Lotta ai Bot dannosi

Fernando Loureiro | Principal Sales Engineer, Fastly

Fernando Bitti Loureiro
Principal Sales Engineer
https://www.fastly.com/

Lotta ai Bot dannosi

Agenda

1. Chi è Fastly
2. Sintesi della soluzione Fastly Bot Management
3. Caso d'uso reale del cliente: JetBlue
4. Parte 1: Ingannando ai Bot dannosi
5. Parte 2: DDoS Protection con Attribute Unmasking
6. Domande e risposte

Chi è Fastly?

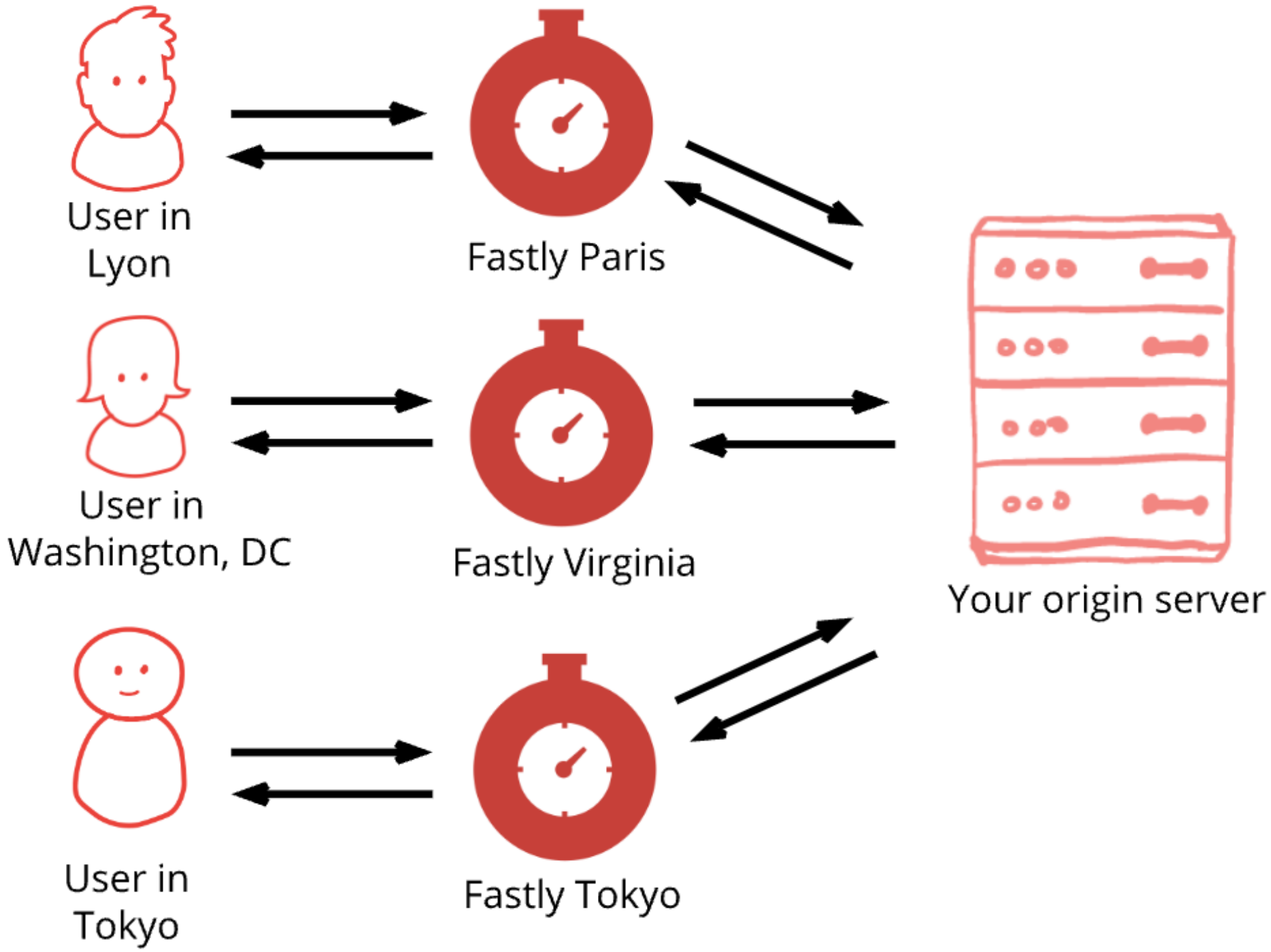
User in Lyon

User in Washington

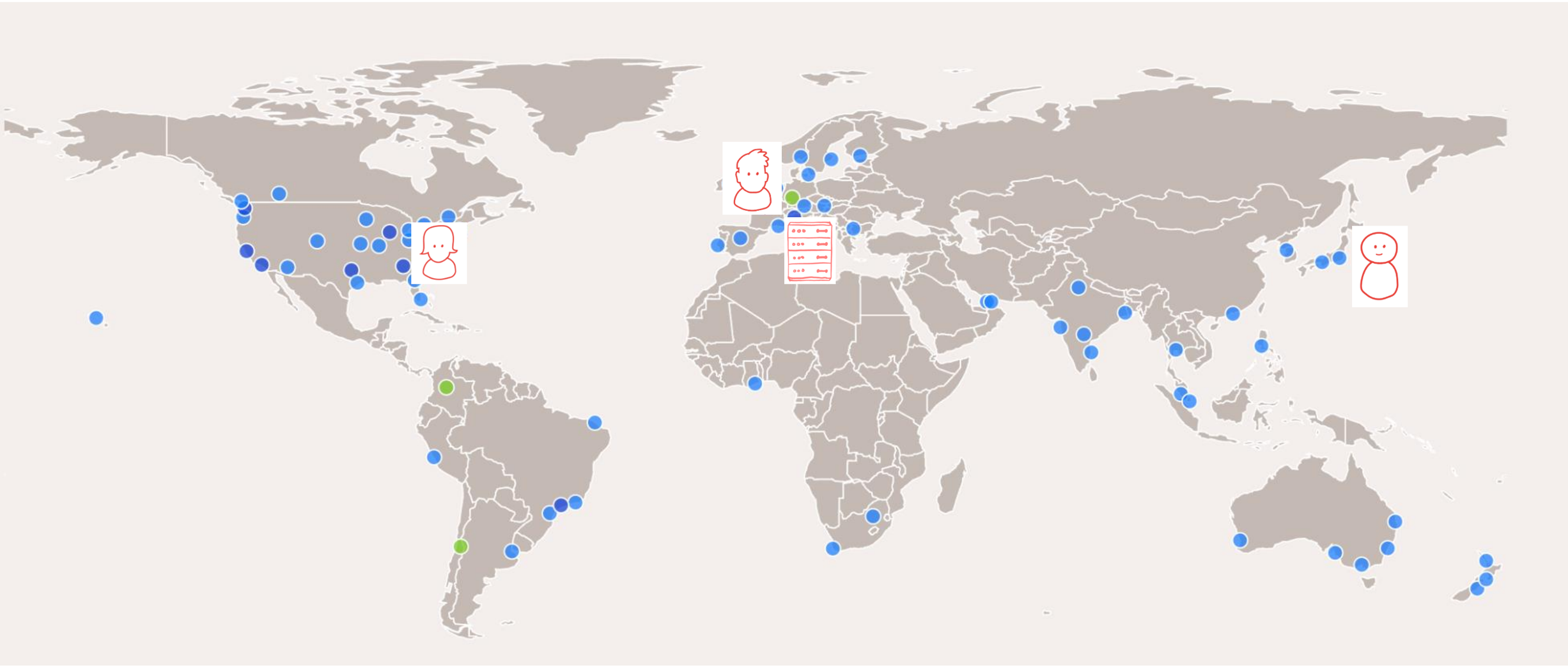
User in Tokyo

Your origin server

Chi è Fastly?


