Ensuring Site Reliability Using Security Controls

Vijay Janakiraman & Anuradha Narayanan
PayPal Inc.
Agenda

1. Introduction
2. Layer 7 Application Defense
3. Detection Strategies
4. Mitigation Strategies
Introduction

Bad Bot vs. Good Bot vs. Human Traffic 2018

- Bad Bots: 20.4%
- Human: 62.1%
- Good Bots: 17.5%

Source: Internet
Introduction

The chart illustrates the percentage of traffic from different industries, categorized by bad bots, good bots, and humans. The data is sourced from the Internet.

- **Financial**: 42.2% Bad Bots, 1.6% Good Bots, 56.2% Humans
- **Ticketing**: 39.3% Bad Bots, 3.5% Good Bots, 57.2% Humans
- **Education**: 37.9% Bad Bots, 5.0% Good Bots, 57.1% Humans
- **IT and Services**: 34.4% Bad Bots, 11.1% Good Bots, 54.5% Humans
- **Marketing & Advertising**: 33.3% Bad Bots, 9.7% Good Bots, 57.1% Humans
- **Adult Entertainment**: 30.0% Bad Bots, 0.5% Good Bots, 69.5% Humans
- **Government**: 29.9% Bad Bots, 6.4% Good Bots, 63.6% Humans
- **Digital Publishing**: 26.9% Bad Bots, 30.0% Good Bots, 43.0% Humans
- **Gambling & Gaming**: 25.9% Bad Bots, 0.1% Good Bots, 74.0% Humans
- **Airlines**: 25.8% Bad Bots, 1.2% Good Bots, 73.0% Humans
- **Insurance**: 20.7% Bad Bots, 0.8% Good Bots, 78.5% Humans
- **Travel**: 19.4% Bad Bots, 3.8% Good Bots, 76.8% Humans
- **Ecommerce**: 18.0% Bad Bots, 12.6% Good Bots, 69.4% Humans
Layer 7 Application Defense

INTERNET → NETWORK PROTECTION → LAYER 7 ROUTER → LAYER 7 DEFENSE → APPLICATIONS

APP-1, APP-2, APP-3, APP-N
Layer 7 Application Defense

- Ensure high availability and thus high reliability
- Embedded at the application router / load balancer
- Detect and mitigate the malicious traffic before it reaches the actual application
  - Not only based on IP
  - More closer to the application and hence more control
Detection Strategies

- **HTTP pattern (WAF)**
  - Pattern based on request parameters
  - Mandatory / missing request parameters
  - Order of headers

- **Rate/Velocity**
  - Low-flying attack
  - Burst attack

- **Reputation Feed**
  - Bad/Suspicious IPs

- **Unverified device**

- **Machine Learning**
Mitigation Strategies

- Block
- Captcha
  - Visible
  - Invisible
- Tarpit
Key Takeaways

- 1/5th of internet traffic is bad!
- Layer 7 Application Defense is the most effective mechanism to detect & mitigate bad traffic
- Keeping the bad traffic away will keep the applications highly available and thus high reliable
- Differentiating good vs bad is becoming tougher
- Machine learning is the future of application defense
- More innovative mitigation strategies is the need of the hour
Questions?

Vijay Janakiraman – https://www.linkedin.com/in/vijayjanakiraman

Anuradha Narayanan - https://www.linkedin.com/in/anunarayanan