# Detecting Blue Team Recon *With Ads*

0x200b

# Disclaimers

*TL;DR plz don’t fire or sue me*

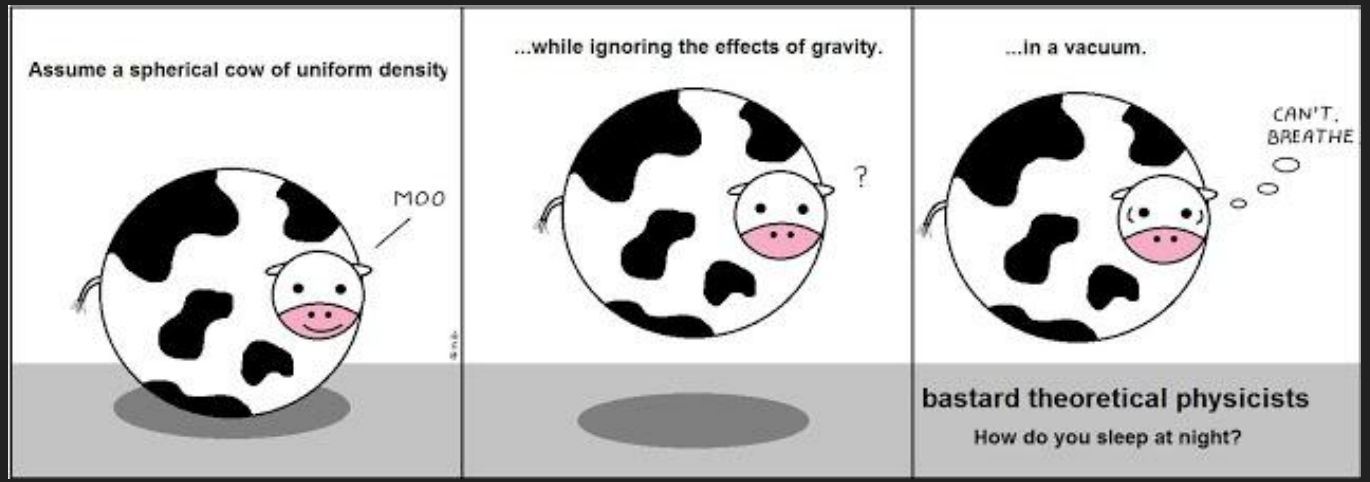
- The views expressed herein do not reflect the views of my current or former employers.
- I am not responsible for any misuse of the information provided nor am I condonding any misuse.

# $whoami?

- Cat pretending to be a human or vice versa
- Classically trained Blue Teamer
  - I’ve made lot of really stupid mistakes
- Using Blue Team mistakes against them ;)

# Caveats

- Target will search for the term
- Target will use a chosen Ad Network
- Ad will register as ‘displayed’ to target



# Backstory

# Problem

- Your Op is your baby
- You worked hard
- You were clever
- Your implant gets discovered

Time to save your baby!