User in
Lyon
Fastly Paris
User in
Washington, DC
Fastly Virginia
Your origin server
User in
Tokyo
Fastly Tokyo

Chi è Fastly?



Accelerazione. Sicurezza. Orientato a DevOps.

Componenti della gestione dei bot

Bot verificati

Consente ai clienti di gestire il traffico proveniente da "bot buoni", come SEO, accessibilità e altro ancora.

Client Fingerprinting

Interrompe l'attività dei bot in blocco con la stessa impronta digitale SSL/TLS

Client Challenges

Sfida JavaScript (passivo) o CAPTCHA (attivo)

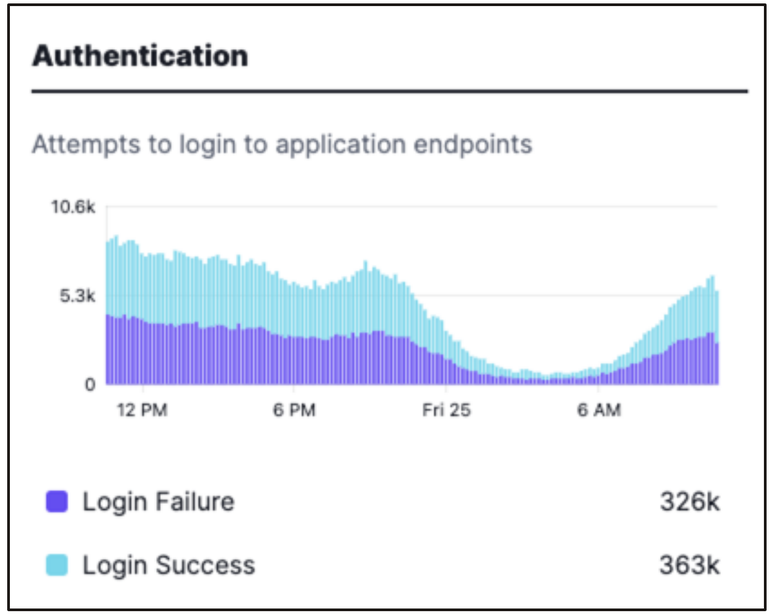
Protezione contro gli attacchi API

Aug 24, 11:35:11 AM EDT
POST accounts.jetblue.com
/api/v1/authn
View request detail

Blocked Request 406
Datacenter Google Cloud
HTTP 4XX 401
SQLI /password=redacted
Suspected Bot User-Agent: Too Short

34.74.38.241
241.38.74.34.bc.googleusercontent.com
JA3: b5eefe582e146aed29a21747a572e11c
ANDROID-OS28-7.4.1-M

- Attacchi in corso contro i vostri endpoint API di autenticazione
- Iniezione OWASP e furto di credenziali
- Rilevamento di segnali malevoli
- Possibilità di sfruttare l'impronta digitale TLS (JA3/JA4) per gli utenti malintenzionati che si scambiano indirizzi IP
- La piattaforma oscura automaticamente le informazioni sensibili dello schema API (ad esempio, i campi password)



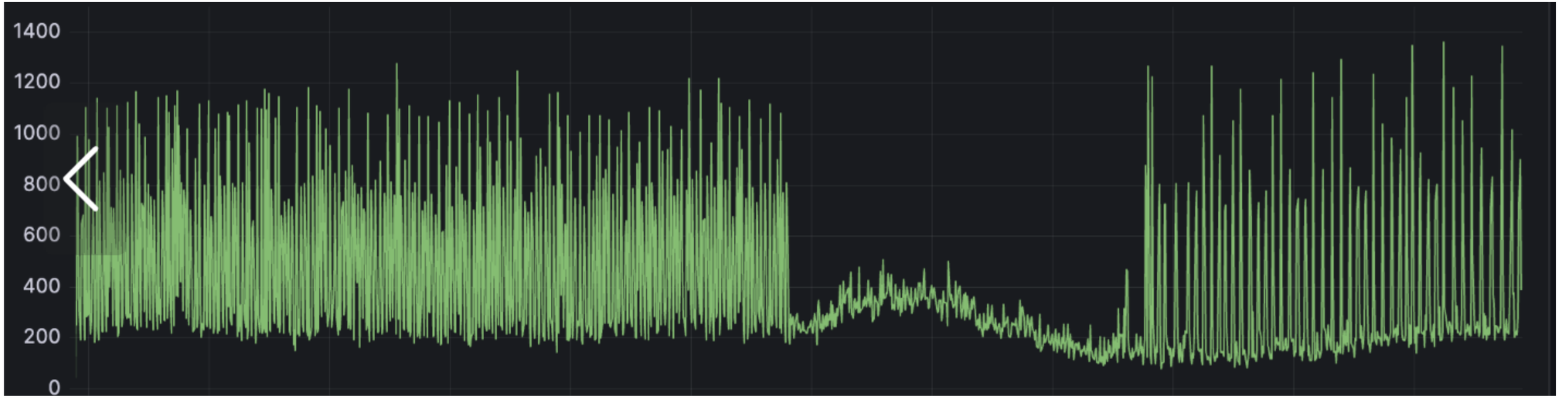
Incidente jetBlue

Durante un fine settimana con relativamente pochi viaggi, abbiamo notato un modello di picchi di errori 404 (bassi e lenti) che saltavano la cache del CDN e raggiungevano l'origine.

Questo iniziava a causare problemi con i pod nel cluster Kubernetes del sito, poiché i picchi di richieste diventavano più frequenti.

Dopo un'analisi delle impronte digitali di prima parte associate a questo comportamento nell'arco di 30 giorni, abbiamo identificato e bloccato il 93% del traffico.

Gli errori restituiti all'aggressore lo hanno indotto ad abbandonare l'attacco.



outBoundLFS errors - top 10 client_ip's with Country codes

client_ip.keyword	geo_country_code.keyword	Count ↓
35.172.84.87	US	243
64.25.25.249	US	230
138.84.58.47	DO	182
165.90.6.63	KE	116
96.238.12.56	US	81
[illegible]	[illegible]	[illegible]

I reviewed the traffic with [redacted] regarding these 2 UAs. When looking at the fingerprints within the last 30 days, there is a fingerprint that accounts for 44% of the traffic with a combined rate of 93% of its traffic resulting in a 404 or 406. We would like to implement a block on this fingerprint if that is okay with the team.

