

# Cymon.io

## Open Threat Intelligence for Fighting Botnets

## » Largest tracker of security reports

- » Botnets
- » Malware
- » Phishing
- » And more



# About

» Almost 200 sources ingested daily

- » VirusTotal
- » Phishtank
- » Blacklists
- » Antivirus vendors



# Quick Stats

**esentire®**

4.6+  
Million

IP Addresses

26.2+  
Million

Security Events

# Web Interface - Events Timeline

Mar. 13, 2015



Malicious activity reported by eSentire AMP

🕒 7 months, 1 week ago

Feb. 22, 2015



C&C reported by AlienVault Reputation System

🕒 8 months ago



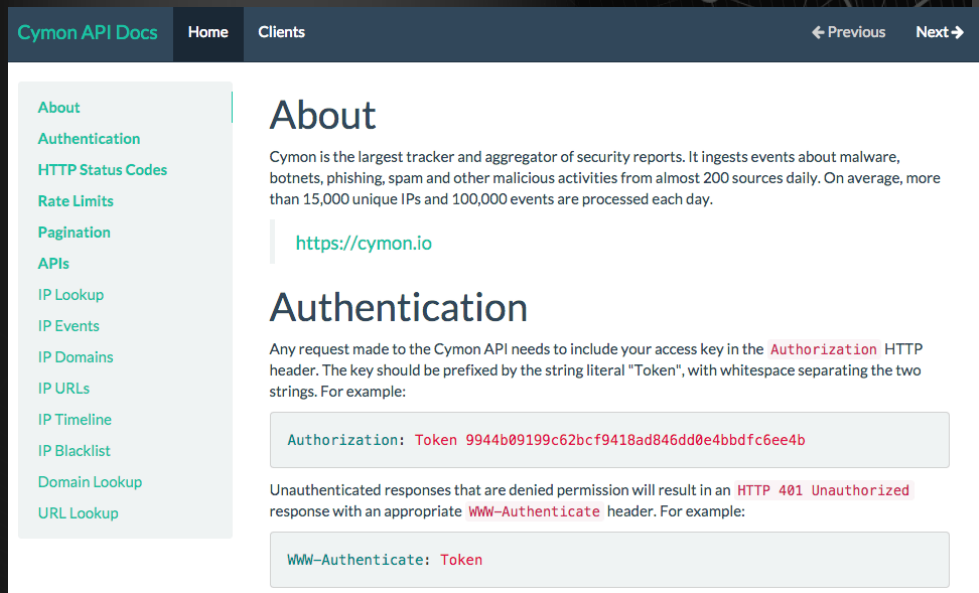
# IP Reputation Examples

- » <https://cymon.io/112.78.7.162>
- » <https://cymon.io/198.50.209.4>
- » <https://cymon.io/84.241.182.218>



# Open API

- » We currently offer free API access for testing
- » Contact me for details



The screenshot shows the 'Cymon API Docs' website. The header includes 'Cymon API Docs', 'Home', and 'Clients' links, along with 'Previous' and 'Next' navigation arrows. A left sidebar lists various API endpoints: About, Authentication, HTTP Status Codes, Rate Limits, Pagination, APIs, IP Lookup, IP Events, IP Domains, IP URLs, IP Timeline, IP Blacklist, Domain Lookup, and URL Lookup. The main content area is titled 'About' and describes Cymon as a security report tracker and aggregator. Below this is a link to 'https://cymon.io'. The next section is 'Authentication', which explains the required 'Authorization' header format. It provides an example: 'Authorization: Token 9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b'. It also notes that unauthenticated requests result in a '401 Unauthorized' response with a 'WWW-Authenticate' header, and provides an example: 'WWW-Authenticate: Token'.

Cymon API Docs Home Clients Previous Next

## About

Cymon is the largest tracker and aggregator of security reports. It ingests events about malware, botnets, phishing, spam and other malicious activities from almost 200 sources daily. On average, more than 15,000 unique IPs and 100,000 events are processed each day.

<https://cymon.io>

## Authentication

Any request made to the Cymon API needs to include your access key in the **Authorization** HTTP header. The key should be prefixed by the string literal "Token", with whitespace separating the two strings. For example:

```
Authorization: Token 9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b
```

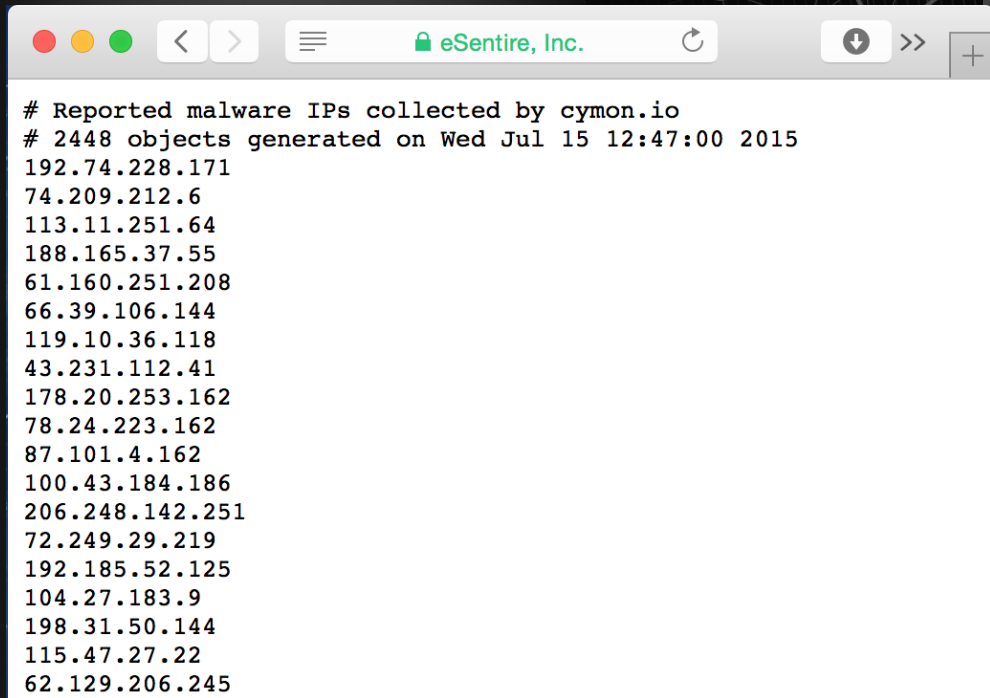
Unauthenticated responses that are denied permission will result in an **HTTP 401 Unauthorized** response with an appropriate **WWW-Authenticate** header. For example:

```
WWW-Authenticate: Token
```

