

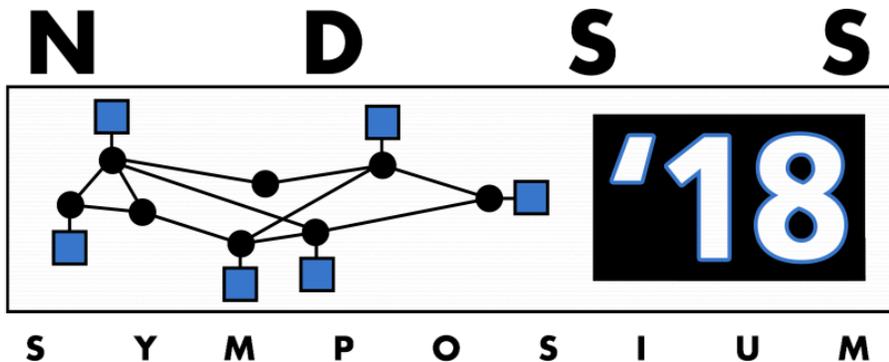
# Measuring and Disrupting Anti-Adblockers Using Differential Execution Analysis

Shitong Zhu<sup>\*</sup>, Xunchao Hu<sup>†</sup>, Zhiyun Qian<sup>\*</sup>, Zubair Shafiq<sup>‡</sup>, Heng Yin<sup>\*</sup>

<sup>\*</sup>University of California, Riverside

<sup>†</sup>Syracuse University

<sup>‡</sup>The University of Iowa



# What Is Happening?

[1] Ad blocking rapidly escalating, says researcher <https://www.networkworld.com/article/2397476/ads-blocking-rapidly-escalating-says-researcher.html>  
Shitong Zhu et al.



# Web Tracking & Ads

**Sponsored**  [See All](#)

**Consider Donating Sperm?**  
spermbank.com



Earn up to \$1200/mo and help people create families by donating your sperm today. Apply now: SPERMBANK.com