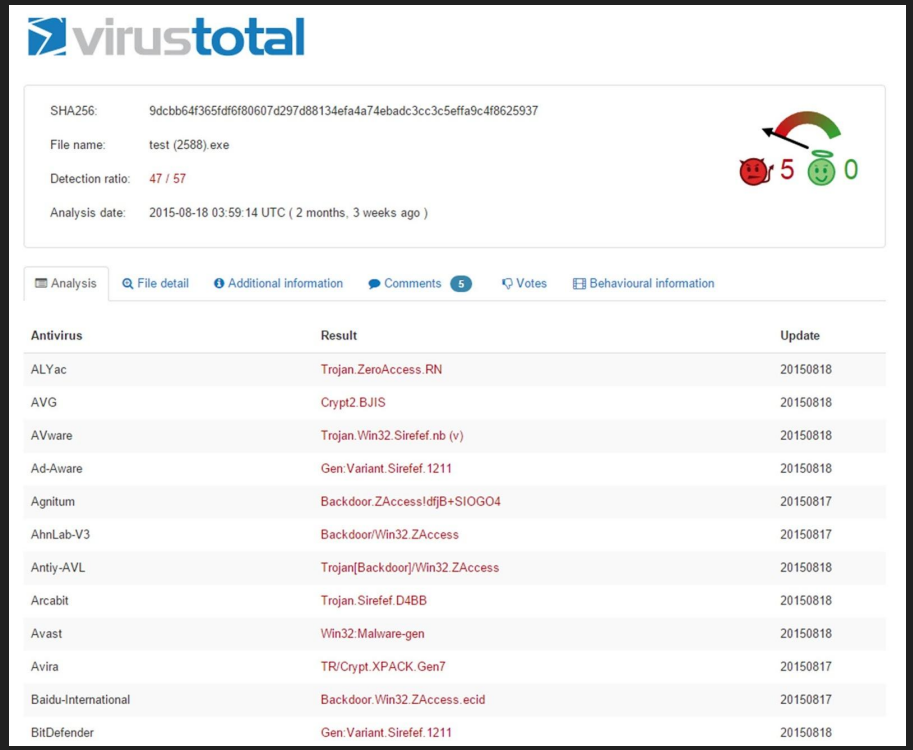


# What IF it gets detected?

- What is a early warning worth?
- What do we care about?
  - Indirect
  - Passive
  - Low effort
- Blue Teams leak tons of info



# Virustotal Uploads




| Antivirus | Result | Update |
|---|---|---|
| ALYac | Trojan.ZeroAccess.RN | 20150818 |
| AVG | Crypt2.BJIS | 20150818 |
| AVware | Trojan.Win32.Sirefef.nb (v) | 20150818 |
| Ad-Aware | Gen:Variant.Sirefef.1211 | 20150818 |
| Agnitum | Backdoor.ZAccess!dfjB+SIOGO4 | 20150817 |
| AhnLab-V3 | Backdoor/Win32.ZAccess | 20150817 |
| Antiy-AVL | Trojan[Backdoor]/Win32.ZAccess | 20150818 |
| Arcabit | Trojan.Sirefef.D4BB | 20150818 |
| Avast | Win32:Malware-gen | 20150818 |
| Avira | TR/Crypt.XPACK.Gen7 | 20150817 |
| Baidu-International | Backdoor.Win32.ZAccess.ecid | 20150817 |
| BitDefender | Gen:Variant.Sirefef.1211 | 20150818 |

- Blue Team uploads unknown file
- Red Team knows file was found

# Blue Teams are Burnt Out

# The SOC Analyst




- False Positive
- False Positive
- False Positive
- Something Stupid
- False Positive
- False Positive
- Something interesting
- ……...

# Investigation Lifecycle

1. Magic happens
2. Human looks at the Event
3. Initial investigation/determination
4. Escalation to specialist



# Target The Human

Prior to the escalation basic analysis will happen:

- Internal tools
- Vendor products
- Public tools



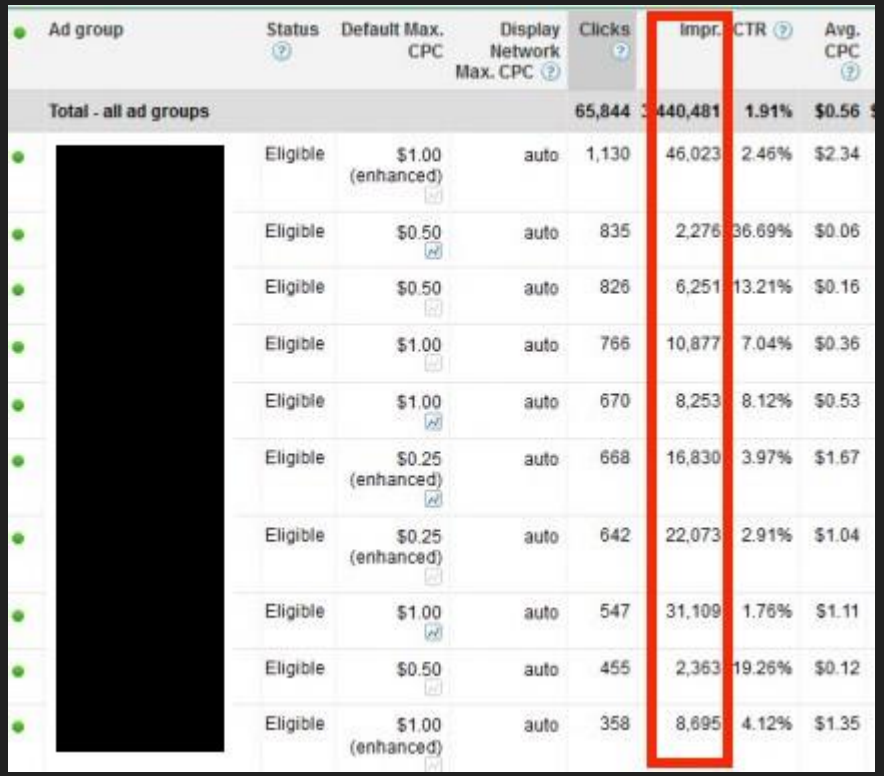
What if I knew when people searched for things?

