Ensuring Site Reliability Using Security Controls

Vijay Janakiraman & Anuradha Narayanan
PayPal Inc.

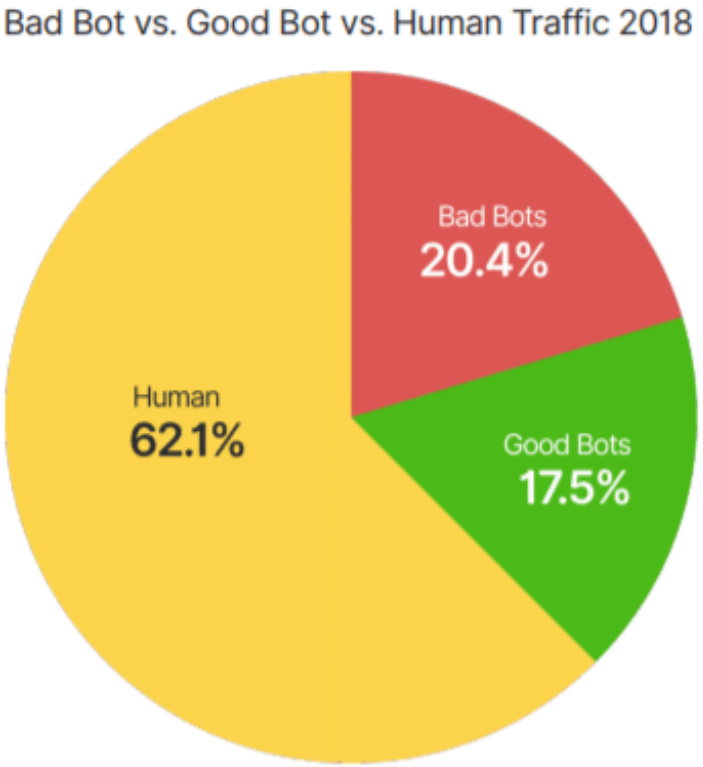
PayPal

Agenda

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

PayPal

Introduction

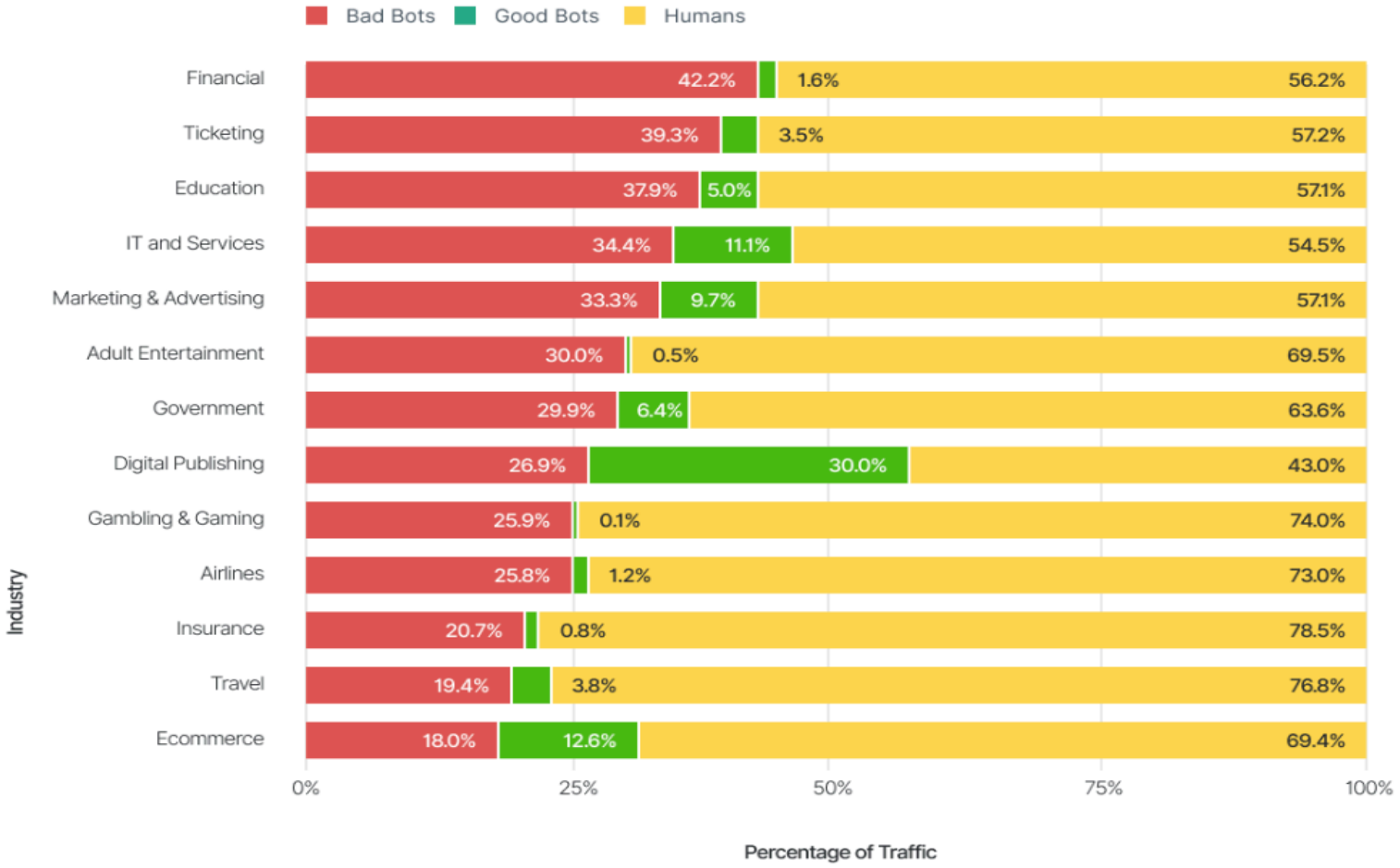


- Impersonators
- Scrapers
- Spammers
- Hacker Tools

- Monitoring Bots
- Commercial Crawlers