**Do You Want A Girlfriend?**



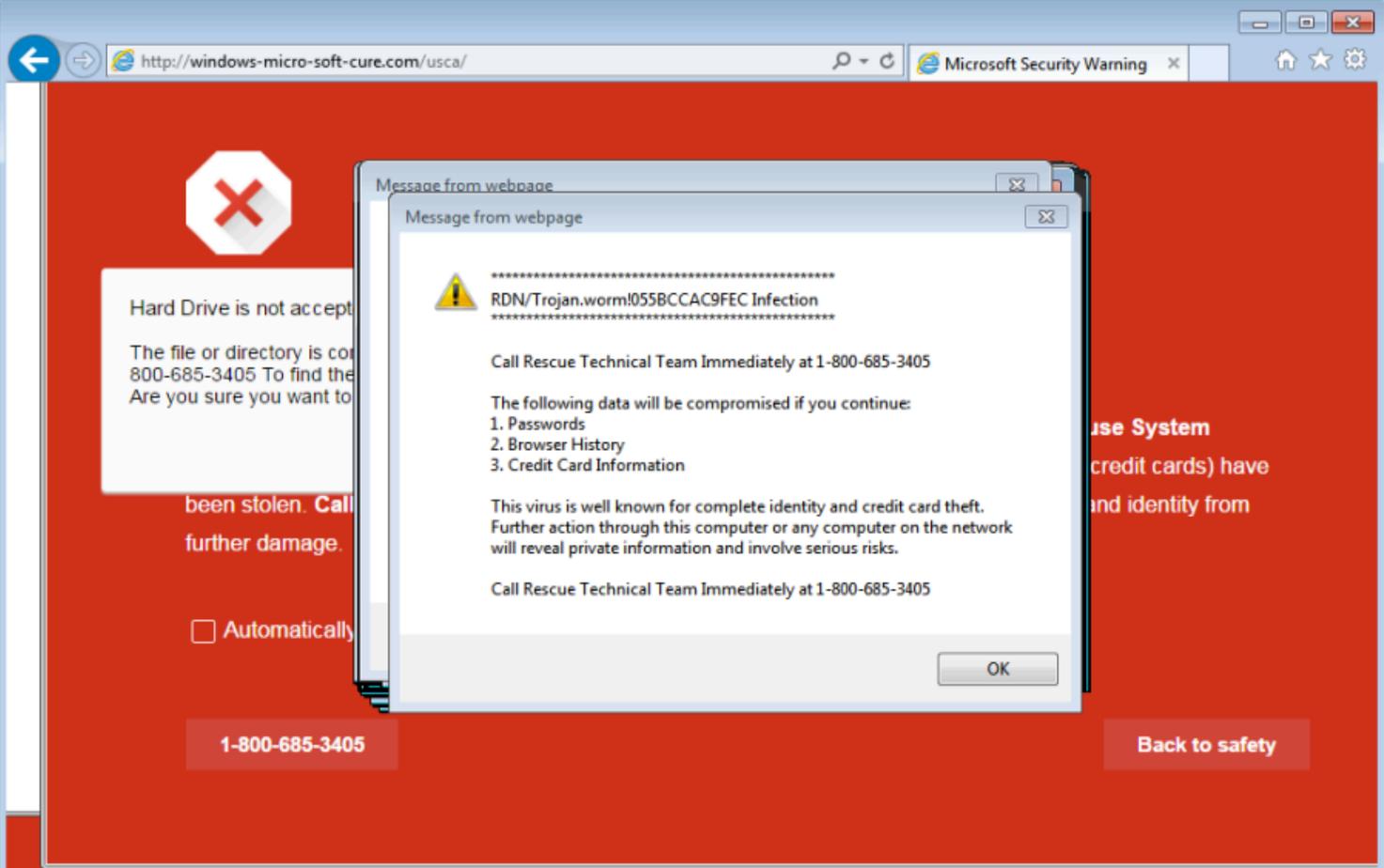
Then start dressing better. Our female stylist ships you mens accessories for \$60 a season

176 people like Curator & Mule.

**tracking-fueled/  
conciseness**

[2] 16 Creepiest Targeted Facebook Ads <http://mashable.com/2014/08/13/facebook-ads-creepy/#kulr6KVMaAqc>

# Or Worse, Malvertising



[3] RoughTed: the anti ad-blocker malvertiser <https://blog.malwarebytes.com/cybercrime/2017/05/rougthed-the-anti-ad-blocker-malvertiser/>  
Shitong Zhu et al.

