Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA

SECURITY SUMMIT

Security Summit

Verona, 24 ottobre 2024

# Mitigazione delle minacce DDoS moderne: Rapid Reset

**Mauro Cicognini** | Comitato Scientifico *Clusit*
**Fernando Bitti Loureiro** | Principal Solutions Architect *Fastly*

# Mauro Cicognini

COMITATO SCIENTIFICO

FOUNDING PARTNER

# Cos’è un attacco DDoS?

- *Distributed* Denial of Service
- Intento: impedire che gli utenti legittimi usino un servizio
- Meccanismo: sovraccarico del sistema o della rete
- Strumento: flusso massiccio e simultaneo di traffico
- Origine: *moltissimi sistemi nel mondo*
- Durata: da pochi secondi a molte ore

# Come si svolge un DDoS?

**Creazione botnet**

- Un gruppo (100.000 e più) di computer compromessi (bot) viene creato da una organizzazione criminale
- I "bot" sono riuniti in una *botnet* controllata da un server di Command & Control

**Attivazione botnet**

- I primi criminali affittano la botnet ad altri criminali che prendono di mira un certo bersaglio
- I secondi criminali accedono al C&C e configurano i bot per generare un flusso massiccio di traffico verso il bersaglio

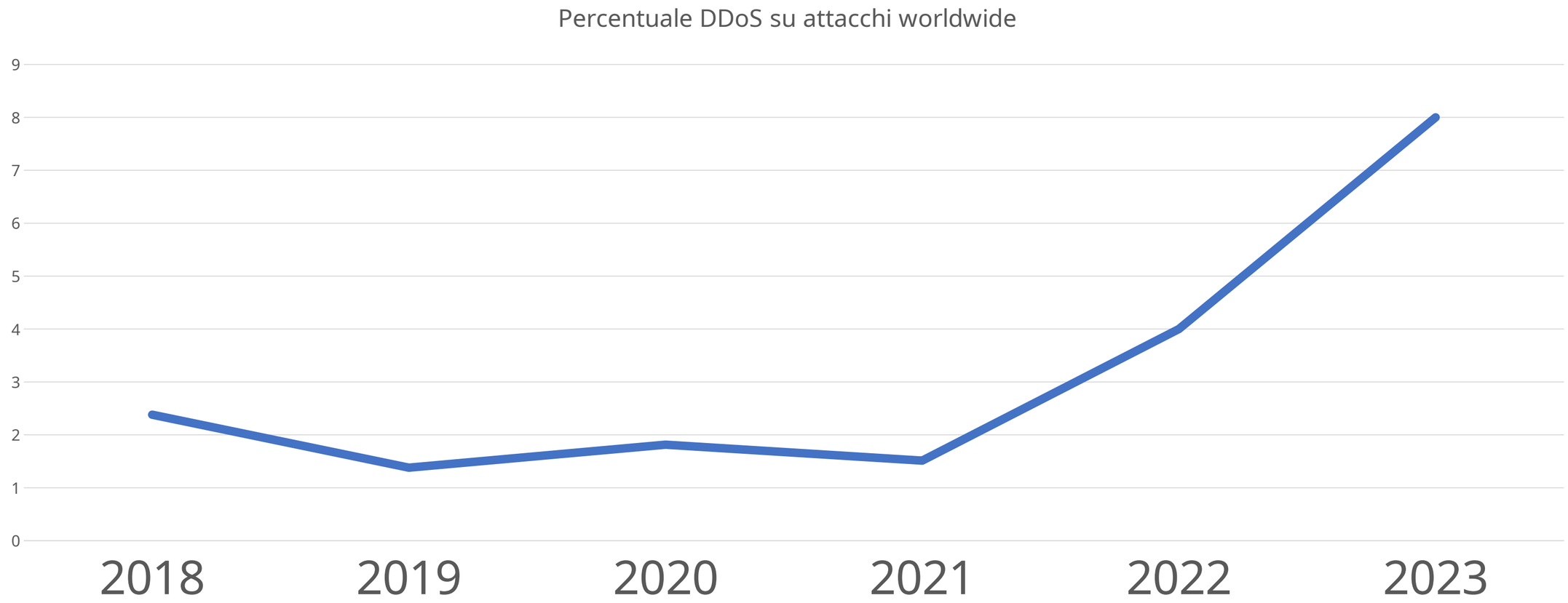
**Effetto attacco**

- Il flusso di traffico sovraccarica il sistema o la rete del bersaglio
- L'attacco dura per il tempo dell'affitto

