PANTHEON

Robot Attack!

Repelling Bots, DDOS, and other Fiends

BADCamp 2015

MEET YOUR GUIDES

Jessi Fischer

Enterprise Onboarding Manager - Pantheon

Suzanne Aldrich

Solutions Engineer - CloudFlare

AGENDA

Surveying Robots

Detecting Attacks

Evading Spam

Withstanding High Traffic

Questions

GLOSSARY

Spam - Unsolicited advertising posted on a blog or sent via email

Phishing - Attempted theft of data or takeover of accounts

Malware - Software designed to be malicious

Robot - Automated software designed to perform functions repeatedly

DDoS - Attempt to make a server or network resource unavailable to Internet users

WAF - Web Application Firewall

DNS - Domain name system answers queries with IPs

OSI - Open System Interconnection Model

- **Layer 3 & 4** - Network and Transport layers (IPv4 & IPv6, TCP, UDP)
- **Layer 7** - Application layer (Chrome, Firefox)

HISTORY OF THE ROBOT

Internet bot:

- Robot, WWW bot, bot, botnet, zombies
- Automated scanning of website resources at high rate
- Good bots: Web spiders
  - Googlebot
  - MSNBot/Bingbot
  - Baidu
  - Yandex
  - Pingdom

Drupal's `robots.txt`

https://api.drupal.org/api/drupal/robots.txt/7

```
User-agent: *

Crawl-delay: 10

Disallow: /includes/

Disallow: /CHANGELOG.txt

Disallow: /cron.php

Disallow: /install.php

Disallow: /update.php

Disallow: /xmlrpc.php
```

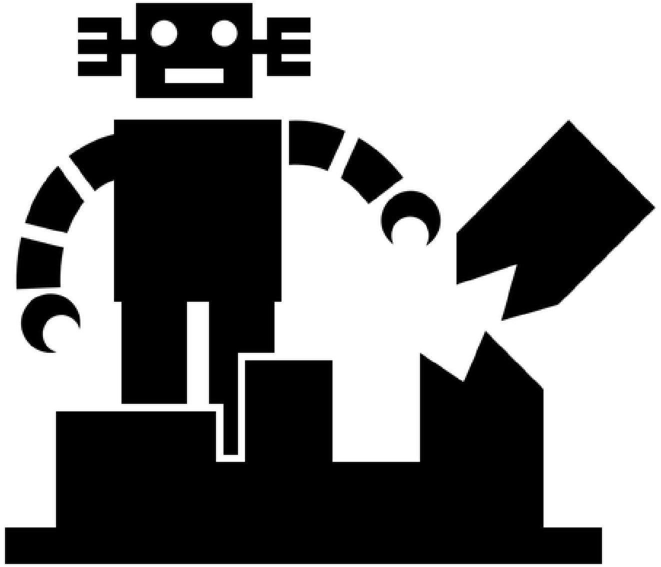
BAD BOTS

Bad bots:

- Spambots - advertising links
- Email harvesters
- Downloaders & scrapers
- Referral & click fraud
- Rogue spiders
  - MegaIndex:

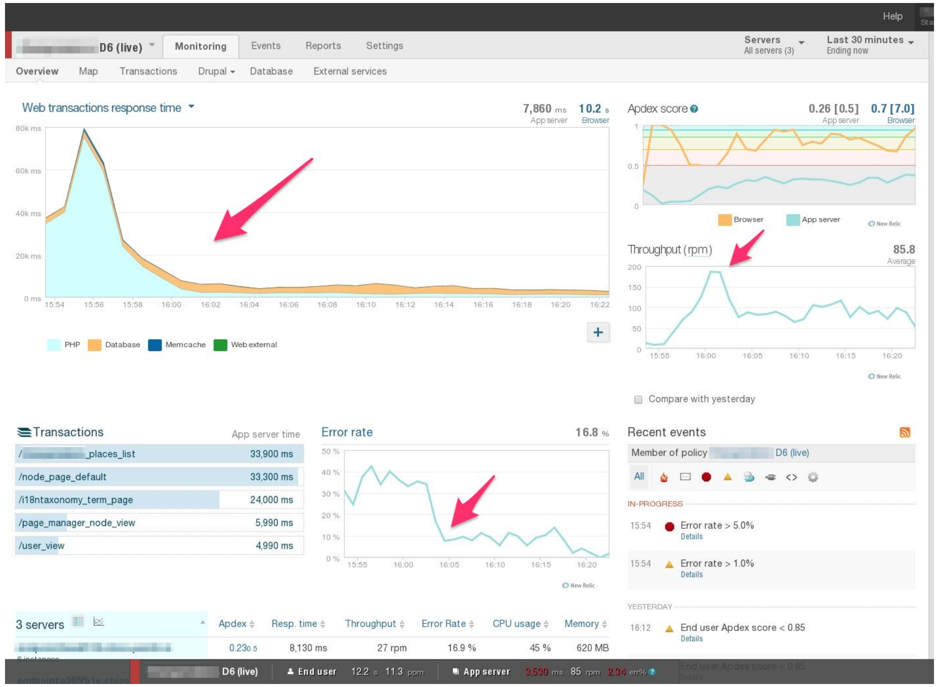
```
Mozilla/5.0 (compatible; MegaIndex.ru/2.0; +https://www.
megaindex.ru/?tab=linkAnalyze)
```

