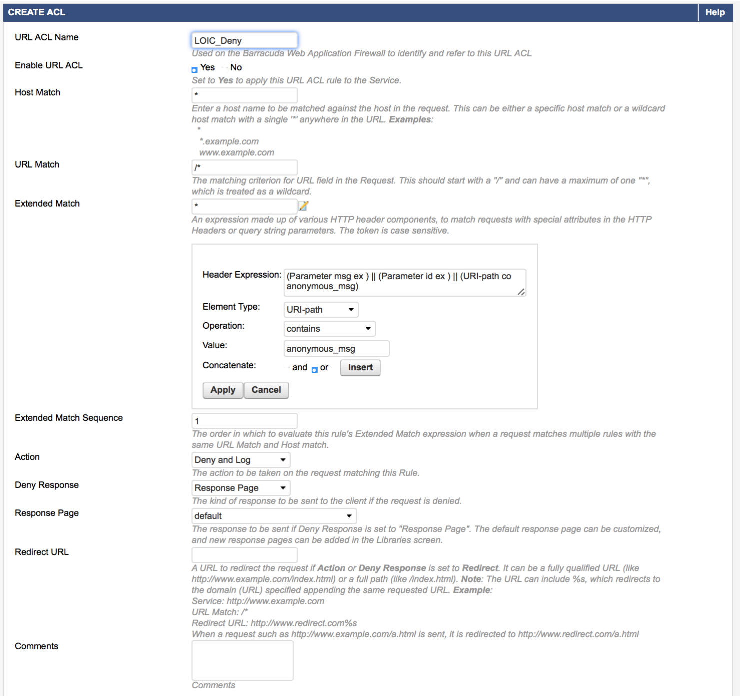
Step 3: Block Requests with Default LOIC Signatures

As the JS LOIC screenshots above show, the tool allows appending random characters and messages to the request. This is not just for sending a retributive message: It's required for technical reasons as well so browsers don't resort to the local cache when fetching the response. If that happens, the requests will never reach the victims.

The Barracuda Web Application Firewall's powerful extended matching engine greatly simplifies creating allow/deny ACLs for such signatures. Assuming the parameters appended by the LOIC tool are called "msg" and "id" and the message appended is "anonymous_msg," a DENY ACL with the following match is easily defined:

(Parameter msg ex) || (Parameter id ex) || (URI-path co anonymous_msg)

You don't have to remember the entire syntax. The extended match widget lets you define these signatures using a WYSIWYG UI widget:



CREATE ACL

URL ACL Name	LOIC_Deny *Used on the Barracuda Web Application Firewall to identify and refer to this URL ACL*
Enable URL ACL	● Yes ○ No *Set to **Yes** to apply this URL ACL rule to the Service.*
Host Match	* *Enter a host name to be matched against the host in the request. This can be either a specific host match or a wildcard host match with a single "*" anywhere in the URL. **Examples**:* * *.example.com www.example.com
URL Match	/* *The matching criterion for URL field in the Request. This should start with a "/" and can have a maximum of one "*", which is treated as a wildcard.*
Extended Match	* *An expression made up of various HTTP header components, to match requests with special attributes in the HTTP Headers or query string parameters. The token is case sensitive.* Header Expression: (Parameter msg ex) || (Parameter id ex) || (URI-path co anonymous_msg) Element Type: URI-path Operation: contains Value: anonymous_msg Concatenate: ○ and ● or
Extended Match Sequence	1 *The order in which to evaluate this rule's Extended Match expression when a request matches multiple rules with the same URL Match and Host match.*
Action	Deny and Log *The action to be taken on the request matching this Rule.*
Deny Response	Response Page *The kind of response to be sent to the client if the request is denied.*
Response Page	default *The response to be sent if Deny Response is set to "Response Page". The default response page can be customized, and new response pages can be added in the Libraries screen.*
Redirect URL	*A URL to redirect the request if **Action** or **Deny Response** is set to **Redirect**. It can be a fully qualified URL (like http://www.example.com/index.html) or a full path (like /index.html). **Note**: The URL can include %s, which redirects to the domain (URL) specified appending the same requested URL. **Example**:* *Service: http://www.example.com* *URL Match: /** *Redirect URL: http://www.redirect.com%s* *When a request such as http://www.example.com/a.html is sent, it is redirected to http://www.redirect.com/a.html*
Comments	*Comments*

This configuration protects against the use of default settings in the attack script, which may be aimed at your application. However, a resourceful attacker could change the parameters frequently to thwart such a basic detection and blocking mechanism. So, this rule set must be augmented by advanced rate-based controls.

