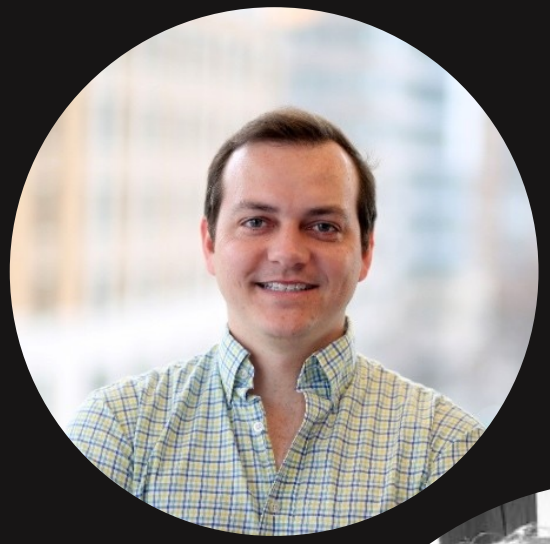
GREYNOISE

INTELLIGENCE

Roll Call

- Nate T
  - Researcher
  - nate@greynoise.io
- Daniel G
  - Data Scientist
  - daniel@greynoise.io
- Matt L
  - Engineer/Researcher
  - matt@greynoise.io
- General
  - hello@greynoise.io



Agenda

- GreyNoise Overview
- Infrastructure
  - Current and future
- What we see

Pitch Perfect

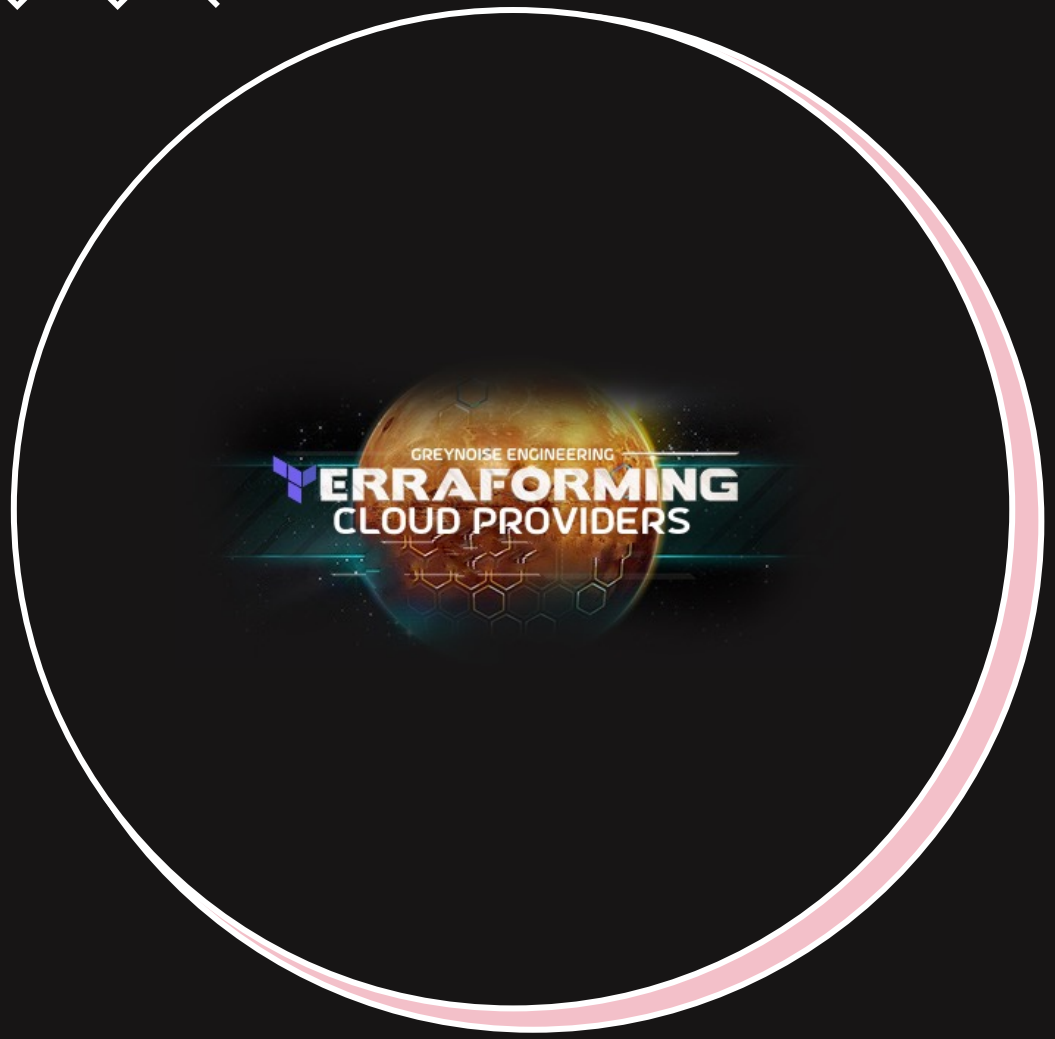
Analyst Efficiency	Compromised Devices	Emerging Threats
• Ignore noise • Add context for IPs	• Monitor your assets • Find your devices that are scanning • Usually Bot related	• New exploits • Who is scanning