<http://docs.cymon.io>

# Firewall RBL

## » Dynamic block list



A screenshot of a web browser window with the address bar showing "eSentire, Inc.". The main content area displays a list of IP addresses, preceded by two lines of comments. The list contains 18 IP addresses, each on a new line.

```
# Reported malware IPs collected by cymon.io
# 2448 objects generated on Wed Jul 15 12:47:00 2015
192.74.228.171
74.209.212.6
113.11.251.64
188.165.37.55
61.160.251.208
66.39.106.144
119.10.36.118
43.231.112.41
178.20.253.162
78.24.223.162
87.101.4.162
100.43.184.186
206.248.142.251
72.249.29.219
192.185.52.125
104.27.183.9
198.31.50.144
115.47.27.22
62.129.206.245
```




# DGA Analysis

- » Detect malware domains

Cymon

Cymon DGA Detection

Enter domain or URL to check if it was created using a Domain Generation Algorithm (DGA)

 myskmlsnvkrgr.com

Submit

<https://cymon.io/dga>

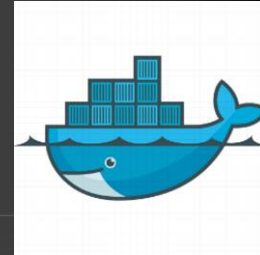
# Technology Stack

- » Django (Python)
- » Node.js
- » Docker
- » Amazon AWS
  - » RDS
  - » Redis
  - » DynamoDB
  - » Elasticsearch

esentire®

django

node

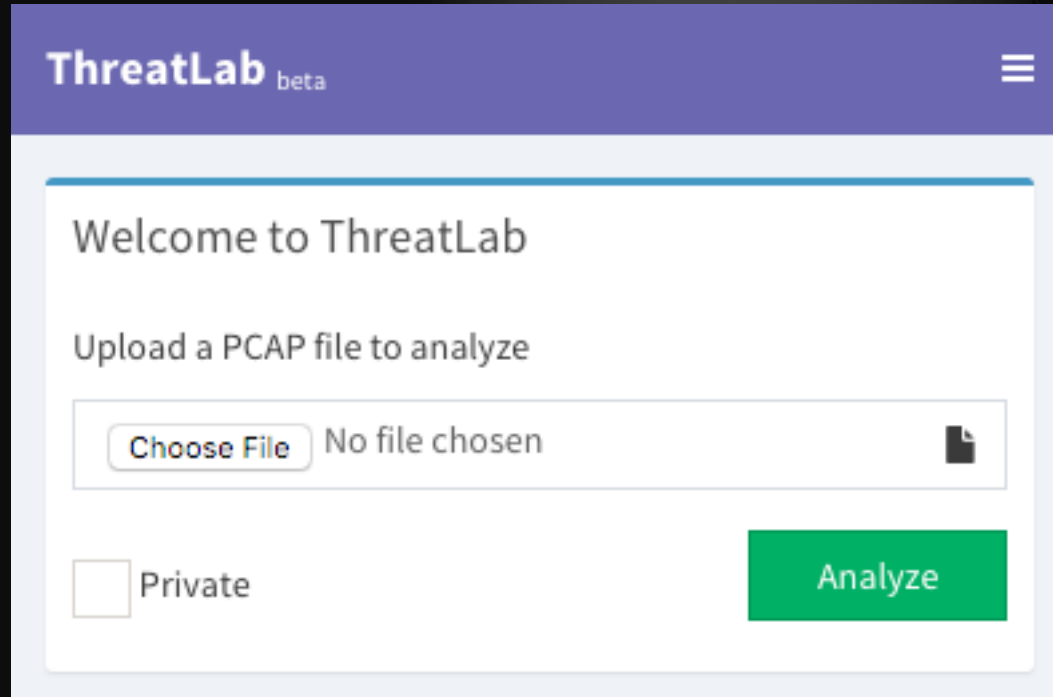


# Google Chrome Plugin



[github.com/eSentire/cymon-interceptor](https://github.com/eSentire/cymon-interceptor)

# Integration with Threat Lab



The screenshot shows the ThreatLab beta web interface. At the top is a purple header with the 'ThreatLab beta' logo and a hamburger menu icon. Below the header is a white content area. It starts with the text 'Welcome to ThreatLab', followed by 'Upload a PCAP file to analyze'. There is a file upload box containing a 'Choose File' button, the text 'No file chosen', and a file icon. Below the upload box is a checkbox labeled 'Private'. To the right of the checkbox is a large green 'Analyze' button.

[www.threatlab.io](http://www.threatlab.io)