# Ad Blockers To The Rescue!

**11%**  
of the global internet population is blocking ads on the web, Dec 2016

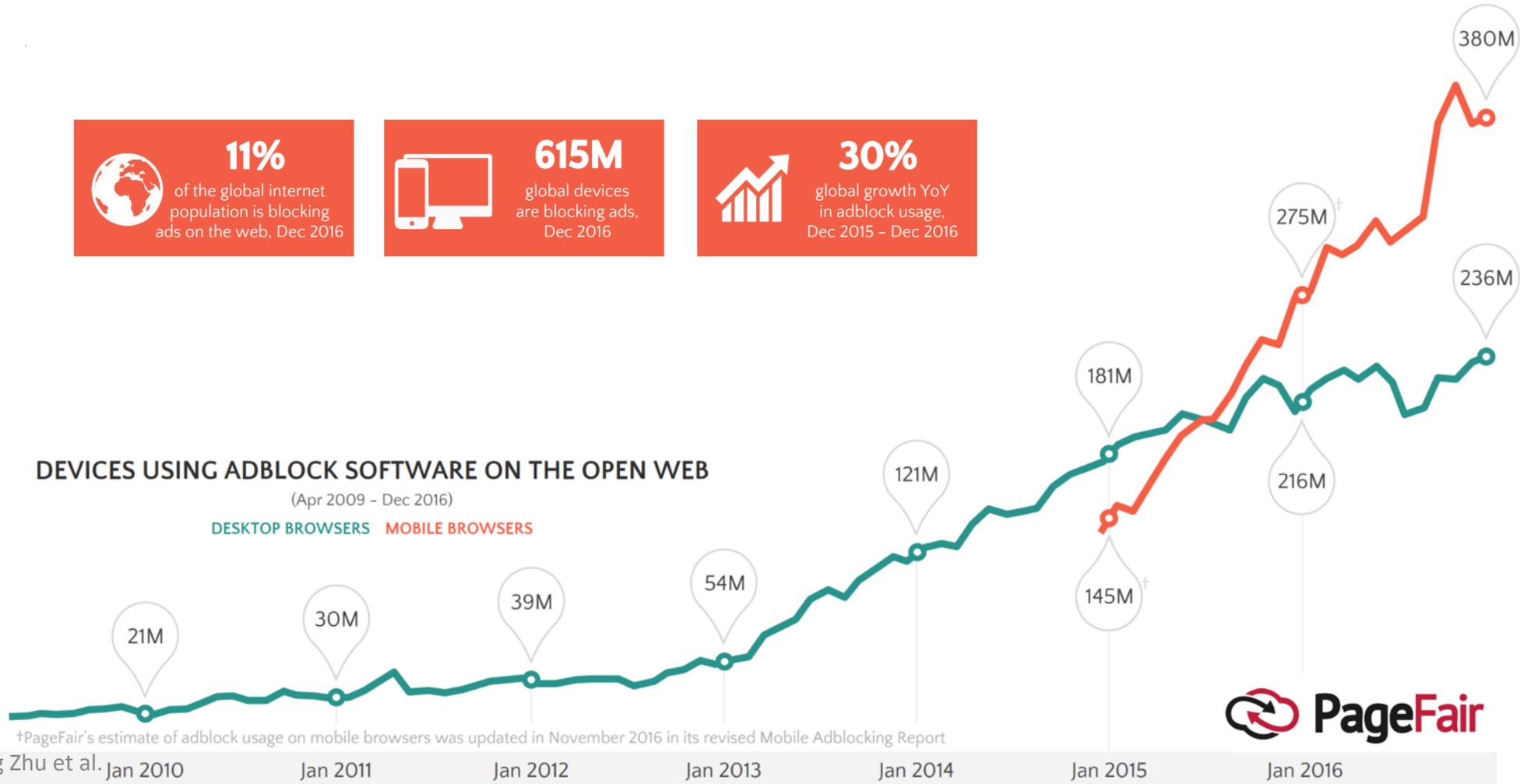
**615M**  
global devices are blocking ads, Dec 2016

**30%**  
global growth YoY in adblock usage, Dec 2015 - Dec 2016

## DEVICES USING ADBLOCK SOFTWARE ON THE OPEN WEB

(Apr 2009 - Dec 2016)

DESKTOP BROWSERS MOBILE BROWSERS

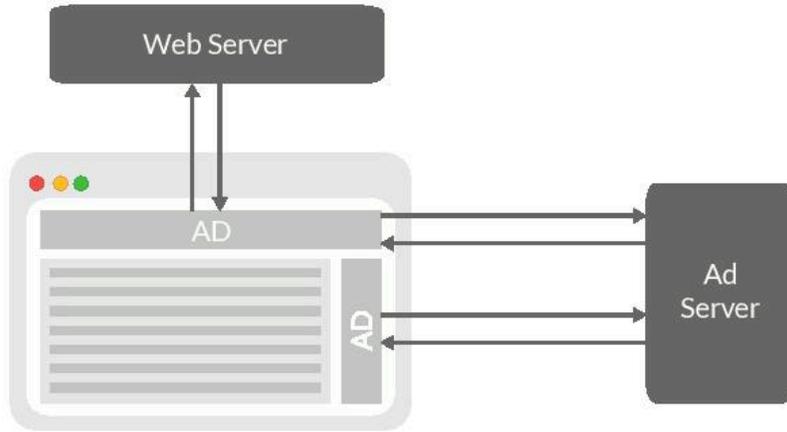


\*PageFair's estimate of adblock usage on mobile browsers was updated in November 2016 in its revised Mobile Adblocking Report