Internet of Listening Things

- 13 providers
  - AWS, GCP, Azure, Alicloud, Linode, Digital Ocean, etc…
- ~700 unique sensors
  - Don’t get to choose IPs
  - Cycled
- 3 types of sensors
  - Rorschach
    - Hoping to open source soon®
  - HTTP (deprecated)
  - Windows
    - Proprietary protocols…

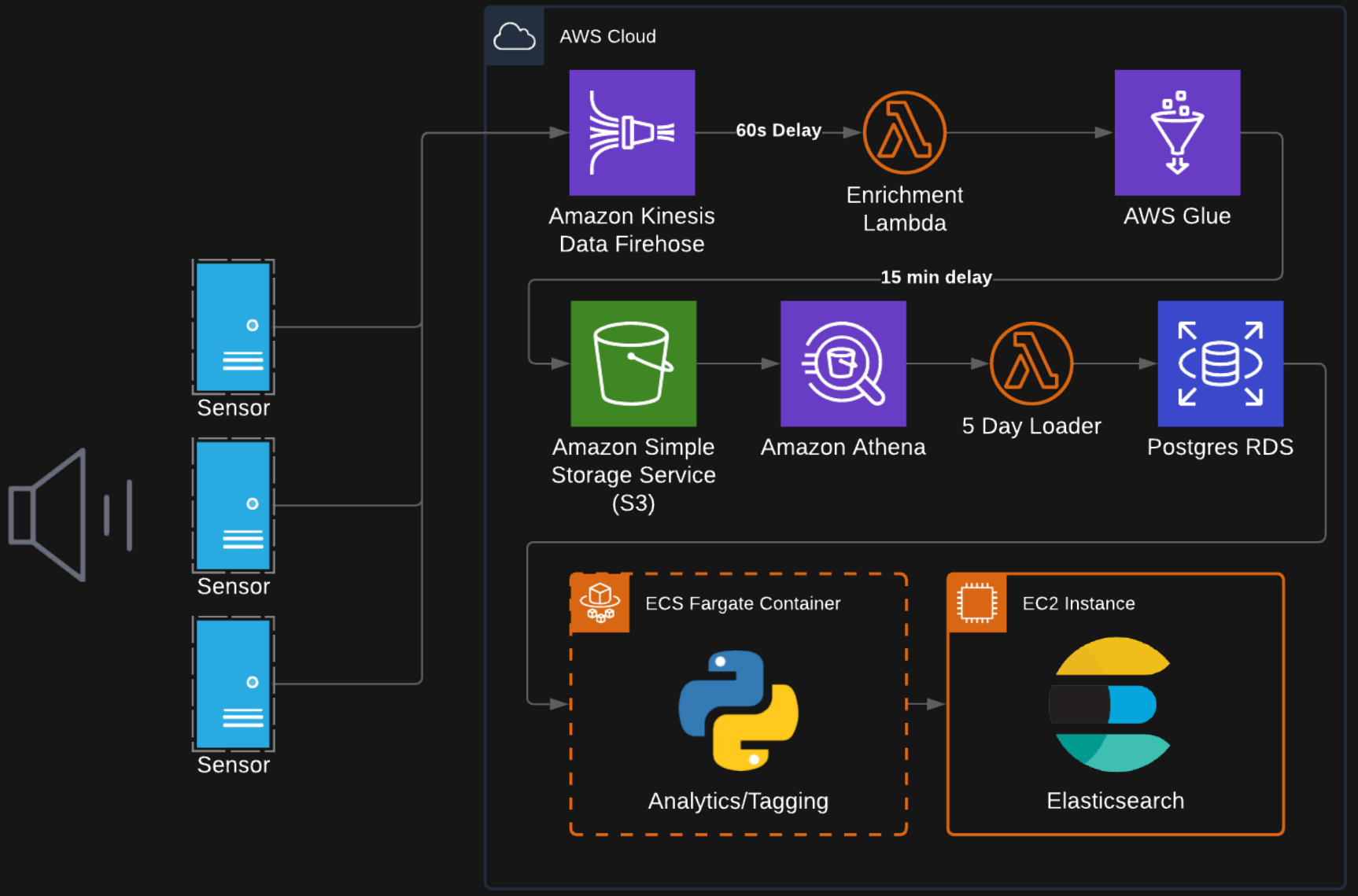
Little Phish, Big Data Lake

- ~2000 hits per sensor
  - Varies highly based on sensor, provider, region, etc…
- 150-200k Unique IPs per day
  - Varies by provider quite a bit
  - Larger providers see more
- Working to better characterize volume
- Nothing close to what CAIDA is seeing in terms of volume
- Collect traffic content and do manual analysis
  - Looking to for ways to automate this



Terraforming Clouds

- Infrastructure-as-Code (IaC)
  - Terraform, Go, GitHub CI
  - Amazon Data Lake
- Each cloud provider has different rules
  - This makes sensor deployments tricky
- “Random” IP Assignment
  - Sets of three


AWS Cloud
Amazon Kinesis Data Firehose
60s Delay
Enrichment Lambda
AWS Glue
15 min delay
Amazon Simple Storage Service (S3)
Amazon Athena
5 Day Loader
Postgres RDS
ECS Fargate Container
Analytics/Tagging
EC2 Instance
Elasticsearch
Sensor
Sensor
Sensor

A Tale of Two DBs

- PostgreSQL
  - \x03\000\000/*\340\000\000\000\000\000Cookie: mstshash=Administr\r\x01\000\x08\000\x03\000\000\000
- Athena
  - /*Cookie: mstshash=Administr%d$ "

select * from rorschach limit 11;

timestamp	source_ip	sensor_uuid	data_escaped	data_hex
2021-07-09 22:21:06.000	125.227.149.119	3db1ec55-9132-463b-5436-b3705fd75f6b		
2021-07-09 22:22:21.000	177.42.162.207	a3c351e9-522d-b0cb-2627-f4f6f0ae1aa4	E◆SMBr ◆◆◆" NT LM 0.12 SMB 2.002 SMB 2.???	00000045FF534D4272000000001801C800000000000