👍 2

[redacted] 2/29 11:56 AM Edited

[redacted] The rule has been enabled, please monitor and keep us updated. Thank you

CONDITIONS	ACTIONS	STATUS
all of Domain equals **jbrest.jetblue.com** JA3 Fingerprint equals **c3bd146e335e754c321db7baee4b2cf1**	Block	Enabled Edit View

Attacchi comuni utilizzati nell'ATO

Forza bruta

"Il modo per recuperare una chiave provando tutte le combinazioni possibili fino a trovare quella che consente l'accesso"

https://es.wikipedia.org/wiki/Ataque_de_fuerza_bruta

Credential Stuffing

"Le credenziali dell'account rubate (spesso da una violazione dei dati) vengono utilizzate per ottenere l'accesso non autorizzato agli account utente"

https://es.wikipedia.org/wiki/Credential_stuffing

Phishing/Malware

"Inganno una vittima guadagnando la sua fiducia per farle compiere azioni che non dovrebbe fare (rivelare informazioni riservate o cliccare su un link)"

https://es.wikipedia.org/wiki/Phishing

Demo (portale non protetto)

ato — -zsh — 118×29

```
dcorbett@C02GD7ZUML85 ato % ./ato.py https://unprotected.bubbsbakery.com/login/
```

Bot Management

Add dashboard

-1h 1 hour ago

2.00 average RPS (last 5 mins) 1 agent 0 observed sources

Verified Bot Activity

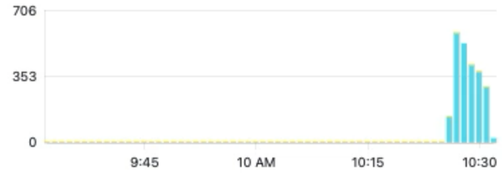
Requests made by verified bots

Accessibility	0
Content Fetcher	0
Monitoring & Site Tools	0
Online Marketing	0
Page Preview	49
Platform Integration	0
Research	0
Search Engine Crawler	182
Search Engine Optimization	74
Security Tools	0

Quick look | View requests

Bot Activity

Requests made by suspected or verified bots



Suspected Bot	0
Suspected Bad Bot	2k
Verified Bot	305

Quick look | View requests

Client Challenges

Requests with a client challenge

Challenged Request	9
Challenge Token Invalid	19
Challenge Token Valid	7

Quick look | View requests

Compromised Credentials

Authentication

Traffic Source Anomalies

Protezione ATO con Client Challenges

Lancia la sfida

Type Request rule

Conditions
all of
- Method equals **GET**
- Domain equals **bubbsbakery.com**
- Path equals **/login/**

Actions Browser challenge

Verifica del token

Type Request rule

Conditions
all of
- Method equals **POST**
- Domain equals **bubbsbakery.com**
- Path equals **/login/**