# Che motivazioni ha un DDoS?

- Ideologiche / Politiche
  - Sabotaggio
- Economiche
  - Danneggiare un concorrente
  - Ricatto
- Confusione
  - Sviare l’attenzione da altre azioni
- Errori

# Ci sono molti DDoS?




Dati © Clusit 2018-2024

# E poi ci sono i DDoS “involontari”…

WIRED SCIENZA ECONOMIA CULTURA GADGET SECURITY DIRITTI IDEE VIDEO PODCAST WIRED CONSIGLIA ABBONAMENTI EV

RAFFAELE ANGIUS LUCA ZORLONI EPIC FAIL 19.10.2024

## Stavolta Piracy Shield l'ha fatta grossa e ha bloccato Google Drive

Un dominio di Big G finisce nel mirino della piattaforma nazionale anti-pirateria, che lo oscura, impedendo i download dei dati da una delle principali piattaforme cloud al mondo

## Google Drive oscurata, il Garante diffida Dazn: “Avete sbagliato, rischiate l’espulsione”

di Aldo Fontanarosa


*L’erronea segnalazione della pay-tv ha causato l’oscuramento del servizio di condivisione di documenti sabato sera. Pesante multa in caso di nuovi errori nelle denuncie. Il commissario Giacomelli: “Lo scudo va chiuso temporaneamente e perfezionato”*

ALTROCONSUMO Cosa vuoi cercare? CERCA Entra

## Google Drive bloccato: scambiato per un sito pirata di calcio in streaming. Perché è successo e cosa fare

Segui - Tariffe internet, telefonia fissa e mobile

Dalla sera di sabato 19 ottobre fino alle prime ore di domenica, migliaia di utenti non hanno potuto scaricare i documenti archiviati nel proprio Google Drive (ma neppure utilizzare in parte Youtube e le immagini di Google Foto). Motivo? Piracy Shield, la piattaforma antipirateria di Agcom, l'ha bloccato come un normale sito che trasmette le partite di serie A illegalmente. Ma come è stato possibile? Ecco tutte le falle di questo

Clusit Associazione Italiana per la Sicurezza Informatica

fastly

SECURITY SUMMIT VERONA

ASTREA

# Conseguenze di un DDoS

- Perdita di dati
- Riduzione delle prestazioni
- Perdita di business
- Risarcimenti
- Sanzioni (GDPR, DORA, NIS, ecc.)

# Prevenzione del DDoS

- **Monitoraggio del traffico**
  - Monitorare i flussi di dati per identificare eventuali attacchi
- **Detection veloce**
  - Per minimizzare la non disponibilità
- **Potenziamento Infrastruttura**
  - Investimenti su ridondanza, resilienza e distribuzione geografica