Step 4: Identify and Block High-Rate Attackers with Malformed Requests

Your website might get hundreds of thousands of unique visitors a day. Unfortunately, a typical Anonymous attack generally originates from thousands of attackers. In the instance of the attacks that caused MegaUpload to shut down, an estimated 5,000 people (unique IP addresses) participated in the attack. Being able to identify these 5,000 IP addresses would ensure service availability to the rest of your visitors.

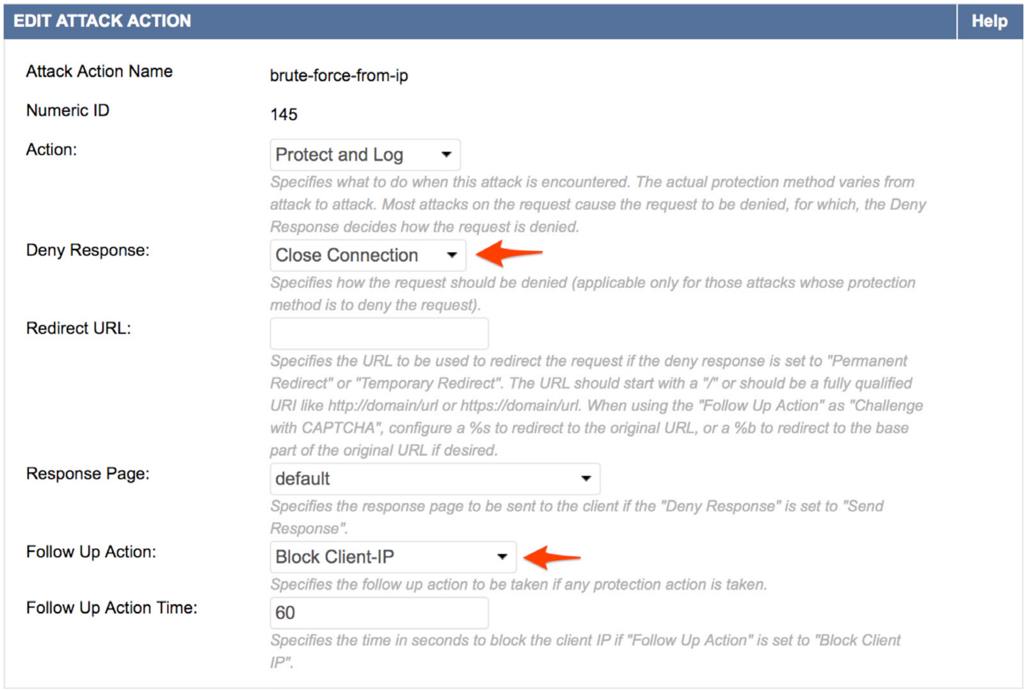
The Barracuda Web Application Firewall's Brute Force Prevention module can easily block and blacklist such IP addresses. The LOIC tool sends a deluge of requests without valid cookies and referrers. The following brute-force prevention rule catches and blocks such requests, and examines all incoming requests from a given client IP without valid cookies and a referrer header. If requests exceed a threshold of five within a 30 second interval, it blocks that IP for a configurable time span. During this time, any subsequent requests from the offending IP are denied at Layer 4.

URL MATCH	/*
Extended Match	(Header Cookie nex) || (Header Referer nex)
Sequence Number	1
Count Window	30
Max Allowed Accesses Per IP	5

Genuine clients are not affected since the very first request from a brand new client can come without a cookie or referrer; however, the subsequent ones would not.