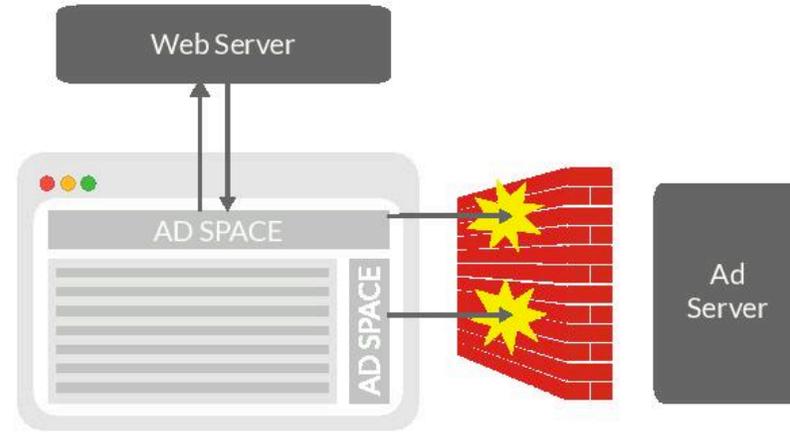


# How Ad blocking Works?

Regular User

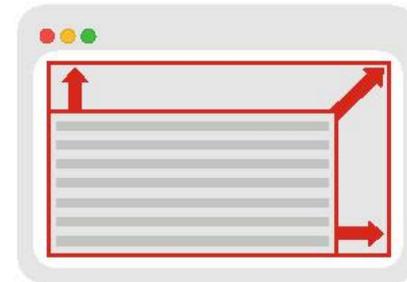


Adblock User



## PHASE 1

Blocks requests from browser to ad server



## PHASE 2

Reformats content to utilize empty ad space

# What Does Ads Industry Think/React?

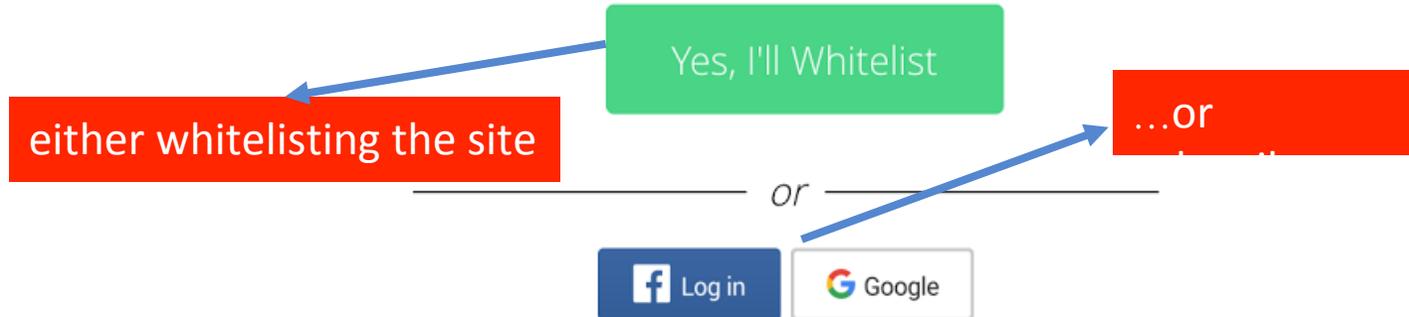
- In a word, not happy...
- Considers adblockers a serious threat to their business model
- Their move: deploying **Anti-Adblocker** that
  - (1) **detects** the presence of adblocker,
  - (2) **reacts** to adblocker by:
    - completely/partly blocking the real content
    - issuing warning messages
    - silently reporting adblocking status

# What Does Ads Industry Think/React?

[Forbes Login](#)