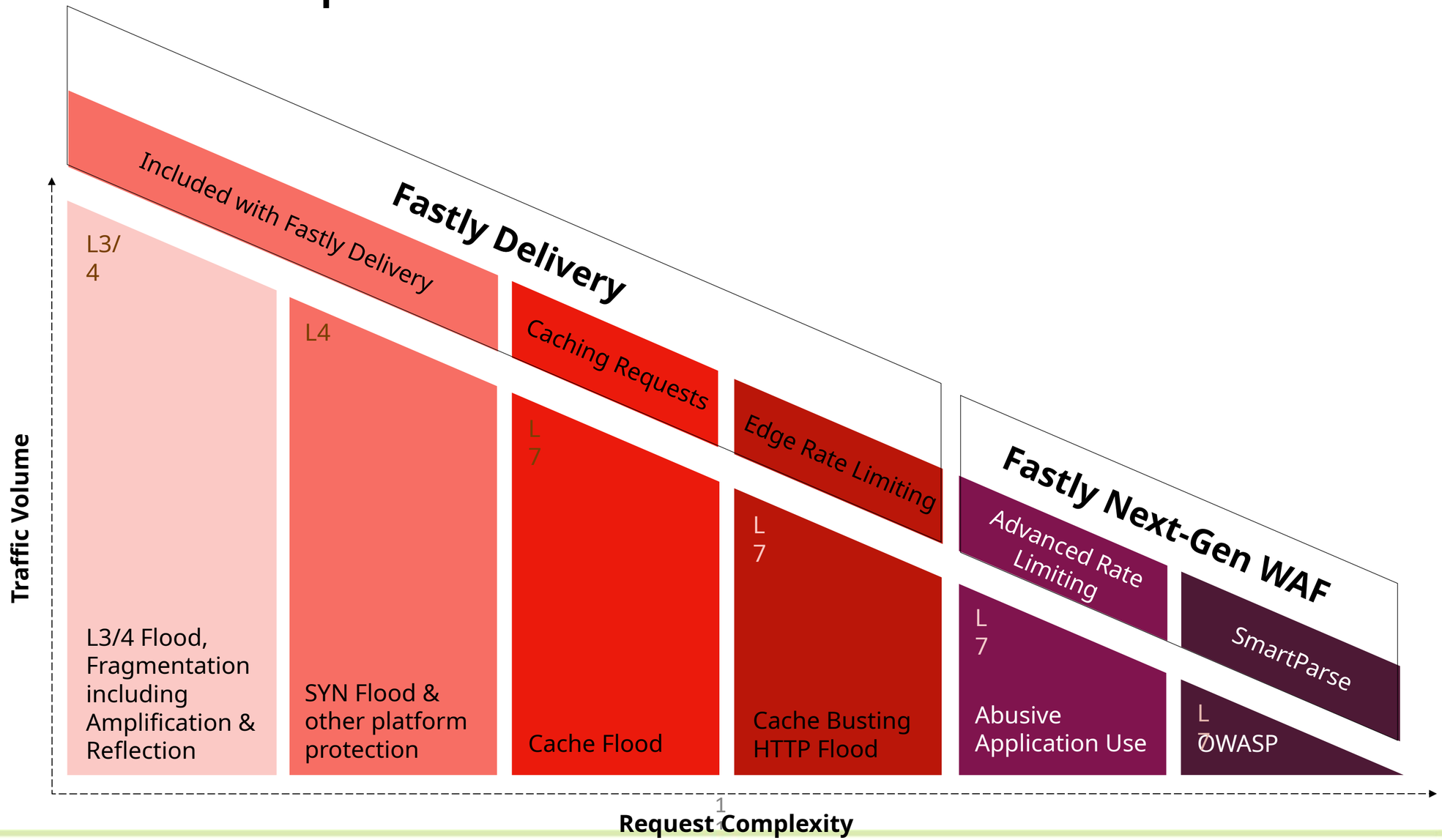
**Fernando Bitti Loureiro**
Principal Sales Engineer
**https://www.fastly.com/**