# Advertising Goals

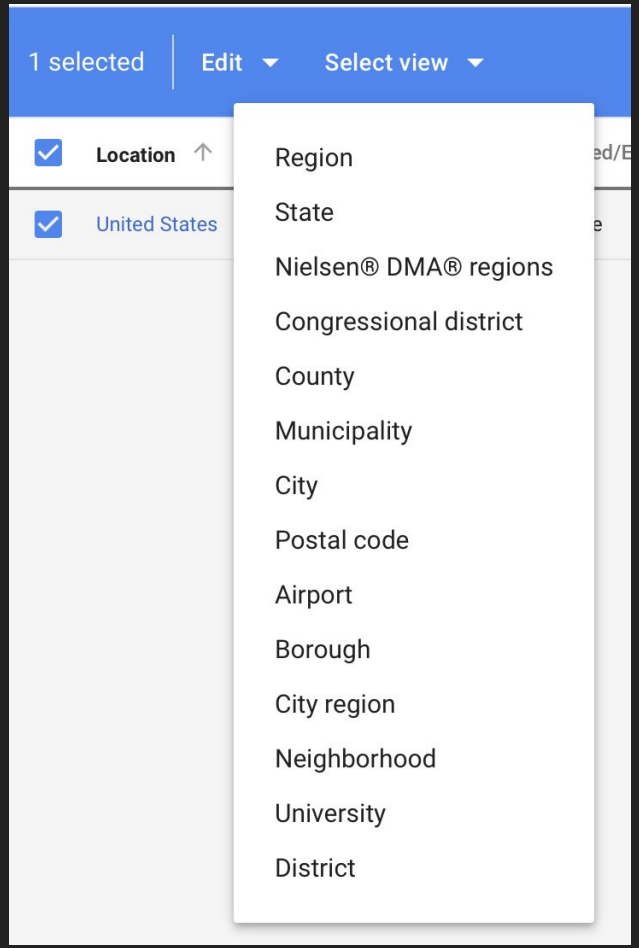
- Show content based on usage
  - Keywords
  - Demographic info
  - Interests
- Give customers tools to tune Ads



# Ad Performance



| Ad group | Status | Default Max. CPC | Display Network Max. CPC | Clicks | Impr. | CTR | Avg. CPC |
|---|---|---|---|---|---|---|---|
| Total - all ad groups | | | | 65,844 | 440,481 | 1.91% | $0.56 |
| [redacted] | Eligible | $1.00 (enhanced) | auto | 1,130 | 46,023 | 2.46% | $2.34 |
| | Eligible | $0.50 | auto | 835 | 2,276 | 36.69% | $0.06 |
| | Eligible | $0.50 | auto | 826 | 6,251 | 13.21% | $0.16 |
| | Eligible | $1.00 | auto | 766 | 10,877 | 7.04% | $0.36 |
| | Eligible | $1.00 | auto | 670 | 8,253 | 8.12% | $0.53 |
| | Eligible | $0.25 (enhanced) | auto | 668 | 16,830 | 3.97% | $1.67 |
| | Eligible | $0.25 (enhanced) | auto | 642 | 22,073 | 2.91% | $1.04 |
| | Eligible | $1.00 | auto | 547 | 31,109 | 1.76% | $1.11 |
| | Eligible | $0.50 | auto | 455 | 2,363 | 19.26% | $0.12 |
| | Eligible | $1.00 (enhanced) | auto | 358 | 8,695 | 4.12% | $1.35 |

