Invalid Traffic & Viewability:
What is the cost of an unseen ad?

May 2016

Paul Barford
Chief Scientist

For info about the proprietary technology used in comScore products, refer to http://comscore.com/About_comScore/Patents
Overview

• Objectives
• Viewability
  – What & how
• Invalid traffic (IVT)
  – What are attackers doing?
• Ad blockers
• Counter measures
  – Detection, filtration and mitigation
• Recent measurements
  – Views, IVT, ad blockers
Measuring viewability

- Ad viewability: ads that appear within viewable space in a browser on a user’s screen
  - MRC standards
- Considerations
  - Screen size
  - Location of the browser
  - Location of the ad relative to the page
  - User actions including tab, scroll, minimize
A hybrid approach

- Both static and dynamic characteristics must be considered to produce accurate viewability measurements
- **Geometry**: consider X,Y coordinates of ad to determine it’s exact location in the viewport
- **Timing**: use clues associated with content to determine if creative is in-view
- Hybrid method enables broad coverage (97%) plus adaptability to browsing dynamics
The threat landscape

• What motivates ad fraud?
  – “Because that’s where the money is.” W. Sutton

• Fraudster’s advantages
  – Anonymity, vulnerabilities, complexity, scale
  – Humans in the loop

• Key requirement – a way to put $$ in the bank
  – Ad exchanges and DSPs are obvious opportunities
Who is harmed?

Brands | Agencies | Trading Desks | DSPs | Exchanges | SSPs | Networks | Publishers

Everyone
Attack vectors

Invalid traffic includes both clicks and impressions that Google suspects to not be the result of genuine user interest

• Invalid traffic falls into four general categories
  – Traffic generators – human & automated
  – Unwanted ads – plugins & injectors
  – Unseen ads – including popunders & PPV
  – Misrepresented placements – placement laundering

• Grey areas abound!
Traffic generation

- Valid traffic generation offerings
  - Adwords, Outbrain, BingAds, Facebook ads, etc.
- Type “purchase web traffic” in Google
  - MANY traffic generation offerings
- Simple threats: script-based page retrieval
  - Ubiquitous - $12/10K impressions
  - Not very human-like
- More complex threats: botnets*
  - Objective – look more “human”
  - As much as $100/10K impressions
Plugins and injectors

• Software that generates ads that are not part of publisher placements
  – Most do not try to hide
• Plugins enhance native browser functionality
  – PageRage, BuzzDock, Sambreel, etc.
• Injectors impose ads other than or in addition to those intended
  – Trick users by promising extended functionality
  – Google: say 5% of their users have an ad injector
  – Superfish, JollyWallet, etc.
What about bots?

• Bots have been around for a long time
  – Originally developed in 90’s to manage host
  – Compromised hosts under the control of remote entity
• Bots are characterized by key capabilities
  – Impressions and injection
• Example: Athena botnet
  – Various ad viewing capabilities
• But, why bother with a botnet?
  – Clouds are better…

Unseen ads and PPV nets

• Ads that appear in invisible frames
  – Simple additions to web pages that can be “viewable”
  – Many not be 0-size, but still invisible
  – Often appear as pupup’s/popunders

• PPV network: groups of sites that run tags from a single TG service
  – Some TG services offer a JS tag that when included on a site pays attractive CPM
  – “…will not block any of your site content…”
  – Tag will “display” camouflaged 3rd party websites

Placement laundering

Placement laundering is the act of sending false information to an ad provider about an ad placement

• How do we know who is requesting an ad or where it’s placed?
  – We typically rely on trust and Javascript
• “Domain laundering” coined by comScore’s Jeff Kline in ’14
  – Recent press release with Google on vulnerability in Safeframe
• Key issue: Low quality ad: $0.01 CPM, High quality ad: $10 CPM

Ad blockers on the rise

- Ad blockers (browser extensions) have received significant attention over the past year
  - Blockers have been available for over a decade
  - “…ad blocking is robbery, plain and simple” R. Rothenberg, AdAge
- Blockers are here to stay, what can we do?
  - Measure and assess their prevalence and impact
  - Develop technical counter-measures
  - Take control of the narrative on responsible advertising
Addressing the threats

• Basic issues are similar to IT security
  – Need to understand (evolving) threats
  – Detection vs. mitigation
  – Tools and processes for decision support and remediation

• Core components for addressing ad fraud
  – Diverse measurement capability
  – Filters to identify/mitigate threats
  – Tools for visualization and forensics
Start with telemetry

• Objective: breadth and depth
  – Any specific measurement method has limits!
• Challenges: scale, diversity and dynamics
• Census/Ad tags: for a wide variety of threats
  – Careful attention to errors/failures
• Panel: for plugins, injectors, traffic generators and publisher side threats
• Crawler: for publisher side threats
• Honeypots: for traffic generation threats
From telemetry to filters

• Objective: accurate, efficient threat identification
• Approach: mine diverse telemetry for signals
  – Hypothesis-based, iterative process
• Write code (i.e., filter) that isolates signals in telemetry associated with fraud
  – General vs. sophisticated
  – Detection vs. active mitigation
• comScore has over 25 different IVT filters

Raw Q1 ’16: impressions/IVT

Gross Impressions
Percent IVT

Jan
Feb
Mar

0% 1% 2% 3% 4% 5%

10,000,000,000 20,000,000,000 30,000,000,000 40,000,000,000 50,000,000,000 60,000,000,000 70,000,000,000 80,000,000,000
Raw Q1 ’16: regional imprsn/IVT

North America

Europe

comScore Inc. Proprietary
Norms Q1 ‘16: IVT

US, desktop

January
February
March

Display
Video

comScore Inc. Proprietary
Norms Q1 ‘16: in-view

US, desktop

- Display
- Video

January
February
March

comScore Inc. Proprietary
Norms Q1 ‘16: direct/indirect
Conclusion

• Summary
  – Your ads may not be seen
    • Viewability has a fixed objective
    • IVT detection and mitigation is a moving target
    • Ad blockers are having an impact
  – Diverse telemetry + data science can address threats

• Q: What is the cost? A: Depends on where you advertise

• Future
  – Broad deployment of active mitigation
  – Anti-ad blocking
  – Cross media
Thank you