fastly

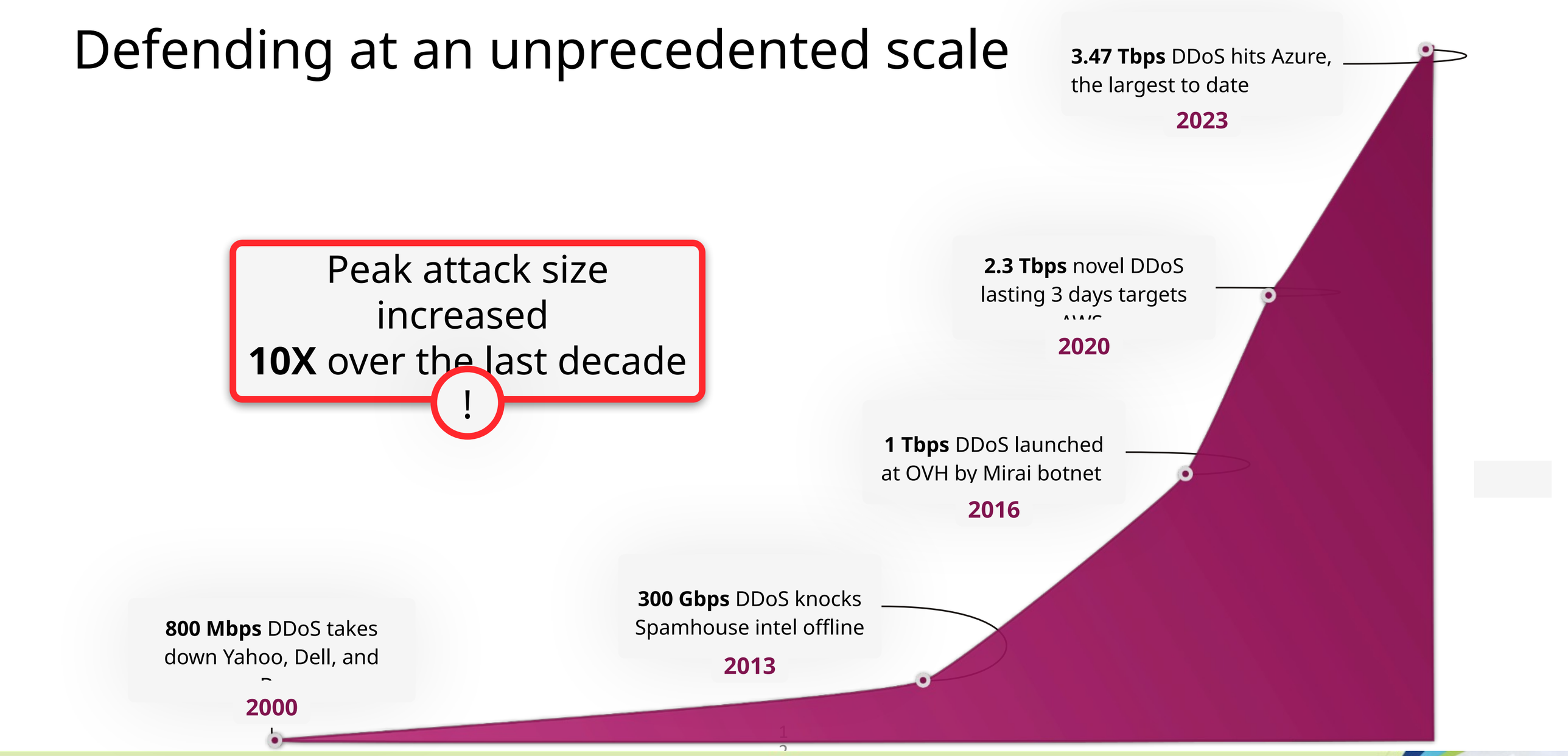
BENDING SPOONS

RCS MEDIAGROUP

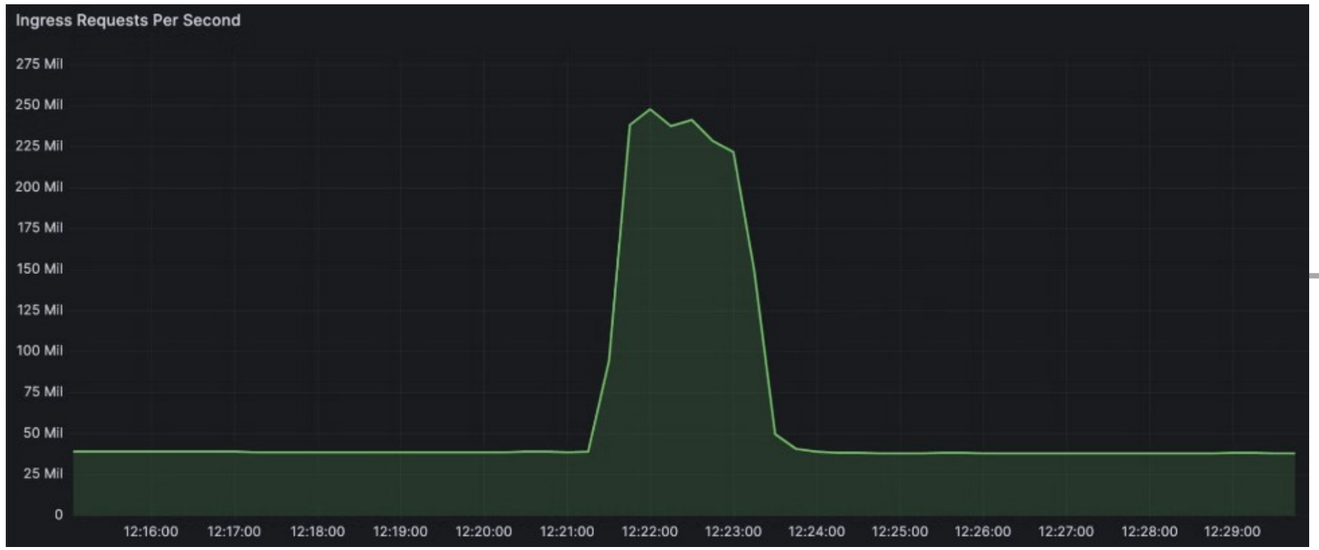
# Solve different phases of DDoS



# Defending at an unprecedented scale

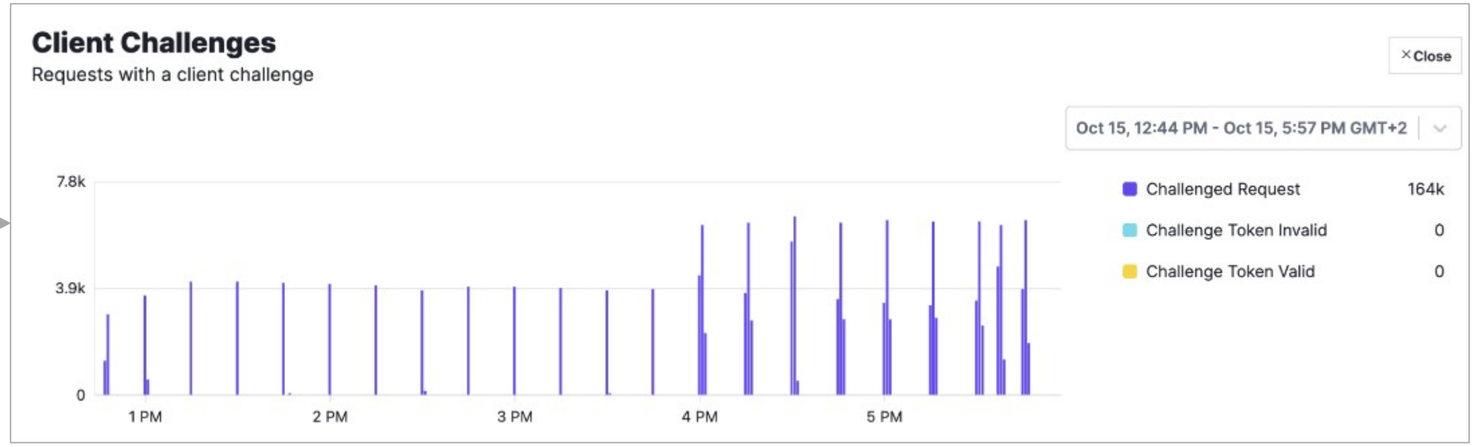


# Application DDoS that only lasts a few minutes




Example: Millions of requests per second during 3 minutes

Or: 1000s of requests lasting 1-3 minutes every 15 minutes



# The principles that drive Attribute Unmasking

## Rapid

Everything starts with rapid detection of malicious traffic