Actions Verify token

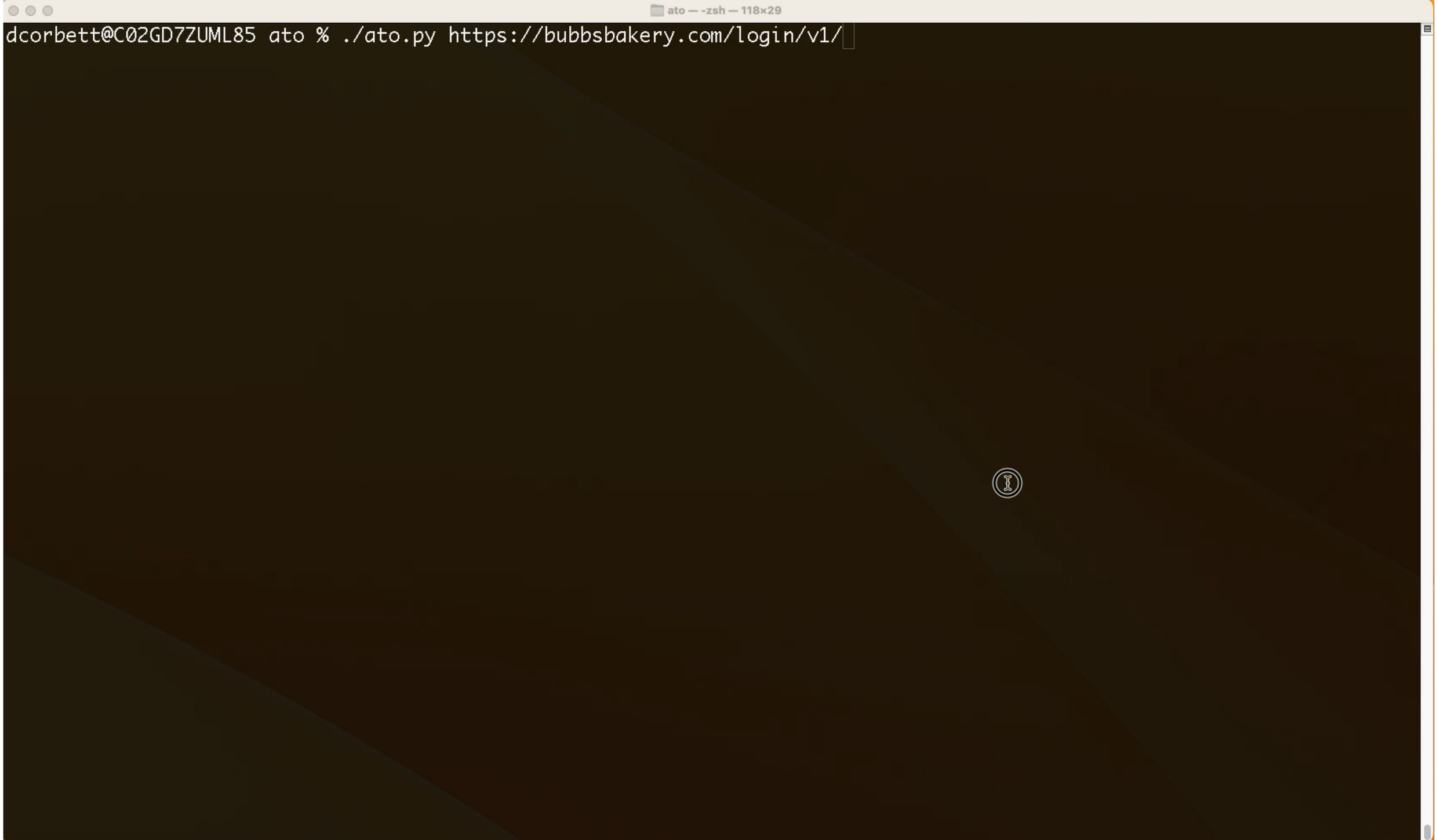
Blocca se non valido

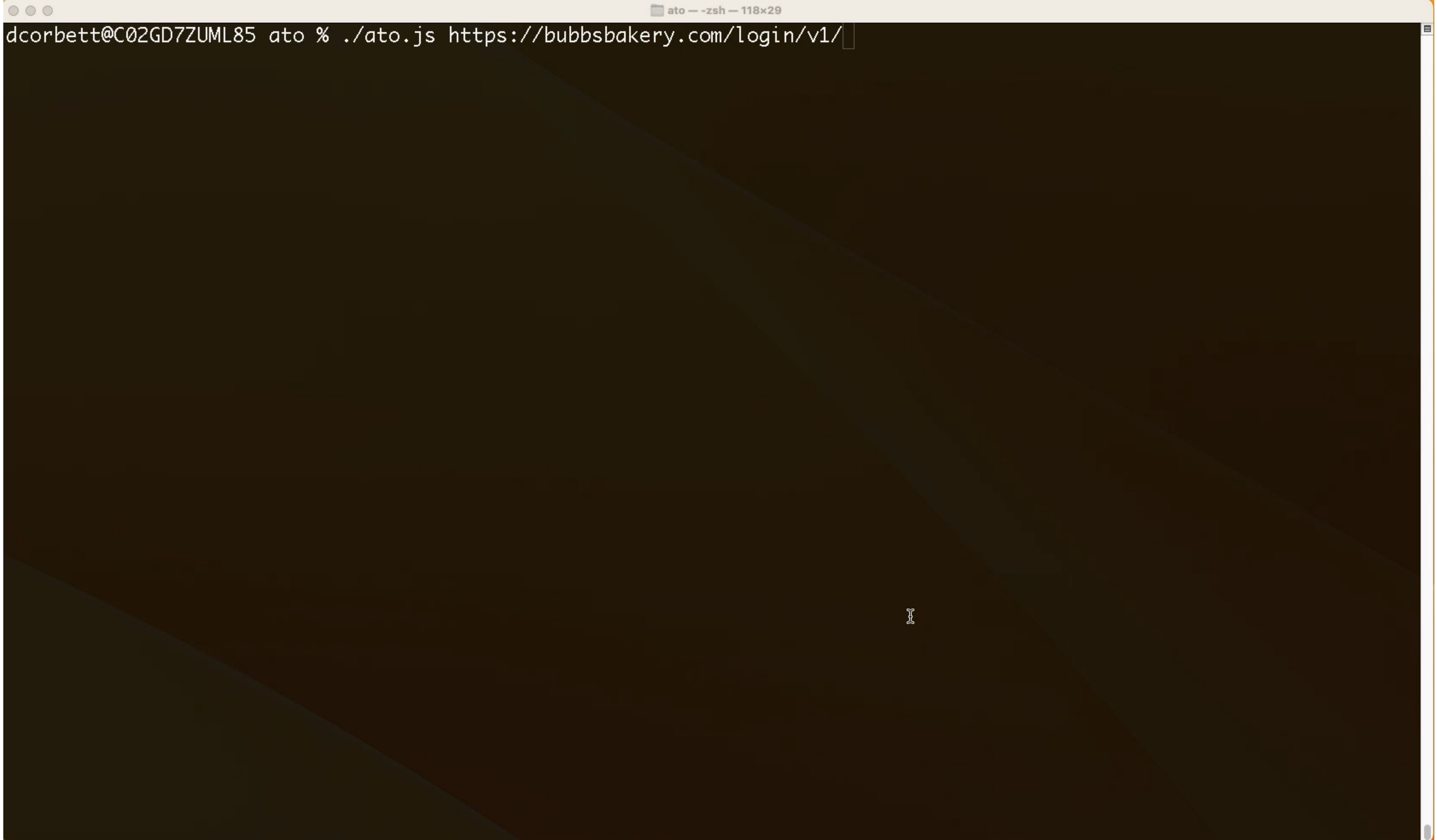
Type Request rule

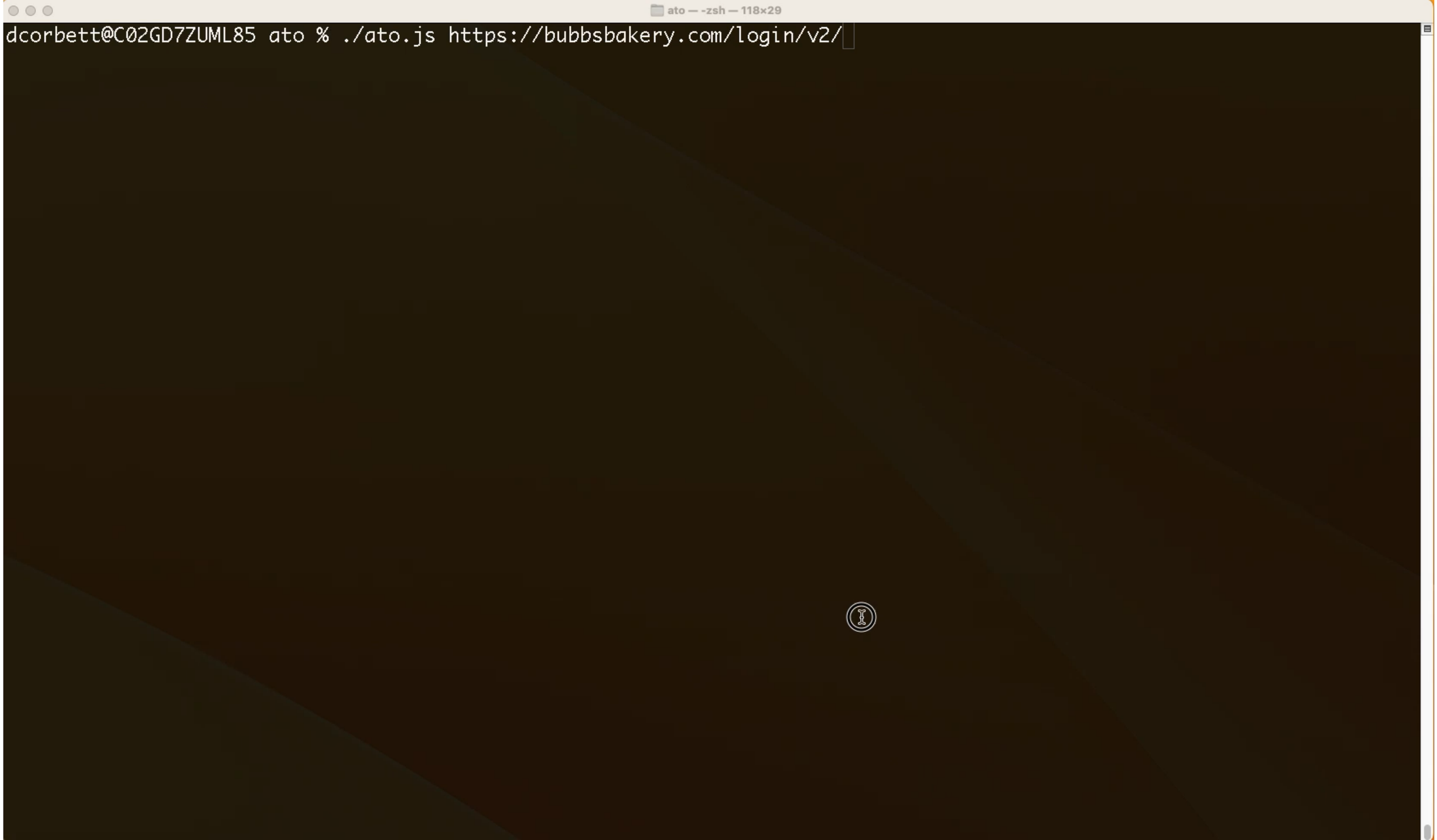
Conditions
all of
- Domain equals **bubbsbakery.com**
- Path equals **/login/**
- Signal exists where
  all of
  - Signal Type equals `Challenge Token Invalid`

Actions
Block
- Respond with 302

Demo (portale protetto)


ato — -zsh — 118×29
dcorbett@C02GD7ZUML85 ato % ./ato.py https://bubbsbakery.com/login/v1/


ato — -zsh — 118×29
dcorbett@C02GD7ZUML85 ato % ./ato.js https://bubbsbakery.com/login/v1/