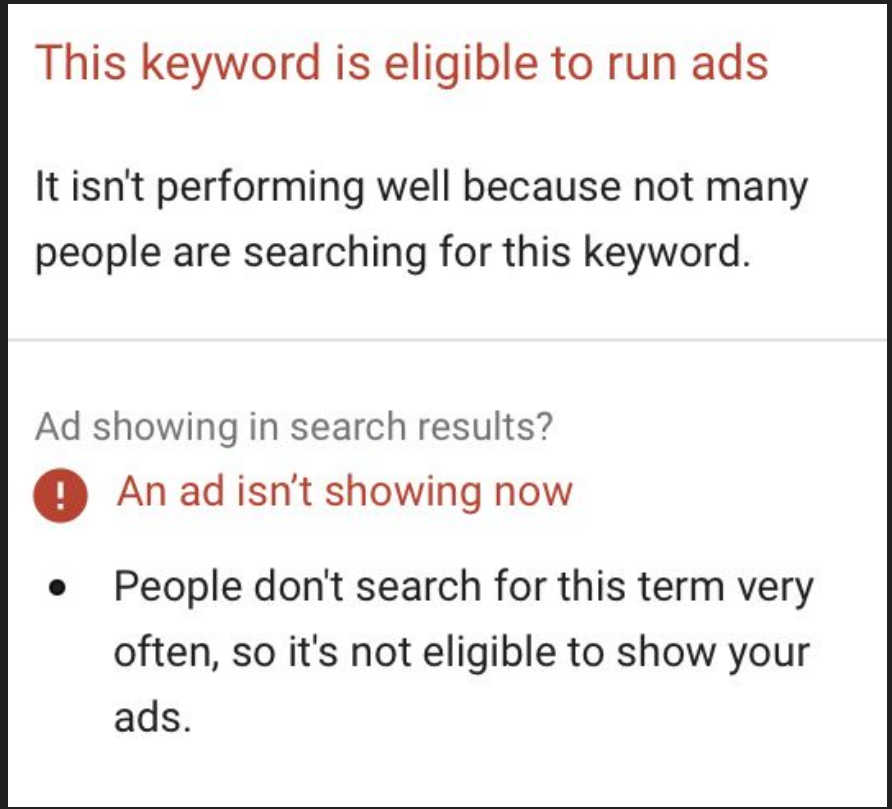


# Is It Possible?

Yes, but...

# Advertising limitations

- Search volume
  - People need to be searching
- Search results
  - There must be something to find



# OPSEC Considerations

- Payment Information
  - Credit Card
  - Address
  - Phone Number
  - Email
- Search results
  - Must be indexed



# Let’s Do It!

# What type of Ad?



- Search Keyword Match
  - Broad
  - Phrase
  - Exact
- Display/Mail/Video Ads
- Bid Strategy

# Other Keyword Possibilities

- Any unique string
  - Author handle
  - Email address
  - Unique File Name
  - Misc. Phrase



# Picking your Keyword(s)

**Do**

- Something unique
  - Low Search Volume
- Keep it simple
- Tailor to your target

**Don’t**

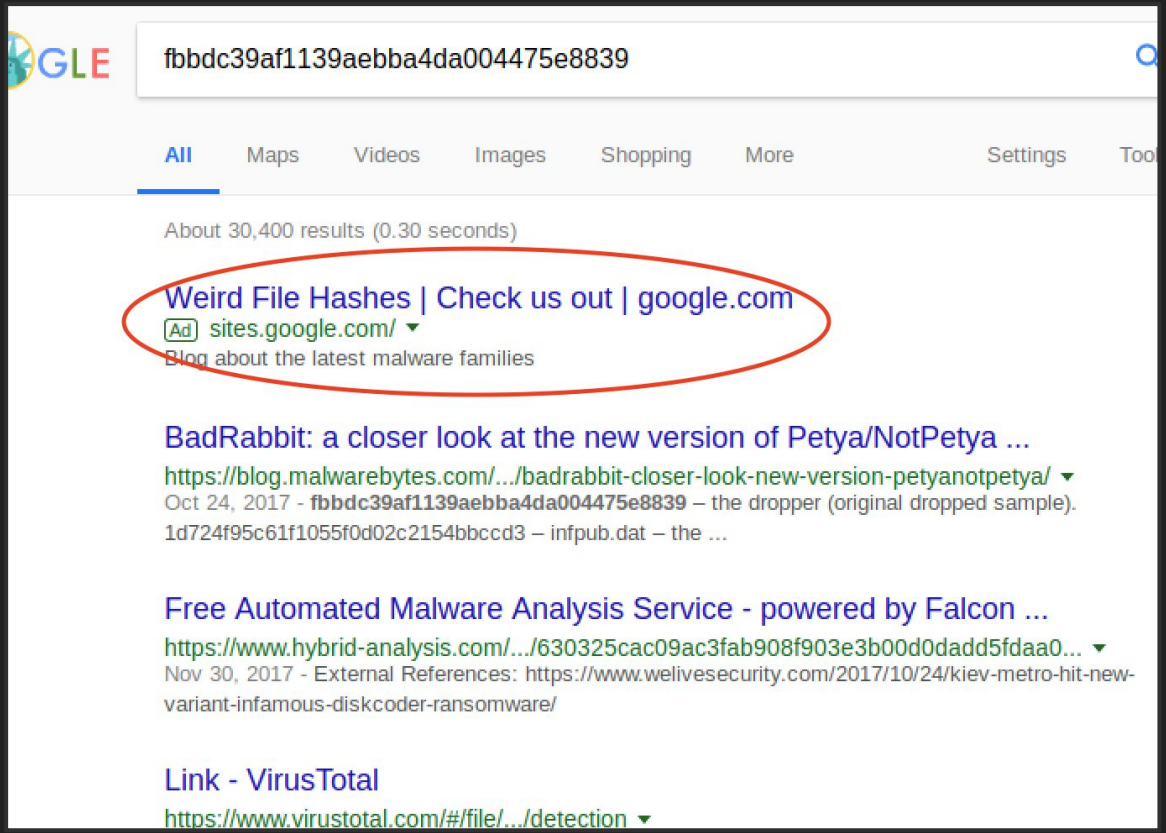
- Use Generic Terms
  - Minimize False Positives
- Complex Ideas
- Domains or IPs