## Accurate

Avoiding false positives is our priority so mitigations must be accurate

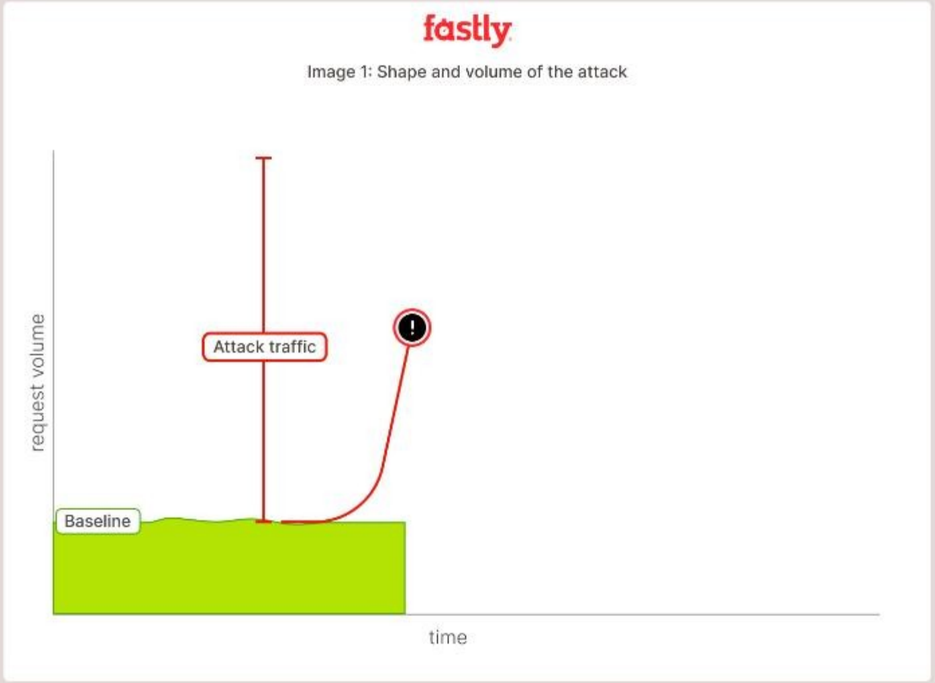
## Deceptive

Our defense tactics should be deceptive, minimizing information available to attackers

# Detection

Distinguish DDoS attacks from traffic deviations

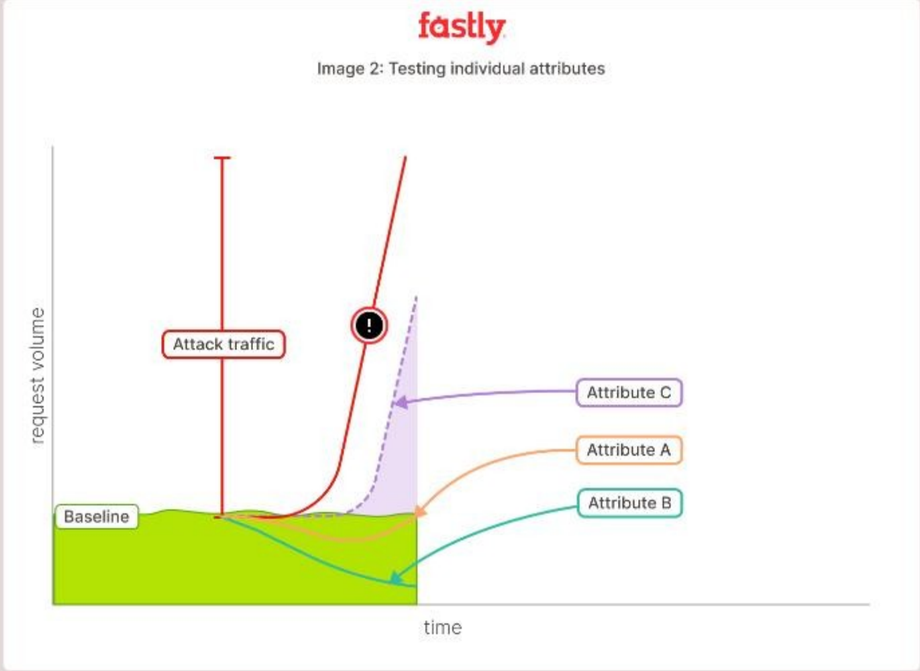
- ➔ Performed at Fastly’s software defined edge and requires no tuning
- ➔ Rate limit is updated continuously based on your running average
- ➔ When anomalous traffic deviations arise, Attribute Unmasking investigates



# Identification

Uncovering attack characteristics  from complex DDoS attacks

- Scans a comprehensive list of Layer 3,4 and 7 characteristics to find one that best matches the curve
  - Layer 3 and Layer 4 headers, TLS info, Layer 7 details, etc.
- Highly accurate foundation and adaptive in nature
- Built on a modular system for quick adaptation to new DDoS attacks