- Infectious agents
- Botnets & zombies



Created by Angela Dinh
from the Noun Project

DETECTING ATTACKS



```
 Id        Date            Severit  Type
Message
 3161818  16/Jun 16:45  notice   spambot
Blocked registration: email=supplyweqz@gmail.
com,ip=120.43.21.95
 3161817  16/Jun 16:45  notice   user
Login attempt failed for JulianHut.
 3161794  16/Jun 16:44  notice   user
Login attempt failed for Julianml.
```

EVADING SPAM

Common SPAM Defense Methods:

- CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart
- Timegate (Time Difference)
- Honeypot
- Content analysis
- Visitor reputation

Popular Drupal Modules:

CAPTCHA/reCAPTCHA - https://www.drupal.org/project/captcha

https://www.drupal.org/project/recaptcha

Mollom - https://www.drupal.org/project/mollom

Honeypot - https://www.drupal.org/project/honeypot

Antispam - https://www.drupal.org/project/antispam

Spambot - https://www.drupal.org/project/spambot

CloudFlare - https://www.drupal.org/project/cloudflare

Spam prevention - https://groups.drupal.org/node/77093

ANTI-SPAM STRATEGIC PITFALLS

Problems with CAPTCHA:

- Cookies prevent anonymous caching
  - High traffic sites require edge cache
- Usability
  - Inconvenient
  - Barrier
- Accessibility
  - Visual impairment

Problems with External APIs:

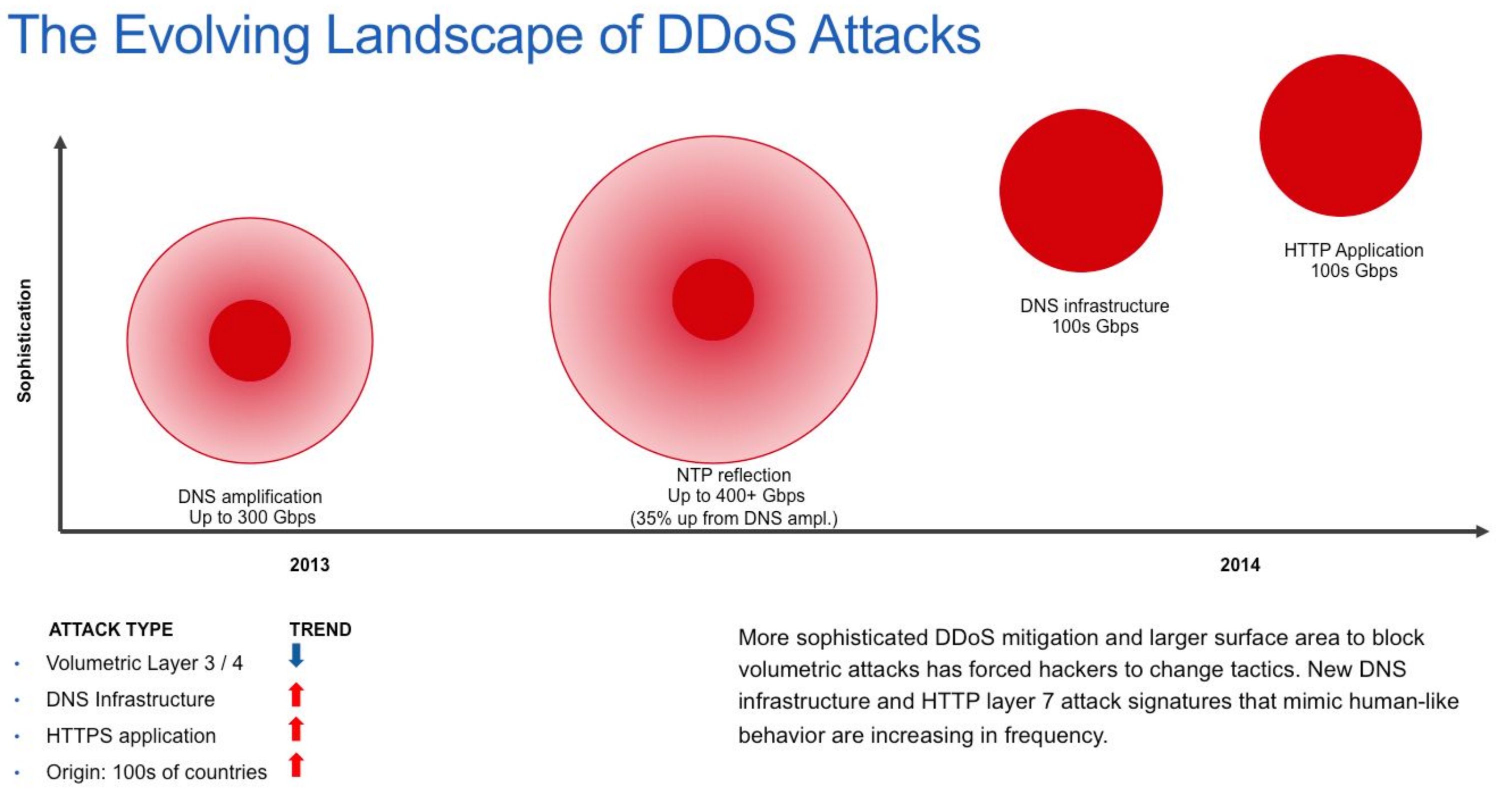
- 3rd party dependency
- Availability & rate limiting
- CAPTCHA fallback
- Cost of service
- User Privacy