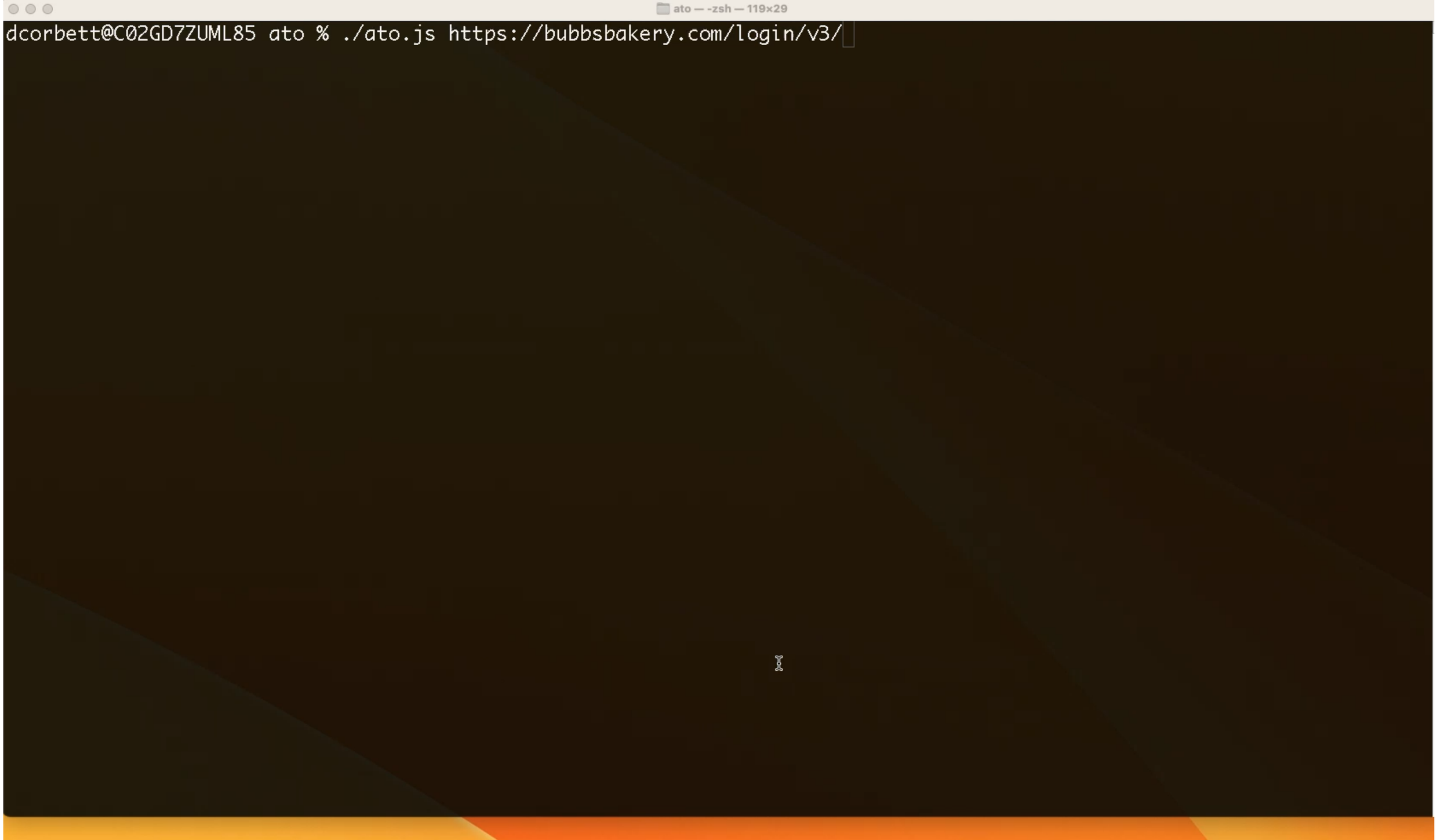

ato — -zsh — 118×29
dcorbett@C02GD7ZUML85 ato % ./ato.js https://bubbsbakery.com/login/v2/

Ingannare i bot (demo)

Combinazione di credenziali compromesse con limitazione della velocità e inganno

Type	Rate limit rule
Signal	compromised-cred-counter (site)
Conditions	all of Method equals **POST** Domain equals **bubbsbakery.com** Path equals **/login/** Signal exists where all of Signal Type equals Compromised Password
Client identifier	IP address (default)
Actions	Add compromised-cred-counter (site) If 20 counting signals in 1 min, take action for 5 min: Block compromised-cred-counter (site) Respond with 418

Preview rate limited sources


ato — -zsh — 119×29
dcorbett@C02GD7ZUML85 ato % ./ato.js https://bubbsbakery.com/login/v3/

Bot Management

Add dashboard

-1h 1 hour ago

2.42 average RPS (last 5 mins) 1 agent 1 observed source

Verified Bot Activity

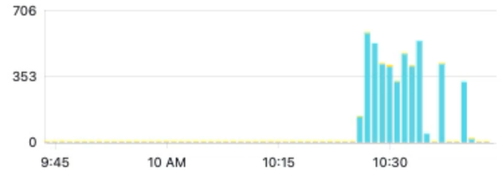
Requests made by verified bots

Accessibility	0
Content Fetcher	0
Monitoring & Site Tools	0
Online Marketing	0
Page Preview	44
Platform Integration	0
Research	0
Search Engine Crawler	187
Search Engine Optimization	72
Security Tools	0