# Example

- AdWord for a Google search of a specific Keyword
- Traffic and results already generated
  - Maximize clicks
  - High bid for Click

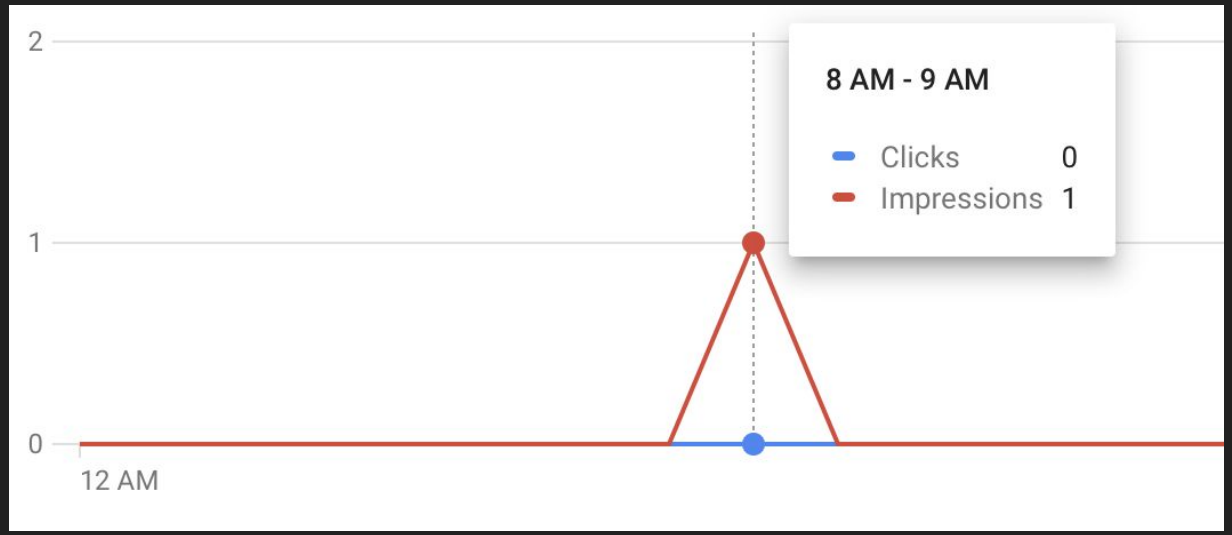


# YEY!


GLE
fbbdc39af1139aebba4da004475e8839
All
Maps
Videos
Images
Shopping
More
Settings
About 30,400 results (0.30 seconds)
Weird File Hashes | Check us out | google.com
Ad sites.google.com/
Blog about the latest malware families
BadRabbit: a closer look at the new version of Petya/NotPetya ...
https://blog.malwarebytes.com/.../badrabbit-closer-look-new-version-petyanotpetya/
Oct 24, 2017 - fbbdc39af1139aebba4da004475e8839 – the dropper (original dropped sample).
1d724f95c61f1055f0d02c2154bbccd3 – infpub.dat – the ...
Free Automated Malware Analysis Service - powered by Falcon ...
https://www.hybrid-analysis.com/.../630325cac09ac3fab908f903e3b00d0dadd5fdaa0...
Nov 30, 2017 - External References: https://www.welivesecurity.com/2017/10/24/kiev-metro-hit-new-variant-infamous-diskcoder-ransomware/
Link - VirusTotal
https://www.virustotal.com/#/file/.../detection