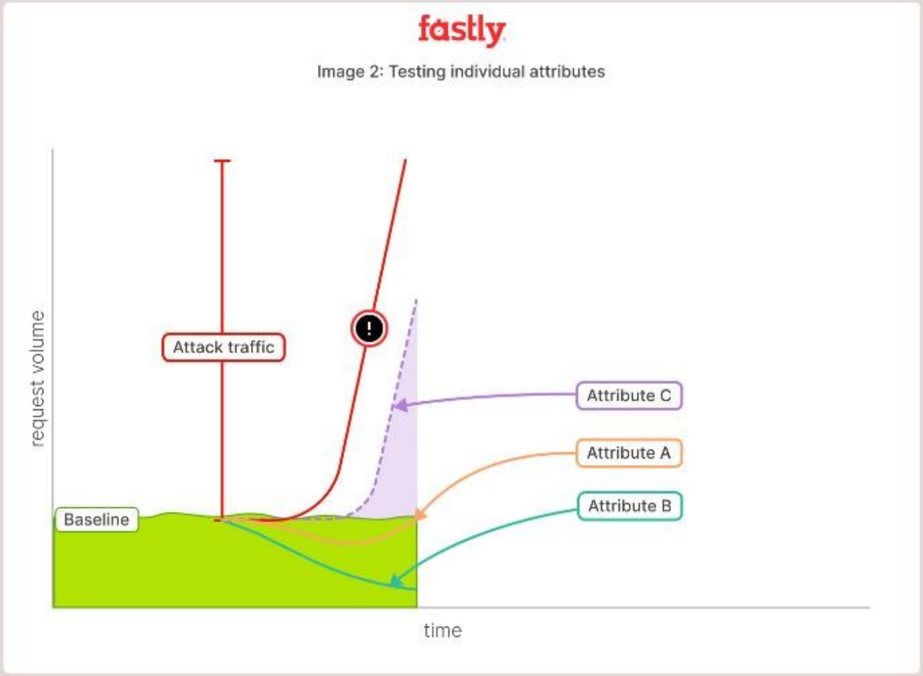
# Identification

Uncovering attack characteristics  from complex DDoS attacks

- Scans a comprehensive list of Layer 3,4 and 7 characteristics to find one that best matches the curve
  - Layer 3 and Layer 4 headers, TLS info, Layer 7 details, etc.
- Highly accurate foundation and adaptive in nature
- Built on a modular system for quick adaptation to new DDoS attacks

**Did you know?** Attribute Unmasking's proprietary technique caught novel attacks like HTTP Reset automatically with no updates.

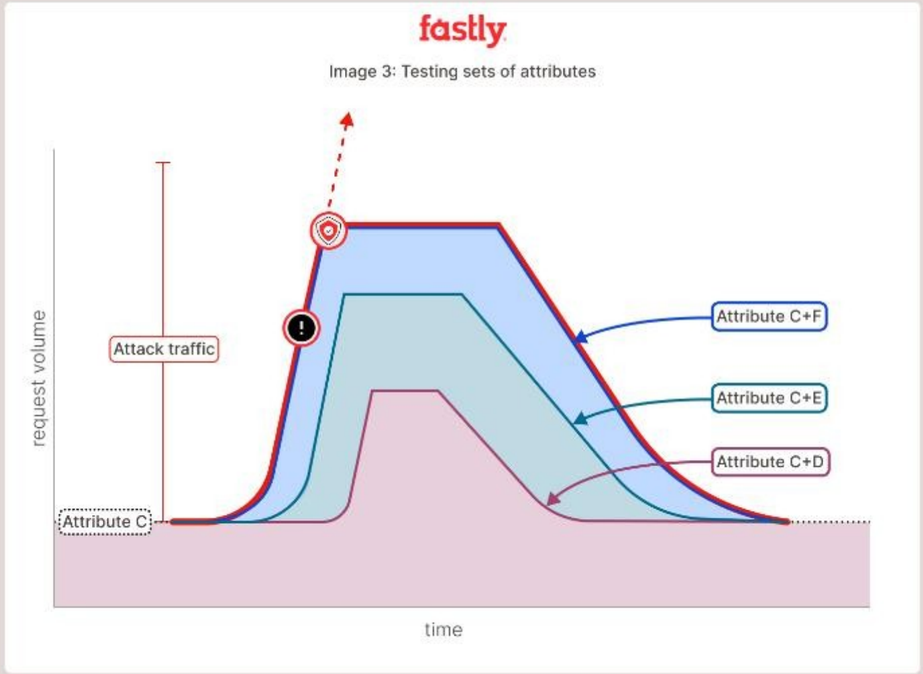
```
User-Agent: 😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀😀
```