Quick look | View requests

Bot Activity

Requests made by suspected or verified bots

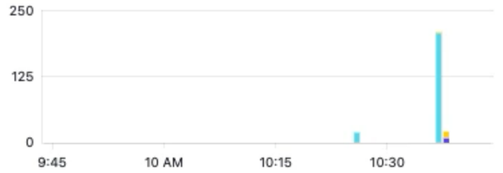


Suspected Bot	0
Suspected Bad Bot	5k
Verified Bot	303

Quick look | View requests

Client Challenges

Requests with a client challenge



Challenged Request	9
Challenge Token Invalid	225
Challenge Token Valid	14

Quick look | View requests

Compromised Credentials

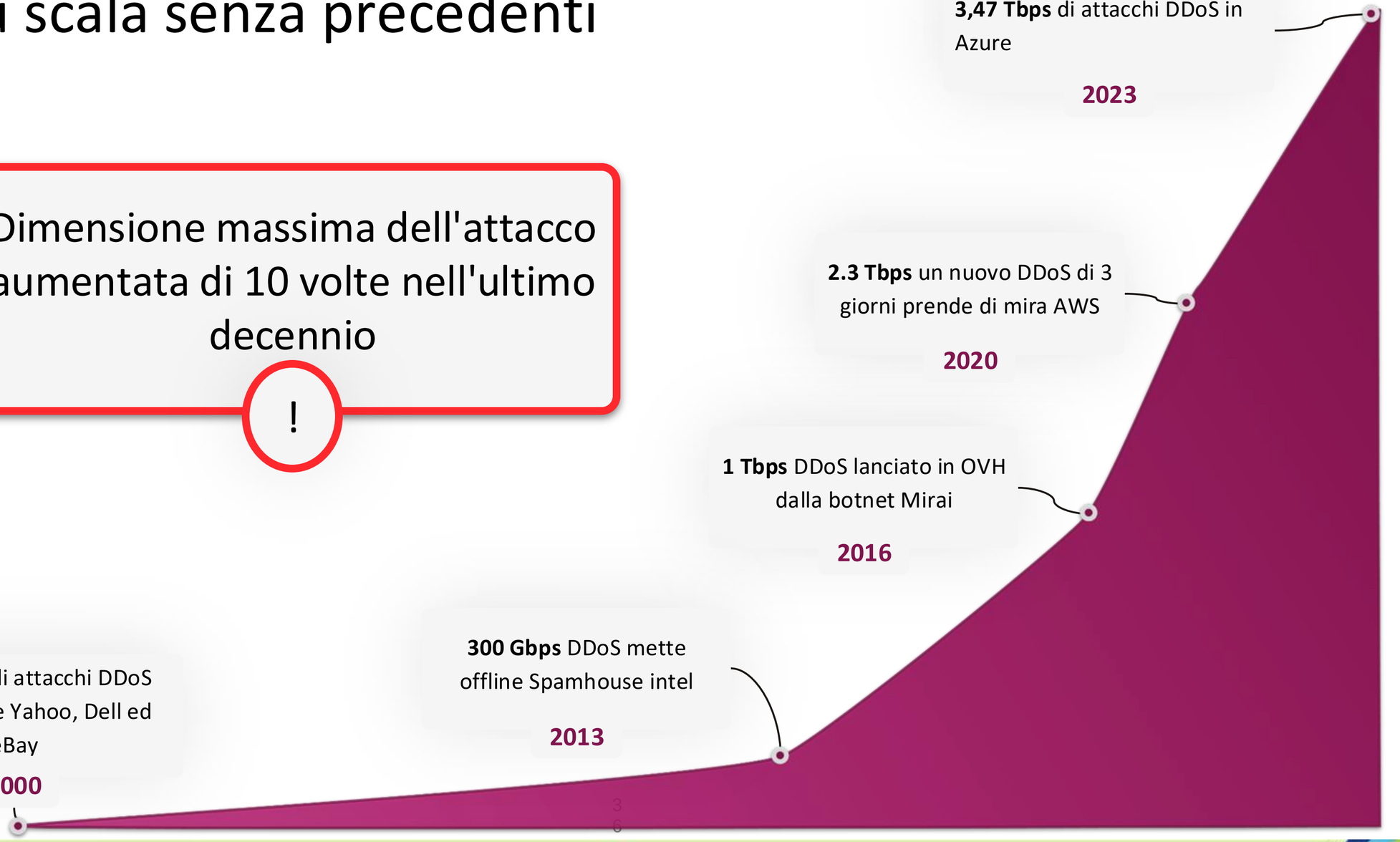
Authentication

Traffic Source Anomalies

Difesa su scala senza precedenti

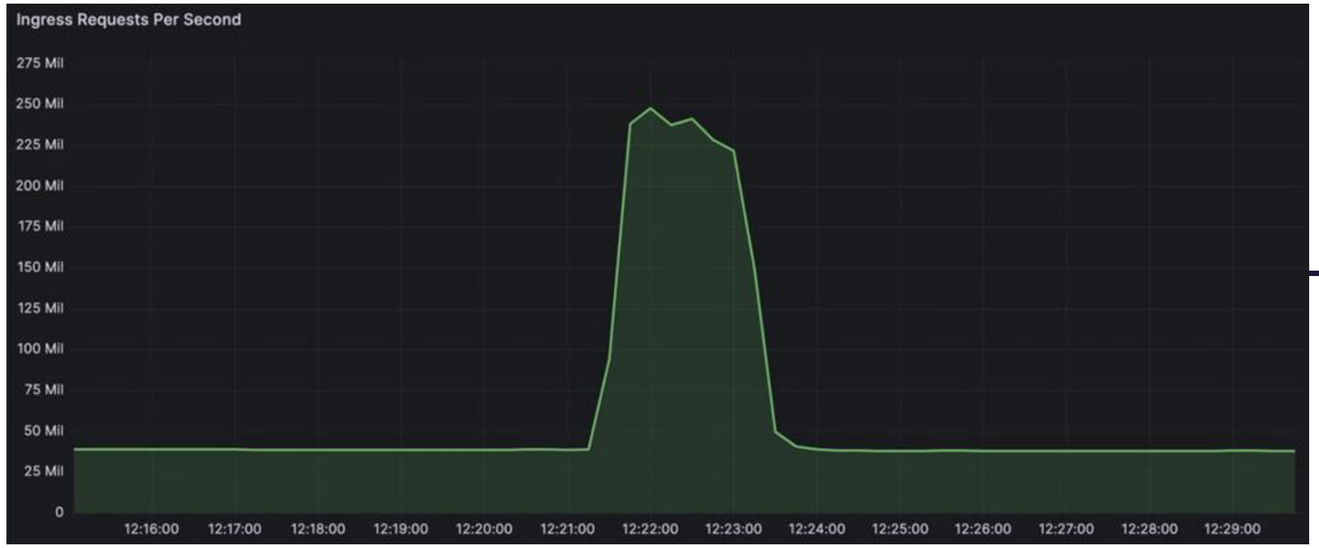
Dimensione massima dell'attacco aumentata di 10 volte nell'ultimo decennio

!



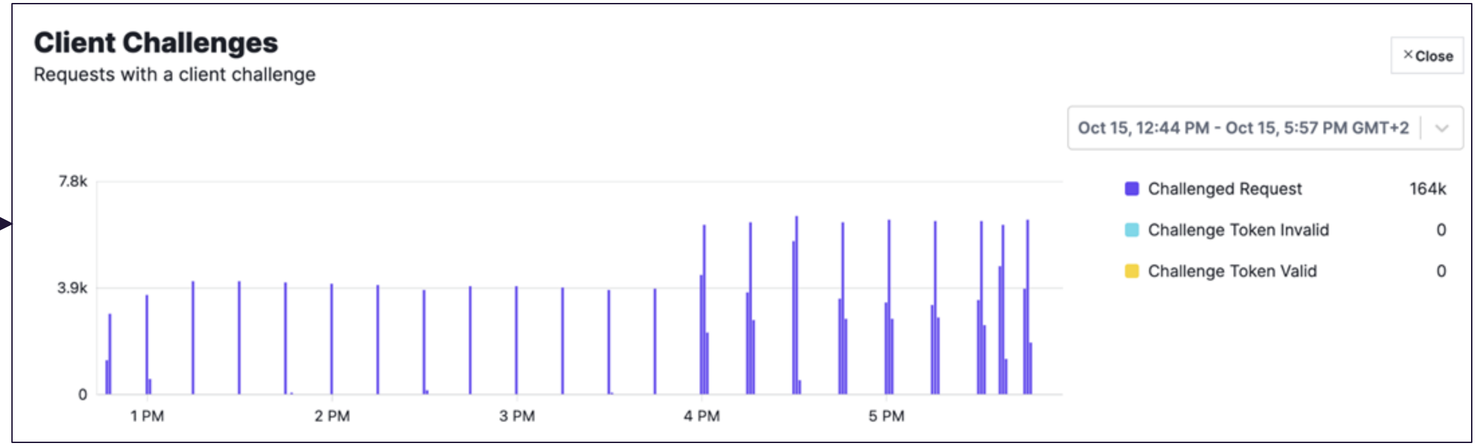
Difesa su scala senza precedenti

DDoS delle applicazioni che dura solo pochi minuti



Esempio: milioni di richieste al secondo in 3 minuti

Oppure: 1000 richieste della durata di 1-3 minuti ogni 15 minuti



I principi che guidano Attribute Unmasking

Velocità

Tutto inizia con il rilevamento rapido del traffico dannoso

Precisione

Evitare falsi positivi è la nostra priorità, quindi le mitigazioni devono essere accurate