2021-07-09 22:21:45.000	138.68.164.226	66c70f23-4803-688d-99f4-e25eefd6cae3	+&◆Cookie: mstshash=hello	0300002B26E00000000000436F6F6B69653A206D73
2021-07-09 22:21:10.000	91.191.209.30	f1785c37-b549-95e2-f2b5-68590ff1e71c	/*◆Cookie: mstshash=Administr % ◆d ◆p◆ ◆ $ ◆ ◆	0300002F2AE00000000000436F6F6B69653A206D73
2021-07-09 22:21:07.000	112.158.130.222	f7888abf-f230-216e-34c3-5693bba9e430	BitTorrent protocol x◆G◆&◆◆◆ ◆3P◆ ◆O◆^-LT11D0-iyZnOQQk4m!r	13426974546F7272656E742070726F746F636F6C0000
2021-07-09 22:21:10.000	123.160.221.52	79e68406-4a3e-e5ca-20fa-1eb47fbae215	B◆ Z=◆◆l◆◆◆◆◆◆◆k◆◆6◆jJ 9x◆K ◆◆◆+ xWL9H {ᴘ◆◆◆◆*◆,n◆[4 ◆)◆◆◆◆f◆-◆ =E◆◆◆◆ & h}t◆"a T◆(◆ wqʊ ◆9w◆◆*}◆◆◆3.◆^F ◆◆◆◆A◆ ◆=ƀl◆f@◆G◆◆◆Hy .◆ ◆◆◆◆ ◆\◆◆C◆◆◆)/K4◆◆e◆RLy	1703030142ED1E5A3DEF92D46CFEBCB18299D5EE6BD
2021-07-09 22:21:11.000	192.241.221.94	c81d0b29-fa94-3c93-4d7a-b0b2eb884552	GET / HTTP/1.1 Host: [redacted] Accept: */* Accept-Encoding: gzip User-Agent: Mozilla/5.0 zgrab/0.x	474554202F20485454502F312E310D0A486F73743A2
2021-07-09 22:21:01.000	192.241.209.157	b8b15603-ee8d-94ce-2174-df437946f3c4	GET / HTTP/1.1 Host: [redacted] Accept: */* Accept-Encoding: gzip User-Agent: Mozilla/5.0 zgrab/0.x	474554202F20485454502F312E310D0A486F73743A2
2021-07-09 22:21:08.000	213.32.122.82	f27d3e90-14f6-693e-ebcb-c64dc9336264	GET / HTTP/1.1 Host: [redacted] Connection: close Connection: close User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36	474554202F20485454502F312E310D0A486F73743A2
2021-07-09 22:21:07.000	118.137.195.105	f7888abf-f230-216e-34c3-5693bba9e430	d1:ad2:id20:◆◆7aY◆g◆Q◆◆6q[◆◆◆9:info_hash20:◆◆7◆_◆◆ O◆, ◆/syA,◆e1:q9:get_peers1:t2:{◆1:v4:LT .1:y1:qe	64313A6164323A696432303A90A6376159EDA59767E
2021-07-09 22:21:07.000	36.228.40.194	f7888abf-f230-216e-34c3-5693bba9e430	◆◆ ◆ ◆◆ >ay◆◆◆◆i◆F◆u◆◆◆0e ◆ ◆◆;◆o6◆٩◆ ◆@(ļ V▤◆◆F◆◆So DV◆ ◆J◆W◆◆◆`& ◆◆◆ ◆◆ų ◆O◆◀	828F1EEA0A10ADA71C3E6179BAA5B2F06998469F75C

