



Identify Early Warning Signs of Bot Attacks and What to Do About Them

August 2020

Presenters



Sumit Bahl

Cloudflare: Product Marketing



Jon Lunsford

ConvertKit: Software Engineering

ConvertKit:

We exist to help creators earn a living online.

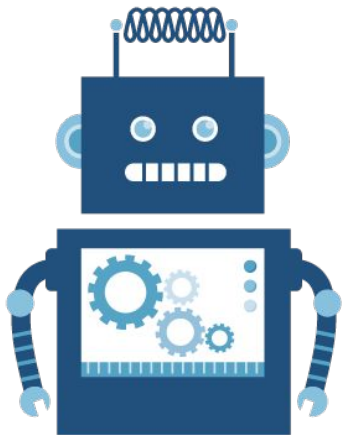
What's a creator? A creator might be a blogger, author, maker, YouTuber, poet, painter, musician, podcaster, chef, designer, or teacher. What binds the creators we serve together is that they make a living doing work that matters, and they earn that living online.

We provide tools to automate your email marketing, grow your audience and to help understand their engagement.

Me:

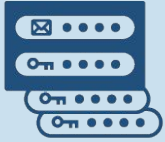
Lead engineer on ConvertKit's compliance team. My team is responsible for managing our exposure to risk, abuse and responding to threats in real time. We provide expertise to our customer's as well as support them technically to provide a best in class service.

What are bots



- Automated program designed to perform specific task
- Execute tasks over and over at a much faster rate than humans
- Good bots needed by businesses for SEO
- Bad bots impact business
 - Brand reputation
 - Financial
 - Security

Bad bots - use case



Credential Stuffing

Take-over of user's account from automatically applying previously stolen account credentials.



Inventory Hoarding

Fraudulently purchase goods to deprive legitimate customers or resell for a higher price



Content Scraping

Scraping and stealing information from a website



Credit Card Stuffing

Attempts to validate stolen credit cards to then make fraudulent purchases



Content Spam

Adding malicious content to web properties such as forums and registration forms



Application DDoS

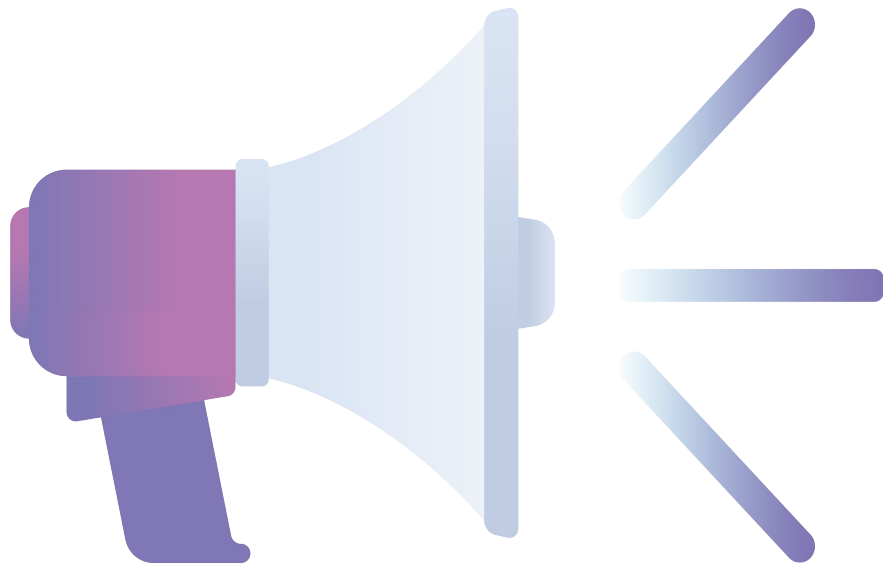
Slowing sites, wasting bandwidth and compute resources