- Search Engine Bots
- Feed Fetchers

Source: Internet

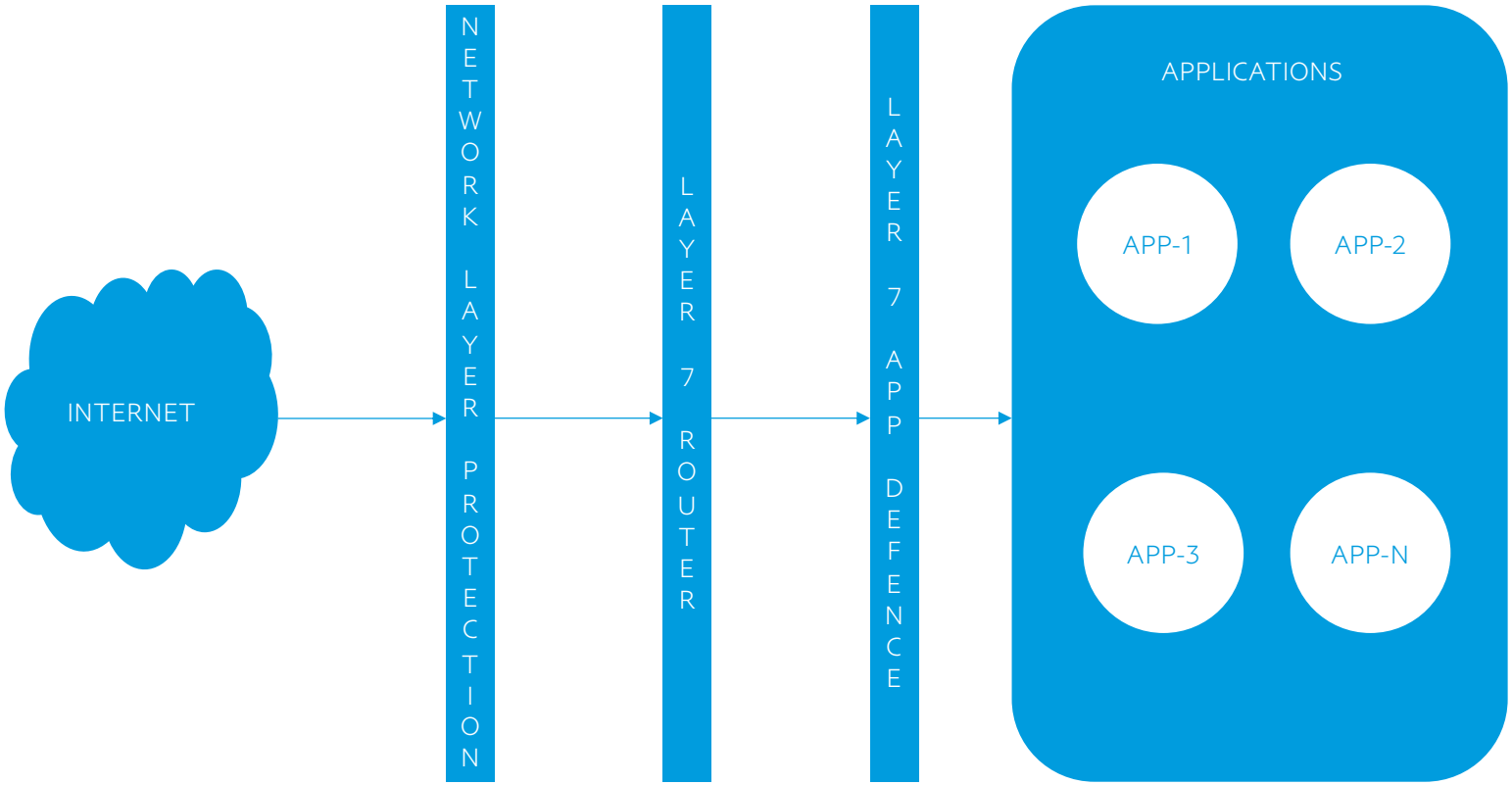
Introduction



PayPal

Source: Internet

Layer 7 Application Defense



PayPal

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

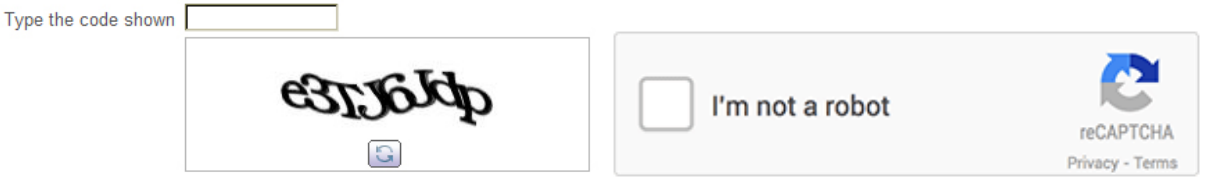
- HTTP pattern (WAF)
  - Pattern based on request parameters
  - Mandatory / missing request parameters
  - Order of headers
- Rate/Velocity
  - Low-flying attack
  - Burst attack
- Reputation Feed
  - Bad/Suspicious IPs
- Unverified device
- Machine Learning

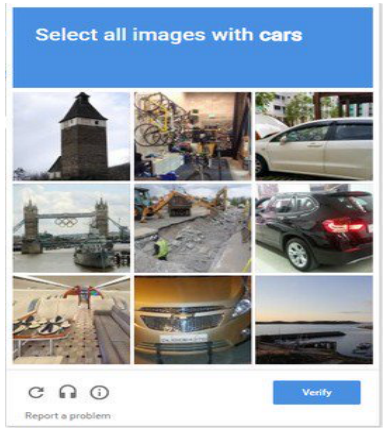
Mitigation Strategies

- Block



- Captcha
  - Visible





  - Invisible

- Tarpit

PayPal

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