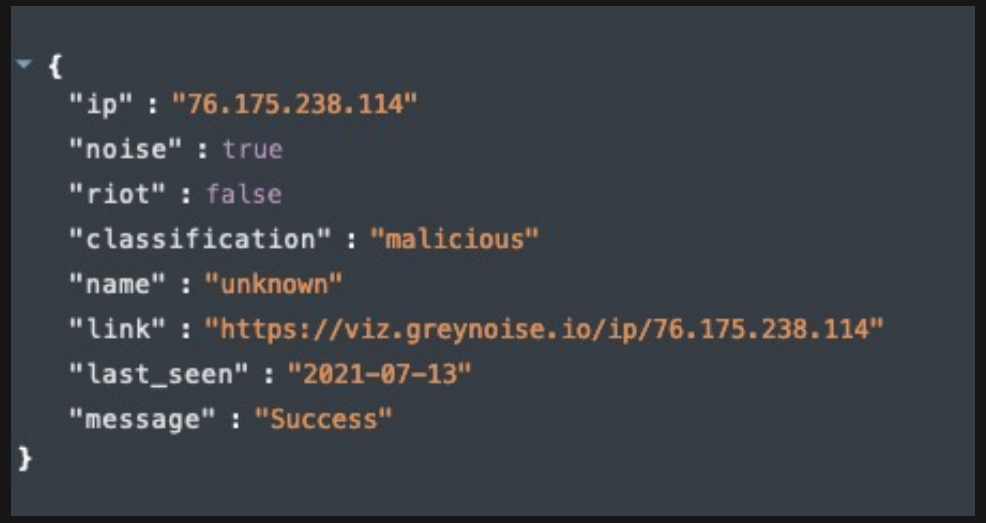
Perfect Practice Makes Perfect

- The Good
  - SQL Search
  - Fingerprinting/Tagging
  - Anecdotally successful ☺
- The Bad
  - Reinventing the wheel
    - Suricata
    - Wireshark
  - Temporal analysis
  - UDP
  - Lack of scientific rigour
- The Ugly
  - Scaling
  - Batch jobs
  - Cost
  - Spoofing