# Usability

- Slight Delay
  - Google says 3 hours
- AdWords API
  - Basic CSV




```
Search keyword,Campaign,Ad group,Clicks,Impressions,CTR,Avg. CPC,Cost,Avg. position,Conversions,View-through conv.,Cost / con
v.,Conv. rate
cb295b4d20c0c0f13ce187f7f18f6e6c27e99cbc,Campaign #1,Hash #1,0,0,0.00%,$0.00,$0.00,0.00,0.00,0,$0.00,0.00%
fbbdc39af1139aebba4da004475e8839,Project Tacet,Ad Group #1,0,1,0.00%,$0.00,$0.00,1.00,0.00,0,$0.00,0.00%
fbbdc39af1139aebba4da004475e8839,Mobile Only,Mobile Ad Group #1,0,0,0.00%,$0.00,$0.00,0.00,0.00,0,$0.00,0.00%
```

# Practical Considerations

- What type of actor are you?
- What is the target?
- How much effort did you put in?
- OPSEC
  - Possible but not easy



# Next Steps

- Ad Tech keeps changing
- Keywords matching on emails
  - Distribution Lists
  - Legacy Ad Tech
  - 3rd Party Apps

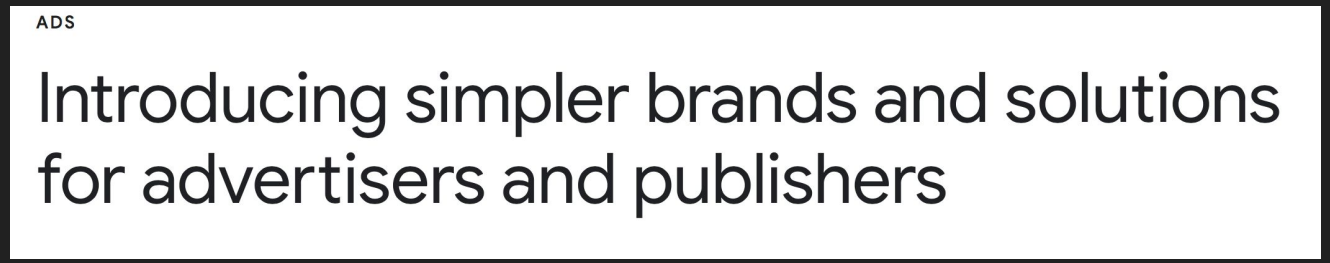


HOME > DIGITAL > NEWS

JUNE 23, 2017 12:43PM PT

**Google Will Keep Reading Your Emails, Just Not for Ads**

By JANKO ROETTGERS



ADS

Introducing simpler brands and solutions for advertisers and publishers

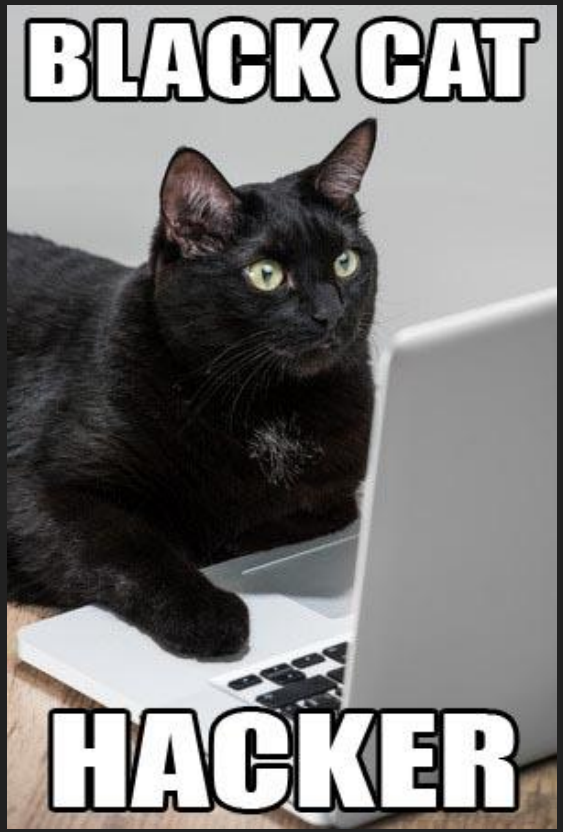


**Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail**

Software developers scan hundreds of millions of emails of users who sign up for email-based services

# Why do you care?

- Everything we do is tracked
- As Advertising evolves the barrier to entry lowers
- Let’s leverage the data for ourselves



# Thank You