WITHSTANDING HIGH TRAFFIC

- Poor performance + bots = downtime
- Server and log monitoring
- Fix site errors in module code and theme templates
- Anonymous page caching
- Views query and rendered results caching
- Dedicated cacheserver - Redis
- Disable comments/cookies/statistics
- Setup CDN for serving assets
- Block IPs at firewall
- Withstand many Layer 7 attacks

```
$ curl -Ik http://www.example.
com/comment/reply/12345

...

X-Varnish: 3649165893

Age: 0

Via: 1.1 varnish

Connection: keep-alive

Vary: Cookie, Cookie
```

DDOS PROTECTION



The Evolving Landscape of DDoS Attacks

ATTACK TYPE	TREND
Volumetric Layer 3 / 4	⬇
DNS Infrastructure	⬆
HTTPS application	⬆
Origin: 100s of countries	⬆

More sophisticated DDoS mitigation and larger surface area to block volumetric attacks has forced hackers to change tactics. New DNS infrastructure and HTTP layer 7 attack signatures that mimic human-like behavior are increasing in frequency.

Types of DDoS Attack:

- DNS Amplification - Layer 3 and 4
- DNS Flood - Layer 3 and 4
- SYN Flood - Layer 3 and 4
- HTTP Application Denial of Service - Layer 7

CLOUDFLARE DRUPAL WAF RULES

D0000 - Block Large Requests to xmlrpc.php for Drupal CMS

D0002 - Block requests with odd array arguments

D0001 - Block Requests to xmlrpc.php for Drupal CMS

URIs:

/xmlrpc.php -- most common

/?q=node&destination=node

/blog/xmlrpc.php

/user/login/

HTTP Method:

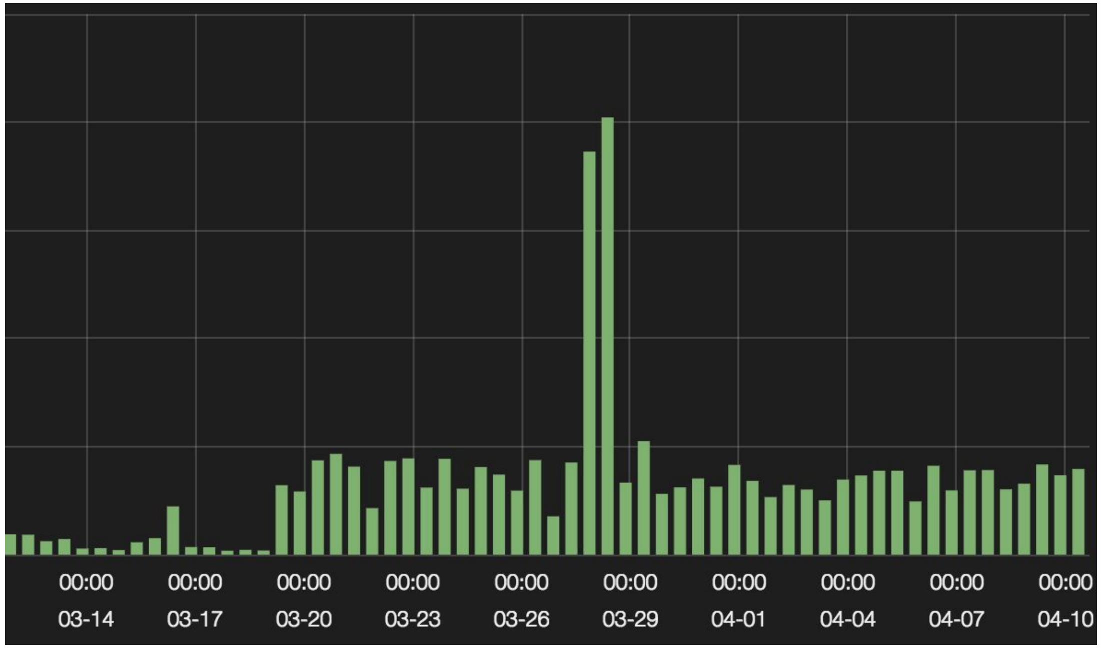
POST -- most common

GET

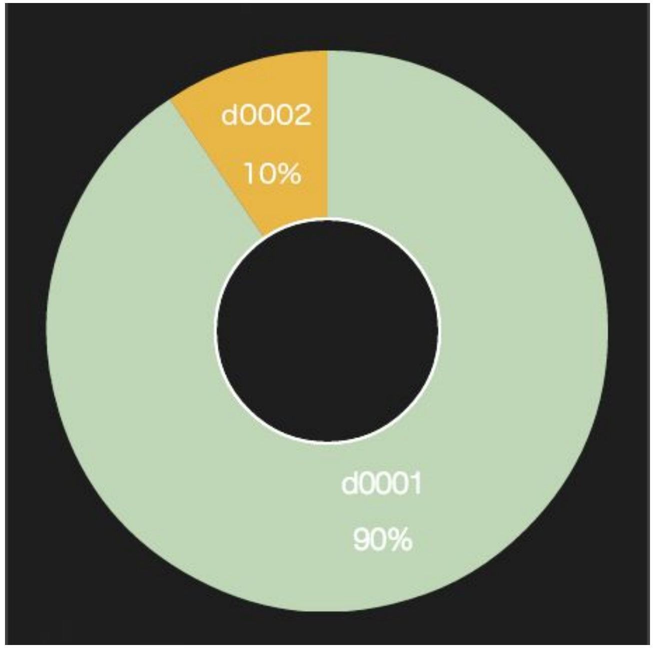
```
10.223.224.238 - - [05/Feb/2015:23:34:47 +0000]  "POST /xmlrpc.
php HTTP/1.1" 404 5377 "-" "Mozilla/4.0 (compatible: MSIE 7.0;
Windows NT 6.0)" 0.251 "5.189.129.224, 108.162.254.28,
10.183.251.3"

10.223.224.238 - - [05/Feb/2015:23:34:47 +0000]  "GET /feed/
HTTP/1.1" 200 6354 "http://example.com/feed/" "SimplePie/1.3.1
(Feed Parser; http://simplepie.org; Allow like Gecko)
Build/20140407093003" 0.201 "54.216.178.194, 141.101.98.27,
10.183.251.3"

10.223.193.24 - - [05/Feb/2015:23:34:47 +0000]  "POST /xmlrpc.
php HTTP/1.1" 404 5377 "-" "Mozilla/4.0 (compatible: MSIE 7.0;
Windows NT 6.0)" 0.233 "5.189.129.224, 108.162.254.28,
10.183.251.3"
```

CLOUDFLARE DRUPAL WAF TRIGGERS

Frequency of WAF Triggers Over 30 Days



Percentage of Triggers by WAF Rule



Q&A

PANTHEON

CLOUDFLARE®