Step 5: Lock Out Offenders

We want to ensure that identified offenders are blocked for a desired time interval. The Barracuda Web Application Firewall's Action Policy supports lockouts for every attack type.



EDIT ATTACK ACTION

Attack Action Name: brute-force-from-ip

Numeric ID: 145

Action: Protect and Log

Specifies what to do when this attack is encountered. The actual protection method varies from attack to attack. Most attacks on the request cause the request to be denied, for which, the Deny Response decides how the request is denied.

Deny Response: Close Connection

Specifies how the request should be denied (applicable only for those attacks whose protection method is to deny the request).

Redirect URL:

Specifies the URL to be used to redirect the request if the deny response is set to "Permanent Redirect" or "Temporary Redirect". The URL should start with a "/" or should be a fully qualified URI like http://domain/url or https://domain/url. When using the "Follow Up Action" as "Challenge with CAPTCHA", configure a %s to redirect to the original URL, or a %b to redirect to the base part of the original URL if desired.

Response Page: default

Specifies the response page to be sent to the client if the "Deny Response" is set to "Send Response".

Follow Up Action: Block Client-IP

Specifies the follow up action to be taken if any protection action is taken.

Follow Up Action Time: 60

Specifies the time in seconds to block the client IP if "Follow Up Action" is set to "Block Client IP".

Step 6: Secure Against TCP SYN and UDP/ICMP Flood Attacks

One option in the LOIC tools is a TCP SYN flooding attack. When thousands of attackers send a SYN flood, this can exhaust the victim's server's TCP buffers, which results in the inability to process new requests. To prevent these attacks, ensure that SYN Guard is turned on in the Barracuda Web Application Firewall.

Ideally, SYN Flood attacks should be blocked by the network perimeter firewalls before they reach your servers or application firewalls. However, the Barracuda Web Application Firewall has the ability to block such attack traffic in case the network firewall failed to block the initial intrusion. Additionally, the Barracuda Web Application Firewall comes with a full-featured network firewall that creates ACLs (Access Control Lists) to block any UDP/ICMP flood attacks that bypassed the network firewall.

Step 7: Work with YOUR ISP and Upstream Network

Note that if your incoming lines are completely burdened with packets floods – i.e. you have two T1 lines with a total capacity of 3 Mbps, but the attack traffic is 100 Mbps, then you will have to tackle the attack at your network edge or ISP level. Ensure that your ISP has an anti-DDoS solution in place and have the right contacts ready.

Other DDoS Mitigation Strategies

Anonymous attacks are typically short lived, but they can cripple a site if Anonymous is able to recruit a sufficient number of volunteers for a long duration. However, since the army of attackers is mostly voluntary opt-ins from people with desktop clients and mobile devices, the attacks are not sustainable.

However, an attack from a botnet can be significantly more challenging. They can last several days with a much larger captive infrastructure and attack motivation. The core proxy architecture of the Barracuda Web Application Firewall can help alleviate several application DDoS challenges that other solutions cannot.

Step 9: Block "Slow Client" Attacks

These are a new breed of "low and slow" application layer attacks that are very hard to detect and block because:

- They are protocol compliant so do not raise any red flags.
- They bring down the victim server resources stealthily without inundating the network.

For example, Slowloris and RUDY attacks send partial HTTP GET and POST requests to the server at a very slow rate, which keeps the connection alive, but it never fully completes the request. The servers keep resources allocated to these partial requests while waiting for the connections to complete. Envetually, the servers finally succumb to resource exhaustion.

The Barracuda Web Application Firewall, with its proxy architecture, buffers and monitors such requests using a sophisticated adaptive timeout algorithm to prevent the server exhaustion.

Step 10: Employ IP Reputation to Reject Malicious Traffic

In a botnet attack, the command and control (C&C) servers instruct the botnet zombies to attack a victim server. There are botnets specializing in spam, banking Trojans, DDoS, and other attacks. Barracuda Central continuously monitors botnets using thousands of sensors in the field, which leads to a state-of-the-art IP reputation database that blacklists botnet-infected IP addresses.