Warning signs of bot attack

#1 - Higher infrastructure costs with no increase in business



#2 - Increased customer complaints



#3 - Increase in failed login attempts



#4 - Skewed page-view analytics



5 - Sudden increase in account creation



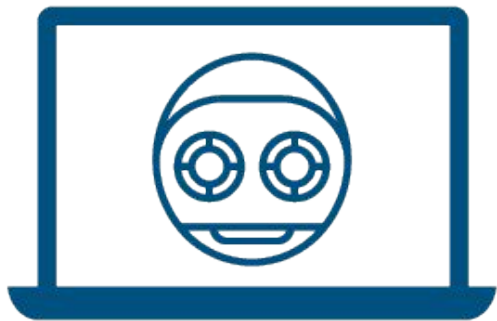
#6 - Traffic originating from unusual geographic locations at unusual time



#7 - Increase in card validation failures



Overview of early signs of bot attacks



- Higher infrastructure costs with no increase in business
- Increased customer complaints
- Increase in failed login attempts
- Skewed page-view analytics
- Sudden increase in account creation
- Traffic originating from unusual geographic locations a
- Increase in card validation failures

What to do with bad bots



- Block bad bots as soon as you catch them
- Whitelist all the good bots you're aware of
- Challenge suspected bots you detect
- Keep detailed logs of all site traffic
- Additional authentication

Monitoring Examples at ConvertKit

Forms: Average Bot Score



Overall Avg Bot Score (0 = bot)

Forms: Total Visits

252,300
Visits

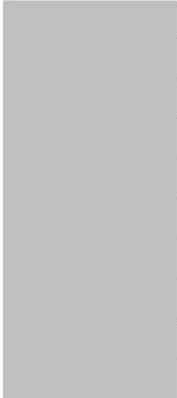
Forms: Quarantined vs Dropped Count

27,797	1,269
Quarantined - Count	Dropped - Count

High level metrics to help add context. These may be quick indicators of current issues requiring action.


Monitoring Examples at ConvertKit

Forms API: Submissions made by integrations (outside of CK bot protection)

Ip Address ▾	Form Submissions ▾
	396,476
	81,114
	43,887
	33,702
	31,202
	26,714
	23,023
	22,993
	21,676
	14,175

Export: [Raw](#)  [Formatted](#) 

Forms: IP Requests

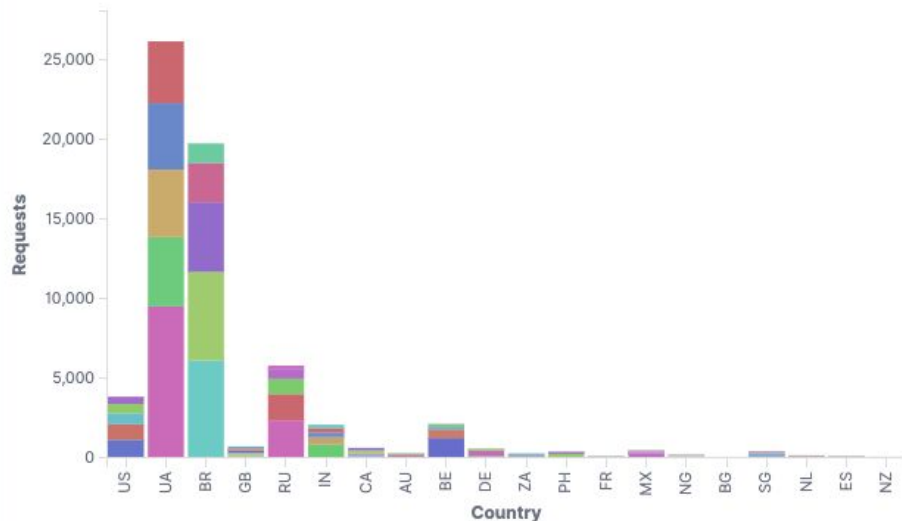
Ip Address ▾	Country ▾	Region ▾	Total Requests ▾
	UA	Crimea	51,126
	RU	Krasnodarskiy Kray	4,969
	BG	Sofia-Capital	1,455
	GB	England	1,126
	US	New York	897
	US	New Jersey	20
	DE	Hesse	525
	US	Ohio	360