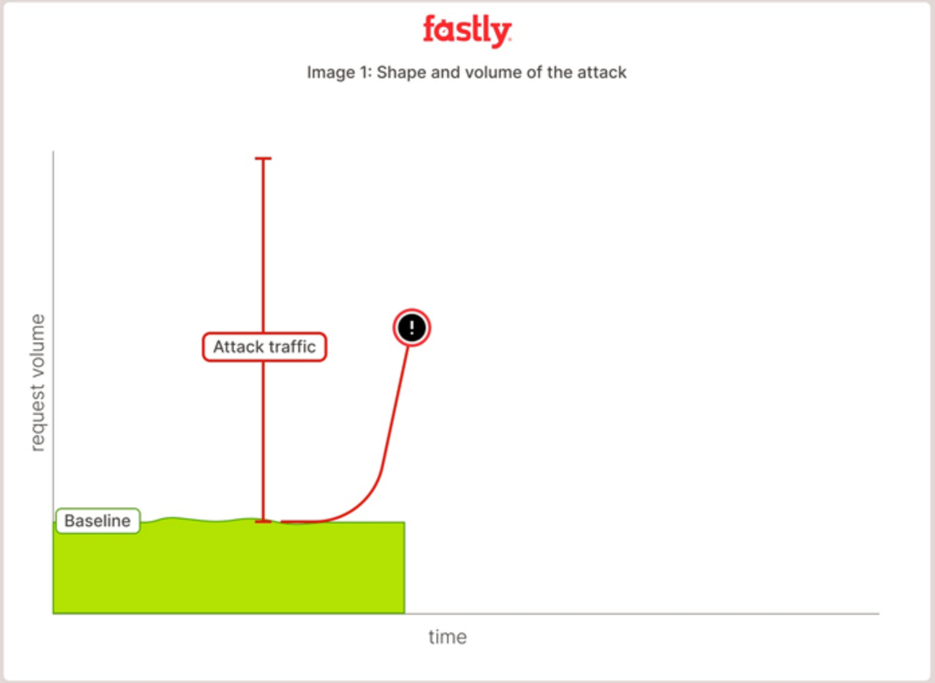
Deceptive

Le nostre tattiche di difesa dovrebbero essere **ingannevoli**, riducendo al minimo le informazioni disponibili per gli aggressori

Detection

Distinguere gli attacchi DDoS dalle deviazioni del traffico

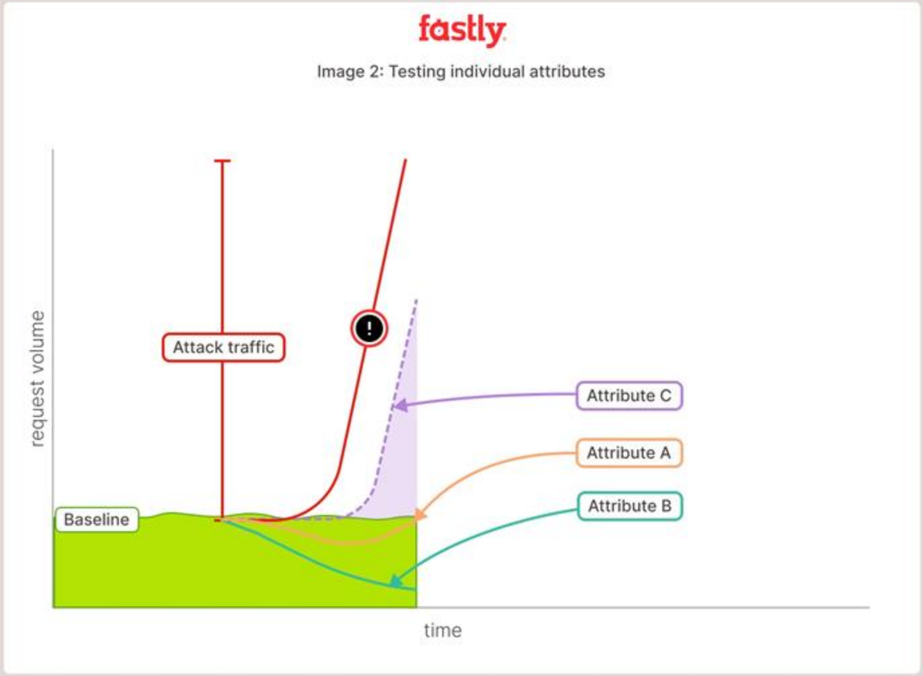
- ➔ Eseguito all'edge definito dal software di Fastly e non richiede alcuna messa a punto
- ➔ Il limite di velocità viene aggiornato continuamente in base alla media di corsa
- ➔ Quando si verificano deviazioni anomale del traffico, Attribute Unmasking indaga



Identificazione

Scoprire le caratteristiche degli attacchi DDoS complessi

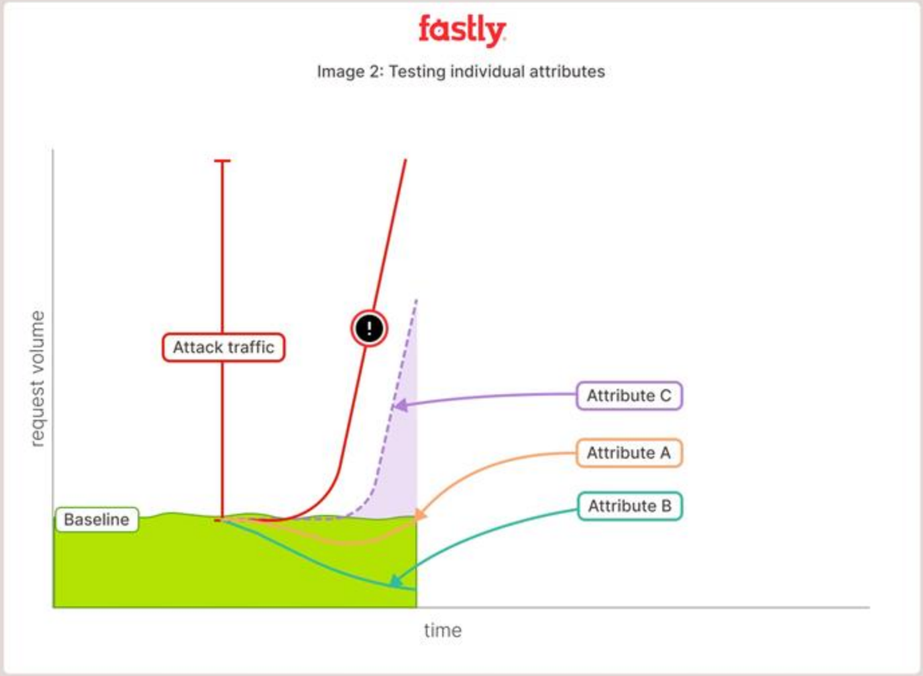
- ➔ Scansiona un elenco completo delle caratteristiche di TLS e dei livelli 3, 4 e 7 per trovare quella che meglio corrisponde alla curva
- ➔ Base altamente accurata e di natura adattiva
- ➔ Costruito su un sistema modulare per un rapido adattamento ai nuovi attacchi DDoS