Apart from botnets, the Barracuda Web Application Firewall can also block anonymous and open proxies and satellite ISPs. These are commonly used by hackers for reconnaissance and carrying out Advanced Persistence Threats (APTs).

Step 11: Optimize Server Resources and Compute Capacity

Compute resources are under increasing pressure due to the proliferation of the Internet and the rise of mobile and cloud computing. When you deploy the Barracuda Web Application Firewall, you have a very beefy ADC front ending your server(s). This reduces the server load drastically, increasing their availability under attack. It offers several optimization features:

- TCP Multiplexing
- SSL Offloading
- Caching and Compression
- Intelligent Content Routing
- AAA (Authentication, Authorization and Access Control) Offloading

Together, these features can reduce the load on your server(s) by 50% or more.

Step 12: Plan for a Scalable Server Infrastructure

Often, an attack happens during peak traffic to gain additional visibility and leverage. You can deflate the DDoS to a large extent using the Barracuda Web Application Firewall. But, even residual traffic can bring your server infrastructure – including your application, web, and database – server to their knees. The Barracuda Web Application Firewall models 460 and above come with built-in intelligent load balancing and application content routing to distribute the load between your server farms. You can also designate backup compute resources to deal with unanticipated load.

SQL Injection

Anonymous hackers attempt reconnaissance of their targets by various SQL injection tools like sqlmap and Havij, as well as manual pentesting. The intent is to extract information from the backend databases and leak out PII (Personally identifiable information) or other sensitive information to embarrass or expose the targeted organization. The Barracuda Web Application Firewall blocks SQL injection using a mix of positive and negative security.

Negative security – The Barracuda Web Application Firewall employs highly tuned regular expression grammar-based signatures that detect SQL language, grammar, and syntax in input fields of the web application. For example:

http://www.mydomain.com/products/products.asp?productid=123 UNION

SELECT user-name, password FROM USERS

Looking for just "union" or "select" etc. to block this can generate false positives. However, the Barracuda Web Application Firewall employs contextual signatures like the following:

union.[^[:alnum:]]select.*[^[:alnum:]]from[^[:alnum:]]*

Other signatures like these completely ensure that SQL commands in any form or obfuscation are not let through, while false positives are completely minimized. The normalization module precedes these rule matches and reduces all obfuscations like UTF-8 content encoding, SQL comments etc. to a neutral form. New applications and modifications to existing apps are instantly protected – there is no "re-learning" period. Performance is fast and admin overhead very low.

Positive Security – In positive security, FORM and URL parameter values are restricted to a known whitelist. For example, a FORM entry representing "Age" is restricted to numerical values from 0-120 only; everything else is denied. Since this can become administrative overhead for large sites, the Barracuda Web Application Firewall can "learn" and auto-generate such application profiles from the request and response traffic using its Adaptive Profiling feature. It then enforces this profile and blocks any anomalies. This feature is also unique in the industry in that it provides complete security even while the profile is being learned.

Conclusion

Application layer DDoS attacks are growing in popularity. The record setting Mirai Botnet contained the code to perform Layer 7 DDoS in addition to the standard volumetric DDoS attacks. The Barracuda Web Application Firewall provides a strong defense against layer 5-7 DDoS using multiple techniques such as IP reputation, geo-awareness, application request throttling, application session tracking, brute force prevention, client fingerprinting, CAPTCHA challenges, and more. Our security analysts constantly evaluate the tools and techniques used by Anonymous and others against the Barracuda Web Application Firewall to ensure that all attacks are blocked and web applications are completely secured.

About Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. 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 configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network security and data protection. For additional information, please visit barracuda.com.

Barracuda Networks, Barracuda, and the Barracuda Networks logo are registered trademarks or trademarks of Barracuda Networks, Inc. in the U.S. and other countries.

US 1.2 Copyright 2015-2017 • 3175 S. Winchester Blvd., Campbell, CA 95008
408-342-5400/888-268-4772 (US & Canada) • 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