# Mitigation

Completing the model and stopping the attacker

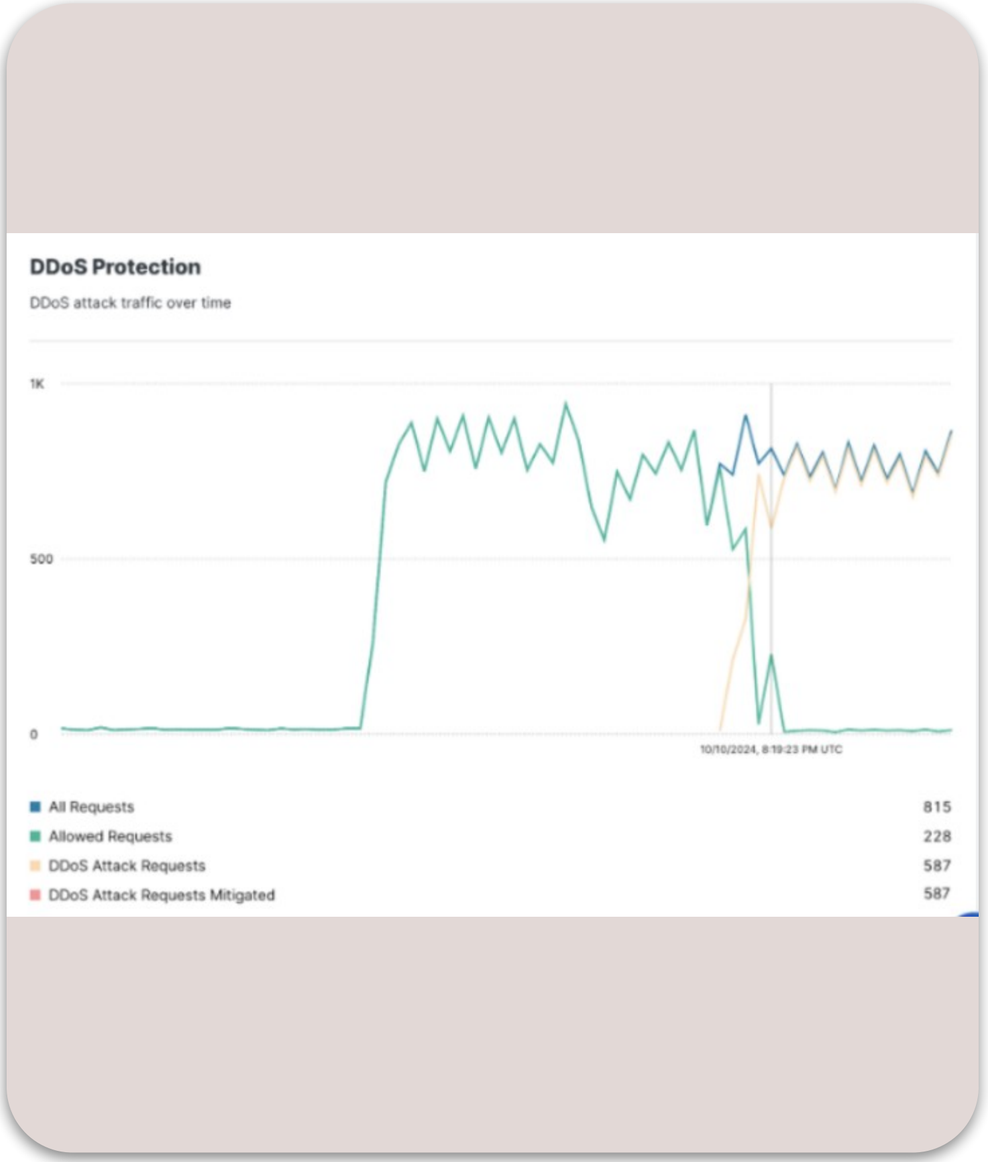
- Stacks attribute combinations until it matches the curve and blocks subsequent requests from matched attack traffic
- Blocks multiple DDoS attacks with anomalous traffic patterns simultaneously
- Near real-time



# DDoS Protection in Action

In seconds, it automatically:

- Detected the attack
- Created a temporary rule comprised of 8 attributes, including:
  - country code
  - JA4 fingerprint
  - OHFP



# Q&A

## Contatti

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

https://www.fastly.com/