Identificazione

Scoprire le caratteristiche degli attacchi DDoS complessi

- ➔ Scansiona un elenco completo delle caratteristiche di TLS e dei livelli 3, 4 e 7 per trovare quella che meglio corrisponde alla curva
- ➔ Base altamente accurata e di natura adattiva
- ➔ Costruito su un sistema modulare per un rapido adattamento ai nuovi attacchi DDoS

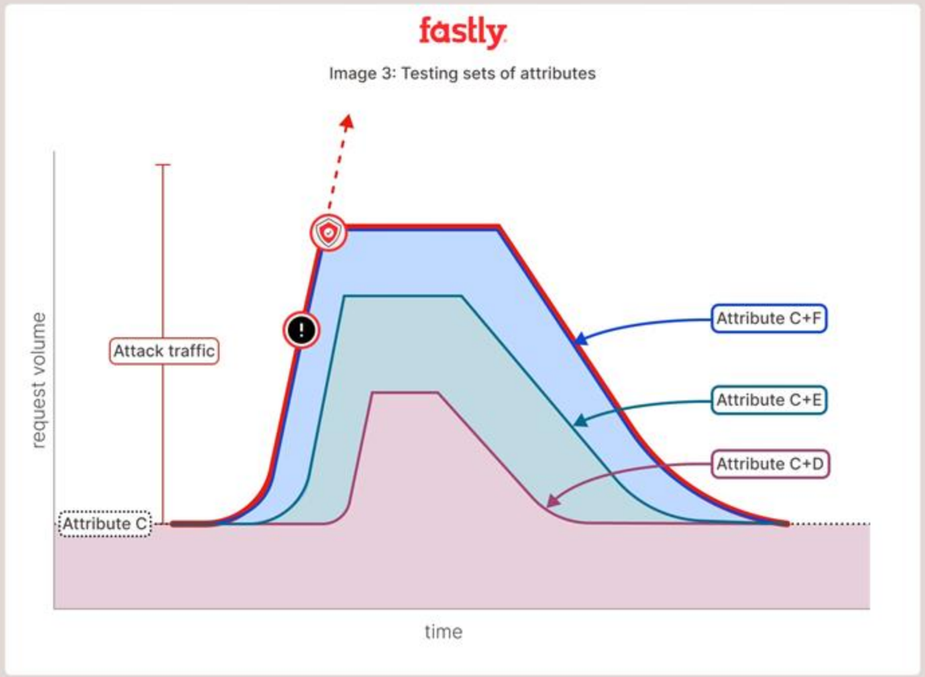



```
User-Agent: 😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀
```

Mitigazione

Completare il modello e fermare l'aggressore

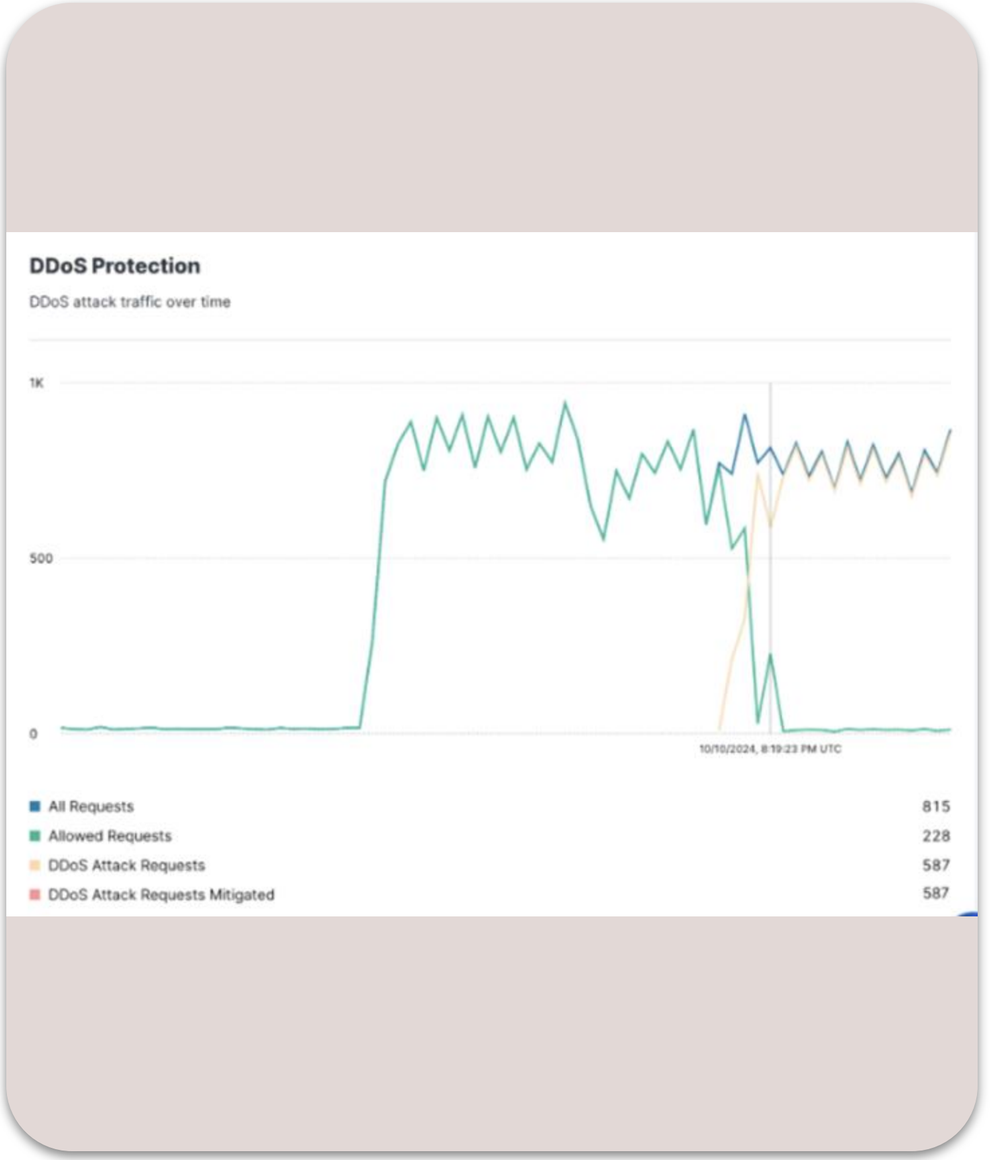
- Impila le combinazioni di attributi fino a quando non corrispondono alla curva e blocca le richieste successive dal traffico di attacco corrispondente
- Blocca contemporaneamente più attacchi DDoS con modelli di traffico anomali
- Quasi in tempo reale



Protezione DDoS in azione

In pochi secondi, automaticamente:

- Rilevato l'attacco
- È stata creata una regola temporanea composta da 8 attributi, tra cui:
  - Paese
  - JA4 fingerprint
  - OHFP – Order of headers fingerprint



Q&A

Contatti

fernando@fastly.com
https://www.linkedin.com/in/fbitti/

https://www.fastly.com/