Export: [Raw](#)  [Formatted](#) 

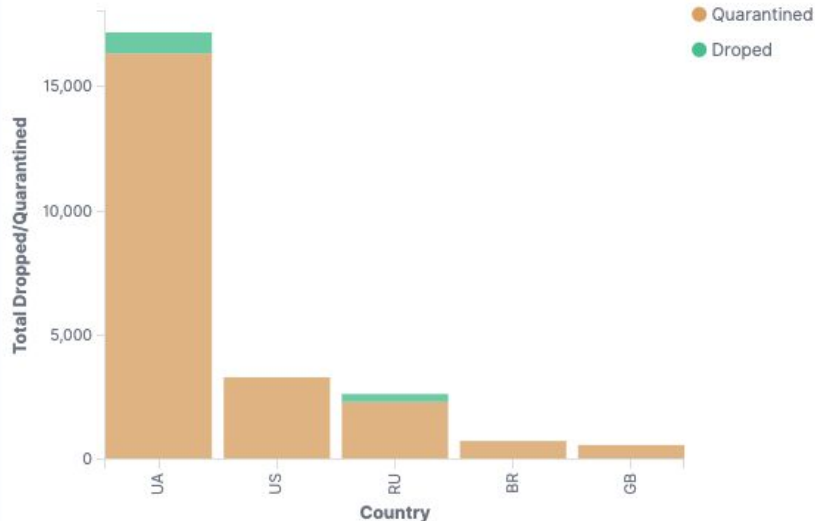
Quick glances at current, potentially problematic, IPs.