## Adblock Detected



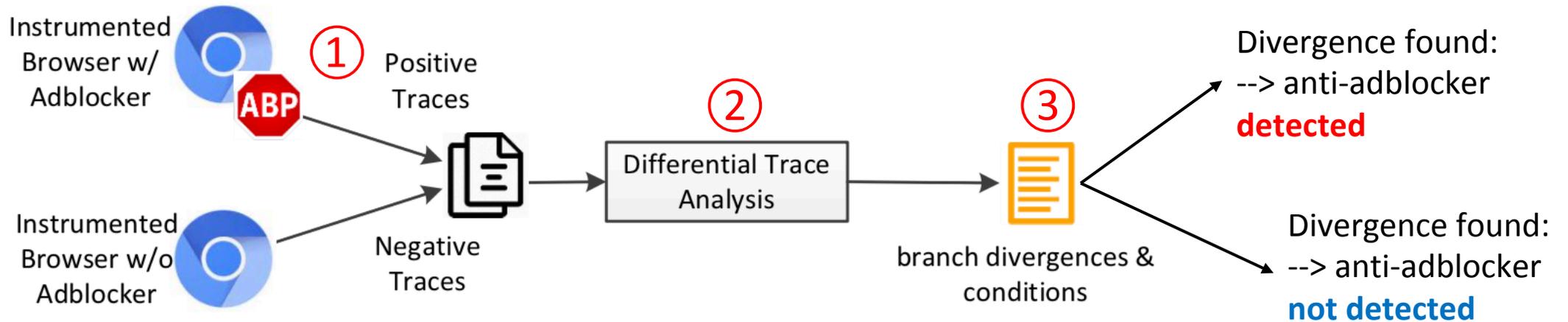
We will never post on your behalf without first obtaining your permission. By joining through Facebook or Google sign-up, you agree to the [Terms Of Membership](#) for all Forbes Media sites.

# Now, Our Turn?

- Already an escalating arms race, with no winner yet
- Goals:
  - 1) **we want to investigate the ongoing arms race**
  - 2) **with this knowledge, we want to escalate this arms race**
- Our prior work:
  - IMC '17: coverage of the current anti-adblock filter-list is NOT good (only ~9%)
  - PETS '17: A/B testing, **static** analysis (only for **visible** ones/**cannot** locate relevant code)
- Our latest move: **differential execution analysis**

# Our Idea & System

- Key observation: a website employing anti-adblocker would have a different JavaScript execution trace if it is loaded with adblocker (**positive** trace) as compared to without adblocker (**negative** trace)
- System overview:



# Differential Execution Analysis? What Is It?

- It's in general a long-awaited program analysis technique, but can be somehow implemented quite straightforward in our case:

```
if (!ad || ad.innerHTML.length == 0 || ad.  
    clientHeight === 0)  
    alert("We've detected an ad blocker running on  
        your browser." + ...);
```

- what will appear in our execution trace when we **enable** adblocker?

```
http://www.example.com/main.js IF 888  
http://www.example.com/main.js THEN 888
```

- what will appear in our execution trace when we **disable** it?

```
http://www.example.com/main.js IF 888
```

# How Good Is It?

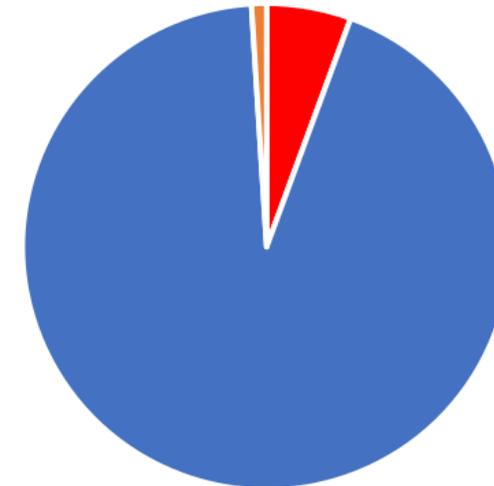
- On ground-truth datasets, our system achieves
  - **True Positive** rate: 86.9% | **False Positive** rate: 0%
- More information beyond the binary results