API Data

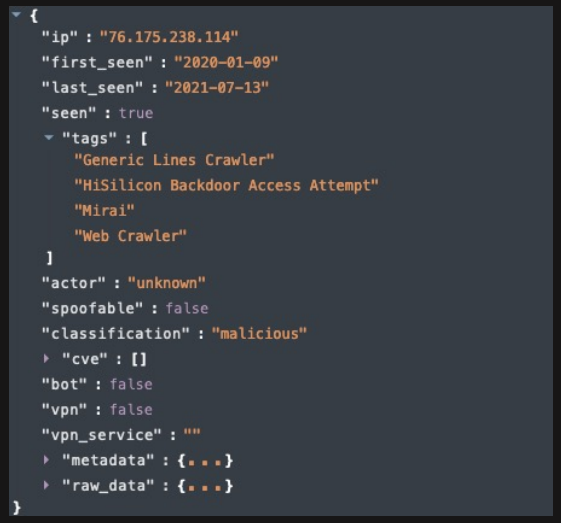
Community

- https://developer.greynoise.io/reference/community-api



IP Lookup

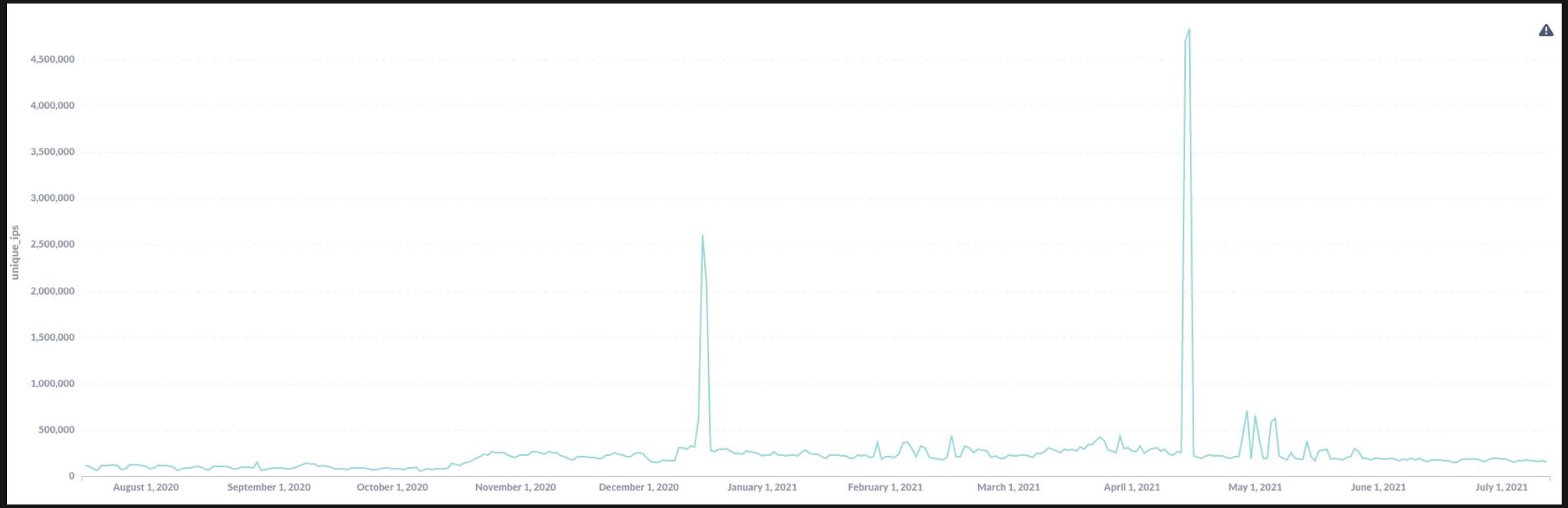
- https://developer.greynoise.io/reference/ip-lookup-1#noisecontextip-1



CAIDA

- Need to grok the scale
  - Costly
  - Massive
- Need to check the overlap
  - Blocklisted ranges in code?
- What is truly opportunistic?

NOISEGATE


unique_ips
4,500,000
4,000,000
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
August 1, 2020
September 1, 2020
October 1, 2020
November 1, 2020
December 1, 2020
January 1, 2021
February 1, 2021
March 1, 2021
April 1, 2021
May 1, 2021
June 1, 2021
July 1, 2021

NOISEGATE

SPOOFED

NIMABIJIAN

```
\x01\x00\x00\x00
\xbf\x02\x00\x88\x13\x00\x00\x87\x00\x00\x00NIMABIJI
AN\x04\x03\x00\x00{\x99Caig\x9c\x03\xc7eB\xc5\t\xc1\
x18a\x11\x1a\x91\x1f\x02\tcof\x91\xc0\x80sJ5\xd2\x80
\xe6\x9a~\xb9\xc7\x83^\x96\xeeN\x16\x96\x96&\xe6\x03
\xea\xb
```

Transmitted as ASCII as seen here, including `\x` prefixes for hex characters…

Regional exploits appear to exist.

Contact or Access

- Free access to our Enterprise API for research purposes
  - vip@greynoise.io
- GreyNoise Public Slack
  - https://join.slack.com/t/greynoiseintel/shared_invite/zt-o66ozahe-9gbu_5yv5tQO80~8CL8lBQ
- Twitter
  - https://twitter.com/GreyNoiseIO
- Feel free to email us at hello@greynoise.io or any of the emais listed on earlier slides

END

hello@greynoise.io