Monitoring Examples at ConvertKit

Forms: Requests By Country

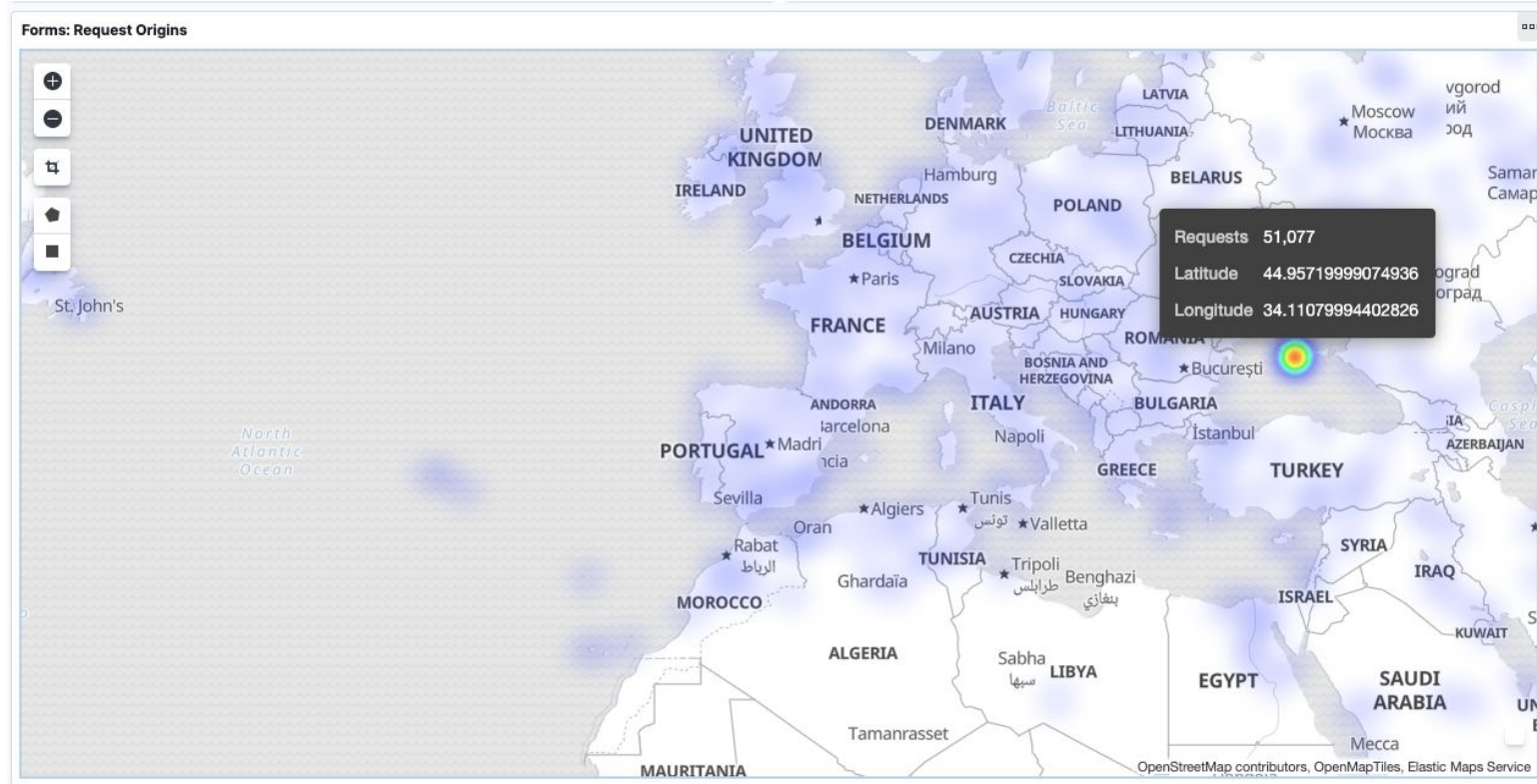


Forms: Country Dropped vs Quarantined



View of which forms or landing pages are potentially experiencing issues. This allows us to detect and mitigate issues quickly. on behalf of our customer's.

Monitoring Examples at ConvertKit



Questions

Advantages of Cloudflare Bot Management

Simple Deployment

- Quick setup
- No JavaScript
- No mobile SDK

Accurate Detection

- Threat intelligence
- Behavioral analysis
- Machine learning
- Fingerprinting

Quick Mitigation

- Alternative content
- Captcha
- Log
- Block

Rich Analytics

- Reports
- SIEM integrations

An integrated global cloud platform

SECURITY



Firewall



IoT Security



Bot Management



DDoS Protection



Zero Trust
Security



SSL/TLS



Secure Origin
Connection



Rate
Limiting

PERFORMANCE



Cache



Intelligent
Routing



Content
Optimization



Mobile
Optimization



Image
Optimization



Mobile SDK

RELIABILITY



Load
Balancing



Anycast
Network



Virtual
Backbone



Domain
Name System
(DNS)



DNS
Resolver



Always
Online

PLATFORM



Serverless Compute



Cloudflare Apps



Analytics

Duplicates of your content on non-approved sites



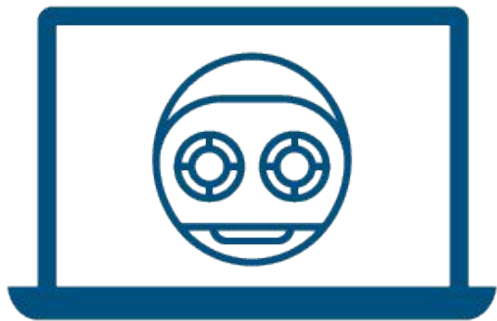
Low yield on advertising spend



Unusual purchases of low-volume, high-demand inventory



Overview of early signs of bot attacks



- Higher infrastructure costs with no increase in business
- Increased customer complaints
- Increase in failed login attempts
- Skewed page-view analytics
- Sudden increase in account creation
- Traffic originating from unusual geographic locations
- Increase in card validation failures
- Low yield on advertising spend
- Duplicates of your content on non-approved sites
- Unusual purchases of low-volume, high-demand inventory

What to do with bad bots



- Block bad bots as soon as you catch them
- Whitelist all the good bots you're aware of
- Challenge suspected bots you detect
- Redirect bots to alternative content
- Slow the bad bots
- Additional authentication