Divergence discovered: `http://www.example.com/main.js 888 w/adb ->` THEN `wo/adb ->` IF

```
if (!ad || ad.innerHTML.length == 0 || ad.  
    clientHeight === 0)  
    alert("We've detected an ad blocker running on  
        your browser." + ...);
```

# Large-Scale Analysis In The Wild

- Key finding:
  - we detected anti ad-blockers on **30.5%** of the Alexa top-10K websites which is **5-52** times more than reported in prior literature
- Why such a big gap?
  - remember that a typical anti-adblocker has two components:
    1. ad blocker detection
    2. subsequent reaction (**possibly silent**)



■ Visible ■ Silent Detection ■ Ads Switching

# Large-Scale Analysis In The Wild

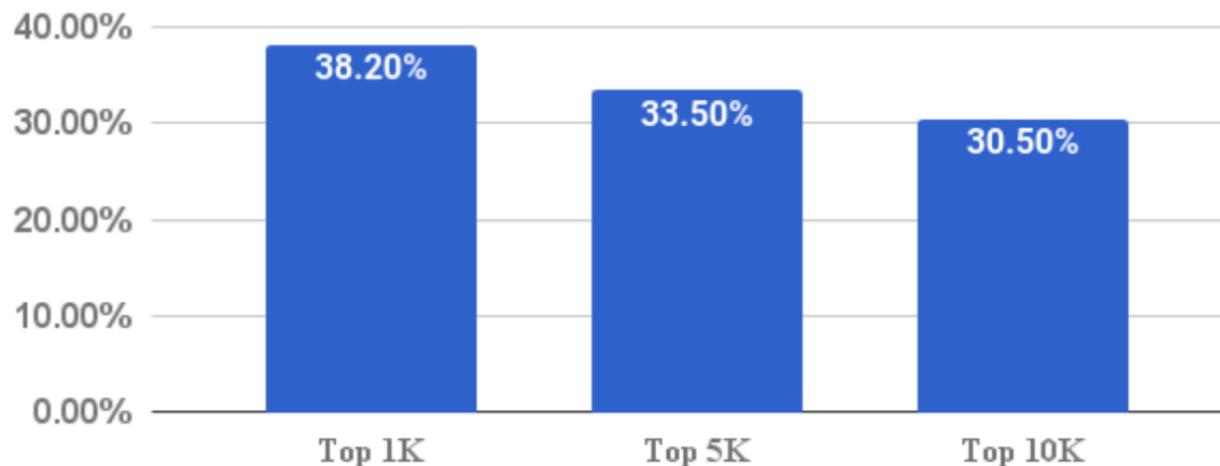
```
1 var blockStatus = 'Unblocked';
2 var ad = $('#adsense')[0];
3 if (!ad || ad.innerHTML.length == 0 || ad.
    clientHeight === 0) blockStatus = 'Blocked';
4 ga('send', 'event', 'Ad block JavaScript',
    blockStatus, 'Desktop', {nonInteraction: true});
5 ga('theLocalNetwork.send', 'event', 'Ad block
    JavaScript', blockStatus, 'Desktop', {
    nonInteraction: true});
```

# Other Findings

- Origins of top scripts containing anti-adblocking logic:



- Popularity of anti-adblockers by website ranking



# Improving Adblockers

- Avoiding Anti-adblockers with JavaScript Rewriting

```
1  if (hasBlock() && matches(StackTrace.getSync(),  
    recorded_stacktrace) && false) {  
2    $(' .notification' ).show();  
3  }
```

- Hiding Adblockers with API Hooking (stealthy adblocker)

- all API calls used by publisher scripts to examine the state of the page (e.g., whether an ad is visible) can be intercepted and modified by a browser extension

# Future

- Users should have the right to make a choice
- Alternative business models
  - Acceptable Ads program & Better Ads standards
  - Ads profit re-distribution: Brave browser

# Q & A

- Complementary Material
- <https://sites.google.com/view/antiadb-proj>

